Documentazione NetApp HCI

HCI

NetApp
December 22, 2023

Sommario

Documentazione NetApp HCI

Soluzioni NetApp HCI

Le soluzioni NetApp HCI possono aiutarti a ottenere performance su larga scala con carichi di lavoro multipli sulla stessa infrastruttura senza alcun attrito.

NetApp HCI ti consente di implementare servizi cloud in più cloud provider pubblici e on-premise. Puoi utilizzare NetApp HCI per implementare servizi simili a quelli che potresti fare con un cloud provider, il tutto in una modalità self-service senza il coinvolgimento DELL'IT.

Per ulteriori informazioni sulle soluzioni NetApp HCI, consultare "Documentazione sulle soluzioni NetApp HCI".

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"

Note di rilascio

Novità di NetApp HCI

NetApp aggiorna periodicamente NetApp HCI per offrire nuove funzionalità, miglioramenti e correzioni di bug. NetApp HCI 1.9P1 include il software NetApp Element 12.3.1 per i cluster di storage.

> L'elemento 12.3.2 contiene la mitigazione che chiude l'esposizione del software Element alla vulnerabilità di Apache Log4j. I cluster di storage NetApp SolidFire con la funzione volumi virtuali (VVol) attivata sono esposti a questa vulnerabilità.
>
> Se il cluster di storage si trova all'elemento 12.3.1 e la funzione VVol è attivata, è necessario eseguire l'aggiornamento al software Element 12.3.2.
>
> Se il cluster di storage si trova su Element 12.3.1 e la funzione VVols è disattivata, l'aggiornamento al software Element 12.3.2 è facoltativo.
>
> NetApp sconsiglia l'esecuzione di versioni a elementi misti in un cluster, ad eccezione della durata dell'aggiornamento.

- Il NetApp HCI 1.9P1 La sezione descrive le nuove funzioni e gli aggiornamenti di NetApp HCI versione 1.9P1.
- Il Elemento 12.3.1 La sezione descrive le nuove funzionalità e gli aggiornamenti di NetApp Element 12.3.1.

NetApp HCI 1.9P1

NetApp HCI 1.9P1 include miglioramenti di sicurezza e stabilità.

Elemento 12.3.1

NetApp HCI 1.9P1 include Element 12.3.1 per cluster di storage.

Bundle firmware per lo storage 2.99.2

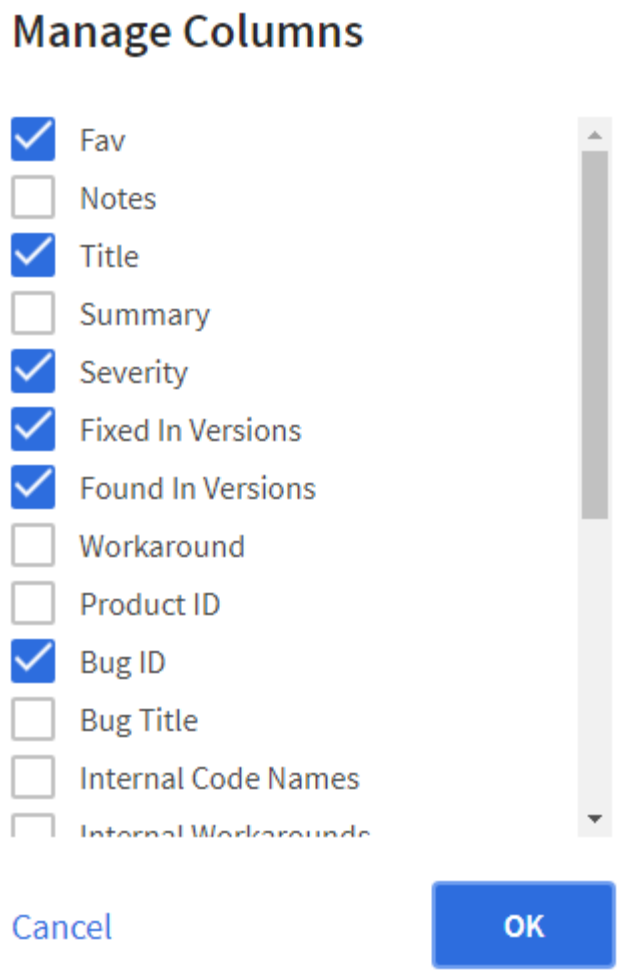
La release Element 12.3.1 include la versione 2.99.2 del bundle firmware di storage. Se il cluster di storage è già in Element 12.3, è possibile installare semplicemente il nuovo bundle firmware 2.99.2.

NetApp Bugs Online contiene problemi noti e risolti

I problemi noti e risolti sono elencati nel tool NetApp Bugs Online. È possibile consultare questi problemi per Element e altri prodotti all'indirizzo "NetApp Bugs Online".

Fasi

1. Passare a. "NetApp Bugs Online".
2. Nel campo **Cerca per parola chiave**, digitare il nome del prodotto, ad esempio "elemento".
3. Selezionare  , Selezionare il filtro **Fixed in Versions** e selezionare **OK**.



4. Selezionare **Nuova ricerca**.
5. Digitare la versione della release nel campo **fixed in Versions**.

Trova ulteriori informazioni

- "Note sulla versione di NetApp Hybrid Cloud Control and Management Services"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"
- "Documentazione software SolidFire ed Element"
- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Ulteriori informazioni sulla release

È possibile trovare collegamenti alle note di rilascio più recenti e precedenti per i vari componenti dell'ambiente di storage NetApp HCI ed Element.

Ti verrà richiesto di effettuare l'accesso utilizzando le credenziali del sito di supporto NetApp.

NetApp HCI

- "NetApp HCI 1.9P1 - Note di rilascio"
- "Note sulla versione di NetApp HCI 1.9"
- "NetApp HCI 1.8P1 - Note di rilascio"
- "Note sulla versione di NetApp HCI 1.8"
- "NetApp HCI 1.7P1 - Note di rilascio"

Software NetApp Element

- "Note sulla versione del software NetApp Element 12.3.2"
- "Note sulla versione del software NetApp Element 12.3.1"
- "Note sulla versione del software NetApp Element 12.3"
- "Note sulla versione del software NetApp Element 12.2.1"
- "Note sulla versione del software NetApp Element 12.2"
- "Note sulla versione del software NetApp Element 12.0.1"
- "Note sulla versione del software NetApp Element 12.0"
- "Note sulla versione del software NetApp Element 11.8"
- "Note sulla versione del software NetApp Element 11.7"
- "Note sulla versione del software NetApp Element 11.5.1"
- "Note sulla versione del software NetApp Element 11.3P1"

Servizi di gestione

- "Note sulla versione di Management Services"

Plug-in NetApp Element per server vCenter

- "VCenter Plug-in 5,2 - Note sulla versione" *NUOVO*
- "Note sulla versione di vCenter Plug-in 5.1"
- "Note sulla versione di vCenter Plug-in 5.0"
- "Note sulla versione di vCenter Plug-in 4.10"
- "Note sulla versione di vCenter Plug-in 4.9"
- "Note sulla versione di vCenter Plug-in 4.8"
- "Note sulla versione di vCenter Plug-in 4.7"
- "Note sulla versione di vCenter Plug-in 4.6"
- "Note sulla versione di vCenter Plug-in 4.5"
- "Note sulla versione di vCenter Plug-in 4.4"
- "Note sulla versione di vCenter Plug-in 4.3"

Firmware di calcolo

- "Note sulla versione di Compute firmware Bundle 2.146"
- "Note sulla versione di Compute firmware Bundle 2.76"
- "Note sulla versione di Compute firmware Bundle 2.27"
- "Note sulla versione di Compute firmware Bundle 12.2.109"
- "Versioni del firmware e dei driver ESXi supportate"

Firmware dello storage

- "Note sulla versione di Storage firmware Bundle 2.146"
- "Note sulla versione di Storage firmware Bundle 2.99.2"
- "Note sulla versione di Storage firmware Bundle 2.76"
- "Note sulla versione di Storage firmware Bundle 2.27"
- "H610S BMC 3.84.07 Release Notes"
- "Versioni del firmware e dei driver ESXi supportate"

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>" class="bare">https://<ManagementNodeIP>; </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"
- "Pagina delle risorse NetApp HCI"
- "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

- "Pagina delle risorse NetApp HCI"
- "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"
- "Pagina delle risorse NetApp HCI"
- "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

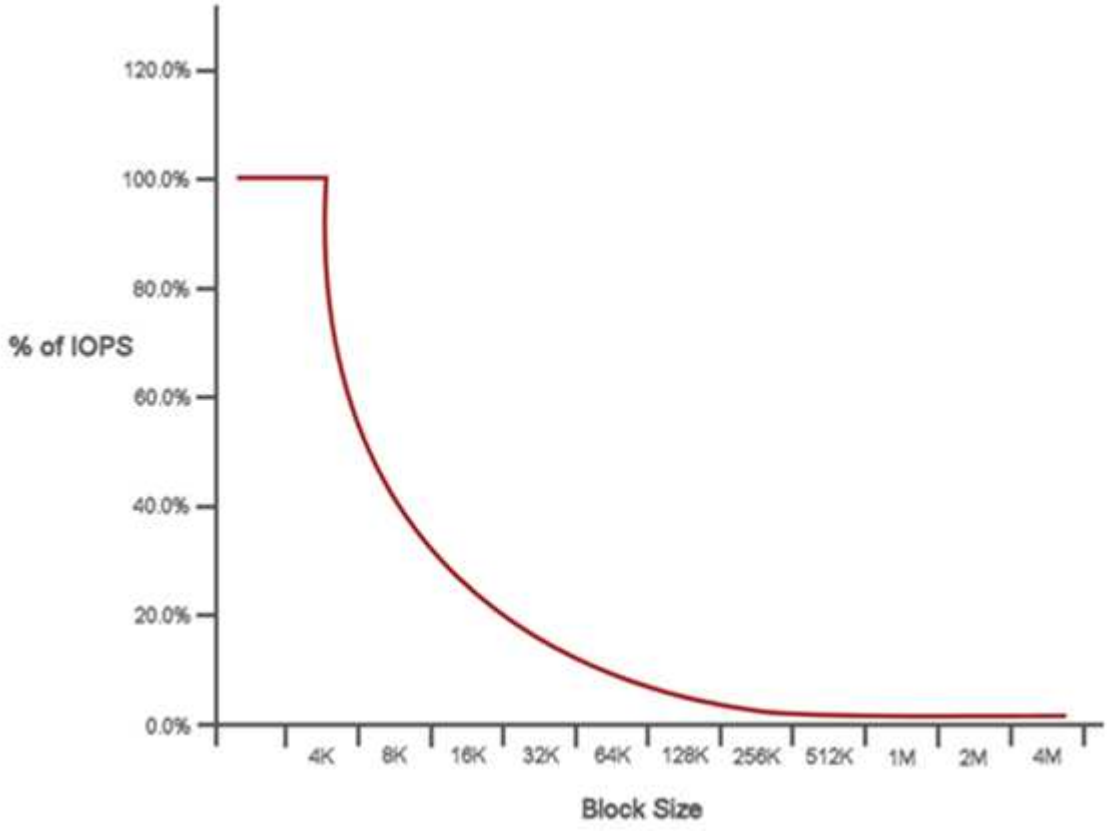
*Queste stime sono approssimative. **È possibile impostare IOPS massimi e IOPS burst fino a 200,000; tuttavia, questa impostazione consente solo di rimuovere efficacemente le prestazioni di un volume. Le performance massime reali di un volume sono limitate dall'utilizzo del cluster e dalle performance 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"

Requisiti e attività di pre-implementazione

Panoramica dei requisiti per l'implementazione di NetApp HCI

NetApp HCI presenta requisiti fisici e di rete specifici per il corretto funzionamento del data center. Assicurarsi di implementare i seguenti requisiti e consigli prima di iniziare l'implementazione.

Prima di ricevere l'hardware NetApp HCI, assicurarsi di completare gli elementi della checklist nel manuale di pre-implementazione dei servizi professionali NetApp. Questo documento contiene un elenco completo delle attività da completare per preparare la rete e l'ambiente per una corretta implementazione di NetApp HCI.

Di seguito sono riportati i collegamenti ai requisiti e alle attività di pre-implementazione:

- "Requisiti delle porte di rete"
- "Requisiti di rete e switch"
- "Requisiti dei cavi di rete"
- "Requisiti dell'indirizzo IP"
- "Configurazione di rete"
- "DNS e requisiti di conservazione dei tempi"
- "Requisiti ambientali"
- "Domini di protezione"
- "Requisiti di risorse di Witness Node per cluster di storage a due nodi"

Trova ulteriori informazioni

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

Requisiti dei nodi di gestione

Come Best practice, associare un solo nodo di gestione a un'istanza di VMware vCenter ed evitare di definire le stesse risorse di storage e calcolo o istanze di vCenter in più nodi di gestione. La definizione delle stesse risorse in più nodi di gestione può causare problemi come la creazione di report sulle risorse non corretti in NetApp ActiveIQ.

Requisiti delle porte di rete

Potrebbe essere necessario consentire le seguenti porte attraverso il firewall edge del data center in modo da poter gestire il sistema in remoto, consentire ai client esterni al data center di connettersi alle risorse e garantire il corretto funzionamento dei servizi interni. Alcune di queste porte, URL o indirizzi IP potrebbero non essere necessari, a seconda delle modalità di utilizzo del sistema.

Tutte le porte sono TCP, se non diversamente specificato, e tutte le porte TCP devono supportare la comunicazione handshake a tre vie tra il server di supporto NetApp, il nodo di gestione e i nodi che eseguono il software Element. Ad esempio, l'host su un'origine del nodo di gestione comunica con l'host su una destinazione MVIP del cluster di storage attraverso la porta TCP 443, e l'host di destinazione comunica nuovamente con l'host di origine attraverso qualsiasi porta.

Nella tabella vengono utilizzate le seguenti abbreviazioni:

- MIP: Indirizzo IP di gestione, un indirizzo per nodo
- SIP: Indirizzo IP dello storage, un indirizzo per nodo
- MVIP: Indirizzo IP virtuale di gestione
- SVIP: Indirizzo IP virtuale dello storage

Origine	Destinazione	Porta	Descrizione
Nodo di calcolo BMC/IPMI	Nodo di gestione	111 TCP/UDP	Comunicazione API di NetApp Hybrid Cloud Control
Nodo di calcolo BMC/IPMI	Nodo di gestione	137-138 UDP	Comunicazione API di NetApp Hybrid Cloud Control
Nodo di calcolo BMC/IPMI	Nodo di gestione	445	Comunicazione API di NetApp Hybrid Cloud Control
Nodo di calcolo BMC/IPMI	Nodo di gestione	623 UDP	Porta RMCP (Remote Management Control Protocol). Richiesto per gli aggiornamenti del firmware di calcolo di NetApp Hybrid Cloud Control.
Nodo di calcolo BMC/IPMI	Nodo di gestione	2049 TCP/UDP	Comunicazione API di NetApp Hybrid Cloud Control
Client iSCSI	Cluster di storage MVIP	443	(Facoltativo) accesso all'interfaccia utente e alle API
Client iSCSI	Cluster di storage SVIP	3260	Comunicazioni iSCSI del client
Client iSCSI	SIP. Nodo storage	3260	Comunicazioni iSCSI del client
Nodo di gestione	`sfsupport.solidfire.com`	22	Tunnel SSH inverso per l'accesso al supporto
Nodo di gestione	MIP nodo storage	22	Accesso SSH per il supporto
Nodo di gestione	Server DNS	53 TCP/UDP	Ricerca DNS

Origine	Destinazione	Porta	Descrizione
Nodo di gestione	Nodo di calcolo BMC/IPMI	139	Comunicazione API di NetApp Hybrid Cloud Control
Nodo di gestione	MIP nodo storage	442	Accesso API e UI agli aggiornamenti del software Element e del nodo di storage
Nodo di gestione	Nodo storage MVIP	442	Accesso API e UI agli aggiornamenti del software Element e del nodo di storage
Nodo di gestione	`23.32.54.122`, `216.240.21.15`	443	Aggiornamenti del software Element
Nodo di gestione	BMC (Baseboard Management Controller)	443	Monitoraggio dell'hardware e connessione all'inventario (comandi Redfish e IPMI)
Nodo di gestione	Nodo di calcolo BMC/IPMI	443	Comunicazione HTTPS di NetApp Hybrid Cloud Control
Nodo di gestione	`monitoring.solidfire.com`	443	Report del cluster di storage a Active IQ
Nodo di gestione	Cluster di storage MVIP	443	Accesso API e UI agli aggiornamenti del software Element e del nodo di storage
Nodo di gestione	VMware vCenter	443	Comunicazione HTTPS di NetApp Hybrid Cloud Control
Nodo di gestione	Nodo di calcolo BMC/IPMI	623 UDP	Porta RMCP (Remote Management Control Protocol). Richiesto per gli aggiornamenti del firmware di calcolo di NetApp Hybrid Cloud Control.
Nodo di gestione	Nodo di storage BMC/IPMI	623 UDP	Porta RMCP. Questo è necessario per gestire i sistemi abilitati IPMI.
Nodo di gestione	VMware vCenter	5988-5989	Comunicazione HTTPS di NetApp Hybrid Cloud Control
Nodo di gestione	Nodo di controllo	9442	Servizio API di configurazione per nodo

Origine	Destinazione	Porta	Descrizione
Nodo di gestione	Server vCenter	9443	Registrazione del plug-in vCenter. La porta può essere chiusa al termine della registrazione.
Server SNMP	Cluster di storage MVIP	161 UDP	Polling SNMP
Server SNMP	MIP nodo storage	161 UDP	Polling SNMP
Nodo di storage BMC/IPMI	Nodo di gestione	623 UDP	Porta RMCP. Questo è necessario per gestire i sistemi abilitati IPMI.
MIP nodo storage	Server DNS	53 TCP/UDP	Ricerca DNS
MIP nodo storage	Nodo di gestione	80	Aggiornamenti del software Element
MIP nodo storage	Endpoint S3/Swift	80	(Opzionale) comunicazione HTTP con l'endpoint S3/Swift per backup e ripristino
MIP nodo storage	Server NTP	123 UDP	NTP
MIP nodo storage	Nodo di gestione	162 UDP	(Facoltativo) trap SNMP
MIP nodo storage	Server SNMP	162 UDP	(Facoltativo) trap SNMP
MIP nodo storage	Server LDAP	389 TCP/UDP	(Facoltativo) Ricerca LDAP
MIP nodo storage	Nodo di gestione	443	Aggiornamenti del software Element
MIP nodo storage	Cluster di storage remoto MVIP	443	Comunicazione di accoppiamento del cluster di replica remota
MIP nodo storage	MIP nodo storage remoto	443	Comunicazione di accoppiamento del cluster di replica remota
MIP nodo storage	Endpoint S3/Swift	443	(Opzionale) comunicazione HTTPS con l'endpoint S3/Swift per backup e ripristino
MIP nodo storage	Server LDAPS	636 TCP/UDP	Ricerca LDAPS
MIP nodo storage	Nodo di gestione	10514 TCP/UDP, 514 TCP/UDP	Inoltro syslog
MIP nodo storage	Server syslog	10514 TCP/UDP, 514 TCP/UDP	Inoltro syslog
MIP nodo storage	MIP nodo storage remoto	2181	Comunicazione tra cluster per la replica remota

Origine	Destinazione	Porta	Descrizione
SIP. Nodo storage	Endpoint S3/Swift	80	(Opzionale) comunicazione HTTP con l'endpoint S3/Swift per backup e ripristino
SIP. Nodo storage	SIP. Nodo di calcolo	442	API del nodo di calcolo, configurazione e convalida e accesso all'inventario software
SIP. Nodo storage	Endpoint S3/Swift	443	(Opzionale) comunicazione HTTPS con l'endpoint S3/Swift per backup e ripristino
SIP. Nodo storage	SIP. Nodo storage remoto	2181	Comunicazione tra cluster per la replica remota
SIP. Nodo storage	SIP. Nodo storage	3260	ISCSI internodo
SIP. Nodo storage	SIP. Nodo storage remoto	da 4000 a 4020	Trasferimento dei dati da nodo a nodo per la replica remota
PC dell'amministratore di sistema	MIP nodo storage	80	(Solo NetApp HCI) pagina iniziale del motore di implementazione NetApp
PC dell'amministratore di sistema	Nodo di gestione	442	Accesso dell'interfaccia utente HTTPS al nodo di gestione
PC dell'amministratore di sistema	MIP nodo storage	442	Accesso API e interfaccia utente HTTPS al nodo di storage (solo NetApp HCI) monitoraggio della configurazione e dell'implementazione nel motore di implementazione NetApp
PC dell'amministratore di sistema	Nodo di calcolo serie BMC/IPMI H410 e H600	443	Accesso API e interfaccia utente HTTPS al controllo remoto del nodo
PC dell'amministratore di sistema	Nodo di gestione	443	Accesso API e interfaccia utente HTTPS al nodo di gestione
PC dell'amministratore di sistema	Cluster di storage MVIP	443	Accesso API e interfaccia utente HTTPS al cluster di storage
PC dell'amministratore di sistema	Nodo storage serie BMC/IPMI H410 e H600	443	Accesso API e interfaccia utente HTTPS al controllo remoto del nodo

Origine	Destinazione	Porta	Descrizione
PC dell'amministratore di sistema	MIP nodo storage	443	Creazione di cluster di storage HTTPS, accesso UI post-implementazione al cluster di storage
PC dell'amministratore di sistema	Nodo di calcolo serie BMC/IPMI H410 e H600	623 UDP	Porta RMCP. Questo è necessario per gestire i sistemi abilitati IPMI.
PC dell'amministratore di sistema	Nodo storage serie BMC/IPMI H410 e H600	623 UDP	Porta RMCP. Questo è necessario per gestire i sistemi abilitati IPMI.
PC dell'amministratore di sistema	Nodo di controllo	8080	Interfaccia utente Web nodo di controllo per nodo
Server vCenter	Cluster di storage MVIP	443	Accesso all'API del plug-in vCenter
Server vCenter	Plug-in remoto	8333	Servizio Remote vCenter Plug-in
Server vCenter	Nodo di gestione	8443	(Facoltativo) servizio QoSSIOC vCenter Plug-in.
Server vCenter	Cluster di storage MVIP	8444	Accesso al provider vCenter VASA (solo VVol)
Server vCenter	Nodo di gestione	9443	Registrazione del plug-in vCenter. La porta può essere chiusa al termine della registrazione.

Trova ulteriori informazioni

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

Requisiti di rete e switch

Gli switch utilizzati per NetApp HCI richiedono una configurazione specifica per garantire una corretta implementazione. Consultare la documentazione dello switch per istruzioni specifiche sull'implementazione di ciascuno dei seguenti requisiti per il proprio ambiente.

Un'implementazione NetApp HCI richiede almeno tre segmenti di rete, uno per ciascuno dei seguenti tipi di traffico:

- Gestione
- VMware vMotion
- Storage/dati

A seconda dei modelli di nodi di calcolo e storage NetApp H-Series e della configurazione di cablaggio

pianificata, è possibile separare fisicamente queste reti utilizzando switch separati o separarle logicamente utilizzando VLAN. Per la maggior parte delle implementazioni, tuttavia, è necessario separare logicamente queste reti (e qualsiasi altra rete di macchine virtuali aggiuntiva) utilizzando VLAN.

I nodi di calcolo e storage devono essere in grado di comunicare prima, durante e dopo l'implementazione. Se si stanno implementando reti di gestione separate per i nodi di storage e di calcolo, assicurarsi che tali reti di gestione dispongano di percorsi di rete tra di esse. A queste reti devono essere assegnati gateway e deve essere presente un percorso tra i gateway. Assicurarsi che ogni nuovo nodo disponga di un gateway assegnato per facilitare la comunicazione tra i nodi e le reti di gestione.

NetApp HCI ha i seguenti requisiti di switch:

- Tutte le porte dello switch collegate ai nodi NetApp HCI devono essere configurate come porte edge spanning tree.
  - Sugli switch Cisco, a seconda del modello dello switch, della versione del software e del tipo di porta, è possibile eseguire questa operazione con uno dei seguenti comandi:
    - `spanning-tree port type edge`
    - `spanning-tree port type edge trunk`
    - `spanning-tree portfast`
    - `spanning-tree portfast trunk`
  - Sui centralini Mellanox, è possibile eseguire questa operazione con `spanning-tree port type edge` comando.
- I nodi NetApp HCI dispongono di porte ridondanti per tutte le funzioni di rete, ad eccezione della gestione fuori banda. Per ottenere la massima resilienza, dividere queste porte su due switch con uplink ridondanti in un'architettura gerarchica tradizionale o in un'architettura di livello 2.
- Gli switch che gestiscono lo storage, la macchina virtuale e il traffico vMotion devono supportare velocità di almeno 10 GbE per porta (sono supportati fino a 25 GbE per porta).
- Gli switch che gestiscono il traffico di gestione devono supportare velocità di almeno 1 GbE per porta.
- È necessario configurare i frame jumbo sulle porte dello switch che gestiscono lo storage e il traffico vMotion. Gli host devono essere in grado di inviare pacchetti da 9000 byte end-to-end per una corretta installazione.
- È necessario configurare le porte dello switch di rete di gestione in modo da consentire a MTU di qualsiasi dimensione le porte NIC di gestione su ciascun host siano configurate. Ad esempio, se le porte della rete di gestione degli host utilizzano una dimensione MTU di 1750 byte, le porte dello switch della rete di gestione devono essere configurate in modo da consentire almeno un MTU di 1750 byte (la rete di gestione non richiede un MTU di 9000 byte). Le impostazioni MTU devono essere coerenti end-to-end
- La latenza di rete di andata e ritorno tra tutti i nodi di storage e di calcolo non deve superare i 2 ms.

Tutti i nodi NetApp HCI offrono funzionalità di gestione out-of-band aggiuntive tramite una porta di gestione dedicata. NETAPP H300S, H300E, H500S, H500E, H700S, I nodi H700E e H410C consentono anche l'accesso IPMI tramite la porta A. Come Best practice, dovresti semplificare la gestione remota di NetApp HCI configurando la gestione out-of-band per tutti i nodi del tuo ambiente.

Trova ulteriori informazioni

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

Requisiti dei cavi di rete

È possibile utilizzare le seguenti linee guida per assicurarsi di disporre di un numero sufficiente di cavi di rete adeguati alle dimensioni dell'implementazione. Per le porte RJ45, è necessario utilizzare cavi con grado di protezione Cat 5e o Cat 6.

- Configurazione del nodo di calcolo a due cavi: Ciascun nodo di calcolo deve essere collegato a una rete 10 GbE tramite due interfacce SFP+/SFP28 (un cavo Cat 5e/6 aggiuntivo è opzionale per la gestione fuori banda).
- Configurazione del nodo di calcolo a sei cavi: Ciascun nodo di calcolo deve essere collegato a una rete 10/25GbE tramite quattro interfacce SFP+/SFP28 e a una rete 1/10GbE tramite due cavi Cat 5e/6 (un cavo Cat 5e/6 aggiuntivo è opzionale per la gestione fuori banda).
- Ciascun nodo storage deve essere collegato a una rete 10/25GbE tramite due interfacce SFP+/SFP28 e a una rete 1/10GbE tramite due cavi Cat 5e/6 (un cavo Cat 5e/6 aggiuntivo è opzionale per la gestione fuori banda).
- Assicurarsi che i cavi di rete utilizzati per collegare il sistema NetApp HCI alla rete siano sufficientemente lunghi per raggiungere comodamente gli switch.

Ad esempio, un'implementazione contenente quattro nodi di storage e tre nodi di calcolo (utilizzando la configurazione a sei cavi) richiede il seguente numero di cavi di rete:

- (14) cavi Cat 5e/6 con connettori RJ45 (più sette cavi per traffico IPMI, se necessario)
- (20) cavi twinax con connettori SFP28/SFP+

Ciò è dovuto ai seguenti motivi:

- Quattro nodi storage richiedono otto (8) cavi Cat 5e/6 e otto (8) cavi Twinax.
- Tre nodi di calcolo che utilizzano la configurazione a sei cavi richiedono sei (6) cavi Cat 5e/6 e dodici (12) cavi Twinax.

> In una configurazione a sei cavi, due porte sono riservate per VMware ESXi e configurate e gestite dal NetApp Deployment Engine. Non è possibile accedere o gestire queste porte dedicate a ESXi utilizzando la TUI Element o la GUI web Element.

Trova ulteriori informazioni

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

Requisiti dell'indirizzo IP

NetApp HCI presenta requisiti specifici per gli indirizzi IP che dipendono dalle dimensioni dell'implementazione. Per impostazione predefinita, gli indirizzi IP iniziali assegnati a ciascun nodo prima di utilizzare NetApp Deployment Engine per implementare il sistema sono temporanei e non possono essere riutilizzati. È necessario mettere da parte un secondo set permanente di indirizzi IP inutilizzati che è possibile assegnare durante l'implementazione finale.

Numero di indirizzi IP necessari per l'implementazione di NetApp HCI

La rete di storage e la rete di gestione NetApp HCI devono utilizzare intervalli contigui di indirizzi IP separati. Utilizzare la seguente tabella per determinare il numero di indirizzi IP necessari per l'implementazione:

Componente del sistema	Gestione degli indirizzi IP di rete necessari	Sono necessari gli indirizzi IP della rete di storage	Sono necessari indirizzi IP di rete VMotion	Totale indirizzi IP necessari per componente
Nodo di calcolo	1	2	1	4
Nodo storage	1	1		2
Cluster di storage	1	1		2
VMware vCenter	1			1
Nodo di gestione	1	1		2
Nodo di controllo	1	1		2 per nodo di controllo (due nodi di controllo sono implementati per ogni cluster di storage a due o tre nodi)

Indirizzi IP riservati da NetApp HCI

NetApp HCI si riserva i seguenti intervalli di indirizzi IP per i componenti del sistema. Durante la pianificazione della rete, evitare di utilizzare questi indirizzi IP:

Intervallo di indirizzi IP	Descrizione
10.0.0.0/24	Rete Docker overlay
10.0.1.0/24	Rete Docker overlay
10.255.0.0/16	Rete di ingresso "swarm" di Docker
169.254.100.1/22	Rete Docker Bridge
169.254.104.0/22	Rete Docker Bridge

Trova ulteriori informazioni

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

Configurazione di rete

Configurazione di rete

NetApp HCI può utilizzare diversi cablaggi di rete e configurazioni VLAN. È importante pianificare la configurazione di rete per garantire un'implementazione corretta.

Segmenti di rete richiesti

NetApp HCI richiede un minimo di tre segmenti di rete: Traffico di gestione, storage e virtualizzazione (che include macchine virtuali e traffico VMware vMotion). È inoltre possibile separare la macchina virtuale e il traffico vMotion. Questi segmenti di rete solitamente esistono come VLAN separate logicamente nell'infrastruttura di rete NetApp HCI.

Il modo in cui i nodi di calcolo e storage si connettono a queste reti dipende dal modo in cui si progetta la rete e si cablano i nodi. Le illustrazioni di esempio di rete di questa guida presuppongono le seguenti reti:

Nome di rete	ID VLAN
Gestione	100
Storage	105
VMotion	107
Macchine virtuali	200, 201

Per il rilevamento e la configurazione automatici dei nodi NetApp HCI nel motore di implementazione NetApp, è necessario disporre di un segmento di rete disponibile come VLAN nativa o senza tag su tutte le porte switch utilizzate per le interfacce SFP+/SFP28 sui nodi. In questo modo si otterrà una comunicazione di livello 2 tra tutti i nodi per il rilevamento e l'implementazione. Senza una VLAN nativa, è necessario configurare manualmente le interfacce SFP+/SFP28 di tutti i nodi con un indirizzo VLAN e IPv4 da individuare. Negli esempi di configurazione di rete riportati in questo documento, viene utilizzata la rete di gestione (ID VLAN 100).

NetApp Deployment Engine consente di configurare rapidamente le reti per i nodi di calcolo e storage durante l'implementazione iniziale. È possibile posizionare alcuni componenti di gestione integrati come vCenter e il nodo di gestione sul proprio segmento di rete. Questi segmenti di rete richiedono il routing per consentire a vCenter e al nodo di gestione di comunicare con le reti di gestione dello storage e del calcolo. Nella maggior parte delle implementazioni, questi componenti utilizzano la stessa rete di gestione (ID VLAN 100 in questo esempio).

> È possibile configurare le reti di macchine virtuali utilizzando vCenter. La rete della macchina virtuale predefinita (gruppo di porte "VM_Network") nelle implementazioni NetApp HCI è configurata senza un ID VLAN. Se si prevede di utilizzare più reti di macchine virtuali con tag (ID VLAN 200 e 201 nell'esempio precedente), assicurarsi di includerle nella pianificazione iniziale della rete.

Configurazione di rete e opzioni di cablaggio

È possibile utilizzare una configurazione di rete a due cavi per i nodi di calcolo H410C, semplificando il routing dei cavi. Questa configurazione utilizza due interfacce SFP+/SFP28 più un'interfaccia RJ45 opzionale (ma consigliata) per la comunicazione IPMI. Questi nodi possono anche utilizzare una configurazione a sei cavi con due interfacce RJ45 e quattro interfacce SFP28/SFP+.

I nodi di storage H410S e H610S supportano una topologia di rete che utilizza quattro porte di rete (porte Da A a D).

I nodi di calcolo supportano tre topologie di rete, a seconda della piattaforma hardware:

Opzione di configurazione	Cablaggio per nodi H410C	Cablaggio per nodi H610C	Cablaggio per nodi H615C
Opzione A.	Due cavi che utilizzano le porte D ed e	Due cavi che utilizzano le porte C e D.	Due cavi che utilizzano le porte A e B.
Opzione B	Sei cavi che utilizzano le porte Da A a F.	Non disponibile	Non disponibile
Opzione C	Simile all'opzione B, ma con VLAN native (o "porte di accesso") sullo switch per le reti di gestione, storage e vMotion		

I nodi che non dispongono del numero corretto di cavi collegati non possono partecipare all'implementazione. Ad esempio, non è possibile implementare un nodo di calcolo in una configurazione a sei cavi se ha solo porte D ed e connesse.

È possibile regolare la configurazione di rete NetApp HCI dopo l'implementazione per soddisfare le esigenze dell'infrastruttura. Tuttavia, quando si espandono le risorse NetApp HCI, tenere presente che i nuovi nodi devono avere la stessa configurazione via cavo dei nodi di calcolo e storage esistenti.

Se il NetApp Deployment Engine si guasta perché la rete non supporta i frame jumbo, è possibile eseguire una delle seguenti soluzioni alternative:

- Utilizzare un indirizzo IP statico e impostare manualmente una MTU (Maximum Transmission Unit) di 9000 byte sulla rete Bond10G.
- Configurare il Dynamic host Configuration Protocol in modo che annunci un MTU di interfaccia di 9000 byte sulla rete Bond10G.

Opzioni di configurazione di rete

- "Opzione Di configurazione di rete A"
- "Opzione di configurazione di rete B"
- "Opzione di configurazione di rete C"

Trova ulteriori informazioni

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

Configurazione di rete

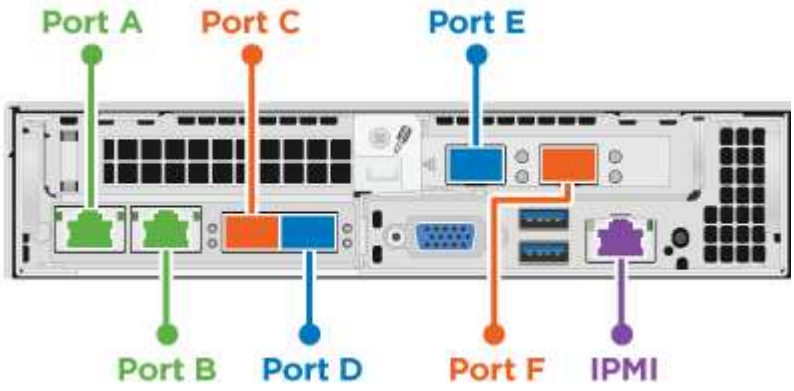
NetApp HCI può utilizzare diversi cablaggi di rete e configurazioni VLAN. La prima configurazione, opzione A, utilizza due cavi di rete per ciascun nodo di calcolo.

Opzione di configurazione A: Due cavi per nodi di calcolo

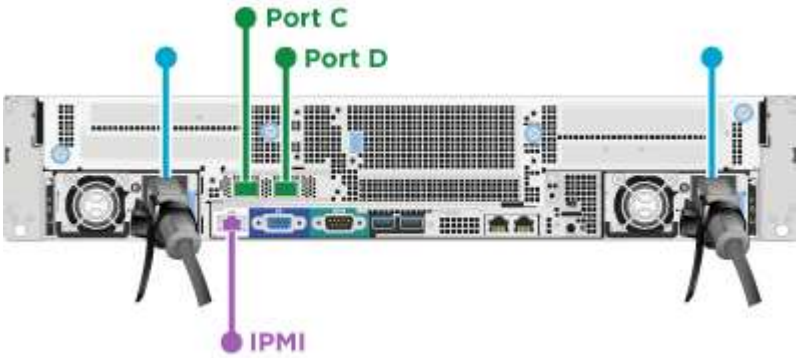
I nodi di calcolo NetApp H410C, H610C e H615C supportano l'utilizzo di due cavi di rete per la connettività a tutte le reti NetApp HCI. Questa configurazione richiede che lo storage, vMotion e qualsiasi rete di macchine virtuali utilizzino il tagging VLAN. Tutti i nodi di calcolo e storage devono utilizzare lo stesso schema di ID VLAN. Questa configurazione utilizza gli switch distribuiti vSphere che richiedono la licenza VMware vSphere Enterprise Plus.

La documentazione NetApp HCI utilizza lettere per fare riferimento alle porte di rete sul pannello posteriore dei nodi della serie H.

Di seguito sono riportate le porte e le posizioni di rete sul nodo di storage H410C:



Di seguito sono riportate le porte e le posizioni di rete sul nodo di calcolo H610C:



Di seguito sono riportate le porte e le posizioni di rete sul nodo di calcolo H615C:

Questa configurazione utilizza le seguenti porte di rete su ciascun nodo:

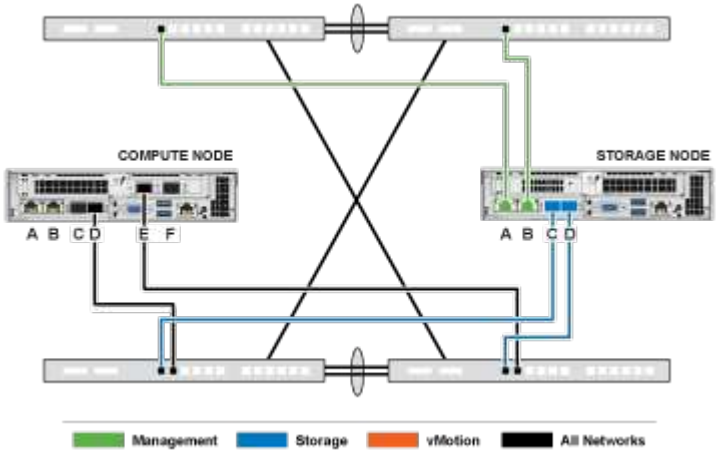
Nodo	Porte di rete utilizzate
H410C	D ed e
H610C	C e D
H615C	A e B.

Configurazione della VLAN

Come Best practice, è necessario configurare i segmenti di rete richiesti su tutte le porte dello switch utilizzate dai nodi. Ad esempio:

Nome di rete	ID VLAN	Configurazione della porta dello switch
Gestione	100	Nativo
Storage	105	Con tag
VMotion	107	Con tag
Macchine virtuali	200, 201	Con tag

La seguente illustrazione mostra la configurazione di cablaggio consigliata per nodi di calcolo H410C a due cavi e nodi storage H410S a quattro cavi. Tutte le porte dello switch in questo esempio condividono la stessa configurazione.



Esempio di comandi di commutazione

È possibile utilizzare i seguenti comandi di esempio per configurare tutte le porte dello switch utilizzate per i nodi NetApp HCI. Questi comandi si basano su una configurazione Cisco, ma potrebbero richiedere solo piccole modifiche per essere applicati agli switch Mellanox. Consultare la documentazione dello switch per i comandi specifici necessari per implementare questa configurazione. Sostituire il nome dell'interfaccia, la descrizione e le VLAN con i valori dell'ambiente.

```
interface {interface name, such as EthernetX/Y or GigabitEthernetX/Y/Z}
description {desired description, such as NetApp-HCI-NodeX-PortY}
mtu 9216
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 105,107,200,201
spanning-tree port type edge trunk
```

> Alcuni switch potrebbero richiedere l'inclusione della VLAN nativa nell'elenco delle VLAN consentite. Consultare la documentazione relativa al modello e alla versione software dello switch in uso.

Trova ulteriori informazioni

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

Configurazione di rete

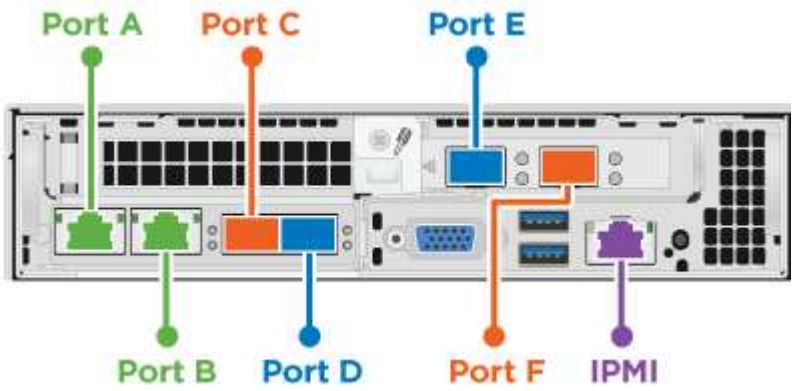
NetApp HCI può utilizzare diversi cablaggi di rete e configurazioni VLAN. La prima configurazione, opzione B, utilizza sei cavi di rete per ciascun nodo di calcolo.

Opzione di configurazione B: Sei cavi per nodi di calcolo

Come opzione di configurazione di rete secondaria, i nodi di calcolo H410C supportano l'utilizzo di sei cavi di rete per la connettività a tutte le reti NetApp HCI. Questa configurazione richiede che lo storage, vMotion e qualsiasi rete di macchine virtuali utilizzino il tagging VLAN. È possibile utilizzare questa configurazione con vSphere Standard Switch o vSphere Distributed Switch (che richiedono la licenza VMware vSphere Enterprise Plus).

La documentazione NetApp HCI utilizza lettere per fare riferimento alle porte di rete sul pannello posteriore dei nodi della serie H.

Di seguito sono riportate le porte e le posizioni di rete sul nodo di calcolo H410C:

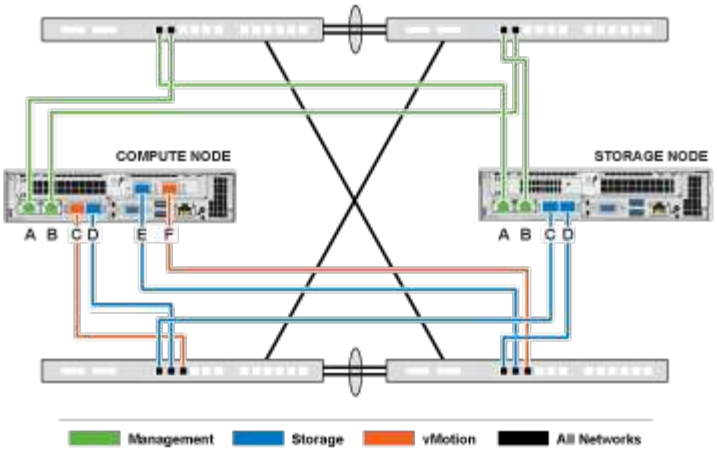


Configurazione della VLAN

Quando si implementano nodi di calcolo utilizzando sei cavi e nodi di storage utilizzando quattro cavi, come Best practice, è necessario configurare i segmenti di rete richiesti su tutte le porte dello switch utilizzate dai nodi. Ad esempio:

Nome di rete	ID VLAN	Configurazione della porta dello switch
Gestione	100	Nativo
Storage	105	Con tag
VMotion	107	Con tag
Macchine virtuali	200, 201	Con tag

La seguente illustrazione mostra la configurazione di cablaggio consigliata per nodi di calcolo a sei cavi e nodi storage a quattro cavi. Tutte le porte dello switch in questo esempio condividono la stessa configurazione.



Esempio di comandi di commutazione

È possibile utilizzare i seguenti comandi di esempio per configurare tutte le porte dello switch utilizzate per i nodi NetApp HCI. Questi comandi si basano su una configurazione Cisco, ma potrebbero richiedere solo piccole modifiche per essere applicati agli switch Mellanox. Consultare la documentazione dello switch per i comandi specifici necessari per implementare questa configurazione. Sostituire il nome dell'interfaccia, la descrizione e le VLAN con i valori dell'ambiente.

```
interface {interface name, such as EthernetX/Y or GigabitEthernetX/Y/Z}
description {desired description, such as NetApp-HCI-NodeX-PortY}
mtu 9216
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 105,107,200,201
spanning-tree port type edge trunk
```

> Alcuni switch potrebbero richiedere l'inclusione della VLAN nativa nell'elenco delle VLAN consentite. Consultare la documentazione relativa al modello e alla versione software dello switch in uso.

Trova ulteriori informazioni

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

Configurazione di rete

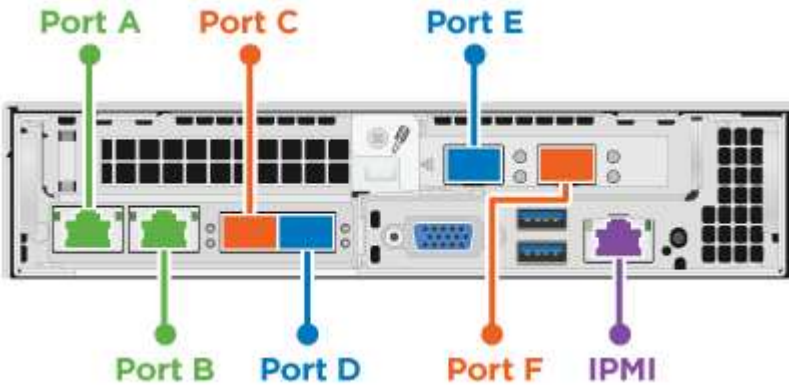
NetApp HCI può utilizzare diversi cablaggi di rete e configurazioni VLAN. La terza configurazione, opzione C, utilizza sei cavi di rete per ciascun nodo di calcolo con VLAN native.

Opzione di configurazione C: Sei cavi per nodi di calcolo con VLAN native

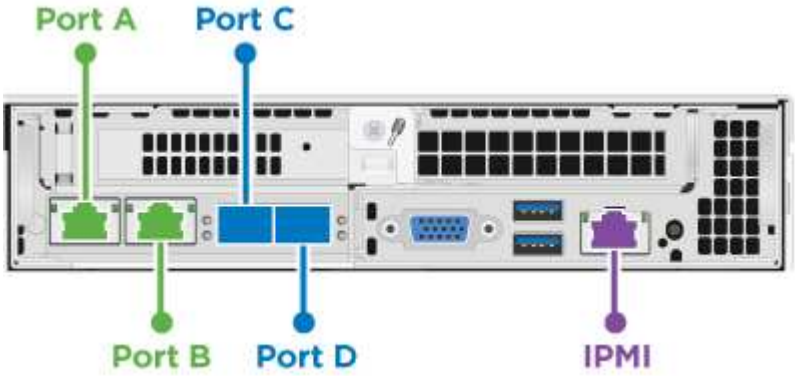
È possibile implementare NetApp HCI senza utilizzare VLAN taggate per il traffico di storage e virtualizzazione e affidarsi invece alla configurazione dello switch per separare i segmenti di rete. È possibile utilizzare questa configurazione con vSphere Standard Switch o vSphere Distributed Switch (che richiedono la licenza VMware vSphere Enterprise Plus).

La documentazione NetApp HCI utilizza lettere per fare riferimento alle porte di rete sul pannello posteriore dei nodi della serie H.

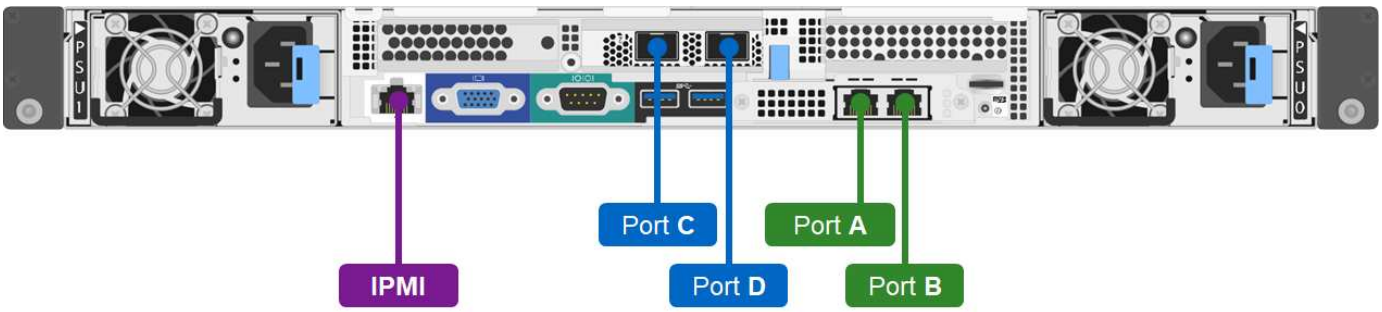
Di seguito sono riportate le porte e le posizioni di rete sul nodo di storage H410C:



Di seguito sono riportate le porte e le posizioni di rete sul nodo di storage H410S:



Di seguito sono riportate le porte e le posizioni di rete sul nodo di storage H610S:



Configurazione della VLAN per i nodi H410C, H410S e H610S

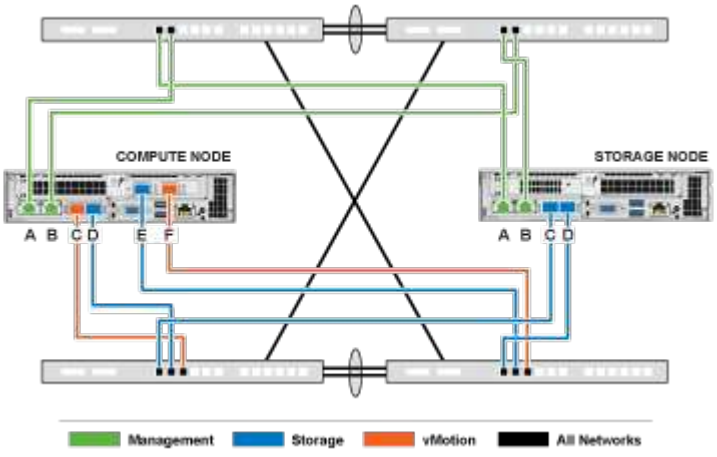
Questa opzione di topologia utilizza la seguente configurazione VLAN sui nodi H410C, H410S e H610S:

Porte del nodo utilizzate	Nome di rete	ID VLAN	Configurazione della porta dello switch collegato
Porte A e B su nodi di calcolo e storage	Gestione	100	Nativo

Porte del nodo utilizzate	Nome di rete	ID VLAN	Configurazione della porta dello switch collegato
Porte D ed e su nodi di calcolo	Storage	105	Nativo
Porte C e D sui nodi di storage	Storage	105	Nativo
Porte C e F su nodi di calcolo	VMotion	107	Nativo
Porte C e F su nodi di calcolo	Macchine virtuali	200, 201	Con tag

Durante l'implementazione di questa configurazione, fare attenzione a configurare le porte dello switch. Gli errori di configurazione in questa topologia di rete possono causare problemi di implementazione difficili da diagnosticare.

La figura seguente mostra la panoramica della configurazione di rete per questa opzione di topologia. Nell'esempio, le porte dei singoli switch sono configurate con il segmento di rete appropriato come rete nativa.



Esempio di comandi di commutazione

È possibile utilizzare i seguenti comandi switch di esempio per configurare le porte dello switch utilizzate per i nodi NetApp HCI. Questi comandi si basano su una configurazione Cisco, ma potrebbero richiedere solo modifiche minime per essere applicati agli switch Mellanox. Consultare la documentazione dello switch per i comandi specifici necessari per implementare questa configurazione.

È possibile utilizzare i seguenti comandi di esempio per configurare le porte dello switch utilizzate per la rete di gestione. Sostituire il nome dell'interfaccia, la descrizione e le VLAN con i valori della configurazione.

```
switchport access vlan 100
spanning-tree port type edge
```

È possibile utilizzare i seguenti comandi di esempio per configurare le porte dello switch utilizzate per la rete di storage. Sostituire il nome dell'interfaccia, la descrizione e le VLAN con i valori della configurazione.

```
mtu 9216
```

```
switchport access vlan 105
spanning-tree port type edge
```

È possibile utilizzare i seguenti comandi di esempio per configurare le porte dello switch utilizzate per la rete di macchine virtuali e vMotion. Sostituire il nome dell'interfaccia, la descrizione e le VLAN con i valori della configurazione.

```
interface {interface name, such as EthernetX/Y or GigabitEthernetX/Y/Z}
description {desired description, such as NetApp-HCI-NodeX-PortC|F}
mtu 9216
switchport mode trunk
switchport trunk native vlan 107
switchport trunk allowed vlan 200,201
spanning-tree port type edge trunk
```

> Alcuni switch potrebbero richiedere l'inclusione della VLAN nativa nell'elenco delle VLAN consentite. Consultare la documentazione relativa al modello e alla versione software dello switch in uso.

Trova ulteriori informazioni

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

DNS e requisiti di conservazione dei tempi

Prima dell'implementazione, è necessario preparare i record DNS (Domain Name System) per il sistema NetApp HCI e raccogliere le informazioni sul server NTP. NetApp HCI richiede un server DNS con le voci DNS corrette e un server NTP per una corretta implementazione.

Prima di implementare NetApp HCI, eseguire le seguenti operazioni di preparazione per il server DNS e il timer:

- Creare eventuali voci DNS necessarie per gli host (ad esempio singoli nodi di calcolo o storage) e documentare il modo in cui le voci host vengono associate ai rispettivi indirizzi IP. Durante l'implementazione, sarà necessario assegnare un prefisso al cluster di storage che verrà applicato a ciascun host; per evitare confusione, tenere a mente i piani di denominazione DNS quando si sceglie un prefisso.
- Se si implementa NetApp HCI con una nuova installazione di VMware vSphere utilizzando un nome di dominio completo, è necessario creare un record di puntatore (PTR) e un record di indirizzo (A) per vCenter Server su qualsiasi server DNS in uso prima dell'implementazione.
- Se si implementa NetApp HCI con una nuova installazione vSphere utilizzando solo indirizzi IP, non è necessario creare nuovi record DNS per vCenter.
- NetApp HCI richiede un server NTP valido per la conservazione dei tempi. Se non si dispone di un server di riferimento orario, è possibile utilizzare un server di riferimento orario pubblico.
- Assicurarsi che tutti i clock dei nodi di calcolo e di storage siano sincronizzati tra loro e che gli orologi dei dispositivi utilizzati per accedere a NetApp HCI siano sincronizzati con i nodi NetApp HCI.

Trova ulteriori informazioni

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

Requisiti ambientali

Assicurarsi che l'alimentazione per il rack utilizzato per installare NetApp HCI sia fornita da prese di alimentazione CA e che il data center fornisca un raffreddamento adeguato alle dimensioni dell'installazione NetApp HCI.

Per informazioni dettagliate sulle funzionalità di ciascun componente di NetApp HCI, consultare la NetApp HCI "scheda informativa".

> Il nodo di calcolo H410C funziona solo con tensione di linea elevata (200-240 VCA). Quando si aggiungono nodi H410C a un'installazione NetApp HCI esistente, è necessario assicurarsi che i requisiti di alimentazione siano soddisfatti.

Trova ulteriori informazioni

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

Domini di protezione

Supporto del software NetApp Element "domini di protezione" che ottimizza il layout dei dati sui nodi di storage per la migliore disponibilità dei dati. Per utilizzare questa funzionalità, è necessario suddividere la capacità dello storage in modo uniforme su tre o più chassis NetApp serie H per un'affidabilità dello storage ottimale. In questo scenario, il cluster di storage attiva automaticamente i domini di protezione.

Trova ulteriori informazioni

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

Requisiti di risorse di Witness Node per cluster di storage a due nodi

NetApp HCI supporta una dimensione minima di installazione di due nodi di storage e due nodi di calcolo. Quando si installa NetApp HCI utilizzando un cluster di storage a due o tre nodi, è necessario conoscere i nodi di controllo NetApp HCI e i requisiti delle risorse delle macchine virtuali (VM).

Quando un cluster di storage utilizza due o tre nodi, implementa anche una coppia di nodi di controllo accanto a ciascun cluster di storage. I nodi di controllo hanno i seguenti requisiti relativi alle risorse delle macchine virtuali:

Risorsa	Requisito
VCPU	4
Memoria	12 GB
Dimensioni del disco	67 GB

NetApp HCI supporta solo alcuni modelli di nodi di storage in cluster di storage a due o tre nodi. Per ulteriori informazioni, consultare le note di rilascio relative alla versione di NetApp HCI in uso.

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).

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

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

Inizia a utilizzare NetApp HCI

Panoramica dell'installazione e dell'implementazione di NetApp HCI

Seguire queste istruzioni per installare e implementare NetApp HCI. Queste istruzioni includono collegamenti a ulteriori dettagli.

Ecco una panoramica del processo:

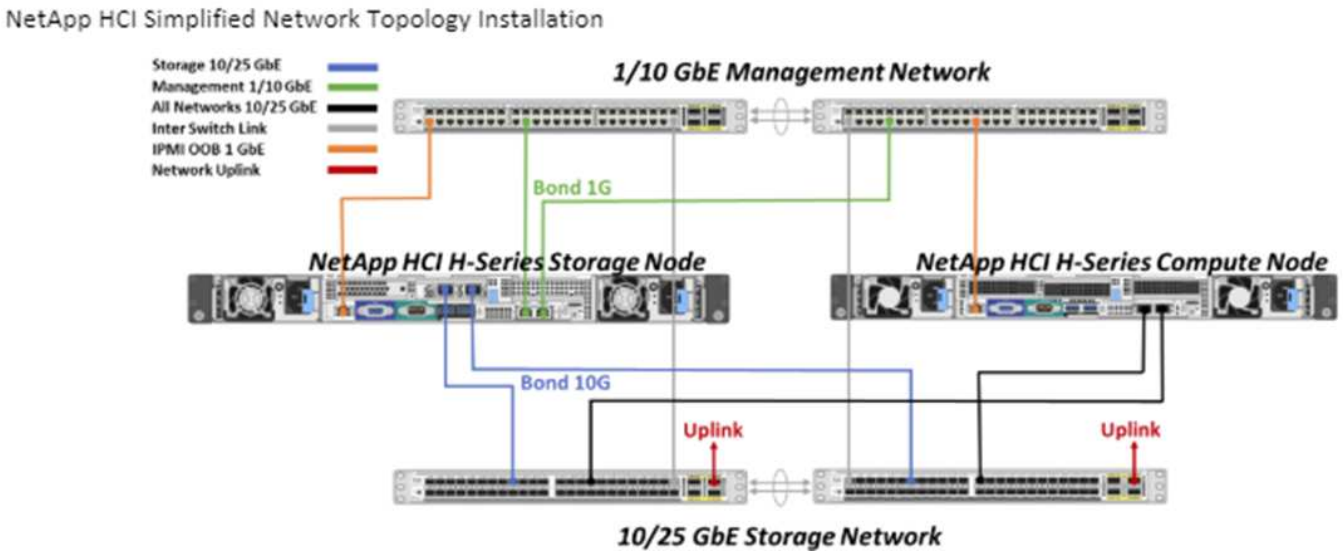
- Preparazione per l'installazione
- Convalida la preparazione della rete con NetApp Active IQ Config Advisor
- Collabora con il tuo team NetApp
- Installare l'hardware NetApp HCI
- Completare le attività opzionali dopo l'installazione dell'hardware
- Implementare NetApp HCI utilizzando il motore di implementazione NetApp (NDE)
- Gestire NetApp HCI utilizzando il plug-in vCenter
- Monitorare o aggiornare NetApp HCI con il controllo del cloud ibrido

Preparazione per l'installazione

Prima di iniziare l'installazione, completare l'elenco di controllo prima del volo del *Workbook di rilevamento dell'installazione di NetApp HCI* inviato prima di ricevere l'hardware.

Preparare la rete e i siti di installazione

Di seguito viene illustrata un'installazione semplificata della topologia di rete NetApp HCI:



Si tratta della topologia di rete semplificata per un singolo nodo di storage e un singolo nodo di calcolo. Il cluster minimo per NetApp HCI è costituito da due nodi di storage e due nodi di calcolo.

> La topologia di rete potrebbe essere diversa da quella illustrata qui. Questo è solo un esempio.

Questa configurazione utilizza due cavi di rete sui nodi di calcolo per la connettività a tutte le reti NetApp HCI.

Leggi queste risorse:

- Utilizzare la *Guida al rilevamento dell'installazione di NetApp HCI* per configurare la rete prima dell'installazione.
- Per informazioni dettagliate e altre configurazioni supportate, vedere "*TR-4820: Guida rapida alla pianificazione delle reti NetApp HCI*" e a. "*Istruzioni per l'installazione e la configurazione di NetApp HCI*".
- Per informazioni sulle configurazioni NetApp HCI più piccole di quattro nodi di storage, vedere "*TR-4823: Cluster di storage a 2 nodi NetApp HCI*".
- Per ulteriori informazioni sulla configurazione del protocollo LACP (link Aggregation Control Protocol) sulle porte dello switch utilizzate per ciascuno dei nodi di storage, vedere "Configurare LCAP per ottenere performance di storage ottimali".

Questa configurazione consolida tutto il traffico su due porte fisiche ridondanti, riducendo il cablaggio e ottimizzando la configurazione di rete. Questa configurazione richiede che i segmenti di rete di storage, vMotion e qualsiasi macchina virtuale utilizzino il tagging VLAN. Il segmento della rete di gestione può utilizzare VLAN native o taggate; tuttavia, la VLAN nativa è la modalità preferita in modo che NetApp Deployment Engine (NDE) possa assegnare le risorse di rete in modo automatizzato (Zero Conf).

Questa modalità richiede vSphere Distributed Switch (VDS), che richiedono la licenza VMware vSphere Enterprise Plus.

Requisiti di rete prima di iniziare

Di seguito sono riportati i prerequisiti principali.

Per ulteriori informazioni sui prerequisiti, vedere "Panoramica dei requisiti per l'implementazione di NetApp HCI".

- Bond1G è un'interfaccia logica che combina porte di rete 1GbE su nodi di storage e un'interfaccia di gestione su nodi di calcolo. Questa rete viene utilizzata per il traffico API NDE. Tutti i nodi devono essere in grado di comunicare attraverso l'interfaccia di gestione nella stessa rete L2.
- Bond10G è un'interfaccia logica che combina porte 10/25GbE e viene utilizzata da NDE per il beaconing e l'inventario. Tutti i nodi devono essere in grado di comunicare tramite l'interfaccia Bond10G con frame jumbo non frammentati.
- NDE richiede almeno un indirizzo IP assegnato manualmente sull'interfaccia Bond1G su un nodo di storage. NDE verrà eseguito da questo nodo.
- Tutti i nodi avranno indirizzi IP temporanei assegnati dalla ricerca NDE, che viene eseguita da Automatic Private IP Addressing (APIPA).

> Durante il processo NDE, a tutti i nodi verranno assegnati indirizzi IP permanenti e gli eventuali IP temporanei assegnati da APIPA verranno rilasciati.

- NDE richiede reti separate per la gestione, iSCSI e vMotion preconfigurati sulla rete dello switch.

Convalida la preparazione della rete con NetApp Active IQ Config Advisor

Per garantire la preparazione della rete per NetApp HCI, installare NetApp Active IQ Config Advisor 5.8.1 o versione successiva. Questo tool di convalida della rete si trova insieme ad altri "Strumenti di supporto NetApp". Utilizza questo tool per convalidare connettività, ID VLAN, requisiti di indirizzo IP, connettività dello switch e altro ancora.

Per ulteriori informazioni, vedere "Validate il vostro ambiente con Active IQ Config Advisor".

Collabora con il tuo team NetApp

Il tuo team NetApp utilizza il report NetApp Active IQ Config Advisor e il *Discovery Workbook* per verificare che il tuo ambiente di rete sia pronto.

Installare l'hardware NetApp HCI

NetApp HCI può essere installato in diverse configurazioni:

- Nodi di calcolo H410C: Configurazione a due cavi o a sei cavi
- Nodo di calcolo H610C: Configurazione a due cavi
- Nodo di calcolo H615C: Configurazione a due cavi
- Nodo storage H410S
- Nodo storage H610S

Per le precauzioni e i dettagli, vedere "Installare l'hardware della serie H.".

Fasi

1. Installare le guide e il telaio.
2. Installare i nodi nello chassis e i dischi per i nodi di storage. (Valido solo se si installano H410C e H410S in uno chassis NetApp serie H.)
3. Installare gli switch.
4. Collegare il nodo di calcolo.
5. Collegare il nodo di storage.
6. Collegare i cavi di alimentazione.
7. Accendere i nodi NetApp HCI.

Completare le attività opzionali dopo l'installazione dell'hardware

Dopo aver installato l'hardware NetApp HCI, è necessario eseguire alcune operazioni facoltative ma consigliate.

Gestire la capacità dello storage su tutti gli chassis

Assicurarsi che la capacità dello storage sia suddivisa in modo uniforme in tutti gli chassis contenenti nodi di storage.

Configurare IPMI per ciascun nodo

Dopo aver eseguito il racking, il cabling e l'accensione dell'hardware NetApp HCI, è possibile configurare l'accesso all'interfaccia di gestione della piattaforma intelligente (IPMI) per ciascun nodo. Assegnare a ciascuna porta IPMI un indirizzo IP e modificare la password IPMI predefinita dell'amministratore non appena si dispone dell'accesso remoto IPMI al nodo.

Vedere "Configurare IPMI".

Implementare NetApp HCI utilizzando il motore di implementazione NetApp (NDE)

L'interfaccia utente NDE è l'interfaccia della procedura guidata del software utilizzata per installare NetApp HCI.

Avviare l'interfaccia utente NDE

NetApp HCI utilizza un indirizzo IPv4 della rete di gestione dei nodi di storage per l'accesso iniziale all'NDE. Come Best practice, connettersi dal primo nodo di storage.

Prerequisiti

- L'indirizzo IP iniziale della rete di gestione del nodo di storage è già stato assegnato manualmente o utilizzando DHCP.
- È necessario disporre dell'accesso fisico all'installazione di NetApp HCI.

Fasi

1. Se non si conosce l'IP della rete di gestione del nodo di storage iniziale, utilizzare l'interfaccia utente terminale (TUI), accessibile tramite tastiera e monitor sul nodo di storage o. "Utilizzare una chiavetta USB".

   Per ulteriori informazioni, vedere "*Accesso al NetApp Deployment Engine*".

2. Se si conosce l'indirizzo IP, da un browser Web, connettersi all'indirizzo Bond1G del nodo primario tramite HTTP, non HTTPS.

   Esempio: `http://<IP_address>:442/nde/`

Implementare NetApp HCI con l'interfaccia utente NDE

1. Nell'NDE, accettare i prerequisiti, selezionare Use Active IQ (Usa licenza) e accettare i contratti di licenza.
2. Facoltativamente, attivare i servizi file del Data Fabric di ONTAP Select e accettare la licenza ONTAP Select.
3. Configurare una nuova implementazione di vCenter. Fare clic su **Configure using a fully qualified Domain Name** (Configura utilizzando un nome di dominio completo) e immettere sia il nome di dominio del server vCenter che l'indirizzo IP del server DNS.

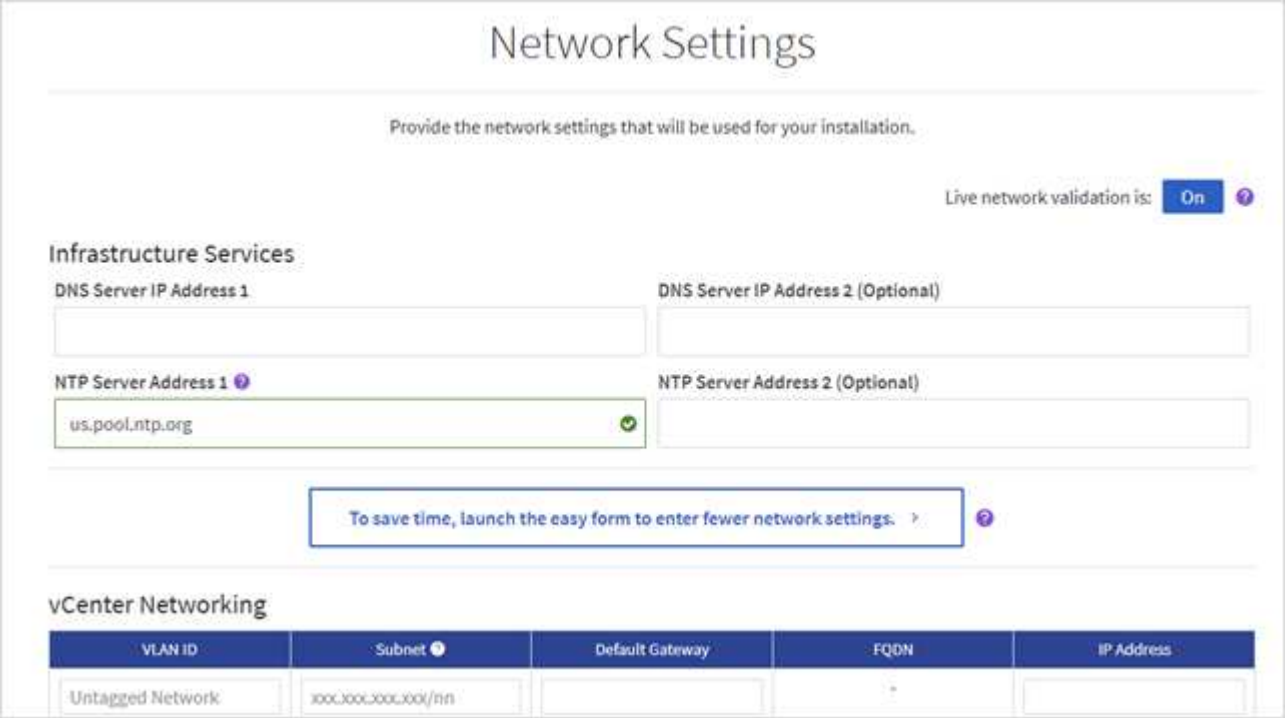
   Si consiglia vivamente di utilizzare l'approccio FQDN per l'installazione di vCenter.

4. Verificare che la valutazione dell'inventario di tutti i nodi sia stata completata correttamente.

   Il nodo di storage che esegue NDE è già selezionato.

5. Selezionare tutti i nodi e fare clic su **continua**.

6. Configurare le impostazioni di rete. Per i valori da utilizzare, fare riferimento al *Eserciziario di rilevamento dell'installazione di NetApp HCI*.
7. Fare clic sulla casella blu per avviare il modulo Easy.



8. Nel modulo semplice Impostazioni di rete:
   a. Digitare il prefisso di denominazione. (Fare riferimento ai dettagli di sistema del *Eserciziario per il rilevamento dell'installazione di NetApp HCI*).
   b. Fare clic su **No** per assegnare gli ID VLAN? Le si assegnano successivamente nella pagina principale Impostazioni di rete.
   c. Digitare la subnet CIDR, il gateway predefinito e l'indirizzo IP iniziale per le reti di gestione, vMotion e iSCI in base alla guida. Per questi valori, fare riferimento alla sezione relativa al metodo di assegnazione IP del *Eserciziario di rilevamento dell'installazione di NetApp HCI*.
   d. Fare clic su **Applica a impostazioni di rete**.
9. Unisciti a un "VCenter esistente" (opzionale).
10. Annotare i numeri di serie dei nodi nel *Eserciziario di rilevamento dell'installazione di NetApp HCI*.
11. Specificare un ID VLAN per la rete vMotion e per qualsiasi rete che richieda il tagging VLAN. Consultare il *Eserciziario per il rilevamento dell'installazione di NetApp HCI*.
12. Scaricare la configurazione come file .CSV.
13. Fare clic su **Avvia implementazione**.
14. Copiare e salvare l'URL visualizzato.

> Il completamento dell'implementazione può richiedere circa 45 minuti.

Verificare l'installazione utilizzando vSphere Web Client

1. Avviare vSphere Web Client ed effettuare l'accesso utilizzando le credenziali specificate durante l'utilizzo di NDE.

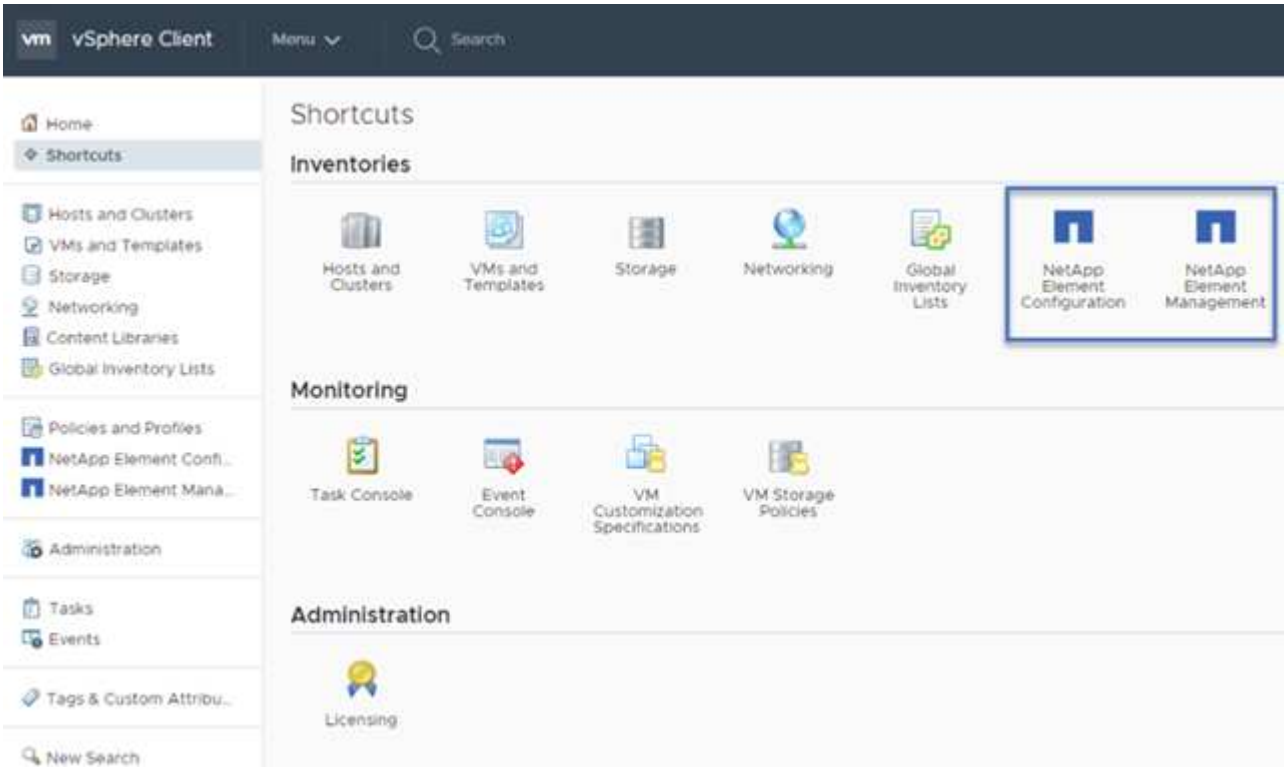
È necessario aggiungere `@vsphere.local` al nome utente.

2. Verificare che non siano presenti allarmi.
3. Verificare che le appliance vCenter, mNode e ONTAP Select (opzionali) siano in esecuzione senza icone di avviso.
4. Osservare che vengono creati i due datastore predefiniti (NetApp-HCI-Datastore_01 e 02).
5. Selezionare ciascun datastore e assicurarsi che tutti i nodi di calcolo siano elencati nella scheda host.
6. Validare vMotion e Datastore-02.
   a. Migrare vCenter Server a NetApp-HCI-Datastore-02 (solo storage vMotion).
   b. Migrare vCenter Server in ciascuno dei nodi di calcolo (solo calcolo vMotion).
7. Accedere al plug-in NetApp Element per vCenter Server e verificare che il cluster sia visibile.
8. Assicurarsi che non vengano visualizzati avvisi sulla dashboard.

Gestire NetApp HCI utilizzando il plug-in vCenter

Dopo aver installato NetApp HCI, è possibile configurare cluster, volumi, datastore, log, gruppi di accesso, Initiator e policy sulla qualità del servizio (QoS) utilizzando il plug-in NetApp Element per vCenter Server.

Per ulteriori informazioni, vedere "*Documentazione del plug-in NetApp Element per vCenter Server*".



Monitorare o aggiornare NetApp HCI con il controllo del cloud ibrido

È possibile utilizzare il controllo del cloud ibrido NetApp HCI per monitorare, aggiornare o espandere il sistema.

Per accedere a NetApp Hybrid Cloud Control, accedere all'indirizzo IP del nodo di gestione.

Utilizzando il controllo del cloud ibrido, puoi:

- "Monitorare l'installazione di NetApp HCI"
- "Aggiorna il tuo sistema NetApp HCI"
- "Espandi lo storage NetApp HCI o le risorse di calcolo"

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.

   Viene visualizzata l'interfaccia NetApp Hybrid Cloud Control.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Istruzioni per l'installazione e la configurazione di NetApp HCI"
- "TR-4820: Guida rapida alla pianificazione delle reti NetApp HCI"
- "Plug-in NetApp Element per la documentazione del server vCenter"
- "NetApp Configuration Advisor" 5.8.1 o successivo tool di convalida della rete
- "Documentazione NetApp SolidFire Active IQ"

Installare l'hardware della serie H.

Prima di iniziare a utilizzare NetApp HCI, è necessario installare correttamente i nodi di calcolo e storage.

Vedere "poster" per una rappresentazione visiva delle istruzioni.

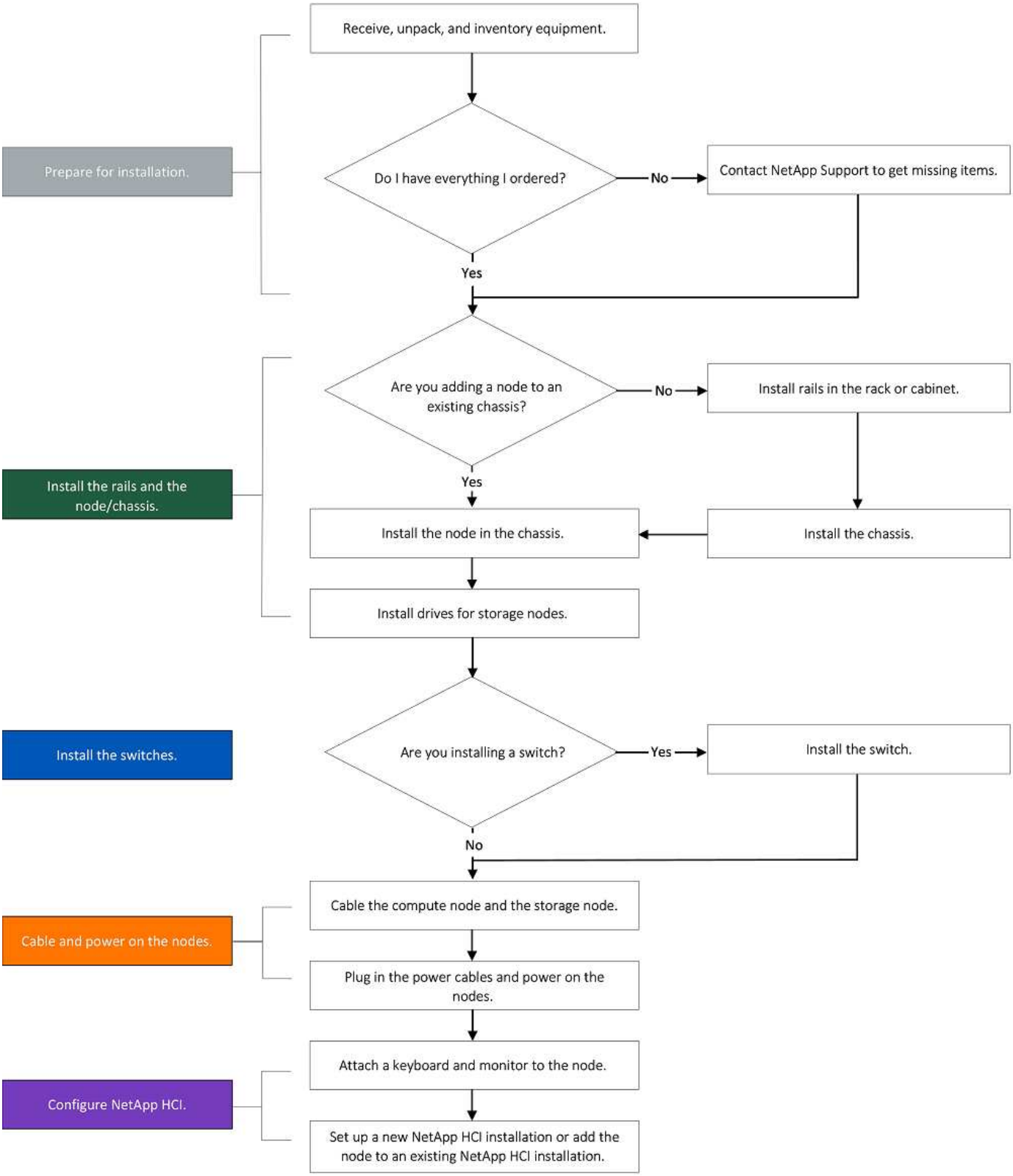
- Diagrammi del flusso di lavoro
- Preparazione per l'installazione
- Montare le guide
- Installare il nodo/chassis
- Installare gli switch
- Collegare i nodi
- Accendere i nodi
- Configurare NetApp HCI
- Eseguire attività di post-configurazione

Diagrammi del flusso di lavoro

I diagrammi del flusso di lavoro forniscono una panoramica generale delle fasi di installazione. Le fasi variano leggermente a seconda del modello della serie H.

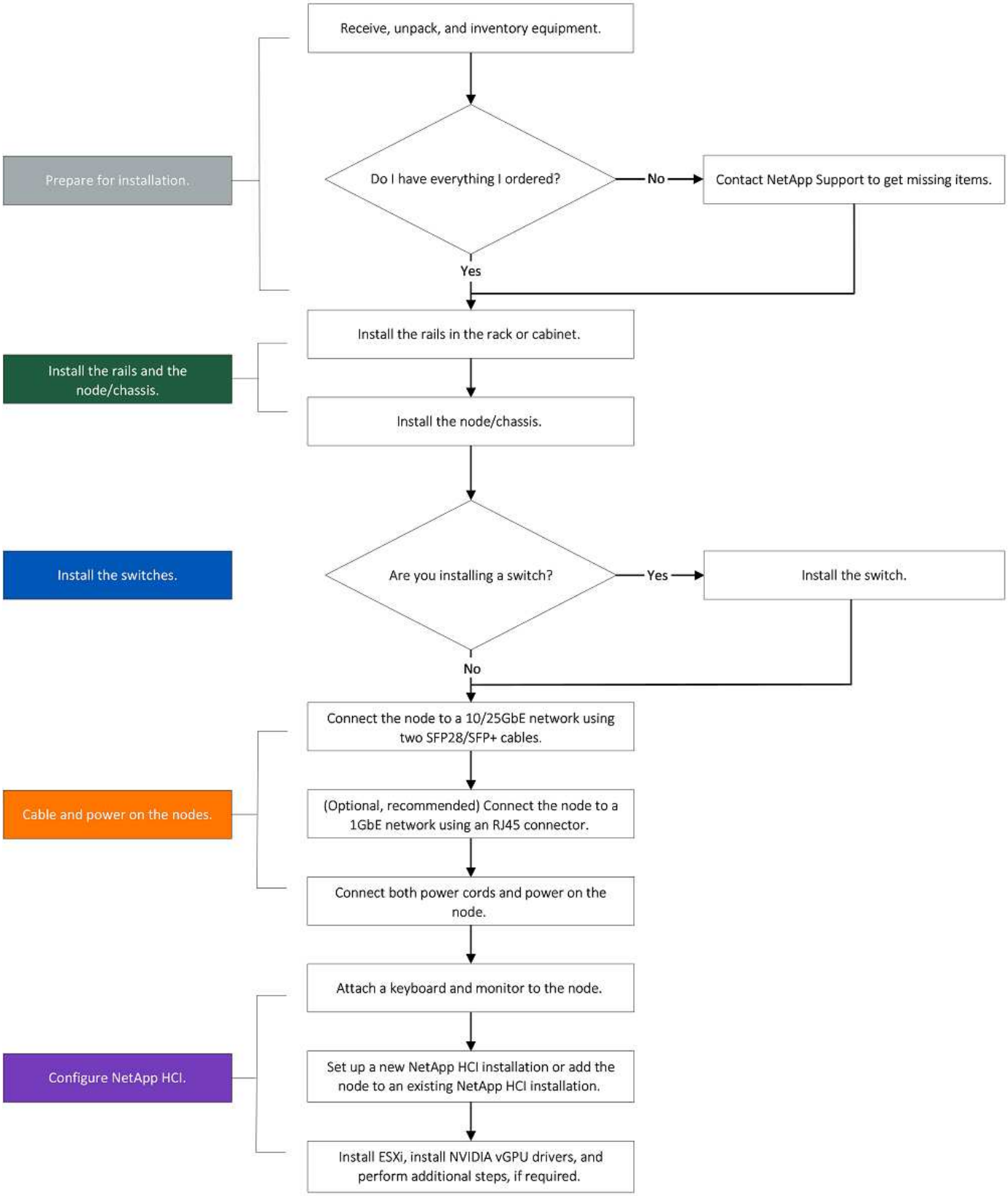
- H410C e H410S
- H610C e H615C
- [H610S]

H410C e H410S



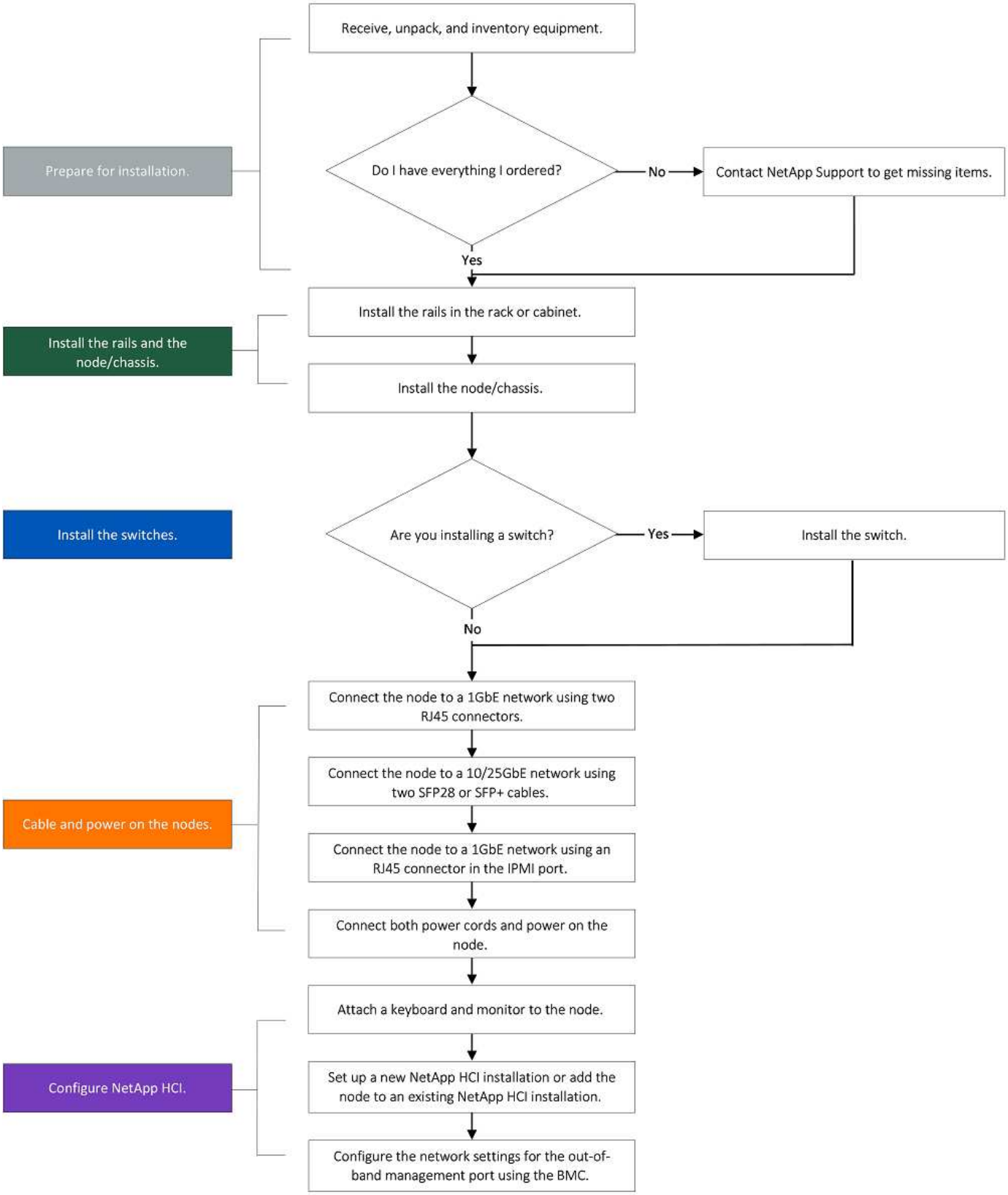
H610C e H615C

I termini "nodo" e "chassis" sono utilizzati in modo intercambiabile nel caso di H610C e H615C, perché nodo e chassis non sono componenti separati, a differenza di quanto avviene nel caso di uno chassis 2U a quattro nodi.


Prepare for installation.
Receive, unpack, and inventory equipment.
Do I have everything I ordered?
No
Contact NetApp Support to get missing items.
Yes
Install the rails and the node/chassis.
Install the rails in the rack or cabinet.
Install the node/chassis.
Install the switches.
Are you installing a switch?
Yes
Install the switch.
No
Cable and power on the nodes.
Connect the node to a 10/25GbE network using two SFP28/SFP+ cables.
(Optional, recommended) Connect the node to a 1GbE network using an RJ45 connector.
Connect both power cords and power on the node.
Configure NetApp HCI.
Attach a keyboard and monitor to the node.
Set up a new NetApp HCI installation or add the node to an existing NetApp HCI installation.
Install ESXi, install NVIDIA vGPU drivers, and perform additional steps, if required.

H610S

I termini "nodo" e "chassis" sono utilizzati in modo intercambiabile nel caso di H610C e H615C, perché nodo e chassis non sono componenti separati, a differenza di quanto avviene nel caso di uno chassis 2U a quattro nodi.


Prepare for installation.
Receive, unpack, and inventory equipment.
Do I have everything I ordered?
No
Contact NetApp Support to get missing items.
Yes
Install the rails and the node/chassis.
Install the rails in the rack or cabinet.
Install the node/chassis.
Install the switches.
Are you installing a switch?
Yes
Install the switch.
No
Cable and power on the nodes.
Connect the node to a 1GbE network using two RJ45 connectors.
Connect the node to a 10/25GbE network using two SFP28 or SFP+ cables.
Connect the node to a 1GbE network using an RJ45 connector in the IPMI port.
Connect both power cords and power on the node.
Configure NetApp HCI.
Attach a keyboard and monitor to the node.
Set up a new NetApp HCI installation or add the node to an existing NetApp HCI installation.
Configure the network settings for the out-of-band management port using the BMC.

Preparazione per l'installazione

In preparazione dell'installazione, inventariare l'hardware spedito e contattare il supporto NetApp se alcuni degli elementi sono mancanti.

Assicurarsi di disporre dei seguenti elementi nella posizione di installazione:

- Spazio rack per il sistema.

Tipo di nodo	Spazio rack
Nodi H410C e H410S	Due unità rack (2U)
Nodo H610C	2U
Nodi H615C e H610S	Un'unità rack (1U)

- Cavi o ricetrasmettitori a collegamento diretto SFP28/SFP+
- Cavi Cat5e o superiori con connettore RJ45
- Uno switch KVM (Keyboard, Video, mouse) per configurare il sistema
- Chiavetta USB (opzionale)

L'hardware spedito dipende da quello che si ordina. Un nuovo ordine 2U a quattro nodi include chassis, pannello, kit guide di scorrimento, dischi per nodi di storage, nodi di storage e calcolo e cavi di alimentazione (due per chassis). Se si ordinano nodi di storage H610S, i dischi verranno installati nello chassis.

Durante l'installazione dell'hardware, assicurarsi di rimuovere tutto il materiale di imballaggio e l'imballaggio dall'unità. In questo modo si eviteranno il surriscaldamento e lo spegnimento dei nodi.

Montare le guide

L'ordine hardware fornito include un set di guide di scorrimento. Per completare l'installazione della guida, è necessario un cacciavite. Le fasi di installazione variano leggermente per ciascun modello di nodo.

Installare l'hardware dalla parte inferiore del rack fino alla parte superiore per evitare che l'apparecchiatura si rovescii. Se il rack include dispositivi di stabilizzazione, installarli prima di installare l'hardware.

- H410C e H410S
- [H610C]
- H610S e H615C

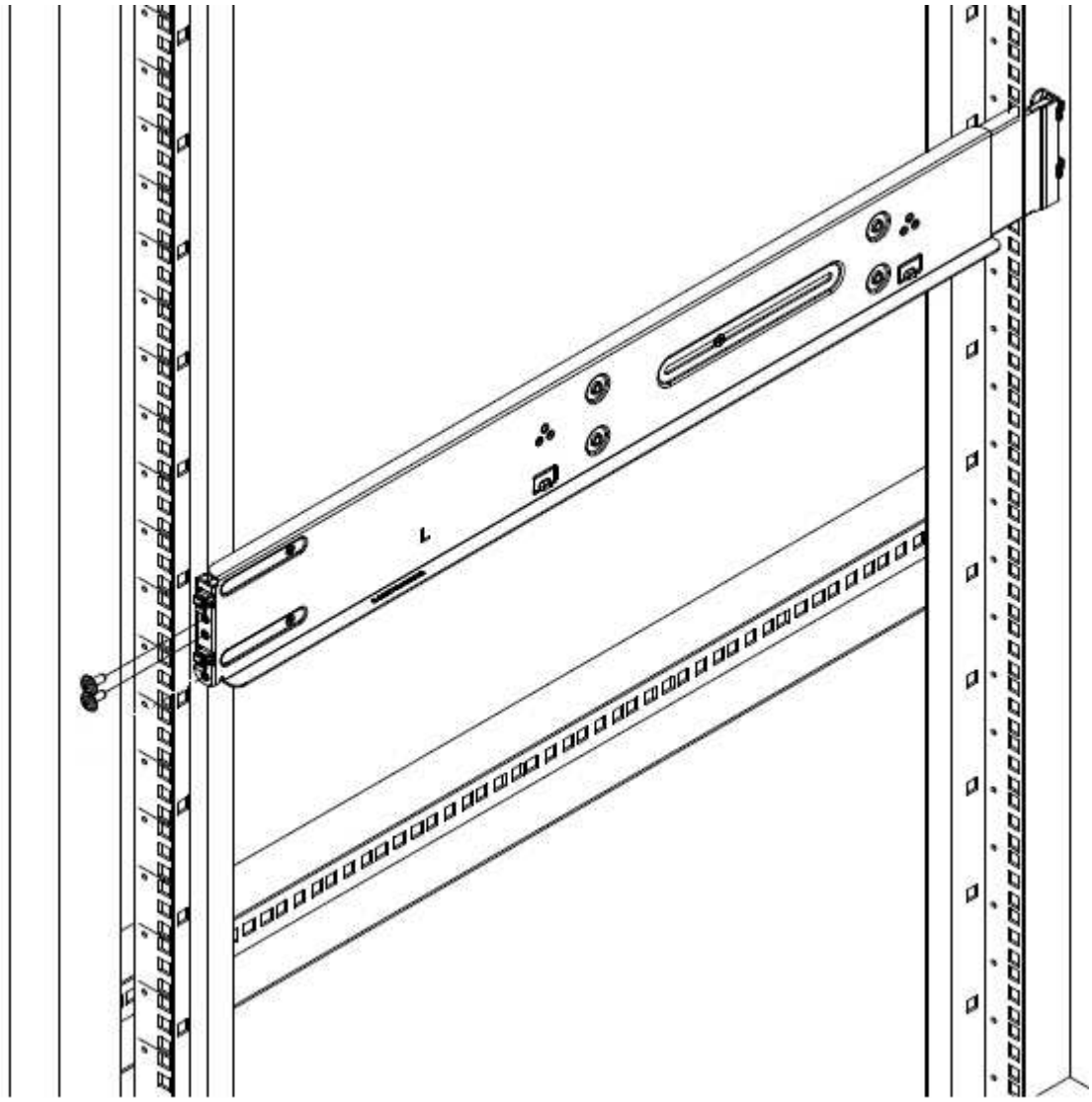
H410C e H410S

I nodi H410C e H410S sono installati in uno chassis 2U a quattro nodi della serie H, fornito con due set di adattatori. Se si desidera installare lo chassis in un rack con fori rotondi, utilizzare gli adattatori appropriati per un rack con fori rotondi. Le guide per i nodi H410C e H410S si adattano a un rack con una profondità compresa tra 29 e 33.5 pollici. Quando la guida è completamente contratta, è lunga 28 pollici e le sezioni anteriore e posteriore della guida sono tenute insieme da una sola vite.

Se si installa il telaio su una guida completamente contratta, le sezioni anteriore e posteriore della guida potrebbero separarsi.

Fasi

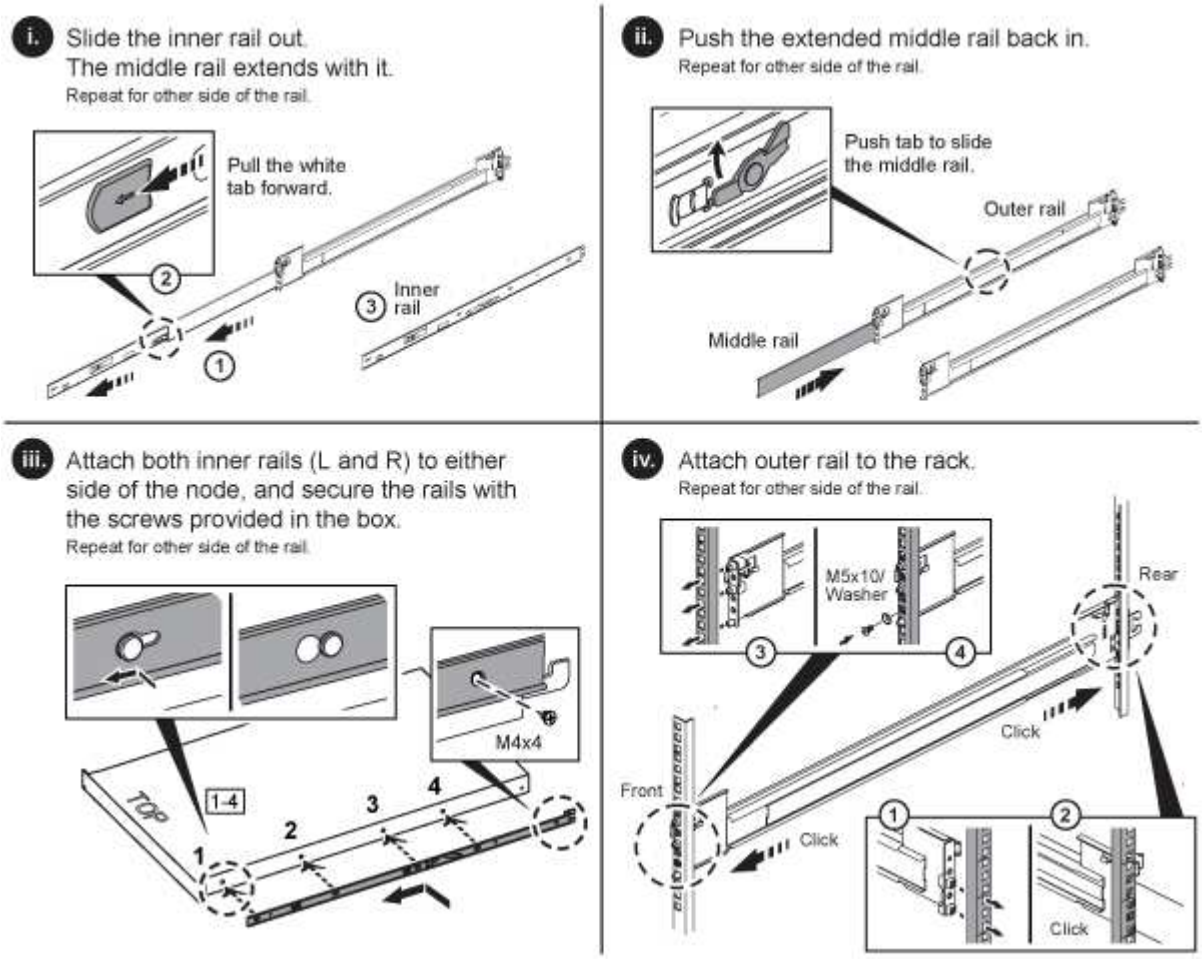
1. Allineare la parte anteriore della guida con i fori sul montante anteriore del rack.
2. Spingere i ganci sulla parte anteriore della guida nei fori sul montante anteriore del rack, quindi abbassarli fino a quando i perni caricati a molla non scattano nei fori del rack.
3. Fissare la guida al rack con le viti. Di seguito viene illustrata la guida sinistra collegata alla parte anteriore del rack:



4. Estendere la sezione posteriore della guida fino al montante posteriore del rack.
5. Allineare i ganci sul retro della guida con i fori appropriati sul montante posteriore, assicurandosi che la parte anteriore e posteriore della guida siano allo stesso livello.
6. Montare la parte posteriore della guida sul rack e fissarla con le viti.
7. Eseguire tutte le operazioni descritte sopra per l'altro lato del rack.

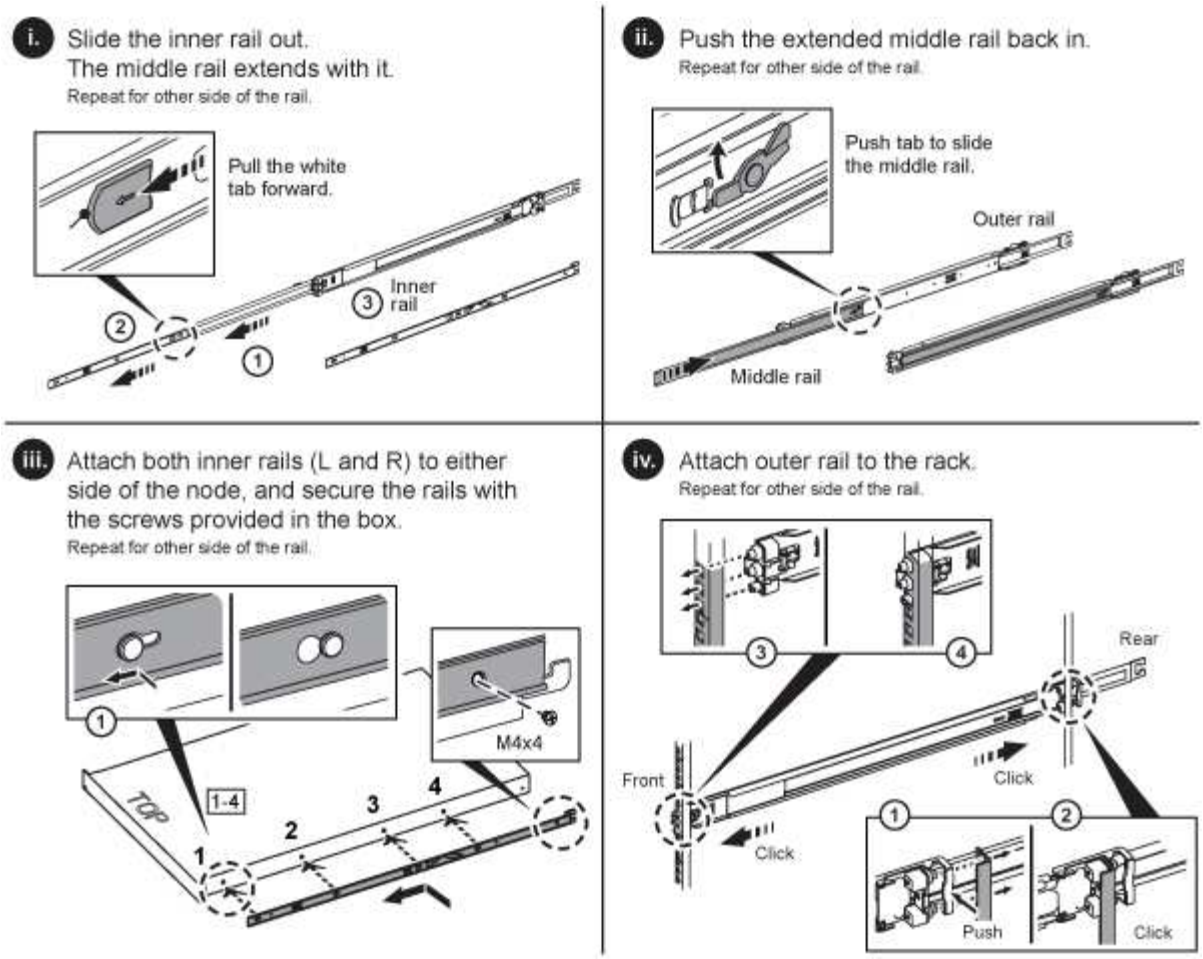
H610C

Di seguito viene illustrata l’installazione delle guide per un nodo di calcolo H61OC:



H610S e H615C

Di seguito viene illustrata l’installazione delle guide per un nodo di storage H610S o un nodo di calcolo H615C:



I modelli H610S e H615C sono con guide di destra e di sinistra. Posizionare il foro della vite verso il basso in modo che la vite a testa zigrinata H610S/H615C possa fissare il telaio alla guida.

Installare il nodo/chassis

Il nodo di calcolo H410C e il nodo di storage H410S vengono installati in uno chassis 2U a quattro nodi. Per H610C, H615C e H610S, installare il telaio/nodo direttamente sulle guide del rack.

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

Rimuovere tutto il materiale di imballaggio e l'imballaggio dall'unità. In questo modo si evitano il surriscaldamento e lo spegnimento dei nodi.

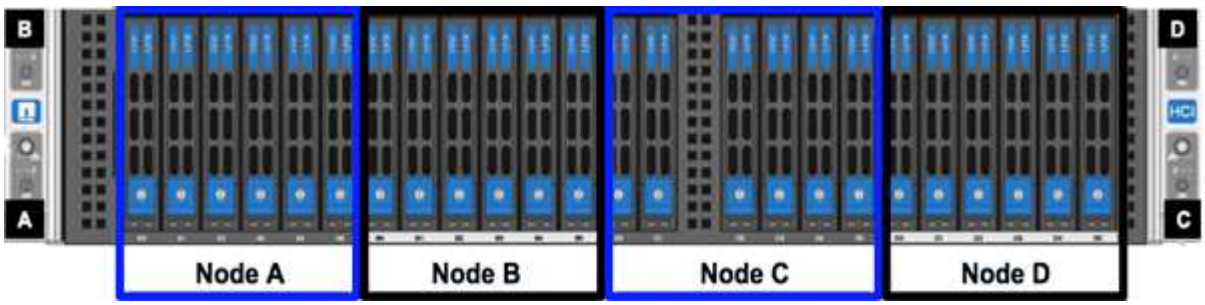
- Nodi H410C e H410S
- Nodo/chassis H610C
- Nodo/chassis H610S e H615C

Nodi H410C e H410S

Fasi

1. Installare i nodi H410C e H410S nello chassis. Ecco un esempio di vista posteriore di uno chassis con quattro nodi installati:

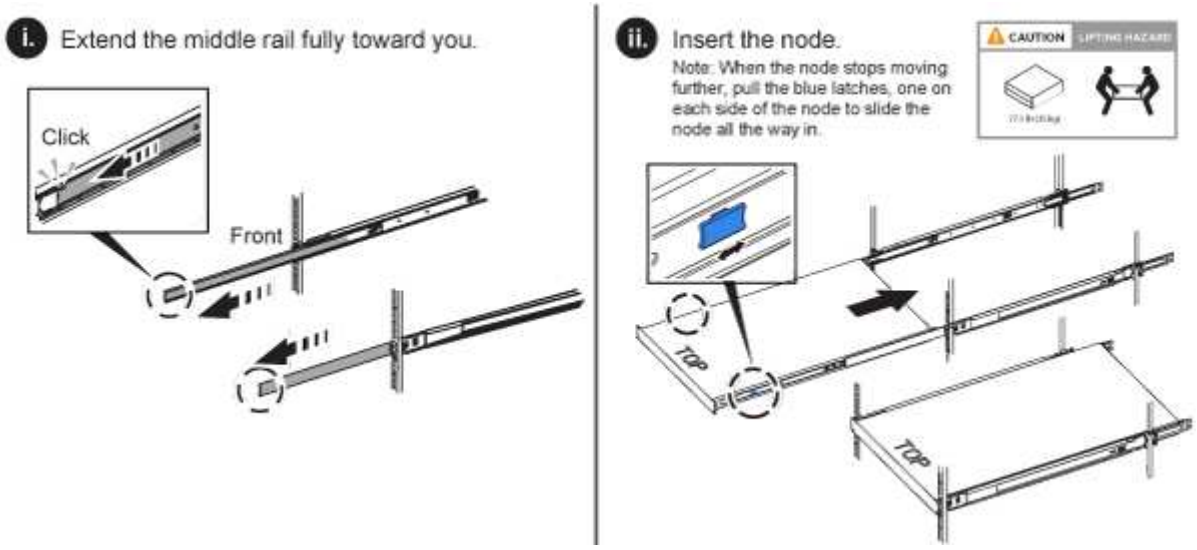
2. Installare le unità per i nodi di storage H410S.



Nodo/chassis H610C

Nel caso di H610C, i termini "nodo" e "chassis" vengono utilizzati in modo intercambiabile perché nodo e chassis non sono componenti separati, a differenza del caso dello chassis 2U a quattro nodi.

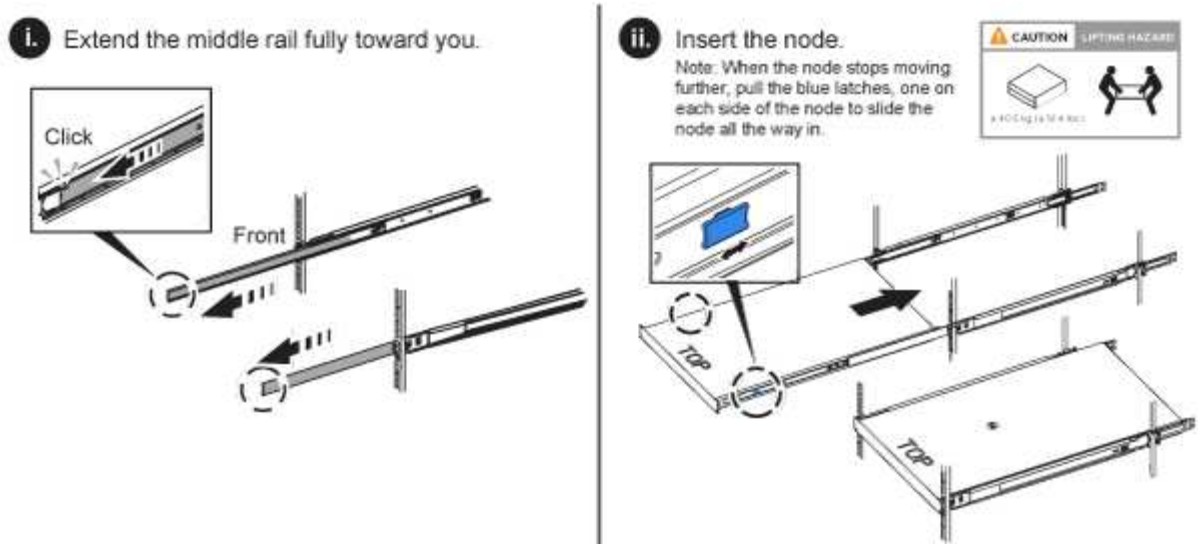
Di seguito viene riportata un'illustrazione per l'installazione del nodo/chassis nel rack:



Nodo/chassis H610S e H615C

Nel caso di H615C e H610S, i termini "nodo" e "chassis" sono utilizzati in modo intercambiabile perché nodo e chassis non sono componenti separati, a differenza del caso di chassis 2U a quattro nodi.

Di seguito viene riportata un'illustrazione per l'installazione del nodo/chassis nel rack:



Installare gli switch

Se si desidera utilizzare gli switch Mellanox SN2010, SN2100 e SN2700 nell'installazione di NetApp HCI, seguire le istruzioni fornite qui per installare e collegare gli switch:

- "Manuale dell'utente dell'hardware Mellanox"
- "TR-4836: Guida al cablaggio dello switch NetApp HCI con Mellanox SN2100 e SN2700 (accesso richiesto)"

Collegare i nodi

Se si aggiungono nodi a un'installazione NetApp HCI esistente, assicurarsi che il cablaggio e la configurazione di rete dei nodi aggiunti siano identici all'installazione esistente.

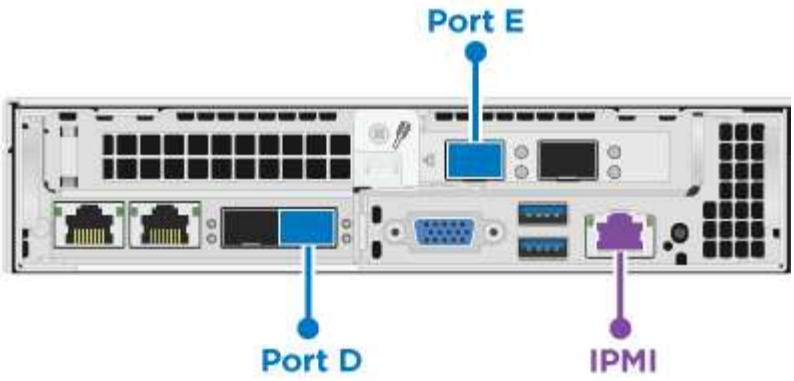
> Assicurarsi che le prese d'aria sul retro del telaio non siano ostruite da cavi o etichette. Ciò può causare guasti prematuri dei componenti dovuti al surriscaldamento.

- Nodo di calcolo H410C e nodo storage H410S
- Nodo di calcolo H610C
- Nodo di calcolo H615C
- Nodo storage H610S

Nodo di calcolo H410C e nodo storage H410S

Sono disponibili due opzioni per il cablaggio del nodo H410C: Due cavi o sei cavi.

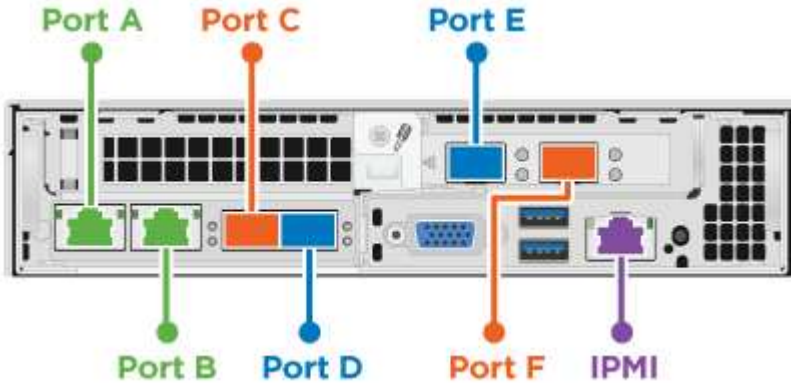
Ecco la configurazione a due cavi:



Per le porte D ed e, collegare due cavi o ricetrasmettitori SFP28/SFP+ per la gestione condivisa, le macchine virtuali e la connettività dello storage.

(Opzionale, consigliato) collegare un cavo CAT5e alla porta IPMI per la connettività di gestione out-of-band.

Ecco la configurazione a sei cavi:



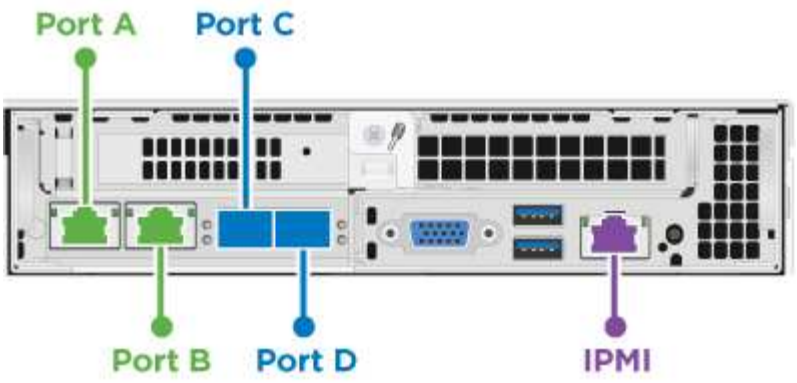
Per le porte A e B, collegare due cavi CAT5e o superiori nelle porte A e B per la connettività di gestione.

Per le porte C e F, collegare due cavi SFP28/SFP+ o ricetrasmettitori per la connettività delle macchine virtuali.

Per le porte D ed e, collegare due cavi SFP28/SFP+ o ricetrasmettitori per la connettività dello storage.

(Opzionale, consigliato) collegare un cavo CAT5e alla porta IPMI per la connettività di gestione out-of-band.

Di seguito sono riportati i cavi per il nodo H410S:



Per le porte A e B, collegare due cavi CAT5e o superiori nelle porte A e B per la connettività di gestione.

Per le porte C e D, collegare due cavi SFP28/SFP+ o ricetrasmettitori per la connettività dello storage.

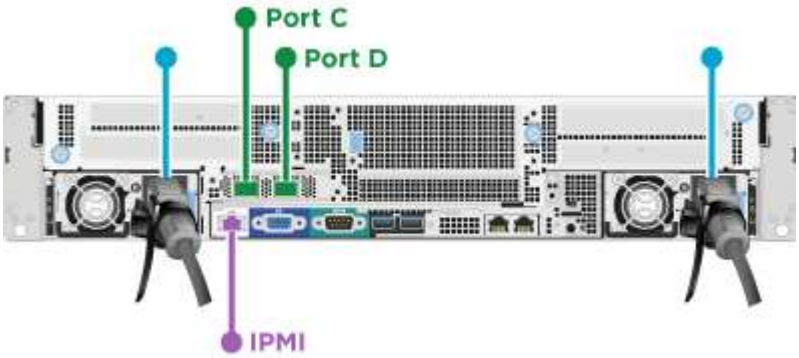
(Opzionale, consigliato) collegare un cavo CAT5e alla porta IPMI per la connettività di gestione out-of-band.

Dopo aver collegato i nodi, collegare i cavi di alimentazione alle due unità di alimentazione per chassis e inserirle nella PDU a 240 V o nella presa di corrente.

Nodo di calcolo H610C

Di seguito sono riportati i cavi per il nodo H610C:

> I nodi H610C vengono implementati solo nella configurazione a due cavi. Assicurarsi che tutte le VLAN siano presenti sulle porte C e D.



Per le porte C e D, collegare il nodo a una rete 10/25GbE utilizzando due cavi SFP28/SFP+.

(Opzionale, consigliato) collegare il nodo a una rete 1GbE utilizzando un connettore RJ45 nella porta IPMI.

Collegare entrambi i cavi di alimentazione al nodo e collegare i cavi di alimentazione a una presa di alimentazione da 200-240 V.

Nodo di calcolo H615C

Di seguito sono riportati i cavi per il nodo H615C:

> I nodi H615C vengono implementati solo nella configurazione a due cavi. Assicurarsi che tutte le VLAN siano presenti sulle porte A e B.

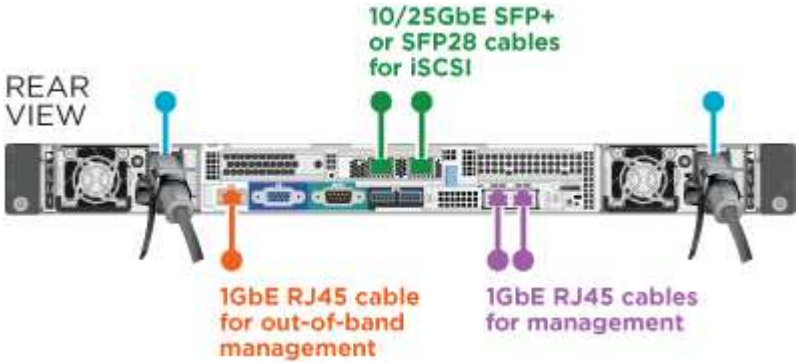
Per le porte A e B, collegare il nodo a una rete 10/25GbE utilizzando due cavi SFP28/SFP+.

(Opzionale, consigliato) collegare il nodo a una rete 1GbE utilizzando un connettore RJ45 nella porta IPMI.

Collegare entrambi i cavi di alimentazione al nodo e collegare i cavi di alimentazione a una presa di alimentazione da 110 V.

Nodo storage H610S

Di seguito sono riportati i cavi per il nodo H610S:



Collegare il nodo a una rete 1GbE utilizzando due connettori RJ45 nella porta IPMI.

Collegare il nodo a una rete 10/25GbE utilizzando due cavi SFP28 o SFP+.

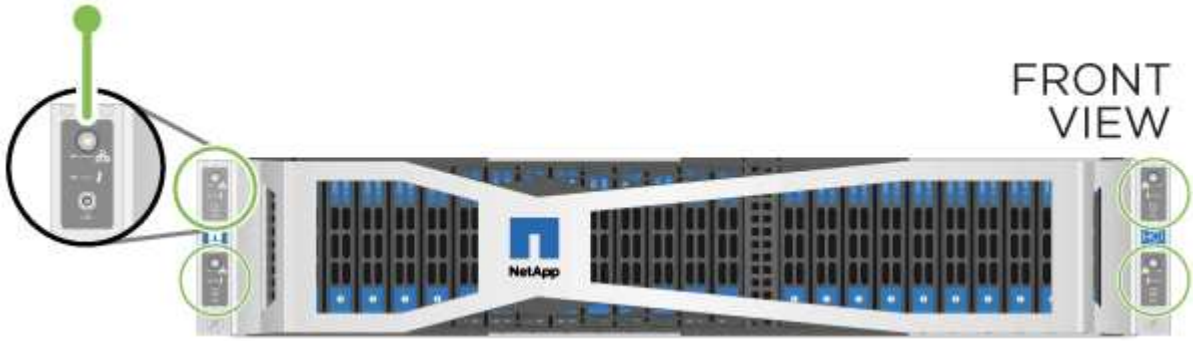
Collegare il nodo a una rete 1GbE utilizzando un connettore RJ45 nella porta IPMI.

Collegare entrambi i cavi di alimentazione al nodo.

Accendere i nodi

L'avvio dei nodi richiede circa sei minuti.

Di seguito è riportata un'illustrazione che mostra il pulsante di accensione sullo chassis NetApp HCI 2U:



Di seguito è riportata un'illustrazione che mostra il pulsante di accensione sul nodo H610C:

Di seguito è riportata un'illustrazione che mostra il pulsante di accensione sui nodi H615C e H610S:

Configurare NetApp HCI

Scegliere una delle seguenti opzioni:

- Nuova installazione di NetApp HCI
- Espandere un'installazione NetApp HCI esistente

Nuova installazione di NetApp HCI

Fasi

1. Configurare un indirizzo IPv4 sulla rete di gestione (Bond1G) su un nodo di storage NetApp HCI.

> Se si utilizza DHCP sulla rete di gestione, è possibile connettersi all'indirizzo IPv4 acquisito da DHCP del sistema di storage.

a. Collegare una tastiera, un video o un mouse (KVM) sul retro di un nodo di storage.
b. Configurare l'indirizzo IP, la subnet mask e l'indirizzo del gateway per Bond1G nell'interfaccia utente. È inoltre possibile configurare un ID VLAN per la rete Bond1G.

2. Utilizzando un browser Web supportato (Mozilla Firefox, Google Chrome o Microsoft Edge), accedere a NetApp Deployment Engine effettuando la connessione all'indirizzo IPv4 configurato nella fase 1.
3. Utilizzare l'interfaccia utente del motore di implementazione NetApp per configurare NetApp HCI.

> Tutti gli altri nodi NetApp HCI verranno rilevati automaticamente.

Espandere un'installazione NetApp HCI esistente

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web.
2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Seguire i passaggi della procedura guidata per aggiungere nodi di storage e/o di calcolo all'installazione di NetApp HCI.

> Per aggiungere nodi di calcolo H410C, l'installazione esistente deve eseguire NetApp HCI 1.4 o versione successiva. Per aggiungere nodi di calcolo H615C, l'installazione esistente deve eseguire NetApp HCI 1.7 o versione successiva.

> I nodi NetApp HCI appena installati sulla stessa rete verranno rilevati automaticamente.

Eseguire attività di post-configurazione

A seconda del tipo di nodo in uso, potrebbe essere necessario eseguire ulteriori operazioni dopo aver installato l'hardware e configurato NetApp HCI.

- Nodo H610C
- Nodi H615C e H610S

Nodo H610C

Installare i driver GPU in ESXi per ciascun nodo H610C installato e convalidarne la funzionalità.

Nodi H615C e H610S

Fasi

1. Utilizzare un browser Web e accedere all'indirizzo IP BMC predefinito: `192.168.0.120`
2. Effettuare l'accesso utilizzando il nome utente `root` e password `calvin`.
3. Dalla schermata di gestione dei nodi, accedere a **Impostazioni > Impostazioni di rete** e configurare i parametri di rete per la porta di gestione fuori banda.

Se nel nodo H615C sono presenti GPU, installare i driver GPU in ESXi per ciascun nodo H615C installato e validarne la funzionalità.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Plug-in NetApp Element per server vCenter"
- "*TR-4820: Guida rapida alla pianificazione delle reti NetApp HCI*"
- "NetApp Configuration Advisor" 5.8.1 o successivo tool di convalida della rete

Configurare LACP per ottenere performance di storage ottimali

Per ottenere prestazioni ottimali del cluster di storage NetApp HCI, è necessario configurare il protocollo LACP (link Aggregation Control Protocol) sulle porte dello switch utilizzate per ciascuno dei nodi di storage.

Prima di iniziare

- Le porte dello switch collegate alle interfacce 10/25GbE dei nodi di storage NetApp HCI sono state configurate come canali di porta LACP.
- I timer LACP sugli switch che gestiscono il traffico di storage sono stati impostati su "fast mode (1s)" per un tempo di rilevamento del failover ottimale. Durante l'implementazione, le interfacce Bond1G su tutti i nodi di storage vengono configurate automaticamente per la modalità attiva/passiva.
- Cisco Virtual PortChannel (VPC) è stato configurato o la tecnologia di stacking dello switch equivalente per gli switch che gestiscono la rete di storage. La tecnologia di stacking dello switch semplifica la configurazione dei canali LACP e delle porte e offre una topologia senza loop tra gli switch e le porte 10/25GbE sui nodi di storage.

Fasi

1. Segui le raccomandazioni del vendor dello switch per abilitare LACP sulle porte dello switch utilizzate per i nodi di storage NetApp serie H.
2. Modificare la modalità bond su tutti i nodi di storage in LACP nell'interfaccia utente on-node (nota anche come interfaccia utente terminale o TUI) prima di implementare NetApp HCI.

Trova ulteriori informazioni

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

Validate il vostro ambiente con Active IQ Config Advisor

Prima di eseguire l'installazione NetApp HCI dell'hardware NetApp HCI su rack, è necessario verificare che l'ambiente soddisfi i requisiti di rete NetApp HCI. Active IQ Config Advisor esegue controlli sull'ambiente convalidando le configurazioni di rete, switch e VMware vSphere. Lo strumento genera un report che può essere utilizzato per risolvere i problemi ed è possibile inoltrare il report al tecnico dei servizi professionali per

preparare e pianificare un'installazione.

Installare Active IQ Config Advisor

Scaricare e installare Active IQ Config Advisor su un PC che ha accesso alle reti NetApp HCI.

Fasi

1. In un browser Web, selezionare **Strumenti** dal menu supporto NetApp, cercare Active IQ Config Advisor e scaricare lo strumento.

   Tool › NetApp Support Site.

   Dopo aver accettato il Contratto di licenza con l'utente finale (EULA), viene visualizzata la pagina Download. I file binari di Microsoft Windows, Linux e Mac sono disponibili nel riquadro **Client Tool**.

2. Eseguire l'eseguibile.
3. Selezionare una lingua e fare clic su **OK**.
4. Fare clic su **Avanti**.
5. Leggere il Contratto di licenza con l'utente finale e fare clic su **Accetto**.
6. Fare clic su **Installa**.
7. Assicurarsi che l'opzione **Esegui Active IQ Config Advisor** sia selezionata e fare clic su **fine**.

   Dopo un breve intervallo di tempo, l'interfaccia utente di Active IQ Config Advisor si apre in una nuova finestra o scheda del browser.

USA Active IQ Config Advisor

Active IQ Config Advisor viene eseguito in una finestra del browser, raccoglie informazioni sulla rete e sull'ambiente e genera un report che è possibile utilizzare per risolvere eventuali problemi di rete o di configurazione che potrebbero interferire con l'implementazione di NetApp HCI.

Prima di iniziare

Active IQ Config Advisor è stato installato su un dispositivo in grado di accedere alla rete di gestione, alla rete di VMware vCenter Server (se si sta unendo a un'installazione VMware esistente) e agli switch che verranno utilizzati per NetApp HCI.

> Se si utilizzano switch Mellanox e i NetApp Professional Services li configurano come parte dell'implementazione, non è necessario fornire informazioni sullo switch.

A proposito di questa attività

Active IQ Config Advisor esegue solo controlli di sola lettura per raccogliere informazioni. Nessuna configurazione viene modificata come parte dell'insieme.

Fasi

1. Aprire Active IQ Config Advisor.

   Config Advisor viene visualizzato con la finestra **Impostazioni di base** in un browser Web. Qui è possibile definire le impostazioni di raccolta globali e crittografare i risultati della raccolta.

2. Immettere una passphrase nella sezione **Encryption Settings** per crittografare il progetto di raccolta.

In questo modo, solo l'utente sarà in grado di caricare questo progetto di raccolta dopo la sua creazione.

3. Identifica questo report di raccolta come tuo inserendo il tuo nome e indirizzo e-mail nella sezione **verifica utente**.
4. Fare clic su **Save** (Salva).
5. Fare clic su **Crea una nuova raccolta di dati**.
6. Selezionare **basato su soluzione** nel menu a discesa **tipo di raccolta**.
7. Selezionare **Pre-implementazione NetApp HCI** nel menu a discesa **Profilo**.
8. Per ciascun tipo di dispositivo nella colonna **tipo**, selezionare il numero del tipo di dispositivo nella rete NetApp HCI nel menu a discesa **azioni**.

   Ad esempio, se si dispone di tre switch Cisco, scegliere 3 dal menu a discesa della colonna **azioni** nella riga. Vengono visualizzate tre righe, una per ogni switch Cisco identificato.

   > Se si utilizzano switch Mellanox e i NetApp Professional Services li configurano come parte dell'implementazione, non è necessario fornire informazioni sullo switch.

9. Per gli switch identificati, inserire l'indirizzo IP di gestione e le credenziali di amministratore.
10. Per i server VMware vCenter identificati, eseguire una delle seguenti operazioni:
    - Se si sta implementando un nuovo vCenter Server, fornire l'indirizzo IP o FQDN (Fully Qualified Domain Name) pianificato per il server.
    - Se si sta entrando in un vCenter Server esistente, fornire l'indirizzo IP o FQDN e le credenziali di amministratore per il server.
11. Facoltativo: Se sono state aggiunte informazioni per gli switch, inserire il numero di nodi di calcolo e storage nella sezione **convalida switch**.
12. Scegliere la configurazione di cablaggio del nodo di calcolo che si desidera utilizzare nella sezione **Compute Node Network**.
13. Inserire le singole porte dello switch e i tag VLAN che si intende utilizzare per le reti di gestione, vMotion e storage per qualsiasi switch nella sezione **Compute Node Network**.
14. Inserire le singole porte dello switch e i tag VLAN che si intende utilizzare per le reti di gestione e storage per qualsiasi switch nella sezione **Storage Node Network**.
15. Nella sezione **verifica delle impostazioni di rete**, immettere gli indirizzi IP e l'indirizzo IP del gateway per la rete di gestione, seguiti da elenchi di server per DNS, NTP e vCenter Server (se si sta implementando un nuovo vCenter Server con NetApp HCI).

    Questa sezione consente a Active IQ Config Advisor di garantire che la rete di gestione sia disponibile per l'utilizzo e garantisce inoltre il corretto funzionamento di servizi come DNS e NTP.

16. Fare clic su **Validate** (convalida) per verificare che tutte le informazioni e le credenziali dell'indirizzo IP siano valide.
17. Fare clic su **Salva o Raccogli**.

    In questo modo, viene avviato il processo di raccolta, che consente di visualizzare l'avanzamento dell'insieme insieme a un registro in tempo reale dei comandi di raccolta. La colonna **Progress** mostra le barre di avanzamento codificate per colore per ciascuna attività di raccolta.

Le barre di avanzamento utilizzano i seguenti colori per visualizzare lo stato:

- **Verde**: L'insieme è terminato senza errori di comando. Per visualizzare i rischi e i consigli di implementazione, fare clic sull'icona **View & Analyze** (Visualizza e analizza) nel menu **Actions** (azioni).
- **Yellow**: L'insieme è terminato con alcuni errori di comando. Per visualizzare i rischi e i consigli di implementazione, fare clic sull'icona **View & Analyze** (Visualizza e analizza) nel menu **Actions** (azioni).
- **Rosso**: L'insieme non è riuscito. È necessario risolvere gli errori ed eseguire nuovamente la raccolta.

18. Facoltativo: Una volta completata la raccolta, è possibile fare clic sull'icona binoculare di qualsiasi riga di raccolta per visualizzare i comandi eseguiti e i dati raccolti.
19. Selezionare la scheda **View & Analyze** (Visualizza e analizza).

    Questa pagina mostra un report generale sullo stato di salute dell'ambiente. È possibile selezionare una sezione del grafico a torta per visualizzare ulteriori dettagli su controlli specifici o descrizioni dei problemi, oltre a consigli sulla risoluzione di eventuali problemi che potrebbero interferire con la corretta implementazione. Puoi risolvere questi problemi da solo o richiedere assistenza ai NetApp Professional Services.

20. Fare clic su **Export** (Esporta) per esportare il report della raccolta come documento PDF o Microsoft Word.

    Gli output dei documenti PDF e Microsoft Word includono le informazioni di configurazione dello switch per l'implementazione, utilizzate dai NetApp Professional Services per verificare le impostazioni di rete.

21. Inviare il file di report esportato al rappresentante dei NetApp Professional Services.

Trova ulteriori informazioni

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

Configurare IPMI per ciascun nodo

Dopo aver eseguito il racking, il cabling e l'accensione dell'hardware NetApp HCI, è possibile configurare l'accesso all'interfaccia di gestione della piattaforma intelligente (IPMI) per ciascun nodo. Assegnare a ciascuna porta IPMI un indirizzo IP e modificare la password di amministratore IPMI predefinita non appena si dispone dell'accesso remoto IPMI al nodo.

Prerequisiti

Dopo aver verificato che l'ambiente è pronto per supportare NetApp HCI e aver risolto eventuali problemi, è necessario completare alcune attività finali prima dell'implementazione.

- Assicurati di avere un report di successo da Active IQ Config Advisor.
- Raccogliere tutte le informazioni pertinenti relative alla rete, all'infrastruttura VMware corrente o pianificata e alle credenziali utente pianificate.

- Rack, cavo e alimentazione per l'installazione di NetApp HCI.

Assegnare manualmente l'indirizzo IP della porta IPMI

Il protocollo DHCP (Dynamic host Configuration Protocol) è attivato per impostazione predefinita per la porta IPMI di ciascun nodo NetApp HCI. Se la rete IPMI non utilizza DHCP, è possibile assegnare manualmente un indirizzo IPv4 statico alla porta IPMI.

Prima di iniziare

Assicurarsi di disporre di uno switch per tastiera, video e mouse (KVM) o di un monitor e di una tastiera utilizzabili per accedere al BIOS di ciascun nodo.

A proposito di questa attività

Utilizzare i tasti freccia per spostarsi all'interno del BIOS. Selezionare una scheda o un'opzione premendo `Enter`. Per tornare alle schermate precedenti, premere `ESC`.

Fasi

1. Accendere il nodo.
2. All'avvio, accedere al BIOS premendo il tasto `Del` chiave.
3. Selezionare la scheda IPMI.
4. Selezionare **BMC Network Configuration** e premere `Enter`.
5. Scegliere **Sì** e premere `Enter`.
6. Selezionare **origine indirizzo di configurazione** e premere `Enter`.
7. Scegliere **statico** e premere `Enter`.
8. Selezionare **Station IP address** (Indirizzo IP stazione) e inserire un nuovo indirizzo IP per la porta IPMI. Premere `Enter` al termine dell'operazione.
9. Selezionare **Subnet mask** e inserire una nuova subnet mask per la porta IPMI. Premere `Enter` al termine dell'operazione.
10. Selezionare **Gateway IP address** (Indirizzo IP gateway) e inserire un nuovo indirizzo IP gateway per la porta IPMI. Premere `Enter` al termine dell'operazione.
11. Collegare un'estremità di un cavo Ethernet alla porta IPMI e l'altra estremità a uno switch.

    La porta IPMI per questo nodo è pronta per l'uso.

12. Ripetere questa procedura per tutti gli altri nodi NetApp HCI con porte IPMI non configurate.

Modificare la password IPMI predefinita per i nodi H410C e H410S

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

Prima di iniziare

L'indirizzo IP IPMI è stato configurato per ciascun nodo di calcolo e storage.

Fasi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e individuare l'indirizzo IP IPMI del nodo.

2. Immettere il nome utente `ADMIN` e password `ADMIN` al prompt di login.
3. Una volta effettuato l'accesso, fare clic sulla scheda **Configuration** (Configurazione).
4. Fare clic su **utenti**.
5. Selezionare `ADMIN` E fare clic su **Modify User** (Modifica utente).
6. Selezionare la casella di controllo **Change Password** (Modifica password).
7. Immettere una nuova password nei campi **Password** e **Conferma password**.
8. Fare clic su **Modify**, quindi su **OK**.
9. Ripetere questa procedura per tutti gli altri nodi NetApp HCI H410C e H410S con password IPMI predefinite.

Modificare la password IPMI predefinita per i nodi H610C, H615C e H610S

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

Prima di iniziare

L'indirizzo IP IPMI è stato configurato per ciascun nodo di calcolo e storage.

Fasi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e individuare l'indirizzo IP IPMI del nodo.
2. Immettere il nome utente `root` e password `calvin` al prompt di login.
3. Una volta effettuato l'accesso, fare clic sull'icona di navigazione del menu in alto a sinistra della pagina per aprire il cassetto della barra laterale.
4. Fare clic su **Impostazioni**.
5. Fare clic su **Gestione utenti**.
6. Selezionare l'utente **Administrator** dall'elenco.
7. Attivare la casella di controllo **Change Password** (Modifica password).
8. Immettere una nuova password complessa nei campi **Password** e **Conferma password**.
9. Fare clic su **Save** (Salva) nella parte inferiore della pagina.
10. Ripetere questa procedura per tutti gli altri nodi NetApp HCI H610C, H615C o H610S con password IPMI predefinite.

Trova ulteriori informazioni

- "Documentazione NetApp SolidFire Active IQ"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Implementare NetApp HCI

Accedi al NetApp Deployment Engine

Panoramica delle opzioni di accesso al NetApp Deployment Engine

Per implementare NetApp HCI, è necessario accedere al motore di implementazione NetApp su uno dei nodi di storage NetApp H-Series tramite l'indirizzo IPv4 assegnato all'interfaccia Bond1G, che è l'interfaccia logica che combina le porte A e B per i nodi di storage. Questo nodo di storage diventa il nodo di storage di controllo per il processo di implementazione. A seconda dell'ambiente in uso, è necessario configurare l'indirizzo IPv4 o recuperarlo da uno dei nodi di storage.

> È possibile accedere al NetApp Deployment Engine solo utilizzando l'interfaccia Bond1G di un nodo di storage. L'utilizzo dell'interfaccia Bond10G, l'interfaccia logica che combina le porte C e D per i nodi di storage, non è supportata.

Per accedere al NetApp Deployment Engine, utilizza uno dei seguenti metodi che meglio descrivono il tuo ambiente di rete:

Scenario	Metodo
DHCP non è presente nell'ambiente	"Accesso al NetApp Deployment Engine in ambienti senza DHCP"
Nell'ambiente in uso è presente il protocollo DHCP	"Accedi al NetApp Deployment Engine negli ambienti con DHCP"
Si desidera assegnare manualmente tutti gli indirizzi IP	"Assegnare manualmente gli indirizzi IP per accedere al NetApp Deployment Engine"

Trova ulteriori informazioni

- "Configurare l'accesso completo all'interfaccia utente Web Domain Name"

Accesso al NetApp Deployment Engine in ambienti senza DHCP

Quando DHCP non è in uso sulla rete, è necessario impostare un indirizzo IPv4 statico sull'interfaccia Bond1G di uno dei nodi di storage (noto anche come nodo di storage di controllo) che si utilizzerà per accedere a NetApp Deployment Engine. Il NetApp Deployment Engine sul nodo storage di controllo rileverà e comunicherà con altri nodi di calcolo e storage utilizzando indirizzi IPv4 configurati automaticamente sulle interfacce Bond10G di tutti i nodi. Utilizzare questo metodo a meno che la rete non presenti requisiti speciali.

Di cosa hai bisogno

- L'utente o l'amministratore di rete hanno completato le operazioni descritte nel documento istruzioni per l'installazione e l'installazione.
- Si dispone dell'accesso fisico ai nodi NetApp HCI.

- Tutti i nodi NetApp HCI sono accesi.
- DHCP non è abilitato per le reti NetApp HCI e i nodi NetApp HCI non hanno ottenuto indirizzi IP dai server DHCP.
- La rete di gestione NetApp HCI è configurata come VLAN nativa sulle interfacce Bond1G e Bond10G di tutti i nodi.

Fasi

1. Inserire un KVM nella parte posteriore di uno dei nodi di storage NetApp HCI (questo nodo diventerà il nodo di storage di controllo).
2. Configurare l'indirizzo IP, la subnet mask e l'indirizzo del gateway per Bond1G nell'interfaccia utente. Se necessario, è anche possibile configurare un ID VLAN per la rete Bond1G.

   Non è possibile riutilizzare questo indirizzo IPv4 in un secondo momento durante l'implementazione con NetApp Deployment Engine.

3. Aprire un browser Web su un computer in grado di accedere alla rete di gestione NetApp HCI.
4. Individuare l'indirizzo IP assegnato al nodo di storage di controllo. Ad esempio:

   ```
   http://<Bond1G IP address>
   ```

   Assicurarsi di utilizzare HTTP qui.

   In questo modo si passa all'interfaccia utente di NetApp Deployment Engine.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Accedi al NetApp Deployment Engine negli ambienti con DHCP

Negli ambienti in cui i server acquisiscono automaticamente la configurazione IPv4 da DHCP, è possibile accedere a NetApp Deployment Engine utilizzando l'indirizzo IPv4 assegnato all'interfaccia Bond1G su uno dei nodi di storage. È possibile utilizzare una chiavetta USB per recuperare l'indirizzo IPv4 da uno dei nodi di storage. NetApp Deployment Engine rileva automaticamente altri nodi di calcolo e storage che utilizzano indirizzi IPv4 assegnati da DHCP. Non utilizzare questo metodo a meno che la rete non presenti requisiti speciali.

Di cosa hai bisogno

- L'utente o l'amministratore di rete hanno completato le operazioni descritte nel documento istruzioni per l'installazione e l'installazione.
- Si dispone dell'accesso fisico ai nodi NetApp HCI.
- Tutti i nodi NetApp HCI sono accesi.
- DHCP è attivato sulle reti di storage e gestione NetApp HCI.

- Il pool di indirizzi DHCP è abbastanza grande da ospitare due indirizzi IPv4 per nodo NetApp HCI.

> Affinché l'implementazione NetApp HCI abbia esito positivo, tutti i nodi dell'implementazione devono disporre di indirizzi IPv4 acquisiti o configurati automaticamente (non è possibile combinare metodi di assegnazione degli indirizzi IPv4).

A proposito di questa attività

Se DHCP viene utilizzato solo per la rete di storage (interfacce Bond10G), attenersi alla procedura descritta nel xref:./docs/"Accesso al NetApp Deployment Engine in ambienti senza DHCP" Per accedere al NetApp Deployment Engine.

Fasi

1. Attendere alcuni minuti per consentire ai nodi di richiedere gli indirizzi IP.
2. Scegliere un nodo di storage e inserire una chiavetta USB nel nodo. Lasciarlo per almeno cinque secondi.
3. Rimuovere la chiavetta USB e inserirla nel computer.
4. Aprire `readme.html` file. In questo modo si passa all'interfaccia utente di NetApp Deployment Engine.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Assegnare manualmente gli indirizzi IP per accedere al NetApp Deployment Engine

È possibile assegnare manualmente indirizzi IPv4 statici alle interfacce Bond1G e Bond10G su tutti i nodi NetApp HCI per accedere al motore di implementazione NetApp e implementare NetApp HCI. Non utilizzare questo metodo a meno che la rete non presenti requisiti speciali.

Di cosa hai bisogno

- L'utente o l'amministratore di rete hanno completato le operazioni descritte nel documento istruzioni per l'installazione e l'installazione.
- Si dispone dell'accesso fisico ai nodi NetApp HCI.
- Tutti i nodi NetApp HCI sono accesi.
- DHCP non è abilitato per le reti NetApp HCI e i nodi NetApp HCI non hanno ottenuto indirizzi IP dai server DHCP. NOTA: Tutti gli indirizzi IP assegnati manualmente prima di utilizzare NetApp Deployment Engine per implementare il sistema sono temporanei e non possono essere riutilizzati. Se si sceglie di assegnare manualmente gli indirizzi IP, è necessario mettere da parte un secondo set permanente di indirizzi IP inutilizzati che è possibile assegnare durante l'implementazione finale.

A proposito di questa attività

In questa configurazione, i nodi di calcolo e storage utilizzeranno indirizzi IPv4 statici per rilevare e comunicare con altri nodi durante l'implementazione. Questa configurazione non è consigliata.

Fasi

1. Inserire un KVM nella parte posteriore di uno dei nodi di storage NetApp HCI (questo nodo diventerà il nodo di storage di controllo).
2. Configurare l'indirizzo IP, la subnet mask e l'indirizzo del gateway per Bond1G e Bond10G nell'interfaccia

utente. È inoltre possibile configurare un ID VLAN per ogni rete, se necessario.

3. Ripetere il passaggio 2 per i nodi di calcolo e storage rimanenti.
4. Aprire un browser Web su un computer in grado di accedere alla rete di gestione NetApp HCI.
5. Individuare l'indirizzo IP Bond1G assegnato al nodo di storage di controllo. Ad esempio:

```
http://<Bond1G IP address>
```

In questo modo si passa all'interfaccia utente di NetApp Deployment Engine.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Avviare l'implementazione

Prima di continuare con l'implementazione di NetApp HCI, è necessario leggere e comprendere i contratti di licenza per l'utente finale.

Fasi

1. Nella pagina **Benvenuti in NetApp HCI**, fare clic su **Guida introduttiva**.
2. Nella pagina **Prerequisiti**, procedere come segue:
   a. Assicurarsi che ogni prerequisito sia soddisfatto e fare clic su ciascuna casella di controllo associata per confermare.
   b. Fare clic su **continua**.
3. Nella pagina **licenze utente finale**, procedere come segue:
   a. Leggi il Contratto di licenza con l'utente finale di NetApp.
   b. Se si accettano i termini, fare clic su **Accetto** nella parte inferiore del testo del contratto.
   c. Leggi il contratto di licenza con l'utente finale di VMware.
   d. Se si accettano i termini, fare clic su **Accetto** nella parte inferiore del testo del contratto.
   e. Fare clic su **continua**.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Importare un profilo di installazione

Se hai ottenuto NetApp "ConfigBuilder" Output del profilo per l'installazione, è possibile importarlo durante il processo di installazione di NetApp HCI per compilare automaticamente i campi nel motore di implementazione NetApp. Questo è un passaggio facoltativo.

A proposito di questa attività

Se si importa un profilo di installazione, è comunque necessario immettere le credenziali per NetApp HCI da utilizzare nella pagina **credenziali** del motore di implementazione NetApp.

> Se i campi nel profilo di installazione vengono lasciati vuoti o inseriti in modo errato, potrebbe essere necessario inserire o correggere manualmente le informazioni nelle pagine del NetApp Deployment Engine. Se è necessario aggiungere o correggere le informazioni, assicurarsi di aggiornare le informazioni contenute nei record e nel profilo di installazione.

Importare un profilo

1. Nella pagina **Installation Profile** (Profilo installazione), fare clic su **Browse** (Sfoglia) per cercare e caricare il profilo di installazione.
2. Nella finestra di dialogo del file, selezionare e aprire il file JSON del profilo.
3. Una volta importato il profilo, fare clic su **continua**.

   È possibile scorrere ciascuna pagina del NetApp Deployment Engine e verificare le impostazioni importate dal profilo di installazione.

Continuare senza importare un profilo

1. Per saltare la fase di importazione, nella pagina **Installation Profile** (Profilo di installazione), fare clic su **Continue** (continua).

Trova ulteriori informazioni

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

Configurare VMware vSphere

Configurazione di VMware vSphere

NetApp HCI utilizza i componenti vCenter Server ed ESXi di VMware vSphere. VCenter Server viene utilizzato per gestire e monitorare l'hypervisor VMware ESXi installato su ciascun nodo di calcolo. È possibile installare e configurare una nuova implementazione vSphere, che installa anche il plug-in NetApp Element per vCenter Server, oppure unirvi ed estendere un'implementazione vSphere esistente.

Quando si utilizza NetApp Deployment Engine per installare una nuova implementazione vSphere, tenere presenti i seguenti avvertimenti:

- NetApp Deployment Engine installa la nuova appliance vCenter Server con l'opzione di implementazione di piccole dimensioni.
- La licenza vCenter Server è una licenza di valutazione temporanea. Per continuare a utilizzare il prodotto dopo il periodo di valutazione, è necessario ottenere una nuova chiave di licenza da VMware e aggiungerla all'inventario delle licenze di vCenter Server.

> Se la configurazione dell'inventario vSphere utilizza una cartella per memorizzare il cluster NetApp HCI all'interno del data center vCenter, alcune operazioni, come l'espansione delle risorse di calcolo NetApp HCI, non avranno esito positivo. Assicurarsi che il cluster NetApp HCI si trovi direttamente sotto il data center nell'albero di inventario del client Web vSphere e non sia memorizzato in una cartella. Per ulteriori informazioni, consulta l'articolo della Knowledge base di NetApp.

Se si installa un nuovo vCenter Server, è possibile installare uno switch vSphere standard o uno switch vSphere Distributed (VDS) durante la configurazione di rete. Un VDS consente una gestione semplificata e centralizzata della configurazione di rete delle macchine virtuali dopo l'implementazione di NetApp HCI. La funzionalità dei servizi dati cloud su NetApp HCI richiede un VDS; gli switch standard vSphere non sono supportati per i servizi dati cloud.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Configurare un nuovo ambiente VMware vSphere

È possibile implementare un nuovo ambiente vSphere come parte del processo di installazione di NetApp HCI fornendo alcune informazioni di rete che vSphere dovrebbe utilizzare. Se si configura vSphere utilizzando un indirizzo IP, l'indirizzo non può essere modificato dopo l'installazione.

Di cosa hai bisogno

Sono state ottenute le informazioni di rete per l'ambiente vSphere pianificato.

Fasi

1. Fare clic su **Configura una nuova implementazione vSphere**.
2. Selezionare la versione di vSphere che il sistema deve installare durante l'implementazione.
3. Configurare il nuovo ambiente vSphere utilizzando una delle seguenti opzioni:

Opzione	Fasi
Utilizzare un nome di dominio (consigliato).	a. Fare clic su **Configura con un nome di dominio completo**. b. Immettere il nome di dominio del server vCenter nel campo **vCenter Server Fully Qualified Domain Name**. c. Inserire l'indirizzo IP del server DNS nel campo **DNS Server IP Address** (Indirizzo IP server DNS). d. Fare clic su **continua**.
Utilizzare un indirizzo IP.	a. Fare clic su **Configura utilizzando un indirizzo IP**. b. Fare clic su **continua**.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Partecipa a un'implementazione VMware vSphere esistente

È possibile configurare NetApp HCI per sfruttare un'implementazione vSphere esistente fornendo le informazioni e le credenziali di rete di vCenter Server.

Di cosa hai bisogno

- Se si sta partecipando a un'implementazione vSphere 6.7 esistente, assicurarsi che vCenter Server esegua la versione 6.7 Update 1.
- Se si sta partecipando a un'implementazione vSphere 6.5 esistente, assicurarsi che vCenter Server esegua la versione 6.5 Update 2 o successiva.
- Ottenere i dettagli di rete e le credenziali di amministratore per l'implementazione vSphere esistente.
- Se il plug-in NetApp Element per vCenter Server è registrato nell'istanza esistente di vCenter, è necessario "annulla registrazione" prima di continuare. Il plug-in viene registrato nuovamente al termine dell'implementazione di NetApp HCI.

A proposito di questa attività

Se si uniscono più sistemi vCenter Server connessi tramite la modalità collegata a vCenter, NetApp HCI riconosce solo uno dei sistemi vCenter Server.

> - A partire da Element Plug-in per vCenter Server 5.0, da utilizzare "Modalità collegata vCenter", È possibile registrare il plug-in Element da un nodo di gestione separato per ogni server vCenter che gestisce i cluster di storage NetApp SolidFire (consigliato).
> - Utilizzo di Element Plug-in per vCenter Server 4.10 e versioni precedenti per gestire le risorse cluster di altri vCenter Server utilizzando "Modalità collegata vCenter" è limitato solo ai cluster di storage locali.

Fasi

1. Fare clic su **partecipa ed estendi un'implementazione vSphere esistente**.
2. Inserire il nome di dominio o l'indirizzo IP nel campo **vCenter Server Domain Name or IP address** (Nome di dominio o indirizzo IP del server vCenter). Se si immette un nome di dominio, è necessario inserire anche l'indirizzo IP di un server DNS attivo nel campo **DNS Server IP Address** (Indirizzo IP server DNS) visualizzato.
3. Immettere le credenziali di un amministratore vSphere nei campi **Nome utente e Password**.
4. Fare clic su **continua**.

> Se il plug-in NetApp Element per il server vCenter è stato registrato durante questa fase, viene visualizzato un messaggio di errore che richiede di eseguire questa operazione "annulla registrazione" il plug-in. Eseguire questa operazione prima di continuare l'implementazione di NetApp HCI. Il plug-in viene registrato nuovamente al termine dell'implementazione.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Configurazione delle credenziali NetApp HCI

Durante l'implementazione, è possibile definire un set di credenziali da utilizzare nell'ambiente VMware vSphere appena implementato, nelle risorse di calcolo e storage NetApp HCI e nel nodo di gestione. Se si implementa NetApp HCI in un ambiente vSphere esistente, queste credenziali non vengono applicate al server vCenter esistente.

A proposito di questa attività

Tenere presenti i seguenti punti relativi alle credenziali impostate nel motore di implementazione di NetApp HCI:

- **NetApp Hybrid Cloud Control (HCC) o Element UI**: Per accedere a NetApp HCC o all'interfaccia utente Element una volta completata l'implementazione, utilizzare il nome utente e la password specificati in questa fase di implementazione.
- **VMware vCenter**: Per accedere a vCenter (se installato come parte dell'implementazione), utilizzare il nome utente con il suffisso `@vsphere.local` o il integrato `Administrator@vsphere.local` e la password specificata in questa fase di implementazione.
- **VMware ESXi**: Per accedere a ESXi sui nodi di calcolo, utilizzare il nome utente `root` e la stessa password specificata in questa fase di implementazione.

Per l'interazione con le istanze di VMware vCenter, NetApp Hybrid Cloud Control utilizzerà uno dei seguenti metodi:

- Il sistema integrato `Administrator@vsphere.local` Account utente sull'istanza di vCenter installata come parte della distribuzione.
- Le credenziali vCenter utilizzate per connettere l'implementazione di NetApp HCI a un server vCenter esistente.

Fasi

1. Nella pagina **credenziali**, immettere un nome utente nel campo **Nome utente**.
2. Inserire una password nel campo **Password**. La password deve essere conforme ai criteri visualizzati nella casella **la password deve contenere**.
3. Confermare la password nel campo **Re-Enter Password**.
4. Fare clic su **continua**.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"
- Per aggiornare le credenziali vCenter ed ESXi in un secondo momento, vedere "Aggiornare le credenziali vCenter o ESXi".

Selezionare una topologia di rete

Quando si collegano i nodi NetApp HCI, è possibile utilizzare diverse configurazioni dei cavi di rete in base alle proprie esigenze. Per ciascun nodo di calcolo, è possibile utilizzare tutte e sei le porte di rete, con diversi tipi di traffico assegnati a ciascuna coppia di porte, oppure utilizzare due porte con tutti i tipi di traffico assegnati alle porte. I nodi di

storage utilizzano la configurazione standard a quattro cavi. La scelta influisce sui nodi di calcolo selezionabili nell'inventario.

Di cosa hai bisogno

Se si sceglie la topologia di rete a due cavi per i nodi di calcolo, considerare i seguenti requisiti:

- Una volta completata l'implementazione, è possibile richiedere una licenza VMware vSphere Enterprise Plus.
- La configurazione degli switch di rete e di rete è stata verificata correttamente.
- Il tagging VLAN è necessario per le reti storage e vMotion per tutti i nodi di calcolo e storage.

Fasi

1. Nella pagina **topologia di rete**, selezionare una topologia di nodo di calcolo che si adatti al modo in cui sono stati installati i nodi di calcolo per NetApp HCI:
   - **6 opzione cavo**: L'opzione a sei cavi fornisce porte dedicate per ogni tipo di traffico (gestione, macchina virtuale e storage). È possibile attivare vSphere Distributed Switch (VDS) come opzione. L'abilitazione di VDS consente di configurare uno switch distribuito, consentendo una gestione semplificata e centralizzata della configurazione di rete delle macchine virtuali al termine dell'implementazione di NetApp HCI. Se la si attiva, è necessario disporre di una licenza vSphere Enterprise Plus pronta per essere applicata dopo l'implementazione.
   - **2 opzione cavo**: L'opzione a due cavi combina il traffico di gestione, macchina virtuale e storage su due porte collegate. Questa opzione di cablaggio richiede VDS e la attiva automaticamente. È necessario disporre di una licenza vSphere Enterprise Plus pronta per l'applicazione dopo l'implementazione.
2. Alcune opzioni di cablaggio visualizzano più viste del pannello posteriore di diversi tipi di hardware del nodo. Scorrere le viste del pannello posteriore per vedere come collegare i cavi di rete per il modello di nodo specifico e l'opzione di cablaggio.
3. Al termine, fare clic su **continua**.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Selezione dell'inventario

Selezione dell'inventario e compatibilità dei nodi

Quando si scelgono i nodi per l'implementazione, alcune limitazioni si applicano alle configurazioni dei nodi che è possibile combinare nella stessa implementazione.

Compatibilità dei nodi di storage

NetApp HCI supporta i nodi e i dischi di storage con SED (unità con crittografia automatica) e funzionalità di crittografia dei dischi FIPS 140-2. Durante l'implementazione o l'espansione di NetApp HCI, è possibile combinare nodi con diversi livelli di crittografia riportati, ma NetApp HCI supporta solo la forma di crittografia più base in questa situazione. Ad esempio, se si combina un nodo di storage che supporta la crittografia FIPS con nodi che supportano solo la crittografia SED, la crittografia SED è supportata con questa configurazione, ma la crittografia del disco FIPS non lo è.

> L'aggiunta di nodi di storage in grado di crittografare le unità FIPS al cluster di storage non attiva automaticamente la funzione di crittografia delle unità FIPS. Dopo aver implementato o ampliato un'installazione con i nodi compatibili con FIPS, è necessario attivare manualmente la crittografia del disco FIPS. Vedere "Documentazione software Element" per istruzioni.

Tutti i nodi di storage devono eseguire la stessa versione minore del software Element per essere compatibili con la stessa implementazione. Ad esempio, non è possibile combinare un nodo di storage che esegue Element 11.3.1 con altri nodi di storage che eseguono Element 11.5.

> A seconda della configurazione hardware del nodo, i nodi di storage H410S potrebbero essere visualizzati nell'elenco di inventario etichettati come nodi di storage H300S, H500S o H700S.

NetApp HCI supporta solo alcuni modelli di nodi di storage in cluster di storage a due nodi. Per ulteriori informazioni, vedere "cluster di storage a due nodi" O le Note di rilascio per la versione di NetApp HCI in uso.

> Per le implementazioni di cluster di storage a due nodi, i tipi di nodi di storage sono limitati ai nodi con dischi da 480 GB e 960 GB.

Compatibilità dei nodi di calcolo

I nodi di calcolo devono soddisfare i seguenti requisiti per essere selezionabili come inventario:

- Le generazioni di CPU in tutti i nodi di calcolo devono corrispondere per la corretta funzionalità di VMware vMotion. Dopo aver selezionato un nodo di calcolo dall'inventario, non è possibile selezionare nodi di calcolo con diverse generazioni di CPU.
- Non è possibile combinare nodi di calcolo con nodi di calcolo abilitati alla GPU nello stesso cluster di calcolo. Se si seleziona un nodo di calcolo abilitato alla GPU, i nodi di calcolo solo CPU diventano non selezionabili e viceversa.
- La versione software in esecuzione sul nodo di calcolo deve corrispondere alla versione principale e minore del NetApp Deployment Engine che ospita l'implementazione. In caso contrario, è necessario eseguire una nuova immagine del nodo di calcolo utilizzando il processo RTFI. Per istruzioni, consulta gli articoli della Knowledge base di NetApp relativi a RTFI.
- Per poter essere selezionato nell'elenco **Compute Nodes** (nodi di calcolo), il nodo di calcolo deve avere la configurazione del cablaggio selezionata nella pagina Network Topology (topologia di rete).
- Le configurazioni di cablaggio di rete per i nodi di calcolo dello stesso modello devono corrispondere all'interno di un singolo cluster di calcolo.

Trova ulteriori informazioni

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

Selezionare l'inventario

Nella pagina **inventario**, il motore di implementazione NetApp rileva automaticamente i nodi di calcolo e storage disponibili, consentendo di selezionare e aggiungere tutte le risorse NetApp HCI all'implementazione. Se un nodo non soddisfa i requisiti per l'implementazione, non è selezionabile e i problemi vengono indicati come errori. È possibile posizionare il cursore sull'errore nella riga del nodo per visualizzare una

spiegazione. Quando si sceglie l'inventario dei nodi nella pagina inventario, il nodo storage che ospita NetApp Deployment Engine viene selezionato automaticamente e non è possibile deselezionarlo.

Di cosa hai bisogno

I frame jumbo devono essere abilitati per un corretto rilevamento dell'inventario. Se nell'inventario non sono presenti nodi o solo un sottoinsieme di nodi, verificare che le porte dello switch utilizzate per i nodi NetApp HCI (tutte le interfacce SFP+/SFP28) siano configurate con frame jumbo.

Fasi

1. Nella pagina **Inventory**, visualizzare l'elenco dei nodi disponibili.

   Se il sistema non rileva alcun inventario, viene visualizzato un errore. Correggere l'errore prima di continuare. Se il sistema utilizza DHCP per l'assegnazione dell'indirizzo IP, le risorse di storage e di calcolo potrebbero non apparire immediatamente nell'inventario.

2. Facoltativo: Se una risorsa non viene visualizzata immediatamente nell'inventario o se si risolve un errore e si desidera aggiornare l'inventario, fare clic su **Refresh Inventory** (Aggiorna inventario). Potrebbe essere necessario aggiornare l'inventario più volte.
3. Facoltativo: Per filtrare l'inventario sugli attributi del nodo, ad esempio il tipo di nodo:
   a. Fare clic su **Filter** (filtro) nell'intestazione degli elenchi **Compute Nodes** (nodi di calcolo) o **Storage Nodes** (nodi di storage).
   b. Scegliere i criteri dagli elenchi a discesa.
   c. Sotto gli elenchi a discesa, immettere le informazioni per soddisfare i criteri.
   d. Fare clic su **Aggiungi filtro**.
   e. Eliminare i singoli filtri facendo clic su **X** accanto a un filtro attivo oppure deselezionare tutti i filtri facendo clic su **X** sopra l'elenco dei filtri.
4. Selezionare tutti i nodi di calcolo forniti con il sistema dall'elenco **nodi di calcolo**.

   Per procedere con l'implementazione, è necessario selezionare almeno due nodi di calcolo.

5. Selezionare tutti i nodi di storage forniti con il sistema dall'elenco **nodi di storage**.

   Per procedere con l'implementazione, è necessario selezionare almeno due nodi di storage.

6. Facoltativo: Se viene contrassegnata una casella di selezione del nodo di storage, tale nodo supera il 33% della capacità totale del cluster di storage. Fare delle seguenti operazioni:
   - Deselezionare la casella di selezione per il nodo di storage contrassegnato.
   - Selezionare nodi di storage aggiuntivi per distribuire in modo più equo la capacità del cluster di storage tra i nodi.
7. Fare clic su **continua**.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"
- "Documentazione software SolidFire ed Element"

Configurare le impostazioni di rete

NetApp HCI fornisce una pagina delle impostazioni di rete con diverse sezioni per semplificare la configurazione di rete. È possibile passare da una sezione all'altra e immettere informazioni o assegnare indirizzi IP per host e nodi in ciascuna rete.

Di cosa hai bisogno

- Sono state ottenute le seguenti informazioni:
  - Il prefisso di denominazione pianificato per gli host e il cluster di storage
  - Tutte le subnet mask pianificate, l'indirizzo IP iniziale, il gateway predefinito e gli ID VLAN per le reti di gestione, iSCSI e vMotion
  - Subnet mask, indirizzo IP, gateway predefinito e ID VLAN per qualsiasi implementazione pianificata di VMware vCenter
  - L'indirizzo del server NTP (Network Time Protocol) per NetApp HCI
  - Le informazioni sull'indirizzo IP del server DNS per NetApp HCI
- Se si sta implementando uno switch distribuito vSphere, si dispone di una licenza vSphere Enterprise Plus pronta per essere applicata al termine dell'implementazione.
- Se sono stati assegnati ID VLAN alle porte del nodo durante la configurazione dell'interfaccia utente terminale (TUI), tali porte sono state configurate con lo stesso ID VLAN durante la configurazione di rete. Non è necessario configurare le porte host contrassegnate come porte di accesso o VLAN native sulle porte degli switch collegati.
- La configurazione dello switch di rete è stata verificata correttamente. Configurazioni dello switch non corrette (ad esempio, VLAN o dimensioni MTU non corrette) possono causare errori di implementazione.

A proposito di questa attività

Se è stata selezionata la topologia di rete a due cavi per i nodi di calcolo, è necessario utilizzare gli ID VLAN per le reti vMotion e storage per tutti i nodi di calcolo e storage nell'implementazione (gli ID VLAN sono opzionali per le reti di gestione). Tenere presente che NetApp HCI convalida gli indirizzi IP immessi durante questi passaggi, ma è possibile disattivare questa convalida con il pulsante **la convalida della rete attiva è**. NetApp HCI esegue anche controlli su altre informazioni inserite durante queste fasi, ad esempio per garantire che non vi siano sovrapposizioni di subnet, per garantire che non siano assegnati ID VLAN a più reti e altre validazioni di base.

> Negli ambienti che richiedono il tagging VLAN lato host prima dell'implementazione, se sono stati configurati ID VLAN sui nodi di calcolo e storage in modo che siano rilevabili dal NetApp Deployment Engine, assicurarsi di utilizzare le VLAN corrette durante la configurazione delle impostazioni di rete nel NetApp Deployment Engine.

Se si sta implementando un cluster di storage a due o tre nodi, è possibile completare le informazioni sull'indirizzo IP per i nodi di controllo nella pagina **Impostazioni di rete**.

> Nelle pagine di assegnazione degli indirizzi IP, le informazioni immesse nella modalità **assegnazione automatica degli indirizzi IP** non influiscono sulle informazioni immesse nella modalità **assegnazione manuale degli indirizzi IP** e viceversa. Se si immettono indirizzi IP in entrambe le modalità, NetApp HCI utilizza le informazioni dell'indirizzo IP in qualsiasi modalità attiva quando si fa clic su **continua** nella parte inferiore della pagina.

Risoluzione dei problemi comuni

NetApp HCI esegue controlli sulle informazioni inserite in queste pagine. Di seguito sono riportati alcuni problemi e soluzioni comuni:

Problema	Soluzione alternativa
Nella modalità di assegnazione automatica dell'indirizzo IP, dopo aver inserito un indirizzo IP iniziale, viene visualizzato il messaggio `IPs in the range are in use`: Con un elenco a discesa scorrevole degli indirizzi IP in uso.	NetApp HCI ha assegnato un intervallo contiguo di indirizzi IP, ma uno o più indirizzi IP sono già in uso. Liberare gli indirizzi IP in uso e riprovare oppure utilizzare la modalità di assegnazione manuale degli indirizzi IP per assegnare indirizzi IP specifici.
Dopo aver inserito un gateway predefinito, viene visualizzato il messaggio `The gateway is not valid`.	L'indirizzo IP del gateway predefinito non corrisponde alla subnet fornita oppure si è verificato un problema relativo alla rete o al server da risolvere. Per ulteriori informazioni, consultare i seguenti articoli della Knowledge base di NetApp: • "Risolvere i problemi di un gateway non valido nel NetApp Deployment Engine" • "Il gateway non è valido nel NetApp Deployment Engine"
È possibile completare diverse pagine di configurazione **Impostazioni di rete** e rendersi conto che una delle pagine precedenti della sequenza contiene informazioni errate.	Utilizzando la sequenza di pagine numerate nella parte superiore della pagina, è possibile selezionare una pagina già completata e modificare le informazioni. Al termine, fare clic su **continua** nelle pagine completate per tornare alla pagina corrente.

Configurare le impostazioni DNS e NTP

Fasi

1. Nella pagina **DNS/NTP**, immettere le informazioni relative al server DNS e NTP per NetApp HCI nei seguenti campi:

Campo	Descrizione
Indirizzo IP del server DNS 1	L'indirizzo IP del server DNS primario per NetApp HCI. Se è stato specificato un server DNS nella pagina di configurazione di vCenter, questo campo viene compilato e di sola lettura.
Indirizzo IP server DNS 2 (opzionale)	Indirizzo IP opzionale di un server DNS secondario per NetApp HCI.
Indirizzo server NTP 1	L'indirizzo IP o il nome di dominio completo del server NTP primario per questa infrastruttura.
Indirizzo server NTP 2 (opzionale)	Un indirizzo IP opzionale o un nome di dominio completo del server NTP secondario per questa infrastruttura.

Assegnare gli ID VLAN

Nella pagina **VLAN ID**, è possibile assegnare gli ID VLAN alle reti NetApp HCI. È anche possibile scegliere di non utilizzare gli ID VLAN. Se è stata selezionata la topologia di rete a due cavi per i nodi di calcolo, è necessario utilizzare gli ID VLAN per le reti vMotion e storage per tutti i nodi di calcolo e storage nell'implementazione (gli ID VLAN sono opzionali per le reti di gestione).

> Quando si assegnano gli ID VLAN, si configurano i tag VLAN che NetApp HCI applicherà al traffico di rete. Non è necessario inserire la VLAN nativa come ID VLAN; per utilizzare la VLAN nativa per una rete, lasciare vuoto il campo appropriato.

Fasi

Scegliere una delle seguenti opzioni:

Opzione	Fasi
Assegnare gli ID VLAN	1. Selezionare **Sì** per l'opzione **assegnare ID VLAN**. 2. Nella colonna **VLAN ID**, inserire un tag VLAN da utilizzare per ogni tipo di traffico di rete che si desidera assegnare a una VLAN. Sia il traffico vMotion che il traffico iSCSI devono utilizzare un ID VLAN non condiviso. 3. Fare clic su **continua**.
Non assegnare ID VLAN	1. Selezionare **No** per l'opzione **si assegneranno gli ID VLAN**. 2. Fare clic su **continua**.

Configurare la rete di gestione

Nella pagina **Gestione**, è possibile scegliere di inserire NetApp HCI automaticamente gli intervalli di indirizzi IP per le reti di gestione in base a un indirizzo IP iniziale, oppure di inserire manualmente tutte le informazioni relative agli indirizzi IP.

Fasi

Scegliere una delle seguenti opzioni:

Opzione	Fasi
Assegnare automaticamente gli indirizzi IP	1. Selezionare l'opzione **Assegna automaticamente indirizzi IP**. 2. Nella colonna **Subnet**, immettere una definizione di subnet in formato CIDR per ciascuna VLAN. 3. Nella colonna **Default Gateway**, immettere un gateway predefinito per ogni VLAN. 4. Nella colonna **Subnet**, inserire un indirizzo IP iniziale da utilizzare per ogni VLAN e tipo di nodo. NetApp HCI inserisce automaticamente gli indirizzi IP finali per ciascun host o gruppo di host. 5. Fare clic su **continua**.
Assegnare manualmente gli indirizzi IP	1. Selezionare l'opzione **assegnazione manuale degli indirizzi IP**. 2. Nella colonna **Subnet**, immettere una definizione di subnet in formato CIDR per ciascuna VLAN. 3. Nella colonna **Default Gateway**, immettere un gateway predefinito per ogni VLAN. 4. Nella riga di ciascun host o nodo, immettere l'indirizzo IP dell'host o del nodo. 5. Inserire l'indirizzo MVIP (Management Virtual IP) per la rete di gestione. 6. Fare clic su **continua**.

Configurare la rete vMotion

Nella pagina **vMotion**, è possibile scegliere di inserire NetApp HCI automaticamente gli intervalli di indirizzi IP per la rete vMotion in base a un indirizzo IP iniziale, oppure di inserire manualmente tutte le informazioni relative all'indirizzo IP.

Fasi

Scegliere una delle seguenti opzioni:

Opzione	Fasi
Assegnare automaticamente gli indirizzi IP	1. Selezionare l'opzione **Assegna automaticamente indirizzi IP**. 2. Nella colonna **Subnet**, immettere una definizione di subnet in formato CIDR per ciascuna VLAN. 3. (Facoltativo) nella colonna **Default Gateway**, inserire un gateway predefinito per ogni VLAN. 4. Nella colonna **Subnet**, inserire un indirizzo IP iniziale da utilizzare per ogni VLAN e tipo di nodo. NetApp HCI inserisce automaticamente gli indirizzi IP finali per ciascun host o gruppo di host. 5. Fare clic su **continua**.
Assegnare manualmente gli indirizzi IP	1. Selezionare l'opzione **assegnazione manuale degli indirizzi IP**. 2. Nella colonna **Subnet**, immettere una definizione di subnet in formato CIDR per ciascuna VLAN. 3. (Facoltativo) nella colonna **Default Gateway**, inserire un gateway predefinito per ogni VLAN. 4. Nella riga di ciascun host o nodo, immettere l'indirizzo IP dell'host o del nodo. 5. Fare clic su **continua**.

Configurare la rete iSCSI

Nella pagina **iSCSI**, è possibile scegliere di inserire NetApp HCI automaticamente gli intervalli di indirizzi IP per la rete iSCSI in base a un indirizzo IP iniziale, oppure di inserire manualmente tutte le informazioni sull'indirizzo IP.

Fasi

Scegliere una delle seguenti opzioni:

Opzione	Fasi
Assegnare automaticamente gli indirizzi IP	1. Selezionare l'opzione **Assegna automaticamente indirizzi IP**. 2. Nella colonna **Subnet**, immettere una definizione di subnet in formato CIDR per la rete iSCSI. 3. (Facoltativo) nella colonna **Default Gateway**, inserire un gateway predefinito per la rete iSCSI. 4. Nella colonna **Subnet**, immettere un indirizzo IP iniziale da utilizzare per ciascun tipo di nodo. NetApp HCI inserisce automaticamente gli indirizzi IP finali per ciascun host o gruppo di host. 5. Fare clic su **continua**.
Assegnare manualmente gli indirizzi IP	1. Selezionare l'opzione **assegnazione manuale degli indirizzi IP**. 2. Nella colonna **Subnet**, immettere una definizione di subnet in formato CIDR per la rete iSCSI. 3. (Facoltativo) nella colonna **Default Gateway**, inserire un gateway predefinito per la rete iSCSI. 4. Nella sezione **nodo di gestione**, immettere un indirizzo IP per il nodo di gestione. 5. Per ciascun nodo nella sezione **Compute Nodes** (nodi di calcolo), inserire gli indirizzi IP iSCSI A e iSCSI B. 6. Nella riga **Storage Virtual IP (SVIP)**, immettere l'indirizzo IP SVIP per la rete iSCSI. 7. Nelle righe rimanenti, per ciascun host o nodo, immettere l'indirizzo IP per tale host o nodo. 8. Fare clic su **continua**.

Assegnare nomi di cluster e host

Nella pagina **Naming**, è possibile scegliere di inserire NetApp HCI automaticamente il nome del cluster e i nomi dei nodi nel cluster in base a un prefisso di denominazione, oppure di inserire manualmente tutti i nomi del cluster e dei nodi.

Fasi

Scegliere una delle seguenti opzioni:

Opzione	Fasi
Assegnare automaticamente i nomi del cluster e degli host	1. Selezionare l'opzione **assegnazione automatica dei nomi cluster/host**. 2. Nella sezione **prefisso di installazione**, immettere un prefisso di denominazione da utilizzare per tutti i nomi host dei nodi nel cluster (inclusi il nodo di gestione e i nodi di controllo). NetApp HCI compila automaticamente i nomi host in base al tipo di nodo, nonché i suffissi per i nomi di nodi comuni (ad esempio i nodi di calcolo e storage). 3. (Facoltativo) nella colonna **Naming Scheme**, modificare uno dei nomi risultanti per gli host. 4. Fare clic su **continua**.
Assegnare manualmente i nomi di cluster e host	1. Selezionare l'opzione **assegnazione manuale dei nomi cluster/host**. 2. Nella colonna **host / Cluster Name**, immettere il nome host per ciascun host e il nome del cluster di storage. 3. Fare clic su **continua**.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"
- "Documentazione software SolidFire ed Element"

Esaminare e implementare la configurazione

È possibile rivedere le informazioni fornite prima di iniziare la distribuzione. È inoltre possibile correggere eventuali informazioni errate o incomplete prima di procedere.

> Durante l'implementazione, il processo di installazione del nodo di gestione crea volumi con nomi che iniziano con `NetApp-HCI-` Nel cluster di storage Element e un account SolidFire che inizia con il nome `tenant_`. Non eliminare questi volumi o account; in questo modo si verificherà una perdita delle funzionalità di gestione.

Fasi

1. Facoltativo: Selezionare l'icona **Download** per scaricare le informazioni di installazione in formato CSV. È possibile salvare questo file e consultarlo in seguito per informazioni sulla configurazione.

> È possibile importare il file CSV come profilo di installazione nella pagina **Installation Profile** di NetApp Deployment Engine (NDE), se necessario durante un'installazione futura.

2. Espandere ciascuna sezione e rivedere le informazioni. Per espandere tutte le sezioni contemporaneamente, selezionare **Espandi tutto**.
3. Facoltativo: Per apportare modifiche alle informazioni in qualsiasi sezione visualizzata:
   a. Selezionare **Modifica** nella sezione corrispondente.
   b. Apportare le modifiche necessarie.
   c. Selezionare **continua** fino a visualizzare la pagina **Rivedi**. Le impostazioni precedenti vengono salvate in ogni pagina.
   d. Ripetere i passaggi 2 e 3 per apportare le altre modifiche necessarie.
4. Se non si desidera inviare statistiche del cluster e informazioni di supporto ai server SolidFire Active IQ ospitati da NetApp, deselezionare la casella di controllo finale.

   In questo modo si disattiva il monitoraggio diagnostico e dello stato di salute in tempo reale per NetApp HCI. La disattivazione di questa funzione elimina la possibilità per NetApp di supportare e monitorare in modo proattivo NetApp HCI per rilevare e risolvere i problemi prima che la produzione venga compromessa.

5. Se tutte le informazioni sono corrette, selezionare **Avvia implementazione**.

   Viene visualizzata una finestra di dialogo. In caso di problemi di connettività di rete o di interruzione dell'alimentazione durante il processo di configurazione finale, o in caso di perdita della sessione del browser, è possibile copiare l'URL visualizzato nella finestra di dialogo e utilizzarlo per accedere alla pagina di avanzamento dell'installazione finale.

6. Esaminare le informazioni nella finestra di dialogo e selezionare **Copia negli Appunti** per copiare l'URL negli Appunti.
7. Salvare l'URL in un file di testo sul computer.
8. Quando si è pronti per procedere con l'implementazione, selezionare **OK**.

   Viene avviata l'implementazione e viene visualizzata una pagina di avanzamento. Non chiudere la finestra del browser né allontanarsi dalla pagina di avanzamento fino al completamento dell'implementazione. Se la sessione del browser viene persa per qualsiasi motivo, è possibile accedere all'URL copiato in precedenza (e accettare eventuali avvisi di sicurezza visualizzati) per accedere nuovamente alla pagina di avanzamento dell'installazione finale.

   > Se l'implementazione non riesce, salvare il testo del messaggio di errore e contattare il supporto NetApp.

   Una volta completata l'implementazione, i nodi di calcolo potrebbero riavviarsi più di una volta prima di essere pronti per l'assistenza.

Al termine

Iniziare a utilizzare NetApp HCI selezionando **Avvia vSphere**.

- Per le installazioni NetApp HCI che utilizzano vSphere 6.7, questo collegamento avvia l'interfaccia Web di HTML5 vSphere. Per le installazioni che utilizzano vSphere 6.5, questo collegamento avvia l'interfaccia Web di Adobe Flash vSphere.
- Nelle configurazioni a due o tre nodi di storage, NDE configura i nodi di controllo per l'utilizzo del datastore locale sui nodi di calcolo. Di conseguenza, il client vSphere visualizza due avvisi **utilizzo del datastore su disco**. Per continuare, selezionare il collegamento **Ripristina verde** in ogni avviso.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"
- "Documentazione software SolidFire ed Element"

Attività post-implementazione

Attività post-implementazione

A seconda delle scelte effettuate durante il processo di implementazione, è necessario completare alcune attività finali prima che il sistema NetApp HCI sia pronto per l'uso in produzione, ad esempio l'aggiornamento di firmware e driver e l'esecuzione delle modifiche di configurazione finali necessarie.

- "Modifiche di rete supportate"
- "Disattiva il servizio smartd sui nodi di calcolo NetApp HCI"
- "Disattivare il comando "lacp-Individual" sugli switch configurati"
- "Creare un ruolo NetApp HCC in vCenter"
- "Aggiornamento di VMware vSphere"
- "Installare i driver della GPU per i nodi di calcolo abilitati alla GPU"
- "Accedi a NetApp Hybrid Cloud Control"
- "Riduci l'usura dei supporti di boot su un nodo di calcolo NetApp HCI"

Trova ulteriori informazioni

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

Modifiche di rete supportate

Dopo aver implementato NetApp HCI, è possibile apportare modifiche limitate alla configurazione di rete predefinita. Tuttavia, alcune impostazioni sono necessarie per un funzionamento regolare e un rilevamento corretto della rete. La modifica di queste impostazioni causerà un comportamento imprevisto e potrebbe impedire l'espansione delle risorse di calcolo e storage.

Dopo aver implementato il sistema, è possibile apportare le seguenti modifiche alla configurazione di rete predefinita in VMware vSphere in base ai requisiti di rete:

- Modificare i nomi di vSwitch
- Modificare i nomi dei gruppi di porte
- Aggiungere e rimuovere gruppi di porte aggiuntivi
- Modificare l'ordine di failover dell'interfaccia vmnic per eventuali gruppi di porte aggiuntivi aggiunti

Nodi di calcolo H300E, H500E, H700E e H410C

NetApp HCI prevede la seguente configurazione di rete per i nodi H300E, H500E, H700E e H410C.

Di seguito è riportata una configurazione a sei interfacce con VMware vSphere Distributed Switching (VDS). Questa configurazione è supportata solo se utilizzata con gli switch distribuiti VMware vSphere e richiede la licenza VMware vSphere Enterprise Plus.

Funzione di rete	vmkernel	vmnic (interfaccia fisica)
Gestione	vmk0	Vmnic2 (porta A), vmnic3 (porta B)
ISCSI-A.	vmk1	Vmnic5 (porta e)
ISCSI-B.	vmk2	Vmnic1 (porta D)
VMotion	vmk3	Vmnic4 (porta C), vmnic0 (porta F)

Di seguito è riportata una configurazione a sei interfacce con VMware vSphere Standard Switching (VSS). Questa configurazione utilizza VMware vSphere Standard Switch (VSS).

Funzione di rete	vmkernel	vmnic (interfaccia fisica)
Gestione	vmk0	Vmnic2 (porta A), vmnic3 (porta B)
ISCSI-A.	vmk2	Vmnic1 (porta e)
ISCSI-B.	vmk3	Vmnic5 (porta D)
VMotion	vmk1	Vmnic4 (porta C), vmnic0 (porta F)

Di seguito è riportata una configurazione a due interfacce. Questa configurazione è supportata solo se utilizzata con VMware vSphere Distributed Switch (VDS) e richiede la licenza VMware vSphere Enterprise Plus.

Funzione di rete	vmkernel	vmnic (interfaccia fisica)
Gestione	vmk0	Vmnic1 (porta D), vmnic5 (porta e)
ISCSI-A.	vmk1	Vmnic1 (porta e)
ISCSI-B.	vmk2	Vmnic5 (porta D)
VMotion	vmk3	Vmnic1 (porta C), vmnic5 (porta F)

Nodi di calcolo H610C

NetApp HCI prevede la seguente configurazione di rete per i nodi H610C.

Questa configurazione è supportata solo se utilizzata con VMware vSphere Distributed Switch (VDS) e richiede la licenza VMware vSphere Enterprise Plus.

Le porte A e B non sono utilizzate sul modello H610C.

Funzione di rete	vmkernel	vmnic (interfaccia fisica)
Gestione	vmk0	Vmnic2 (porta C), vmnic3 (porta D)
ISCSI-A.	vmk1	Vmnic3 (porta D)
ISCSI-B.	vmk2	Vmnic2 (porta C)
VMotion	vmk3	Vmnic2 (porta C), vmnic3 (porta D)

Nodi di calcolo H615C

NetApp HCI prevede la seguente configurazione di rete per i nodi H615C.

Questa configurazione è supportata solo se utilizzata con VMware vSphere Distributed Switch (VDS) e richiede la licenza VMware vSphere Enterprise Plus.

Funzione di rete	vmkernel	vmnic (interfaccia fisica)
Gestione	vmk0	Vmnic0 (porta A), vmnic1 (porta B)
ISCSI-A.	vmk1	Vmnic0 (porta B)
ISCSI-B.	vmk2	Vmnic1 (porta A)
VMotion	vmk3	Vmnic0 (porta A), vmnic1 (porta B)

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"
- "Documentazione software SolidFire ed Element"

Disattiva il servizio smartd sui nodi di calcolo NetApp HCI

Per impostazione predefinita, il `smartd` il servizio esegue periodicamente il polling dei dischi nei nodi di calcolo. Disattivare questo servizio su tutti i nodi di calcolo dopo aver implementato NetApp HCI.

Fasi

1. Utilizzando SSH o una sessione della console locale, accedere a VMware ESXi sul nodo di calcolo utilizzando le credenziali root.
2. Interrompere la corsa `smartd` servizio:

```
/etc/init.d/smartd stop
```

3. Impedire il `smartd` servizio dall'avvio:

```
chkconfig smartd off
```

4. Ripetere questi passaggi sugli altri nodi di calcolo dell'installazione.

Trova ulteriori informazioni

- "Disattivare il servizio Smartd in VMware ESXi"
- "Articolo della Knowledge base di VMware 2133286"

Disattivare il comando "lacp-Individual" sugli switch configurati

Per impostazione predefinita, lo switch Mellanox `lacp-individual` E lo switch Cisco `lacp suspend-individual` il comando rimane configurato dopo l'implementazione. Questo comando non è richiesto dopo l'installazione; se rimane configurato, può causare problemi di accesso al volume durante la risoluzione dei problemi o il riavvio di uno switch. Dopo l'implementazione, controllare la configurazione di ciascuno switch Mellanox e Cisco e rimuovere `lacp-individual` oppure `lacp suspend-individual` comando.

Fasi

1. Utilizzando SSH, aprire una sessione per lo switch.
2. Mostra la configurazione in esecuzione:

   ```
   show running-config
   ```

3. Controllare l'output di configurazione dello switch per `lacp-individual` oppure `lacp suspend-individual` comando.

   > Il `xxx-xxx` è il numero o i numeri di interfaccia forniti dall'utente. Se necessario, è possibile accedere al numero dell'interfaccia visualizzando le interfacce del gruppo di aggregazione di collegamenti multi-chassis: `show mlag interfaces`

   a. Per uno switch Mellanox, verificare che l'output contenga la seguente riga:

      ```
      interface mlag-port-channel xxx-xxx lacp-individual enable force
      ```

   b. Per uno switch Cisco, verificare che l'output contenga la seguente riga:

      ```
      interface mlag-port-channel xxx-xxx lacp suspend-individual enable force
      ```

4. Se il comando è presente, rimuoverlo dalla configurazione.
   a. Per uno switch Mellanox:

      ```
      no interface mlag-port-channel xxx-xxx lacp-individual enable force
      ```

b. Per uno switch Cisco:
   `no interface mlag-port-channel xxx-xxx lacp suspend-individual enable force`

5. Ripetere questa procedura per ogni switch della configurazione.

Trova ulteriori informazioni

- "Il nodo storage si spegne durante la risoluzione dei problemi"

Creare un ruolo NetApp HCC in vCenter

È necessario creare un ruolo NetApp HCC in vCenter per aggiungere manualmente le risorse vCenter (controller) o i nodi di calcolo (nodi) al nodo di gestione dopo l'installazione o per modificare i controller o i nodi esistenti.

Questo ruolo di NetApp HCC limita la visualizzazione dei servizi del nodo di gestione alle risorse solo NetApp.

A proposito di questa attività

- Questa procedura descrive i passaggi disponibili nella versione 6.7 di vSphere. L'interfaccia utente di vSphere potrebbe differire leggermente da quanto descritto a seconda della versione di vSphere installata. Per ulteriore assistenza, consultare la documentazione di VMware vCenter.
- A. "Creare un nuovo ruolo NetApp HCC", È necessario prima configurare un nuovo account utente in vCenter, creare un ruolo NetApp HCC e quindi assegnare le autorizzazioni utente.
- Per le configurazioni host NetApp ESXi, è necessario aggiornare l'account utente creato da NDE al nuovo ruolo NetApp HCC:
  - Utilizzare "questa opzione" Se l'host NetApp ESXi non esiste all'interno di un cluster host vCenter
  - Utilizzare "questa opzione" Se l'host NetApp ESXi esiste all'interno di un cluster host vCenter
- È possibile "configurare una risorsa controller" già presente nel nodo di gestione.
- Utilizza il nuovo ruolo di NetApp HCC per "aggiungere una risorsa o un nodo di calcolo" al nodo di gestione.

Creare un nuovo ruolo NetApp HCC

Impostare un nuovo account utente in vCenter, creare un ruolo NetApp HCC e assegnare le autorizzazioni utente.

Impostare un nuovo account utente in vCenter

Per configurare un nuovo account utente in vCenter, procedere come segue.

Fasi

1. Accedere a vSphere Web Client come `administrator@vsphere.local` o equivalente.
2. Dal menu, selezionare **Administration** (Amministrazione).
3. Nella sezione **Single Sign on**, selezionare **Users** e **Groups**.
4. Nell'elenco **dominio**, selezionare `vsphere.local` O il dominio LDAP.
5. Selezionare **Aggiungi utente**.
6. Completare il modulo **Aggiungi utente**.

Creare un nuovo ruolo NetApp HCC in vCenter

Per creare un nuovo ruolo di NetApp HCC in vCenter, attenersi alla seguente procedura.

Fasi

1. Selezionare **Edit role** (Modifica ruolo) e assegnare le autorizzazioni richieste.
2. Nel riquadro di navigazione a sinistra, selezionare **Global**.
3. Selezionare **Diagnostics** (Diagnostica) e **Licenses** (licenze).
4. Nel riquadro di navigazione a sinistra, selezionare **hosts**.
5. Selezionare **Maintenance**, **Power**, **Storage partition Configuration** e **firmware**.
6. Salva con nome `NetApp Role`.

Assegnare le autorizzazioni utente a vCenter

Attenersi alla seguente procedura per assegnare le autorizzazioni utente al nuovo ruolo NetApp HCC in vCenter.

Fasi

1. Dal menu, selezionare **hosts** e **Clusters**.
2. Nel riquadro di spostamento di sinistra, selezionare una delle seguenti opzioni:
   - VCenter di livello superiore.
   - Il vCenter desiderato se si è in Linked Mode (modalità collegata).

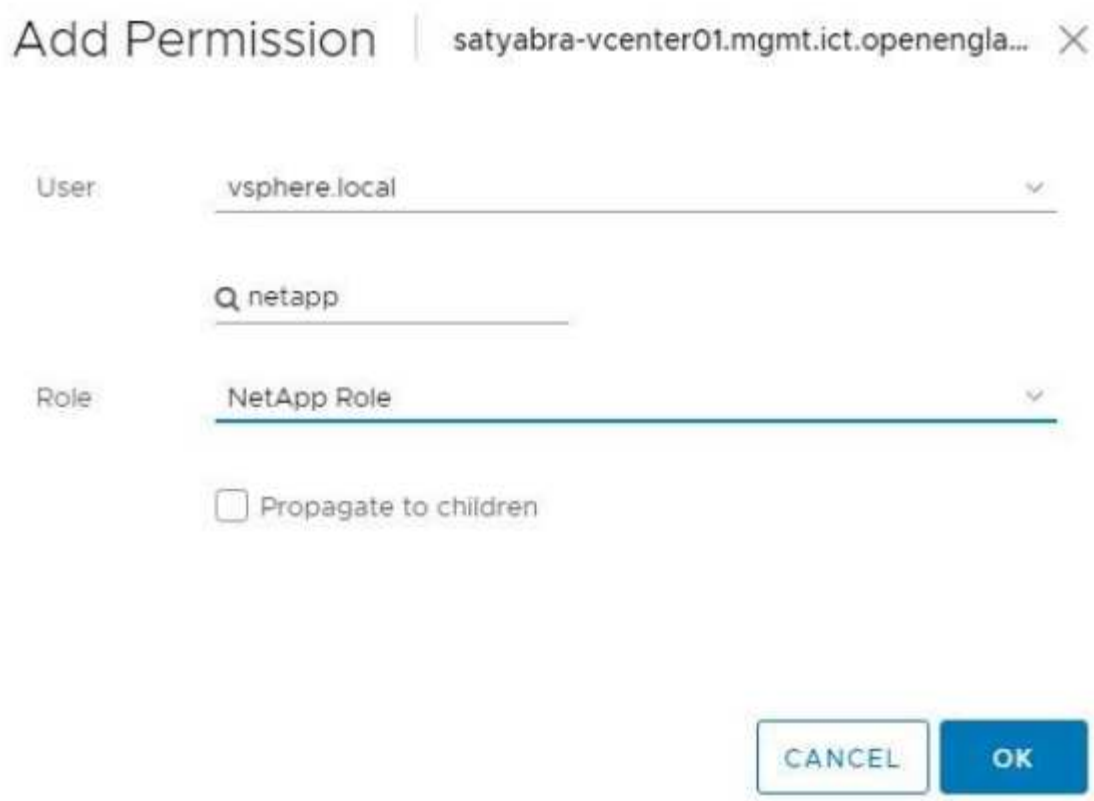
   > - A partire dal plug-in NetApp Element per vCenter Server 5.0, da utilizzare "Modalità collegata vCenter", È possibile registrare il plug-in Element da un nodo di gestione separato per ogni server vCenter che gestisce i cluster di storage NetApp SolidFire (consigliato).
   > - Utilizzo del plug-in NetApp Element per vCenter Server 4.10 e versioni precedenti per gestire le risorse cluster di altri vCenter Server utilizzando "Modalità collegata vCenter" è limitato solo ai cluster di storage locali.

3. Nel riquadro di navigazione a destra, selezionare **Permissions** (autorizzazioni).
4. Selezionare l'icona **+** per aggiungere il nuovo utente.

   Aggiungere i seguenti dettagli nella finestra **Aggiungi permesso**:

   a. Selezionare `vsphere.local` O il dominio LDAP
   b. Utilizzare la ricerca per trovare il nuovo utente creato in Impostare un nuovo account utente in vCenter.
   c. Selezionare `NetApp Role`.

      > Non selezionare **propaga ai figli**.



Assegnare le autorizzazioni utente al data center

Attenersi alla seguente procedura per assegnare le autorizzazioni utente al data center in vCenter.

Fasi

1. Nel riquadro di sinistra, selezionare **Datacenter**.
2. Nel riquadro di navigazione a destra, selezionare **Permissions** (autorizzazioni).
3. Selezionare l'icona **+** per aggiungere il nuovo utente.

   Aggiungere i seguenti dettagli nella finestra **Aggiungi permesso**:

   a. Selezionare `vsphere.local` O il dominio LDAP.

   b. Utilizzare la ricerca per trovare il nuovo utente HCC creato in Impostare un nuovo account utente in vCenter.

   c. Selezionare `ReadOnly role`.

   > Non selezionare **propaga ai figli**.

Assegnare le autorizzazioni utente agli archivi dati NetApp HCI

Per assegnare le autorizzazioni utente agli archivi dati NetApp HCI in vCenter, procedere come segue.

Fasi

1. Nel riquadro di sinistra, selezionare **Datacenter**.
2. Creare una nuova cartella di storage. Fare clic con il pulsante destro del mouse su **Datacenter** e

selezionare **Create storage folder**.

3. Trasferire tutti i datastore NetApp HCI dal cluster di storage e localmente al nodo di calcolo nella nuova cartella di storage.
4. Selezionare la nuova cartella di storage.
5. Nel riquadro di navigazione a destra, selezionare **Permissions** (autorizzazioni).
6. Selezionare l'icona **+** per aggiungere il nuovo utente.

   Aggiungere i seguenti dettagli nella finestra **Aggiungi permesso**:

   a. Selezionare `vsphere.local` O il dominio LDAP.
   b. Utilizzare la ricerca per trovare il nuovo utente HCC creato in Impostare un nuovo account utente in vCenter.
   c. Selezionare `Administrator role`.
   d. Selezionare **propaga ai figli**.

Assegnare le autorizzazioni utente a un cluster host NetApp

Attenersi alla seguente procedura per assegnare le autorizzazioni utente a un cluster host NetApp in vCenter.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare il cluster host NetApp.
2. Nel riquadro di navigazione a destra, selezionare **Permissions** (autorizzazioni).
3. Selezionare l'icona **+** per aggiungere il nuovo utente.

   Aggiungere i seguenti dettagli nella finestra **Aggiungi permesso**:

   a. Selezionare `vsphere.local` O il dominio LDAP.
   b. Utilizzare la ricerca per trovare il nuovo utente HCC creato in Impostare un nuovo account utente in vCenter.
   c. Selezionare `NetApp Role` oppure `Administrator`.
   d. Selezionare **propaga ai figli**.

Configurazioni host NetApp ESXi

Per le configurazioni host NetApp ESXi, è necessario aggiornare l'account utente creato da NDE al nuovo ruolo NetApp HCC.

L'host NetApp ESXi non esiste in un cluster host vCenter

Se l'host NetApp ESXi non esiste all'interno di un cluster host vCenter, è possibile utilizzare la seguente procedura per assegnare il ruolo NetApp HCC e le autorizzazioni utente in vCenter.

Fasi

1. Dal menu, selezionare **hosts** e **Clusters**.
2. Nel riquadro di navigazione a sinistra, selezionare l'host NetApp ESXi.
3. Nel riquadro di navigazione a destra, selezionare **Permissions** (autorizzazioni).
4. Selezionare l'icona **+** per aggiungere il nuovo utente.

Aggiungere i seguenti dettagli nella finestra **Aggiungi permesso**:

a. Selezionare `vsphere.local` O il dominio LDAP.
b. Utilizzare la ricerca per trovare il nuovo utente creato in Impostare un nuovo account utente in vCenter.
c. Selezionare `NetApp Role` oppure `Administrator`.

5. Selezionare **propaga ai figli**.

L'host NetApp ESXi esiste in un cluster host vCenter

Se un host NetApp ESXi esiste all'interno di un cluster host vCenter con host ESXi di altri fornitori, è possibile utilizzare la seguente procedura per assegnare il ruolo NetApp HCC e le autorizzazioni utente in vCenter.

1. Dal menu, selezionare **hosts** e **Clusters**.
2. Nel riquadro di spostamento di sinistra, espandere il cluster host desiderato.
3. Nel riquadro di navigazione a destra, selezionare **Permissions** (autorizzazioni).
4. Selezionare l'icona **+** per aggiungere il nuovo utente.

   Aggiungere i seguenti dettagli nella finestra **Aggiungi permesso**:

   a. Selezionare `vsphere.local` O il dominio LDAP.
   b. Utilizzare la ricerca per trovare il nuovo utente creato in Impostare un nuovo account utente in vCenter.
   c. Selezionare `NetApp Role`.

   > Non selezionare **propaga ai figli**.

5. Nel riquadro di navigazione a sinistra, selezionare un host NetApp ESXi.
6. Nel riquadro di navigazione a destra, selezionare **Permissions** (autorizzazioni).
7. Selezionare l'icona **+** per aggiungere il nuovo utente.

   Aggiungere i seguenti dettagli nella finestra **Aggiungi permesso**:

   a. Selezionare `vsphere.local` O il dominio LDAP.
   b. Utilizzare la ricerca per trovare il nuovo utente creato in Impostare un nuovo account utente in vCenter.
   c. Selezionare `NetApp Role` oppure `Administrator`.
   d. Selezionare **propaga ai figli**.

8. Ripetere l'operazione per gli host NetApp ESXi rimanenti nel cluster host.

La risorsa del controller esiste già nel nodo di gestione

Se nel nodo di gestione è già presente una risorsa controller, attenersi alla seguente procedura per configurare il controller utilizzando `PUT /assets /{asset_id} /controllers /{controller_id}`.

Fasi

1. Accedere all'interfaccia utente API del servizio mnode sul nodo di gestione:

   `https://<ManagementNodeIP>/mnode`

2. Selezionare **autorizzare** e immettere le credenziali per accedere alle chiamate API.
3. Selezionare `GET /assets` Per ottenere l'ID principale.
4. Selezionare `PUT /assets /{asset_id} /controllers /{controller_id}`.
   a. Inserire le credenziali create nella configurazione dell'account nel corpo della richiesta.

Aggiungere una risorsa o un nodo di calcolo al nodo di gestione

Se è necessario aggiungere manualmente una nuova risorsa o un nodo di calcolo (e le risorse BMC) dopo l'installazione, utilizzare il nuovo account utente HCC creato in Impostare un nuovo account utente in vCenter. Per ulteriori informazioni, vedere "Aggiungere risorse di calcolo e controller al nodo di gestione".

Trova ulteriori informazioni

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

Aggiornamento di VMware vSphere

Dopo aver implementato NetApp HCI, è necessario utilizzare VMware vSphere Lifecycle Manager per applicare le patch di sicurezza più recenti per la versione di VMware vSphere utilizzata con NetApp HCI.

Utilizzare "Tool di matrice di interoperabilità" per garantire la compatibilità di tutte le versioni del software. Vedere "Documentazione di VMware vSphere Lifecycle Manager" per ulteriori informazioni.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"
- "Documentazione software SolidFire ed Element"

Installare i driver della GPU per i nodi di calcolo abilitati alla GPU

I nodi di calcolo con unità di elaborazione grafica NVIDIA (GPU), come il modello H610C, necessitano di driver software NVIDIA installati in VMware ESXi per poter sfruttare la maggiore potenza di elaborazione. Dopo aver implementato nodi di calcolo con GPU, è necessario eseguire questi passaggi su ogni nodo di calcolo abilitato alla GPU per installare i driver GPU in ESXi.

Fasi

1. Aprire un browser e accedere al portale delle licenze NVIDIA al seguente URL:

```
https://nvid.nvidia.com/dashboard/
```

2. Scaricare uno dei seguenti pacchetti di driver sul computer, a seconda dell'ambiente in uso:

Versione di vSphere	Pacchetto di driver
VSphere 6.5	`NVIDIA-GRID-vSphere-6.5-410.92-410.91-412.16.zip`
VSphere 6.7	`NVIDIA-GRID-vSphere-6.7-410.92-410.91-412.16.zip`

3. Estrarre il pacchetto di driver sul computer.

   Il file .VIB risultante è il file del driver non compresso.

4. Copiare il `.VIB` File di driver dal computer a ESXi in esecuzione sul nodo di calcolo. I seguenti comandi di esempio per ciascuna versione presuppongono che il driver si trovi in `$HOME/NVIDIA/ESX6.x/` directory sull'host di gestione. L'utility SCP è facilmente disponibile nella maggior parte delle distribuzioni Linux o è disponibile come utility scaricabile per tutte le versioni di Windows:

Versione di ESXi	Descrizione
ESXi 6.5	`scp $HOME/NVIDIA/ESX6.5/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.`
ESXi 6.7	`scp $HOME/NVIDIA/ESX6.7/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.`

5. Attenersi alla seguente procedura per accedere come root all'host ESXi e installare NVIDIA vGPU Manager in ESXi.
   a. Eseguire il seguente comando per accedere all'host ESXi come utente root:

   ```
   ssh root@<ESXi_IP_ADDRESS>
   ```

   b. Eseguire il seguente comando per verificare che non siano installati driver NVIDIA GPU:

   ```
   nvidia-smi
   ```

   Questo comando dovrebbe restituire il messaggio `nvidia-smi: not found`.

   c. Eseguire i seguenti comandi per attivare la modalità di manutenzione sull'host e installare NVIDIA vGPU Manager dal file VIB:

   ```
   esxcli system maintenanceMode set --enable true
   esxcli software vib install -v /NVIDIA**.vib
   ```

   Viene visualizzato il messaggio `Operation finished successfully`.

   d. Eseguire il seguente comando e verificare che tutti gli otto driver GPU siano elencati nell'output del comando:

```
nvidia-smi
```

e. Eseguire il seguente comando per verificare che il pacchetto NVIDIA vGPU sia stato installato e caricato correttamente:

```
vmkload_mod -l | grep nvidia
```

Il comando dovrebbe restituire un output simile al seguente: `nvidia 816 13808`

f. Eseguire il seguente comando per riavviare l'host:

```
reboot -f
```

g. Eseguire il seguente comando per uscire dalla modalità di manutenzione:

```
esxcli system maintenanceMode set --enable false
```

6. Ripetere i passaggi 4-6 per tutti gli altri nodi di calcolo appena implementati con GPU NVIDIA.
7. Eseguire le seguenti operazioni seguendo le istruzioni riportate nel sito della documentazione NVIDIA:
   a. Installare il server di licenza NVIDIA.
   b. Configurare le macchine virtuali guest per il software NVIDIA vGPU.
   c. Se si utilizzano desktop compatibili con vGPU in un contesto di infrastruttura di desktop virtuale (VDI), configurare VMware Horizon View per il software NVIDIA vGPU.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Documentazione software SolidFire ed Element"

Accedi a NetApp Hybrid Cloud Control

Il controllo del cloud ibrido NetApp ti consente di gestire NetApp HCI. È possibile aggiornare i servizi di gestione e altri componenti di NetApp HCI ed espandere e monitorare l'installazione. Per accedere a NetApp Hybrid Cloud Control, accedere all'indirizzo IP del nodo di gestione.

Di cosa hai bisogno

- **Cluster Administrator permissions** (autorizzazioni amministratore cluster): Si dispone delle autorizzazioni di amministratore per il cluster di storage.
- **Servizi di gestione**: I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326. NetApp Hybrid Cloud Control non è disponibile nelle versioni precedenti del service bundle. Per informazioni sulla versione corrente del service bundle, consultare "Note sulla versione di Management Services".

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

```
https://<ManagementNodeIP>
```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.

   Viene visualizzata l'interfaccia NetApp Hybrid Cloud Control.

> Se si è effettuato l'accesso utilizzando autorizzazioni insufficienti, viene visualizzato il messaggio "Impossibile caricare" nelle pagine delle risorse HCC e le risorse non saranno disponibili.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Documentazione software SolidFire ed Element"

Riduci l'usura dei supporti di boot su un nodo di calcolo NetApp HCI

Quando si utilizza una memoria flash o un supporto di avvio NVDIMM con un nodo di calcolo NetApp HCI, mantenendo i log di sistema su tale supporto si ottengono scritture frequenti su quel supporto. In questo modo, la memoria flash potrebbe essere degradata. Seguire le istruzioni contenute nel seguente articolo della Knowledge base per spostare il file di log dell'host e il file di dump core in una posizione di storage condivisa, in modo da prevenire il degrado del supporto di avvio nel tempo e prevenire errori del disco di avvio completo.

"Come ridurre l'usura del disco di avvio di un nodo di calcolo NetApp HCI"

Trova ulteriori informazioni

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

Gestire NetApp HCI

Panoramica sulla gestione di NetApp HCI

È possibile configurare il nome di dominio completo e gestire le credenziali per NetApp HCI, account utente, cluster di storage, volumi, gruppi di accesso ai volumi, Iniziatori, policy di QoS dei volumi e nodo di gestione.

Di seguito sono riportati gli elementi che è possibile utilizzare:

- "Configurare l'accesso completo all'interfaccia utente Web Domain Name"
- "Modificare le credenziali in NetApp HCI"
- "Aggiornare le credenziali vCenter ed ESXi"
- "Gestire le risorse di storage NetApp HCI"
- "Lavorare con il nodo di gestione"
- "Spegnere e riaccendere il sistema NetApp HCI"

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"

Configurare l'accesso completo all'interfaccia utente Web Domain Name

NetApp HCI con software Element 12.2 o versione successiva consente di accedere alle interfacce Web del cluster di storage utilizzando il nome di dominio completo (FQDN). Se si desidera utilizzare l'FQDN per accedere alle interfacce utente Web, ad esempio l'interfaccia utente Web Element, l'interfaccia utente per nodo o l'interfaccia utente del nodo di gestione, è necessario prima aggiungere un'impostazione del cluster di storage per identificare l'FQDN utilizzato dal cluster.

È ora possibile accedere alle interfacce Web del cluster di storage utilizzando il nome di dominio completo (FQDN, Fully Qualified Domain Name). Se si desidera utilizzare l'FQDN per accedere alle interfacce utente Web, ad esempio l'interfaccia utente Web Element, l'interfaccia utente per nodo o l'interfaccia utente del nodo di gestione, è necessario prima aggiungere un'impostazione del cluster di storage per identificare l'FQDN utilizzato dal cluster. Ciò consente al cluster di reindirizzare correttamente una sessione di accesso e di migliorare l'integrazione con servizi esterni come i key manager e i provider di identità per l'autenticazione a più fattori.

Di cosa hai bisogno

- Questa funzione richiede Element 12.2 o versione successiva.
- La configurazione di questa funzionalità utilizzando le API REST di NetApp Hybrid Cloud Control richiede servizi di gestione 2.15 o successivi.
- La configurazione di questa funzione mediante l'interfaccia utente di NetApp Hybrid Cloud Control richiede servizi di gestione 2.19 o successivi.

- Per utilizzare le API REST, è necessario aver implementato un nodo di gestione con versione 11.5 o successiva.
- Sono necessari nomi di dominio completi per il nodo di gestione e ciascun cluster di storage che si risolvono correttamente nell'indirizzo IP del nodo di gestione e in ciascun indirizzo IP del cluster di storage.

È possibile configurare o rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control e l'API REST. È inoltre possibile risolvere i problemi relativi a FQDN configurati in modo errato.

- Configurare l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control
- Configurare l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST
- Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control
- Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST
- Risoluzione dei problemi

Configurare l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare l'icona del menu nella parte superiore destra della pagina.
4. Selezionare **Configura**.
5. Nel riquadro **Fully Qualified Domain Names**, selezionare **Set Up**.
6. Nella finestra visualizzata, immettere gli FQDN per il nodo di gestione e ciascun cluster di storage.
7. Selezionare **Salva**.

   Il riquadro **Fully Qualified Domain Names** elenca ciascun cluster di storage con i relativi MVIP e FQDN associati.

   > Solo i cluster di storage connessi con il set FQDN sono elencati nel riquadro **Fully Qualified Domain Names**.

Configurare l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST

Fasi

1. Assicurarsi che i nodi storage Element e il nodo di gestione abbiano il DNS configurato correttamente per l'ambiente di rete in modo che gli FQDN nell'ambiente possano essere risolti. Per impostare il DNS, accedere all'interfaccia utente per nodo per i nodi di storage e al nodo di gestione, quindi selezionare **Impostazioni di rete** > **rete di gestione**.
   a. Interfaccia utente per nodo per nodi di storage: `https://<storage_node_management_IP>:442`
   b. Interfaccia utente per nodo per il nodo di gestione: `https://<management_node_IP>:442`

2. Modificare le impostazioni del cluster di storage utilizzando l'API Element.

   a. Accedere all'API Element e creare la seguente preferenza di interfaccia cluster utilizzando `CreateClusterInterfacePreference` API e inserire l'FQDN MVIP del cluster come valore di preferenza:

      - Nome: `mvip_fqdn`
      - Valore: <Fully Qualified Domain Name for the Cluster MVIP>

        Ad esempio, il nome FQDN è `storagecluster.my.org`:

```
https://<Cluster_MVIP>/json-
rpc/12.2?method=CreateClusterInterfacePreference&name=mvip_fqdn&value=st
oragecluster.my.org
```

3. Modificare le impostazioni del nodo di gestione utilizzando l'API REST sul nodo di gestione:

   a. Accedere all'interfaccia utente API REST per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/2/`. Ad esempio:

```
https://<management_node_IP>/mnode/2/
```

   b. Selezionare **autorizzare** o un'icona a forma di lucchetto e inserire il nome utente e la password del cluster di elementi.
   c. Immettere l'ID client come `mnode-client`.
   d. Selezionare **autorizzare** per avviare una sessione.
   e. Chiudere la finestra.
   f. Selezionare **GET /settings**.
   g. Selezionare **Provalo**.
   h. Selezionare **Esegui**.
   i. Si noti se il proxy viene utilizzato o meno come indicato nella `"use_proxy"` di `true` oppure `false`.
   j. Selezionare **PUT /settings**.
   k. Selezionare **Provalo**.
   l. Nell'area del corpo della richiesta, inserire il nodo di gestione FQDN come valore per `mnode_fqdn` parametro. Specificare inoltre se utilizzare il proxy (`true` oppure `false` dalla fase precedente) per `use_proxy` parametro.

```
{
  "mnode_fqdn": "mnode.my.org",
  "use_proxy": false
}
```

   m. Selezionare **Esegui**.

Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control

È possibile utilizzare questa procedura per rimuovere l'accesso Web FQDN per il nodo di gestione e i cluster di storage.

Fasi

1. Nel riquadro **Fully Qualified Domain Names**, selezionare **Edit** (Modifica).
2. Nella finestra visualizzata, eliminare il contenuto del campo di testo **FQDN**.
3. Selezionare **Salva**.

   La finestra si chiude e l'FQDN non è più elencato nel riquadro **Fully Qualified Domain Names**.

Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST

Fasi

1. Modificare le impostazioni del cluster di storage utilizzando l'API Element.

   a. Accedere all'API Element ed eliminare la seguente preferenza di interfaccia cluster utilizzando `DeleteClusterInterfacePreference` Metodo API:

      - Nome: `mvip_fqdn`

        Ad esempio:

```
https://<Cluster_MVIP>/json-rpc/12.2?method=DeleteClusterInterfacePreference&name=mvip_fqdn
```

2. Modificare le impostazioni del nodo di gestione utilizzando l'API REST sul nodo di gestione:

   a. Accedere all'interfaccia utente API REST per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/2/`. Ad esempio:

```
https://<management_node_IP>/mnode/2/
```

   b. Selezionare **autorizzare** o un'icona a forma di lucchetto e inserire il nome utente e la password del cluster di elementi.

   c. Immettere l'ID client come `mnode-client`.

   d. Selezionare **autorizzare** per avviare una sessione.

   e. Chiudere la finestra.

   f. Selezionare **PUT /settings**.

   g. Selezionare **Provalo**.

   h. Nell'area del corpo della richiesta, non inserire un valore per `mnode_fqdn` parametro. Specificare inoltre se utilizzare il proxy (`true` oppure `false`) per `use_proxy` parametro.

```
{
  "mnode_fqdn": "",
  "use_proxy": false
}
```

i. Selezionare **Esegui**.

Risoluzione dei problemi

Se gli FQDN non sono configurati correttamente, potrebbero verificarsi problemi di accesso al nodo di gestione, a un cluster di storage o a entrambi. Utilizzare le seguenti informazioni per risolvere il problema.

Problema	Causa	Risoluzione
• Viene visualizzato un errore del browser quando si tenta di accedere al nodo di gestione o al cluster di storage utilizzando l'FQDN. • Non è possibile accedere al nodo di gestione o al cluster di storage utilizzando un indirizzo IP.	L'FQDN del nodo di gestione e l'FQDN del cluster di storage non sono configurati correttamente.	Utilizzare le istruzioni REST API riportate in questa pagina per rimuovere le impostazioni FQDN del nodo di gestione e del cluster di storage e configurarle di nuovo.
• Viene visualizzato un errore del browser quando si tenta di accedere al FQDN del cluster di storage. • Non è possibile accedere al nodo di gestione o al cluster di storage utilizzando un indirizzo IP.	L'FQDN del nodo di gestione è configurato correttamente, ma l'FQDN del cluster di storage non è configurato correttamente.	Utilizzare le istruzioni REST API riportate in questa pagina per rimuovere le impostazioni FQDN del cluster di storage e configurarle di nuovo.
• Si verifica un errore del browser quando si tenta di accedere al nodo di gestione FQDN. • È possibile accedere al nodo di gestione e al cluster di storage utilizzando un indirizzo IP.	L'FQDN del nodo di gestione non è configurato correttamente, ma l'FQDN del cluster di storage è configurato correttamente.	Accedere a NetApp Hybrid Cloud Control per correggere le impostazioni FQDN del nodo di gestione nell'interfaccia utente oppure utilizzare le istruzioni API REST in questa pagina per correggere le impostazioni.

Trova ulteriori informazioni

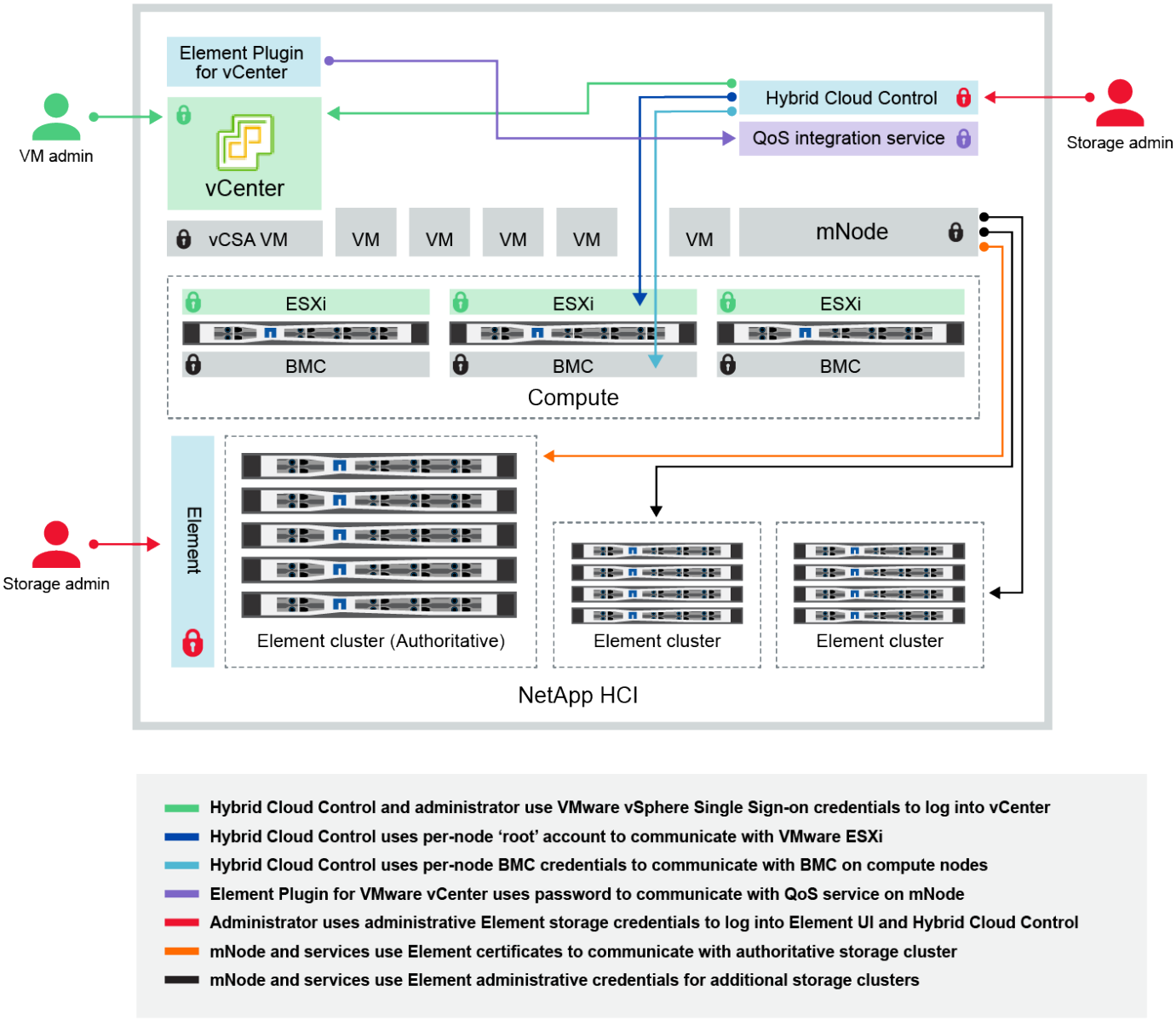
- "CreateClusterInterfacePerferta le informazioni API nella documentazione SolidFire ed Element"
- "Pagina delle risorse NetApp HCI"
- "Documentazione software SolidFire ed Element"

Modificare le credenziali in NetApp HCI e NetApp SolidFire

A seconda delle policy di sicurezza dell'organizzazione che ha implementato NetApp HCI o NetApp SolidFire, la modifica delle credenziali o delle password è generalmente parte delle procedure di sicurezza. Prima di modificare le password, è necessario essere consapevoli dell'impatto sugli altri componenti software nell'implementazione.

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

Interazioni dei componenti NetApp HCI:



Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Credenziali dell'elemento	**Applicabile a**: NetApp HCI e SolidFire Gli amministratori utilizzano queste credenziali per accedere a: • Interfaccia utente Element sul cluster di storage Element • Controllo del cloud ibrido sul nodo di gestione (mnode) Quando Hybrid Cloud Control gestisce più cluster di storage, accetta solo le credenziali di amministratore per i cluster di storage, noto come *cluster autorevole* per cui è stato inizialmente configurato mnode. Per i cluster di storage aggiunti in seguito a Hybrid Cloud Control, mnode memorizza in modo sicuro le credenziali di amministratore. Se le credenziali per i cluster di storage aggiunti successivamente vengono modificate, le credenziali devono essere aggiornate anche in mnode utilizzando l'API mnode.	• "Aggiornare le password di amministrazione del cluster di storage". • Aggiornare le credenziali di amministratore del cluster di storage in mnode utilizzando "API modifyclusteradmin".
Credenziali vSphere Single Sign-on	**Applicabile a**: Solo NetApp HCI Gli amministratori utilizzano queste credenziali per accedere a VMware vSphere Client. Quando vCenter fa parte dell'installazione di NetApp HCI, le credenziali vengono configurate nel motore di implementazione NetApp come segue: • username@vsphere.local con la password specificata, e. • administrator@vsphere.local con la password specificata. Quando si utilizza un vCenter esistente per implementare NetApp HCI, le credenziali di accesso singolo vSphere vengono gestite dagli amministratori IT VMware.	"Aggiornare le credenziali vCenter ed ESXi".

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Credenziali BMC (Baseboard Management Controller)	**Applicabile a**: Solo NetApp HCI Gli amministratori utilizzano queste credenziali per accedere al BMC dei nodi di calcolo NetApp in un'implementazione NetApp HCI. BMC offre funzioni di base per il monitoraggio dell'hardware e la console virtuale. Le credenziali BMC (a volte denominate *IPMI*) per ciascun nodo di calcolo NetApp vengono memorizzate in modo sicuro sull'mnode nelle implementazioni NetApp HCI. NetApp Hybrid Cloud Control utilizza le credenziali BMC in una capacità di account di servizio per comunicare con BMC nei nodi di calcolo durante gli aggiornamenti del firmware del nodo di calcolo. Quando le credenziali BMC vengono modificate, le credenziali per i rispettivi nodi di calcolo devono essere aggiornate anche su mnode per mantenere tutte le funzionalità di controllo del cloud ibrido.	• "Configurare IPMI per ogni nodo su NetApp HCI". • Per i nodi H410C, H610C e H615C, "Modificare la password IPMI predefinita". • Per i nodi H410S e H610S, "Modificare la password IPM predefinita". • "Modificare le credenziali BMC sul nodo di gestione".
Credenziali ESXi	**Applicabile a**: Solo NetApp HCI Gli amministratori possono accedere agli host ESXi utilizzando SSH o DCUI locale con un account root locale. Nelle implementazioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale del nodo di calcolo nel motore di implementazione NetApp. Le credenziali radice ESXi per ciascun nodo di calcolo NetApp vengono memorizzate in modo sicuro sull'mnode nelle implementazioni NetApp HCI. NetApp Hybrid Cloud Control utilizza le credenziali in una capacità di account di servizio per comunicare direttamente con gli host ESXi durante gli aggiornamenti del firmware del nodo di calcolo e i controlli dello stato. Quando le credenziali root di ESXi vengono modificate da un amministratore VMware, le credenziali per i rispettivi nodi di calcolo devono essere aggiornate su mnode per mantenere la funzionalità di controllo del cloud ibrido.	"Aggiorna le credenziali per gli host vCenter e ESXi".

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Password di integrazione QoS	**Applicabile a**: NetApp HCI e opzionale in SolidFire Non utilizzato dagli amministratori per gli accessi interattivi. L'integrazione QoS tra VMware vSphere ed Element Software è abilitata tramite: • Plug-in Element per vCenter Server e. • Servizio QoS su mnode. Per l'autenticazione, il servizio QoS utilizza una password utilizzata esclusivamente in questo contesto. La password QoS viene specificata durante l'installazione iniziale del plug-in Element per vCenter Server o generata automaticamente durante l'implementazione di NetApp HCI. Nessun impatto su altri componenti.	"Aggiornare le credenziali QoSSIOC nel plug-in NetApp Element per vCenter Server". Il plug-in NetApp Element per la password SIOC del server vCenter è noto anche come *password QoSSIOC*. Consulta l'articolo Element Plug-in for vCenter Server KB article.
Credenziali di vCenter Service Appliance	**Applicabile a**: NetApp HCI solo se configurato dal motore di implementazione NetApp Gli amministratori possono accedere alle macchine virtuali dell'appliance vCenter Server. Nelle implementazioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale del nodo di calcolo nel motore di implementazione NetApp. A seconda della versione di VMware vSphere implementata, alcuni amministratori del dominio di Single Sign-on di vSphere possono anche accedere all'appliance. Nessun impatto su altri componenti.	Non sono necessarie modifiche.
Credenziali amministratore di NetApp Management Node	**Applicabile a**: NetApp HCI e opzionale in SolidFire Gli amministratori possono accedere alle macchine virtuali del nodo di gestione NetApp per la configurazione avanzata e la risoluzione dei problemi. A seconda della versione del nodo di gestione implementata, l'accesso tramite SSH non è attivato per impostazione predefinita. Nelle implementazioni NetApp HCI, il nome utente e la password sono stati specificati dall'utente durante l'installazione iniziale di tale nodo di calcolo nel motore di implementazione NetApp. Nessun impatto su altri componenti.	Non sono necessarie modifiche.

Trova ulteriori informazioni

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

Aggiornare le credenziali vCenter ed ESXi

Per mantenere la piena funzionalità di NetApp Hybrid Cloud Control per la tua installazione NetApp HCI, quando modifichi le tue credenziali negli host vCenter ed ESXi, devi anche aggiornare tali credenziali nel servizio asset sul nodo di gestione.

A proposito di questa attività

NetApp Hybrid Cloud Control comunica con vCenter e i singoli nodi di calcolo che eseguono VMware vSphere ESXi per recuperare le informazioni per la dashboard e facilitare gli aggiornamenti a rotazione di firmware, software e driver. NetApp Hybrid Cloud Control e i relativi servizi sul nodo di gestione utilizzano credenziali (nome utente/password) per l'autenticazione con VMware vCenter ed ESXi.

Se la comunicazione tra questi componenti non riesce, NetApp Hybrid Cloud Control e vCenter visualizzano messaggi di errore quando si verificano problemi di autenticazione. Se non riesce a comunicare con l'istanza di VMware vCenter associata nell'installazione di NetApp HCI, il controllo del cloud ibrido NetApp visualizza un banner di errore rosso. VMware vCenter visualizza i messaggi di blocco dell'account ESXi per i singoli host ESXi in seguito al NetApp Hybrid Cloud Control che utilizza credenziali obsolete.

Il nodo di gestione in NetApp HCI fa riferimento a questi componenti utilizzando i seguenti nomi:

- Le "risorse dei controller" sono istanze di vCenter associate all'installazione di NetApp HCI.
- Le "risorse dei nodi di calcolo" sono gli host ESXi presenti nell'installazione di NetApp HCI.

Durante l'installazione iniziale di NetApp HCI utilizzando il motore di implementazione NetApp, il nodo di gestione ha memorizzato le credenziali dell'utente amministrativo specificato per vCenter e la password dell'account "root" sui server ESXi.

Aggiornare la password di vCenter utilizzando l'API REST del nodo di gestione

Seguire la procedura per aggiornare le risorse del controller. Vedere "Visualizzare o modificare le risorse dei controller esistenti".

Aggiornare la password ESXi utilizzando l'API REST del nodo di gestione

Fasi

1. Per una panoramica dell'interfaccia utente REST API del nodo di gestione, vedere "Panoramica dell'interfaccia utente REST API del nodo di gestione".
2. Accedere all'interfaccia utente API REST per i servizi di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/mnode
```

Sostituire <management node IP> con l'indirizzo IPv4 del nodo di gestione sulla rete di gestione utilizzata per NetApp HCI.

3. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password amministrativi del cluster NetApp SolidFire.
   b. Immettere l'ID client come `mnode-client`.
   c. Fare clic su **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
4. Dall'interfaccia utente API REST, fare clic su **GET /Assets/compute_nodes**.

   In questo modo vengono recuperati i record delle risorse dei nodi di calcolo memorizzate nel nodo di gestione.

   Di seguito viene riportato il collegamento diretto a questa API nell'interfaccia utente:

```
https://<ManagementNodeIP>/mnode/#/assets/routes.v1.assets_api.get_compu
te_nodes
```

5. Fare clic su **Provalo**.
6. Fare clic su **Execute** (Esegui).
7. Dal corpo di risposta, identificare i record delle risorse del nodo di calcolo che richiedono credenziali aggiornate. È possibile utilizzare le proprietà "ip" e "nome_host" per trovare i record host ESXi corretti.

```
"config": { },
"credentialid": <credential_id>,
"hardware_tag": <tag>,
"host_name": <host_name>,
"id": <id>,
"ip": <ip>,
"parent": <parent>,
"type": ESXi Host
```

> Il passaggio successivo utilizza i campi "padre" e "id" nel record di risorsa di calcolo per fare riferimento al record da aggiornare.

8. Configurare la risorsa specifica del nodo di calcolo:
   a. Fare clic su **PUT /assets/{asset_id}/compute-nodes/{compute_id}**.

      Di seguito viene riportato il collegamento diretto all'API nell'interfaccia utente:

```
https://<ManagementNodeIP>/mnode/#/assets/routes.v1.assets_api.put_asset
s_compute_id
```

a. Fare clic su **Provalo**.
b. Inserire l'"asset_id" con le informazioni "padre".
c. Inserire l'"ID_calcolo" con le informazioni "id".
d. Modificare il corpo della richiesta nell'interfaccia utente per aggiornare solo i parametri di password e nome utente nel record della risorsa di calcolo:

```
{
"password": "<password>",
"username": "<username>"
}
```

e. Fare clic su **Execute** (Esegui).
f. Verificare che la risposta sia HTTP 200, che indica che le nuove credenziali sono state memorizzate nel record delle risorse di calcolo a cui si fa riferimento

9. Ripetere i due passaggi precedenti per le risorse aggiuntive dei nodi di calcolo che devono essere aggiornate con una nuova password.
10. Selezionare https://<mNode_ip>/inventory/1/.
    a. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
        i. Inserire il nome utente e la password amministrativi del cluster NetApp SolidFire.
        ii. Immettere l'ID client come `mnode-client`.
        iii. Fare clic su **autorizzare** per avviare una sessione.
        iv. Chiudere la finestra.
    b. Dall'interfaccia utente API REST, fare clic su **GET /Installations**.
    c. Fare clic su **Provalo**.
    d. Selezionare **True** dall'elenco a discesa Refresh description (Descrizione aggiornamento).
    e. Fare clic su **Execute** (Esegui).
    f. Verificare che la risposta sia HTTP 200.
11. Attendere circa 15 minuti per far scomparire il messaggio di blocco dell'account in vCenter.

Trova ulteriori informazioni

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

Gestire lo storage NetApp HCI

Panoramica sullo storage Manage NetApp HCI

Con NetApp HCI, puoi gestire queste risorse di storage utilizzando il controllo del cloud ibrido NetApp.

- "Creare e gestire gli account utente"

- "Aggiungere e gestire cluster di storage"
- "Creare e gestire i volumi"
- "Creare e gestire i gruppi di accesso ai volumi"
- "Creare e gestire gli iniziatori"
- "Creare e gestire policy di QoS per volumi"

Trova ulteriori informazioni

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

Creare e gestire gli account utente utilizzando NetApp Hybrid Cloud Control

Nei sistemi storage basati su elementi, è possibile creare utenti di cluster autorevoli per consentire l'accesso a NetApp Hybrid Cloud Control in base alle autorizzazioni che si desidera concedere agli utenti "Administrator" o "Read-only". Oltre agli utenti del cluster, esistono anche account di volume che consentono ai client di connettersi ai volumi su un nodo di storage.

Gestire i seguenti tipi di account:

- Gestire gli account cluster autorevoli
- Gestire gli account dei volumi

Attivare LDAP

Per utilizzare LDAP per qualsiasi account utente, è necessario prima attivare LDAP.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, fare clic sull'icona Opzioni in alto a destra e selezionare **Gestione utenti**.
3. Nella pagina utenti, fare clic su **Configura LDAP**.
4. Definire la configurazione LDAP.
5. Selezionare il tipo di autenticazione Search and Bind (Cerca e bind) o Direct Bind (Bind diretto).
6. Prima di salvare le modifiche, fare clic su **Test LDAP Log in** (verifica accesso LDAP) nella parte superiore della pagina, immettere il nome utente e la password di un utente noto esistente e fare clic su **Test**.
7. Fare clic su **Save** (Salva).

Gestire gli account cluster autorevoli

"Account utente autorevoli" Sono gestiti dal menu in alto a destra dell'opzione User Management in NetApp Hybrid Cloud Control. Questi tipi di account consentono di eseguire l'autenticazione con qualsiasi risorsa di storage associata a un'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.

Creare un account cluster autorevole

Puoi creare un account utilizzando NetApp Hybrid Cloud Control.

Questo account può essere utilizzato per accedere al controllo del cloud ibrido, all'interfaccia utente per nodo per il cluster e al cluster di storage nel software NetApp Element.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, fare clic sull'icona Opzioni in alto a destra e selezionare **Gestione utenti**.
3. Selezionare **Create User** (Crea utente).
4. Selezionare il tipo di autenticazione del cluster o LDAP.
5. Completare una delle seguenti operazioni:
   - Se si seleziona LDAP, inserire il DN.

     Per utilizzare LDAP, è necessario prima attivare LDAP o LDAPS. Vedere Attivare LDAP.

   - Se si seleziona Cluster come tipo di autorizzazione, immettere un nome e una password per il nuovo account.
6. Selezionare le autorizzazioni di amministratore o di sola lettura.

   Per visualizzare le autorizzazioni dal software NetApp Element, fare clic su **Mostra permessi legacy**. Se si seleziona un sottoinsieme di queste autorizzazioni, all'account vengono assegnate autorizzazioni di sola lettura. Se si selezionano tutte le autorizzazioni legacy, all'account vengono assegnate le autorizzazioni di amministratore.

   Per garantire che tutti i figli di un gruppo ereditino le autorizzazioni, creare un gruppo di amministratori dell'organizzazione DN nel server LDAP. Tutti gli account figlio di quel gruppo erediteranno tali autorizzazioni.

7. Selezionare la casella "ho letto e accettato il Contratto di licenza con l'utente finale di NetApp".
8. Fare clic su **Create User** (Crea utente).

Modificare un account cluster autorevole

È possibile modificare le autorizzazioni o la password di un account utente utilizzando NetApp Hybrid Cloud Control.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, fare clic sull'icona in alto a destra e selezionare **User Management** (Gestione utenti).
3. È possibile filtrare l'elenco degli account utente selezionando **Cluster**, **LDAP** o **IDP**.

   Se sono stati configurati utenti sul cluster di storage con LDAP, questi account visualizzano il tipo utente "LDAP". Se sono stati configurati utenti sul cluster di storage con IDP, questi account mostrano un tipo di utente "IDP".

4. Nella colonna **azioni** della tabella, espandere il menu dell'account e selezionare **Modifica**.
5. Apportare le modifiche necessarie.
6. Selezionare **Salva**.
7. Disconnettersi da NetApp Hybrid Cloud Control.
8. "Aggiornare le credenziali" Per la risorsa cluster autorevole che utilizza l'API di controllo del cloud ibrido di NetApp.

> L'aggiornamento dell'inventario potrebbe richiedere fino a 2 minuti dall'interfaccia utente di NetApp Hybrid Cloud Control. Per aggiornare manualmente l'inventario, accedere al servizio di inventario dell'interfaccia utente REST API `https://<ManagementNodeIP>/inventory/1/` ed eseguire `GET /installations/{id}` per il cluster.

9. Accedi a NetApp Hybrid Cloud Control.

Eliminare un account utente autorevole

È possibile eliminare uno o più account quando non sono più necessari. È possibile eliminare un account utente LDAP.

Non è possibile eliminare l'account utente amministratore principale per il cluster autorevole.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, fare clic sull'icona in alto a destra e selezionare **User Management** (Gestione utenti).
3. Nella colonna **azioni** della tabella utenti, espandere il menu dell'account e selezionare **Elimina**.
4. Confermare l'eliminazione selezionando **Sì**.

Gestire gli account dei volumi

"Account di volume" Sono gestiti all'interno della tabella NetApp Hybrid Cloud Control Volumes. Questi account sono specifici solo per il cluster di storage in cui sono stati creati. Questi tipi di account consentono di impostare le autorizzazioni sui volumi in rete, ma non hanno alcun effetto al di fuori di tali volumi.

Un account volume contiene l'autenticazione CHAP richiesta per accedere ai volumi assegnati.

Creare un account volume

Creare un account specifico per questo volume.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, selezionare **Storage** > **Volumes**.
3. Selezionare la scheda **account**.
4. Selezionare il pulsante **Crea account**.
5. Immettere un nome per il nuovo account.
6. Nella sezione CHAP Settings (Impostazioni CHAP), immettere le seguenti informazioni:

- Initiator Secret per l'autenticazione della sessione del nodo CHAP
- Segreto di destinazione per l'autenticazione della sessione del nodo CHAP

> Per generare automaticamente una password, lasciare vuoti i campi delle credenziali.

7. Selezionare **Crea account**.

Modificare un account volume

È possibile modificare le informazioni CHAP e modificare se un account è attivo o bloccato.

> L'eliminazione o il blocco di un account associato al nodo di gestione comporta un nodo di gestione inaccessibile.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, selezionare **Storage** > **Volumes**.
3. Selezionare la scheda **account**.
4. Nella colonna **azioni** della tabella, espandere il menu dell'account e selezionare **Modifica**.
5. Apportare le modifiche necessarie.
6. Confermare le modifiche selezionando **Sì**.

Eliminare un account volume

Eliminare un account non più necessario.

Prima di eliminare un account di volume, eliminare e rimuovere i volumi associati all'account.

> L'eliminazione o il blocco di un account associato al nodo di gestione comporta un nodo di gestione inaccessibile.

> I volumi persistenti associati ai servizi di gestione vengono 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. Se si eliminano questi account, si potrebbe rendere inutilizzabile il nodo di gestione.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, selezionare **Storage** > **Volumes**.
3. Selezionare la scheda **account**.
4. Nella colonna **azioni** della tabella, espandere il menu dell'account e selezionare **Elimina**.
5. Confermare l'eliminazione selezionando **Sì**.

Trova ulteriori informazioni

- "Scopri di più sugli account"
- "Utilizzare gli account utente"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Aggiungi e gestisci cluster di storage utilizzando NetApp Hybrid Cloud Control

È possibile aggiungere cluster di storage all'inventario delle risorse dei nodi di gestione in modo che possano essere gestiti utilizzando NetApp Hybrid Cloud Control (HCC). Il primo cluster di storage aggiunto durante l'installazione del sistema è quello predefinito "cluster di storage autorevole", Ma è possibile aggiungere cluster aggiuntivi utilizzando l'interfaccia utente HCC.

Dopo l'aggiunta di un cluster di storage, è possibile monitorare le prestazioni del cluster, modificare le credenziali del cluster di storage per la risorsa gestita o rimuovere un cluster di storage dall'inventario delle risorse del nodo di gestione se non è più necessario gestirlo con HCC.

A partire da Element 12.2, è possibile utilizzare "modalità di manutenzione" opzioni per attivare e disattivare la modalità di manutenzione per i nodi del cluster di storage.

Di cosa hai bisogno

- **Cluster Administrator permissions** (autorizzazioni amministratore cluster): Si dispone delle autorizzazioni di amministratore su "cluster di storage autorevole". Il cluster autorevole è il primo cluster aggiunto all'inventario dei nodi di gestione durante l'installazione del sistema.
- **Software Element**: La versione del cluster di storage in uso esegue il software NetApp Element 11.3 o versione successiva.
- **Nodo di gestione**: È stato implementato un nodo di gestione con versione 11.3 o successiva.
- **Servizi di gestione**: Il bundle di servizi di gestione è stato aggiornato alla versione 2.17 o successiva.

Opzioni

- Aggiungere un cluster di storage
- Confermare lo stato del cluster di storage
- Modificare le credenziali del cluster di storage
- Rimuovere un cluster di storage
- Attiva e disattiva la modalità di manutenzione

Aggiungere un cluster di storage

È possibile aggiungere un cluster di storage all'inventario delle risorse del nodo di gestione utilizzando NetApp Hybrid Cloud Control. Ciò consente di gestire e monitorare il cluster utilizzando l'interfaccia utente HCC.

Fasi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
2. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
3. Nel riquadro **Storage Clusters**, selezionare **Storage Cluster Details** (Dettagli cluster di storage).
4. Selezionare **Add Storage Cluster** (Aggiungi cluster di storage).

5. Inserire le seguenti informazioni:
    - Indirizzo IP virtuale per la gestione del cluster di storage

    > È possibile aggiungere solo cluster di storage remoto che non sono attualmente gestiti da un nodo di gestione.

    - Nome utente e password del cluster di storage
6. Selezionare **Aggiungi**.

    > Dopo aver aggiunto il cluster di storage, l'inventario del cluster può impiegare fino a 2 minuti per l'aggiornamento e la visualizzazione della nuova aggiunta. Potrebbe essere necessario aggiornare la pagina del browser per visualizzare le modifiche.

7. Se si aggiungono cluster eSDS Element, inserire o caricare la chiave privata SSH e l'account utente SSH.

Confermare lo stato del cluster di storage

È possibile monitorare lo stato di connessione delle risorse dei cluster di storage utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.

Fasi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
2. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
3. Esaminare lo stato dei cluster di storage nell'inventario.
4. Dal riquadro **Storage Clusters**, selezionare **Storage Cluster Details** per ulteriori dettagli.

Modificare le credenziali del cluster di storage

È possibile modificare il nome utente e la password dell'amministratore del cluster di storage utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.

Fasi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
2. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
3. Nel riquadro **Storage Clusters**, selezionare **Storage Cluster Details** (Dettagli cluster di storage).
4. Selezionare il menu **azioni** del cluster e selezionare **Modifica credenziali cluster**.
5. Aggiornare il nome utente e la password del cluster di storage.
6. Selezionare **Salva**.

Rimuovere un cluster di storage

La rimozione di un cluster di storage da NetApp Hybrid Cloud Control rimuove il cluster dall'inventario dei nodi di gestione. Dopo aver rimosso un cluster di storage, il cluster non può più essere gestito da HCC e l'accesso è possibile solo accedendo direttamente al relativo indirizzo IP di gestione.

> Non è possibile rimuovere il cluster autorevole dall'inventario. Per determinare il cluster autorevole, accedere a **User Management > Users** (Gestione utenti > utenti). Il cluster autorevole è elencato accanto all'intestazione **Users**.

Fasi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
2. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
3. Nel riquadro **Storage Clusters**, selezionare **Storage Cluster Details** (Dettagli cluster di storage).
4. Selezionare il menu **azioni** del cluster e selezionare **Rimuovi cluster di storage**.

   Facendo clic su **Yes** NEXT (Sì), il cluster viene rimosso dall'installazione.

5. Selezionare **Sì**.

Attiva e disattiva la modalità di manutenzione

Questo "modalità di manutenzione" le opzioni delle funzionalità ti offrono la possibilità di abilitare e. disattiva modalità di manutenzione per un nodo del cluster di storage.

Di cosa hai bisogno

- **Software Element**: La versione del cluster di storage in uso esegue il software NetApp Element 12.2 o versione successiva.
- **Nodo di gestione**: È stato implementato un nodo di gestione con versione 12.2 o successiva.
- **Servizi di gestione**: Il bundle di servizi di gestione è stato aggiornato alla versione 2.19 o successiva.
- Hai accesso per accedere al livello di amministratore.

attiva la modalità di manutenzione

È possibile utilizzare la procedura seguente per attivare la modalità di manutenzione per un nodo del cluster di storage.

Solo un nodo può essere in modalità di manutenzione alla volta.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

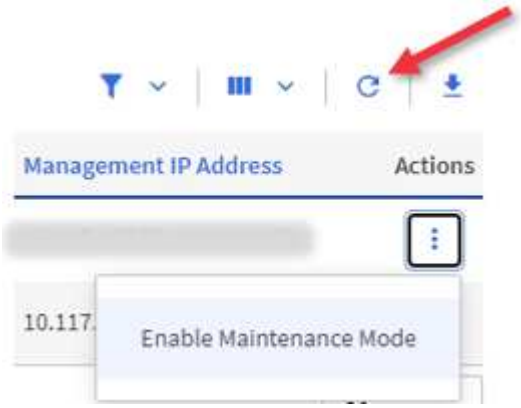
   ```
   https://<ManagementNodeIP>
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.

   Le opzioni della funzione della modalità di manutenzione sono disattivate a livello di sola lettura.

3. Nella casella blu di navigazione a sinistra, selezionare l'installazione di NetApp HCI.
4. Nel riquadro di navigazione a sinistra, selezionare **Nodes** (nodi).
5. Per visualizzare le informazioni sull'inventario dello storage, selezionare **Storage**.
6. Abilitare la modalità di manutenzione su un nodo di storage:

La tabella dei nodi di storage viene aggiornata automaticamente ogni due minuti per le azioni non avviate dall'utente. Prima di eseguire un'azione, per assicurarsi di disporre dello stato più aggiornato, è possibile aggiornare la tabella Nodes utilizzando l'icona di refresh situata nella parte superiore destra della tabella Nodes.



a. In **azioni**, selezionare **Enable Maintenance Mode** (attiva modalità di manutenzione).

   Mentre è attivata la modalità **Maintenance Mode**, le azioni della modalità di manutenzione non sono disponibili per il nodo selezionato e per tutti gli altri nodi dello stesso cluster.

Una volta completata l'attivazione della modalità di manutenzione*, nella colonna **Node Status** (Stato nodo) viene visualizzata l'icona di una chiave a forma di chiave e il testo "**Maintenance Mode**" (modalità di manutenzione) per il nodo in modalità di manutenzione.

Disattiva la modalità di manutenzione

Dopo che un nodo è stato impostato correttamente in modalità di manutenzione, l'azione **Disable Maintenance Mode** (Disattiva modalità di manutenzione) è disponibile per questo nodo. Le azioni sugli altri nodi non sono disponibili fino a quando la modalità di manutenzione non viene disattivata correttamente sul nodo sottoposto a manutenzione.

Fasi

1. Per il nodo in modalità di manutenzione, in **azioni**, selezionare **Disattiva modalità di manutenzione**.

   Mentre **Maintenance Mode** è disattivato, le azioni della modalità di manutenzione non sono disponibili per il nodo selezionato e per tutti gli altri nodi dello stesso cluster.

   Una volta completata la funzione **Disabling Maintenance Mode** (disattivazione modalità di manutenzione), la colonna **Node Status** (Stato nodo) visualizza **Active** (attivo).

   Quando un nodo è in modalità di manutenzione, non accetta nuovi dati. Di conseguenza, la disattivazione della modalità di manutenzione può richiedere più tempo, poiché il nodo deve sincronizzare il backup dei dati prima di uscire dalla modalità di manutenzione. Maggiore è il tempo impiegato in modalità di manutenzione, maggiore sarà il tempo necessario per disattivare la modalità di manutenzione.

Risolvere i problemi

Se si verificano errori durante l'attivazione o la disattivazione della modalità di manutenzione, viene visualizzato un errore di intestazione nella parte superiore della tabella Nodes (nodi). Per ulteriori informazioni

sull'errore, selezionare il collegamento **Mostra dettagli** fornito sul banner per visualizzare i risultati dell'API.

Trova ulteriori informazioni

- "Creare e gestire le risorse del cluster di storage"
- "Pagina delle risorse NetApp HCI"

Crea e gestisci i volumi utilizzando NetApp Hybrid Cloud Control

È possibile creare un volume e associarlo a un determinato account. L'associazione di un volume a un account consente all'account di accedere al volume tramite gli iniziatori iSCSI e le credenziali CHAP.

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

Puoi gestire i volumi in NetApp Hybrid Cloud Control nei seguenti modi:

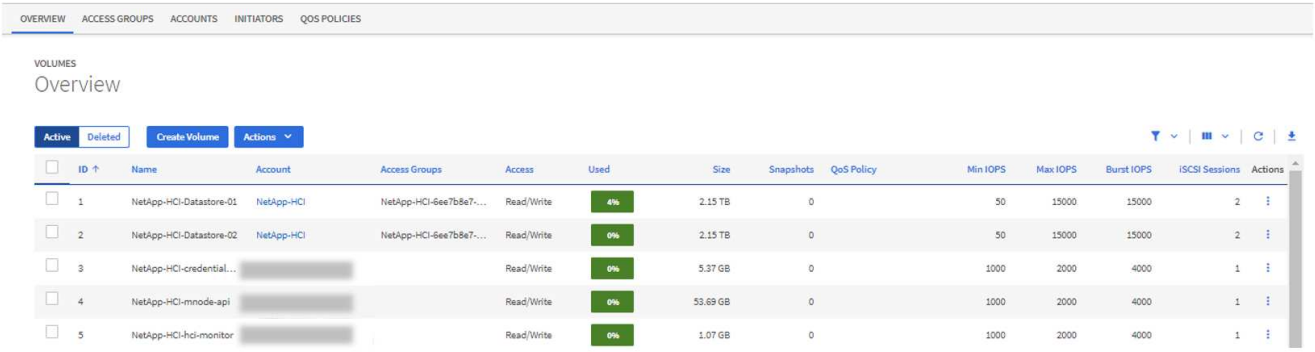
- Creare un volume
- Applicare un criterio QoS a un volume
- Modificare un volume
- Clonare i volumi
- Aggiungere volumi a un gruppo di accesso al volume
- Eliminare un volume
- Ripristinare un volume cancellato
- Eliminare un volume cancellato

Creare un volume

È possibile creare un volume di storage utilizzando NetApp Hybrid Cloud Control.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare la scheda **volumi** > **Panoramica**.



4. Selezionare **Create Volume** (Crea volume).

5. Immettere un nome per il nuovo volume.
6. Inserire le dimensioni totali del volume.

> La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB: 1 GB = 1 000 000 000 byte 1 GiB = 1 073 741 824 byte

7. Selezionare una dimensione di blocco per il volume.
8. Dall'elenco **account**, selezionare l'account che deve avere accesso al volume.

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

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

9. Per configurare la qualità del servizio per il volume, effettuare una delle seguenti operazioni:
   - In **Quality of Service Settings** (Impostazioni qualità del servizio), impostare i valori minimi, massimi e burst personalizzati per IOPS o utilizzare i valori QoS predefiniti.
   - Selezionare una policy QoS esistente attivando il comando **Assign Quality of Service Policy** (Assegna policy di qualità del servizio) e scegliendo una policy QoS esistente dall'elenco risultante.
   - Creare e assegnare una nuova policy QoS attivando l'opzione **Assign Quality of Service Policy** (Assegna policy di qualità del servizio) e facendo clic su **Create New QoS Policy** (Crea nuova policy QoS). Nella finestra visualizzata, immettere un nome per il criterio QoS, quindi immettere i valori QoS. Al termine, fare clic su **Crea policy sulla qualità del servizio**.

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

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

Applicare un criterio QoS a un volume

È possibile applicare una policy di QoS ai volumi di storage esistenti utilizzando NetApp Hybrid Cloud Control. Se invece è necessario impostare valori QoS personalizzati per un volume, è possibile Modificare un volume. Per creare un nuovo criterio QoS, vedere "Creare e gestire policy di QoS per volumi".

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare uno o più volumi da associare a un criterio QoS.
5. Fare clic sull'elenco a discesa **Actions** (azioni) nella parte superiore della tabella Volumes (volumi) e selezionare **Apply QoS Policy** (Applica policy QoS).
6. Nella finestra visualizzata, selezionare un criterio QoS dall'elenco e fare clic su **Apply QoS Policy** (Applica policy QoS).

> Se si utilizzano policy QoS su un volume, è possibile impostare una QoS personalizzata per rimuovere l'affiliazione della policy QoS con il volume. I valori di QoS personalizzati sovrascrivono i valori dei criteri di QoS per le impostazioni di QoS del volume.

Modificare un volume

Utilizzando NetApp Hybrid Cloud Control, è possibile modificare gli attributi del volume, ad esempio i valori QoS, le dimensioni del volume e l'unità di misura in base alla quale vengono calcolati i valori di byte. È inoltre possibile modificare l'accesso all'account per l'utilizzo della replica o per limitare l'accesso al volume.

A proposito di questa attività

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

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

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Nella colonna **azioni** della tabella volumi, espandere il menu del volume e selezionare **Modifica**.
5. Apportare le modifiche necessarie:

   a. Modificare le dimensioni totali del volume.

   > È possibile aumentare, ma non diminuire, le dimensioni del volume. È possibile ridimensionare un solo volume in una singola operazione di ridimensionamento. Le operazioni di garbage collection e gli aggiornamenti software non interrompono l'operazione di ridimensionamento.

   > Se si stanno regolando le dimensioni del volume per la replica, aumentare innanzitutto le dimensioni del volume assegnato come destinazione della replica. Quindi, è possibile ridimensionare il volume di origine. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

   > La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB: 1 GB = 1 000 000 000 byte 1 GiB = 1 073 741 824 byte

   b. Selezionare un diverso livello di accesso all'account:
      - Di sola lettura
      - Lettura/scrittura
      - Bloccato

    - Destinazione della replica

c. Selezionare l'account che deve avere accesso al volume.

   Inizia a digitare e la funzione di completamento automatico visualizza i valori possibili da scegliere.

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

d. Modificare la qualità del servizio effettuando una delle seguenti operazioni:

   i. Selezionare un criterio esistente.

   ii. In Custom Settings (Impostazioni personalizzate), impostare i valori minimo, massimo e burst per IOPS o utilizzare i valori predefiniti.

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

   > Quando si modificano i valori IOPS, è necessario aumentare in decine o centinaia. I valori di input richiedono numeri interi validi. Configurare volumi con un valore burst estremamente elevato. Ciò consente al sistema di elaborare più rapidamente carichi di lavoro sequenziali a blocchi di grandi dimensioni occasionali, limitando al contempo gli IOPS sostenuti per un volume.

6. Selezionare **Salva**.

Clonare i volumi

È possibile creare un clone di un singolo volume di storage o clonare un gruppo di volumi per creare una copia point-in-time dei dati. Quando si clonano un volume, il sistema crea uno snapshot del volume e quindi una copia dei dati a cui fa riferimento lo snapshot.

Prima di iniziare

- È necessario aggiungere ed eseguire almeno un cluster.
- È stato creato almeno un volume.
- È stato creato un account utente.
- Lo spazio disponibile senza provisioning deve essere uguale o superiore alle dimensioni del volume.

A proposito di questa attività

Il cluster supporta fino a due richieste di cloni in esecuzione per volume alla volta e fino a 8 operazioni di cloni di volume attivi alla volta. Le richieste che superano questi limiti vengono messe in coda per l'elaborazione successiva.

La clonazione del volume è un processo asincrono e il tempo richiesto dal processo dipende dalle dimensioni del volume che si sta clonando e dal carico corrente del cluster.

> I volumi clonati non ereditano l'appartenenza al gruppo di accesso al volume dal volume di origine.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare la scheda **volumi** > **Panoramica**.
4. Selezionare ciascun volume che si desidera clonare.
5. Fare clic sull'elenco a discesa **azioni** nella parte superiore della tabella volumi e selezionare **Clone**.
6. Nella finestra visualizzata, procedere come segue:

   a. Immettere un prefisso per il nome del volume (facoltativo).

   b. Scegliere il tipo di accesso dall'elenco **Access**.

   c. Scegliere un account da associare al nuovo clone del volume (per impostazione predefinita, è selezionata l'opzione **Copy from Volume** (Copia da volume), che utilizzerà lo stesso account utilizzato dal volume originale).

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

   Utilizzare le Best practice di denominazione descrittive. Ciò è particolarmente importante se nell'ambiente vengono utilizzati più cluster o server vCenter.

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

   a. Fare clic su **Clone Volumes** (Copia volumi).

   Il tempo necessario per completare un'operazione di cloning dipende dalle dimensioni del volume e dal carico corrente del cluster. Aggiornare la pagina se il volume clonato non compare nell'elenco dei volumi.

Aggiungere volumi a un gruppo di accesso al volume

È possibile aggiungere un singolo volume o un gruppo di volumi a un gruppo di accesso al volume.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare uno o più volumi da associare a un gruppo di accesso al volume.
5. Fare clic sull'elenco a discesa **azioni** nella parte superiore della tabella volumi e selezionare **Aggiungi a gruppo di accesso**.
6. Nella finestra visualizzata, selezionare un gruppo di accesso al volume dall'elenco **Volume Access Group**.

7. Fare clic su **Add Volume** (Aggiungi volume).

Eliminare un volume

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

A proposito di questa attività

Il sistema non elimina immediatamente i volumi cancellati, ma rimangono disponibili per circa otto ore. Dopo otto ore, vengono eliminati e non più disponibili. Se si ripristina un volume prima che venga spurgato dal sistema, il volume torna online e le connessioni iSCSI vengono ripristinate.

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

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

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare uno o più volumi da eliminare.
5. Fare clic sull'elenco a discesa **Actions** (azioni) nella parte superiore della tabella Volumes (volumi) e selezionare **Delete** (Elimina).
6. Nella finestra visualizzata, confermare l'azione facendo clic su **Sì**.

Ripristinare un volume cancellato

Una volta eliminato un volume di storage, è comunque possibile ripristinarlo entro otto ore dall'eliminazione.

Il sistema non elimina immediatamente i volumi cancellati, ma rimangono disponibili per circa otto ore. Dopo otto ore, vengono eliminati e non più disponibili. Se si ripristina un volume prima che venga spurgato dal sistema, il volume torna online e le connessioni iSCSI vengono ripristinate.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare **Deleted**.
5. Nella colonna **Actions** della tabella Volumes, espandere il menu del volume e selezionare **Restore**.
6. Confermare il processo selezionando **Sì**.

Eliminare un volume cancellato

Una volta cancellati, i volumi di storage rimangono disponibili per circa otto ore. Dopo otto ore, vengono eliminati automaticamente e non più disponibili. Se non si desidera attendere le otto ore, è possibile eliminare

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare **Deleted**.
5. Selezionare uno o più volumi da eliminare.
6. Effettuare una delle seguenti operazioni:
   - Se sono stati selezionati più volumi, fare clic sul filtro rapido **Purge** nella parte superiore della tabella.
   - Se è stato selezionato un singolo volume, nella colonna **Actions** della tabella Volumes (volumi), espandere il menu del volume e selezionare **Purge** (Rimuovi).
7. Nella colonna **Actions** della tabella Volumes, espandere il menu del volume e selezionare **Purge**.
8. Confermare il processo selezionando **Sì**.

Trova ulteriori informazioni

- "Scopri i volumi"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Creare e gestire i gruppi di accesso ai volumi

È possibile creare nuovi gruppi di accesso ai volumi, apportare modifiche al nome, agli iniziatori associati o ai volumi associati dei gruppi di accesso oppure eliminare i gruppi di accesso ai volumi esistenti utilizzando NetApp Hybrid Cloud Control.

Di cosa hai bisogno

- Si dispone delle credenziali di amministratore per questo sistema NetApp HCI.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.15.28. La gestione dello storage NetApp Hybrid Cloud Control non è disponibile nelle versioni precedenti dei service bundle.
- Assicurarsi di disporre di uno schema di denominazione logico per i gruppi di accesso ai volumi.

Aggiungere un gruppo di accesso al volume

È possibile aggiungere un gruppo di accesso a un volume a un cluster di storage utilizzando NetApp Hybrid Cloud Control.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.

2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **gruppi di accesso**.
5. Selezionare il pulsante **Create Access Group** (Crea gruppo di accesso).
6. Nella finestra di dialogo visualizzata, immettere un nome per il nuovo gruppo di accesso al volume.
7. (Facoltativo) nella sezione **initiator**, selezionare uno o più iniziatori da associare al nuovo gruppo di accesso al volume.

   Se si associa un iniziatore al gruppo di accesso al volume, tale iniziatore può accedere a ciascun volume del gruppo senza necessità di autenticazione.

8. (Facoltativo) nella sezione **volumi**, selezionare uno o più volumi da includere in questo gruppo di accesso al volume.
9. Selezionare **Crea gruppo di accesso**.

Modificare un gruppo di accesso al volume

È possibile modificare le proprietà di un gruppo di accesso a un volume esistente utilizzando NetApp Hybrid Cloud Control. È possibile modificare il nome, gli iniziatori associati o i volumi associati di un gruppo di accesso.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **gruppi di accesso**.
5. Nella colonna **azioni** della tabella dei gruppi di accesso, espandere il menu delle opzioni del gruppo di accesso da modificare.
6. Nel menu delle opzioni, selezionare **Modifica**.
7. Apportare le modifiche necessarie al nome, agli iniziatori associati o ai volumi associati.
8. Confermare le modifiche selezionando **Salva**.
9. Nella tabella **gruppi di accesso**, verificare che il gruppo di accesso rifletta le modifiche.

Eliminare un gruppo di accesso al volume

È possibile rimuovere un gruppo di accesso al volume utilizzando NetApp Hybrid Cloud Control e, allo stesso tempo, rimuovere dal sistema gli iniziatori associati a questo gruppo di accesso.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **gruppi di accesso**.

5. Nella colonna **azioni** della tabella dei gruppi di accesso, espandere il menu delle opzioni per il gruppo di accesso da eliminare.
6. Nel menu delle opzioni, selezionare **Delete** (Elimina).
7. Se non si desidera eliminare gli iniziatori associati al gruppo di accesso, deselezionare la casella di controllo **Delete initiator in this access group** (Elimina iniziatori in questo gruppo di accesso).
8. Confermare l'operazione di eliminazione selezionando **Sì**.

Trova ulteriori informazioni

- "Informazioni sui gruppi di accesso ai volumi"
- "Aggiungere l'iniziatore a un gruppo di accesso al volume"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Creare e gestire gli iniziatori

È possibile utilizzare "iniziatori" Per l'accesso ai volumi basato su CHAP e non basato su account. È possibile creare ed eliminare gli iniziatori e assegnare loro alias semplici per semplificare l'amministrazione e l'accesso ai volumi. Quando si aggiunge un iniziatore a un gruppo di accesso al volume, tale iniziatore consente l'accesso a tutti i volumi del gruppo.

Di cosa hai bisogno

- Si dispone delle credenziali di amministratore del cluster.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.17. La gestione degli iniziatori di NetApp Hybrid Cloud Control non è disponibile nelle versioni precedenti dei service bundle.

Opzioni

- Creare un iniziatore
- Aggiungere gli iniziatori a un gruppo di accesso al volume
- Modificare un alias iniziatore
- Eliminare gli iniziatori

Creare un iniziatore

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

A proposito di questa attività

Il formato accettato di un IQN Initiator è `iqn.yyyy-mm` dove y e m sono cifre seguite da testo che deve contenere solo cifre, caratteri alfabetici minuscoli e un punto (`.`), due punti (`:`) o trattino (`-`). Un esempio del formato è il seguente:

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

Il formato accettato di un iniziatore Fibre Channel WWPN è `:Aa:bB:CC:dd:11:22:33:44` oppure `AabBCCdd11223344`. Un esempio del formato è il seguente:

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

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **iniziatori**.
5. Selezionare il pulsante **Crea iniziatori**.

Opzione	Fasi
Creare uno o più iniziatori	a. Immettere l'IQN o il WWPN dell'iniziatore nel campo **IQN/WWPN**. b. Immettere un nome descrittivo per l'iniziatore nel campo **Alias**. c. (Facoltativo) selezionare **Add Initiator** (Aggiungi iniziatore) per aprire nuovi campi iniziatore o utilizzare l'opzione di creazione in blocco. d. Selezionare **Crea iniziatori**.
Iniziatori di creazione in blocco	a. Selezionare **Aggiungi IQN/WWPN in blocco**. b. Inserire un elenco di IQN o WWPN nella casella di testo. Ogni IQN o WWPN deve essere separato da virgole o spazi o su una propria riga. c. Selezionare **Aggiungi IQN/WWPN**. d. (Facoltativo) aggiungere alias univoci a ciascun iniziatore. e. Rimuovere dall'elenco qualsiasi iniziatore che potrebbe già esistere nell'installazione. f. Selezionare **Crea iniziatori**.

Aggiungere gli iniziatori a un gruppo di accesso al volume

È possibile aggiungere gli iniziatori a un gruppo di accesso al volume. Quando si aggiunge un iniziatore a un gruppo di accesso al volume, l'iniziatore consente l'accesso a tutti i volumi in tale gruppo di accesso al volume.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.

4. Selezionare la scheda **iniziatori**.
5. Selezionare uno o più iniziatori da aggiungere.
6. Selezionare **azioni > Aggiungi a gruppo di accesso**.
7. Selezionare il gruppo di accesso.
8. Confermare le modifiche selezionando **Add Initiator** (Aggiungi iniziatore).

Modificare un alias iniziatore

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

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **iniziatori**.
5. Nella colonna **azioni**, espandere il menu delle opzioni per l'iniziatore.
6. Selezionare **Modifica**.
7. Apportare le modifiche necessarie all'alias o aggiungere un nuovo alias.
8. Selezionare **Salva**.

Eliminare gli iniziatori

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

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **iniziatori**.
5. Eliminare uno o più iniziatori:
   a. Selezionare uno o più iniziatori da eliminare.
   b. Selezionare **azioni > Elimina**.
   c. Confermare l'operazione di eliminazione e selezionare **Sì**.

Trova ulteriori informazioni

- "Scopri di più sugli iniziatori"
- "Informazioni sui gruppi di accesso ai volumi"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Creare e gestire policy di QoS per volumi

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

> Per ulteriori informazioni sull'utilizzo, consulta il contenuto dei concetti di NetApp HCI "Policy di QoS" invece di un singolo volume "QoS".

Utilizzando NetApp Hybrid Cloud Control, è possibile creare e gestire policy QoS completando le seguenti attività:

- Creare una policy QoS
- Applicare un criterio QoS a un volume
- Modificare l'assegnazione del criterio QoS di un volume
- Modificare un criterio QoS
- Eliminare una policy QoS

Creare una policy QoS

È possibile creare policy QoS e applicarle a volumi che devono avere performance equivalenti.

> 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.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Fare clic sulla scheda **QoS Policies** (Criteri QoS).
5. Fare clic su **Crea policy**.
6. Inserire il nome * Policy Name*.

   > Utilizzare le Best practice di denominazione descrittive. Ciò è particolarmente importante se nell'ambiente vengono utilizzati più cluster o server vCenter.

7. Inserire i valori minimo IOPS, massimo IOPS e burst IOPS.
8. Fare clic su **Crea policy QoS**.

   Viene generato un ID di sistema per il criterio e il criterio viene visualizzato nella pagina QoS Policies (Criteri QoS) con i relativi valori QoS assegnati.

Applicare un criterio QoS a un volume

È possibile assegnare una policy QoS esistente a un volume utilizzando NetApp Hybrid Cloud Control.

Di cosa hai bisogno

Il criterio QoS che si desidera assegnare è stato creato.

A proposito di questa attività

Questa attività descrive come assegnare un criterio QoS a un singolo volume modificandone le impostazioni. La versione più recente di NetApp Hybrid Cloud Control non dispone di un'opzione di assegnazione in blocco per più di un volume. Fino a quando la funzionalità di assegnazione in blocco non sarà fornita in una release futura, è possibile utilizzare l'interfaccia utente Web Element o l'interfaccia utente del plug-in vCenter per assegnare in blocco i criteri QoS.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Fare clic sul menu **azioni** accanto al volume che si desidera modificare.
5. Nel menu visualizzato, selezionare **Edit** (Modifica).
6. Nella finestra di dialogo, attivare **Assign QoS Policy** (Assegna policy QoS) e selezionare il criterio QoS dall'elenco a discesa da applicare al volume selezionato.

   L'assegnazione di QoS sovrascriverà i valori di QoS dei singoli volumi precedentemente applicati.

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

   Il volume aggiornato con il criterio QoS assegnato viene visualizzato nella pagina Panoramica.

Modificare l'assegnazione del criterio QoS di un volume

È possibile rimuovere l'assegnazione di una policy QoS da un volume o selezionare una policy QoS diversa o una QoS personalizzata.

Di cosa hai bisogno

Il volume che si desidera modificare è assegnato Una policy QoS.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Fare clic sul menu **azioni** accanto al volume che si desidera modificare.
5. Nel menu visualizzato, selezionare **Edit** (Modifica).
6. Nella finestra di dialogo, eseguire una delle seguenti operazioni:

- Disattivare **Assign QoS Policy** e modificare i valori **min IOPS**, **Max IOPS** e **Burst IOPS** per la QoS dei singoli volumi.

  > Quando i criteri QoS sono disattivati, il volume utilizza i valori IOPS QoS predefiniti, a meno che non vengano modificati diversamente.

- Selezionare un criterio QoS diverso dall'elenco a discesa da applicare al volume selezionato.

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

   Il volume aggiornato viene visualizzato nella pagina Panoramica.

Modificare un criterio QoS

È possibile modificare il nome di un criterio QoS esistente o i valori associati al criterio. La modifica dei valori delle performance dei criteri QoS influisce sulla QoS per tutti i volumi associati al criterio.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Fare clic sulla scheda **QoS Policies** (Criteri QoS).
5. Fare clic sul menu **azioni** accanto al criterio QoS che si desidera modificare.
6. Fare clic su **Edit** (Modifica).
7. Nella finestra di dialogo **Edit QoS Policy** (Modifica policy QoS), modificare una o più delle seguenti opzioni:
   - **Name**: Il nome definito dall'utente per la policy QoS.
   - **IOPS min**: Il numero minimo di IOPS garantito per il volume. Impostazione predefinita = 50.
   - **IOPS max**: Il numero massimo di IOPS consentito per il volume. Impostazione predefinita = 15,000.
   - **Burst IOPS**: Il numero massimo di IOPS consentito per un breve periodo di tempo per il volume. Impostazione predefinita = 15,000.
8. Fare clic su **Save** (Salva).

   Il criterio QoS aggiornato viene visualizzato nella pagina QoS Policies (Criteri QoS).

   > È possibile fare clic sul collegamento nella colonna **volumi attivi** per visualizzare un elenco filtrato dei volumi assegnati a tale criterio.

Eliminare una policy QoS

È possibile eliminare una policy QoS se non è più necessaria. Quando si elimina un criterio QoS, tutti i volumi assegnati con il criterio mantengono i valori QoS precedentemente definiti dal criterio, ma come QoS dei singoli volumi. Qualsiasi associazione con la policy QoS eliminata viene rimossa.

Fasi

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.

2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Fare clic sulla scheda **QoS Policies** (Criteri QoS).
5. Fare clic sul menu **azioni** accanto al criterio QoS che si desidera modificare.
6. Fare clic su **Delete** (Elimina).
7. Confermare l'azione.

Trova ulteriori informazioni

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

Lavorare con il nodo di gestione

Panoramica del nodo di gestione

È possibile utilizzare il nodo di gestione (mNode) per utilizzare i servizi di sistema, gestire le risorse e le impostazioni del cluster, eseguire test e utility di sistema, configurare Active IQ per il monitoraggio del sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi.

> Come Best practice, associare un solo nodo di gestione a un'istanza di VMware vCenter ed evitare di definire le stesse risorse di storage e calcolo o istanze di vCenter in più nodi di gestione.

Per i cluster che eseguono Element Software versione 11.3 o successiva, è possibile utilizzare il nodo di gestione utilizzando una delle due interfacce seguenti:

- Con l'interfaccia utente del nodo di gestione (`https://[mNode IP]:442`), è possibile apportare modifiche alle impostazioni di rete e del cluster, eseguire test di sistema o utilizzare le utility di sistema.
- Con l'interfaccia utente API REST integrata (`https://[mNode IP]/mnode`), è possibile eseguire o comprendere le API relative ai servizi del nodo di gestione, tra cui la configurazione del server proxy, gli aggiornamenti del livello di servizio o la gestione delle risorse.

Installare o ripristinare un nodo di gestione:

- "Installare un nodo di gestione"
- "Configurazione di un NIC (Network Interface Controller) per lo storage"
- "Ripristinare un nodo di gestione"

Accedere al nodo di gestione:

- "Accedere al nodo di gestione (UI o REST API)"

Modificare il certificato SSL predefinito:

- "Modificare il certificato SSL predefinito del nodo di gestione"

Eseguire le attività con l'interfaccia utente del nodo di gestione:

- "Panoramica dell'interfaccia utente del nodo di gestione"

Eseguire le attività con le API REST del nodo di gestione:

- "Panoramica dell'interfaccia utente REST API del nodo di gestione"

Disattivare o attivare la funzionalità SSH remota o avviare una sessione di tunnel di supporto remoto con il supporto NetApp per risolvere i problemi:

- "Abilitare le connessioni remote del supporto NetApp"
- "Gestire la funzionalità SSH sul nodo di gestione"

Trova ulteriori informazioni

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

Installare o ripristinare un nodo di gestione

Installare un nodo di gestione

È possibile installare manualmente il nodo di gestione del cluster che esegue il software NetApp Element utilizzando l'immagine appropriata per la configurazione.

Questo processo manuale è destinato agli amministratori NetApp HCI che non utilizzano il motore di implementazione NetApp per l'installazione del nodo di gestione.

Di cosa hai bisogno

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- L'installazione utilizza IPv4. Il nodo di gestione 11.3 non supporta IPv6.

  Se è necessario supportare IPv6, è possibile utilizzare il nodo di gestione 11.1.

- Hai il permesso di scaricare il software dal NetApp Support Site.
- Hai identificato il tipo di immagine del nodo di gestione corretto per la tua piattaforma:

Piattaforma	Tipo di immagine di installazione
Microsoft Hyper-V.	iso
KVM	iso
VMware vSphere	iso, .ova
Citrix XenServer	iso
OpenStack	iso

- (Nodo di gestione 12.0 e versioni successive con server proxy) hai aggiornato NetApp Hybrid Cloud Control alla versione 2.16 dei servizi di gestione prima di configurare un server proxy.

A proposito di questa attività

Il nodo di gestione di Element 12.2 è un aggiornamento opzionale. Non è richiesto per le implementazioni esistenti.

Prima di seguire questa procedura, è necessario conoscere "volumi persistenti" e se si desidera o meno utilizzarli. I volumi persistenti sono opzionali ma consigliati per il ripristino dei dati di configurazione del nodo di gestione in caso di perdita di macchine virtuali.

Fasi

1. Scarica ISO o OVA e implementa la macchina virtuale
2. Creare il nodo di gestione admin e configurare la rete
3. Configurare la sincronizzazione dell'ora
4. Configurare il nodo di gestione
5. Configurare le risorse dei controller
6. (Solo NetApp HCI) configurare le risorse dei nodi di calcolo

Scarica ISO o OVA e implementa la macchina virtuale

1. Scaricare l'OVA o l'ISO per l'installazione dal "NetApp HCI" Pagina sul sito di supporto NetApp:
   a. Selezionare **Download Latest Release** (Scarica ultima versione) e accettare il contratto EULA.
   b. Selezionare l'immagine del nodo di gestione che si desidera scaricare.
2. Se l'OVA è stato scaricato, attenersi alla seguente procedura:
   a. Implementare OVA.
   b. Se il cluster di storage si trova su una subnet separata dal nodo di gestione (eth0) e si desidera utilizzare volumi persistenti, aggiungere un secondo controller di interfaccia di rete (NIC) alla VM sulla subnet di storage (ad esempio eth1) o assicurarsi che la rete di gestione possa instradare verso la rete di storage.
3. Se è stato scaricato l'ISO, attenersi alla seguente procedura:
   a. Creare una nuova macchina virtuale a 64 bit dall'hypervisor con la seguente configurazione:
      - Sei CPU virtuali
      - 24 GB DI RAM
      - Tipo di scheda di storage impostato su LSI Logic Parallel

      > L'impostazione predefinita per il nodo di gestione potrebbe essere LSI Logic SAS. Nella finestra **Nuova macchina virtuale**, verificare la configurazione della scheda di storage selezionando **Personalizza hardware** > **hardware virtuale**. Se necessario, modificare LSI Logic SAS in **LSI Logic Parallel**.

      - Disco virtuale da 400 GB, con thin provisioning
      - Un'interfaccia di rete virtuale con accesso a Internet e accesso allo storage MVIP.
      - Un'interfaccia di rete virtuale con accesso alla rete di gestione al cluster di storage. Se il cluster di storage si trova su una subnet separata dal nodo di gestione (eth0) e si desidera utilizzare volumi persistenti, aggiungere un secondo controller di interfaccia di rete (NIC) alla macchina virtuale sulla subnet di storage (eth1) o assicurarsi che la rete di gestione possa essere instradata alla rete di storage.

> Non accendere la macchina virtuale prima della fase indicata in questa procedura.

b. Collegare l'ISO alla macchina virtuale e avviare l'immagine di installazione .iso.

> L'installazione di un nodo di gestione mediante l'immagine potrebbe causare un ritardo di 30 secondi prima della visualizzazione della schermata iniziale.

4. Al termine dell'installazione, accendere la macchina virtuale per il nodo di gestione.

Creare il nodo di gestione admin e configurare la rete

1. Utilizzando l'interfaccia utente del terminale (TUI), creare un utente admin del nodo di gestione.

> Per spostarsi tra le opzioni di menu, premere i tasti freccia su o giù. Per spostarsi tra i pulsanti, premere Tab. Per spostarsi dai pulsanti ai campi, premere Tab. Per spostarsi tra i campi, premere i tasti freccia su o giù.

2. Configurare la rete dei nodi di gestione (eth0).

> Se è necessaria una scheda di rete aggiuntiva per isolare il traffico di storage, consultare le istruzioni per la configurazione di un'altra scheda di rete: "Configurazione di un NIC (Network Interface Controller) per lo storage".

Configurare la sincronizzazione dell'ora

1. Assicurarsi che il tempo sia sincronizzato tra il nodo di gestione e il cluster di storage utilizzando NTP:

> A partire dall'elemento 12.3.1, i passaggi da (a) a (e) vengono eseguiti automaticamente. Per il nodo di gestione 12.3.1, passare a. sottopase (f) per completare la configurazione di time sync.

a. Accedere al nodo di gestione utilizzando SSH o la console fornita dall'hypervisor.

b. Stop NTPD:

```
sudo service ntpd stop
```

c. Modificare il file di configurazione NTP `/etc/ntp.conf`:

   i. Commentare i server predefiniti (`server 0.gentoo.pool.ntp.org`) aggiungendo un `#` davanti a ciascuno.

   ii. Aggiungere una nuova riga per ciascun server di riferimento orario predefinito che si desidera aggiungere. I server di riferimento orario predefiniti devono essere gli stessi server NTP utilizzati nel cluster di storage in "passo successivo".

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time
server>
```

iii. Al termine, salvare il file di configurazione.

d. Forzare una sincronizzazione NTP con il server appena aggiunto.

```
sudo ntpd -gq
```

e. Riavviare NTPD.

```
sudo service ntpd start
```

f. Disattiva la sincronizzazione dell'ora con l'host tramite l'hypervisor (il seguente è un esempio VMware):

> Se si implementa mNode in un ambiente hypervisor diverso da VMware, ad esempio dall'immagine .iso in un ambiente OpenStack, fare riferimento alla documentazione dell'hypervisor per i comandi equivalenti.

i. Disattivare la sincronizzazione periodica dell'ora:

```
vmware-toolbox-cmd timesync disable
```

ii. Visualizzare e confermare lo stato corrente del servizio:

```
vmware-toolbox-cmd timesync status
```

iii. In vSphere, verificare che `Synchronize guest time with host` Nelle opzioni della macchina virtuale, la casella di controllo non è selezionata.

> Non attivare questa opzione se si apportano modifiche future alla macchina virtuale.

> Non modificare l'NTP dopo aver completato la configurazione di Time Sync, in quanto influisce sull'NTP quando si esegue "comando di installazione" sul nodo di gestione.

Configurare il nodo di gestione

1. Configurare ed eseguire il comando di setup del nodo di gestione:

> Viene richiesto di inserire le password in un prompt sicuro. Se il cluster si trova dietro un server proxy, è necessario configurare le impostazioni del proxy in modo da poter accedere a una rete pubblica.

```
sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

a. Sostituire il valore tra parentesi [ ] (comprese le parentesi) per ciascuno dei seguenti parametri richiesti:

> La forma abbreviata del nome del comando è tra parentesi ( ) e può essere sostituita con il nome completo.

- **--mnode_admin_user (-mu) [nome utente]**: Il nome utente per l'account amministratore del nodo di gestione. Probabilmente si tratta del nome utente dell'account utente utilizzato per accedere al nodo di gestione.
- **--storage_mvip (-SM) [indirizzo MVIP]**: L'indirizzo IP virtuale di gestione (MVIP) del cluster di storage che esegue il software Element. Configurare il nodo di gestione con lo stesso cluster di storage utilizzato durante "Configurazione dei server NTP".
- **--storage_Username (-su) [Username]**: Il nome utente dell'amministratore del cluster di storage per il cluster specificato da `--storage_mvip` parametro.
- **--Telemetry_Active (-t) [true]**: Conserva il valore true che consente la raccolta dei dati per l'analisi di Active IQ.

b. (Facoltativo): Aggiungere i parametri dell'endpoint Active IQ al comando:

- **--Remote_host (-rh) [AIQ_endpoint]**: L'endpoint in cui vengono inviati i dati di telemetria Active IQ per l'elaborazione. Se il parametro non è incluso, viene utilizzato l'endpoint predefinito.

c. (Consigliato): Aggiungere i seguenti parametri di volume persistente. Non modificare o eliminare l'account e i volumi creati per la funzionalità dei volumi persistenti, altrimenti si verificherà una perdita delle funzionalità di gestione.

- **--use_persistent_Volumes (-pv) [true/false, default: False]**: Attiva o disattiva i volumi persistenti. Inserire il valore true per abilitare la funzionalità dei volumi persistenti.
- **--Persistent_Volumes_account (-pva) [nome_account]**: IF `--use_persistent_volumes` è impostato su true, utilizzare questo parametro e inserire il nome dell'account di storage che verrà utilizzato per i volumi persistenti.

> Utilizzare un nome account univoco per i volumi persistenti diverso da qualsiasi nome account esistente nel cluster. È di fondamentale importanza mantenere l'account dei volumi persistenti separato dal resto dell'ambiente.

- **--persistent_Volumes_mvip (-pvm) [mvip]**: Immettere l'indirizzo IP virtuale di gestione (MVIP) del cluster di storage che esegue il software Element che verrà utilizzato con i volumi persistenti. Questo è necessario solo se il nodo di gestione gestisce più cluster di storage. Se non vengono gestiti più cluster, viene utilizzato il cluster predefinito MVIP.

d. Configurare un server proxy:
   - **--use_proxy (-up) [true/false, default: False]**: Attiva o disattiva l'utilizzo del proxy. Questo parametro è necessario per configurare un server proxy.
   - **--proxy_hostname_or_ip (-pi) [host]**: Il nome host o l'IP del proxy. Questa opzione è necessaria se si desidera utilizzare un proxy. Se si specifica questa opzione, viene richiesto di immettere `--proxy_port`.
   - **--proxy_Username (-pu) [nome utente]**: Il nome utente del proxy. Questo parametro è facoltativo.
   - **--proxy_password (-pp) [password]**: La password del proxy. Questo parametro è facoltativo.
   - **--proxy_port (-pq) [port, default: 0]**: La porta proxy. Se si specifica questa opzione, viene richiesto di inserire il nome host o l'IP del proxy (`--proxy_hostname_or_ip`).
   - **--proxy_ssh_port (-ps) [port, default: 443]**: La porta proxy SSH. Per impostazione predefinita, viene impostata la porta 443.
e. (Facoltativo) utilizzare la guida ai parametri se sono necessarie ulteriori informazioni su ciascun parametro:
   - **--help (-h)**: Restituisce informazioni su ciascun parametro. I parametri sono definiti come obbligatori o facoltativi in base all'implementazione iniziale. I requisiti dei parametri di aggiornamento e ridistribuzione potrebbero variare.
f. Eseguire `setup-mnode` comando.

Configurare le risorse dei controller

1. Individuare l'ID di installazione:
   a. Da un browser, accedere all'interfaccia utente API REST del nodo di gestione:
   b. Accedere a Storage MVIP ed effettuare l'accesso. Questa azione fa sì che il certificato venga accettato per la fase successiva.
   c. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   d. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
   e. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   f. Selezionare **Provalo**.
   g. Selezionare **Esegui**.
   h. Dal corpo della risposta del codice 200, copiare e salvare `id` per l'installazione da utilizzare in un passaggio successivo.

      L'installazione dispone di una configurazione delle risorse di base creata durante l'installazione o l'aggiornamento.

2. (Solo NetApp HCI) individuare il tag hardware per il nodo di calcolo in vSphere:

a. Selezionare l'host in vSphere Web Client Navigator.

b. Selezionare la scheda **Monitor** e selezionare **hardware Health**.

c. Vengono elencati il produttore e il numero di modello del BIOS del nodo. Copiare e salvare il valore per `tag` da utilizzare in un passaggio successivo.

3. Aggiungere una risorsa del controller vCenter per il monitoraggio NetApp HCI (solo installazioni NetApp HCI) e il controllo del cloud ibrido (per tutte le installazioni) al nodo di gestione risorse note:

   a. Accedere all'interfaccia utente API del servizio mnode sul nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode`:

   ```
   https:/<ManagementNodeIP>/mnode
   ```

   b. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:

      i. Inserire il nome utente e la password del cluster.

      ii. Immettere l'ID client come `mnode-client`.

      iii. Selezionare **autorizzare** per avviare una sessione.

      iv. Chiudere la finestra.

   c. Selezionare **POST /assets/{asset_id}/controller** per aggiungere una sottorisorsa del controller.

   > È necessario creare un nuovo ruolo NetApp HCC in vCenter per aggiungere una sottorisorsa del controller. Questo nuovo ruolo di NetApp HCC limiterà la vista dei servizi del nodo di gestione alle risorse solo NetApp. Vedere "Creare un ruolo NetApp HCC in vCenter".

   d. Selezionare **Provalo**.

   e. Inserire l'ID risorsa base principale copiato negli Appunti nel campo **asset_id**.

   f. Inserire i valori del payload richiesti con il tipo `vCenter` E vCenter.

   g. Selezionare **Esegui**.

(Solo NetApp HCI) configurare le risorse dei nodi di calcolo

1. (Solo per NetApp HCI) aggiungere una risorsa di nodo di calcolo al nodo di gestione risorse note:

   a. Selezionare **POST /assets/{asset_id}/compute-nodes** per aggiungere una sottorisorsa del nodo di calcolo con credenziali per la risorsa del nodo di calcolo.

   b. Selezionare **Provalo**.

   c. Inserire l'ID risorsa base principale copiato negli Appunti nel campo **asset_id**.

   d. Nel payload, inserire i valori del payload richiesti come definito nella scheda Model (modello). Invio `ESXi Host` come `type` e inserire il tag hardware salvato durante un passaggio precedente per `hardware_tag`.

   e. Selezionare **Esegui**.

Ulteriori informazioni

- "Volumi persistenti"

- "Aggiungere risorse di calcolo e controller al nodo di gestione"
- "Configurare una NIC storage"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Configurazione di un NIC (Network Interface Controller) per lo storage

Se si utilizza una scheda NIC aggiuntiva per lo storage, è possibile accedere al nodo di gestione tramite SSH o utilizzare la console vCenter ed eseguire un comando curl per impostare un'interfaccia di rete con tag o senza tag.

Prima di iniziare

- Conosci il tuo indirizzo IP eth0.
- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione 11.3 o successivo.

Opzioni di configurazione

Scegli l'opzione più adatta al tuo ambiente:

- Configurare un Network Interface Controller (NIC) per un'interfaccia di rete senza tag
- Configurare un NIC (Network Interface Controller) per lo storage per un'interfaccia di rete con tag

Configurare un Network Interface Controller (NIC) per un'interfaccia di rete senza tag

Fasi

1. Aprire una console SSH o vCenter.
2. Sostituire i valori nel seguente modello di comando ed eseguire il comando:

> I valori sono rappresentati da `$` per ciascuno dei parametri richiesti per la nuova interfaccia di rete dello storage. Il `cluster` l'oggetto nel seguente modello è obbligatorio e può essere utilizzato per la ridenominazione del nome host del nodo di gestione. `--insecure` oppure `-k` le opzioni non devono essere utilizzate negli ambienti di produzione.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
     "params": {
               "network": {
                         "$eth1": {
                                  "#default" : false,
                                  "address" : "$storage_IP",
                                  "auto" : true,
                                  "family" : "inet",
                                  "method" : "static",
                                  "mtu" : "9000",
                                  "netmask" : "$subnet_mask",
                                  "status" : "Up"
                                  }
                         },
               "cluster": {
                         "name": "$mnode_host_name"
                         }
             },
    "method": "SetConfig"
}
'
```

Configurare un NIC (Network Interface Controller) per lo storage per un'interfaccia di rete con tag

Fasi

1. Aprire una console SSH o vCenter.
2. Sostituire i valori nel seguente modello di comando ed eseguire il comando:

> I valori sono rappresentati da `$` per ciascuno dei parametri richiesti per la nuova interfaccia di rete dello storage. Il `cluster` l'oggetto nel seguente modello è obbligatorio e può essere utilizzato per la ridenominazione del nome host del nodo di gestione. `--insecure` oppure `-k` le opzioni non devono essere utilizzate negli ambienti di produzione.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
     "params": {
               "network": {
                         "$eth1": {
                                  "#default" : false,
                                  "address" : "$storage_IP",
                                  "auto" : true,
                                  "family" : "inet",
                                  "method" : "static",
                                  "mtu" : "9000",
                                  "netmask" : "$subnet_mask",
                                  "status" : "Up",
                                  "virtualNetworkTag" : "$vlan_id"
                                  }
                          },
               "cluster": {
                         "name": "$mnode_host_name",
                         "cipi": "$eth1.$vlan_id",
                         "sipi": "$eth1.$vlan_id"
                         }
             },
    "method": "SetConfig"
}
'
```

Ulteriori informazioni

- "Aggiungere risorse di calcolo e controller al nodo di gestione"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Ripristinare un nodo di gestione

È possibile ripristinare e ridistribuire manualmente il nodo di gestione per il cluster che esegue il software NetApp Element se il nodo di gestione precedente utilizzava volumi persistenti.

È possibile implementare un nuovo OVA ed eseguire uno script di ridistribuzione per estrarre i dati di configurazione da un nodo di gestione precedentemente installato che esegue la versione 11.3 e successive.

Di cosa hai bisogno

- Il nodo di gestione precedente eseguiva il software NetApp Element versione 11.3 o successiva con "volumi persistenti" funzionalità attivata.
- Conosci MVIP e SVIP del cluster contenente i volumi persistenti.
- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- L'installazione utilizza IPv4. Il nodo di gestione 11.3 non supporta IPv6.
- Hai il permesso di scaricare il software dal NetApp Support Site.
- Hai identificato il tipo di immagine del nodo di gestione corretto per la tua piattaforma:

Piattaforma	Tipo di immagine di installazione
Microsoft Hyper-V.	iso
KVM	iso
VMware vSphere	iso, .ova
Citrix XenServer	iso
OpenStack	iso

Fasi

1. Scarica ISO o OVA e implementa la macchina virtuale
2. Configurare la rete
3. Configurare la sincronizzazione dell'ora
4. Configurare il nodo di gestione

Scarica ISO o OVA e implementa la macchina virtuale

1. Scaricare l'OVA o l'ISO per l'installazione dal "NetApp HCI" Pagina sul sito di supporto NetApp:
   a. Fare clic su **Download Latest Release** (Scarica ultima versione) e accettare il contratto di licenza con l'utente finale.
   b. Selezionare l'immagine del nodo di gestione che si desidera scaricare.
2. Se l'OVA è stato scaricato, attenersi alla seguente procedura:
   a. Implementare OVA.
   b. Se il cluster di storage si trova su una subnet separata dal nodo di gestione (eth0) e si desidera utilizzare volumi persistenti, aggiungere un secondo controller di interfaccia di rete (NIC) alla VM sulla subnet di storage (ad esempio eth1) o assicurarsi che la rete di gestione possa instradare verso la rete di storage.
3. Se è stato scaricato l'ISO, attenersi alla seguente procedura:
   a. Creare una nuova macchina virtuale a 64 bit dall'hypervisor con la seguente configurazione:
      - Sei CPU virtuali
      - 24 GB DI RAM
      - Disco virtuale da 400 GB, con thin provisioning
      - Un'interfaccia di rete virtuale con accesso a Internet e accesso allo storage MVIP.
      - Un'interfaccia di rete virtuale con accesso alla rete di gestione al cluster di storage. Se il cluster di storage si trova su una subnet separata dal nodo di gestione (eth0) e si desidera utilizzare volumi

persistenti, aggiungere un secondo controller di interfaccia di rete (NIC) alla macchina virtuale sulla subnet di storage (eth1) o assicurarsi che la rete di gestione possa essere instradata alla rete di storage.

> Non accendere la macchina virtuale prima della fase indicata in questa procedura.

b. Collegare l'ISO alla macchina virtuale e avviare l'immagine di installazione .iso.

> L'installazione di un nodo di gestione mediante l'immagine potrebbe causare un ritardo di 30 secondi prima della visualizzazione della schermata iniziale.

4. Al termine dell'installazione, accendere la macchina virtuale per il nodo di gestione.

Configurare la rete

1. Utilizzando l'interfaccia utente del terminale (TUI), creare un utente admin del nodo di gestione.

> Per spostarsi tra le opzioni di menu, premere i tasti freccia su o giù. Per spostarsi tra i pulsanti, premere Tab. Per spostarsi dai pulsanti ai campi, premere Tab. Per spostarsi tra i campi, premere i tasti freccia su o giù.

2. Configurare la rete dei nodi di gestione (eth0).

> Se è necessaria una scheda di rete aggiuntiva per isolare il traffico di storage, consultare le istruzioni per la configurazione di un'altra scheda di rete: "Configurazione di un NIC (Network Interface Controller) per lo storage".

Configurare la sincronizzazione dell'ora

1. Assicurarsi che il tempo sia sincronizzato tra il nodo di gestione e il cluster di storage utilizzando NTP:

> A partire dall'elemento 12.3.1, i passaggi da (a) a (e) vengono eseguiti automaticamente. Per il nodo di gestione 12.3.1, passare a. sottopase (f) per completare la configurazione di time sync.

1. Accedere al nodo di gestione utilizzando SSH o la console fornita dall'hypervisor.
2. Stop NTPD:

```
sudo service ntpd stop
```

3. Modificare il file di configurazione NTP `/etc/ntp.conf`:
   a. Commentare i server predefiniti (`server 0.gentoo.pool.ntp.org`) aggiungendo un `#` davanti a ciascuno.
   b. Aggiungere una nuova riga per ciascun server di riferimento orario predefinito che si desidera aggiungere. I server di riferimento orario predefiniti devono essere gli stessi server NTP utilizzati nel cluster di storage in "passo successivo".

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. Al termine, salvare il file di configurazione.

4. Forzare una sincronizzazione NTP con il server appena aggiunto.

```
sudo ntpd -gq
```

5. Riavviare NTPD.

```
sudo service ntpd start
```

6. Disattiva la sincronizzazione dell'ora con l'host tramite l'hypervisor (il seguente è un esempio VMware):

> Se si implementa mNode in un ambiente hypervisor diverso da VMware, ad esempio dall'immagine .iso in un ambiente OpenStack, fare riferimento alla documentazione dell'hypervisor per i comandi equivalenti.

a. Disattivare la sincronizzazione periodica dell'ora:

```
vmware-toolbox-cmd timesync disable
```

b. Visualizzare e confermare lo stato corrente del servizio:

```
vmware-toolbox-cmd timesync status
```

c. In vSphere, verificare che `Synchronize guest time with host` Nelle opzioni della macchina virtuale, la casella di controllo non è selezionata.

> Non attivare questa opzione se si apportano modifiche future alla macchina virtuale.

> Non modificare l'NTP dopo aver completato la configurazione di Time Sync, in quanto influisce sull'NTP quando si esegue comando di ridistribuzione sul nodo di gestione.

Configurare il nodo di gestione

1. Creare una directory di destinazione temporanea per il contenuto del bundle di servizi di gestione:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Scaricare il bundle di servizi di gestione (versione 2.15.28 o successiva) precedentemente installato sul nodo di gestione esistente e salvarlo in `/sf/etc/mnode/` directory.
3. Estrarre il bundle scaricato utilizzando il seguente comando, sostituendo il valore tra parentesi quadre [ ] (comprese le parentesi quadre) con il nome del file bundle:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle
file]
```

4. Estrarre il file risultante in `/sf/etc/mnode-archive` directory:

```
tar -C /sf/etc/mnode/mnode-archive -xvf
/sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. Creare un file di configurazione per account e volumi:

```
echo '{"trident": true, "mvip": "[mvip IP address]", "account_name":
"[persistent volume account name]"}' | sudo tee /sf/etc/mnode/mnode-
archive/management-services-metadata.json
```

   a. Sostituire il valore tra parentesi [ ] (comprese le parentesi) per ciascuno dei seguenti parametri richiesti:
      - **[mvip IP address]**: L'indirizzo IP virtuale di gestione del cluster di storage. Configurare il nodo di gestione con lo stesso cluster di storage utilizzato durante "Configurazione dei server NTP".
      - **[nome account volume persistente]**: Il nome dell'account associato a tutti i volumi persistenti in questo cluster di storage.
6. Configurare ed eseguire il comando di ridistribuzione del nodo di gestione per connettersi ai volumi persistenti ospitati sul cluster e avviare i servizi con i dati di configurazione del nodo di gestione precedenti:

> Viene richiesto di inserire le password in un prompt sicuro. Se il cluster si trova dietro un server proxy, è necessario configurare le impostazioni del proxy in modo da poter accedere a una rete pubblica.

```
sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

   a. Sostituire il valore tra parentesi quadre [ ] (comprese le parentesi quadre) con il nome utente dell'account amministratore del nodo di gestione. Probabilmente si tratta del nome utente dell'account utente utilizzato per accedere al nodo di gestione.

> È possibile aggiungere il nome utente o consentire allo script di richiedere le informazioni.

b. Eseguire `redeploy-mnode` comando. Al termine della ridistribuzione, lo script visualizza un messaggio di esito positivo.

c. Se si accede alle interfacce web Element o NetApp HCI (come il nodo di gestione o il controllo cloud ibrido NetApp) utilizzando il nome di dominio completo (FQDN) del sistema, "riconfigurare l'autenticazione per il nodo di gestione".

> Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 e versioni successive. Se in precedenza era stata attivata la funzionalità SSH sul nodo di gestione, potrebbe essere necessario "Disattivare nuovamente SSH" sul nodo di gestione ripristinato.

Ulteriori informazioni

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

Accedere al nodo di gestione

A partire dal software NetApp Element versione 11.3, il nodo di gestione contiene due UI: 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.

Per i cluster che eseguono Element Software versione 11.3 o successiva, è possibile utilizzare una delle due interfacce seguenti:

- Utilizzando l'interfaccia utente del nodo di gestione (`https:// [mNode IP}:442`), è possibile apportare modifiche alle impostazioni di rete e del cluster, eseguire test di sistema o utilizzare le utility di sistema.
- Utilizzando l'interfaccia utente REST API integrata (`https://[mNode IP}/mnode`), è possibile eseguire o comprendere le API relative ai servizi del nodo di gestione, tra cui la configurazione del server proxy, gli aggiornamenti del livello di servizio o la gestione delle risorse.

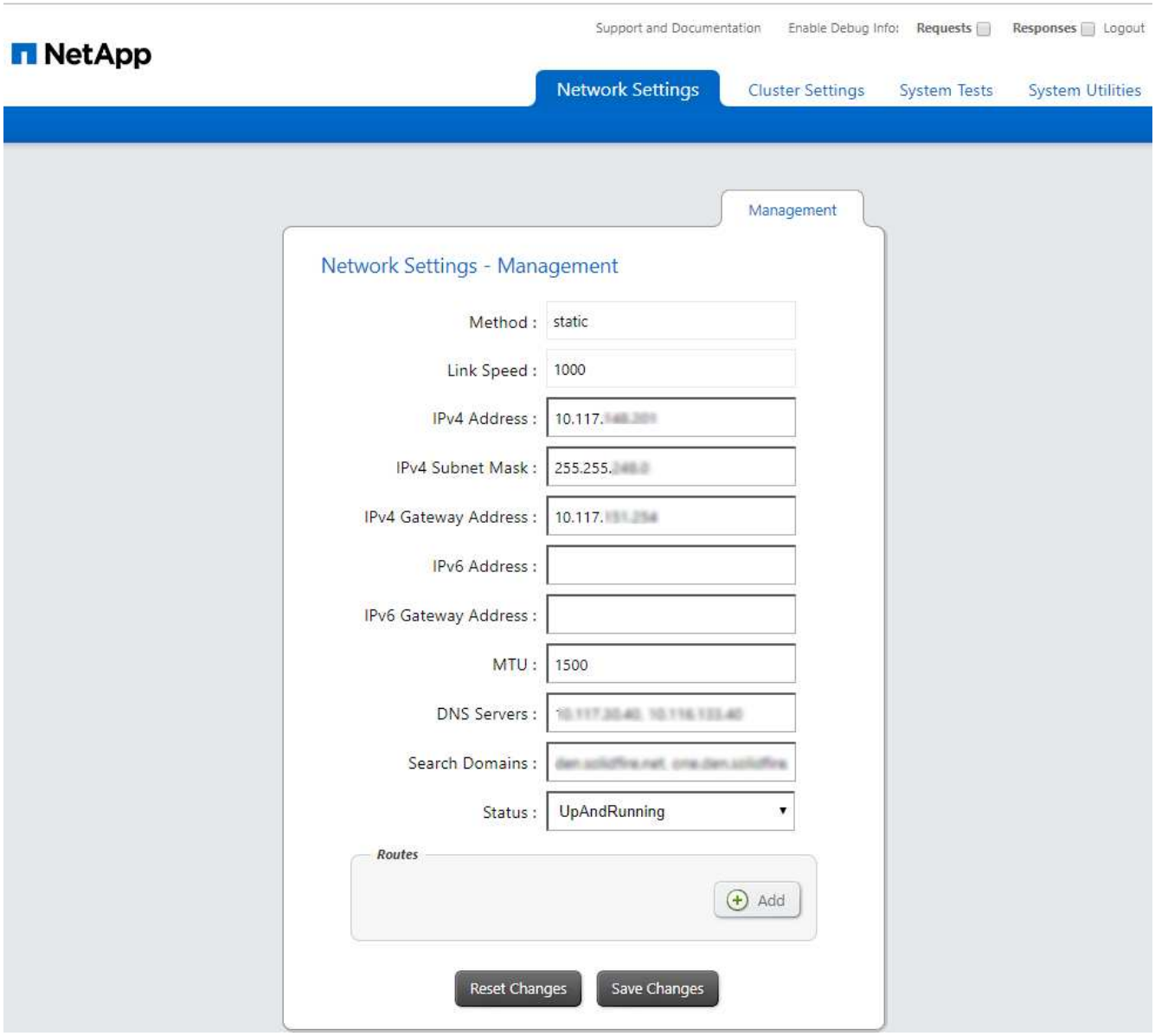
Accedere all'interfaccia utente del nodo di gestione per nodo

Dall'interfaccia utente per nodo, è possibile accedere alle impostazioni di rete e cluster e utilizzare le utility e i test di sistema.

Fasi

1. Accedere all'interfaccia utente per nodo per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da :442

```
https://[IP address]:442
```



2. Inserire il nome utente e la password del nodo di gestione quando richiesto.

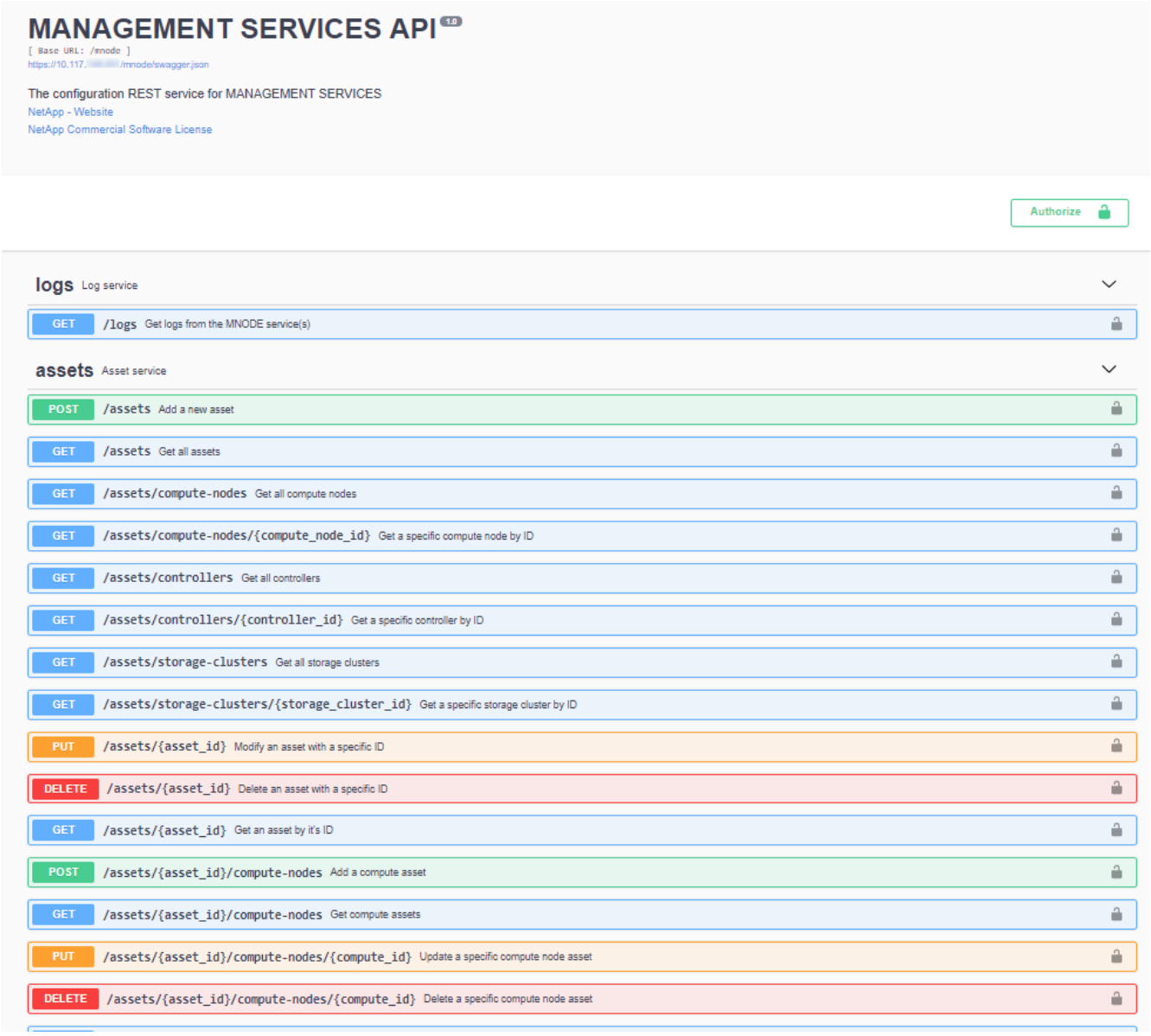
Accedere all'interfaccia utente REST API del nodo di gestione

Dall'interfaccia utente dell'API REST, è possibile accedere a un menu di API correlate al servizio che controllano i servizi di gestione sul nodo di gestione.

Fasi

1. Per accedere all'interfaccia utente API REST per i servizi di gestione, immettere l'indirizzo IP del nodo di gestione seguito da `/mnode`:

```
https://[IP address]/mnode
```



2. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e immettere le credenziali di amministratore del cluster per le autorizzazioni per l'utilizzo delle API.

Ulteriori informazioni

- "Abilitare il monitoraggio Active IQ e NetApp HCI"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Modificare il certificato SSL predefinito del nodo di gestione

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

Quando si configura un nodo di gestione, viene creato un certificato SSL (Secure Sockets Layer) e una chiave privata univoci, utilizzati per tutte le comunicazioni HTTPS tramite l'interfaccia utente elemento, l'interfaccia utente per nodo o le API. Il software Element supporta i certificati autofirmati e quelli emessi e verificati da

un'autorità di certificazione (CA) attendibile.

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

- **GetNodeSSLCertificate**

  È possibile utilizzare "Metodo GetNodeSSLCertificate" Per recuperare informazioni sul certificato SSL attualmente installato, inclusi tutti i dettagli del certificato.

- **SetNodeSSLCertificate**

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

- **RemoveNodeSSLCertificate**

  Questo "Metodo RemoveNodeSSLCertificate" Rimuove il certificato SSL e la chiave privata attualmente installati. Il cluster genera quindi un nuovo certificato autofirmato e una nuova chiave privata.

Trova ulteriori informazioni

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

Utilizzare l'interfaccia utente del nodo di gestione

Panoramica dell'interfaccia utente del nodo di gestione

Con l'interfaccia utente del nodo di gestione (`https://<mNodeIP>:442`), è possibile apportare modifiche alle impostazioni di rete e del cluster, eseguire test di sistema o utilizzare le utility di sistema.

Attività che è possibile eseguire con l'interfaccia utente del nodo di gestione:

- "Configurare il monitoraggio degli avvisi su NetApp HCI"
- "Modificare e verificare le impostazioni di rete, cluster e sistema del nodo di gestione"
- "Eseguire le utility di sistema dal nodo di gestione"

Trova ulteriori informazioni

- "Accedere al nodo di gestione"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Configurare il monitoraggio degli avvisi su NetApp HCI

È possibile configurare le impostazioni per monitorare gli avvisi sul sistema NetApp HCI.

Il monitoraggio degli avvisi di NetApp HCI inoltra gli avvisi di sistema del cluster di storage NetApp HCI a vCenter Server, consentendo di visualizzare tutti gli avvisi per NetApp HCI dall'interfaccia del client Web vSphere.

1. Aprire l'interfaccia utente del nodo di gestione per nodo (`https://[IP address]:442`).
2. Fare clic sulla scheda **Alert Monitor**.
3. Configurare le opzioni di monitoraggio degli avvisi.

Opzioni di monitoraggio degli avvisi

opzioni	Descrizione
Eseguire i test di Alert Monitor	Esegue i test di sistema del monitor per verificare quanto segue: • Connettività NetApp HCI e VMware vCenter • Associazione di NetApp HCI e VMware vCenter tramite le informazioni del datastore fornite dal servizio QoSSIOC • Elenchi degli allarmi NetApp HCI e vCenter correnti
Raccogli avvisi	Attiva o disattiva l'inoltro degli allarmi di storage NetApp HCI a vCenter. È possibile selezionare il cluster di storage di destinazione dall'elenco a discesa. L'impostazione predefinita per questa opzione è `Enabled`.
Raccogliere gli avvisi delle Best practice	Attiva o disattiva l'inoltro degli avvisi di Best practice per lo storage NetApp HCI a vCenter. Gli avvisi di Best practice sono errori che vengono generati da una configurazione di sistema non ottimale. L'impostazione predefinita per questa opzione è `Disabled`. Se disattivato, gli avvisi di Best practice per lo storage NetApp HCI non vengono visualizzati in vCenter.

opzioni	Descrizione
Inviare i dati di supporto ad AIQ	Controlla il flusso di dati di supporto e monitoraggio da VMware vCenter a NetApp SolidFire Active IQ. Le opzioni sono le seguenti: • Enabled (attivato): Tutti gli allarmi vCenter, gli allarmi storage NetApp HCI e i dati di supporto vengono inviati a NetApp SolidFire Active IQ. Ciò consente a NetApp di supportare e monitorare in modo proattivo l'installazione di NetApp HCI, in modo che i possibili problemi possano essere rilevati e risolti prima di influire sul sistema. • Disabled (Disattivato): Non vengono inviati allarmi vCenter, allarmi storage NetApp HCI o dati di supporto a NetApp SolidFire Active IQ. Se è stata disattivata l'opzione **Send data to AIQ** (Invia dati ad AIQ*) utilizzando NetApp Deployment Engine, è necessario "abilitare la telemetria" Utilizzando nuovamente l'API REST del nodo di gestione per configurare il servizio da questa pagina.
Inviare i dati del nodo di calcolo ad AIQ	Controlla il flusso di dati di supporto e monitoraggio dai nodi di calcolo a NetApp SolidFire Active IQ. Le opzioni sono le seguenti: • Abilitato: I dati di supporto e monitoraggio relativi ai nodi di calcolo vengono trasmessi a NetApp SolidFire Active IQ per consentire il supporto proattivo per l'hardware del nodo di calcolo. • Disattivato: I dati di supporto e monitoraggio relativi ai nodi di calcolo non vengono trasmessi a NetApp SolidFire Active IQ. Se è stata disattivata l'opzione **Send data to AIQ** (Invia dati ad AIQ*) utilizzando NetApp Deployment Engine, è necessario "abilitare la telemetria" Utilizzando nuovamente l'API REST del nodo di gestione per configurare il servizio da questa pagina.

Ulteriori informazioni

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

Modificare e verificare le impostazioni di rete, cluster e sistema del nodo di gestione

È possibile modificare e verificare le impostazioni di rete, cluster e sistema del nodo di gestione.

- Aggiornare le impostazioni di rete del nodo di gestione
- Aggiornare le impostazioni del cluster del nodo di gestione
- Verificare le impostazioni del nodo di gestione

Aggiornare le impostazioni di rete del nodo di gestione

Nella scheda Network Settings (Impostazioni di rete) dell'interfaccia utente del nodo di gestione per nodo, è possibile modificare i campi dell'interfaccia di rete del nodo di gestione.

1. Aprire l'interfaccia utente del nodo di gestione per nodo.
2. Fare clic sulla scheda **Impostazioni di rete**.
3. Visualizzare o inserire le seguenti informazioni:
   a. **Metodo**: Scegliere uno dei seguenti metodi per configurare l'interfaccia:
      - `loopback`: Consente di definire l'interfaccia di loopback IPv4.
      - `manual`: Consente di definire le interfacce per le quali non viene eseguita alcuna configurazione per impostazione predefinita.
      - `dhop`Consente di ottenere un indirizzo IP tramite DHCP.
      - `static`: Consente di definire le interfacce Ethernet con indirizzi IPv4 allocati in modo statico.
   b. **Velocità di collegamento**: La velocità negoziata dalla NIC virtuale.
   c. **IPv4 Address**: Indirizzo IPv4 per la rete eth0.
   d. **IPv4 Subnet Mask**: Suddivisioni di indirizzi della rete IPv4.
   e. **IPv4 Gateway Address** (Indirizzo gateway IPv4): Indirizzo di rete del router per l'invio dei pacchetti dalla rete locale.
   f. **IPv6 Address**: L'indirizzo IPv6 per la rete eth0.
   g. **IPv6 Gateway Address** (Indirizzo gateway IPv6): Indirizzo di rete del router per l'invio dei pacchetti dalla rete locale.

      > Le opzioni IPv6 non sono supportate per la versione 11.3 o successive del nodo di gestione.

   h. **MTU**: Dimensione massima dei pacchetti che un protocollo di rete può trasmettere. Deve essere maggiore o uguale a 1500. Se si aggiunge una seconda scheda di rete per lo storage, il valore deve essere 9000.
   i. **Server DNS**: Interfaccia di rete utilizzata per la comunicazione del cluster.
   j. **Search Domains** (Cerca domini): Consente di cercare ulteriori indirizzi MAC disponibili per il sistema.
   k. **Status**: Valori possibili:

- `UpAndRunning`
- `Down`
- `Up`

l. **Routes**: Route statiche verso host o reti specifici tramite l'interfaccia associata per l'utilizzo da parte dei percorsi.

Aggiornare le impostazioni del cluster del nodo di gestione

Nella scheda Cluster Settings (Impostazioni cluster) dell'interfaccia utente per nodo per il nodo di gestione, è possibile modificare i campi dell'interfaccia cluster quando un nodo si trova negli stati Available (disponibile), PendingActive (PendingActive) e Active (attivo).

1. Aprire l'interfaccia utente del nodo di gestione per nodo.
2. Fare clic sulla scheda **Cluster Settings** (Impostazioni cluster).
3. Visualizzare o inserire le seguenti informazioni:
   - **Ruolo**: Ruolo del nodo di gestione nel cluster. Valore possibile: `Management`.
   - **Version**: Versione del software Element in esecuzione sul cluster.
   - **Default Interface**: Interfaccia di rete predefinita utilizzata per la comunicazione del nodo di gestione con il cluster che esegue il software Element.

Verificare le impostazioni del nodo di gestione

Dopo aver modificato le impostazioni di gestione e di rete per il nodo di gestione e aver eseguito le modifiche, è possibile eseguire test per convalidare le modifiche apportate.

1. Aprire l'interfaccia utente del nodo di gestione per nodo.
2. Nell'interfaccia utente del nodo di gestione, fare clic su **Test di sistema**.
3. Completare una delle seguenti operazioni:
   a. Per verificare che le impostazioni di rete configurate siano valide per il sistema, fare clic su **Test Network Config**.
   b. Per verificare la connettività di rete a tutti i nodi del cluster su entrambe le interfacce 1G e 10G utilizzando pacchetti ICMP, fare clic su **Test Ping**.
4. Visualizzare o inserire quanto segue:
   - **Hosts**: Specificare un elenco separato da virgole di indirizzi o nomi host dei dispositivi da ping.
   - **Tentativi**: Specificare il numero di volte in cui il sistema deve ripetere il test ping. Predefinito: 5.
   - **Packet Size** (dimensione pacchetto): Specificare il numero di byte da inviare nel pacchetto ICMP inviato a ciascun IP. Il numero di byte deve essere inferiore al valore MTU massimo specificato nella configurazione di rete.
   - **Timeout msec**: Specificare il numero di millisecondi da attendere per ogni singola risposta ping. Impostazione predefinita: 500 ms.
   - **Total Timeout sec**: Specificare il tempo in secondi in cui il ping deve attendere una risposta di sistema prima di eseguire il successivo tentativo di ping o terminare il processo. Predefinito: 5.
   - **Proibisci frammentazione**: Attiva il flag DF (do not fragment) per i pacchetti ICMP.

Ulteriori informazioni

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

Eseguire le utility di sistema dal nodo di gestione

È possibile utilizzare l'interfaccia utente per nodo per il nodo di gestione per creare o eliminare i bundle di supporto del cluster, reimpostare le impostazioni di configurazione del nodo o riavviare la rete.

Fasi

1. Aprire l'interfaccia utente del nodo di gestione per nodo utilizzando le credenziali admin del nodo di gestione.
2. Fare clic su **Utilità di sistema**.
3. Fare clic sul pulsante dell'utilità che si desidera eseguire:
   a. **Control Power** (alimentazione controllo): Riavvia, spegne e riaccende il nodo. Specificare una delle seguenti opzioni.

      Questa operazione causa la perdita temporanea della connettività di rete.

      - **Azione**: Le opzioni includono `Restart` e. `Halt` (spegnere).
      - **Wakeup Delay** (ritardo di attivazione): Qualsiasi tempo aggiuntivo prima che il nodo torni online.

   b. **Create Cluster Support Bundle**: Crea il bundle di supporto del cluster per assistere le valutazioni diagnostiche del supporto NetApp di uno o più nodi in un cluster. Specificare le seguenti opzioni:
      - **Nome bundle**: Nome univoco per ciascun bundle di supporto creato. Se non viene fornito alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo.
      - **MVIP**: L'MVIP del cluster. I bundle vengono raccolti da tutti i nodi del cluster. Questo parametro è obbligatorio se il parametro Nodes non è specificato.
      - **Nodes**: Gli indirizzi IP dei nodi da cui raccogliere i bundle. Utilizzare nodi o MVIP, ma non entrambi, per specificare i nodi da cui raccogliere i bundle. Questo parametro è obbligatorio se MVIP non è specificato.
      - **Username**: Il nome utente dell'amministratore del cluster.
      - **Password**: La password di amministrazione del cluster.
      - **Allow Incomplete** (Consenti incompleto): Consente di continuare l'esecuzione dello script se non è possibile raccogliere bundle da uno o più nodi.
      - **Extra args**: Questo parametro viene inviato a. `sf_make_support_bundle` script. Questo parametro deve essere utilizzato solo su richiesta del supporto NetApp.

   c. **Delete All Support Bundle** (Elimina tutti i pacchetti di supporto): Elimina tutti i pacchetti di supporto correnti sul nodo di gestione.

   d. **Reset Node**: Ripristina il nodo di gestione su una nuova immagine di installazione. In questo modo, tutte le impostazioni, ad eccezione della configurazione di rete, vengono modificate nello stato predefinito. Specificare le seguenti opzioni:
      - **Build**: URL di un'immagine software di elementi remoti in cui il nodo verrà reimpostato.
      - **Opzioni**: Specifiche per l'esecuzione delle operazioni di ripristino. I dettagli sono forniti dal supporto NetApp, se necessario.

Questa operazione causa la perdita temporanea della connettività di rete.

e. **Restart Networking** (Riavvia rete): Riavvia tutti i servizi di rete sul nodo di gestione.

Questa operazione causa la perdita temporanea della connettività di rete.

Ulteriori informazioni

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

Utilizzare l'API REST del nodo di gestione

Panoramica dell'interfaccia utente REST API del nodo di gestione

Utilizzando l'interfaccia utente REST API integrata (`https://<ManagementNodeIP>/mnode`), è possibile eseguire o comprendere le API relative ai servizi del nodo di gestione, tra cui la configurazione del server proxy, gli aggiornamenti del livello di servizio o la gestione delle risorse.

Attività che è possibile eseguire con le API REST:

Autorizzazione

- "Ottenere l'autorizzazione per utilizzare le API REST"

Configurazione delle risorse

- "Abilitare il monitoraggio Active IQ e NetApp HCI"
- "Configurare un server proxy per il nodo di gestione"
- "Configurare NetApp Hybrid Cloud Control per più vCenter"
- "Aggiungere risorse di calcolo e controller al nodo di gestione"
- "Creare e gestire le risorse del cluster di storage"

Gestione delle risorse

- "Visualizzare o modificare le risorse dei controller esistenti"
- "Creare e gestire le risorse del cluster di storage"
- "Rimuovere una risorsa dal nodo di gestione"
- "Utilizzare l'API REST per raccogliere i log NetApp HCI"
- "Verificare le versioni dei sistemi operativi e dei servizi del nodo di gestione"
- "Recupero dei log dai servizi di gestione"

Trova ulteriori informazioni

- "Accedere al nodo di gestione"
- "Plug-in NetApp Element per server vCenter"

- "Pagina delle risorse NetApp HCI"

Ottenere l'autorizzazione per utilizzare le API REST

È necessario autorizzare prima di poter utilizzare le API per i servizi di gestione nell'interfaccia utente REST API. A tale scopo, è necessario ottenere un token di accesso.

Per ottenere un token, fornire le credenziali di amministratore del cluster e un ID client. Ogni token dura circa dieci minuti. Dopo la scadenza di un token, puoi autorizzare di nuovo per un nuovo token di accesso.

La funzionalità di autorizzazione viene impostata durante l'installazione e l'implementazione del nodo di gestione. Il servizio token si basa sul cluster di storage definito durante l'installazione.

Prima di iniziare

- La versione del cluster in uso deve disporre del software NetApp Element 11.3 o versione successiva.
- Si dovrebbe aver implementato un nodo di gestione con versione 11.3 o successiva.

Comando API

```
TOKEN=`curl -k -X POST https://MVIP/auth/connect/token -F client_id=mnode-
client -F grant_type=password -F username=CLUSTER_ADMIN -F
password=CLUSTER_PASSWORD|awk -F':' '{print $2}'|awk -F',' '{print
$1}'|sed s/\"//g`
```

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio immettendo, ad esempio, l'indirizzo IP del nodo di gestione seguito dal nome del servizio `/mnode/`:

   ```
   https://<ManagementNodeIP>/mnode/
   ```

2. Fare clic su **autorizzare**.

   In alternativa, è possibile fare clic su un'icona a forma di lucchetto accanto a qualsiasi API del servizio.

3. Completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Non inserire un valore per il client secret.
   d. Fare clic su **autorizzare** per avviare una sessione.
4. Chiudere la finestra di dialogo **Available Authorisations** (autorizzazioni disponibili).

   Se si tenta di eseguire un comando dopo la scadenza del token, viene visualizzato un `401 Error: UNAUTHORIZED` viene visualizzato il messaggio. Se compare questo, autorizzare di nuovo.

Trova ulteriori informazioni

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

Abilitare il monitoraggio Active IQ e NetApp HCI

È possibile attivare il monitoraggio dello storage Active IQ per il monitoraggio del calcolo di NetApp HCI e NetApp HCI, se non lo si è già fatto durante l'installazione o l'aggiornamento. Potrebbe essere necessario utilizzare questa procedura se la telemetria è stata disattivata utilizzando il motore di implementazione di NetApp HCI.

Il servizio Active IQ Collector inoltra i dati di configurazione e le metriche delle performance del cluster basate su software Element a NetApp Active IQ per il reporting storico e il monitoraggio delle performance quasi in tempo reale. Il servizio di monitoraggio NetApp HCI consente di inoltrare gli errori del cluster di storage a vCenter per la notifica degli avvisi.

Prima di iniziare

- Il cluster di storage esegue il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione con versione 11.3 o successiva.
- Hai accesso a Internet. Il servizio Active IQ Collector non può essere utilizzato da siti oscuri che non dispongono di connettività esterna.

Fasi

1. Ottenere l'ID risorsa di base per l'installazione:
   a. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Fare clic su **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Fare clic su **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra.
   c. Dall'interfaccia utente API REST, fare clic su **GET /Installations** (OTTIENI installazione/installazioni).
   d. Fare clic su **Provalo**.
   e. Fare clic su **Execute** (Esegui).
   f. Dal corpo della risposta del codice 200, copiare il `id` per l'installazione.

```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
```

L'installazione dispone di una configurazione delle risorse di base creata durante l'installazione o l'aggiornamento.

2. Attivare la telemetria:
   a. Accedere all'interfaccia utente API del servizio mnode sul nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode`:

      ```
      https://<ManagementNodeIP>/mnode
      ```

   b. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Fare clic su **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra.
   c. Configurare la risorsa di base:
      i. Fare clic su **PUT /assets/{asset_id}**.
      ii. Fare clic su **Provalo**.
      iii. Inserire quanto segue nel payload JSON:

      ```
      {
      "telemetry_active": true
      "config": {}
      }
      ```

      iv. Inserire l'ID di base del passaggio precedente in **asset_ID**.
      v. Fare clic su **Execute** (Esegui).

      Il servizio Active IQ viene riavviato automaticamente ogni volta che si modificano le risorse. La modifica delle risorse comporta un breve ritardo prima dell'applicazione delle impostazioni.

3. Se non l'hai già fatto, Aggiungi una risorsa controller vCenter per il monitoraggio NetApp HCI (solo installazioni NetApp HCI) e il controllo cloud ibrido (per tutte le installazioni) al nodo di gestione risorse note:

   Per i servizi di monitoraggio NetApp HCI è necessaria una risorsa controller.

   a. Fare clic su **POST /assets/{asset_id}/controller** per aggiungere una sottorisorsa del controller.
   b. Fare clic su **Provalo**.
   c. Inserire l'ID risorsa base principale copiato negli Appunti nel campo **asset_id**.
   d. Inserire i valori del payload richiesti con `type` come `vCenter` E vCenter.

```
{
"username": "string",
"password": "string",
"ip": "string",
"type": "vCenter",
"host_name": "string",
"config": {}
}
```

   `ip` È l'indirizzo IP di vCenter.

   e. Fare clic su **Execute** (Esegui).

Trova ulteriori informazioni

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

Configurare NetApp Hybrid Cloud Control per più vCenter

È possibile configurare NetApp Hybrid Cloud Control per gestire le risorse di due o più vCenter che non utilizzano Linked Mode.

Questa procedura deve essere utilizzata dopo l'installazione iniziale quando è necessario aggiungere risorse per un'installazione scalata di recente o quando le nuove risorse non sono state aggiunte automaticamente alla configurazione. Utilizza queste API per aggiungere risorse aggiunte di recente all'installazione.

Di cosa hai bisogno

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione con versione 11.3 o successiva.

Fasi

1. "Aggiungere nuovi vCenter come risorse del controller" alla configurazione del nodo di gestione.
2. "Aggiungi nuovi nodi di calcolo come risorse di calcolo" alla configurazione del nodo di gestione.

> Potrebbe essere necessario "Modificare le credenziali BMC per i nodi di calcolo" per risolvere un `Hardware ID not available` oppure `Unable to Detect` Errore indicato in NetApp Hybrid Cloud Control.

3. Aggiornare l'API del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

> In alternativa, è possibile attendere 2 minuti per l'aggiornamento dell'inventario nell'interfaccia utente di NetApp Hybrid Cloud Control.

   a. Fare clic su **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Fare clic su **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra.
   b. Dall'interfaccia utente API REST, fare clic su **GET /Installations** (OTTIENI installazione/installazioni).
   c. Fare clic su **Provalo**.
   d. Fare clic su **Execute** (Esegui).
   e. Dalla risposta, copiare l'ID della risorsa di installazione (`"id"`).
   f. Dall'interfaccia utente API REST, fare clic su **GET /Installations/{id}**.
   g. Fare clic su **Provalo**.
   h. Impostare Refresh su `True`.
   i. Incollare l'ID della risorsa di installazione nel campo **id**.
   j. Fare clic su **Execute** (Esegui).
4. Aggiorna il browser NetApp Hybrid Cloud Control per vedere le modifiche.

Trova ulteriori informazioni

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

Aggiungere risorse di calcolo e controller al nodo di gestione

È possibile aggiungere risorse di calcolo e controller alla configurazione del nodo di gestione utilizzando l'interfaccia utente REST API.

Potrebbe essere necessario aggiungere una risorsa se l'installazione è stata scalata di recente e le nuove risorse non sono state aggiunte automaticamente alla configurazione. Utilizza queste API per aggiungere risorse aggiunte di recente all'installazione.

Di cosa hai bisogno

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.

- È stato implementato un nodo di gestione con versione 11.3 o successiva.
- Lo hai fatto "Ha creato un nuovo ruolo NetApp HCC in vCenter" Per limitare la vista dei servizi del nodo di gestione alle risorse solo NetApp.
- Si dispone dell'indirizzo IP e delle credenziali per la gestione di vCenter.
- Si dispone dell'indirizzo IP di gestione del nodo di calcolo (ESXi) e delle credenziali root.
- Si dispone dell'indirizzo IP di gestione dell'hardware (BMC) e delle credenziali di amministratore.

A proposito di questa attività

(Solo NetApp HCI) se non vengono visualizzati nodi di calcolo nel controllo del cloud ibrido (HCC) dopo aver scalato il sistema NetApp HCI, è possibile aggiungere un nodo di calcolo utilizzando `POST /assets/{asset_id}/compute-nodes` descritto in questa procedura.

> Quando si aggiungono manualmente i nodi di calcolo, assicurarsi di aggiungere anche le risorse BMC, altrimenti viene restituito un errore.

Fasi

1. Ottenere l'ID risorsa di base per l'installazione:
   a. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

   ```
   https://<ManagementNodeIP>/inventory/1/
   ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra.
   c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   d. Selezionare **Provalo**.
   e. Selezionare **Esegui**.
   f. Dal corpo della risposta del codice 200, copiare il `id` per l'installazione.

   ```
   {
     "installations": [
       {
         "_links": {
           "collection":
   "https://10.111.211.111/inventory/1/installations",
           "self":
   "https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
   91ee-12f111xxc7x0x"
         },
         "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
   ```

> L'installazione dispone di una configurazione delle risorse di base creata durante l'installazione o l'aggiornamento.

g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.
h. Selezionare **Provalo**.
i. Incollare l'ID della risorsa di installazione nel campo **id**.
j. Selezionare **Esegui**.
k. Dalla risposta, copiare e salvare l'ID del controller del cluster (`"controllerId"`) da utilizzare in un passaggio successivo.

2. (Solo per nodi di calcolo) Individuare il tag hardware per il nodo di calcolo In vSphere.
3. Per aggiungere una risorsa controller (vCenter), un nodo di calcolo (ESXi) o un hardware (BMC) a una risorsa di base esistente, selezionare una delle seguenti opzioni.

Opzione	Descrizione
POST /Assets/{asset_id}/controller	a. Aprire l'interfaccia utente dell'API REST del servizio mNode sul nodo di gestione: `https://<ManagementNodeIP>/mnode` i. Selezionare **autorizzare** e completare le seguenti operazioni: A. Inserire il nome utente e la password del cluster. B. Immettere l'ID client come `mnode-client`. C. Selezionare **autorizzare** per avviare una sessione. D. Chiudere la finestra. b. Selezionare **POST /assets/{asset_id}/controller**. c. Selezionare **Provalo**. d. Inserire l'ID risorsa di base principale nel campo **asset_id**. e. Aggiungere i valori richiesti al payload. f. Selezionare **Esegui**.

Opzione	Descrizione
POST /assets/{asset_id}/nodi di calcolo	a. Aprire l'interfaccia utente dell'API REST del servizio mNode sul nodo di gestione: `https://<ManagementNodeIP>/mnode` i. Selezionare **autorizzare** e completare le seguenti operazioni: A. Inserire il nome utente e la password del cluster. B. Immettere l'ID client come `mnode-client`. C. Selezionare **autorizzare** per avviare una sessione. D. Chiudere la finestra. b. Selezionare **POST /assets/{asset_id}/compute-nodes**. c. Selezionare **Provalo**. d. Inserire l'ID risorsa base principale copiato in un passaggio precedente nel campo **asset_id**. e. Nel payload, procedere come segue: i. Inserire l'IP di gestione per il nodo in `ip` campo. ii. Per `hardwareTag`, inserire il valore del tag hardware salvato in una fase precedente. iii. Inserire altri valori, come richiesto. f. Selezionare **Esegui**.

Opzione	Descrizione
POST /assets/{asset_id}/nodi-hardware	a. Aprire l'interfaccia utente dell'API REST del servizio mNode sul nodo di gestione: `https://<ManagementNodeIP>/mnode` i. Selezionare **autorizzare** e completare le seguenti operazioni: A. Inserire il nome utente e la password del cluster. B. Immettere l'ID client come `mnode-client`. C. Selezionare **autorizzare** per avviare una sessione. D. Chiudere la finestra. b. Selezionare **POST /assets/{asset_id}/hardware-nodes**. c. Selezionare **Provalo**. d. Inserire l'ID risorsa di base principale nel campo **asset_id**. e. Aggiungere i valori richiesti al payload. f. Selezionare **Esegui**.

Trova ulteriori informazioni

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

Come individuare un tag hardware per un nodo di calcolo

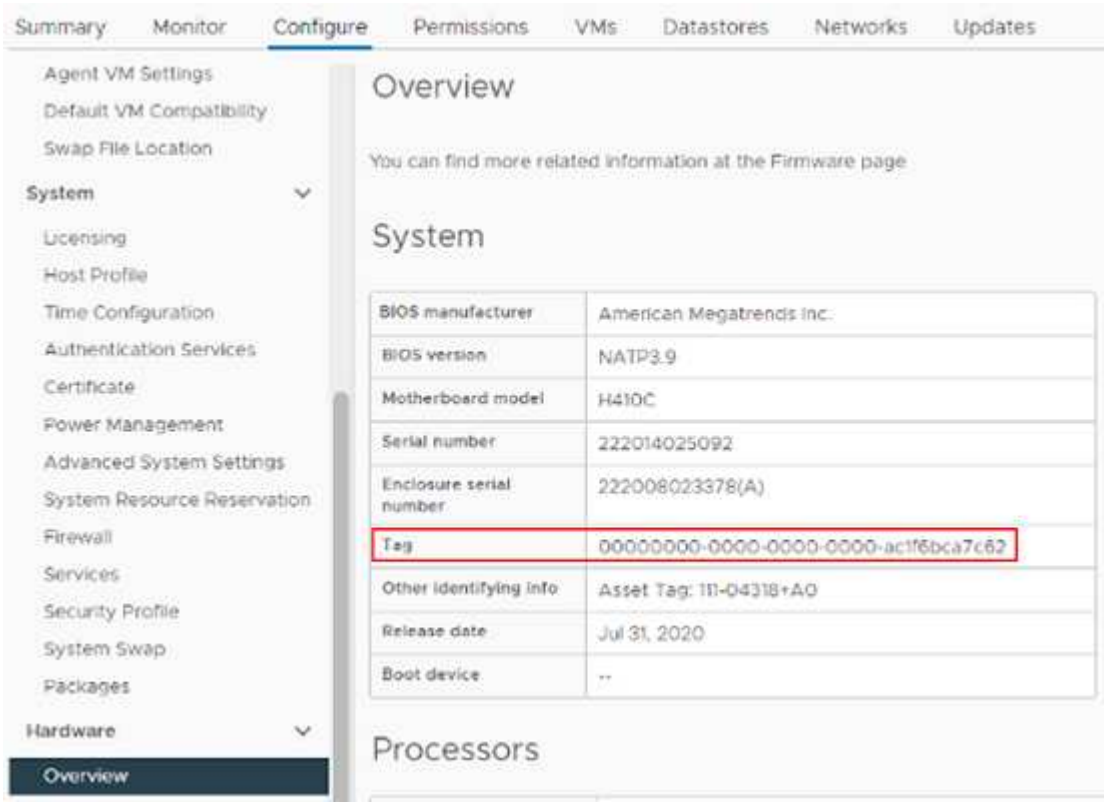
È necessario il tag hardware per aggiungere le risorse del nodo di calcolo alla configurazione del nodo di gestione utilizzando l'interfaccia utente REST API.

VMware vSphere 8.0 e 7.0

Individuare il tag hardware per un nodo di calcolo in VMware vSphere Web Client 8.0 e 7.0.

Fasi

1. Selezionare l'host in vSphere Web Client Navigator.
2. Selezionare la scheda **Configura**.
3. Dalla barra laterale, selezionare **hardware** > **Panoramica**. Controllare se il tag hardware è elencato in `System` tabella.



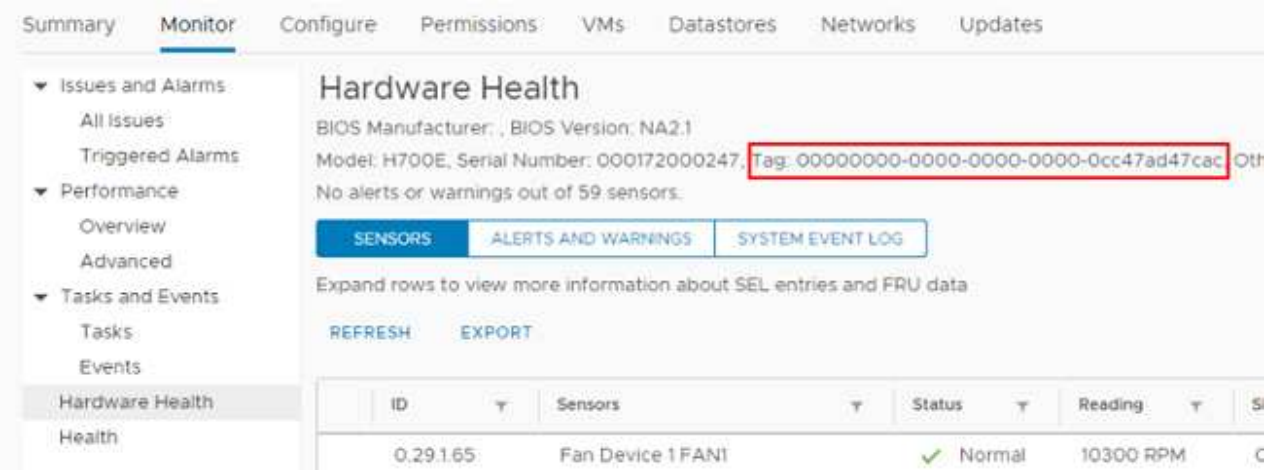
4. Copiare e salvare il valore per **Tag**.
5. Aggiungi le risorse di calcolo e controller al nodo di gestione.

VMware vSphere 6.7 e 6.5

Individuare il tag hardware per un nodo di calcolo in VMware vSphere Web Client 6.7 e 6.5.

Fasi

1. Selezionare l'host in vSphere Web Client Navigator.
2. Selezionare la scheda **Monitor** e selezionare **hardware Health**.
3. Verificare che il tag sia elencato con il produttore e il numero di modello del BIOS.



4. Copiare e salvare il valore per **Tag**.
5. Aggiungi le risorse di calcolo e controller al nodo di gestione.

Creare e gestire le risorse del cluster di storage

È possibile aggiungere nuove risorse del cluster di storage al nodo di gestione, modificare le credenziali memorizzate per le risorse del cluster di storage note ed eliminare le risorse del cluster di storage dal nodo di gestione utilizzando l'API REST.

Di cosa hai bisogno

- Assicurarsi che la versione del cluster di storage in uso utilizzi il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver implementato un nodo di gestione con versione 11.3 o successiva.

Opzioni di gestione delle risorse del cluster di storage

Scegliere una delle seguenti opzioni:

- Recuperare l'ID di installazione e l'ID del cluster di una risorsa del cluster di storage
- Aggiungere una nuova risorsa di cluster di storage
- Modificare le credenziali memorizzate per una risorsa del cluster di storage
- Eliminare una risorsa del cluster di storage

Recuperare l'ID di installazione e l'ID del cluster di una risorsa del cluster di storage

È possibile utilizzare L'API REST per ottenere l'ID di installazione e l'ID del cluster di storage. Per aggiungere una nuova risorsa del cluster di storage è necessario l'ID dell'installazione e l'ID del cluster per modificare o eliminare una risorsa specifica del cluster di storage.

Fasi

1. Accedere all'interfaccia utente API REST per il servizio di inventario immettendo l'indirizzo IP del nodo di gestione seguito da `/inventory/1/`:

```
https://<ManagementNodeIP>/inventory/1/
```

2. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Fare clic su **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Fare clic su **GET /Installations**.
4. Fare clic su **Provalo**.
5. Fare clic su **Execute** (Esegui).

   L'API restituisce un elenco di tutte le installazioni note.

6. Dal corpo di risposta del codice 200, salvare il valore in `id` che si trova nell'elenco delle installazioni. Questo è l'ID dell'installazione. Ad esempio:

```
"installations": [
    {
      "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",
      "name": "my-hci-installation",
      "_links": {
        "collection": "https://localhost/inventory/1/installations",
        "self": "https://localhost/inventory/1/installations/1234a678-
12ab-35dc-7b4a-1234a5b6a7ba"
      }
    }
  ]
```

7. Accedere all'interfaccia utente API REST per il servizio di storage immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

8. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Fare clic su **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
9. Fare clic su **GET /Clusters**.
10. Fare clic su **Provalo**.
11. Inserire l'ID di installazione salvato in precedenza in `installationId` parametro.
12. Fare clic su **Execute** (Esegui).

    L'API restituisce un elenco di tutti i cluster di storage noti in questa installazione.

13. Dal corpo di risposta del codice 200, individuare il cluster di storage corretto e salvare il valore nel cluster `storageId` campo. Questo è l'ID del cluster di storage.

Aggiungere una nuova risorsa di cluster di storage

È possibile utilizzare l'API REST per aggiungere una o più nuove risorse del cluster di storage all'inventario dei nodi di gestione. Quando si aggiunge una nuova risorsa del cluster di storage, questa viene automaticamente registrata con il nodo di gestione.

Di cosa hai bisogno

- È stata copiata la ID cluster storage e ID installazione per qualsiasi cluster di storage che si desidera aggiungere.
- Se si aggiungono più nodi di storage, sono state lette e comprese le limitazioni di "cluster autorevole" e supporto di più cluster di storage.

> Tutti gli utenti definiti nel cluster autorevole sono definiti come utenti su tutti gli altri cluster legati all'istanza di Hybrid Cloud Control.

Fasi

1. Accedere all'interfaccia utente API REST per il servizio di storage immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

2. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Fare clic su **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Fare clic su **POST /cluster**.
4. Fare clic su **Provalo**.
5. Inserire le informazioni del nuovo cluster di storage nei seguenti parametri nel campo **Request Body** (corpo richiesta):

   ```
   {
     "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
     "mvip": "10.0.0.1",
     "password": "admin",
     "userId": "admin"
   }
   ```

Parametro	Tipo	Descrizione
`installationId`	stringa	L'installazione in cui aggiungere il nuovo cluster di storage. Inserire l'ID di installazione salvato in precedenza in questo parametro.
`mvip`	stringa	L'indirizzo IP virtuale di gestione IPv4 (MVIP) del cluster di storage.
`password`	stringa	La password utilizzata per comunicare con il cluster di storage.
`userId`	stringa	L'ID utente utilizzato per comunicare con il cluster di storage (l'utente deve disporre dei privilegi di amministratore).

6. Fare clic su **Execute** (Esegui).

   L'API restituisce un oggetto contenente informazioni sulla risorsa del cluster di storage appena aggiunta, ad esempio il nome, la versione e l'indirizzo IP.

Modificare le credenziali memorizzate per una risorsa del cluster di storage

È possibile modificare le credenziali memorizzate che il nodo di gestione utilizza per accedere a un cluster di storage. L'utente scelto deve disporre dell'accesso di amministratore del cluster.

> Assicurarsi di aver seguito i passaggi descritti in Recuperare l'ID di installazione e l'ID del cluster di una risorsa del cluster di storage prima di continuare.

Fasi

1. Accedere all'interfaccia utente API REST per il servizio di storage immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

2. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Fare clic su **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Fare clic su **PUT /clusters/{storageId}**.
4. Fare clic su **Provalo**.
5. Incollare l'ID del cluster di storage precedentemente copiato in `storageId` parametro.
6. Modificare uno o entrambi i seguenti parametri nel campo **corpo della richiesta**:

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

Parametro	Tipo	Descrizione
`password`	stringa	La password utilizzata per comunicare con il cluster di storage.
`userId`	stringa	L'ID utente utilizzato per comunicare con il cluster di storage (l'utente deve disporre dei privilegi di amministratore).

7. Fare clic su **Execute** (Esegui).

Eliminare una risorsa del cluster di storage

Se il cluster di storage non è più in servizio, è possibile eliminare una risorsa del cluster di storage. Quando si rimuove una risorsa del cluster di storage, questa viene automaticamente annullata dalla registrazione dal nodo di gestione.

> Assicurarsi di aver seguito i passaggi descritti in Recuperare l'ID di installazione e l'ID del cluster di una risorsa del cluster di storage prima di continuare.

Fasi

1. Accedere all'interfaccia utente API REST per il servizio di storage immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Fare clic su **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Fare clic su **DELETE /clusters/{storageId}**.
4. Fare clic su **Provalo**.
5. Inserire l'ID del cluster di storage copiato in precedenza in `storageId` parametro.
6. Fare clic su **Execute** (Esegui).

   All'esito positivo, l'API restituisce una risposta vuota.

Trova ulteriori informazioni

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

Visualizzare o modificare le risorse dei controller esistenti

È possibile visualizzare informazioni sui controller VMware vCenter esistenti e modificarli nella configurazione del nodo di gestione utilizzando l'API REST. I controller sono istanze di VMware vCenter registrate nel nodo di gestione per l'installazione di NetApp HCI.

Prima di iniziare

- Assicurarsi che la versione del cluster in uso utilizzi il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver implementato un nodo di gestione con versione 11.3 o successiva.

Accedere all'API REST dei servizi di gestione

Fasi

1. Accedere all'interfaccia utente API REST per i servizi di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/vcenter/1/`:

   ```
   https://<ManagementNodeIP>/vcenter/1/
   ```

2. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Fare clic su **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.

Visualizzare le informazioni memorizzate sui controller esistenti

È possibile elencare i controller vCenter esistenti registrati con il nodo di gestione e visualizzare le informazioni memorizzate utilizzando l'API REST.

Fasi

1. Fare clic su **GET /compute/controller**.
2. Fare clic su **Provalo**.
3. Fare clic su **Execute** (Esegui).

   L'API restituisce un elenco di tutti i controller vCenter conosciuti, insieme all'indirizzo IP, all'ID del controller, al nome host e all'ID utente utilizzati per comunicare con ciascun controller.

4. Se si desidera lo stato di connessione di un controller specifico, copiare l'ID del controller da `id` del controller negli appunti e vedere Visualizzare lo stato di un controller esistente.

Visualizzare lo stato di un controller esistente

È possibile visualizzare lo stato di uno dei controller vCenter esistenti registrati con il nodo di gestione. L'API restituisce uno stato che indica se NetApp Hybrid Cloud Control è in grado di connettersi al controller vCenter e il motivo di tale stato.

Fasi

1. Fare clic su **GET /compute/controllers/{controller_id}/status**.
2. Fare clic su **Provalo**.
3. Inserire l'ID controller copiato in precedenza in `controller_id` parametro.
4. Fare clic su **Execute** (Esegui).

   L'API restituisce uno stato di questo particolare controller vCenter, insieme a un motivo per tale stato.

Modificare le proprietà memorizzate di un controller

È possibile modificare il nome utente o la password memorizzati per qualsiasi controller vCenter esistente registrato con il nodo di gestione. Non è possibile modificare l'indirizzo IP memorizzato di un controller vCenter esistente.

Fasi

1. Fare clic su **PUT /compute/controllers/{controller_id}**.
2. Inserire l'ID del controller di un controller vCenter in `controller_id` parametro.
3. Fare clic su **Provalo**.
4. Modificare uno dei seguenti parametri nel campo **corpo della richiesta**:

Parametro	Tipo	Descrizione
`userId`	stringa	Modificare l'ID utente utilizzato per comunicare con il controller vCenter (l'utente deve disporre dei privilegi di amministratore).
`password`	stringa	Modificare la password utilizzata per comunicare con il controller vCenter.

5. Fare clic su **Execute** (Esegui).

   L'API restituisce informazioni aggiornate sul controller.

Trova ulteriori informazioni

- "Aggiungere risorse di calcolo e controller al nodo di gestione"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Rimuovere una risorsa dal nodo di gestione

Se si sostituisce fisicamente un nodo di calcolo o si desidera rimuoverlo dal cluster

NetApp HCI, è necessario rimuovere la risorsa del nodo di calcolo utilizzando le API del nodo di gestione.

Di cosa hai bisogno

- Il cluster di storage esegue il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione con versione 11.3 o successiva.

Fasi

1. Inserire l'indirizzo IP del nodo di gestione seguito da `/mnode/1/`:

   ```
   https://<ManagementNodeIP>/mnode/1/
   ```

2. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e immettere le credenziali di amministratore del cluster per le autorizzazioni per l'utilizzo delle API.
   a. Inserire il nome utente e la password del cluster.
   b. Selezionare **corpo richiesta** dall'elenco a discesa tipo se il valore non è già selezionato.
   c. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
   d. Non inserire un valore per il client secret.
   e. Fare clic su **autorizzare** per avviare una sessione.
   f. Chiudere la finestra.
3. Chiudere la finestra di dialogo **Available Authorisations** (autorizzazioni disponibili).
4. Fare clic su **GET/Assets**.
5. Fare clic su **Provalo**.
6. Fare clic su **Execute** (Esegui).
7. Scorrere verso il basso nel corpo della risposta fino alla sezione **calcolo** e copiare `parent` e. `id` valori per il nodo di calcolo guasto.
8. Fare clic su **DELETE/assets/{asset_id}/compute-nodes/{compute_id}**.
9. Fare clic su **Provalo**.
10. Inserire il `parent` e. `id` valori copiati in un passaggio precedente.
11. Fare clic su **Execute** (Esegui).

Configurare un server proxy

Se il cluster si trova dietro un server proxy, è necessario configurare le impostazioni del proxy in modo da poter accedere a una rete pubblica.

Un server proxy viene utilizzato per i servizi di raccolta di telemetria e le connessioni di reverse tunnel. È possibile attivare e configurare un server proxy utilizzando l'interfaccia utente API REST se non è già stato configurato un server proxy durante l'installazione o l'aggiornamento. È inoltre possibile modificare le impostazioni del server proxy esistente o disattivare un server proxy.

Il comando per configurare un server proxy viene aggiornato e restituisce le impostazioni proxy correnti per il nodo di gestione. Le impostazioni proxy vengono utilizzate da Active IQ, il servizio di monitoraggio NetApp HCI implementato dal motore di implementazione NetApp e da altre utility software Element installate nel nodo di

gestione, incluso il tunnel di supporto inverso per il supporto NetApp.

Prima di iniziare

- È necessario conoscere le informazioni relative all'host e alle credenziali per il server proxy che si sta configurando.
- Assicurarsi che la versione del cluster in uso utilizzi il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver implementato un nodo di gestione con versione 11.3 o successiva.
- (Nodo di gestione 12.0 e versioni successive) hai aggiornato NetApp Hybrid Cloud Control alla versione 2.16 dei servizi di gestione prima di configurare un server proxy.

Fasi

1. Accedere all'interfaccia utente API REST sul nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode`:

   ```
   https://<ManagementNodeIP>/mnode
   ```

2. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Fare clic su **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Fare clic su **PUT /settings**.
4. Fare clic su **Provalo**.
5. Per attivare un server proxy, è necessario impostare `use_proxy` a vero. Immettere l'IP o il nome host e le destinazioni della porta proxy.

   Il nome utente del proxy, la password del proxy e la porta SSH sono opzionali e devono essere omessi se non utilizzati.

   ```
   {
   "proxy_ip_or_hostname": "[IP or name]",
   "use_proxy": [true/false],
   "proxy_username": "[username]",
   "proxy_password": "[password]",
   "proxy_port": [port value],
   "proxy_ssh_port": [port value: default is 443]
   }
   ```

6. Fare clic su **Execute** (Esegui).

   Potrebbe essere necessario riavviare il nodo di gestione a seconda dell'ambiente in uso.

Trova ulteriori informazioni

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

Verificare le versioni dei sistemi operativi e dei servizi del nodo di gestione

È possibile verificare i numeri di versione del sistema operativo del nodo di gestione, del bundle di servizi di gestione e dei singoli servizi in esecuzione sul nodo di gestione utilizzando l'API REST nel nodo di gestione.

Di cosa hai bisogno

- Nel cluster è in esecuzione il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione con versione 11.3 o successiva.

Opzioni

- Comandi API
- FASI DELL'INTERFACCIA UTENTE API REST

Comandi API

- Ottenere informazioni sulla versione del sistema operativo del nodo di gestione, del bundle di servizi di gestione e del servizio API del nodo di gestione (mnode-api) in esecuzione sul nodo di gestione:

```
curl -X GET "https://<ManagementNodeIP>/mnode/about" -H  "accept:
application/json"
```

- Ottenere informazioni sulla versione dei singoli servizi in esecuzione sul nodo di gestione:

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running"
-H  "accept: */*" -H  "Authorization: Bearer ${TOKEN}"
```

> Puoi trovare il portatore `${TOKEN}` Utilizzato dal comando API quando si "autorizzare". Il portatore `${TOKEN}` è nella risposta di arricciamento.

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Effettuare una delle seguenti operazioni:
   - Ottenere informazioni sulla versione del sistema operativo del nodo di gestione, del bundle di servizi di gestione e del servizio API del nodo di gestione (mnode-api) in esecuzione sul nodo di gestione:
     i. Selezionare **GET /About**.

ii. Selezionare **Provalo**.

iii. Selezionare **Esegui**.

La versione del bundle dei servizi di gestione (`"mnode_bundle_version"`), versione del sistema operativo del nodo di gestione (`"os_version"`) E la versione API del nodo di gestione (`"version"`) sono indicati nel corpo di risposta.

- Ottenere informazioni sulla versione dei singoli servizi in esecuzione sul nodo di gestione:

  i. Selezionare **GET /Services**.

  ii. Selezionare **Provalo**.

  iii. Selezionare lo stato **in esecuzione**.

  iv. Selezionare **Esegui**.

  I servizi in esecuzione sul nodo di gestione sono indicati nel corpo della risposta.

Trova ulteriori informazioni

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

Recupero dei log dai servizi di gestione

È possibile recuperare i log dai servizi in esecuzione sul nodo di gestione utilizzando l'API REST. È possibile estrarre i log da tutti i servizi pubblici o specificare servizi specifici e utilizzare i parametri di query per definire meglio i risultati restituiti.

Di cosa hai bisogno

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione con versione 11.3 o successiva.

Fasi

1. Aprire l'interfaccia utente API REST sul nodo di gestione.
   - A partire dai servizi di gestione 2.21.61:

     ```
     https://<ManagementNodeIP>/mnode/4/
     ```

   - Per i servizi di gestione 2.20.69 o precedenti:

     ```
     https://<ManagementNodeIP>/mnode
     ```

2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Inserire l'ID client come mnode-client se il valore non è già stato compilato.
   c. Selezionare **autorizzare** per avviare una sessione.

d. Chiudere la finestra.

3. Selezionare **GET /logs**.
4. Selezionare **Provalo**.
5. Specificare i seguenti parametri:
   - `Lines`: Inserire il numero di righe che si desidera restituire al registro. Questo parametro è un numero intero che per impostazione predefinita è 1000.

     Evitare di richiedere l'intera cronologia del contenuto del registro impostando le righe su 0.

   - `since`: Aggiunge un timestamp ISO-8601 per il punto di inizio dei registri del servizio.

     Utilizzare un ragionevole `since` parametro durante la raccolta di log di intervalli di tempo più ampi.

   - `service-name`: Inserire un nome di servizio.

     Utilizzare `GET /services` comando per elencare i servizi sul nodo di gestione.

   - `stopped`: Impostare su `true` per recuperare i log dai servizi interrotti.
6. Selezionare **Esegui**.
7. Dal corpo della risposta, selezionare **Download** per salvare l'output del log.

Ulteriori informazioni

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

Gestire le connessioni di supporto

Avviare una sessione remota di NetApp Support

Se hai bisogno di supporto tecnico per il tuo sistema NetApp HCI, il supporto NetApp può connetterti in remoto con il tuo sistema. Per avviare una sessione e ottenere l'accesso remoto, il supporto NetApp può aprire una connessione Secure Shell (SSH) inversa al proprio ambiente.

Con il supporto NetApp è possibile aprire una porta TCP per una connessione a tunnel inverso SSH. Questa connessione consente al supporto NetApp di accedere al nodo di gestione.

Prima di iniziare

- Per i servizi di gestione 2.18 e versioni successive, la funzionalità di accesso remoto è disattivata per impostazione predefinita nel nodo di gestione. Per attivare la funzionalità di accesso remoto, vedere "Gestire la funzionalità SSH sul nodo di gestione".
- Se il nodo di gestione si trova dietro un server proxy, nel file sshd.config sono necessarie le seguenti porte TCP:

Porta TCP	Descrizione	Direzione di connessione
443	Chiamate API/HTTPS per l'inoltro inverso delle porte all'interfaccia utente Web tramite tunnel di supporto aperto	Nodo di gestione ai nodi di storage
22	Accesso SSH	Nodo di gestione per nodi di storage o da nodi di storage a nodi di gestione

Fasi

- Accedere al nodo di gestione e aprire una sessione terminale.
- Quando richiesto, immettere quanto segue:

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- Per chiudere il tunnel di supporto remoto, immettere quanto segue:

```
rst --killall
```

- (Facoltativo) Disattiva "funzionalità di accesso remoto" di nuovo.

> SSH rimane attivato se non viene disattivato. La configurazione abilitata SSH persiste sul nodo di gestione tramite aggiornamenti e aggiornamenti fino a quando non viene disattivata manualmente.

Trova ulteriori informazioni

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

Gestire la funzionalità SSH sul nodo di gestione

È possibile disattivare, riattivare o determinare lo stato della funzionalità SSH sul nodo di gestione (mNode) utilizzando l'API REST. Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive.

A partire da Management Services 2.20.69, è possibile attivare e disattivare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.

Di cosa hai bisogno

- **NetApp Hybrid Cloud Control Permissions**: Hai le autorizzazioni di amministratore.
- **Cluster Administrator permissions** (autorizzazioni amministratore cluster): Si dispone delle autorizzazioni di amministratore per il cluster di storage.
- **Software Element**: Il cluster esegue il software NetApp Element 11.3 o versione successiva.
- **Nodo di gestione**: È stato implementato un nodo di gestione con versione 11.3 o successiva.

- **Aggiornamenti dei servizi di gestione**:
  - Per utilizzare l'interfaccia utente di NetApp Hybrid Cloud Control, è stato aggiornato il "bundle di servizi di gestione" alla versione 2.20.69 o successiva.
  - Per utilizzare l'interfaccia utente API REST, è stato aggiornato il "bundle di servizi di gestione" alla versione 2.17.

Opzioni

- Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control

Dopo di che, è possibile eseguire una delle seguenti attività "autenticare":

- Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando le API
- Determinare lo stato della funzionalità SSH sul nodo di gestione utilizzando le API

Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control

È possibile disattivare o riattivare la funzionalità SSH sul nodo di gestione. Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive. La disattivazione di SSH non interrompe o disconnette le sessioni client SSH esistenti al nodo di gestione. Se si disattiva SSH e si sceglie di riattivarlo in un secondo momento, è possibile farlo utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.

> Per attivare o disattivare l'accesso al supporto utilizzando SSH per un cluster di storage, è necessario utilizzare "Pagina delle impostazioni del cluster dell'interfaccia utente Element".

Fasi

1. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
2. Nella schermata **Support Access for Management Node** (accesso supporto per nodo di gestione), attivare lo switch per attivare il nodo di gestione SSH.
3. Una volta completata la risoluzione dei problemi, nella schermata **Support Access for Management Node** (accesso supporto per nodo di gestione), impostare lo switch su Disable Management Node SSH (Disattiva SSH nodo di gestione).

Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando le API

È possibile disattivare o riattivare la funzionalità SSH sul nodo di gestione. Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive. La disattivazione di SSH non interrompe o disconnette le sessioni client SSH esistenti al nodo di gestione. Se si disattiva SSH e si sceglie di riattivarlo in un secondo momento, è possibile utilizzare la stessa API.

Comando API

Per i servizi di gestione 2.18 o versioni successive:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Per i servizi di gestione 2.17 o precedenti:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Puoi trovare il portatore `${TOKEN}` Utilizzato dal comando API quando si "autorizzare". Il portatore `${TOKEN}` è nella risposta di arricciamento.

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio API del nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/`:

   ```
   https://<ManagementNodeIP>/mnode/
   ```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Dall'interfaccia utente API REST, selezionare **PUT /settings/ssh**.
   a. Fare clic su **Provalo**.
   b. Impostare il parametro **enabled** su `false` Per disattivare SSH o. `true` Per riattivare la funzionalità SSH precedentemente disattivata.
   c. Fare clic su **Execute** (Esegui).

Determinare lo stato della funzionalità SSH sul nodo di gestione utilizzando le API

È possibile determinare se la funzionalità SSH è attivata sul nodo di gestione utilizzando un'API di servizio del nodo di gestione. SSH è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive.

Comando API

Per i servizi di gestione 2.18 o versioni successive:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Per i servizi di gestione 2.17 o precedenti:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Puoi trovare il portatore `${TOKEN}` Utilizzato dal comando API quando si "autorizzare". Il portatore `${TOKEN}` è nella risposta di arricciamento.

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio API del nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/`:

   ```
   https://<ManagementNodeIP>/mnode/
   ```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Dall'interfaccia utente API REST, selezionare **GET /settings/ssh**.
   a. Fare clic su **Provalo**.
   b. Fare clic su **Execute** (Esegui).

Trova ulteriori informazioni

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

Spegnere e riaccendere il sistema NetApp HCI

Accensione e spegnimento del sistema NetApp HCI

È possibile spegnere o accendere il sistema NetApp HCI se si verifica un'interruzione pianificata, se è necessario eseguire la manutenzione dell'hardware o se è necessario espandere il sistema. Utilizzare le seguenti operazioni per spegnere o accendere il sistema NetApp HCI secondo necessità.

Potrebbe essere necessario spegnere il sistema NetApp HCI in diverse circostanze, ad esempio:

- Interruzioni pianificate
- Sostituzioni delle ventole dello chassis
- Aggiornamenti del firmware
- Espansione dello storage o delle risorse di calcolo

Di seguito viene riportata una panoramica delle attività da completare per spegnere un sistema NetApp HCI:

- Spegnere tutte le macchine virtuali, ad eccezione del server VMware vCenter (vCSA).
- Spegnere tutti i server ESXi ad eccezione di quello che ospita vCSA.
- Spegnere vCSA.
- Spegnere il sistema storage NetApp HCI.

Di seguito viene riportata una panoramica delle attività da completare per accendere un sistema NetApp HCI:

- Accendere tutti i nodi di storage fisici.
- Accendere tutti i nodi di calcolo fisici.
- Accendere vCSA.
- Verificare il sistema e accendere altre macchine virtuali.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Spegnere le risorse di calcolo per un sistema NetApp HCI

Per spegnere le risorse di calcolo NetApp HCI, è necessario spegnere i singoli host VMware ESXi e l'appliance server VMware vCenter in un determinato ordine.

Fasi

1. Accedere all'istanza di vCenter che controlla il sistema NetApp HCI e determinare la macchina ESXi che ospita l'appliance virtuale vCenter Server (vCSA).
2. Dopo aver determinato l'host ESXi che esegue vCSA, spegnere tutte le altre macchine virtuali diverse da vCSA come segue:
   a. Selezionare una macchina virtuale.
   b. Fare clic con il pulsante destro del mouse e selezionare **alimentazione > Arresta il sistema operativo guest**.
3. Spegnere tutti gli host ESXi che non sono l'host ESXi che esegue vCSA.
4. Spegnere vCSA.

   In questo modo, la sessione vCenter si interrompe perché vCSA si disconnette durante il processo di spegnimento. Tutte le macchine virtuali devono ora essere spese con un solo host ESXi acceso.

5. Accedere all'host ESXi in esecuzione.
6. Verificare che tutte le macchine virtuali sull'host siano spente.

7. Arrestare l'host ESXi.

   In questo modo, tutte le sessioni iSCSI aperte al cluster di storage NetApp HCI vengono disconnesse.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Spegnere le risorse di storage per un sistema NetApp HCI

Quando si spengono le risorse di storage per NetApp HCI, è necessario utilizzare `Shutdown` Metodo API Element per arrestare correttamente i nodi di storage.

Fasi

Dopo aver spento le risorse di calcolo, utilizzare un browser Web per chiudere tutti i nodi del cluster di storage NetApp HCI.

1. Accedere al cluster di storage e verificare di essere connessi all'MVIP corretto.
2. (Facoltativo) verificare che tutte le operazioni di i/o degli host siano state interrotte:
   a. Interrompere l'i/o dal lato host utilizzando i comandi appropriati per uno o più hypervisor in uso.
   b. Nell'interfaccia utente del cluster, selezionare **Reporting** > **Overview**. Non dovrebbe essere presente alcuna attività nel grafico "Cluster Input/Output" (Input/Output cluster).
   c. Una volta interrotte tutte le operazioni di i/o, attendere 20 minuti prima di spegnere il cluster.
3. Verificare che il numero di sessioni iSCSI sia pari a zero.
4. Accedere a **Cluster > Nodes > Active** (cluster > nodi > attivo) e registrare gli ID dei nodi per tutti i nodi attivi nel cluster.
5. Per spegnere il cluster di storage NetApp HCI, aprire un browser Web e utilizzare il seguente URL per richiamare la procedura di spegnimento e arresto, dove `{MVIP}` È l'indirizzo IP di gestione del sistema di storage NetApp HCI e di `nodes=[]` L'array include gli ID dei nodi registrati al punto 4. Ad esempio:

   ```
   https://{MVIP}/json-rpc/1.0?method=Shutdown&nodes=[1,2,3,4]&option=halt
   ```

   > È possibile eseguire il comando in una finestra in incognito per evitare di eseguirlo nuovamente in una fase successiva dall'URL salvato.

6. Inserire il nome utente e la password dell'amministratore del cluster.
7. Verificare che la chiamata API sia stata restituita correttamente verificando che tutti i nodi del cluster di storage siano inclusi in `successful` Del risultato API.

   Tutti i nodi di storage NetApp HCI sono stati spenti correttamente.

8. Chiudere il browser o la scheda per evitare di selezionare il pulsante "Indietro" e ripetere la chiamata API.

Quando si riavvia il cluster, è necessario seguire alcuni passaggi per verificare che tutti i nodi siano in linea:

1. Verificare che tutti i livelli critici di severità e. `volumesOffline` i guasti del cluster sono stati risolti.
2. Attendere da 10 a 15 minuti per consentire al cluster di stabilizzarsi.
3. Avviare la creazione degli host per accedere ai dati.

Se si desidera dedicare più tempo all'accensione dei nodi e alla verifica dell'integrità dei nodi dopo la manutenzione, contattare il supporto tecnico per ricevere assistenza con il ritardo della sincronizzazione dei dati per evitare una sincronizzazione bin non necessaria.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Accendere le risorse di storage per un sistema NetApp HCI

È possibile accendere NetApp HCI una volta completata l'interruzione pianificata.

Fasi

1. Accendere tutti i nodi di storage utilizzando il pulsante di accensione fisico o BMC.
2. Se si utilizza BMC, accedere a ciascun nodo e selezionare **Remote Control > Power Control > Power on Server**.
3. Quando tutti i nodi di storage sono online, accedere al sistema di storage NetApp HCI e verificare che tutti i nodi siano operativi.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Accendere le risorse di calcolo per un sistema NetApp HCI

È possibile accendere le risorse di calcolo per un sistema NetApp HCI una volta completata l'interruzione pianificata.

Fasi

1. Accendere i nodi di calcolo seguendo le stesse procedure eseguite per l'accensione dei nodi di storage.
2. Quando tutti i nodi di calcolo sono operativi, accedere all'host ESXi che esegue vCSA.
3. Accedere all'host di calcolo e verificare che siano presenti tutti gli archivi dati NetApp HCI. Per un sistema NetApp HCI tipico, è necessario visualizzare tutti gli archivi dati locali ESXi e almeno i seguenti archivi dati condivisi:

```
NetApp-HCI-Datastore-[01,02]
```

1. Supponendo che tutto lo storage sia accessibile, accendere vCSA e tutte le altre macchine virtuali richieste come segue:
   a. Selezionare le macchine virtuali nel navigatore, selezionare tutte le macchine virtuali che si desidera accendere e fare clic sul pulsante **Power on** (accensione).
2. Dopo aver acceso le macchine virtuali, attendere circa 5 minuti, quindi utilizzare un browser Web per accedere all'indirizzo IP o all'FQDN dell'applicazione vCSA.

   Se non si attende abbastanza a lungo, viene visualizzato un messaggio che indica che il server Web del client vSphere è in fase di inizializzazione.

3. Dopo l'inizializzazione del client vSphere, accedere e verificare che tutti gli host ESXi e le macchine virtuali siano online.

Trova ulteriori informazioni

- "Versioni del firmware e dei driver ESXi supportate per NetApp HCI e versioni del firmware per i nodi di storage NetApp HCI"

Monitorate il vostro sistema NetApp HCI con il controllo del cloud ibrido NetApp

Monitorate le risorse di storage e di calcolo sulla dashboard di controllo del cloud ibrido

Con la dashboard di controllo del cloud ibrido di NetApp, puoi visualizzare tutte le risorse di storage e di calcolo in un colpo d'occhio. Inoltre, è possibile monitorare la capacità dello storage, le performance dello storage e l'utilizzo del calcolo.

> Quando avvii una nuova sessione di NetApp Hybrid Cloud Control per la prima volta, potrebbe verificarsi un ritardo nel caricamento della vista di NetApp Hybrid Cloud Control Dashboard quando il nodo di gestione gestisce molti cluster. Il tempo di caricamento varia in base al numero di cluster gestiti attivamente dal nodo di gestione. Per i lanci successivi, si verificheranno tempi di caricamento più rapidi.

Solo i nodi di calcolo gestiti e i cluster con almeno un nodo gestito nell'hardware serie H vengono visualizzati sul dashboard di controllo del cloud ibrido.

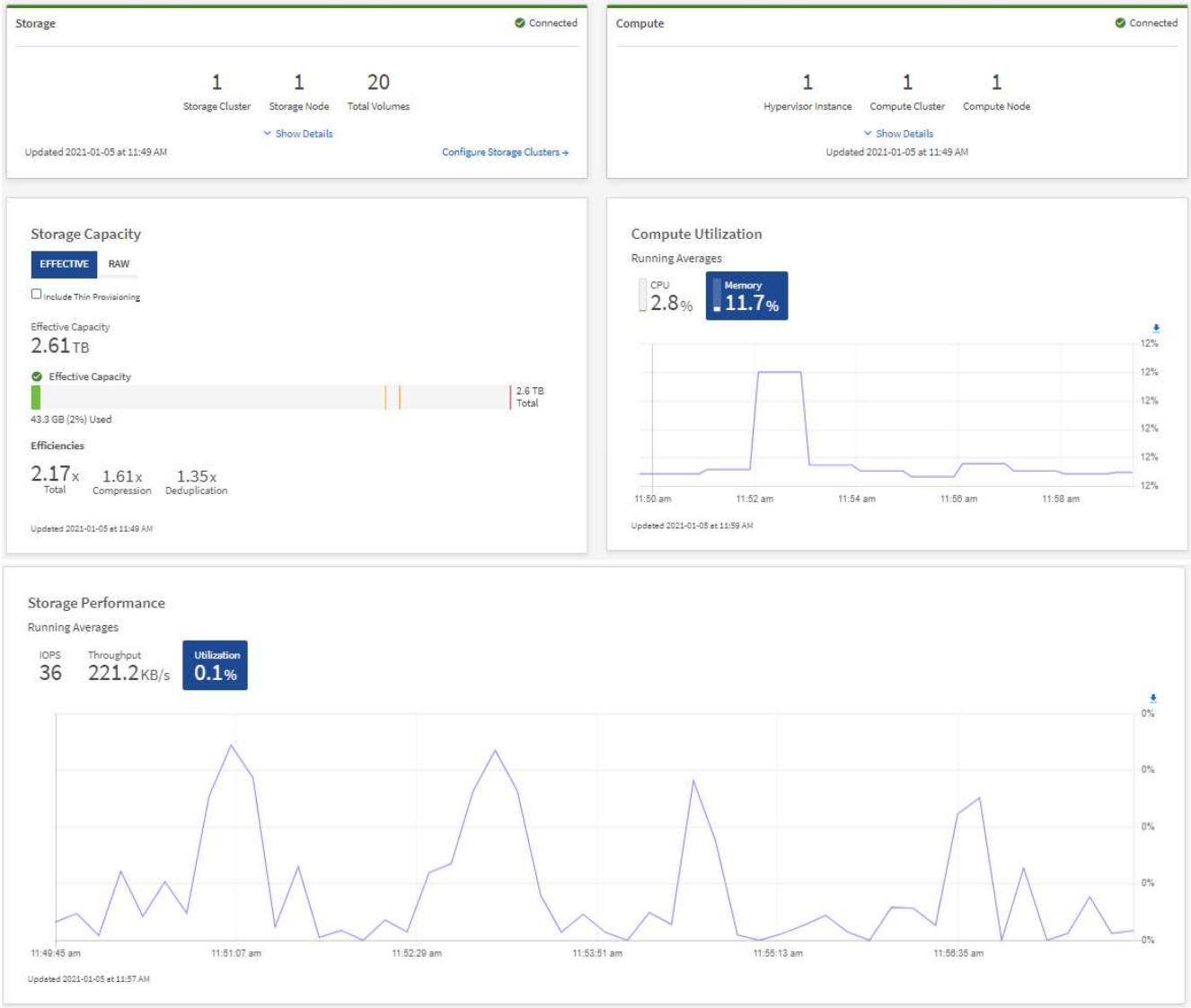
- Accedere al dashboard di NetApp HCC
- Monitorare le risorse di storage
- Monitorare le risorse di calcolo
- Monitorare la capacità dello storage
- Monitorare le performance dello storage
- Monitorare l'utilizzo del calcolo

Accedere al dashboard di NetApp HCC

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Visualizza la dashboard di controllo del cloud ibrido.

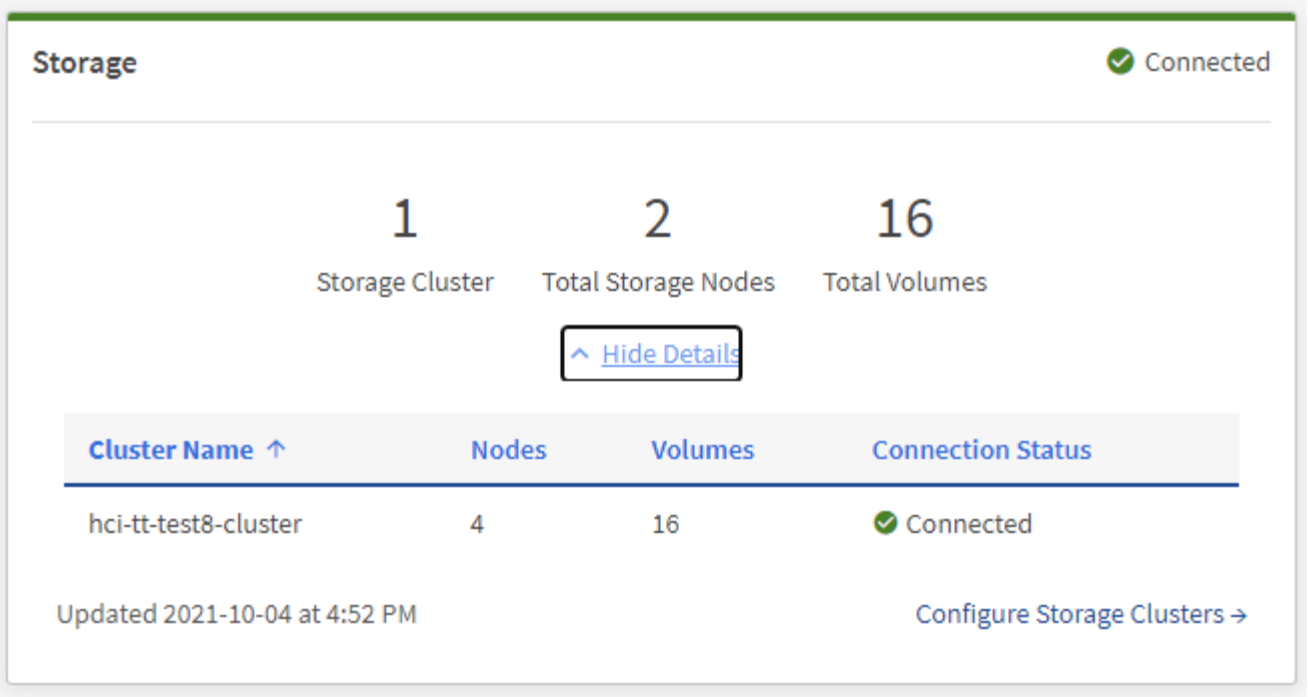


A seconda dell'installazione, potrebbero essere visualizzati alcuni o tutti questi riquadri. Ad esempio, per le installazioni solo storage, la dashboard di controllo del cloud ibrido mostra solo il riquadro Storage, il riquadro Storage Capacity e il riquadro Storage Performance.

Monitorare le risorse di storage

Utilizzare il riquadro **Storage** per visualizzare l'intero ambiente di storage. È possibile monitorare il numero di cluster di storage, nodi di storage e volumi totali.

Per visualizzare i dettagli, nel riquadro Storage (archiviazione), selezionare **Show Details** (Mostra dettagli).



Il numero dei nodi di storage totali non include i nodi di controllo dei cluster di storage a due nodi. I nodi di controllo sono inclusi nel numero dei nodi nella sezione dei dettagli del cluster.

Per visualizzare i dati più recenti del cluster di storage, utilizzare la pagina Storage Clusters, in cui il polling viene eseguito con maggiore frequenza rispetto alla dashboard.

Monitorare le risorse di calcolo

Utilizza il riquadro **Compute** per visualizzare il tuo ambiente di calcolo NetApp H-Series. È possibile monitorare il numero di cluster di calcolo e i nodi di calcolo totali.

Per visualizzare i dettagli, nei riquadri calcolo, selezionare **Mostra dettagli**.

Le istanze di vCenter vengono visualizzate nel riquadro di calcolo solo quando almeno un nodo di calcolo NetApp HCI è associato a tale istanza. Per elencare le istanze di vCenter collegate in NetApp Hybrid Cloud Control, è possibile utilizzare "API".

Per gestire un nodo di calcolo in NetApp Hybrid Cloud Control, è necessario "Aggiungere il nodo di calcolo a un cluster host vCenter".

Monitorare la capacità dello storage

Il monitoraggio della capacità di storage del tuo ambiente è fondamentale. Il riquadro Storage Capacity (capacità storage) consente di determinare i vantaggi in termini di efficienza della capacità dello storage con o senza funzionalità di compressione, deduplica e thin provisioning abilitate.

È possibile visualizzare lo spazio fisico di storage totale disponibile nel cluster nella scheda **RAW** e le informazioni sullo storage fornito nella scheda **EFFETTIVO**.

Per visualizzare lo stato del cluster, consultare anche la dashboard di SolidFire Active IQ. Vedere "Monitorate performance, capacità e stato dei cluster in NetApp SolidFire Active IQ".

Fasi

1. Selezionare la scheda **RAW** per visualizzare lo spazio di storage fisico totale utilizzato e disponibile nel cluster.

   Esaminare le linee verticali per determinare se la capacità utilizzata è inferiore al totale o inferiore alle soglie di avviso, errore o critico. Passare il mouse sulle linee per visualizzare i dettagli.

   È possibile impostare la soglia di avviso, che per impostazione predefinita è inferiore del 3% alla soglia di errore. Le soglie di errore e critico sono preimpostate e non configurabili in base alla progettazione. La soglia di errore indica che nel cluster rimane meno di un nodo di capacità. Per informazioni sull'impostazione della soglia, vedere "Impostazione della soglia cluster full".

   Per ulteriori informazioni sull'API degli elementi delle soglie del cluster correlati, vedere ""GetClusterFullThreshold"" Nella *documentazione API del software Element*. Per ulteriori informazioni sulla capacità di blocchi e metadati, vedere "Comprensione dei livelli di completezza del cluster" Nella *documentazione software Element*.

2. Selezionare la scheda **EFFETTIVO** per visualizzare le informazioni sullo storage totale fornito agli host connessi e le valutazioni di efficienza.
   a. Facoltativamente, selezionare **Includi thin provisioning** per visualizzare i tassi di efficienza del thin provisioning nel grafico a barre capacità effettiva.
   b. **Grafico a barre capacità effettiva**: Esaminare le linee verticali per determinare se la capacità utilizzata è inferiore al totale o inferiore alle soglie di avviso, errore o critico. Analogamente alla scheda Raw, è possibile passare il mouse sulle linee verticali per visualizzare i dettagli.
   c. **Efficienze**: Guarda queste valutazioni per determinare i tuoi guadagni in termini di efficienza della capacità dello storage con le funzionalità di compressione, deduplica e thin provisioning abilitate. Ad esempio, se la compressione viene visualizzata come "1.3x", significa che l'efficienza dello storage con compressione abilitata è 1.3 volte più efficiente che senza di essa.

> Efficienze totali pari a (fattore di efficienza maxUsedSpace *) / 2, dove EfficiencyFactor = (thinProvisioningFactor * deDuplicationFactor * compressionFactor). Quando il thin provisioning non è selezionato, non viene incluso nel Total Efficiency.

d. Se la capacità di storage effettiva si avvicina a una soglia di errore o critica, considerare l'eliminazione dei dati nel sistema. In alternativa, è possibile espandere il sistema.

   Vedere "Panoramica dell'espansione".

3. Per ulteriori analisi e contesto storico, vedere "Dettagli di NetApp SolidFire Active IQ".

Monitorare le performance dello storage

È possibile osservare la quantità di IOPS o di throughput che è possibile ottenere da un cluster senza superare le utili performance di tale risorsa utilizzando il riquadro Storage Performance (prestazioni dello storage). Le performance dello storage sono il punto in cui si ottiene il massimo utilizzo prima che la latenza diventi un problema.

Il pannello delle performance dello storage ti aiuta a identificare se le performance stanno raggiungendo il punto in cui le performance potrebbero degradarsi se i carichi di lavoro aumentano.

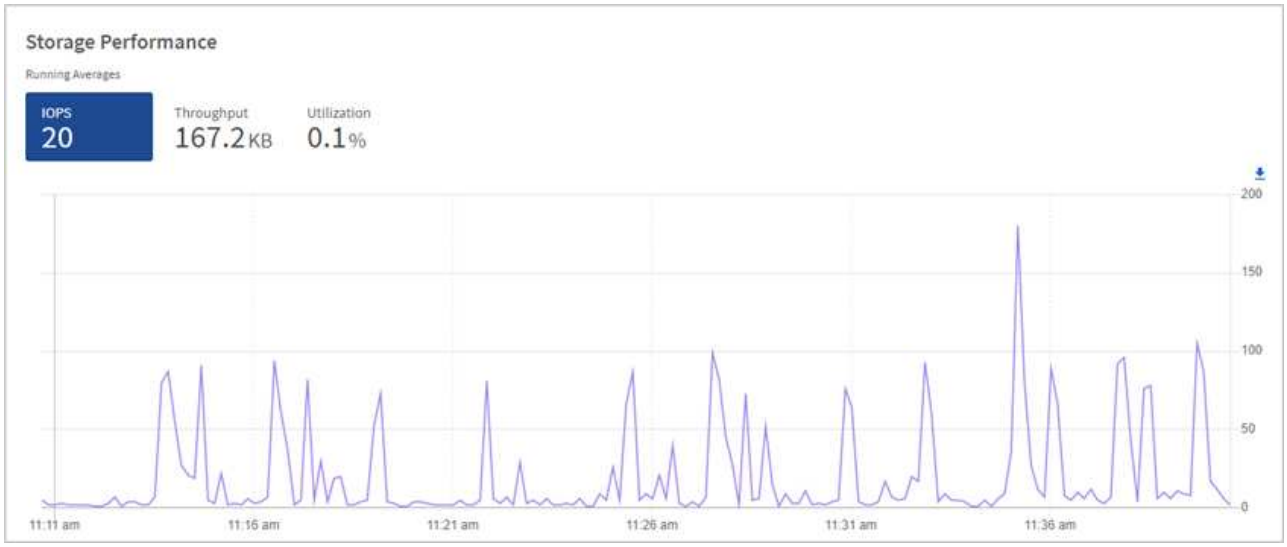
Le informazioni di questo riquadro vengono aggiornate ogni 10 secondi e vengono visualizzate in media tutti i punti del grafico.

Per ulteriori informazioni sul metodo API Element associato, vedere "GetClusterStats" Metodo nella *documentazione API del software Element*.

Fasi

1. Visualizzare il riquadro Storage Performance (prestazioni storage). Per i dettagli, passare il mouse sui punti del grafico.

   a. Scheda **IOPS**: Visualizza le operazioni correnti al secondo. Cerca tendenze in termini di dati o picchi. Ad esempio, se si nota che il numero massimo di IOPS è pari a 160.000 e 100.000 di IOPS gratuiti o disponibili, si potrebbe prendere in considerazione l'aggiunta di più carichi di lavoro a questo cluster. D'altra parte, se si vede che sono disponibili solo 140K, si potrebbe prendere in considerazione l'offload dei carichi di lavoro o l'espansione del sistema.



   b. Scheda **throughput**: Monitorare gli schemi o i picchi di throughput. Inoltre, è possibile monitorare i

valori di throughput costantemente elevati, che potrebbero indicare che si stanno avvicinando alle massime prestazioni utili della risorsa.

c. Scheda **Utilization** (utilizzo): Consente di monitorare l'utilizzo degli IOPS in relazione al totale degli IOPS disponibili sommato a livello di cluster.

2. Per ulteriori analisi, esaminare le performance dello storage utilizzando il plug-in NetApp Element per vCenter Server.

   "Le performance mostrate nel plug-in NetApp Element per vCenter Server".

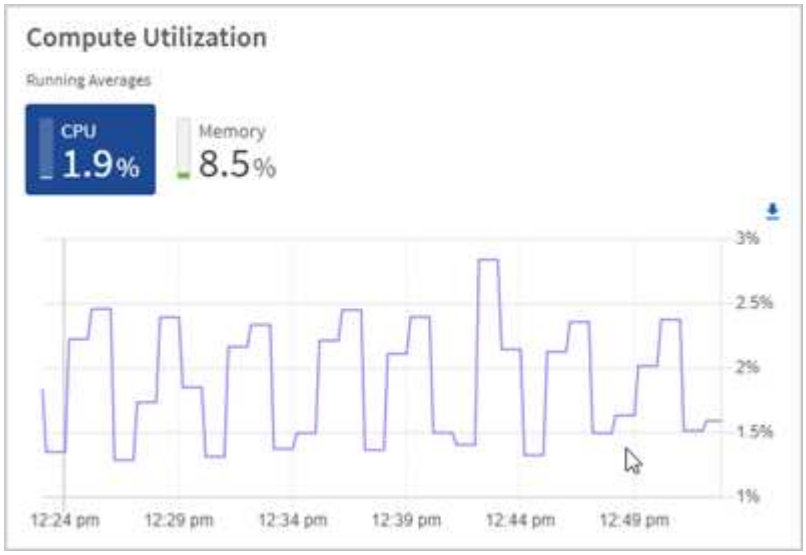
Monitorare l'utilizzo del calcolo

Oltre al monitoraggio degli IOPS e del throughput delle risorse di storage, è possibile visualizzare l'utilizzo della CPU e della memoria delle risorse di calcolo. Gli IOPS totali che un nodo può fornire si basano sulle caratteristiche fisiche del nodo, ad esempio il numero di CPU, la velocità della CPU e la quantità di RAM.

Fasi

1. Visualizzare il riquadro **Compute Utilization** (utilizzo calcolo). Utilizzando le schede CPU e memoria, cercare modelli o picchi di utilizzo. Inoltre, è necessario verificare un utilizzo costantemente elevato, a indicare che si sta avvicinando all'utilizzo massimo per i cluster di calcolo.

Questo pannello mostra i dati solo per i cluster di calcolo gestiti da questa installazione.



a. Scheda **CPU**: Visualizza la media corrente dell'utilizzo della CPU nel cluster di calcolo.
b. Scheda **Memory** (memoria): Consente di visualizzare l'utilizzo medio corrente della memoria nel cluster di calcolo.

2. Per ulteriori analisi sulle informazioni di calcolo, vedere "NetApp SolidFire Active IQ per i dati storici".

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"
- "Documentazione di NetApp SolidFire Active IQ"

Visualizzare l'inventario nella pagina nodi

È possibile visualizzare le risorse di storage e di calcolo nel sistema e determinare gli indirizzi IP, i nomi e le versioni software.

È possibile visualizzare le informazioni di storage per i sistemi a più nodi e qualsiasi nodo di controllo NetApp HCI associato a cluster a due o tre nodi. Se "domini di protezione personalizzati" è possibile visualizzare i domini di protezione assegnati a nodi specifici.

I nodi di controllo gestiscono il quorum all'interno del cluster e non vengono utilizzati per lo storage. I nodi di controllo sono applicabili solo a NetApp HCI e non agli ambienti di storage all-flash.

Per ulteriori informazioni sui nodi di controllo, vedere "Definizioni dei nodi".

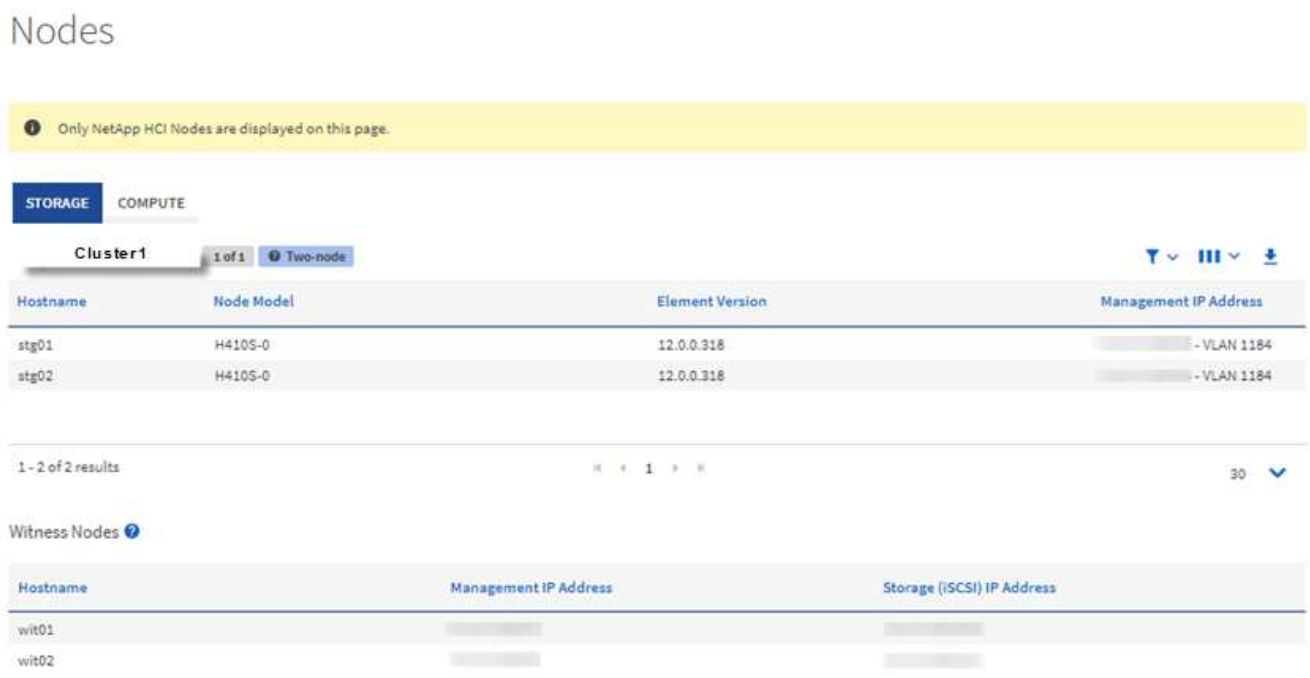
Per i nodi SDS aziendali SolidFire, è possibile monitorare l'inventario nella scheda Storage.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

```
https://<ManagementNodeIP>
```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Nella barra di navigazione a sinistra, fare clic su **Nodes** (nodi).



> Quando avvii una nuova sessione di NetApp Hybrid Cloud Control per la prima volta, potrebbe verificarsi un ritardo nel caricamento della pagina dei nodi di NetApp Hybrid Cloud Control quando il nodo di gestione gestisce molti cluster. Il tempo di caricamento varia in base al numero di cluster gestiti attivamente dal nodo di gestione. Per i lanci successivi, si verificheranno tempi di caricamento più rapidi.

4. Nella scheda **Storage** della pagina Nodes (nodi), esaminare le seguenti informazioni:
   a. Cluster a due nodi: Nella scheda Storage viene visualizzata un'etichetta a due nodi e vengono elencati i nodi di controllo associati.
   b. Cluster a tre nodi: Vengono elencati i nodi di storage e i nodi di controllo associati. I cluster a tre nodi dispongono di un nodo di controllo implementato in standby per mantenere un'elevata disponibilità in caso di guasto del nodo.
   c. Cluster con quattro o più nodi: Vengono visualizzate le informazioni relative ai cluster con quattro o più nodi. I nodi di controllo non sono applicabili. Se si è iniziato con due o tre nodi di storage e sono stati aggiunti altri nodi, i nodi di controllo continuano a essere visualizzati. In caso contrario, la tabella dei nodi di controllo non viene visualizzata.
   d. Versione del bundle firmware: A partire dalla versione 2.14 dei servizi di gestione, se si utilizzano cluster con Element 12.0 o versione successiva, è possibile visualizzare la versione del bundle firmware per questi cluster. Se i nodi di un cluster hanno versioni firmware diverse, nella colonna **firmware Bundle Version** viene visualizzato **multiple**.
   e. Domini di protezione personalizzati: Se nel cluster sono in uso domini di protezione personalizzati, è possibile visualizzare le assegnazioni dei domini di protezione personalizzati per ciascun nodo del

cluster. Se i domini di protezione personalizzati non sono abilitati, questa colonna non viene visualizzata.

5. Per visualizzare le informazioni sull'inventario di calcolo, fare clic su **Calcola**.
6. È possibile modificare le informazioni presenti in queste pagine in diversi modi:
   a. Per filtrare l'elenco degli elementi nei risultati, fare clic sull'icona **Filter** (filtro) e selezionare i filtri. È anche possibile inserire il testo per il filtro.
   b. Per visualizzare o nascondere le colonne, fare clic sull'icona **Mostra/Nascondi colonne**.
   c. Per scaricare la tabella, fare clic sull'icona **Download**.
   d. Per aggiungere o modificare le credenziali BMC memorizzate per un nodo di calcolo con errori di connessione BMC, fare clic su **Modifica impostazioni di connessione** nel testo del messaggio di errore nella colonna **Stato connessione BMC**. Solo se il tentativo di connessione non riesce per un nodo di calcolo, in questa colonna viene visualizzato un messaggio di errore per quel nodo.

Per visualizzare il numero di risorse di storage e calcolo, consulta la dashboard di NetApp Hybrid Cloud Control (HCC). Vedere "Monitorate le risorse di storage e di calcolo con HCC Dashboard".

Per gestire un nodo di calcolo in NetApp Hybrid Cloud Control, è necessario "Aggiungere il nodo di calcolo a un cluster host vCenter".

Trova ulteriori informazioni

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

Modificare le informazioni di connessione del Baseboard Management Controller

È possibile modificare le credenziali di amministratore di Baseboard Management Controller (BMC) in NetApp Hybrid Cloud Control per ciascuno dei nodi di calcolo. Potrebbe essere necessario modificare le credenziali prima di aggiornare il firmware BMC o per risolvere un `Hardware ID not available` oppure `Unable to Detect` Errore indicato in NetApp Hybrid Cloud Control.

Di cosa hai bisogno

Autorizzazioni di amministratore del cluster per modificare le credenziali BMC.

Se si impostano le credenziali BMC durante un controllo dello stato di salute, può verificarsi un ritardo di 2 minuti prima che la modifica venga riflessa nella pagina **nodi**.

Opzioni

Scegliere una delle seguenti opzioni per modificare le credenziali BMC:

- Utilizza NetApp Hybrid Cloud Control per modificare le informazioni BMC
- Utilizzare l'API REST per modificare le informazioni BMC

Utilizza NetApp Hybrid Cloud Control per modificare le informazioni BMC

È possibile modificare le credenziali BMC memorizzate utilizzando il NetApp Hybrid Cloud Control Dashboard.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Nella casella blu di navigazione a sinistra, selezionare l'installazione di NetApp HCI.

   Viene visualizzata la dashboard NetApp Hybrid Cloud Control.

4. Nella barra di navigazione a sinistra, fare clic su **Nodes** (nodi).
5. Per visualizzare le informazioni sull'inventario di calcolo, fare clic su **Calcola**.

   Viene visualizzato un elenco dei nodi di calcolo. La colonna **BMC Connection Status** mostra il risultato dei tentativi di connessione BMC per ciascun nodo di calcolo. Se il tentativo di connessione non riesce per un nodo di calcolo, in questa colonna viene visualizzato un messaggio di errore per quel nodo.

6. Per aggiungere o modificare le credenziali BMC memorizzate per un nodo di calcolo con errori di connessione BMC, fare clic su **Modifica impostazioni di connessione** nel testo del messaggio di errore.
7. Nella finestra di dialogo visualizzata, aggiungere il nome utente e la password dell'amministratore corretti per il BMC di questo nodo di calcolo.
8. Fare clic su **Save** (Salva).
9. Ripetere i passaggi da 6 a 8 per qualsiasi nodo di calcolo che dispone di credenziali BMC memorizzate mancanti o errate.

> L'aggiornamento delle informazioni BMC aggiorna l'inventario e garantisce che i servizi dei nodi di gestione siano a conoscenza di tutti i parametri hardware necessari per completare l'aggiornamento.

Utilizzare l'API REST per modificare le informazioni BMC

È possibile modificare le credenziali BMC memorizzate utilizzando l'API REST di NetApp Hybrid Cloud Control.

Fasi

1. Individuare il tag hardware del nodo di calcolo e le informazioni BMC:
   a. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Fare clic su **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.

ii. Immettere l'ID client come `mnode-client`.

iii. Fare clic su **autorizzare** per avviare una sessione.

iv. Chiudere la finestra di autorizzazione.

c. Dall'interfaccia utente API REST, fare clic su **GET /Installations**.

d. Fare clic su **Provalo**.

e. Fare clic su **Execute** (Esegui).

f. Dalla risposta, copiare l'ID della risorsa di installazione (`id`).

g. Dall'interfaccia utente API REST, fare clic su **GET /Installations/{id}**.

h. Fare clic su **Provalo**.

i. Incollare l'ID della risorsa di installazione nel campo **id**.

j. Fare clic su **Execute** (Esegui).

k. Dalla risposta, copiare e salvare l'id risorsa del nodo (`id`), indirizzo IP BMC (`bmcAddress`) e il numero di serie del nodo (`chassisSerialNumber`) da utilizzare in un passaggio successivo.

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.117.1.111",
      "credentialsAvailable": false,
      "credentialsValidated": false
    },
    "chassisSerialNumber": "221111019323",
    "chassisSlot": "C",
    "hardwareId": null,
    "hardwareTag": "00000000-0000-0000-0000-ac1f6ab4ecf6",
    "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
```

2. Aprire l'interfaccia utente dell'API REST del servizio hardware sul nodo di gestione:

```
https://<ManagementNodeIP>/hardware/2/
```

3. Fare clic su **autorizzare** e completare le seguenti operazioni:

   a. Inserire il nome utente e la password del cluster.

   b. Immettere l'ID client come `mnode-client` se il valore non è già compilato.

   c. Fare clic su **autorizzare** per avviare una sessione.

   d. Chiudere la finestra.

4. Fare clic su **PUT /nodes/{hardware_id}**.

5. Fare clic su **Provalo**.

6. Inserire l'id risorsa del nodo salvato in precedenza in `hardware_id` parametro.

7. Inserire le seguenti informazioni nel payload:

Parametro	Descrizione
`assetId`	l'id della risorsa di installazione (`id`) salvato al punto 1(f).
`bmcIp`	L'indirizzo IP BMC (`bmcAddress`) salvato al punto 1(k).
`bmcPassword`	Una password aggiornata per accedere al BMC.
`bmcUsername`	Un nome utente aggiornato per accedere al BMC.
`serialNumber`	Il numero di serie dello chassis dell'hardware.

Payload di esempio:

```
{
  "assetId": "7bb41e3c-2e9c-2151-b00a-8a9b49c0b0fe",
  "bmcIp": "10.117.1.111",
  "bmcPassword": "mypassword1",
  "bmcUsername": "admin1",
  "serialNumber": "221111019323"
}
```

8. Fare clic su **Esegui** per aggiornare le credenziali BMC. Un risultato positivo restituisce una risposta simile a quanto segue:

```
{
  "credentialid": "33333333-cccc-3333-cccc-333333333333",
  "host_name": "hci-host",
  "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
  "ip": "1.1.1.1",
  "parent": "abcd01y3-ab30-1ccc-11ee-11f123zx7d1b",
  "type": "BMC"
}
```

Trova ulteriori informazioni

- "Problemi noti e soluzioni per gli aggiornamenti dei nodi di calcolo"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Monitorare i volumi nel cluster di storage

Il sistema SolidFire esegue il provisioning dello storage utilizzando i volumi. I volumi sono

dispositivi a blocchi a cui si accede in rete dai client iSCSI o Fibre Channel. È possibile monitorare i dettagli relativi a gruppi di accesso, account, iniziatori, capacità utilizzata, stato di protezione dei dati Snapshot, numero di sessioni iSCSI e policy di qualità del servizio (QoS) associate al volume.

È inoltre possibile visualizzare i dettagli sui volumi attivi ed eliminati.

Con questa visualizzazione, è possibile monitorare prima la colonna capacità utilizzata.

Puoi accedere a queste informazioni solo se disponi dei privilegi amministrativi di NetApp Hybrid Cloud Control.

Fasi

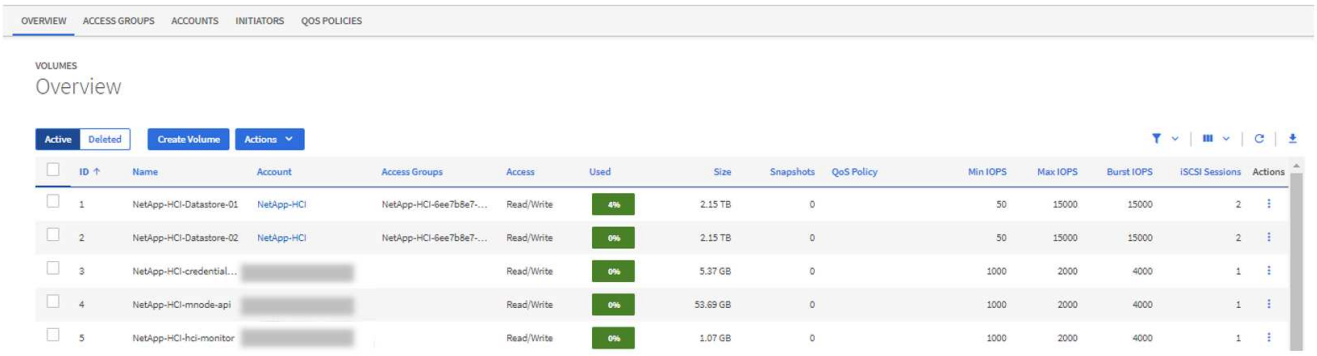
1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

```
https://<ManagementNodeIP>
```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Nella casella blu di navigazione a sinistra, selezionare l'installazione di NetApp HCI.

   Viene visualizzata la dashboard di controllo del cloud ibrido.

4. Nella barra di navigazione a sinistra, selezionare il cluster e scegliere **Storage** > **Volumes**.



5. Nella pagina Volumes (volumi), utilizzare le seguenti opzioni:

   a. Filtrare i risultati facendo clic sull'icona **Filter** (filtro).
   b. Per nascondere o visualizzare le colonne, fare clic sull'icona **Nascondi/Mostra**.
   c. Aggiornare i dati facendo clic sull'icona **Refresh** (Aggiorna).
   d. Scaricare un file CSV facendo clic sull'icona **Download**.
6. Monitorare la colonna capacità utilizzata. Se vengono raggiunte le soglie di avviso, errore o critico, il colore rappresenta lo stato della capacità utilizzata:
   a. Avvertenza - giallo

b. Errore - arancione

c. Critico - Rosso

7. Dalla vista Volumes (volumi), fare clic sulle schede per visualizzare ulteriori dettagli sui volumi:

   a. **Gruppi di accesso**: È possibile visualizzare i gruppi di accesso al volume mappati dagli iniziatori a un insieme di volumi per un accesso protetto.

      Vedere le informazioni su "gruppi di accesso ai volumi".

   b. **Account**: È possibile visualizzare gli account utente, che consentono ai client di connettersi ai volumi su un nodo. Quando si crea un volume, questo viene assegnato a un account utente specifico.

      Vedere le informazioni su "Account utente NetApp HCI".

   c. **Initiator**: È possibile visualizzare le WWPN iSCSI Initiator IQN o Fibre Channel per il volume. Ogni IQN aggiunto a un gruppo di accesso può accedere a ciascun volume del gruppo senza richiedere l'autenticazione CHAP. Ogni WWPN aggiunto a un gruppo di accesso abilita l'accesso alla rete Fibre Channel ai volumi del gruppo di accesso.

   d. **QoS Policies** (Criteri QoS): È possibile visualizzare il criterio QoS applicato al volume. Una policy di QoS applica impostazioni standardizzate per IOPS minimi, IOPS massimi e IOPS burst a più volumi.

      Vedere le informazioni su "Policy di performance e QoS".

Trova ulteriori informazioni

- "SolidFire e documentazione degli elementi"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Monitoraggio delle performance, della capacità e dello stato dei cluster con SolidFire Active IQ

Utilizzando SolidFire Active IQ, è possibile monitorare gli eventi, le performance e la capacità dei cluster. Puoi accedere a SolidFire Active IQ dalla dashboard di controllo del cloud ibrido di NetApp.

Prima di iniziare

- Per usufruire di questo servizio, è necessario disporre di un account NetApp Support.
- È necessario disporre dell'autorizzazione per utilizzare le API REST del nodo di gestione.
- È stato implementato un nodo di gestione con versione 12.0 o successiva.
- La versione del cluster in uso esegue il software NetApp Element 12.0 o versione successiva.
- Hai accesso a Internet. Il servizio di raccolta Active IQ non può essere utilizzato da siti oscuri.

A proposito di questa attività è possibile ottenere viste storiche costantemente aggiornate delle statistiche a livello di cluster. È possibile impostare le notifiche per avvisarti di eventi, soglie o metriche specifici su un cluster, in modo da poterli affrontare rapidamente.

Come parte del tuo normale contratto di supporto, il supporto NetApp monitora questi dati e ti avvisa in caso di

potenziali problemi di sistema.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

```
https://<ManagementNodeIP>
```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Dalla dashboard, selezionare il menu in alto a destra.
4. Selezionare **Visualizza Active IQ**.

   Il "Dashboard di SolidFire Active IQ" viene visualizzato.

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

   È inoltre possibile accedere alla documentazione di SolidFire Active IQ dalla dashboard selezionando l'icona del menu in alto a destra e selezionando **documentazione**.

6. Dall'interfaccia SolidFire Active IQ, verificare che i nodi di calcolo e storage NetApp HCI riportino correttamente la telemetria a Active IQ:
   a. Se si dispone di più installazioni NetApp HCI, selezionare **Seleziona un cluster** e scegliere il cluster dall'elenco.
   b. Nel riquadro di navigazione a sinistra, selezionare **Nodes** (nodi).
7. Se uno o più nodi non sono presenti nell'elenco, contattare il supporto NetApp.

> Per visualizzare il numero di risorse di storage e calcolo, consulta la dashboard di controllo del cloud ibrido (HCC). Vedere "Monitorate le risorse di storage e di calcolo con HCC Dashboard".

Trova ulteriori informazioni

- "Documentazione NetApp SolidFire Active IQ"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Raccogliere i registri per la risoluzione dei problemi

In caso di problemi con l'installazione dello storage all-flash NetApp HCI o SolidFire, è possibile raccogliere i registri da inviare al supporto NetApp per fornire assistenza nella diagnosi. È possibile utilizzare il controllo del cloud ibrido NetApp o l'API REST per raccogliere i log sui sistemi NetApp HCI o Element.

Di cosa hai bisogno

- Assicurarsi che la versione del cluster di storage in uso utilizzi il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver implementato un nodo di gestione con versione 11.3 o successiva.

Opzioni di raccolta dei log

Scegliere una delle seguenti opzioni:

- Utilizza NetApp Hybrid Cloud Control per raccogliere i log
- Utilizzare l'API REST per raccogliere i registri

Utilizza NetApp Hybrid Cloud Control per raccogliere i log

È possibile accedere all'area di raccolta dei log dal NetApp Hybrid Cloud Control Dashboard.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
3. Dalla dashboard, fare clic sul menu in alto a destra.
4. Selezionare **Collect Logs** (raccolta registri).

   Viene visualizzata la pagina **Collect Logs**. Se in precedenza sono stati raccolti dei log, è possibile scaricare il pacchetto di log esistente o iniziare una nuova raccolta di log.

5. Selezionare un intervallo di date nel menu a discesa **intervallo di date** per specificare le date da includere nei registri.

   Se si specifica una data di inizio personalizzata, è possibile selezionare la data in cui iniziare l'intervallo di date. I registri verranno raccolti da tale data fino all'ora corrente.

6. Nella sezione **Log Collection**, selezionare i tipi di file di log che il pacchetto di log deve includere.

   Per i log di storage e calcolo, è possibile espandere l'elenco dei nodi di storage o di calcolo e selezionare i singoli nodi da cui raccogliere i log (o tutti i nodi nell'elenco).

7. Fare clic su **Collect Logs** per avviare la raccolta dei log.

   La raccolta dei log viene eseguita in background e la pagina mostra lo stato di avanzamento.

   > A seconda dei registri raccolti, la barra di avanzamento potrebbe rimanere a una determinata percentuale per alcuni minuti o avanzare molto lentamente in alcuni punti.

8. Fare clic su **Download Logs** per scaricare il pacchetto di log.

   Il pacchetto di log è in un formato di file .tgz UNIX compresso.

Utilizzare l'API REST per raccogliere i registri

È possibile utilizzare l'API REST per raccogliere i log NetApp HCI o Element.

Fasi

1. Individuare l'ID del cluster di storage:
   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/logs/1/
      ```

   b. Fare clic su **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
      iii. Fare clic su **autorizzare** per avviare una sessione.
2. Raccogliere i log da NetApp HCI o Element:
   a. Fare clic su **POST /bundle**.
   b. Fare clic su **Provalo**.
   c. Modificare i valori dei seguenti parametri nel campo **corpo della richiesta** in base al tipo di log da raccogliere e all'intervallo di tempo:

Parametro	Tipo	Descrizione
`modifiedSince`	Stringa di dati	Includere solo i registri modificati dopo questa data e ora. Ad esempio, il valore "2020-07-14T20:19:00.000Z" definisce una data di inizio del 14 luglio 2020 alle 20:19 UTC.
`computeLogs`	Booleano	Impostare questo parametro su `true` per includere i log dei nodi di calcolo.
`computeIds`	Array UUID	Se `computeLogs` è impostato su `true`, Popolare questo parametro con gli ID delle risorse del nodo di gestione dei nodi di calcolo per limitare la raccolta dei log a quei nodi di calcolo specifici. Utilizzare `GET` `https://<ManagementNodeIP>/logs/1/bundle/options` Endpoint per visualizzare tutti i possibili ID di nodo che è possibile utilizzare.
`mnodeLogs`	Booleano	Impostare questo parametro su `true` per includere i log dei nodi di gestione.
`storageCrashDumps`	Booleano	Impostare questo parametro su `true` per includere i log di debug del crash del nodo di storage.

Parametro	Tipo	Descrizione
`storageLogs`	Booleano	Impostare questo parametro su `true` per includere i log dei nodi di storage.
`storageNodeIds`	Array UUID	Se `storageLogs` è impostato su `true`, Popolare questo parametro con gli ID dei nodi del cluster di storage per limitare la raccolta dei log a quei nodi di storage specifici. Utilizzare `GET` `https://<ManagementNodeIP>/logs/1/bundle/options` Endpoint per visualizzare tutti i possibili ID di nodo che è possibile utilizzare.

d. Fare clic su **Execute** (Esegui) per avviare la raccolta dei log. La risposta dovrebbe restituire una risposta simile a quanto segue:

```
{
  "_links": {
    "self": "https://10.1.1.5/logs/1/bundle"
  },
  "taskId": "4157881b-z889-45ce-adb4-92b1843c53ee",
  "taskLink": "https://10.1.1.5/logs/1/bundle"
}
```

3. Verificare lo stato dell'attività di raccolta dei log:
   a. Fare clic su **GET /bundle**.
   b. Fare clic su **Provalo**.
   c. Fare clic su **Execute** (Esegui) per tornare allo stato dell'attività di raccolta.
   d. Scorrere fino alla parte inferiore del corpo della risposta.

      Viene visualizzato un `percentComplete` attributo che descrive l'avanzamento della raccolta. Se la raccolta è completa, il `downloadLink` l'attributo contiene il link completo per il download, incluso il nome del file del pacchetto di log.

   e. Copiare il nome del file alla fine di `downloadLink` attributo.
4. Scarica il pacchetto di log raccolto:
   a. Fare clic su **GET /bundle/{filename}**.
   b. Fare clic su **Provalo**.
   c. Incollare il nome del file precedentemente copiato in `filename` campo di testo del parametro.
   d. Fare clic su **Execute** (Esegui).

      Al termine dell'esecuzione, viene visualizzato un collegamento per il download nell'area del corpo della

risposta.

e. Fare clic su **Download file** (Scarica file) e salvare il file risultante sul computer.

   Il pacchetto di log è in un formato di file .tgz UNIX compresso.

Trova ulteriori informazioni

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

Aggiornare il sistema NetApp HCI versione 1.9 o 1.9P1

Panoramica della sequenza di aggiornamento

È possibile mantenere aggiornato il sistema NetApp HCI dopo l'implementazione aggiornando in sequenza tutti i componenti software di NetApp HCI.

Questi componenti includono servizi di gestione, HealthTools, NetApp Hybrid Cloud Control, software Element, nodo di gestione, firmware di calcolo, driver di calcolo, E il plug-in Element per vCenter Server.

> A partire dal 2023 novembre, non puoi avviare un aggiornamento dei componenti utilizzando il controllo cloud ibrido di NetApp o l'API REST perché i certificati delle chiavi di firma (privati e pubblici) sono scaduti il 5 novembre 2023. Per risolvere questo problema, seguire la soluzione alternativa descritta nell'articolo della Knowledge base "Impossibile avviare gli aggiornamenti di SolidFire e HCI a causa di un errore di caricamento del pacchetto di aggiornamento".

Il sequenza di aggiornamento del sistema Il contenuto descrive le attività necessarie per completare un aggiornamento del sistema NetApp HCI. Idealmente, queste procedure vengono eseguite come parte di una sequenza di aggiornamento più ampia e non in maniera isolata. Se è necessario un aggiornamento o un aggiornamento basato su componenti, consultare i prerequisiti della procedura per assicurarsi che vengano risolte ulteriori complessità.

Il Sequenza di aggiornamento di vSphere L'inclusione del contenuto di Element Plug-in per vCenter Server descrive le fasi aggiuntive di pre e post-aggiornamento necessarie per reinstallare Element Plug-in per vCenter Server.

Di cosa hai bisogno

- Si sta eseguendo il nodo di gestione 11.3 o versione successiva. Le versioni più recenti del nodo di gestione dispongono di un'architettura modulare che fornisce servizi individuali.

  > Per controllare la versione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso. Se non si dispone di 11.3, vedere "Aggiorna il nodo di gestione".

- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326.

  Gli aggiornamenti che utilizzano NetApp Hybrid Cloud Control non sono disponibili nelle versioni precedenti del service bundle.

- Hai garantito che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di storage e i nodi. Ciascun nodo deve essere configurato con un server dei nomi DNS nell'interfaccia utente Web per nodo (`https://[IP address]:442`) senza errori del cluster irrisolti correlati all'inclinazione temporale.

sequenza di upgrade del sistema

Per aggiornare il sistema NetApp HCI, seguire la sequenza riportata di seguito.

Fasi

1. "Servizi di gestione degli aggiornamenti da Hybrid Cloud Control".

> Se si aggiornano i servizi di gestione alla versione 2.16 o successiva e si esegue un nodo di gestione da 11.3 a 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione.

> Prima di aggiornare il software Element, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente.

2. "(Opzionale) Aggiorna alla versione più recente di HealthTools".

> L'aggiornamento di HealthTools è necessario solo se il nodo di gestione e il software Element in esecuzione sono 11.1 o precedenti. HealthTools non è necessario per eseguire gli aggiornamenti degli elementi utilizzando NetApp Hybrid Cloud Control.

3. "Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage".
4. "Aggiorna il software Element e il firmware dello storage".
5. "(Opzionale) aggiornare solo il firmware dello storage Element".

> È possibile eseguire questa operazione quando un nuovo aggiornamento del firmware dello storage diventa disponibile al di fuori di una release principale.

6. "(Facoltativo) Aggiorna il nodo di gestione".

> L'aggiornamento del sistema operativo del nodo di gestione non è più necessario per aggiornare il software Element sul cluster di storage. Se il nodo di gestione è la versione 11.3 o superiore, è sufficiente aggiornare i servizi di gestione alla versione più recente per eseguire gli aggiornamenti degli elementi utilizzando NetApp Hybrid Cloud Control. Se si desidera aggiornare il sistema operativo del nodo di gestione per altri motivi, ad esempio la risoluzione dei problemi di protezione, seguire la procedura di aggiornamento del nodo di gestione per lo scenario in uso.

7. "Aggiorna il plug-in Element per vCenter Server".
8. "Eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware di calcolo".
9. "Aggiornare i driver dei nodi di calcolo".
10. "Aggiorna il firmware del tuo nodo di calcolo utilizzando NetApp Hybrid Cloud Control" oppure "Automatizza gli aggiornamenti del firmware di calcolo con Ansible".

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"
- "Aggiorna un sistema storage all-flash NetApp SolidFire"

Procedure di aggiornamento del sistema

Servizi di gestione degli aggiornamenti

È possibile aggiornare i servizi di gestione alla versione più recente del bundle dopo aver installato il nodo di gestione 11.3 o successivo.

A partire dalla release del nodo di gestione Element 11.3, la progettazione del nodo di gestione è stata modificata in base a una nuova architettura modulare che fornisce servizi individuali. Questi servizi modulari offrono funzionalità di gestione centralizzata ed estesa per i sistemi NetApp HCI. I servizi di gestione includono servizi di telemetria, registrazione e aggiornamento del sistema, il servizio QoSSIOC per Element Plug-in per vCenter Server, NetApp Hybrid Cloud Control e molto altro ancora.

A proposito di questa attività

- Prima di aggiornare il software Element, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente.

> - Management Services 2.22.7 include Element Plug-in per vCenter Server 5.0 che contiene il plug-in remoto. Se si utilizza il plug-in Element, è necessario eseguire l'aggiornamento ai servizi di gestione 2.22.7 o versioni successive per rispettare la direttiva VMware che rimuove il supporto per i plug-in locali. "Scopri di più".
> - Per le ultime note di rilascio dei servizi di gestione che descrivono i principali servizi, le nuove funzionalità, le correzioni dei bug e le soluzioni alternative per ciascun bundle di servizi, vedere "note di rilascio dei servizi di gestione"

Di cosa hai bisogno

A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare il Contratto di licenza con l'utente finale (EULA) prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare i servizi di gestione:

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

Opzioni di aggiornamento

Puoi aggiornare i servizi di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control o l'API REST del nodo di gestione:

- Servizi di gestione degli aggiornamenti con Hybrid Cloud Control (Metodo consigliato)
- Aggiornare i servizi di gestione utilizzando l'API del nodo di gestione

Servizi di gestione degli aggiornamenti con Hybrid Cloud Control

Puoi aggiornare i tuoi servizi di gestione NetApp utilizzando NetApp Hybrid Cloud Control.

I bundle di servizi di gestione offrono funzionalità e correzioni avanzate per l'installazione al di fuori delle release principali.

Prima di iniziare

- Si sta eseguendo il nodo di gestione 11.3 o versione successiva.
- Se si aggiornano i servizi di gestione alla versione 2.16 o successiva e si esegue un nodo di gestione da 11.3 a 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione:
  a. Spegnere la VM del nodo di gestione.
  b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
  c. Accendere la VM del nodo di gestione.
- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326. Gli aggiornamenti di NetApp Hybrid Cloud Control non sono disponibili nei pacchetti di servizi precedenti.

> Per un elenco dei servizi disponibili per ciascuna versione del bundle di servizi, vedere "Note sulla versione di Management Services".

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina Upgrades (aggiornamenti), selezionare la scheda **Management Services** (servizi di gestione).
5. Seguire le istruzioni riportate nella pagina per scaricare e salvare un pacchetto di aggiornamento dei servizi di gestione sul computer.
6. Selezionare **Sfoglia** per individuare il pacchetto salvato e caricarlo.

   Dopo aver caricato il pacchetto, l'aggiornamento viene avviato automaticamente.

   Una volta avviato l'aggiornamento, lo stato dell'aggiornamento viene visualizzato in questa pagina. Durante l'aggiornamento, potresti perdere la connessione con NetApp Hybrid Cloud Control e devi effettuare nuovamente l'accesso per visualizzare i risultati dell'aggiornamento.

Aggiornare i servizi di gestione utilizzando l'API del nodo di gestione

Gli utenti dovrebbero idealmente eseguire aggiornamenti dei servizi di gestione da NetApp Hybrid Cloud Control. Tuttavia, è possibile caricare, estrarre e distribuire manualmente un aggiornamento del bundle di servizi per i servizi di gestione nel nodo di gestione utilizzando l'API REST. È possibile eseguire ciascun comando dall'interfaccia utente API REST per il nodo di gestione.

Prima di iniziare

- È stato implementato un nodo di gestione software NetApp Element 11.3 o successivo.
- Se si aggiornano i servizi di gestione alla versione 2.16 o successiva e si esegue un nodo di gestione da 11.3 a 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione:

a. Spegnere la VM del nodo di gestione.
b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
c. Accendere la VM del nodo di gestione.

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326. Gli aggiornamenti di NetApp Hybrid Cloud Control non sono disponibili nei pacchetti di servizi precedenti.

> Per un elenco dei servizi disponibili per ciascuna versione del bundle di servizi, vedere "Note sulla versione di Management Services".

Fasi

1. Aprire l'interfaccia utente API REST sul nodo di gestione: `https://<ManagementNodeIP>/mnode`
2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Caricare ed estrarre il bundle di servizi sul nodo di gestione utilizzando questo comando: `PUT /services/upload`
4. Implementare i servizi di gestione sul nodo di gestione: `PUT /services/deploy`
5. Monitorare lo stato dell'aggiornamento: `GET /services/update/status`

   Un aggiornamento riuscito restituisce un risultato simile al seguente esempio:

```
{
"current_version": "2.10.29",
"details": "Updated to version 2.17.52",
"status": "success"
}
```

Trova ulteriori informazioni

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

Effettua l'aggiornamento alla versione più recente di HealthTools

Prima di iniziare un aggiornamento dello storage Element dalla versione 11.1 o precedente, è necessario aggiornare la suite HealthTools. L'aggiornamento di HealthTools è necessario solo se il nodo di gestione e il software Element in esecuzione sono 11.1 o precedenti. HealthTools non sono richiesti per "Esecuzione di upgrade degli elementi utilizzando NetApp Hybrid Cloud Control".

> Il software Element 12.3.2 è la versione finale a cui è possibile eseguire l'aggiornamento utilizzando NetApp HealthTools. Se si utilizza il software Element 11.3 o versioni successive, è necessario utilizzare NetApp Hybrid Cloud Control per aggiornare il software Element. È possibile aggiornare Element versione 11.1 o precedente utilizzando NetApp HealthTools.

Di cosa hai bisogno

- Si sta eseguendo il nodo di gestione 11.0, 11.1 o versione successiva.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326.

  Gli aggiornamenti di NetApp Hybrid Cloud Control non sono disponibili nelle versioni precedenti dei service bundle.

- È stata scaricata l'ultima versione di "HealthTools" e ha copiato il file di installazione nel nodo di gestione.

  > È possibile verificare la versione installata localmente di HealthTools eseguendo `sfupdate-healthtools -v` comando.

- Per utilizzare HealthTools con i siti oscuri, è necessario eseguire i seguenti passaggi aggiuntivi:
  - Scaricare un "File JSON" Dal NetApp Support Site su un computer che non è il nodo di gestione e rinominarlo in `metadata.json`.
  - Far funzionare il nodo di gestione al sito buio.

A proposito di questa attività

I comandi della suite HealthTools richiedono privilegi di escalation per l'esecuzione. Entrambi i comandi precedano `sudo` oppure eseguire l'escalation dell'utente ai privilegi root.

> La versione di HealthTools utilizzata potrebbe essere più aggiornata rispetto all'input e alla risposta di esempio riportati di seguito.

Fasi

1. Eseguire `sfupdate-healthtools <path to install file>` Per installare il nuovo software HealthTools.

   Esempio di input:

   ```
   sfupdate-healthtools /tmp/solidfire-healthtools-2020.03.01.09.tgz
   ```

   Esempio di risposta:

```
Checking key signature for file /tmp/solidfirehealthtools-
2020.03.01.09/components.tgz
installing command sfupdate-healthtools
Restarting on version 2020.03.01.09
sfupdate-healthtools /sf/bin/sfupdate-healthtools -r 2020.03.01.09
installing command sfupgradecheck
installing command sfinstall
installing command sfresetupgrade
```

2. Eseguire `sfupdate-healthtools -v` per verificare che la versione installata sia stata aggiornata.

   Esempio di risposta:

```
Currently installed version of HealthTools:
2020.03.01.09
```

Trova ulteriori informazioni

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

Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

Prima di aggiornare lo storage Element, è necessario eseguire controlli di integrità per assicurarsi che tutti i nodi di storage nel cluster siano pronti per l'upgrade dello storage Element successivo.

Di cosa hai bisogno

- **Servizi di gestione**: È stato eseguito l'aggiornamento al bundle di servizi di gestione più recente (2.10.27 o versione successiva).

  > Prima di aggiornare il software Element, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente.

- **Nodo di gestione**: Si sta eseguendo il nodo di gestione 11.3 o successivo.
- **Software Element**: La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per eseguire i controlli dello stato dello storage Element:
  a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.

c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.

d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

Opzioni di controllo dello stato di salute

È possibile eseguire controlli di integrità utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control (HCC), l'API HCC o la suite HealthTools:

- Utilizza NetApp Hybrid Cloud Control per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage (Metodo preferito)
- Utilizzare l'API per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage
- Utilizzare HealthTools per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

Per ulteriori informazioni sui controlli dello stato dello storage eseguiti dal servizio, consultare:

- Controlli dello stato dello storage eseguiti dal servizio

Utilizza NetApp Hybrid Cloud Control per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

Utilizzando NetApp Hybrid Cloud Control (HCC), è possibile verificare che un cluster di storage sia pronto per l'aggiornamento.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare la scheda **Storage**.
5. Selezionare il controllo dello stato di salute per il cluster che si desidera controllare per verificare la disponibilità all'aggiornamento.
6. Nella pagina **Storage Health Check**, selezionare **Run Health Check**.
7. In caso di problemi, procedere come segue:

   a. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.

   b. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.

   c. Una volta risolti i problemi del cluster, selezionare **Riesegui controllo stato di salute**.

Una volta completato il controllo dello stato di salute senza errori, il cluster di storage è pronto per l'aggiornamento. Vedere aggiornamento del nodo di storage "istruzioni" per procedere.

Utilizzare l'API per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

È possibile utilizzare REST API per verificare che un cluster di storage sia pronto per l'aggiornamento. Il controllo dello stato di salute verifica che non vi siano ostacoli all'aggiornamento, ad esempio nodi in sospeso, problemi di spazio su disco e guasti del cluster.

Fasi

1. Individuare l'ID del cluster di storage:

   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

   ```
   https://<ManagementNodeIP>/mnode
   ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:

      i. Inserire il nome utente e la password del cluster.

      ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.

      iii. Selezionare **autorizzare** per avviare una sessione.

      iv. Chiudere la finestra di autorizzazione.

   c. Dall'interfaccia utente API REST, selezionare `GET /assets`.

   d. Selezionare **Provalo**.

   e. Selezionare **Esegui**.

   f. Dalla risposta, copiare `"id"` dal `"storage"` sezione del cluster che si intende controllare per verificare la disponibilità all'aggiornamento.

   > Non utilizzare `"parent"` Valore in questa sezione perché si tratta dell'ID del nodo di gestione, non dell'ID del cluster di storage.

   ```
   "config": {},
   "credentialid": "12bbb2b2-f1be-123b-1234-12c3d4bc123e",
   "host_name": "SF_DEMO",
   "id": "12cc3a45-e6e7-8d91-a2bb-0bdb3456b789",
   "ip": "10.123.12.12",
   "parent": "d123ec42-456e-8912-ad3e-4bd56f4a789a",
   "sshcredentialid": null,
   "ssl_certificate": null
   ```

2. Eseguire i controlli di integrità sul cluster di storage:

   a. Aprire l'interfaccia utente dell'API REST dello storage sul nodo di gestione:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:

i. Inserire il nome utente e la password del cluster.
ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
iii. Selezionare **autorizzare** per avviare una sessione.
iv. Chiudere la finestra di autorizzazione.

c. Selezionare **POST /Health-checks**.
d. Selezionare **Provalo**.
e. Nel campo Parameter (parametro), inserire l'ID del cluster di storage ottenuto nella fase 1.

```
{
  "config": {},
  "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
}
```

f. Selezionare **Esegui** per eseguire un controllo dello stato di salute sul cluster di storage specificato.

   La risposta deve indicare lo stato come `initializing`:

```
{
  "_links": {
    "collection": "https://10.117.149.231/storage/1/health-checks",
    "log": "https://10.117.149.231/storage/1/health-checks/358f073f-
896e-4751-ab7b-ccbb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-
896e-4751-ab7b-ccbb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccbb5f61f9fc",
  "state": "initializing",
  "status": null,
  "storageId": "c6d124b2-396a-4417-8a47-df10d647f4ab",
  "taskId": "73f4df64-bda5-42c1-9074-b4e7843dbb77"
}
```

a. Copiare il `healthCheckID` ciò fa parte della risposta.

3. Verificare i risultati dei controlli di stato:

a. Selezionare **GET /Health-checks/{healthCheckId}**.
b. Selezionare **Provalo**.
c. Inserire l'ID del controllo di salute nel campo dei parametri.
d. Selezionare **Esegui**.

e. Scorrere fino alla parte inferiore del corpo della risposta.

   Se tutti i controlli di integrità hanno esito positivo, il reso è simile al seguente esempio:

```
"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"
```

4. Se il `message` la restituzione indica la presenza di problemi relativi allo stato del cluster, procedere come segue:
   a. Selezionare **GET /Health-checks/{healthCheckId}/log**
   b. Selezionare **Provalo**.
   c. Inserire l'ID del controllo di salute nel campo dei parametri.
   d. Selezionare **Esegui**.
   e. Esaminare eventuali errori specifici e ottenere i relativi collegamenti agli articoli della Knowledge base.
   f. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.
   g. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.
   h. Dopo aver risolto i problemi del cluster, eseguire di nuovo **GET /Health-checks/{healthCheckId}/log**.

Utilizzare HealthTools per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

È possibile verificare che il cluster di storage sia pronto per l'aggiornamento utilizzando `sfupgradecheck` comando. Questo comando verifica informazioni quali nodi in sospeso, spazio su disco e guasti del cluster.

Se il nodo di gestione si trova in una sede buia senza connettività esterna, il controllo di preparazione dell'aggiornamento richiede `metadata.json` file scaricato durante "Aggiornamenti di HealthTools" per eseguire correttamente.

A proposito di questa attività

Questa procedura descrive come risolvere i controlli di aggiornamento che producono uno dei seguenti risultati:

- Esecuzione di `sfupgradecheck` il comando viene eseguito correttamente. Il cluster è pronto per l'aggiornamento.
- Controlli all'interno di `sfupgradecheck` errore dello strumento con un messaggio di errore. Il cluster non è pronto per l'aggiornamento e sono necessari ulteriori passaggi.
- Il controllo dell'aggiornamento non riesce e viene visualizzato un messaggio di errore che indica che HealthTools non è aggiornato.
- Il controllo dell'upgrade non riesce perché il nodo di gestione si trova in un sito oscuro.

Fasi

1. Eseguire `sfupgradecheck` comando:

```
sfupgradecheck -u <cluster-user-name> MVIP
```

> Per le password che contengono caratteri speciali, aggiungere una barra rovesciata (`\`) prima di ogni carattere speciale. Ad esempio, `mypass!@1` deve essere inserito come `mypass\!\@`.

Esempio di comando di input con output di esempio in cui non vengono visualizzati errori e si è pronti per l'aggiornamento:

```
sfupgradecheck -u admin 10.117.78.244
```

```
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/
SolidFire-Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnecti
vity
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the
management node
Node ID: 1 Upload speed: 90063.90 KBs/sec
Node ID: 3 Upload speed: 106511.44 KBs/sec
Node ID: 2 Upload speed: 85038.75 KBs/sec
```

2. In caso di errori, sono necessarie ulteriori azioni. Per ulteriori informazioni, consultare le seguenti sottosezioni.

Il cluster non è pronto per l'aggiornamento

Se viene visualizzato un messaggio di errore relativo a uno dei controlli di integrità, attenersi alla seguente procedura:

1. Esaminare `sfupgradecheck` messaggio di errore.

   Esempio di risposta:

```
The following tests failed:
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Severity: ERROR
Failed node IDs: 2
Remedy: Remove unneeded files from root drive
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnectivi
ty
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the management node
Node ID: 1 Upload speed: 86518.82 KBs/sec
Node ID: 3 Upload speed: 84112.79 KBs/sec
Node ID: 2 Upload speed: 93498.94 KBs/sec
```

In questo esempio, il nodo 1 ha poco spazio su disco. Per ulteriori informazioni, consultare "knowledge base" (KB) nel messaggio di errore.

HealthTools non è aggiornato

Se viene visualizzato un messaggio di errore che indica che HealthTools non è la versione più recente, seguire queste istruzioni:

1. Esaminare il messaggio di errore e notare che il controllo dell'aggiornamento non riesce.

   Esempio di risposta:

   ```
   sfupgradecheck failed: HealthTools is out of date:
   installed version: 2018.02.01.200
   latest version: 2020.03.01.09.
   The latest version of the HealthTools can be downloaded from:
   https://mysupport.netapp.com/NOW/cgi-bin/software/
   Or rerun with the -n option
   ```

2. Seguire le istruzioni descritte nella risposta.

Il nodo di gestione si trova in un sito oscuro

1. Leggere il messaggio e notare che il controllo dell'aggiornamento non riesce:

   Esempio di risposta:

   ```
   sfupgradecheck failed: Unable to verify latest available version of
   healthtools.
   ```

2. Scaricare un "File JSON" Dal NetApp Support Site su un computer che non è il nodo di gestione e rinominarlo in `metadata.json`.
3. Eseguire il seguente comando:

   ```
   sfupgradecheck -l --metadata=<path-to-metadata-json>
   ```

4. Per ulteriori informazioni, consultare ulteriori informazioni "Aggiornamenti di HealthTools" informazioni per i siti oscuri.
5. Verificare che la suite HealthTools sia aggiornata eseguendo il seguente comando:

   ```
   sfupgradecheck -u <cluster-user-name> -p <cluster-password> MVIP
   ```

Controlli dello stato dello storage eseguiti dal servizio

I controlli dello stato dello storage effettuano i seguenti controlli per cluster.

Selezionare Nome	Nodo/cluster	Descrizione
check_async_results	Cluster	Verifica che il numero di risultati asincroni nel database sia inferiore a un numero di soglia.
check_cluster_faults	Cluster	Verifica che non vi siano errori del cluster che bloccano l'aggiornamento (come definito nell'origine dell'elemento).
check_upload_speed	Nodo	Misura la velocità di caricamento tra il nodo di storage e il nodo di gestione.
connection_speed_check	Nodo	Verifica che i nodi dispongano di connettività al nodo di gestione che fornisce pacchetti di aggiornamento e stima la velocità di connessione.
check_core	Nodo	Verifica la presenza di un crash dump del kernel e dei file core sul nodo. Il controllo non riesce per eventuali crash in un periodo di tempo recente (soglia 7 giorni).
check_root_disk_space	Nodo	Verifica che il file system root disponga di spazio libero sufficiente per eseguire un aggiornamento.
check_var_log_disk_space	Nodo	Lo verifica `/var/log` lo spazio libero soddisfa una certa soglia percentuale di spazio libero. In caso contrario, il controllo ruota e elimina i registri meno recenti per scendere sotto la soglia. Il controllo non riesce se non riesce a creare spazio libero sufficiente.
check_pending_nodes	Cluster	Verifica che non vi siano nodi in sospeso nel cluster.

Trova ulteriori informazioni

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

Aggiornare il software Element

Per aggiornare il software NetApp Element, è possibile utilizzare l'interfaccia utente per il controllo del cloud ibrido, l'API REST o la suite di tool HealthTools. Alcune operazioni vengono soppresse durante l'aggiornamento di un software Element, ad esempio l'aggiunta e la rimozione di nodi, l'aggiunta e la rimozione di dischi e i comandi associati a iniziatori, gruppi di accesso ai volumi e reti virtuali.

Di cosa hai bisogno

- **Privilegi di amministratore**: Si dispone delle autorizzazioni di amministratore del cluster di storage per eseguire l'aggiornamento.
- **Percorso di aggiornamento valido**: Sono state verificate le informazioni sul percorso di aggiornamento per la versione dell'elemento a cui si sta eseguendo l'aggiornamento e il percorso di aggiornamento è valido.https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Software/What_is_the_upgrade_matrix_for_storage_clusters_running_NetApp_Element_software%3F["KB di NetApp: Matrice di aggiornamento per cluster di storage che eseguono il software NetApp Element"^]
- **System Time Sync**: Hai garantito che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di storage e i nodi. Ciascun nodo deve essere configurato con un server dei nomi DNS nell'interfaccia utente Web per nodo (`https://[IP address]:442`) senza errori del cluster irrisolti correlati all'inclinazione temporale.
- **Porte di sistema**: Se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, si è assicurati che le porte necessarie siano aperte. Vedere "Porte di rete" per ulteriori informazioni.
- **Nodo di gestione**: Per l'interfaccia utente e l'API di NetApp Hybrid Cloud Control, il nodo di gestione nel tuo ambiente esegue la versione 11.3.
- **Servizi di gestione**: Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente.

> Prima di aggiornare il software Element alla versione 12.3.x, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente Se si sta aggiornando il software Element alla versione 12.3.x, per procedere sono necessari i servizi di gestione 2.14.60 o versione successiva.

- **Cluster Health**: Hai verificato che il cluster è pronto per l'aggiornamento. Vedere "Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage".
- **BMC aggiornato per nodi H610S**: È stata aggiornata la versione BMC per i nodi H610S. Vedere "note di rilascio e istruzioni per l'aggiornamento".
- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare il software Element:
  a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

  ```
  https://<ManagementNodeIP>
  ```

  b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
  c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
  d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

Opzioni di upgrade

Scegliere una delle seguenti opzioni di aggiornamento del software Element:

- Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare lo storage Element
- Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare lo storage degli elementi
- Aggiorna il software Element nei siti connessi utilizzando HealthTools

- Aggiorna il software Element nei siti oscuri utilizzando HealthTools

> Se si sta aggiornando un nodo della serie H610S a Element 12.3.x e il nodo esegue una versione di Element precedente alla 11.8, sarà necessario eseguire ulteriori passaggi di aggiornamento (fase 2) per ciascun nodo di storage. Se si esegue Element 11.8 o versioni successive, non sono necessarie ulteriori fasi di aggiornamento (fase 2).

Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare lo storage Element

Utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control, è possibile aggiornare un cluster di storage.

> Per i potenziali problemi durante l'aggiornamento dei cluster di storage utilizzando NetApp Hybrid Cloud Control e le relative soluzioni alternative, vedere "Articolo della Knowledge base".

> Il processo di aggiornamento richiede circa 30 minuti per nodo per le piattaforme non H610S.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare **Storage**.

   La scheda **Storage** elenca i cluster di storage che fanno parte dell'installazione. Se un cluster non è accessibile da NetApp Hybrid Cloud Control, non verrà visualizzato nella pagina **Upgrade**.

5. Scegliere una delle seguenti opzioni ed eseguire la serie di passaggi applicabili al cluster:

Opzione	Fasi
Tutti i cluster che eseguono Element 11.8 e versioni successive	a. Selezionare **Sfoglia** per caricare il pacchetto di aggiornamento scaricato. b. Attendere il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento. Se ci si allontana dalla finestra del browser, il caricamento del file viene perso. Una volta caricato e validato il file, viene visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere alcuni minuti. Se in questa fase ci si allontana dalla finestra del browser, il caricamento del file viene preservato. c. Selezionare **Avvia aggiornamento**. Lo stato dell'aggiornamento viene modificato durante l'aggiornamento per riflettere lo stato del processo. Cambia anche in risposta alle azioni intraprese, come la sospensione dell'aggiornamento o se l'aggiornamento restituisce un errore. Vedere Lo stato dell'aggiornamento cambia. Mentre l'aggiornamento è in corso, è possibile uscire dalla pagina e tornare ad essa in un secondo momento per continuare a monitorare i progressi. La pagina non aggiorna dinamicamente lo stato e la versione corrente se la riga del cluster viene compressa. La riga del cluster deve essere espansa per aggiornare la tabella oppure è possibile aggiornare la pagina. Una volta completato l'aggiornamento, è possibile scaricare i registri.

Opzione	Fasi
Si sta eseguendo l'aggiornamento di un cluster H610S con una versione di Element precedente alla 11.8.	a. Selezionare la freccia verso il basso accanto al cluster che si sta aggiornando e scegliere una delle versioni di aggiornamento disponibili. b. Selezionare **Avvia aggiornamento**. Al termine dell'aggiornamento, l'interfaccia utente richiede di eseguire la fase 2 del processo. c. Completare le fasi aggiuntive richieste (fase 2) in "Articolo della Knowledge base"E confermare nell'interfaccia utente che la fase 2 è stata completata. Una volta completato l'aggiornamento, è possibile scaricare i registri. Per informazioni sulle varie modifiche dello stato dell'aggiornamento, vedere Lo stato dell'aggiornamento cambia.

Lo stato dell'aggiornamento cambia

Di seguito sono riportati i diversi stati visualizzati nella colonna **Upgrade Status** (Stato aggiornamento) dell'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Aggiornato	Il cluster è stato aggiornato alla versione più recente di Element disponibile.
Versioni disponibili	Le versioni più recenti del firmware per elementi e/o storage sono disponibili per l'aggiornamento.
In corso	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento. I messaggi a schermo mostrano anche gli errori a livello di nodo e visualizzano l'ID di ogni nodo nel cluster durante l'aggiornamento. È possibile monitorare lo stato di ciascun nodo utilizzando l'interfaccia utente Element o il plug-in NetApp Element per l'interfaccia utente del server vCenter.
Aggiornamento in pausa	È possibile scegliere di sospendere l'aggiornamento. A seconda dello stato del processo di aggiornamento, l'operazione di pausa può avere esito positivo o negativo. Viene visualizzato un prompt dell'interfaccia utente che richiede di confermare l'operazione di pausa. Per garantire che il cluster si trovi in una posizione sicura prima di mettere in pausa un aggiornamento, l'operazione di aggiornamento può richiedere fino a due ore. Per riprendere l'aggiornamento, selezionare **Riprendi**.
In pausa	L'aggiornamento è stato sospeso. Selezionare **Riprendi** per riprendere il processo.

Stato di aggiornamento	Descrizione
Errore	Si è verificato un errore durante l'aggiornamento. È possibile scaricare il registro degli errori e inviarlo al supporto NetApp. Dopo aver risolto l'errore, tornare alla pagina e selezionare **Riprendi**. Quando si riprende l'aggiornamento, la barra di avanzamento si sposta indietro per alcuni minuti mentre il sistema esegue il controllo dello stato di salute e verifica lo stato corrente dell'aggiornamento.
Completo di follow-up	Solo per l'aggiornamento dei nodi H610S dalla versione Element precedente alla 11.8. Una volta completata la fase 1 del processo di aggiornamento, questo stato richiede di eseguire la fase 2 dell'aggiornamento (vedere la "Articolo della Knowledge base"). Dopo aver completato la fase 2 e aver riconosciuto di averlo completato, lo stato diventa **aggiornato**.

Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare lo storage degli elementi

È possibile utilizzare le API per aggiornare i nodi di storage in un cluster alla versione più recente del software Element. È possibile utilizzare uno strumento di automazione a scelta per eseguire le API. Il flusso di lavoro API qui documentato utilizza l'interfaccia utente REST API disponibile sul nodo di gestione come esempio.

Fasi

1. Scaricare il pacchetto di aggiornamento dello storage su un dispositivo accessibile al nodo di gestione; accedere al software NetApp HCI "pagina download" e scaricare l'immagine più recente del nodo di storage.
2. Caricare il pacchetto di aggiornamento dello storage nel nodo di gestione:
   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/package-repository/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Dall'interfaccia utente API REST, selezionare **POST /packages**.
   d. Selezionare **Provalo**.
   e. Selezionare **Sfoglia** e selezionare il pacchetto di aggiornamento.
   f. Selezionare **Esegui** per avviare il caricamento.
   g. Dalla risposta, copiare e salvare l'ID del pacchetto (`"id"`) da utilizzare in un passaggio successivo.
3. Verificare lo stato del caricamento.

a. Dall'interfaccia utente API REST, selezionare **GET /packages/{id}/status**.
b. Selezionare **Provalo**.
c. Inserire l'ID del pacchetto copiato nel passaggio precedente in **id**.
d. Selezionare **Esegui** per avviare la richiesta di stato.

   La risposta indica `state` come `SUCCESS` al termine dell'operazione.

4. Individuare l'ID del cluster di storage:
   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

   ```
   https://<ManagementNodeIP>/inventory/1/
   ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   d. Selezionare **Provalo**.
   e. Selezionare **Esegui**.
   f. Dalla risposta, copiare l'ID della risorsa di installazione (`"id"`).
   g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.
   h. Selezionare **Provalo**.
   i. Incollare l'ID della risorsa di installazione nel campo **id**.
   j. Selezionare **Esegui**.
   k. Dalla risposta, copiare e salvare l'ID del cluster di storage (`"id"`) del cluster che si intende aggiornare per utilizzarlo in un secondo momento.
5. Eseguire l'aggiornamento dello storage:
   a. Aprire l'interfaccia utente dell'API REST dello storage sul nodo di gestione:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Selezionare **POST /upgrade**.

d. Selezionare **Provalo**.
e. Inserire l'ID del pacchetto di aggiornamento nel campo dei parametri.
f. Inserire l'ID del cluster di storage nel campo dei parametri.

   Il payload dovrebbe essere simile al seguente esempio:

```
{
  "config": {},
  "packageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4",
  "storageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4"
}
```

g. Selezionare **Esegui** per avviare l'aggiornamento.

   La risposta deve indicare lo stato come `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055`-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
```

```
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",
        "description": "string",
        "remedy": "string",
        "severity": "string",
        "data": {},
        "nodeID": 0
      }
    ]
  },
  "taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
  "dateCompleted": "2020-04-21T22:10:57.057Z",
  "dateCreated": "2020-04-21T22:10:57.057Z"
}
```


a. Copiare l'ID dell'aggiornamento (`"upgradeId"`) che fa parte della risposta.

6. Verificare l'avanzamento e i risultati dell'aggiornamento:

   a. Selezionare **GET /upgrades/{upgradeId}**.
   b. Selezionare **Provalo**.
   c. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**.
   d. Selezionare **Esegui**.
   e. In caso di problemi o requisiti speciali durante l'aggiornamento, eseguire una delle seguenti operazioni:

Opzione	Fasi
È necessario correggere i problemi di integrità del cluster dovuti a. `failedHealthChecks` messaggio nel corpo della risposta.	i. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata. ii. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base. iii. Una volta risolti i problemi del cluster, eseguire nuovamente l'autenticazione, se necessario, e selezionare **PUT /upgrades/{upgradeId}**. iv. Selezionare **Provalo**. v. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. vi. Invio `"action":"resume"` nel corpo della richiesta. `{ "action": "resume" }` vii. Selezionare **Esegui**.
È necessario sospendere l'aggiornamento perché la finestra di manutenzione si sta chiudendo o per un altro motivo.	i. Se necessario, eseguire nuovamente l'autenticazione e selezionare **PUT /upgrades/{upgradeId}**. ii. Selezionare **Provalo**. iii. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. iv. Invio `"action":"pause"` nel corpo della richiesta. `{ "action": "pause" }` v. Selezionare **Esegui**.

Opzione	Fasi
Se si sta aggiornando un cluster H610S con una versione di Element precedente alla 11.8, viene visualizzato lo stato `finishedNeedsAck` nel corpo di risposta. È necessario eseguire ulteriori passaggi di aggiornamento (fase 2) per ciascun nodo di storage H610S.	i. Vedere [Upgrading H610S storage nodes to Element 12.3.x or later (phase 2)] e completare il processo per ciascun nodo. ii. Se necessario, eseguire nuovamente l'autenticazione e selezionare **PUT /upgrades/{upgradeId}**. iii. Selezionare **Provalo**. iv. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. v. Invio `"action":"acknowledge"` nel corpo della richiesta. `{ "action": "acknowledge" }` vi. Selezionare **Esegui**.

f. Eseguire l'API **GET /upgrades/{upgradeId}** più volte, in base alle necessità, fino al completamento del processo.

   Durante l'aggiornamento, il `status` indica `running` se non si riscontrano errori. Man mano che ogni nodo viene aggiornato, il `step` il valore cambia in `NodeFinished`.

L'aggiornamento è stato completato correttamente quando `percent` il valore è `100` e a. `state` indica `finished`.

Cosa succede se un aggiornamento non riesce utilizzando NetApp Hybrid Cloud Control

In caso di guasto di un disco o di un nodo durante un aggiornamento, l'interfaccia utente dell'elemento visualizza gli errori del cluster. Il processo di aggiornamento non passa al nodo successivo e attende la risoluzione dei guasti del cluster. La barra di avanzamento nell'interfaccia utente mostra che l'aggiornamento è in attesa della risoluzione degli errori del cluster. In questa fase, la selezione di **Pausa** nell'interfaccia utente non funzionerà, perché l'aggiornamento attende che il cluster sia integro. Sarà necessario contattare il supporto NetApp per fornire assistenza durante l'indagine sul guasto.

NetApp Hybrid Cloud Control dispone di un periodo di attesa di tre ore preimpostato, durante il quale può verificarsi uno dei seguenti scenari:

- Gli errori del cluster vengono risolti entro tre ore e l'aggiornamento riprende. In questo scenario non è necessario eseguire alcuna azione.
- Il problema persiste dopo tre ore e lo stato dell'aggiornamento visualizza **Error** (errore) con un banner rosso. Una volta risolto il problema, è possibile riprendere l'aggiornamento selezionando **Riprendi**.
- Il supporto NetApp ha stabilito che l'aggiornamento deve essere temporaneamente interrotto per intraprendere un'azione correttiva prima della finestra di tre ore. Il supporto utilizzerà l'API per interrompere l'aggiornamento.

L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe causare la rimozione dei dischi dal nodo. Se i dischi vengono rimossi in modo non corretto, l'aggiunta dei dischi durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe richiedere più tempo per eseguire gli aggiornamenti del firmware o le attività di sincronizzazione post-aggiornamento. Se l'aggiornamento sembra bloccato, contattare il supporto NetApp per assistenza.

Aggiorna il software Element nei siti connessi utilizzando HealthTools

Fasi

1. Scaricare il pacchetto di aggiornamento dello storage e accedere al software NetApp HCI "pagina download" e scaricare l'immagine più recente del nodo di storage su un dispositivo che non è il nodo di gestione.

   Per aggiornare il software di storage Element è necessaria l'ultima versione di HealthTools.

2. Copiare il file ISO nel nodo di gestione in una posizione accessibile come /tmp.

   Quando si carica il file ISO, assicurarsi che il nome del file non venga modificato, altrimenti i passaggi successivi non avranno esito positivo.

3. **Opzionale**: Scaricare l'ISO dal nodo di gestione ai nodi del cluster prima dell'aggiornamento.

   Questo passaggio riduce i tempi di aggiornamento pre-organizzando l'ISO sui nodi di storage ed eseguendo ulteriori controlli interni per garantire che il cluster sia in buono stato da aggiornare. L'esecuzione di questa operazione non consente di impostare il cluster in modalità di "upgrade" o di limitare le operazioni del cluster.

   ```
   sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO> --stage
   ```

   Omettere la password dalla riga di comando per consentire `sfinstall` per richiedere le informazioni. Per le password che contengono caratteri speciali, aggiungere una barra rovesciata (`\`) prima di ogni carattere speciale. Ad esempio, `mypass!@1` deve essere inserito come `mypass\!\@`.

   Esempio vedere il seguente esempio di input:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfisodium-11.0.0.345.iso
   --stage
   ```

   L'output dell'esempio mostra questo `sfinstall` tenta di verificare se una versione più recente di `sfinstall` è disponibile:

```
sfinstall 10.117.0.244 -u admin
/tmp/solidfire-rtfisodium-11.0.0.345.iso 2018-10-01 16:52:15:
Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https:// mysupport.netapp.com/NOW/cgi-bin/software/
or rerun with --skip-version-check
```

Vedere il seguente estratto di esempio da un'operazione pre-fase di successo:

> Al termine della gestione temporanea, viene visualizzato il messaggio `Storage Node Upgrade Staging Successful` dopo l'aggiornamento.

```
flabv0004 ~ # sfinstall -u admin
10.117.0.87 solidfire-rtfi-sodium-patch3-11.3.0.14171.iso --stage
2019-04-03 13:19:58: sfinstall Release Version: 2019.01.01.49 Management
Node Platform:
Ember Revision: 26b042c3e15a Build date: 2019-03-12 18:45
2019-04-03 13:19:58: Checking connectivity to MVIP 10.117.0.87
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.86
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.87
...
2019-04-03 13:19:58: Successfully connected to cluster and all nodes
...
2019-04-03 13:20:00: Do you want to continue? ['Yes', 'No']: Yes
...
2019-04-03 13:20:55: Staging install pack on cluster nodes
2019-04-03 13:20:55: newVersion: 11.3.0.14171
2019-04-03 13:21:01: nodeToStage: nlabp2814, nlabp2815, nlabp2816,
nlabp2813
2019-04-03 13:21:02: Staging Node nlabp2815 mip=[10.117.0.87] nodeID=[2]
(1 of 4 nodes)
2019-04-03 13:21:02: Node Upgrade serving image at
http://10.117.0.204/rtfi/solidfire-rtfisodium-
patch3-11.3.0.14171/filesystem.squashfs
...
2019-04-03 13:25:40: Staging finished. Repeat the upgrade command
without the --stage option to start the upgrade.
```

Gli ISO in più fasi verranno eliminati automaticamente al termine dell'aggiornamento. Tuttavia, se l'aggiornamento non è stato avviato e deve essere ripianificato, gli ISO possono essere disconfigurati manualmente utilizzando il comando:

```
sfinstall <MVIP> -u <cluster_username> --destage
```

Una volta avviato l'aggiornamento, l'opzione di de-stage non è più disponibile.

4. Avviare l'aggiornamento con `sfinstall` E il percorso del file ISO:

```
sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO>
```

Esempio

Vedere il seguente esempio di comando di input:

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
11.0.0.345.iso
```

L'output dell'esempio mostra questo `sfinstall` tenta di verificare se una versione più recente di `sfinstall` è disponibile:

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
11.0.0.345.iso
2018-10-01 16:52:15: Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/ or rerun with --skip
-version-check
```

Vedere il seguente estratto di esempio da un aggiornamento riuscito. Gli eventi di aggiornamento possono essere utilizzati per monitorare l'avanzamento dell'aggiornamento.

```
# sfinstall 10.117.0.161 -u admin solidfire-rtfi-sodium-11.0.0.761.iso
2018-10-11 18:28
Checking connectivity to MVIP 10.117.0.161
Checking connectivity to node 10.117.0.23
Checking connectivity to node 10.117.0.24
...
Successfully connected to cluster and all nodes
##################################################################
You are about to start a new upgrade
10.117.0.161
10.3.0.161
solidfire-rtfi-sodium-11.0.0.761.iso
Nodes:
10.117.0.23 nlabp1023 SF3010 10.3.0.161
10.117.0.24 nlabp1025 SF3010 10.3.0.161
10.117.0.26 nlabp1027 SF3010 10.3.0.161
10.117.0.28 nlabp1028 SF3010 10.3.0.161
##################################################################
```

```
Do you want to continue? ['Yes', 'No']: yes
...
Watching for new network faults. Existing fault IDs are set([]).
Checking for legacy network interface names that need renaming
Upgrading from 10.3.0.161 to 11.0.0.761 upgrade method=rtfi
Waiting 300 seconds for cluster faults to clear
Waiting for caches to fall below threshold
...
Installing mip=[10.117.0.23] nodeID=[1] (1 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[7] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
Moving primary slice=[12] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
...
Installing mip=[10.117.114.24] nodeID=[2] (2 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[5] away from mip[10.117.114.24] nodeID[2] ssid[7]
to new ssid[11]
...
Install of solidfire-rtfi-sodium-11.0.0.761 complete.
Removing old software
No staged builds present on nodeID=[1]
No staged builds present on nodeID=[2]
...
Starting light cluster block service check
```

Se si sta aggiornando un nodo della serie H610S a Element 12.3.x e il nodo esegue una versione di Element precedente alla 11.8, sarà necessario eseguire ulteriori passaggi di aggiornamento (fase 2) per ciascun nodo di storage. Se si esegue Element 11.8 o versioni successive, non sono necessarie ulteriori fasi di aggiornamento (fase 2).

Aggiorna il software Element nei siti oscuri utilizzando HealthTools

È possibile utilizzare la suite di strumenti HealthTools per aggiornare il software NetApp Element in un sito buio che non dispone di connettività esterna.

Di cosa hai bisogno

1. Accedere al software NetApp HCI "pagina download".
2. Selezionare la versione software corretta e scaricare l'immagine più recente del nodo di storage su un computer che non è il nodo di gestione.

   Per aggiornare il software di storage Element è necessaria l'ultima versione di HealthTools.

3. Scarica questo "File JSON" Dal NetApp Support Site su un computer che non è il nodo di gestione e rinominarlo in `metadata.json`.
4. Copiare il file ISO nel nodo di gestione in una posizione accessibile come `/tmp`.

> È possibile eseguire questa operazione utilizzando, ad esempio, SCP. Quando si carica il file ISO, assicurarsi che il nome del file non venga modificato, altrimenti i passaggi successivi non avranno esito positivo.

Fasi

1. Eseguire `sfupdate-healthtools` comando:

```
sfupdate-healthtools <path-to-healthtools-package>
```

2. Controllare la versione installata:

```
sfupdate-healthtools -v
```

3. Verificare la versione più recente rispetto al file JSON di metadati:

```
sfupdate-healthtools -l --metadata=<path-to-metadata-json>
```

4. Assicurarsi che il cluster sia pronto:

```
sudo sfupgradecheck -u <cluster_username> -p <cluster_password> MVIP
--metadata=<path-to-metadata-json>
```

5. Eseguire `sfinstall` Comando con il percorso del file ISO e del file JSON di metadati:

```
sfinstall -u <cluster_username> <MVIP> <path-toinstall-file-ISO>
--metadata=<path-to-metadata-json-file>
```

Vedere il seguente esempio di comando di input:

```
sfinstall -u admin 10.117.78.244 /tmp/solidfire-rtfi-11.3.0.345.iso
--metadata=/tmp/metadata.json
```

Opzionale è possibile aggiungere `--stage` contrassegna con il `sfinstall` comando per pre-preparare l'aggiornamento in anticipo.

> Se si sta aggiornando un nodo della serie H610S a Element 12.3.x e il nodo esegue una versione di Element precedente alla 11.8, sarà necessario eseguire ulteriori passaggi di aggiornamento (fase 2) per ciascun nodo di storage. Se si esegue Element 11.8 o versioni successive, non sono necessarie ulteriori fasi di aggiornamento (fase 2).

Cosa succede se un aggiornamento non riesce con HealthTools

Se l'aggiornamento del software non riesce, è possibile sospendere l'aggiornamento.

> Si consiglia di sospendere un aggiornamento solo con Ctrl-C. In questo modo, il sistema può essere pulito.

Quando `sfinstall` attende la cancellazione dei guasti del cluster e, se un guasto dovesse causare il persistere dei guasti, `sfinstall` non passa al nodo successivo.

Fasi

1. Dovresti smettere `sfinstall` Con Ctrl+C.
2. Contattare il supporto NetApp per assistenza nell'indagine sul guasto.
3. Riprendere l'aggiornamento con lo stesso `sfinstall` comando.
4. Quando un aggiornamento viene messo in pausa utilizzando Ctrl+C, se l'aggiornamento sta aggiornando un nodo, scegliere una delle seguenti opzioni:
   - **Wait**: Consente al nodo in fase di aggiornamento di terminare prima di reimpostare le costanti del cluster.
   - **Continua**: Continua l'aggiornamento, annullando la pausa.
   - **Abort**: Ripristinare le costanti del cluster e interrompere immediatamente l'aggiornamento.

   > L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe causare la rimozione dei dischi dal nodo. Se i dischi vengono rimossi in modo non corretto, l'aggiunta dei dischi durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe richiedere più tempo per eseguire gli aggiornamenti del firmware o le attività di sincronizzazione post-aggiornamento. Se l'aggiornamento sembra bloccato, contattare il supporto NetApp per assistenza.

Aggiornamento dei nodi di storage H610S a Element 12.3.x (fase 2)

Se si aggiorna un nodo della serie H610S a Element 12.3.x e il nodo esegue una versione di Element precedente alla 11.8, il processo di aggiornamento prevede due fasi.

La fase 1, che viene eseguita per prima, segue le stesse fasi del processo standard di aggiornamento a Element 12.3.x. Installa Element Software e tutti e 5 gli aggiornamenti del firmware in modo variabile nel cluster, un nodo alla volta. A causa del payload del firmware, il processo richiede circa 1.5 - 2 ore per nodo H610S, incluso un singolo ciclo di avvio a freddo al termine dell'aggiornamento per ciascun nodo.

La fase 2 prevede il completamento delle fasi necessarie per eseguire un arresto completo del nodo e la disconnessione dell'alimentazione per ciascun nodo H610S descritto in un'operazione richiesta "KB". Si stima che questa fase richiede circa un'ora per nodo H610S.

> Una volta completata la fase 1, quattro dei cinque aggiornamenti del firmware vengono attivati durante l'avvio a freddo su ciascun nodo H610S; tuttavia, il firmware CPLD (Complex Programmable Logic Device) richiede uno scollegamento completo dell'alimentazione e una riconnessione per l'installazione completa. L'aggiornamento del firmware CPLD protegge da guasti NVDIMM e dall'utilizzo dei metadati durante riavvii o cicli di alimentazione futuri. Il ripristino dell'alimentazione richiede circa un'ora per nodo H610S. Richiede lo spegnimento del nodo, la rimozione dei cavi di alimentazione o la disconnessione dell'alimentazione tramite una Smart PDU, l'attesa di circa 3 minuti e il ricollegamento dell'alimentazione.

Prima di iniziare

- Hai completato la fase 1 del processo di aggiornamento di H610S e hai aggiornato i nodi di storage utilizzando una delle procedure standard di upgrade dello storage Element.

> La fase 2 richiede personale on-site.

Fasi

1. (Fase 2) completare il processo di ripristino dell'alimentazione richiesto per ciascun nodo H610S nel cluster:

> Se il cluster dispone anche di nodi non H610S, questi nodi non H610S sono esenti dalla fase 2 e non devono essere spenti o scollegati.

1. Contattare il supporto NetApp per assistenza e per pianificare questo aggiornamento.
2. Seguire la procedura di aggiornamento della fase 2 descritta in questa sezione "KB" Necessario per completare un aggiornamento per ciascun nodo H610S.

Trova ulteriori informazioni

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

Aggiornare il firmware dello storage

A partire da Element 12.0 e dalla versione 2.14 dei servizi di gestione, è possibile eseguire aggiornamenti solo firmware sui nodi di storage utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control e l'API REST. Questa procedura non aggiorna il software Element e consente di aggiornare il firmware dello storage al di fuori di una release elemento principale.

Di cosa hai bisogno

- **Privilegi di amministratore**: Si dispone delle autorizzazioni di amministratore del cluster di storage per eseguire l'aggiornamento.
- **System Time Sync**: Hai garantito che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di storage e i nodi. Ciascun nodo deve essere configurato con un server dei nomi DNS nell'interfaccia utente Web per nodo (`https://[IP address]:442`) senza errori del cluster irrisolti correlati all'inclinazione temporale.
- **Porte di sistema**: Se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, si è assicurati che le porte necessarie siano aperte. Vedere "Porte di rete" per ulteriori informazioni.

- **Nodo di gestione**: Per l'interfaccia utente e l'API di NetApp Hybrid Cloud Control, il nodo di gestione nel tuo ambiente esegue la versione 11.3.
- **Servizi di gestione**: Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente.

> Per i nodi di storage H610S che eseguono il software Element versione 12.0, applicare D-patch SUST-909 prima di eseguire l'aggiornamento al bundle firmware di storage 2.27. Contattare il supporto NetApp per ottenere la D-patch prima di eseguire l'aggiornamento. Vedere "Note sulla versione di Storage firmware Bundle 2.27".

> Prima di aggiornare il firmware sui nodi di storage, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente. Se si sta aggiornando il software Element alla versione 12.2 o successiva, per procedere sono necessari i servizi di gestione 2.14.60 o successiva.

> Per aggiornare il firmware iDRAC/BIOS, contattare il supporto NetApp. Per ulteriori informazioni, consultare questa sezione "Articolo della Knowledge base".

- **Cluster Health**: Sono stati eseguiti controlli di integrità. Vedere "Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage".
- **BMC aggiornato per nodi H610S**: È stata aggiornata la versione BMC per i nodi H610S. Vedere "note di rilascio e istruzioni per l'aggiornamento".

> Per una matrice completa di firmware e firmware del driver per l'hardware, vedere "Versioni firmware supportate per i nodi di storage NetApp HCI".

- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare il firmware dello storage:
  a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

  ```
  https://<ManagementNodeIP>
  ```

  b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
  c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
  d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

Opzioni di upgrade

Scegliere una delle seguenti opzioni di aggiornamento del firmware dello storage:

- Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware dello storage
- Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare il firmware dello storage

Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware dello storage

È possibile utilizzare l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware dei nodi di storage nel cluster.

Di cosa hai bisogno

Se il nodo di gestione non è connesso a Internet "Scaricato il pacchetto firmware dello storage per i cluster di storage NetApp HCI".

> Per i potenziali problemi durante l'aggiornamento dei cluster di storage utilizzando NetApp Hybrid Cloud Control e le relative soluzioni alternative, vedere "Articolo della Knowledge base".

> Il processo di aggiornamento richiede circa 30 minuti per nodo di storage. Se si sta aggiornando un cluster di storage Element a un firmware di storage più recente della versione 2.76, i singoli nodi di storage si riavvieranno durante l'aggiornamento solo se è stato scritto un nuovo firmware nel nodo.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare **Storage**.

> La scheda **Storage** elenca i cluster di storage che fanno parte dell'installazione. Se un cluster non è accessibile da NetApp Hybrid Cloud Control, non verrà visualizzato nella pagina **Upgrade**. Se si utilizzano cluster con Element 12.0 o versioni successive, viene visualizzata la versione corrente del bundle firmware per questi cluster. Se i nodi di un singolo cluster dispongono di versioni firmware diverse o durante il processo di aggiornamento, nella colonna **versione corrente del bundle del firmware** verrà visualizzato **multiplo**. È possibile selezionare **multipli** per accedere alla pagina **nodi** e confrontare le versioni del firmware. Se tutti i cluster eseguono versioni di Element precedenti alla 12.0, non verranno visualizzate informazioni relative ai numeri di versione del bundle del firmware. Queste informazioni sono disponibili anche nella pagina **nodi**. Vedere "Visualizza l'inventario".
>
> Se il cluster è aggiornato e/o non sono disponibili pacchetti di aggiornamento, le schede **Element** e **firmware only** non vengono visualizzate. Queste schede non vengono visualizzate anche quando è in corso un aggiornamento. Se viene visualizzata la scheda **Element**, ma non la scheda **firmware only**, non sono disponibili pacchetti firmware.

5. Selezionare la freccia verso il basso accanto al cluster che si sta aggiornando.
6. Selezionare **Sfoglia** per caricare il pacchetto di aggiornamento scaricato.
7. Attendere il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento.

   > Se ci si allontana dalla finestra del browser, il caricamento del file viene perso.

   Una volta caricato e validato il file, viene visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere alcuni minuti. Se in questa fase ci si allontana dalla finestra del browser, il caricamento del file viene preservato.

8. Selezionare **solo firmware** e scegliere una delle versioni di aggiornamento disponibili.
9. Selezionare **Avvia aggiornamento**.

> Lo stato dell'aggiornamento viene modificato durante l'aggiornamento per riflettere lo stato del processo. Cambia anche in risposta alle azioni intraprese, come la sospensione dell'aggiornamento o se l'aggiornamento restituisce un errore. Vedere Lo stato dell'aggiornamento cambia.

> Mentre l'aggiornamento è in corso, è possibile uscire dalla pagina e tornare ad essa in un secondo momento per continuare a monitorare i progressi. La pagina non aggiorna dinamicamente lo stato e la versione corrente se la riga del cluster viene compressa. La riga del cluster deve essere espansa per aggiornare la tabella oppure è possibile aggiornare la pagina.

Una volta completato l'aggiornamento, è possibile scaricare i registri.

Lo stato dell'aggiornamento cambia

Di seguito sono riportati i diversi stati visualizzati nella colonna **Upgrade Status** (Stato aggiornamento) dell'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Aggiornato	Il cluster è stato aggiornato alla versione più recente disponibile di Element o il firmware è stato aggiornato alla versione più recente.
Impossibile rilevare	Questo stato viene visualizzato quando l'API del servizio di storage restituisce uno stato di aggiornamento non presente nell'elenco degli stati di aggiornamento possibili.
Versioni disponibili	Le versioni più recenti del firmware per elementi e/o storage sono disponibili per l'aggiornamento.
In corso	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento. I messaggi a schermo mostrano anche gli errori a livello di nodo e visualizzano l'ID di ogni nodo nel cluster durante l'aggiornamento. È possibile monitorare lo stato di ciascun nodo utilizzando l'interfaccia utente Element o il plug-in NetApp Element per l'interfaccia utente del server vCenter.
Aggiornamento in pausa	È possibile scegliere di sospendere l'aggiornamento. A seconda dello stato del processo di aggiornamento, l'operazione di pausa può avere esito positivo o negativo. Viene visualizzato un prompt dell'interfaccia utente che richiede di confermare l'operazione di pausa. Per garantire che il cluster si trovi in una posizione sicura prima di mettere in pausa un aggiornamento, l'operazione di aggiornamento può richiedere fino a due ore. Per riprendere l'aggiornamento, selezionare **Riprendi**.

Stato di aggiornamento	Descrizione
In pausa	L'aggiornamento è stato sospeso. Selezionare **Riprendi** per riprendere il processo.
Errore	Si è verificato un errore durante l'aggiornamento. È possibile scaricare il registro degli errori e inviarlo al supporto NetApp. Dopo aver risolto l'errore, tornare alla pagina e selezionare **Riprendi**. Quando si riprende l'aggiornamento, la barra di avanzamento si sposta indietro per alcuni minuti mentre il sistema esegue il controllo dello stato di salute e verifica lo stato corrente dell'aggiornamento.

Cosa succede se un aggiornamento non riesce utilizzando NetApp Hybrid Cloud Control

In caso di guasto di un disco o di un nodo durante un aggiornamento, l'interfaccia utente dell'elemento visualizza gli errori del cluster. Il processo di aggiornamento non passa al nodo successivo e attende la risoluzione dei guasti del cluster. La barra di avanzamento nell'interfaccia utente mostra che l'aggiornamento è in attesa della risoluzione degli errori del cluster. In questa fase, la selezione di **Pausa** nell'interfaccia utente non funzionerà, perché l'aggiornamento attende che il cluster sia integro. Sarà necessario contattare il supporto NetApp per fornire assistenza durante l'indagine sul guasto.

NetApp Hybrid Cloud Control dispone di un periodo di attesa di tre ore preimpostato, durante il quale può verificarsi uno dei seguenti scenari:

- Gli errori del cluster vengono risolti entro tre ore e l'aggiornamento riprende. In questo scenario non è necessario eseguire alcuna azione.
- Il problema persiste dopo tre ore e lo stato dell'aggiornamento visualizza **Error** (errore) con un banner rosso. Una volta risolto il problema, è possibile riprendere l'aggiornamento selezionando **Riprendi**.
- Il supporto NetApp ha stabilito che l'aggiornamento deve essere temporaneamente interrotto per intraprendere un'azione correttiva prima della finestra di tre ore. Il supporto utilizzerà l'API per interrompere l'aggiornamento.

> L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe causare la rimozione dei dischi dal nodo. Se i dischi vengono rimossi in modo non corretto, l'aggiunta dei dischi durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe richiedere più tempo per eseguire gli aggiornamenti del firmware o le attività di sincronizzazione post-aggiornamento. Se l'aggiornamento sembra bloccato, contattare il supporto NetApp per assistenza.

Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare il firmware dello storage

È possibile utilizzare le API per aggiornare i nodi di storage in un cluster alla versione più recente del software Element. È possibile utilizzare uno strumento di automazione a scelta per eseguire le API. Il flusso di lavoro API qui documentato utilizza l'interfaccia utente REST API disponibile sul nodo di gestione come esempio.

Fasi

1. Scaricare il pacchetto di aggiornamento del firmware dello storage più recente su un dispositivo accessibile al nodo di gestione; accedere a. "Pagina bundle firmware storage software Element" e scaricare l'immagine più recente del firmware dello storage.
2. Caricare il pacchetto di aggiornamento del firmware dello storage nel nodo di gestione:

a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/package-repository/1/
```

b. Selezionare **autorizzare** e completare le seguenti operazioni:
   i. Inserire il nome utente e la password del cluster.
   ii. Immettere l'ID client come `mnode-client`.
   iii. Selezionare **autorizzare** per avviare una sessione.
   iv. Chiudere la finestra di autorizzazione.
c. Dall'interfaccia utente API REST, selezionare **POST /packages**.
d. Selezionare **Provalo**.
e. Selezionare **Sfoglia** e selezionare il pacchetto di aggiornamento.
f. Selezionare **Esegui** per avviare il caricamento.
g. Dalla risposta, copiare e salvare l'ID del pacchetto (`"id"`) da utilizzare in un passaggio successivo.

3. Verificare lo stato del caricamento.
   a. Dall'interfaccia utente API REST, selezionare **GET /packages/{id}/status**.
   b. Selezionare **Provalo**.
   c. Inserire l'ID del pacchetto firmware copiato nella fase precedente in **id**.
   d. Selezionare **Esegui** per avviare la richiesta di stato.

      La risposta indica `state` come `SUCCESS` al termine dell'operazione.

4. Individuare l'ID della risorsa di installazione:
   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   d. Selezionare **Provalo**.
   e. Selezionare **Esegui**.
   f. Dalla risposta, copiare l'ID della risorsa di installazione (`id`).

```
"id": "abcd01e2-xx00-4ccf-11ee-11f111xx9a0b",
"management": {
  "errors": [],
  "inventory": {
    "authoritativeClusterMvip": "10.111.111.111",
    "bundleVersion": "2.14.19",
    "managementIp": "10.111.111.111",
    "version": "1.4.12"
```

g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.
h. Selezionare **Provalo**.
i. Incollare l'ID della risorsa di installazione nel campo **id**.
j. Selezionare **Esegui**.
k. Dalla risposta, copiare e salvare l'ID del cluster di storage (`"id"`) del cluster che si intende aggiornare per utilizzarlo in un secondo momento.

```
"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",
```

5. Eseguire l'aggiornamento del firmware dello storage:

a. Aprire l'interfaccia utente dell'API REST dello storage sul nodo di gestione:

```
https://<ManagementNodeIP>/storage/1/
```

b. Selezionare **autorizzare** e completare le seguenti operazioni:
   i. Inserire il nome utente e la password del cluster.
   ii. Immettere l'ID client come `mnode-client`.
   iii. Selezionare **autorizzare** per avviare una sessione.
   iv. Chiudere la finestra.
c. Selezionare **POST /upgrade**.
d. Selezionare **Provalo**.
e. Inserire l'ID del pacchetto di aggiornamento nel campo dei parametri.
f. Inserire l'ID del cluster di storage nel campo dei parametri.
g. Selezionare **Esegui** per avviare l'aggiornamento.

La risposta deve indicare lo stato come `initializing`:


```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",
        "description": "string",
        "remedy": "string",
        "severity": "string",
        "data": {},
        "nodeID": 0
      }
    ]
  },
```

```
  "taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
  "dateCompleted": "2020-04-21T22:10:57.057Z",
  "dateCreated": "2020-04-21T22:10:57.057Z"
}
```

a. Copiare l'ID dell'aggiornamento (`"upgradeId"`) che fa parte della risposta.

6. Verificare l'avanzamento e i risultati dell'aggiornamento:

   a. Selezionare **GET /upgrades/{upgradeId}**.
   b. Selezionare **Provalo**.
   c. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**.
   d. Selezionare **Esegui**.
   e. In caso di problemi o requisiti speciali durante l'aggiornamento, eseguire una delle seguenti operazioni:

Opzione	Fasi
È necessario correggere i problemi di integrità del cluster dovuti a. `failedHealthChecks` messaggio nel corpo della risposta.	i. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata. ii. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base. iii. Una volta risolti i problemi del cluster, eseguire nuovamente l'autenticazione, se necessario, e selezionare **PUT /upgrades/{upgradeId}**. iv. Selezionare **Provalo**. v. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. vi. Invio `"action":"resume"` nel corpo della richiesta. `{ "action": "resume" }` vii. Selezionare **Esegui**.

Opzione	Fasi
È necessario sospendere l'aggiornamento perché la finestra di manutenzione si sta chiudendo o per un altro motivo.	i. Se necessario, eseguire nuovamente l'autenticazione e selezionare **PUT /upgrades/{upgradeId}**. ii. Selezionare **Provalo**. iii. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. iv. Invio `"action":"pause"` nel corpo della richiesta. `{ "action": "pause" }` v. Selezionare **Esegui**.

f. Eseguire l'API **GET /upgrades/{upgradeId}** più volte, in base alle necessità, fino al completamento del processo.

   Durante l'aggiornamento, il `status` indica `running` se non si riscontrano errori. Man mano che ogni nodo viene aggiornato, il `step` il valore cambia in `NodeFinished`.

L'aggiornamento è stato completato correttamente quando `percent` il valore è `100` e a. `state` indica `finished`.

Trova ulteriori informazioni

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

Aggiornare un nodo di gestione

È possibile aggiornare il nodo di gestione alla versione 12.3.x del nodo di gestione dalla versione 11.0 o successiva.

L'aggiornamento del sistema operativo del nodo di gestione non è più necessario per aggiornare il software Element sul cluster di storage. Se il nodo di gestione è la versione 11.3 o successiva, è sufficiente aggiornare i servizi di gestione alla versione più recente per eseguire gli aggiornamenti degli elementi utilizzando NetApp Hybrid Cloud Control. Se si desidera aggiornare il sistema operativo del nodo di gestione per altri motivi, ad esempio la risoluzione dei problemi di protezione, seguire la procedura di aggiornamento del nodo di gestione per lo scenario in uso.

> Il plug-in vCenter 4.4 o versione successiva richiede un nodo di gestione 11.3 o versione successiva, creato con architettura modulare e che fornisce singoli servizi.

Opzioni di upgrade

Scegliere una delle seguenti opzioni di aggiornamento del nodo di gestione:

> - Il nodo di gestione 12.3.2 contiene una mitigazione della sicurezza per i cluster di storage con la funzione Virtual Volumes (VVol) attivata. Se il cluster di storage si trova già all'elemento 12.3 e la funzione VVols è attivata, eseguire l'aggiornamento alla versione 12.3.2.
> - Nel nodo di gestione 12.3 non sono state apportate modifiche aggiuntive alle funzionalità o correzioni di bug. Se si sta già eseguendo il nodo di gestione 12.3, non è necessario aggiornarlo alla versione 12.3.1.

- Se si esegue l'aggiornamento dal nodo di gestione 12.3: Non sono presenti modifiche di funzionalità aggiuntive o correzioni di bug nel nodo di gestione 12.3.1. Se si sta già eseguendo il nodo di gestione 12.3, non è necessario aggiornarlo alla versione 12.3.1.

> Se si sceglie di procedere con un aggiornamento su un nodo di gestione 12.3 implementato con NDE, l'aggiornamento alla versione 12.3.x verrà completato. Tuttavia, l'aggiornamento potrebbe riscontrare un errore durante il riavvio. In questo caso, riavviare il nodo di gestione in modo che venga visualizzato correttamente 12.3.x.

- Se si esegue l'aggiornamento dal nodo di gestione 12.2:Aggiornare un nodo di gestione alla versione 12.3.x dalla versione 12.2
- Se si esegue l'aggiornamento dal nodo di gestione 12.0:Aggiornare un nodo di gestione alla versione 12.3.x dalla versione 12.0
- Se si esegue l'aggiornamento dal nodo di gestione 11.3, 11.5, 11.7 o 11.8:Aggiornare un nodo di gestione alla versione 12.3.x dalla 11.3 alla 11.8
- Se si esegue l'aggiornamento dal nodo di gestione 11.0 o 11.1:Aggiornare un nodo di gestione alla versione 12.3.x da 11.1 o 11.0
- Se si esegue l'aggiornamento da un nodo di gestione versione 10.x:Migrazione dal nodo di gestione versione 10.x a 11.x.

Scegliere la seguente opzione se è stato aggiornato in modo **sequenziale** (1) la versione dei servizi di gestione e (2) la versione dello storage Element e si desidera **conservare** il nodo di gestione esistente:

> Se non si aggiornano in sequenza i servizi di gestione seguiti dallo storage degli elementi, non è possibile riconfigurare la riautenticazione utilizzando questa procedura. Seguire invece la procedura di aggiornamento appropriata.

- Se si mantiene un nodo di gestione esistente:Riconfigurare l'autenticazione utilizzando l'API REST del nodo di gestione

Aggiornare un nodo di gestione alla versione 12.3.x dalla versione 12.2

È possibile eseguire un aggiornamento in-place del nodo di gestione dalla versione 12.2 alla versione 12.3.x senza dover eseguire il provisioning di una nuova macchina virtuale con nodo di gestione.

> Il nodo di gestione Element 12.3.x è un aggiornamento opzionale. Non è richiesto per le implementazioni esistenti.

Di cosa hai bisogno

- La RAM della VM del nodo di gestione è di 24 GB.

- Il nodo di gestione che si intende aggiornare è la versione 12.0 e utilizza la rete IPv4. La versione 12.3.x del nodo di gestione non supporta IPv6.

> Per verificare la versione del nodo di gestione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso.

- Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente utilizzando NetApp Hybrid Cloud Control (HCC). È possibile accedere a HCC dal seguente indirizzo IP: <code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt;</code>
- Se si sta aggiornando il nodo di gestione alla versione 12.3.x, per procedere sono necessari i servizi di gestione 2.14.60 o versione successiva.
- È stato configurato un adattatore di rete aggiuntivo (se necessario) seguendo le istruzioni per "Configurazione di una scheda di rete storage aggiuntiva".

> I volumi persistenti potrebbero richiedere un adattatore di rete aggiuntivo se eth0 non è in grado di essere instradato a SVIP. Configurare un nuovo adattatore di rete sulla rete di storage iSCSI per consentire la configurazione di volumi persistenti.

- I nodi di storage eseguono Element 11.3 o versione successiva.

Fasi

1. Accedere alla macchina virtuale del nodo di gestione utilizzando l'accesso a SSH o alla console.
2. Scaricare il "Nodo di gestione ISO" Per NetApp HCI dal sito di supporto NetApp alla macchina virtuale del nodo di gestione.

> Il nome dell'ISO è simile a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Verificare l'integrità del download eseguendo md5sum sul file scaricato e confrontare l'output con quello disponibile sul sito del supporto NetApp per il software NetApp HCI o Element, come nell'esempio seguente:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

4. Montare l'immagine ISO del nodo di gestione e copiare il contenuto nel file system utilizzando i seguenti comandi:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
   ```

   ```
   sudo cp -r /mnt/* /upgrade
   ```

5. Passare alla home directory e smontare il file ISO da `/mnt`:

```
sudo umount /mnt
```

6. Eliminare l'ISO per risparmiare spazio sul nodo di gestione:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

7. Sul nodo di gestione che si sta aggiornando, eseguire il comando seguente per aggiornare la versione del sistema operativo del nodo di gestione. Lo script conserva tutti i file di configurazione necessari dopo l'aggiornamento, ad esempio le impostazioni di Active IQ Collector e proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

Al termine del processo di aggiornamento, il nodo di gestione viene riavviato con un nuovo sistema operativo.

> Dopo aver eseguito il comando sudo descritto in questo passaggio, la sessione SSH viene terminata. L'accesso alla console è necessario per il monitoraggio continuo. Se non è disponibile alcun accesso alla console durante l'aggiornamento, riprovare a eseguire l'accesso SSH e verificare la connettività dopo 15 - 30 minuti. Una volta effettuato l'accesso, è possibile confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è stato eseguito correttamente.

8. Sul nodo di gestione, eseguire `redeploy-mnode` script per conservare le impostazioni di configurazione dei servizi di gestione precedenti:

> Lo script conserva la precedente configurazione dei servizi di gestione, inclusa la configurazione dal servizio di raccolta Active IQ, dai controller (vCenter) o dal proxy, a seconda delle impostazioni.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

> Se in precedenza era stata disattivata la funzionalità SSH sul nodo di gestione, è necessario "Disattivare nuovamente SSH" sul nodo di gestione ripristinato. Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è attivato sul nodo di gestione per impostazione predefinita.

Aggiornare un nodo di gestione alla versione 12.3.x dalla versione 12.0

È possibile eseguire un aggiornamento in-place del nodo di gestione dalla versione 12.0 alla versione 12.3.x senza dover eseguire il provisioning di una nuova macchina virtuale con nodo di gestione.

Il nodo di gestione Element 12.3.x è un aggiornamento opzionale. Non è richiesto per le implementazioni esistenti.

Di cosa hai bisogno

- Il nodo di gestione che si intende aggiornare è la versione 12.0 e utilizza la rete IPv4. La versione 12.3.x del nodo di gestione non supporta IPv6.

  Per verificare la versione del nodo di gestione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso.

- Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente utilizzando NetApp Hybrid Cloud Control (HCC). È possibile accedere a HCC dal seguente indirizzo IP: <code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt;</code>
- Se si sta aggiornando il nodo di gestione alla versione 12.3.x, per procedere sono necessari i servizi di gestione 2.14.60 o versione successiva.
- È stato configurato un adattatore di rete aggiuntivo (se necessario) seguendo le istruzioni per "Configurazione di una scheda di rete storage aggiuntiva".

  I volumi persistenti potrebbero richiedere un adattatore di rete aggiuntivo se eth0 non è in grado di essere instradato a SVIP. Configurare un nuovo adattatore di rete sulla rete di storage iSCSI per consentire la configurazione di volumi persistenti.

- I nodi di storage eseguono Element 11.3 o versione successiva.

Fasi

1. Configurare il nodo di gestione VM RAM:
   a. Spegnere la VM del nodo di gestione.
   b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
   c. Accendere la VM del nodo di gestione.
2. Accedere alla macchina virtuale del nodo di gestione utilizzando l'accesso a SSH o alla console.
3. Scaricare il "Nodo di gestione ISO" Per NetApp HCI dal sito di supporto NetApp alla macchina virtuale del nodo di gestione.

   Il nome dell'ISO è simile a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Verificare l'integrità del download eseguendo md5sum sul file scaricato e confrontare l'output con quello disponibile sul sito del supporto NetApp per il software NetApp HCI o Element, come nell'esempio seguente:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

5. Montare l'immagine ISO del nodo di gestione e copiare il contenuto nel file system utilizzando i seguenti comandi:

   ```
   sudo mkdir -p /upgrade
   ```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>
/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. Passare alla home directory e smontare il file ISO da `/mnt`:

```
sudo umount /mnt
```

7. Eliminare l'ISO per risparmiare spazio sul nodo di gestione:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. Sul nodo di gestione che si sta aggiornando, eseguire il comando seguente per aggiornare la versione del sistema operativo del nodo di gestione. Lo script conserva tutti i file di configurazione necessari dopo l'aggiornamento, ad esempio le impostazioni di Active IQ Collector e proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

Al termine del processo di aggiornamento, il nodo di gestione viene riavviato con un nuovo sistema operativo.

> Dopo aver eseguito il comando sudo descritto in questo passaggio, la sessione SSH viene terminata. L'accesso alla console è necessario per il monitoraggio continuo. Se non è disponibile alcun accesso alla console durante l'aggiornamento, riprovare a eseguire l'accesso SSH e verificare la connettività dopo 15 - 30 minuti. Una volta effettuato l'accesso, è possibile confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è stato eseguito correttamente.

9. Sul nodo di gestione, eseguire `redeploy-mnode` script per conservare le impostazioni di configurazione dei servizi di gestione precedenti:

> Lo script conserva la precedente configurazione dei servizi di gestione, inclusa la configurazione dal servizio di raccolta Active IQ, dai controller (vCenter) o dal proxy, a seconda delle impostazioni.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

> Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 e versioni successive. Se in precedenza era stata attivata la funzionalità SSH sul nodo di gestione, potrebbe essere necessario "Disattivare nuovamente SSH" sul nodo di gestione aggiornato.

Aggiornare un nodo di gestione alla versione 12.3.x dalla 11.3 alla 11.8

È possibile eseguire un aggiornamento in-place del nodo di gestione dalla versione 11.3, 11.5, 11.7 o 11.8 alla versione 12.3.x senza dover eseguire il provisioning di una nuova macchina virtuale con nodo di gestione.

> Il nodo di gestione Element 12.3.x è un aggiornamento opzionale. Non è richiesto per le implementazioni esistenti.

Di cosa hai bisogno

- Il nodo di gestione che si intende aggiornare è la versione 11.3, 11.5, 11.7 o 11.8 e utilizza la rete IPv4. La versione 12.3.x del nodo di gestione non supporta IPv6.

  > Per verificare la versione del nodo di gestione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso.

- Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente utilizzando NetApp Hybrid Cloud Control (HCC). È possibile accedere a HCC dal seguente indirizzo IP: <code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt;</code>
- Se si sta aggiornando il nodo di gestione alla versione 12.3.x, per procedere sono necessari i servizi di gestione 2.14.60 o versione successiva.
- È stato configurato un adattatore di rete aggiuntivo (se necessario) seguendo le istruzioni per "Configurazione di una scheda di rete storage aggiuntiva".

  > I volumi persistenti potrebbero richiedere un adattatore di rete aggiuntivo se eth0 non è in grado di essere instradato a SVIP. Configurare un nuovo adattatore di rete sulla rete di storage iSCSI per consentire la configurazione di volumi persistenti.

- I nodi di storage eseguono Element 11.3 o versione successiva.

Fasi

1. Configurare il nodo di gestione VM RAM:
   a. Spegnere la VM del nodo di gestione.
   b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
   c. Accendere la VM del nodo di gestione.
2. Accedere alla macchina virtuale del nodo di gestione utilizzando l'accesso a SSH o alla console.
3. Scaricare il "Nodo di gestione ISO" Per NetApp HCI dal sito di supporto NetApp alla macchina virtuale del nodo di gestione.

   > Il nome dell'ISO è simile a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Verificare l'integrità del download eseguendo md5sum sul file scaricato e confrontare l'output con quello

disponibile sul sito del supporto NetApp per il software NetApp HCI o Element, come nell'esempio seguente:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

5. Montare l'immagine ISO del nodo di gestione e copiare il contenuto nel file system utilizzando i seguenti comandi:

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>
/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. Passare alla home directory e smontare il file ISO da `/mnt`:

```
sudo umount /mnt
```

7. Eliminare l'ISO per risparmiare spazio sul nodo di gestione:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. Nel nodo di gestione 11.3, 11.5, 11.7 o 11.8, eseguire il seguente comando per aggiornare la versione del sistema operativo del nodo di gestione. Lo script conserva tutti i file di configurazione necessari dopo l'aggiornamento, ad esempio le impostazioni di Active IQ Collector e proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

Al termine del processo di aggiornamento, il nodo di gestione viene riavviato con un nuovo sistema operativo.

> Dopo aver eseguito il comando sudo descritto in questo passaggio, la sessione SSH viene terminata. L'accesso alla console è necessario per il monitoraggio continuo. Se non è disponibile alcun accesso alla console durante l'aggiornamento, riprovare a eseguire l'accesso SSH e verificare la connettività dopo 15 - 30 minuti. Una volta effettuato l'accesso, è possibile confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è stato eseguito correttamente.

9. Sul nodo di gestione, eseguire `redeploy-mnode` script per conservare le impostazioni di configurazione dei servizi di gestione precedenti:

> Lo script conserva la precedente configurazione dei servizi di gestione, inclusa la configurazione dal servizio di raccolta Active IQ, dai controller (vCenter) o dal proxy, a seconda delle impostazioni.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

> Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 e versioni successive. Se in precedenza era stata attivata la funzionalità SSH sul nodo di gestione, potrebbe essere necessario "Disattivare nuovamente SSH" sul nodo di gestione aggiornato.

Aggiornare un nodo di gestione alla versione 12.3.x da 11.1 o 11.0

È possibile eseguire un aggiornamento in-place del nodo di gestione da 11.0 o 11.1 alla versione 12.3.x senza dover eseguire il provisioning di una nuova macchina virtuale con nodo di gestione.

Di cosa hai bisogno

- I nodi di storage eseguono Element 11.3 o versione successiva.

> Utilizza gli strumenti HealthTools più recenti per aggiornare il software Element.

- Il nodo di gestione che si intende aggiornare è la versione 11.0 o 11.1 e utilizza la rete IPv4. La versione 12.3.x del nodo di gestione non supporta IPv6.

> Per verificare la versione del nodo di gestione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso.

- Per il nodo di gestione 11.0, la memoria delle macchine virtuali deve essere aumentata manualmente fino a 12 GB.
- È stato configurato un adattatore di rete aggiuntivo (se necessario) seguendo le istruzioni per la configurazione di una scheda di rete storage (eth1) nella guida utente del nodo di gestione del prodotto.

> I volumi persistenti potrebbero richiedere un adattatore di rete aggiuntivo se eth0 non è in grado di essere instradato a SVIP. Configurare un nuovo adattatore di rete sulla rete di storage iSCSI per consentire la configurazione di volumi persistenti.

Fasi

1. Configurare il nodo di gestione VM RAM:
   a. Spegnere la VM del nodo di gestione.
   b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
   c. Accendere la VM del nodo di gestione.
2. Accedere alla macchina virtuale del nodo di gestione utilizzando l'accesso a SSH o alla console.

3. Scaricare il "Nodo di gestione ISO" Per NetApp HCI dal sito di supporto NetApp alla macchina virtuale del nodo di gestione.

> Il nome dell'ISO è simile a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Verificare l'integrità del download eseguendo md5sum sul file scaricato e confrontare l'output con quello disponibile sul sito del supporto NetApp per il software NetApp HCI o Element, come nell'esempio seguente:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

5. Montare l'immagine ISO del nodo di gestione e copiare il contenuto nel file system utilizzando i seguenti comandi:

```
sudo mkdir -p /upgrade
```

```
sudo mount solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso /mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. Passare alla home directory e smontare il file ISO da /mnt:

```
sudo umount /mnt
```

7. Eliminare l'ISO per risparmiare spazio sul nodo di gestione:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. Eseguire uno dei seguenti script con opzioni per aggiornare la versione del sistema operativo del nodo di gestione. Eseguire solo lo script appropriato per la versione in uso. Ogni script conserva tutti i file di configurazione necessari dopo l'aggiornamento, ad esempio le impostazioni di Active IQ Collector e proxy.

   a. Su un nodo di gestione 11.1 (11.1.0.73), eseguire il seguente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.3.2288
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
/sf/packages/nma"
```

b. Su un nodo di gestione 11.1 (11.1.0.72), eseguire il seguente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.1.2281
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
/sf/packages/nma"
```

c. Su un nodo di gestione 11.0 (11.0.0.781), eseguire il seguente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.0.2253
/sf/packages/solidfire-nma-1.4.8/conf /sf/packages/sioc
/sf/packages/nma"
```

Al termine del processo di aggiornamento, il nodo di gestione viene riavviato con un nuovo sistema operativo.

> Dopo aver eseguito il comando sudo descritto in questo passaggio, la sessione SSH viene terminata. L'accesso alla console è necessario per il monitoraggio continuo. Se non è disponibile alcun accesso alla console durante l'aggiornamento, riprovare a eseguire l'accesso SSH e verificare la connettività dopo 15 - 30 minuti. Una volta effettuato l'accesso, è possibile confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è stato eseguito correttamente.

9. Nel nodo di gestione 12.3.x, eseguire `upgrade-mnode` script per conservare le impostazioni di configurazione precedenti.

> Se si esegue la migrazione da un nodo di gestione 11.0 o 11.1, lo script copia il Active IQ Collector nel nuovo formato di configurazione.

a. Per un singolo cluster di storage gestito da un nodo di gestione esistente 11.0 o 11.1 con volumi persistenti:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
persistent volume> -pva <persistent volume account name - storage
volume account>
```

b. Per un singolo cluster di storage gestito da un nodo di gestione esistente 11.0 o 11.1 senza volumi persistenti:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user>
```

c. Per più cluster di storage gestiti da un nodo di gestione esistente 11.0 o 11.1 con volumi persistenti:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
persistent volume> -pva <persistent volume account name - storage
volume account> -pvm <persistent volumes mvip>
```

d. Per più cluster di storage gestiti da un nodo di gestione esistente 11.0 o 11.1 senza volumi persistenti (il `-pvm` Il flag deve fornire uno degli indirizzi MVIP del cluster):

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for
persistent volumes>
```

10. (Per tutte le installazioni NetApp HCI con plug-in NetApp Element per vCenter Server) aggiornare il plug-in vCenter sul nodo di gestione 12.3.x seguendo la procedura descritta nella "Aggiornare il plug-in Element per vCenter Server" argomento.
11. Individuare l'ID risorsa per l'installazione utilizzando l'API del nodo di gestione:
    a. Da un browser, accedere all'interfaccia utente API REST del nodo di gestione:
        i. Accedere a Storage MVIP ed effettuare l'accesso. Questa azione fa sì che il certificato venga accettato per la fase successiva.
    b. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

    c. Selezionare **autorizzare** e completare le seguenti operazioni:
        i. Inserire il nome utente e la password del cluster.
        ii. Immettere l'ID client come `mnode-client`.
        iii. Selezionare **autorizzare** per avviare una sessione.
        iv. Chiudere la finestra.
    d. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
    e. Selezionare **Provalo**.
    f. Selezionare **Esegui**.
    g. Dal corpo della risposta del codice 200, copiare il `id` per l'installazione.

    L'installazione dispone di una configurazione delle risorse di base creata durante l'installazione o l'aggiornamento.

12. Individuare il tag hardware per il nodo di calcolo in vSphere:
    a. Selezionare l'host in vSphere Web Client Navigator.
    b. Selezionare la scheda **Monitor** e selezionare **hardware Health**.
    c. Vengono elencati il produttore e il numero di modello del BIOS del nodo. Copiare e salvare il valore per `tag` da utilizzare in un passaggio successivo.
13. Aggiungere una risorsa vCenter controller per il monitoraggio HCI e il controllo del cloud ibrido al nodo di gestione risorse note:
    a. Selezionare **POST /assets/{asset_id}/controller** per aggiungere una sottorisorsa del controller.
    b. Selezionare **Provalo**.
    c. Inserire l'ID risorsa base principale copiato negli Appunti nel campo **asset_id**.
    d. Inserire i valori del payload richiesti con il tipo `vCenter` E vCenter.
    e. Selezionare **Esegui**.
14. Aggiungere una risorsa del nodo di calcolo alle risorse note del nodo di gestione:
    a. Selezionare **POST /assets/{asset_id}/compute-nodes** per aggiungere una sottorisorsa del nodo di calcolo con credenziali per la risorsa del nodo di calcolo.
    b. Selezionare **Provalo**.
    c. Inserire l'ID risorsa base principale copiato negli Appunti nel campo **asset_id**.
    d. Nel payload, inserire i valori del payload richiesti come definito nella scheda Model (modello). Invio `ESXi Host` come `type` e incollare il tag hardware salvato durante un passaggio precedente per `hardware_tag`.
    e. Selezionare **Esegui**.

Migrazione dal nodo di gestione versione 10.x a 11.x.

Se si dispone di un nodo di gestione alla versione 10.x, non è possibile eseguire l'aggiornamento da 10.x a 11.x. È invece possibile utilizzare questa procedura di migrazione per copiare la configurazione da 10.x a un nodo di gestione 11.1 appena distribuito. Se il nodo di gestione è attualmente alla versione 11.0 o superiore, ignorare questa procedura. È necessario il nodo di gestione 11.0 o 11.1 e il "Gli ultimi HealthTools" Per aggiornare il software Element da 10.3 + a 11.x.

Fasi

1. Dall'interfaccia di VMware vSphere, implementare il nodo di gestione 11.1 OVA e accenderlo.
2. Aprire la console VM del nodo di gestione, che consente di visualizzare l'interfaccia utente del terminale (TUI).
3. Utilizzare l'interfaccia telefonica utente per creare un nuovo ID amministratore e assegnare una password.
4. Nel nodo di gestione TUI, accedere al nodo di gestione con il nuovo ID e la nuova password e verificare che funzioni.
5. Dal vCenter o dal nodo di gestione TUI, ottenere l'indirizzo IP del nodo di gestione 11.1 e accedere all'indirizzo IP sulla porta 9443 per aprire l'interfaccia utente del nodo di gestione.

```
https://<mNode 11.1 IP address>:9443
```

6. In vSphere, selezionare **Configurazione NetApp Element** > **Impostazioni mNode**. (Nelle versioni

precedenti, il menu di primo livello è **Configurazione NetApp SolidFire**).

7. Selezionare **azioni** > **Cancella**.
8. Per confermare, selezionare **Sì**. Il campo mNode Status (Stato mNode) deve riportare non configurato.

> Quando si accede alla scheda **mNode Settings** (Impostazioni mNode) per la prima volta, il campo mNode Status (Stato mNode) potrebbe essere visualizzato come **Not Configured** (non configurato*) anziché come **UP** previsto; potrebbe non essere possibile selezionare **Actions** (azioni) > **Clear** (Cancella). Aggiornare il browser. Il campo mNode Status (Stato mNode) visualizza **UP**.

9. Disconnettersi da vSphere.
10. In un browser Web, aprire l'utility di registrazione del nodo di gestione e selezionare **QoSSIOC Service Management**:

```
https://<mNode 11.1 IP address>:9443
```

11. Impostare la nuova password QoSSIOC.

> La password predefinita è `solidfire`. Questa password è necessaria per impostare la nuova password.

12. Selezionare la scheda **vCenter Plug-in Registration**.
13. Selezionare **Aggiorna plug-in**.
14. Inserire i valori richiesti. Al termine, selezionare **UPDATE**.
15. Accedere a vSphere e selezionare **Configurazione NetApp Element** > **Impostazioni mNode**.
16. Selezionare **azioni** > **Configura**.
17. Fornire l'indirizzo IP del nodo di gestione, l'ID utente del nodo di gestione (il nome utente è `admin`), la password impostata nella scheda **QoSSIOC Service Management** dell'utilità di registrazione, nonché l'ID utente e la password di vCenter.

    In vSphere, la scheda **mNode Settings** (Impostazioni mNode) dovrebbe visualizzare lo stato di mNode come **UP**, che indica che il nodo di gestione 11.1 è registrato in vCenter.

18. Dall'utility di registrazione del nodo di gestione (`https://<mNode 11.1 IP address>:9443`), riavviare il servizio SIOC da **QoSSIOC Service Management**.
19. Attendere un minuto e selezionare la scheda **Configurazione NetApp Element** > **Impostazioni mNode**. Lo stato di mNode dovrebbe essere **UP**.

    Se lo stato è **DOWN**, controllare le autorizzazioni per `/sf/packages/sioc/app.properties`. Il file deve disporre dei permessi di lettura, scrittura ed esecuzione per il proprietario del file. Le autorizzazioni corrette dovrebbero essere visualizzate come segue:

```
-rwx------
```

20. Una volta avviato il processo SIOC e visualizzato lo stato di mNode in **UP**, controllare i registri per `sf-hci-nma` sul nodo di gestione. Non dovrebbero essere presenti messaggi di errore.

21. (Solo per il nodo di gestione 11.1) SSH nel nodo di gestione versione 11.1 con privilegi root e avviare il servizio NMA con i seguenti comandi:

```
# systemctl enable /sf/packages/nma/systemd/sf-hci-nma.service
```

```
# systemctl start sf-hci-nma21
```

22. Eseguire azioni da vCenter per rimuovere un disco, aggiungere un disco o riavviare i nodi. In questo modo vengono attivati gli avvisi relativi allo storage, che devono essere riportati in vCenter. Se funziona, gli avvisi di sistema NMA funzionano come previsto.
23. Se ONTAP Select è configurato in vCenter, configurare gli avvisi ONTAP Select in NMA copiando `.ots.properties` dal nodo di gestione precedente al nodo di gestione versione 11.1 `/sf/packages/nma/conf/.ots.properties` E riavviare il servizio NMA utilizzando il seguente comando:

```
systemctl restart sf-hci-nma
```

24. Verificare che ONTAP Select funzioni visualizzando i registri con il seguente comando:

```
journalctl -f | grep -i ots
```

25. Configurare Active IQ seguendo questa procedura:
    a. Accedere alla versione 11.1 del nodo di gestione e passare a. `/sf/packages/collector` directory.
    b. Eseguire il seguente comando:

    ```
    sudo ./manage-collector.py --set-username netapp --set-password --set
    -mvip <MVIP>
    ```

    c. Inserire la password dell'interfaccia utente del nodo di gestione quando richiesto.
    d. Eseguire i seguenti comandi:

    ```
    ./manage-collector.py --get-all
    ```

    ```
    sudo systemctl restart sfcollector
    ```

    e. Verificare `sfcollector` registri per confermare che funziona.
26. In vSphere, la scheda **Configurazione NetApp Element** > **Impostazioni mNode** dovrebbe visualizzare lo stato di mNode come **UP**.

27. Verificare che l'NMA stia segnalando gli avvisi di sistema e gli avvisi ONTAP Select.
28. Se tutto funziona come previsto, chiudere ed eliminare il nodo di gestione 10.x VM.

Riconfigurare l'autenticazione utilizzando l'API REST del nodo di gestione

È possibile mantenere il nodo di gestione esistente se sono stati aggiornati in sequenza (1) servizi di gestione e (2) storage di elementi. Se si è seguito un ordine di aggiornamento diverso, consultare le procedure per gli aggiornamenti dei nodi di gestione in-place.

Prima di iniziare

- I servizi di gestione sono stati aggiornati alla versione 2.10.29 o successiva.
- Il cluster di storage esegue Element 12.0 o versione successiva.
- Il nodo di gestione è 11.3 o successivo.
- I servizi di gestione sono stati aggiornati in sequenza, seguito dall'aggiornamento dello storage Element. Non è possibile riconfigurare l'autenticazione utilizzando questa procedura a meno che non siano stati completati gli aggiornamenti nella sequenza descritta.

Fasi

1. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

   ```
   https://<ManagementNodeIP>/mnode
   ```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
   c. Selezionare **autorizzare** per avviare una sessione.
3. Dall'interfaccia utente API REST, selezionare **POST /Services/reconfigure-auth**.
4. Selezionare **Provalo**.
5. Per il parametro **load_images**, selezionare `true`.
6. Selezionare **Esegui**.

   Il corpo della risposta indica che la riconfigurazione è stata eseguita correttamente.

Trova ulteriori informazioni

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

Aggiornare il plug-in Element per vCenter Server

Per gli ambienti vSphere esistenti con un plug-in NetApp Element registrato per VMware vCenter Server, è possibile aggiornare la registrazione del plug-in dopo il primo aggiornamento del pacchetto di servizi di gestione che contiene il servizio plug-in.

È possibile aggiornare la registrazione del plug-in su vCenter Server Virtual Appliance (vCSA) o Windows

utilizzando l'utility di registrazione. È necessario modificare la registrazione per il plug-in vCenter su ogni vCenter Server in cui è necessario utilizzare il plug-in.

> Management Services 2.22.7 include Element Plug-in per vCenter Server 5.0 che contiene il plug-in remoto. Se si utilizza il plug-in Element, è necessario eseguire l'aggiornamento ai servizi di gestione 2.22.7 o versioni successive per rispettare la direttiva VMware che rimuove il supporto per i plug-in locali. "Scopri di più".

Plug-in Element per vCenter 5.0 e versioni successive

Questa procedura di aggiornamento riguarda i seguenti scenari di aggiornamento:

- Stai effettuando l'aggiornamento a Element Plug-in per vCenter Server 5,2, 5,1 o 5,0.
- Si sta eseguendo l'aggiornamento a 8.0 o 7.0 HTML5 vSphere Web Client.

> Il plug-in Element per vCenter 5,0 o versioni successive non è compatibile con vCenter Server 6,7 e 6,5.

> Quando si esegue l'aggiornamento da Element Plug-in per vCenter Server 4.x a 5.x, i cluster già configurati con il plug-in vengono persi perché i dati non possono essere copiati da un'istanza di vCenter a un plug-in remoto. È necessario aggiungere nuovamente i cluster al plug-in remoto. Si tratta di un'attività singola durante l'aggiornamento da un plug-in locale a un plug-in remoto.

Plug-in Element per vCenter 4.10 e versioni precedenti

Questa procedura di aggiornamento riguarda i seguenti scenari di aggiornamento:

- Si sta eseguendo l'aggiornamento a Element Plug-in per VMware vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6, 4.5 o 4.4.
- Si sta eseguendo l'aggiornamento a un client Web 7.0, 6.7 o 6.5 HTML5 vSphere.

- Il plug-in non è compatibile con VMware vCenter Server 8.0 per Element Plug-in per VMware vCenter Server 4.x.
- Il plug-in non è compatibile con VMware vCenter Server 6.5 per Element Plug-in per VMware vCenter Server 4.6, 4.7 e 4.8.

- Si sta eseguendo l'aggiornamento a 6.7 Flash vSphere Web Client.

> Il plug-in non è compatibile con la versione 6.7 U2 build 13007421 del client Web vSphere HTML5 e con altre build 6.7 U2 rilasciate prima dell'aggiornamento 2a (build 13643870). Per ulteriori informazioni sulle versioni di vSphere supportate, consultare le note sulla versione di "versione del plug-in".

Di cosa hai bisogno

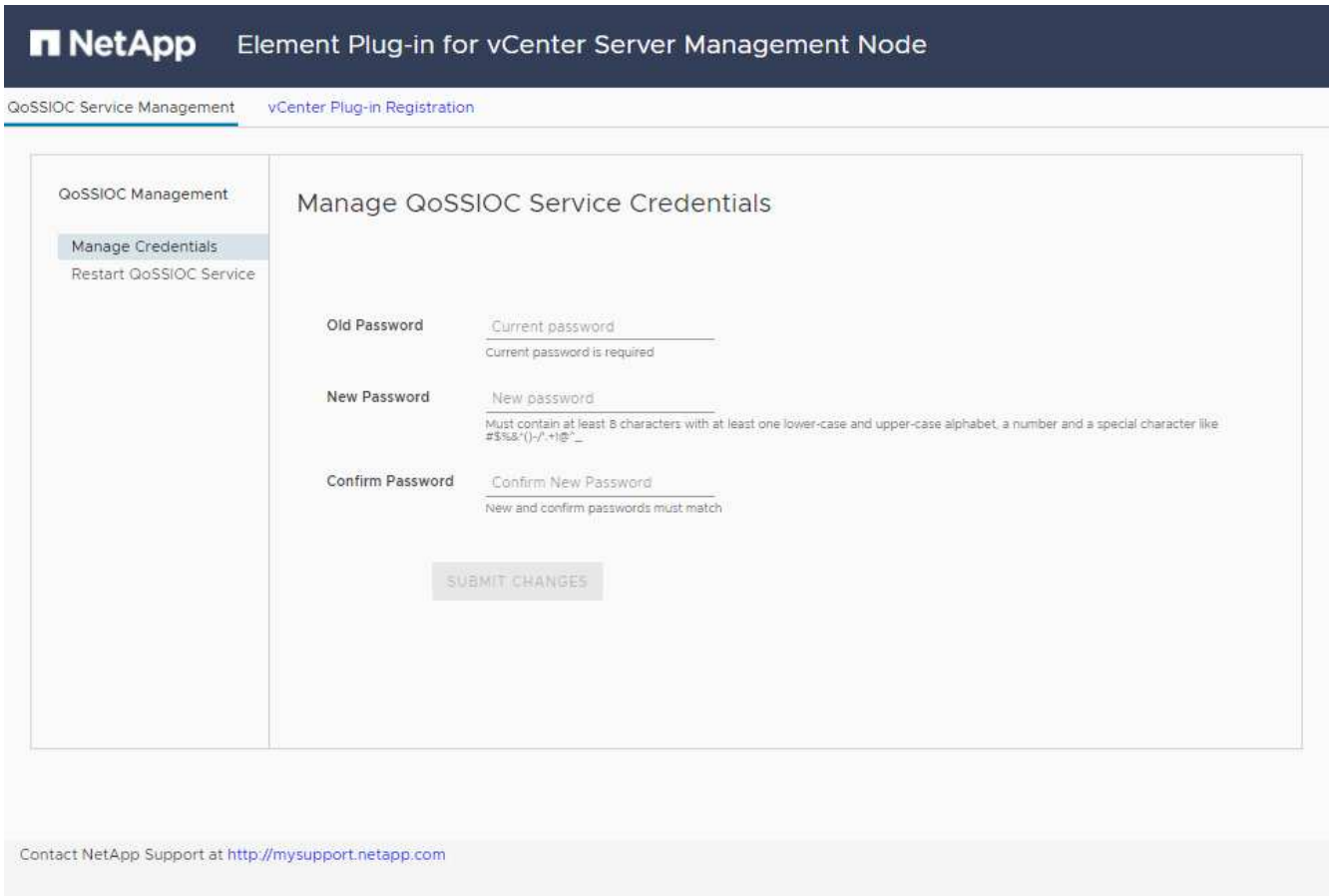
- **Privilegi di amministratore**: Si dispone dei privilegi di amministratore vCenter per installare un plug-in.
- **Aggiornamenti vSphere**: Sono stati eseguiti tutti gli aggiornamenti vCenter necessari prima di aggiornare il plug-in NetApp Element per vCenter Server. Questa procedura presuppone che gli aggiornamenti di

vCenter siano già stati completati.

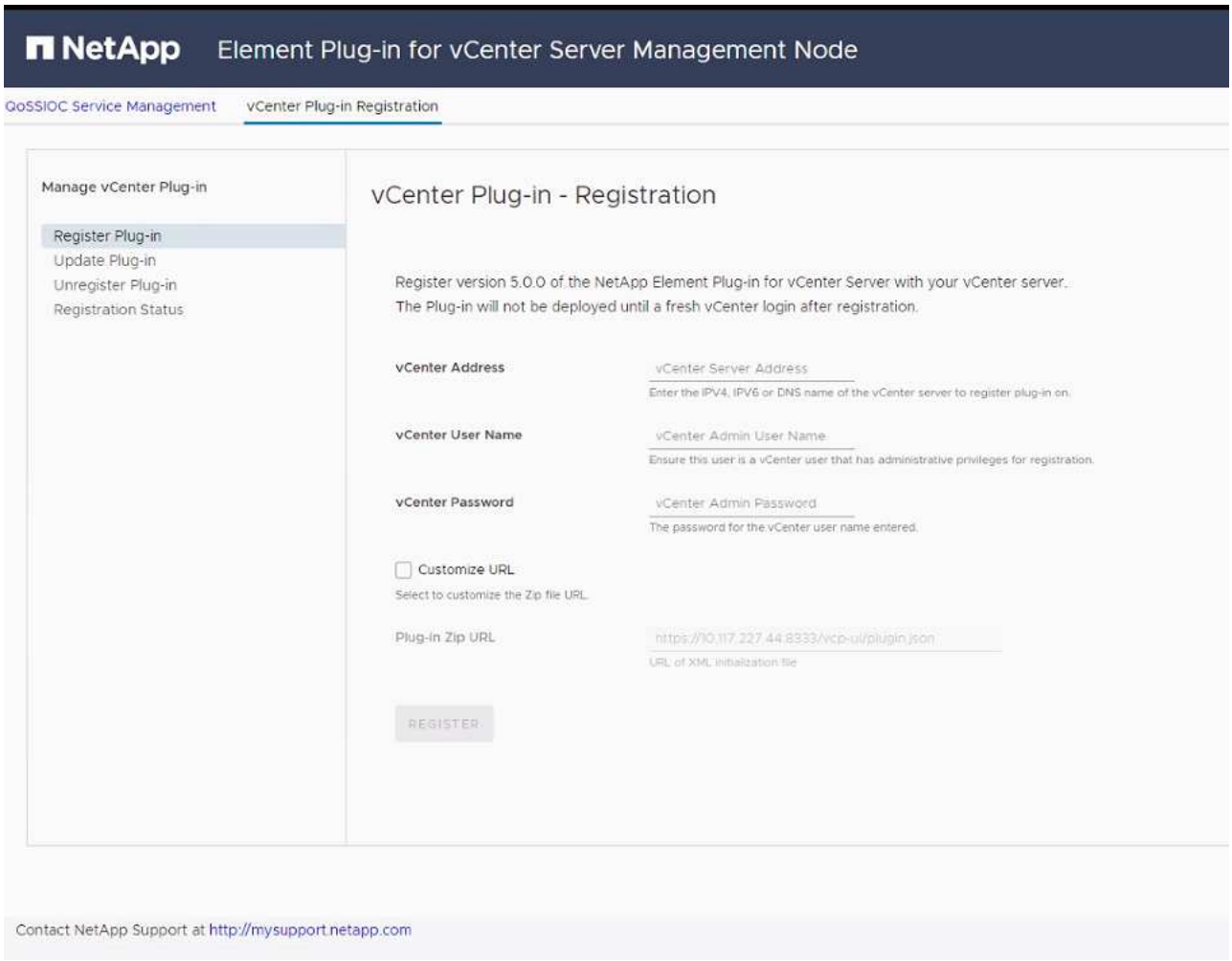
- **VCenter Server**: Il plug-in vCenter versione 5.x o 4.x è registrato con vCenter Server. Dall'utility di registrazione (`https://[management node IP]:9443`), selezionare **Registration Status** (Stato registrazione), completare i campi necessari e selezionare **Check Status** (Controlla stato) per verificare che il plug-in vCenter sia già registrato e che il numero di versione dell'installazione corrente.
- **Aggiornamenti dei servizi di gestione**: È stato aggiornato il "bundle di servizi di gestione" alla versione più recente. Gli aggiornamenti del plug-in vCenter vengono distribuiti utilizzando gli aggiornamenti dei servizi di gestione rilasciati al di fuori delle principali release di prodotti per NetApp HCI.
- **Aggiornamenti del nodo di gestione**:
  - A partire dal plug-in Element vCenter 5.0, viene eseguito un nodo di gestione "aggiornato" alla versione 12.3.x o successiva.
  - Per il plug-in Element vCenter da 4.4 a 4.10, si sta eseguendo un nodo di gestione che lo è stato "aggiornato" alla versione 11.3 o successiva. VCenter Plug-in 4.4 o versione successiva richiede un nodo di gestione 11.3 o versione successiva con un'architettura modulare che fornisce singoli servizi. Il nodo di gestione deve essere acceso con il relativo indirizzo IP o DHCP configurato.
- **Upgrade dello storage Element**:
  - A partire dal plug-in Element vCenter 5.0, si dispone di un cluster che esegue il software NetApp Element 12.3.x o versione successiva.
  - Per il plug-in Element vCenter 4.10 o versione precedente, si dispone di un cluster che esegue il software NetApp Element 11.3 o versione successiva.
- **VSphere Web Client**: Si è disconnessi da vSphere Web Client prima di iniziare qualsiasi aggiornamento del plug-in. Il client Web non riconosce gli aggiornamenti effettuati durante questo processo al plug-in se non si effettua la disconnessione.

Fasi

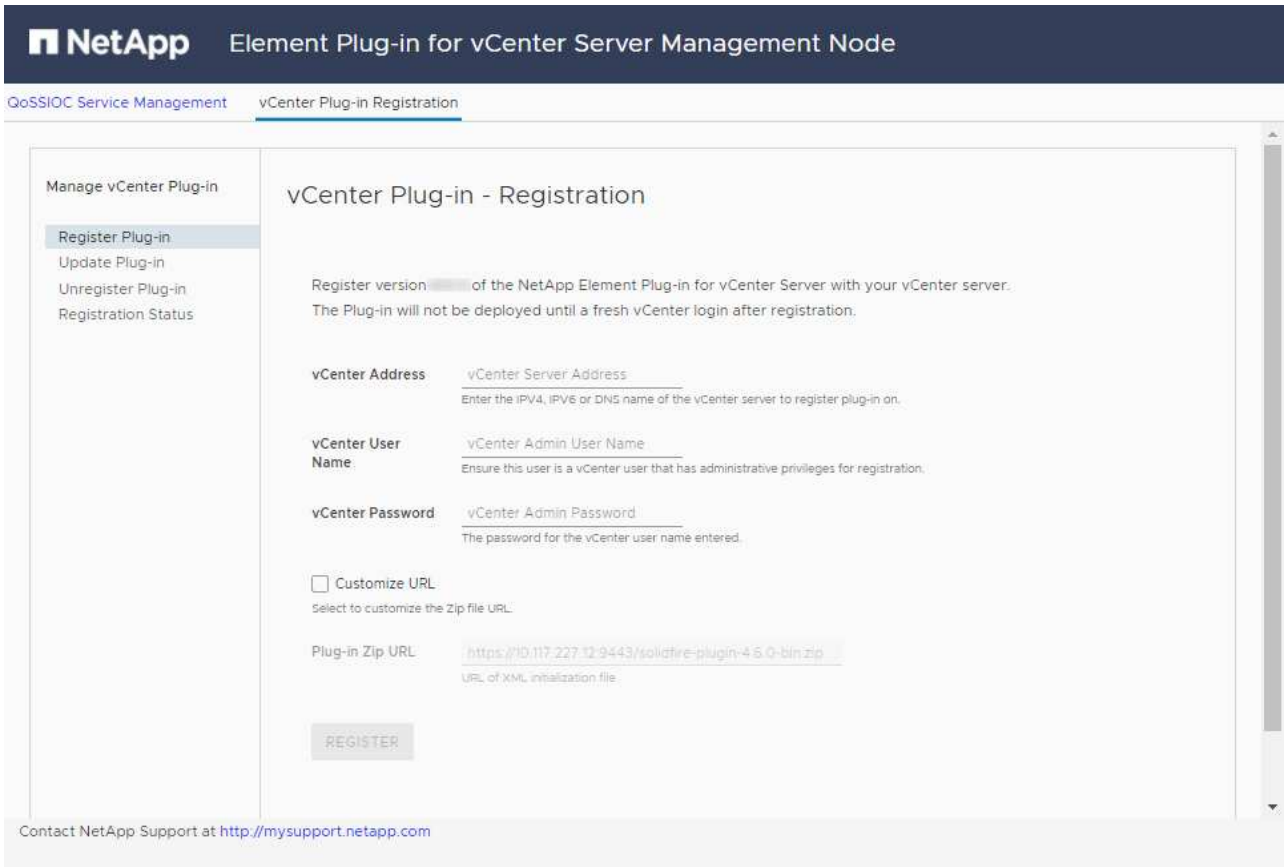
1. Inserire l'indirizzo IP del nodo di gestione in un browser, inclusa la porta TCP per la registrazione: `https://[management node IP]:9443`L'interfaccia utente dell'utility di registrazione apre la pagina **Manage QoSSIOC Service Credentials** (Gestisci credenziali servizio QoSSIOC) per il plug-in.



2. Selezionare **vCenter Plug-in Registration**.
   - La pagina di registrazione del plug-in vCenter per il plug-in Element per vCenter Server 5.x:



- La pagina di registrazione del plug-in vCenter per il plug-in Element per vCenter Server 4.10 o versioni precedenti:



3. In **Manage vCenter Plug-in** (Gestisci plug-in vCenter), selezionare **Update Plug-in** (Aggiorna plug-in).
4. Confermare o aggiornare le seguenti informazioni:
   a. L'indirizzo IPv4 o l'FQDN del servizio vCenter su cui si desidera registrare il plug-in.
   b. Il nome utente vCenter Administrator.

      Il nome utente e la password immessi devono essere assegnati a un utente con privilegi di ruolo vCenter Administrator.

   c. La password di vCenter Administrator.
   d. (Per server interni/siti oscuri) a seconda del plug-in Element per la versione di vCenter, un URL personalizzato per il file JSON del plug-in o il plug-in ZIP:
      i. A partire da Element Plug-in per vCenter Server 5.0, un URL personalizzato per il file JSON del plug-in.

         È possibile selezionare **Custom URL** (URL personalizzato) per personalizzare l'URL se si utilizza un server HTTP o HTTPS (sito scuro) o se sono state modificate le impostazioni di rete o il nome del file JSON. Per ulteriori procedure di configurazione se si intende personalizzare un URL, vedere la documentazione di Element Plug-in for vCenter Server sulla modifica delle proprietà di vCenter per un server HTTP interno (sito scuro).

      ii. Per Element Plug-in per vCenter Server 4.10 o versioni precedenti, un URL personalizzato per il plug-in ZIP.

> È possibile selezionare **Custom URL** (URL personalizzato) per personalizzare l'URL se si utilizza un server HTTP o HTTPS (sito scuro) o se sono state modificate le impostazioni di rete o il nome del file ZIP. Per ulteriori procedure di configurazione se si intende personalizzare un URL, vedere la documentazione di Element Plug-in for vCenter Server sulla modifica delle proprietà di vCenter per un server HTTP interno (sito scuro).

5. Selezionare **Aggiorna**.

   Una volta completata la registrazione, nell'interfaccia utente dell'utility di registrazione viene visualizzato un banner.

6. Accedere a vSphere Web Client come vCenter Administrator. Se si è già connessi a vSphere Web Client, è necessario prima disconnettersi, attendere due o tre minuti, quindi eseguire nuovamente l'accesso.

   > Questa azione crea un nuovo database e completa l'installazione in vSphere Web Client.

7. In vSphere Web Client, cercare le seguenti attività completate nel task monitor per assicurarsi che l'installazione sia stata completata: `Download plug-in` e. `Deploy plug-in`.
8. Verificare che i punti di estensione del plug-in siano visualizzati nella scheda **Shortcuts** di vSphere Web Client e nel pannello laterale.
   - A partire dal plug-in Element per vCenter Server 5.0, viene visualizzato il punto di estensione del plug-in remoto NetApp Element:
   - Per il plug-in Element per vCenter Server 4.10 o versioni precedenti, vengono visualizzati i punti di estensione per la configurazione e la gestione di NetApp Element:

   > Se le icone del plug-in vCenter non sono visibili, vedere "Plug-in Element per vCenter Server" documentazione sulla risoluzione dei problemi del plug-in.
   >
   > Dopo aver eseguito l'aggiornamento al plug-in NetApp Element per vCenter Server 4.8 o versioni successive con VMware vCenter Server 6.7U1, se i cluster di storage non sono elencati o viene visualizzato un errore del server nelle sezioni **Clusters** e **QoSSIOC Settings** della configurazione NetApp Element, vedere "Plug-in Element per vCenter Server" documentazione sulla risoluzione di questi errori.

9. Verificare la modifica della versione nella scheda **About** (informazioni su) nel punto di estensione **NetApp Element Configuration** del plug-in.

   Dovrebbero essere visualizzati i seguenti dettagli di versione o dettagli di una versione più recente:

```
NetApp Element Plug-in Version: 5.2
NetApp Element Plug-in Build Number: 12
```

> Il plug-in vCenter contiene il contenuto della Guida in linea. Per assicurarsi che la guida contenga i contenuti più recenti, cancellare la cache del browser dopo aver aggiornato il plug-in.

Trova ulteriori informazioni

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

Eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware di calcolo

Prima di aggiornare il firmware di calcolo, è necessario eseguire i controlli dello stato di salute per assicurarsi che tutti i nodi di calcolo del cluster siano pronti per l'aggiornamento. I controlli dello stato dei nodi di calcolo possono essere eseguiti solo su cluster di calcolo di uno o più nodi di calcolo NetApp HCI gestiti.

Di cosa hai bisogno

- **Servizi di gestione**: È stato eseguito l'aggiornamento al bundle di servizi di gestione più recente (2.11 o versione successiva).
- **Nodo di gestione**: Si sta eseguendo il nodo di gestione 11.3 o successivo.
- **Software Element**: Il cluster di storage esegue il software NetApp Element 11.3 o versione successiva.
- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per eseguire i controlli dello stato dei nodi di calcolo:
  a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

  ```
  https://<ManagementNodeIP>
  ```

  b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
  c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
  d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

Opzioni di controllo dello stato di salute

Puoi eseguire controlli di integrità utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control o l'API di NetApp Hybrid Cloud Control:

- Utilizzare NetApp Hybrid Cloud Control per eseguire controlli dello stato dei nodi di calcolo prima di aggiornare il firmware (Metodo preferito)
- Utilizzare l'API per eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware

Ulteriori informazioni sui controlli dello stato dei nodi di calcolo eseguiti dal servizio sono disponibili:

- Verifiche dello stato dei nodi di calcolo effettuate dal servizio

Utilizzare NetApp Hybrid Cloud Control per eseguire controlli dello stato dei nodi di calcolo prima di aggiornare il firmware

Utilizzando NetApp Hybrid Cloud Control, è possibile verificare che un nodo di calcolo sia pronto per l'aggiornamento del firmware.

> Se si dispone di più configurazioni di cluster di storage a due nodi, ciascuna all'interno del proprio vCenter, i controlli di stato dei nodi di controllo potrebbero non generare report accurati. Pertanto, quando si è pronti per aggiornare gli host ESXi, è necessario arrestare solo il nodo di controllo dell'host ESXi da aggiornare. È necessario assicurarsi di avere sempre un nodo di controllo in esecuzione nell'installazione di NetApp HCI spegnendo i nodi di controllo in modo alternativo.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>/hcc
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare la scheda **Compute firmware** (calcolo firmware).
5. Selezionare il controllo dello stato di salute per il cluster che si desidera controllare per verificare la disponibilità all'aggiornamento.
6. Nella pagina **Compute Health Check**, selezionare **Run Health Check**.
7. In caso di problemi, la pagina fornisce un report. Effettuare le seguenti operazioni:
   a. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.
   b. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.
   c. Una volta risolti i problemi del cluster, selezionare **Riesegui controllo stato di salute**.

Una volta completato il controllo dello stato di salute senza errori, i nodi di calcolo nel cluster sono pronti per l'aggiornamento. Vedere "Aggiornare il firmware del nodo di calcolo" per procedere.

Utilizzare l'API per eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware

È possibile utilizzare REST API per verificare che i nodi di calcolo di un cluster siano pronti per l'aggiornamento. Il controllo dello stato di salute verifica che non vi siano ostacoli all'aggiornamento, ad esempio problemi dell'host ESXi o altri problemi di vSphere. Sarà necessario eseguire controlli dello stato dei nodi di calcolo per ciascun cluster di calcolo dell'ambiente.

Fasi

1. Individuare l'ID del controller e l'ID del cluster:
   a. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.

ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.

iii. Selezionare **autorizzare** per avviare una sessione.

c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.

d. Selezionare **Provalo**.

e. Selezionare **Esegui**.

f. Dal corpo della risposta del codice 200, copiare il `"id"` per l'installazione che si intende utilizzare per i controlli di integrità.

g. Dall'interfaccia utente API REST, selezionare **GET /installations/{id}**.

h. Selezionare **Provalo**.

i. Inserire l'ID di installazione.

j. Selezionare **Esegui**.

k. Dal corpo della risposta del codice 200, copiare gli ID per ciascuno dei seguenti elementi:

i. L'ID del cluster (`"clusterID"`)

ii. Un ID del controller (`"controllerId"`)


```
{
  "_links": {
    "collection":
"https://10.117.187.199/inventory/1/installations",
    "self":
"https://10.117.187.199/inventory/1/installations/xx94f6f0-12a6-
412f-8b5e-4cf2z58329x0"
  },
  "compute": {
    "errors": [],
    "inventory": {
      "clusters": [
        {
          "clusterId": "domain-1",
          "controllerId": "abc12c3a-aa87-4e33-9f94-xx588c2cdcf6",
          "datacenterName": "NetApp-HCI-Datacenter-01",
          "installationId": "xx94f6f0-12a6-412f-8b5e-
4cf2z58329x0",
          "installationName": "test-nde-mnode",
          "inventoryType": "managed",
          "name": "NetApp-HCI-Cluster-01",
          "summary": {
            "nodeCount": 2,
            "virtualMachineCount": 2
          }
        }
      ],
```

2. Eseguire controlli di integrità sui nodi di calcolo nel cluster:

   a. Aprire l'interfaccia utente REST API del servizio di calcolo sul nodo di gestione:

   ```
   https://<ManagementNodeIP>/vcenter/1/
   ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:

      i. Inserire il nome utente e la password del cluster.

      ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.

      iii. Selezionare **autorizzare** per avviare una sessione.

   c. Selezionare **POST /compute/{CONTROLLER_ID}/Health-checks**.

   d. Selezionare **Provalo**.

   e. Inserire il `"controllerId"` È stata copiata dalla fase precedente nel campo del parametro **Controller_ID**.

   f. Nel payload, inserire `"clusterId"` che è stato copiato dal passaggio precedente come `"cluster"` valutare e rimuovere il valore `"nodes"` parametro.

   ```
   {
     "cluster": "domain-1"
   }
   ```

   g. Selezionare **Esegui** per eseguire un controllo dello stato di salute sul cluster.

      La risposta del codice 200 fornisce un `"resourceLink"` URL con l'ID attività aggiunto, necessario per confermare i risultati del controllo di integrità.

```
{
  "resourceLink": "https://10.117.150.84/vcenter/1/compute/tasks/[This
is the task ID for health check task results]",
  "serviceName": "vcenter-v2-svc",
  "taskId": "ab12c345-06f7-42d7-b87c-7x64x56x321x",
  "taskName": "VCenter service health checks"
}
```

   a. Copiare la parte dell'ID attività di `"resourceLink"` URL per verificare il risultato dell'attività.

3. Verificare il risultato dei controlli di integrità:

   a. Tornare all'interfaccia utente REST API del servizio di calcolo sul nodo di gestione:

   ```
   https://<ManagementNodeIP>/vcenter/1/
   ```

   b. Selezionare **GET /compute/tasks/{task_id}**.

c. Selezionare **Provalo**.

d. Inserire l'ID attività di `"resourceLink"` URL della risposta **POST /compute/{CONTROLLER_ID}/Health-checks** codice 200 in `task_id` campo del parametro.

e. Selezionare **Esegui**.

f. Se il `status` il messaggio restituito indica che si sono verificati problemi relativi allo stato del nodo di calcolo, procedere come segue:

   i. Consultare l'articolo specifico della Knowledge base (`KbLink`) elencati per ciascun problema o eseguire il rimedio specificato.

   ii. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.

   iii. Dopo aver risolto i problemi del cluster, eseguire di nuovo **POST /compute/{CONTROLLER_ID}/Health-checks** (vedere il passaggio 2).

Se i controlli di integrità vengono completati senza problemi, il codice di risposta 200 indica un risultato positivo.

Verifiche dello stato dei nodi di calcolo effettuate dal servizio

I controlli di stato del calcolo, eseguiti con i metodi API o con NetApp Hybrid Cloud Control, eseguono i seguenti controlli per nodo. A seconda dell'ambiente in uso, alcuni di questi controlli potrebbero essere ignorati. È necessario eseguire nuovamente i controlli di integrità dopo aver risolto eventuali problemi rilevati.

Controllare la descrizione	Nodo/cluster	Azione necessaria per risolvere il problema	Articolo della Knowledge base con procedura
DRS è abilitato e completamente automatizzato?	Cluster	Attivare DRS e assicurarsi che sia completamente automatizzato.	"Consulta questa KB". NOTA: Se si dispone di licenze standard, impostare l'host ESXi in modalità di manutenzione e ignorare questo avviso di errore del controllo dello stato di salute.
DPM è disattivato in vSphere?	Cluster	Disattivare Distributed Power Management.	"Consulta questa KB".
Il controllo di ammissione ha è disattivato in vSphere?	Cluster	Disattivare il controllo di ammissione ha.	"Consulta questa KB".
FT è abilitato per una macchina virtuale su un host nel cluster?	Nodo	Sospendere Fault Tolerance su tutte le macchine virtuali interessate.	"Consulta questa KB".
Vi sono allarmi critici in vCenter per il cluster?	Cluster	Avviare vSphere e risolvere e/o riconoscere eventuali avvisi prima di procedere.	Nessun KB necessario per risolvere il problema.

Controllare la descrizione	Nodo/cluster	Azione necessaria per risolvere il problema	Articolo della Knowledge base con procedura
Sono presenti avvisi informativi generici/globali in vCenter?	Cluster	Avviare vSphere e risolvere e/o riconoscere eventuali avvisi prima di procedere.	Nessun KB necessario per risolvere il problema.
I servizi di gestione sono aggiornati?	Sistema HCI	È necessario aggiornare i servizi di gestione prima di eseguire un aggiornamento o un controllo dello stato di salute prima dell'aggiornamento.	Nessun KB necessario per risolvere il problema. Vedere "questo articolo" per ulteriori informazioni.
Ci sono errori sul nodo ESXi corrente in vSphere?	Nodo	Avviare vSphere e risolvere e/o riconoscere eventuali avvisi prima di procedere.	Nessun KB necessario per risolvere il problema.
I supporti virtuali sono montati su una macchina virtuale su un host nel cluster?	Nodo	Smontare tutti i dischi di supporti virtuali (CD/DVD/floppy) dalle macchine virtuali.	Nessun KB necessario per risolvere il problema.
La versione di BMC è la versione minima richiesta con supporto per redfish?	Nodo	Aggiornare manualmente il firmware BMC.	Nessun KB necessario per risolvere il problema.
L'host ESXi è attivo e in esecuzione?	Nodo	Avviare l'host ESXi.	Nessun KB necessario per risolvere il problema.
Alcune macchine virtuali risiedono nello storage ESXi locale?	Nodo/VM	Rimuovere o migrare lo storage locale collegato alle macchine virtuali.	Nessun KB necessario per risolvere il problema.
BMC è attivo?	Nodo	Accendere il BMC e assicurarsi che sia connesso a una rete raggiungibile da questo nodo di gestione.	Nessun KB necessario per risolvere il problema.
Sono disponibili host ESXi partner?	Nodo	Rendere disponibili uno o più host ESXi nel cluster (non in modalità di manutenzione) per la migrazione delle macchine virtuali.	Nessun KB necessario per risolvere il problema.
Sei in grado di connetterti a BMC tramite il protocollo IPMI?	Nodo	Abilitare il protocollo IPMI su Baseboard Management Controller (BMC).	Nessun KB necessario per risolvere il problema.

Controllare la descrizione	Nodo/cluster	Azione necessaria per risolvere il problema	Articolo della Knowledge base con procedura
L'host ESXi è mappato correttamente all'host hardware (BMC)?	Nodo	L'host ESXi non è mappato correttamente al Baseboard Management Controller (BMC). Correggere la mappatura tra host ESXi e host hardware.	Nessun KB necessario per risolvere il problema. Vedere "questo articolo" per ulteriori informazioni.
Qual è lo stato dei nodi di controllo nel cluster? Nessuno dei nodi di controllo identificati è attivo e in esecuzione.	Nodo	Un nodo di controllo non è in esecuzione su un host ESXi alternativo. Accendere il nodo di controllo su un host ESXi alternativo ed eseguire nuovamente il controllo dello stato di salute. **Un nodo di controllo deve essere sempre in esecuzione nell'installazione HCI**.	"Consulta questa KB"
Qual è lo stato dei nodi di controllo nel cluster? Il nodo testimone è attivo e in esecuzione su questo host ESXi e il nodo testimone alternativo non è attivo e in esecuzione.	Nodo	Un nodo di controllo non è in esecuzione su un host ESXi alternativo. Accendere il nodo di controllo su un host ESXi alternativo. Quando si è pronti ad aggiornare questo host ESXi, arrestare il nodo di controllo in esecuzione su questo host ESXi ed eseguire nuovamente il controllo dello stato di salute. **Un nodo di controllo deve essere sempre in esecuzione nell'installazione HCI**.	"Consulta questa KB"

Controllare la descrizione	Nodo/cluster	Azione necessaria per risolvere il problema	Articolo della Knowledge base con procedura
Qual è lo stato dei nodi di controllo nel cluster? Il nodo testimone è attivo e in esecuzione su questo host ESXi e il nodo alternativo è attivo ma è in esecuzione sullo stesso host ESXi.	Nodo	Entrambi i nodi di controllo sono in esecuzione su questo host ESXi. Spostare un nodo di controllo su un host ESXi alternativo. Quando si è pronti ad aggiornare questo host ESXi, arrestare il nodo di controllo rimanente su questo host ESXi ed eseguire nuovamente il controllo dello stato di salute. **Un nodo di controllo deve essere sempre in esecuzione nell'installazione HCI**.	"Consulta questa KB"
Qual è lo stato dei nodi di controllo nel cluster? Il nodo testimone è attivo e in esecuzione su questo host ESXi e il nodo testimone alternativo è attivo e in esecuzione su un altro host ESXi.	Nodo	Un nodo di controllo è in esecuzione localmente su questo host ESXi. Quando si è pronti ad aggiornare questo host ESXi, arrestare il nodo di controllo solo su questo host ESXi ed eseguire nuovamente il controllo dello stato di salute. **Un nodo di controllo deve essere sempre in esecuzione nell'installazione HCI**.	"Consulta questa KB"

Trova ulteriori informazioni

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

Aggiornare i driver dei nodi di calcolo

Per qualsiasi nodo di calcolo della serie H, è possibile aggiornare i driver utilizzati sui nodi utilizzando VMware Update Manager.

Di cosa hai bisogno

Consultare la matrice del firmware e dei driver per l'hardware all'indirizzo "Versioni del firmware e dei driver ESXi supportate".

A proposito di questa attività

Eseguire una sola di queste operazioni di aggiornamento alla volta.

Prima di tentare di eseguire gli aggiornamenti del firmware di calcolo, controllare la versione corrente del driver ESXi. Se il driver non è aggiornato, aggiornarlo. Quindi, aggiornare il firmware di calcolo per i nodi di calcolo.

Fasi

1. Accedere a. "Download del software NetApp HCI" E selezionare il collegamento per scaricare la versione corretta di NetApp HCI.
2. Selezionare **ESXI_drivers** dall'elenco a discesa.
3. Accettare il Contratto di licenza con l'utente finale.
4. Scarica il pacchetto di driver per il tuo tipo di nodo e la versione di ESXi.
5. Estrarre il pacchetto di driver scaricato sul computer locale.

> Il bundle di driver NetApp include uno o più file ZIP VMware Offline Bundle; non estrarre questi file ZIP.

6. Accedere a **VMware Update Manager** in VMware vCenter.
7. Importare il file bundle offline del driver per i nodi di calcolo in **Patch Repository**.
   - Per VMware ESXi 7.0, tutti i driver necessari per i nodi di calcolo NetApp H610C, H615C, H410C e Hx00E e i relativi componenti di sistema integrati sono inclusi nell'immagine ISO di installazione standard di VMware ESXi 7.0. Non sono necessari driver aggiuntivi o aggiornati per i nodi di calcolo NetApp HCI che eseguono VMware ESXi 7.0 (e aggiornamenti).
   - Per VMware ESXi 6.x, attenersi alla seguente procedura per importare il file bundle offline del driver:
     i. Selezionare la scheda **aggiornamenti**.
     ii. SELEZIONARE **UPLOAD FROM FILE** (CARICA DA FILE).
     iii. Individuare il bundle offline scaricato in precedenza e selezionare **IMPORT**.
8. Creare una nuova baseline host per il nodo di calcolo.
9. Scegliere **host Extension** per Nome e tipo e selezionare tutti i pacchetti di driver importati da includere nella nuova linea di base.
10. Nel menu **host and Clusters** di vCenter, selezionare il cluster con i nodi di calcolo che si desidera aggiornare e passare alla scheda **Update Manager**.
11. Selezionare **bonifica** e selezionare la baseline dell'host appena creata. Assicurarsi che siano selezionati i driver inclusi nella linea di base.
12. Passare alla procedura guidata **Opzioni di correzione dell'host** e assicurarsi che l'opzione **Do Not Change VM Power state** (non modificare lo stato di alimentazione della macchina virtuale) sia selezionata per mantenere le macchine virtuali in linea durante l'aggiornamento del driver.

> Se VMware Distributed Resource Scheduler (DRS) è attivato sul cluster (impostazione predefinita nelle installazioni NetApp HCI), le macchine virtuali vengono migrate automaticamente in altri nodi del cluster.

13. Passare alla pagina **Pronto per il completamento** della procedura guidata e selezionare **fine**.

    I driver per tutti i nodi di calcolo nel cluster vengono aggiornati un nodo alla volta, mentre le macchine virtuali rimangono online.

Trova ulteriori informazioni

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

Aggiornare il firmware del nodo di calcolo

Per i nodi di calcolo della serie H, è possibile aggiornare il firmware per i componenti hardware come BMC, BIOS e NIC. Per aggiornare il firmware del nodo di calcolo, è possibile utilizzare l'interfaccia utente di NetApp Hybrid Cloud Control, l'API REST, un'unità USB con l'immagine firmware più recente o l'interfaccia utente BMC.

Dopo l'aggiornamento, il nodo di calcolo si avvia in ESXi e funziona come prima, mantenendo la configurazione.

Di cosa hai bisogno

- **Compute Drivers**: Hai aggiornato i driver dei nodi di calcolo. Se i driver dei nodi di calcolo non sono compatibili con il nuovo firmware, l'aggiornamento non viene avviato. Vedere "Tool di matrice di interoperabilità (IMT)" per informazioni sulla compatibilità di driver e firmware, consultare la versione più recente "note di rilascio del firmware del nodo di calcolo" per informazioni importanti su firmware e driver all'avanguardia.
- **Privilegi di amministratore**: Si dispone delle autorizzazioni di amministratore del cluster e BMC per eseguire l'aggiornamento.
- **Porte di sistema**: Se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, si è assicurati che le porte necessarie siano aperte. Vedere "Porte di rete" per ulteriori informazioni.
- **Versioni minime di BMC e BIOS**: Il nodo che intendi aggiornare utilizzando NetApp Hybrid Cloud Control soddisfa i seguenti requisiti minimi:

Modello	Versione minima di BMC	Versione minima del BIOS
H410C	Tutte le versioni supportate (non è richiesto alcun aggiornamento)	Tutte le versioni supportate (non è richiesto alcun aggiornamento)
H610C	3.96.07	3B01
H615C	4.68.07	3B08.CO

> I nodi di calcolo H615C devono aggiornare il firmware BMC alla versione 4.68 utilizzando "bundle firmware di calcolo 2.27" Per consentire a NetApp Hybrid Cloud Control di eseguire futuri aggiornamenti del firmware.

> Per una matrice completa di firmware e firmware del driver per l'hardware, vedere "Versioni del firmware e dei driver ESXi supportate".

- **BIOS boot order** (Ordine di avvio del BIOS): Modificare manualmente l'ordine di avvio nella configurazione del BIOS per ciascun nodo per garantire `USB CD/DVD` viene visualizzato nell'elenco di avvio. Vedi questo "articolo" per ulteriori informazioni.
- **Credenziali BMC**: Aggiornare le credenziali utilizzate da NetApp Hybrid Cloud Control per connettersi al nodo di calcolo BMC. Puoi farlo utilizzando il NetApp Hybrid Cloud Control "INTERFACCIA UTENTE" oppure "API". L'aggiornamento delle informazioni BMC prima dell'aggiornamento aggiorna l'inventario e garantisce che i servizi dei nodi di gestione siano a conoscenza di tutti i parametri hardware necessari per completare l'aggiornamento.

- **Supporto collegato**: Scollegare qualsiasi USB o ISO fisico prima di avviare un aggiornamento del nodo di calcolo.
- Console **KVM ESXi**: Chiudere tutte le sessioni Serial-over-LAN (Sol) aperte e le sessioni KVM attive nell'interfaccia utente BMC prima di avviare un aggiornamento del nodo di calcolo.
- **Requisiti del nodo di controllo**: In cluster di storage a due e tre nodi, uno "Nodo di controllo" Deve essere sempre in esecuzione nell'installazione di NetApp HCI.
- **Verifica dello stato del nodo di calcolo**: È stato verificato che il nodo è pronto per l'aggiornamento. Vedere "Eseguire i controlli dello stato dei nodi di calcolo prima di aggiornare il firmware di calcolo".
- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare il firmware del nodo di calcolo:
  a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

  ```
  https://<ManagementNodeIP>
  ```

  b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
  c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
  d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

A proposito di questa attività

Negli ambienti di produzione, aggiornare il firmware su un nodo di calcolo alla volta.

> L'host ESXi deve essere disattivato dalla modalità di blocco prima di eseguire un controllo dello stato di salute e procedere con l'aggiornamento del firmware. Vedere "Come disattivare la modalità di blocco sull'host ESXi" e. "Comportamento della modalità di blocco VMware" per ulteriori informazioni.

Per gli aggiornamenti API o dell'interfaccia utente di NetApp Hybrid Cloud Control, l'host ESXi verrà automaticamente impostato in modalità di manutenzione durante il processo di aggiornamento, se si dispone della funzione DRS e delle licenze richieste. Il nodo verrà riavviato e, una volta completato il processo di aggiornamento, l'host ESXi verrà disattivato dalla modalità di manutenzione. Per le opzioni dell'interfaccia utente di USB e BMC, è necessario impostare manualmente l'host ESXi in modalità di manutenzione, come descritto in ciascuna procedura.

> Prima di eseguire l'aggiornamento, verificare la versione corrente del driver ESXi. Se il driver non è aggiornato, aggiornarlo. Quindi, aggiornare il firmware di calcolo per i nodi di calcolo.

Opzioni di upgrade

Scegliere l'opzione appropriata per lo scenario di aggiornamento:

- Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare un nodo di calcolo (Consigliato)
- Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare un nodo di calcolo
- Utilizza un'unità USB con l'immagine del più recente bundle di firmware di calcolo
- Utilizzo dell'interfaccia utente (UI) del Baseboard Management Controller (BMC)

Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare un nodo di calcolo

A partire dai servizi di gestione 2.14, è possibile aggiornare un nodo di calcolo utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control. Dall'elenco dei nodi, selezionare il nodo da aggiornare. La scheda **Current Versions** (versioni correnti) mostra le versioni correnti del firmware e la scheda **Proposed Versions** (versioni proposte) mostra le eventuali versioni di aggiornamento disponibili.

> Per un aggiornamento corretto, assicurarsi che il controllo dello stato di salute del cluster vSphere sia stato eseguito correttamente.

> L'aggiornamento di NIC, BIOS e BMC può richiedere circa 60 minuti per nodo, a seconda della velocità di connettività di rete tra il nodo di gestione e l'host BMC.

> L'utilizzo dell'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware di calcolo sui nodi di calcolo H300E/H500E/H700E non è più supportato. Per eseguire l'aggiornamento, utilizzare un Unità USB o il INTERFACCIA UTENTE BMC per montare il bundle del firmware di calcolo.

Di cosa hai bisogno

- Se il nodo di gestione non è connesso a Internet, il bundle del firmware di calcolo è stato scaricato da "Sito di supporto NetApp".

  > Estrarre il `TAR.GZ` file su a. `TAR` ed estrarre il `TAR` file nel bundle del firmware di calcolo.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare **Compute firmware** (calcolo firmware).
5. Selezionare il cluster da aggiornare.

   Verranno visualizzati i nodi nel cluster elencati insieme alle versioni del firmware correnti e alle versioni più recenti, se disponibili per l'aggiornamento.

6. Selezionare **Browse** (Sfoglia) per caricare il bundle del firmware di calcolo scaricato da "Sito di supporto NetApp".
7. Attendere il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento.

   > Il caricamento del file avviene in background se ci si allontana dalla finestra del browser.

   Una volta caricato e validato il file, viene visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere alcuni minuti.

8. Selezionare il bundle del firmware di calcolo.

9. Selezionare **Avvia aggiornamento**.

   Dopo aver selezionato **Begin Upgrade** (Avvia aggiornamento), nella finestra vengono visualizzati i controlli di integrità non riusciti, se presenti.

   > L'aggiornamento non può essere messo in pausa dopo l'inizio. Il firmware verrà aggiornato in sequenza nel seguente ordine: NIC, BIOS e BMC. Non accedere all'interfaccia utente BMC durante l'aggiornamento. L'accesso al BMC termina la sessione Sol (Serial-over-LAN) di Hybrid Cloud Control che monitora il processo di aggiornamento.

10. Se i controlli di integrità a livello di cluster o nodo vengono superati con avvisi, ma senza errori critici, viene visualizzato **Ready to be upgrade** (Pronto per l'aggiornamento). Selezionare **Aggiorna nodo**.

    > Mentre l'aggiornamento è in corso, è possibile uscire dalla pagina e tornare ad essa in un secondo momento per continuare a monitorare i progressi. Durante l'aggiornamento, l'interfaccia utente visualizza diversi messaggi sullo stato dell'aggiornamento.

    > Durante l'aggiornamento del firmware sui nodi di calcolo H610C e H615C, non aprire la console Serial-over-LAN (Sol) attraverso l'interfaccia utente Web BMC. Questo potrebbe causare un errore nell'aggiornamento.

    Al termine dell'aggiornamento, l'interfaccia utente visualizza un messaggio. Una volta completato l'aggiornamento, è possibile scaricare i registri. Per informazioni sulle varie modifiche dello stato dell'aggiornamento, vedere Lo stato dell'aggiornamento cambia.

    > Se si verifica un errore durante l'aggiornamento, NetApp Hybrid Cloud Control riavvierà il nodo, ne disconnetterà la modalità di manutenzione e visualizzerà lo stato di errore con un link al registro degli errori. È possibile scaricare il log degli errori, che contiene istruzioni specifiche o collegamenti agli articoli della Knowledge base, per diagnosticare e correggere qualsiasi problema. Per ulteriori informazioni sui problemi di aggiornamento del firmware del nodo di calcolo con NetApp Hybrid Cloud Control, consulta questo articolo "KB" articolo.

Lo stato dell'aggiornamento cambia

Di seguito sono riportati i diversi stati visualizzati dall'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Il nodo non ha superato uno o più controlli di integrità. Espandere per visualizzare i dettagli.	Uno o più controlli di integrità non sono riusciti.
Errore	Si è verificato un errore durante l'aggiornamento. È possibile scaricare il registro degli errori e inviarlo al supporto NetApp.
Impossibile rilevare	Questo stato viene visualizzato se NetApp Hybrid Cloud Control non è in grado di eseguire query sul nodo di calcolo quando la risorsa del nodo di calcolo non dispone del tag hardware.
Pronto per l'aggiornamento.	Tutti i controlli di integrità sono stati superati e il nodo è pronto per essere aggiornato.

Stato di aggiornamento	Descrizione
Si è verificato un errore durante l'aggiornamento.	L'aggiornamento non riesce con questa notifica quando si verifica un errore critico. Scaricare i registri selezionando il collegamento **Download Logs** per risolvere l'errore. Dopo aver risolto l'errore, riprovare ad eseguire l'aggiornamento.
Aggiornamento del nodo in corso.	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento.

Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare un nodo di calcolo

È possibile utilizzare le API per aggiornare ciascun nodo di calcolo di un cluster alla versione più recente del firmware. È possibile utilizzare uno strumento di automazione a scelta per eseguire le API. Il flusso di lavoro API qui documentato utilizza l'interfaccia utente REST API disponibile sul nodo di gestione come esempio.

> L'utilizzo dell'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware di calcolo sui nodi di calcolo H300E/H500E/H700E non è più supportato. Per eseguire l'aggiornamento, utilizzare un Unità USB o il INTERFACCIA UTENTE BMC per montare il bundle del firmware di calcolo.

Di cosa hai bisogno

Le risorse dei nodi di calcolo, incluse le risorse vCenter e hardware, devono essere note alle risorse dei nodi di gestione. È possibile utilizzare le API del servizio di inventario per verificare le risorse (`https://<ManagementNodeIP>/inventory/1/`).

Fasi

1. Accedere al software NetApp HCI "pagina di download" e scaricare l'ultimo bundle di firmware di calcolo su un dispositivo accessibile al nodo di gestione.
2. Caricare il bundle del firmware di calcolo nel nodo di gestione:
   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/package-repository/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Dall'interfaccia utente API REST, selezionare **POST /packages**.
   d. Selezionare **Provalo**.
   e. Selezionare **Browse** (Sfoglia) e selezionare il bundle del firmware di calcolo.
   f. Selezionare **Esegui** per avviare il caricamento.
   g. Dalla risposta, copiare e salvare l'ID bundle del firmware di calcolo (`"id"`) da utilizzare in un passaggio successivo.

3. Verificare lo stato del caricamento.
   a. Dall'interfaccia utente API REST, selezionare **GET /packages/{id}/status**.
   b. Selezionare **Provalo**.
   c. Inserire l'ID del pacchetto copiato nel passaggio precedente in **id**.
   d. Selezionare **Esegui** per avviare la richiesta di stato.

      La risposta indica `state` come `SUCCESS` al termine dell'operazione.

   e. Dalla risposta, copiare e salvare il nome del bundle del firmware di calcolo (`"name"`) e la versione (`"version"`) da utilizzare in un passaggio successivo.
4. Individuare l'ID del controller di calcolo e l'ID hardware del nodo da aggiornare:
   a. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   d. Selezionare **Provalo**.
   e. Selezionare **Esegui**.
   f. Dalla risposta, copiare l'ID della risorsa di installazione (`"id"`).
   g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.
   h. Selezionare **Provalo**.
   i. Incollare l'ID della risorsa di installazione nel campo **id**.
   j. Selezionare **Esegui**.
   k. Dalla risposta, copiare e salvare l'ID del controller del cluster (`"controllerId"`) E l'ID hardware del nodo (`"hardwareId"`) per l'utilizzo in un passaggio successivo:

      ```
      "compute": {
        "errors": [],
        "inventory": {
          "clusters": [
            {
              "clusterId": "Test-1B",
              "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
      ```

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.111.0.111",
      "credentialsAvailable": true,
      "credentialsValidated": true
    },
    "chassisSerialNumber": "111930011231",
    "chassisSlot": "D",
    "hardwareId": "123a4567-01b1-1243-a12b-11ab11ab0a15",
    "hardwareTag": "00000000-0000-0000-0000-ab1c2de34f5g",
    "id": "e1111d10-1a1a-12d7-1a23-ab1cde23456f",
    "model": "H410C",
```

5. Eseguire l'aggiornamento del firmware del nodo di calcolo:
   a. Aprire l'interfaccia utente dell'API REST del servizio hardware sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/hardware/2/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Selezionare **POST /nodi/{hardware_id}/upgrade**.
   d. Selezionare **Provalo**.
   e. Inserire l'ID della risorsa host hardware (`"hardwareId"` salvato da un passo precedente) nel campo dei parametri.
   f. Eseguire le seguenti operazioni con i valori del payload:
      i. Conservare i valori `"force": false` e. `"maintenanceMode": true"` In modo che i controlli di integrità vengano eseguiti sul nodo e che l'host ESXi sia impostato sulla modalità di manutenzione.
      ii. Inserire l'ID del controller del cluster (`"controllerId"` salvato da un passaggio precedente).
      iii. Inserire il nome e la versione del bundle del firmware di calcolo salvati in un passaggio precedente.

```
{
  "config": {
    "force": false,
    "maintenanceMode": true
  },
  "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
  "packageName": "compute-firmware-12.2.109",
  "packageVersion": "12.2.109"
}
```

g. Selezionare **Esegui** per avviare l'aggiornamento.

> L'aggiornamento non può essere messo in pausa dopo l'inizio. Il firmware verrà aggiornato in sequenza nel seguente ordine: NIC, BIOS e BMC. Non accedere all'interfaccia utente BMC durante l'aggiornamento. L'accesso al BMC termina la sessione Sol (Serial-over-LAN) di Hybrid Cloud Control che monitora il processo di aggiornamento.

h. Copiare l'ID dell'attività di aggiornamento che fa parte del link delle risorse (`"resourceLink"`) Nella risposta.

6. Verificare l'avanzamento e i risultati dell'aggiornamento:

   a. Selezionare **GET /task/{task_id}/logs**.

   b. Selezionare **Provalo**.

   c. Inserire l'ID attività del passaggio precedente in **task_Id**.

   d. Selezionare **Esegui**.

   e. In caso di problemi o requisiti speciali durante l'aggiornamento, eseguire una delle seguenti operazioni:

Opzione	Fasi
È necessario correggere i problemi di integrità del cluster dovuti a. `failedHealthChecks` messaggio nel corpo della risposta.	i. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata. ii. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base. iii. Una volta risolti i problemi del cluster, eseguire nuovamente l'autenticazione, se necessario, e selezionare **POST /nodes/{hardware_id}/upgrade**. iv. Ripetere i passaggi descritti in precedenza nella fase di aggiornamento.
L'aggiornamento non riesce e i passaggi di mitigazione non sono elencati nel log di aggiornamento.	i. Vedi questo "Articolo della Knowledge base" (accesso richiesto).

f. Eseguire l'API **GET /task/{task_id}/logs** più volte, in base alle necessità, fino al completamento del processo.

   Durante l'aggiornamento, il `status` indica `running` se non si riscontrano errori. Al termine di ogni fase, il `status` il valore cambia in `completed`.

L'aggiornamento è stato completato correttamente quando lo stato di ogni passaggio è `completed` e a. `percentageCompleted` il valore è `100`.

7. (Facoltativo) confermare le versioni del firmware aggiornate per ciascun componente:
   a. Aprire l'interfaccia utente dell'API REST del servizio hardware sul nodo di gestione:

```
https://<ManagementNodeIP>/hardware/2/
```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Dall'interfaccia utente API REST, selezionare **GET /nodes/{hardware_id}/upgrade**.
   d. (Facoltativo) inserire i parametri di data e stato per filtrare i risultati.
   e. Inserire l'ID della risorsa host hardware (`"hardwareId"` salvato da un passo precedente) nel campo dei parametri.
   f. Selezionare **Provalo**.
   g. Selezionare **Esegui**.
   h. Verificare nella risposta che il firmware per tutti i componenti sia stato aggiornato correttamente dalla versione precedente alla versione più recente.

Utilizza un'unità USB con l'immagine del più recente bundle di firmware di calcolo

È possibile inserire un'unità USB con il pacchetto di firmware di calcolo più recente scaricato su una porta USB del nodo di calcolo. In alternativa all'utilizzo del metodo USB thumb drive descritto in questa procedura, è possibile montare il bundle del firmware di calcolo sul nodo di calcolo utilizzando l'opzione **Virtual CD/DVD** nella console virtuale nell'interfaccia Baseboard Management Controller (BMC). Il metodo BMC impiega molto più tempo del metodo USB thumb drive. Assicurarsi che la workstation o il server disponga della larghezza di banda di rete necessaria e che la sessione del browser con BMC non sia in timeout.

Di cosa hai bisogno

- Se il nodo di gestione non è connesso a Internet, il bundle del firmware di calcolo è stato scaricato da "Sito di supporto NetApp".

> Estrarre il `TAR.GZ` file su a. `TAR` ed estrarre il `TAR` file nel bundle del firmware di calcolo.

Fasi

1. Utilizzare l'utility etcher per aggiornare il bundle del firmware di calcolo su un'unità USB.

2. Impostare il nodo di calcolo in modalità di manutenzione utilizzando VMware vCenter e svuotare tutte le macchine virtuali dall'host.

> Se VMware Distributed Resource Scheduler (DRS) è attivato sul cluster (impostazione predefinita nelle installazioni NetApp HCI), le macchine virtuali vengono migrate automaticamente in altri nodi del cluster.

3. Inserire la chiavetta USB in una porta USB sul nodo di calcolo e riavviare il nodo di calcolo utilizzando VMware vCenter.
4. Durante il ciclo POST del nodo di calcolo, premere **F11** per aprire Boot Manager. Potrebbe essere necessario premere **F11** più volte in rapida successione. È possibile eseguire questa operazione collegando un video/una tastiera o utilizzando la console in `BMC`.
5. Selezionare **One Shot** > **USB Flash Drive** dal menu visualizzato. Se la chiavetta USB non viene visualizzata nel menu, verificare che l'unità flash USB faccia parte dell'ordine di avvio precedente nel BIOS del sistema.
6. Premere **Invio** per avviare il sistema dalla chiavetta USB. Viene avviato il processo di aggiornamento del firmware.

   Una volta completato il flash del firmware e riavviato il nodo, l'avvio di ESXi potrebbe richiedere alcuni minuti.

7. Una volta completato il riavvio, uscire dalla modalità di manutenzione sul nodo di calcolo aggiornato utilizzando vCenter.
8. Rimuovere l'unità flash USB dal nodo di calcolo aggiornato.
9. Ripetere questa attività per gli altri nodi di calcolo nel cluster ESXi fino a quando tutti i nodi di calcolo non vengono aggiornati.

Utilizzo dell'interfaccia utente (UI) del Baseboard Management Controller (BMC)

È necessario eseguire le operazioni sequenziali per caricare il bundle del firmware di calcolo e riavviare il nodo nel bundle del firmware di calcolo per garantire che l'aggiornamento sia stato eseguito correttamente. Il bundle del firmware di calcolo deve trovarsi sul sistema o sulla macchina virtuale (VM) che ospita il browser Web. Prima di avviare il processo, verificare di aver scaricato il bundle del firmware di calcolo.

> Si consiglia di avere il sistema o la macchina virtuale e il nodo sulla stessa rete.

> L'aggiornamento tramite l'interfaccia utente BMC richiede da 25 a 30 minuti circa.

- Aggiornare il firmware sui nodi H410C e H300E/H500E/H700E
- Aggiornare il firmware sui nodi H610C/H615C

Aggiornare il firmware sui nodi H410C e H300E/H500E/H700E

Se il nodo fa parte di un cluster, è necessario impostare il nodo in modalità di manutenzione prima dell'aggiornamento e portarlo fuori dalla modalità di manutenzione dopo l'aggiornamento.

> Ignorare il seguente messaggio informativo visualizzato durante il processo: `Untrusty Debug Firmware Key is used, SecureFlash is currently in Debug Mode`

Fasi

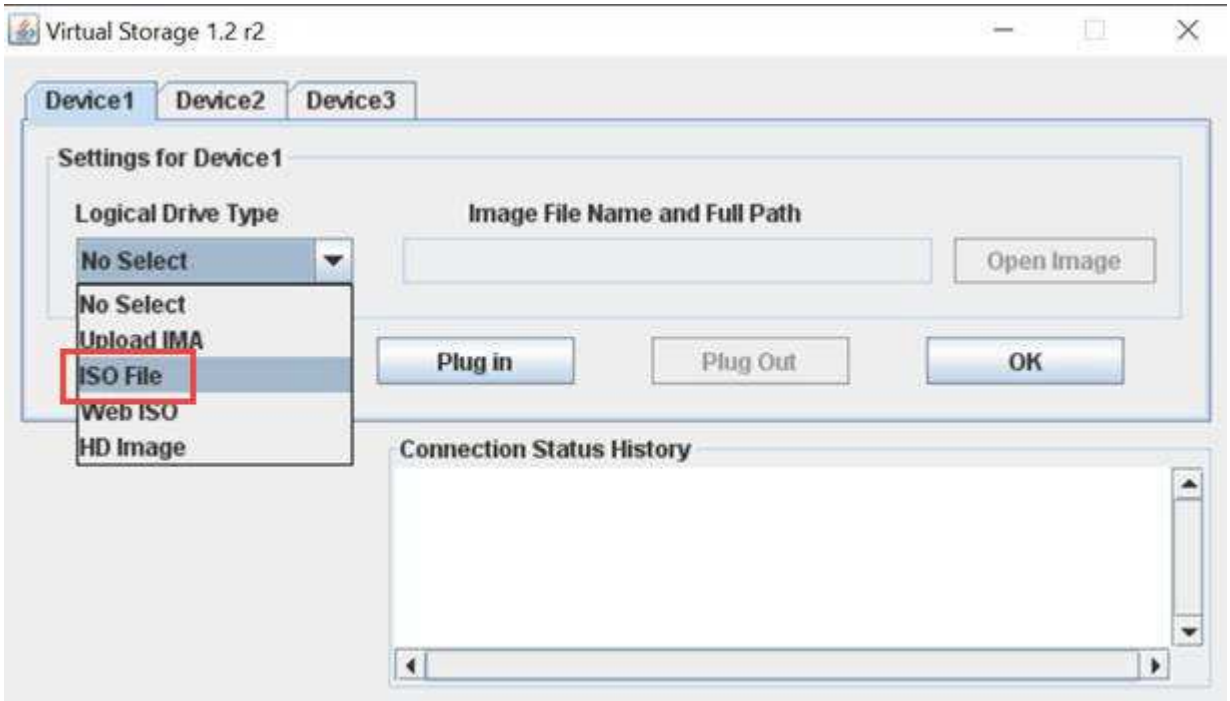
1. Se il nodo fa parte di un cluster, metterlo in modalità di manutenzione come indicato di seguito. In caso contrario, passare alla fase 2.
   a. Accedere al client Web di VMware vCenter.
   b. Fare clic con il pulsante destro del mouse sul nome dell'host (nodo di calcolo) e selezionare **Maintenance Mode (modalità di manutenzione) > Enter Maintenance Mode (attiva modalità di manutenzione)**.
   c. Selezionare **OK**. Le VM sull'host verranno migrate su un altro host disponibile. La migrazione delle macchine virtuali può richiedere tempo a seconda del numero di macchine virtuali da migrare.

   > Prima di procedere, assicurarsi che tutte le macchine virtuali dell'host vengano migrate.

2. Accedere all'interfaccia utente BMC, `https://BMCIP/#login`, Dove BMCIP è l'indirizzo IP del BMC.
3. Accedere utilizzando le credenziali.
4. Selezionare **Remote Control > Console Redirection** (controllo remoto > reindirizzamento console).
5. Selezionare **Launch Console** (Avvia console).

   > Potrebbe essere necessario installare Java o aggiornarlo.

6. All'apertura della console, selezionare **Virtual Media > Virtual Storage**.
7. Nella schermata **Virtual Storage**, selezionare **Logical Drive Type** (tipo di unità logica) e selezionare **ISO file**.

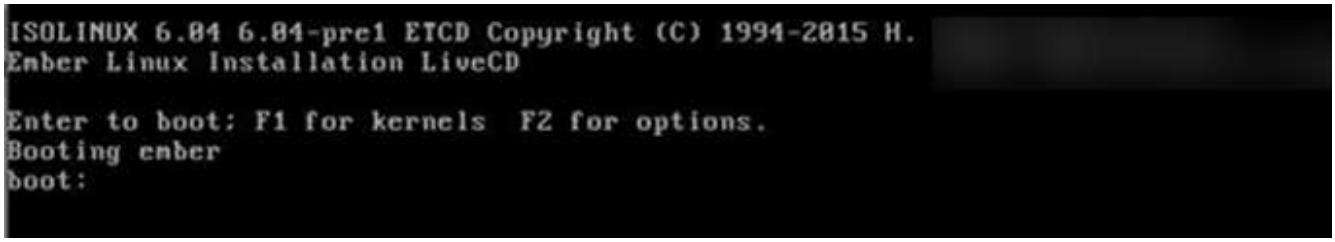


8. Selezionare **Open Image** (Apri immagine) per accedere alla cartella in cui è stato scaricato il file bundle del firmware di calcolo e selezionare il file bundle del firmware di calcolo.
9. Selezionare **Plug-in**.
10. Quando viene visualizzato lo stato della connessione `Device#: VM Plug-in OK!!`, Selezionare **OK**.
11. Riavviare il nodo premendo **F12** e selezionando **Riavvia** o selezionando **controllo alimentazione >**

Imposta ripristino alimentazione.

12. Durante il riavvio, premere **F11** per selezionare le opzioni di avvio e caricare il bundle del firmware di calcolo. Potrebbe essere necessario premere F11 alcune volte prima che venga visualizzato il menu di avvio.

    Viene visualizzata la seguente schermata:



13. Nella schermata precedente, premere **Invio**. A seconda della rete in uso, potrebbero essere necessari alcuni minuti dopo aver premuto **Invio** per l'avvio dell'aggiornamento.

    > Alcuni aggiornamenti del firmware potrebbero causare la disconnessione della console e/o la disconnessione della sessione sul BMC. È possibile accedere nuovamente a BMC, tuttavia alcuni servizi, come la console, potrebbero non essere disponibili a causa degli aggiornamenti del firmware. Una volta completati gli aggiornamenti, il nodo esegue un riavvio a freddo, che può richiedere circa cinque minuti.

14. Accedere nuovamente all'interfaccia utente BMC e selezionare **System** per verificare la versione del BIOS e il tempo di creazione dopo l'avvio del sistema operativo. Se l'aggiornamento è stato completato correttamente, vengono visualizzate le nuove versioni di BIOS e BMC.

    > La versione del BIOS non mostrerà la versione aggiornata fino a quando il nodo non avrà completato l'avvio.

15. Se il nodo fa parte di un cluster, completare la procedura riportata di seguito. Se si tratta di un nodo standalone, non sono necessarie ulteriori azioni.
    a. Accedere al client Web di VMware vCenter.
    b. Portare l'host fuori dalla modalità di manutenzione. Potrebbe essere visualizzato un segnale d'allarme disconnesso. Attendere che tutti gli stati siano cancellati.
    c. Accendere tutte le macchine virtuali rimanenti che sono state spente.

Aggiornare il firmware sui nodi H610C/H615C

I passaggi variano a seconda che il nodo sia standalone o parte di un cluster. La procedura può richiedere circa 25 minuti e comprende lo spegnimento del nodo, il caricamento del bundle del firmware di calcolo, l'aggiornamento dei dispositivi e la riaccensione del nodo dopo l'aggiornamento.

Fasi

1. Se il nodo fa parte di un cluster, metterlo in modalità di manutenzione come indicato di seguito. In caso contrario, passare alla fase 2.
    a. Accedere al client Web di VMware vCenter.
    b. Fare clic con il pulsante destro del mouse sul nome dell'host (nodo di calcolo) e selezionare **Maintenance Mode (modalità di manutenzione) > Enter Maintenance Mode (attiva modalità di manutenzione)**.

c. Selezionare **OK**. Le VM sull'host verranno migrate su un altro host disponibile. La migrazione delle macchine virtuali può richiedere tempo a seconda del numero di macchine virtuali da migrare.

> Prima di procedere, assicurarsi che tutte le macchine virtuali dell'host vengano migrate.

2. Accedere all'interfaccia utente BMC, `https://BMCIP/#login`, Dove BMC IP è l'indirizzo IP del BMC.
3. Accedere utilizzando le credenziali.
4. Selezionare **Remote Control > Launch KVM (Java)**.
5. Nella finestra della console, selezionare **Media > Virtual Media Wizard**.

6. Selezionare **Browse** (Sfoglia) e selezionare il firmware di calcolo `.iso` file.
7. Selezionare **Connect**. Viene visualizzata una finestra a comparsa che indica il successo, insieme al percorso e al dispositivo visualizzati in basso. È possibile chiudere la finestra **Virtual Media**.

8. Riavviare il nodo premendo **F12** e selezionando **Riavvia** o selezionando **controllo alimentazione > Imposta ripristino alimentazione**.
9. Durante il riavvio, premere **F11** per selezionare le opzioni di avvio e caricare il bundle del firmware di calcolo.
10. Selezionare **AMI Virtual CDROM** dall'elenco visualizzato e selezionare **Invio**. Se nell'elenco non viene visualizzato AMI Virtual CDROM, accedere al BIOS e attivarlo nell'elenco di avvio. Il nodo viene riavviato dopo il salvataggio. Durante il riavvio, premere **F11**.

11. Nella schermata visualizzata, selezionare **Invio**.

> Alcuni aggiornamenti del firmware potrebbero causare la disconnessione della console e/o la disconnessione della sessione sul BMC. È possibile accedere nuovamente a BMC, tuttavia alcuni servizi, come la console, potrebbero non essere disponibili a causa degli aggiornamenti del firmware. Una volta completati gli aggiornamenti, il nodo esegue un riavvio a freddo, che può richiedere circa cinque minuti.

12. Se ci si disconnette dalla console, selezionare **Remote Control** e selezionare **Launch KVM** or **Launch KVM (Java)** per riconnettersi e verificare quando il nodo ha terminato il backup. Potrebbero essere necessarie più riconnessione per verificare che il nodo sia stato avviato correttamente.

> Durante il processo di accensione, per circa cinque minuti, la console KVM visualizza **Nessun segnale**.

13. Una volta acceso il nodo, selezionare **Dashboard > Device Information > More info** (pannello di controllo > informazioni dispositivo > ulteriori informazioni) per verificare le versioni del BIOS e del BMC. Vengono visualizzate le versioni aggiornate del BIOS e di BMC. La versione aggiornata del BIOS non viene visualizzata fino a quando il nodo non si è avviato completamente.
14. Se il nodo è stato impostato in modalità di manutenzione, dopo l'avvio del nodo in ESXi, fare clic con il pulsante destro del mouse sul nome dell'host (nodo di calcolo) e selezionare **modalità di manutenzione > Esci dalla modalità di manutenzione**, quindi eseguire nuovamente la migrazione delle macchine virtuali nell'host.
15. In vCenter, con il nome host selezionato, configurare e verificare la versione del BIOS.

Trova ulteriori informazioni

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

Automatizza gli aggiornamenti del firmware dei nodi di calcolo con Ansible

È possibile aggiornare il firmware di sistema sui nodi di calcolo NetApp HCI, incluso il firmware per componenti come BMC, BIOS e NIC, utilizzando i flussi di lavoro in NetApp

Hybrid Cloud Control. Per le installazioni con cluster di calcolo di grandi dimensioni, è possibile automatizzare i flussi di lavoro utilizzando Ansible per eseguire un aggiornamento continuo dell'intero cluster.

> Mentre il ruolo Ansible per automatizzare gli aggiornamenti del firmware dei nodi di calcolo è reso disponibile da NetApp, l'automazione è un componente ausiliario che richiede una configurazione aggiuntiva e l'esecuzione di componenti software. La modifica dell'automazione Ansible è supportata solo con il massimo sforzo.

> Il ruolo Ansible per gli upgrade funziona solo sui nodi di calcolo NetApp HCI serie H. Non è possibile utilizzare questo ruolo per aggiornare i nodi di calcolo di terze parti.

Di cosa hai bisogno

- **Disponibilità e prerequisiti per gli aggiornamenti del firmware**: L'installazione di NetApp HCI deve essere pronta per l'aggiornamento del firmware, come indicato nelle istruzioni per "esecuzione degli aggiornamenti del firmware".
- **Possibilità di eseguire l'automazione sul nodo di controllo Ansible**: Un server fisico o virtuale per eseguire l'automazione dell'aggiornamento del firmware in Ansible.

A proposito di questa attività

In un ambiente di produzione, è necessario aggiornare i nodi di calcolo in un cluster in un'installazione NetApp HCI in modo variabile; un nodo alla volta, uno alla volta. Le API di NetApp Hybrid Cloud Control orchestrano il processo di aggiornamento del firmware del nodo di calcolo complessivo per un singolo nodo di calcolo, tra cui l'esecuzione di controlli dello stato di salute, il posizionamento di ESXi sui nodi di calcolo e il riavvio del nodo di calcolo per applicare gli aggiornamenti del firmware. Il ruolo Ansible consente di orchestrare l'aggiornamento del firmware per un gruppo di nodi di calcolo o interi cluster.

Inizia a utilizzare l'automazione dell'aggiornamento del firmware

Per iniziare, accedere a. "Repository NetApp Ansible su GitHub" e scaricare `nar_compute_nodes_firmware_upgrades` ruolo e documentazione.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"

Aggiorna i componenti vSphere per un sistema NetApp HCI con il plug-in Element per vCenter Server

Quando si aggiornano i componenti VMware vSphere dell'installazione di NetApp HCI, è necessario eseguire alcuni passaggi aggiuntivi per il plug-in Element per vCenter Server.

Fasi

1. Per gli aggiornamenti vCSA, "chiaro" Impostazioni QoSSIOC nel plug-in (**Configurazione NetApp Element > Impostazioni QoSSIOC**). Viene visualizzato il campo **QoSSIOC Status** `Not Configured` al termine del processo.
2. Per gli aggiornamenti vCSA e Windows, "annulla registrazione" Il plug-in di vCenter Server a cui è associato mediante l'utility di registrazione.
3. "Aggiornamento di vSphere, inclusi vCenter Server, ESXi, VM e altri componenti VMware".

> È necessario eseguire l'aggiornamento al plug-in NetApp Element per vCenter Server 5.0 o versioni successive per consentire di implementare il plug-in con VMware vCenter 7.0 Update 3 senza applicare una soluzione alternativa.
>
> Con Element Plug-in per vCenter Server 4.x, quando si esegue l'aggiornamento a VMware vCenter Server 7.0 Update 3, il plug-in 4.x non riesce a implementarlo. Per risolvere questo problema utilizzando Spring Framework 4, vedere "Questo articolo della Knowledge base".

> Durante l'aggiornamento di ESXi per nodi di calcolo per a. "cluster a due nodi", aggiornare solo un nodo di calcolo alla volta in modo che un solo nodo di controllo sia temporaneamente non disponibile e che sia possibile mantenere il quorum del cluster.

4. "Registrati" Il plug-in Element per vCenter Server con vCenter.
5. "Aggiungere cluster" utilizzando il plug-in.
6. "Configurare le impostazioni QoSSIOC" utilizzando il plug-in.
7. "Abilitare QoSSIOC" per tutti i datastore controllati dal plug-in.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"
- "Report tecnico sul cluster di storage a due nodi NetApp HCI"

Espandere il sistema NetApp HCI

Panoramica dell'espansione

Puoi espandere il tuo sistema NetApp HCI utilizzando il controllo del cloud ibrido NetApp. È possibile espandere le risorse di storage o di calcolo separatamente o allo stesso tempo.

> I nodi storage H610S nuovi e spare potrebbero avere requisiti di installazione aggiuntivi in base alla versione software Element esistente del cluster di storage. Per ulteriori informazioni, contatta il supporto NetApp.

Dopo aver installato il nodo nello chassis NetApp HCI, si utilizza il controllo del cloud ibrido NetApp per configurare NetApp HCI in modo che utilizzi le nuove risorse. NetApp HCI rileva la configurazione di rete esistente e offre opzioni di configurazione all'interno delle reti e delle VLAN esistenti, se presenti.

> Se l'installazione è stata recentemente ampliata e le nuove risorse non sono state aggiunte automaticamente alla configurazione, potrebbe essere necessario aggiungerle manualmente. Vedere "Panoramica del nodo di gestione".

NetApp HCI utilizza la compatibilità vMotion avanzata di VMware per garantire la funzionalità vMotion in presenza di nodi di calcolo con diverse generazioni di CPU nel cluster vSphere. Quando è necessario un EVC per l'espansione, NetApp HCI lo abilita automaticamente ogni volta che è possibile.

Nelle seguenti situazioni, potrebbe essere necessario modificare manualmente le impostazioni EVC nel client vSphere per completare l'espansione:

- I nodi di calcolo esistenti hanno una generazione di CPU più recente rispetto ai nodi di calcolo che si sta tentando di aggiungere.
- L'istanza vCenter di controllo non supporta il livello EVC richiesto.
- I nodi di calcolo che si sta tentando di aggiungere hanno una generazione di CPU precedente rispetto all'impostazione EVC dell'istanza vCenter di controllo.

> Quando si espandono le risorse di calcolo o storage NetApp HCI nel motore di implementazione NetApp, è necessario connettersi all'istanza di vCenter che gestisce i nodi di calcolo NetApp HCI esistenti.

Trova ulteriori informazioni

- "Espandere le risorse di calcolo di NetApp HCI"
- "Espandere le risorse di storage NetApp HCI"
- "Espandere le risorse di calcolo e storage NetApp HCI contemporaneamente"
- "Pagina delle risorse NetApp HCI"
- "Plug-in NetApp Element per server vCenter"

Espandere le risorse di storage NetApp HCI

Al termine dell'implementazione di NetApp HCI, puoi espandere e configurare le risorse di storage NetApp HCI utilizzando il controllo del cloud ibrido NetApp.

Prima di iniziare

- Assicurarsi di disporre di indirizzi IPv4 liberi e inutilizzati sullo stesso segmento di rete dei nodi esistenti (ciascun nuovo nodo deve essere installato sulla stessa rete dei nodi esistenti del suo tipo).
- Assicurarsi di disporre di uno dei seguenti tipi di account cluster di storage SolidFire:
  - L'account amministratore nativo creato durante la distribuzione iniziale
  - Un account utente personalizzato con autorizzazioni Cluster Admin, Drives, Volumes e Node
- Assicurarsi di aver eseguito le seguenti azioni con ogni nuovo nodo:
  - Ha installato il nuovo nodo nello chassis NetApp HCI seguendo la "istruzioni per l'installazione".
  - Collegato e acceso al nuovo nodo
- Assicurarsi di disporre dell'indirizzo IPv4 di gestione di un nodo di storage già installato. L'indirizzo IP si trova nella scheda **Gestione NetApp Element** > **cluster** > **nodi** del plug-in NetApp Element per vCenter Server.
- Assicurarsi che ogni nuovo nodo utilizzi la stessa topologia di rete e lo stesso cablaggio dei cluster di calcolo o di storage esistenti.

> Quando si espandono le risorse di storage, la capacità di storage deve essere suddivisa in modo uniforme in tutti gli chassis per ottenere la massima affidabilità.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Fare clic su **Espandi** nell'angolo in alto a destra dell'interfaccia.

   Il browser apre NetApp Deployment Engine.

4. Accedere al motore di implementazione NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI locale.

   > Non è possibile accedere utilizzando le credenziali Lightweight Directory Access Protocol.

5. Nella pagina **Benvenuto**, fare clic su **No** e fare clic su **continua**.
6. Nella pagina **Available Inventory** (inventario disponibile), selezionare i nodi di storage che si desidera aggiungere e fare clic su **Continue** (continua).
7. Nella pagina **Impostazioni di rete**, alcune informazioni di rete sono state rilevate dalla distribuzione iniziale. Ogni nuovo nodo di storage viene elencato in base al numero di serie ed è necessario assegnarvi le nuove informazioni di rete. Per ogni nuovo nodo di storage, attenersi alla seguente procedura:

a. **Nome host**: Se NetApp HCI ha rilevato un prefisso di denominazione, copiarlo dal campo prefisso di denominazione rilevato e inserirlo come prefisso per il nuovo nome host univoco aggiunto nel campo Nome host.

b. **Management Address** (Indirizzo di gestione): Immettere un indirizzo IP di gestione per il nuovo nodo di storage all'interno della subnet della rete di gestione.

c. **Storage (iSCSI) IP Address (Indirizzo IP storage (iSCSI))**: Inserire un indirizzo IP iSCSI per il nuovo nodo di storage all'interno della subnet di rete iSCSI.

d. Fare clic su **continua**.

> NetApp HCI potrebbe impiegare del tempo per convalidare gli indirizzi IP immessi. Il pulsante continua diventa disponibile al termine della convalida dell'indirizzo IP.

8. Nella pagina **Review** della sezione Network Settings (Impostazioni di rete), i nuovi nodi vengono visualizzati in grassetto. Per apportare modifiche in qualsiasi sezione, procedere come segue:

   a. Fare clic su **Edit** (Modifica) per la sezione.

   b. Al termine, fare clic su **continua** nelle pagine successive per tornare alla pagina di revisione.

9. **Opzionale**: Se non si desidera inviare statistiche del cluster e informazioni di supporto ai server Active IQ in hosting NetApp, deselezionare la casella di controllo finale.

   In questo modo si disattiva il monitoraggio diagnostico e dello stato di salute in tempo reale per NetApp HCI. La disattivazione di questa funzione elimina la possibilità per NetApp di supportare e monitorare in modo proattivo NetApp HCI per rilevare e risolvere i problemi prima che la produzione ne risenta.

10. Fare clic su **Aggiungi nodi**.

    È possibile monitorare l'avanzamento mentre NetApp HCI aggiunge e configura le risorse.

11. **Opzionale**: Verificare che i nuovi nodi di storage siano visibili nel plug-in Element per vCenter Server.

> Se si è espanso un cluster di storage a due nodi a quattro o più nodi, la coppia di nodi di controllo utilizzati in precedenza dal cluster di storage rimane visibile come macchine virtuali in standby in vSphere. Il nuovo cluster di storage espanso non li utilizza; se si desidera recuperare risorse di macchine virtuali, è possibile "rimuovere manualmente" Le macchine virtuali Witness Node.

Trova ulteriori informazioni

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

Espandere le risorse di calcolo di NetApp HCI

Una volta completata l'implementazione di NetApp HCI, puoi espandere e configurare le risorse di calcolo di NetApp HCI utilizzando il controllo del cloud ibrido NetApp.

Prima di iniziare

- Assicurarsi che l'istanza vSphere di NetApp HCI utilizzi la licenza vSphere Enterprise Plus se si sta espandendo un'implementazione con Virtual Distributed Switch.

- Assicurarsi che nessuna delle istanze vCenter o vSphere in uso con NetApp HCI disponga di licenze scadute.
- Assicurarsi di disporre di indirizzi IPv4 liberi e inutilizzati sullo stesso segmento di rete dei nodi esistenti (ciascun nuovo nodo deve essere installato sulla stessa rete dei nodi esistenti del suo tipo).
- Assicurarsi di disporre delle credenziali dell'account amministratore vCenter.
- Assicurarsi di aver eseguito le seguenti azioni con ogni nuovo nodo:
  - Ha installato il nuovo nodo nello chassis NetApp HCI seguendo la "istruzioni per l'installazione".
  - Collegato e acceso al nuovo nodo
- Assicurarsi che ogni nuovo nodo utilizzi la stessa topologia di rete e lo stesso cablaggio dei cluster di calcolo o di storage esistenti.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Fare clic su **Espandi** nell'angolo in alto a destra dell'interfaccia.

   Il browser apre NetApp Deployment Engine.

4. Accedere al motore di implementazione NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI locale.

   Non è possibile accedere utilizzando le credenziali Lightweight Directory Access Protocol.

5. Nella pagina **Benvenuto**, fare clic su **Sì** e fare clic su **continua**.
6. Nella pagina **licenza per l'utente finale**, leggere il contratto di licenza per l'utente finale VMware e fare clic su **Accetto** per accettare i termini e fare clic su **continua**.
7. Nella pagina **vCenter**, completare la seguente procedura:
   a. Immettere un indirizzo FQDN o IP e le credenziali di amministratore per l'istanza di vCenter associata all'installazione di NetApp HCI.
   b. Fare clic su **continua**.
   c. Selezionare un data center vSphere in cui aggiungere i nodi di calcolo oppure fare clic su **Create New Datacenter** (Crea nuovo data center) per aggiungere i nodi di calcolo a un nuovo data center.

      Se si fa clic su Create New Datacenter (Crea nuovo data center), il campo Cluster viene compilato automaticamente.

   d. Se è stato selezionato un data center esistente, selezionare un cluster vSphere a cui associare i nuovi nodi di calcolo.

> Se NetApp HCI non riconosce le impostazioni di rete del cluster selezionato per l'espansione, assicurarsi che il mapping vmkernel e vmnic per le reti di gestione, storage e vMotion sia impostato sui valori predefiniti di implementazione. Vedere "modifiche di rete supportate" per ulteriori informazioni.

   e. Fare clic su **continua**.

8. Nella pagina **credenziali ESXi**, immettere una password radice ESXi per il nodo di calcolo o i nodi che si desidera aggiungere.

   Utilizzare la stessa password creata durante la distribuzione iniziale di NetApp HCI.

9. Fare clic su **continua**.
10. Se è stato creato un nuovo cluster di data center vSphere, nella pagina **topologia di rete**, selezionare una topologia di rete che corrisponda ai nuovi nodi di calcolo che si stanno aggiungendo.

> Selezionare l'opzione due cavi solo se i nodi di calcolo utilizzano la topologia a due cavi e l'implementazione NetApp HCI esistente è configurata con ID VLAN.

11. Nella pagina **inventario disponibile**, selezionare i nodi che si desidera aggiungere all'installazione di NetApp HCI esistente.

> Per alcuni nodi di calcolo, potrebbe essere necessario abilitare EV al livello più elevato supportato dalla versione di vCenter prima di poterli aggiungere all'installazione. È necessario utilizzare il client vSphere per abilitare EVC per questi nodi di calcolo. Una volta attivata, aggiornare la pagina Inventory e provare ad aggiungere nuovamente i nodi di calcolo.

12. Fare clic su **continua**.
13. **Opzionale**: Se è stato creato un nuovo cluster di data center vSphere, nella pagina **Impostazioni di rete**, importare le informazioni di rete da un'implementazione NetApp HCI esistente selezionando la casella di controllo **Copia impostazione da un cluster esistente**.

    In questo modo vengono inserite le informazioni predefinite relative al gateway e alla subnet per ciascuna rete.

14. Nella pagina **Impostazioni di rete**, alcune informazioni di rete sono state rilevate dalla distribuzione iniziale. Ogni nuovo nodo di calcolo viene elencato in base al numero di serie ed è necessario assegnarvi nuove informazioni di rete. Per ogni nuovo nodo di calcolo, completare i seguenti passaggi:
    a. **Nome host**: Se NetApp HCI ha rilevato un prefisso di denominazione, copiarlo dal campo **prefisso di denominazione rilevato** e inserirlo come prefisso per il nuovo nome host.
    b. **Management IP Address** (Indirizzo IP di gestione): Immettere un indirizzo IP di gestione per il nuovo nodo di calcolo che si trova nella subnet della rete di gestione.
    c. **VMotion IP Address** (Indirizzo IP vMotion): Immettere un indirizzo IP vMotion per il nuovo nodo di calcolo all'interno della subnet di rete vMotion.
    d. **ISCSI A - Indirizzo IP**: Inserire un indirizzo IP per la prima porta iSCSI del nodo di calcolo presente nella subnet di rete iSCSI.
    e. **ISCSI B - Indirizzo IP**: Inserire un indirizzo IP per la seconda porta iSCSI del nodo di calcolo che si trova nella subnet di rete iSCSI
    f. Fare clic su **continua**.

15. Nella pagina **Review** della sezione Network Settings (Impostazioni di rete), i nuovi nodi vengono visualizzati in grassetto. Per apportare modifiche in qualsiasi sezione, procedere come segue:
    a. Fare clic su **Edit** (Modifica) per la sezione.
    b. Al termine, fare clic su **continua** nelle pagine successive per tornare alla pagina **Revisione**.
16. **Opzionale**: Se non si desidera inviare statistiche del cluster e informazioni di supporto ai server SolidFire Active IQ in hosting NetApp, deselezionare la casella di controllo finale.

    In questo modo si disattiva il monitoraggio diagnostico e dello stato di salute in tempo reale per NetApp HCI. La disattivazione di questa funzione elimina la possibilità per NetApp di supportare e monitorare in modo proattivo NetApp HCI per rilevare e risolvere i problemi prima che la produzione ne risenta.
17. Fare clic su **Aggiungi nodi**.

    È possibile monitorare l'avanzamento mentre NetApp HCI aggiunge e configura le risorse.
18. **Opzionale**: Verificare che i nuovi nodi di calcolo siano visibili in VMware vSphere Web Client.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Istruzioni per l'installazione e la configurazione dei nodi di calcolo e storage NetApp HCI"
- "VMware Knowledge base: Supporto avanzato del processore vMotion Compatibility (EVC)"

Espandere le risorse di calcolo e storage NetApp HCI contemporaneamente

Una volta completata l'implementazione di NetApp HCI, puoi espandere e configurare le risorse di calcolo e storage di NetApp HCI contemporaneamente utilizzando il controllo del cloud ibrido di NetApp.

Prima di iniziare

- Assicurarsi che l'istanza vSphere di NetApp HCI utilizzi la licenza vSphere Enterprise Plus se si sta espandendo un'implementazione con Virtual Distributed Switch.
- Assicurarsi che nessuna delle istanze vCenter o vSphere in uso con NetApp HCI disponga di licenze scadute.
- Assicurarsi di disporre delle credenziali dell'account amministratore vCenter.
- Assicurarsi di disporre di indirizzi IPv4 liberi e inutilizzati sullo stesso segmento di rete dei nodi esistenti (ciascun nuovo nodo deve essere installato sulla stessa rete dei nodi esistenti del suo tipo).
- Assicurarsi di disporre di uno dei seguenti tipi di account cluster di storage SolidFire:
    - L'account amministratore nativo creato durante la distribuzione iniziale
    - Un account utente personalizzato con autorizzazioni Cluster Admin, Drives, Volumes e Node
- Assicurarsi di aver eseguito le seguenti azioni con ogni nuovo nodo:
    - Ha installato il nuovo nodo nello chassis NetApp HCI seguendo la "istruzioni per l'installazione".
    - Collegato e acceso al nuovo nodo
- Assicurarsi di disporre dell'indirizzo IPv4 di gestione di un nodo di storage già installato. L'indirizzo IP si

trova nella scheda **Gestione NetApp Element** > **cluster** > **nodi** del plug-in NetApp Element per vCenter Server.

- Assicurarsi che ogni nuovo nodo utilizzi la stessa topologia di rete e lo stesso cablaggio dei cluster di calcolo o di storage esistenti.

A proposito di questa attività

- È possibile combinare il nodo di calcolo H410C con i nodi di calcolo e storage NetApp HCI esistenti nello stesso chassis e cluster.
- Non è possibile combinare nodi di calcolo e nodi di calcolo abilitati per BPU nello stesso cluster. Se si seleziona un nodo di calcolo abilitato alla GPU, i nodi di calcolo solo CPU diventano non selezionabili e viceversa.
- Se si aggiungono nodi di calcolo con generazioni di CPU diverse dalla generazione della CPU dei nodi di calcolo esistenti e l'opzione Enhanced vMotion Compatibility (EVC) è disattivata sull'istanza di vCenter di controllo, è necessario attivare EVC prima di procedere. Ciò garantisce la funzionalità vMotion al termine dell'espansione.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Fare clic su **Espandi** nell'angolo in alto a destra dell'interfaccia.

   Il browser apre NetApp Deployment Engine.

4. Accedere al motore di implementazione NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI locale.

   > Non è possibile accedere utilizzando le credenziali Lightweight Directory Access Protocol.

5. Nella pagina **Benvenuto**, fare clic su **Sì** e fare clic su **continua**.
6. Nella pagina **licenza per l'utente finale**, leggere il contratto di licenza per l'utente finale VMware e fare clic su **Accetto** per accettare i termini e fare clic su **continua**.
7. Nella pagina **vCenter**, completare la seguente procedura:
   a. Immettere un indirizzo FQDN o IP e le credenziali di amministratore per l'istanza di vCenter associata all'installazione di NetApp HCI.
   b. Fare clic su **continua**.
   c. Selezionare un data center vSphere in cui aggiungere i nodi di calcolo oppure fare clic su **Create New Datacenter** (Crea nuovo data center) per aggiungere i nodi di calcolo a un nuovo data center.

      > Se si fa clic su Create New Datacenter (Crea nuovo data center), il campo Cluster viene compilato automaticamente.

   d. Se è stato selezionato un data center esistente, selezionare un cluster vSphere a cui associare i nuovi nodi di calcolo.

> Se NetApp HCI non riconosce le impostazioni di rete del cluster selezionato per l'espansione, assicurarsi che il mapping vmkernel e vmnic per le reti di gestione, storage e vMotion sia impostato sui valori predefiniti di implementazione. Vedere "modifiche di rete supportate" per ulteriori informazioni.

   e. Fare clic su **continua**.

8. Nella pagina **credenziali ESXi**, immettere una password radice ESXi per il nodo di calcolo o i nodi che si desidera aggiungere.

   Utilizzare la stessa password creata durante la distribuzione iniziale di NetApp HCI.

9. Fare clic su **continua**.
10. Se è stato creato un nuovo cluster di data center vSphere, nella pagina **topologia di rete**, selezionare una topologia di rete che corrisponda ai nuovi nodi di calcolo che si stanno aggiungendo.

> Selezionare l'opzione due cavi solo se i nodi di calcolo utilizzano la topologia a due cavi e l'implementazione NetApp HCI esistente è configurata con ID VLAN.

11. Nella pagina **Available Inventory** (inventario disponibile), selezionare i nodi di storage e calcolo che si desidera aggiungere e fare clic su **Continue** (continua).

> Per alcuni nodi di calcolo, potrebbe essere necessario abilitare EV al livello più elevato supportato dalla versione di vCenter prima di poterli aggiungere all'installazione. È necessario utilizzare il client vSphere per abilitare EVC per questi nodi di calcolo. Una volta attivata, aggiornare la pagina Inventory e provare ad aggiungere nuovamente i nodi di calcolo.

12. Fare clic su **continua**.
13. **Opzionale**: Se è stato creato un nuovo cluster di data center vSphere, nella pagina **Impostazioni di rete**, importare le informazioni di rete da un'implementazione NetApp HCI esistente selezionando la casella di controllo **Copia impostazione da un cluster esistente**.

    In questo modo vengono inserite le informazioni predefinite relative al gateway e alla subnet per ciascuna rete.

14. Nella pagina **Impostazioni di rete**, alcune informazioni di rete sono state rilevate dalla distribuzione iniziale. Ogni nuovo nodo di storage viene elencato in base al numero di serie ed è necessario assegnarvi le nuove informazioni di rete. Per ogni nuovo nodo di storage, attenersi alla seguente procedura:
    a. **Nome host**: Se NetApp HCI ha rilevato un prefisso di denominazione, copiarlo dal campo prefisso di denominazione rilevato e inserirlo come prefisso per il nuovo nome host univoco aggiunto nel campo Nome host.
    b. **Management Address** (Indirizzo di gestione): Immettere un indirizzo IP di gestione per il nuovo nodo di storage all'interno della subnet della rete di gestione.
    c. **Storage (iSCSI) IP Address (Indirizzo IP storage (iSCSI))**: Inserire un indirizzo IP iSCSI per il nuovo nodo di storage all'interno della subnet di rete iSCSI.
    d. Fare clic su **continua**.

> NetApp HCI potrebbe impiegare del tempo per convalidare gli indirizzi IP immessi. Il pulsante continua diventa disponibile al termine della convalida dell'indirizzo IP.

15. Nella pagina **Review** della sezione Network Settings (Impostazioni di rete), i nuovi nodi vengono visualizzati in grassetto. Per apportare modifiche in qualsiasi sezione, procedere come segue:
    a. Fare clic su **Edit** (Modifica) per la sezione.
    b. Al termine, fare clic su **continua** nelle pagine successive per tornare alla pagina di revisione.
16. **Opzionale**: Se non si desidera inviare statistiche del cluster e informazioni di supporto ai server Active IQ in hosting NetApp, deselezionare la casella di controllo finale.

    In questo modo si disattiva il monitoraggio diagnostico e dello stato di salute in tempo reale per NetApp HCI. La disattivazione di questa funzione elimina la possibilità per NetApp di supportare e monitorare in modo proattivo NetApp HCI per rilevare e risolvere i problemi prima che la produzione ne risenta.
17. Fare clic su **Aggiungi nodi**.

    È possibile monitorare l'avanzamento mentre NetApp HCI aggiunge e configura le risorse.
18. **Opzionale**: Verificare che i nuovi nodi siano visibili in VMware vSphere Web Client (per i nodi di calcolo) o nel plug-in Element per vCenter Server (per i nodi di storage).

> Se si è espanso un cluster di storage a due nodi a quattro o più nodi, la coppia di nodi di controllo utilizzati in precedenza dal cluster di storage rimane visibile come macchine virtuali in standby in vSphere. Il nuovo cluster di storage espanso non li utilizza; se si desidera recuperare risorse di macchine virtuali, è possibile "rimuovere manualmente" Le macchine virtuali Witness Node.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Plug-in NetApp Element per server vCenter"
- "Istruzioni per l'installazione e la configurazione dei nodi di calcolo e storage NetApp HCI"
- "VMware Knowledge base: Supporto avanzato del processore vMotion Compatibility (EVC)"

Rimuovere i nodi di controllo dopo l'espansione del cluster

Dopo aver espanso un cluster di storage a due nodi in quattro o più nodi, è possibile eliminare la coppia di nodi di controllo per liberare risorse di calcolo nell'installazione di NetApp HCI. I nodi di controllo utilizzati in precedenza dal cluster di storage sono ancora visibili come macchine virtuali in standby (VM) in vSphere Web Client.

A proposito di questa attività

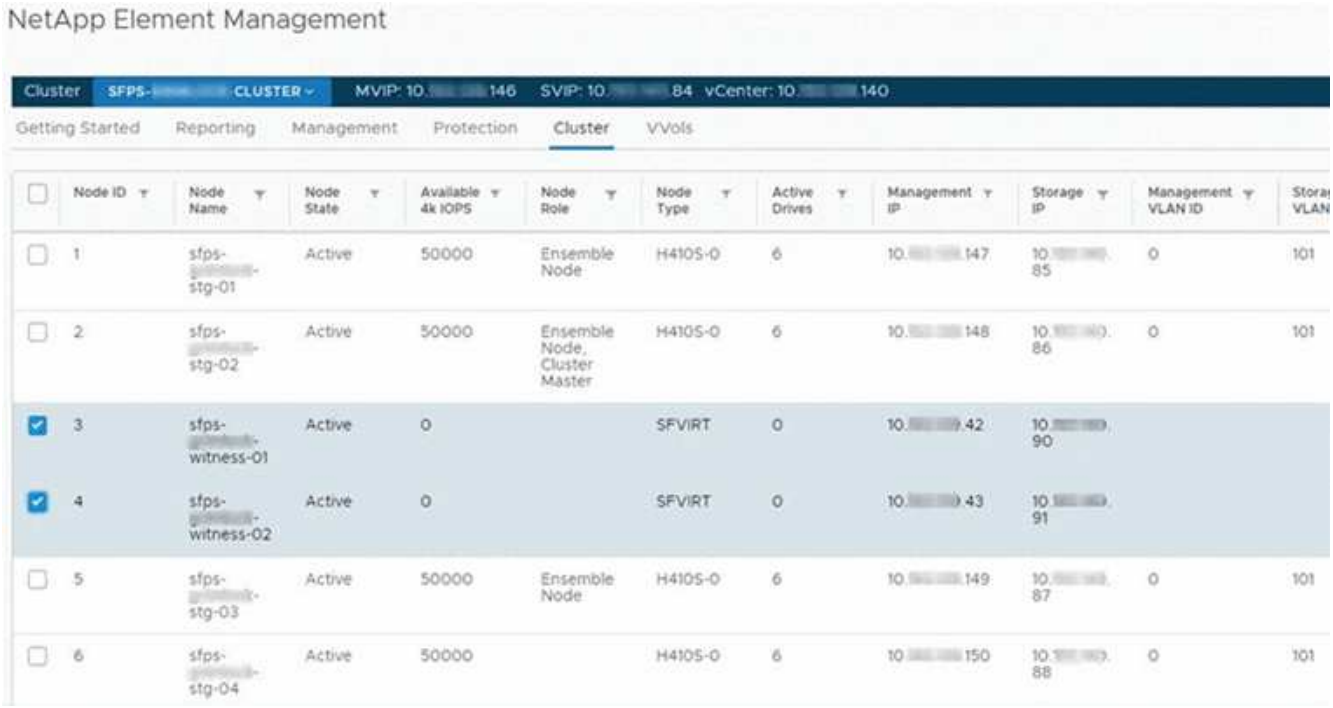
I nodi di controllo non sono richiesti nei cluster con più di quattro nodi di storage. Questa procedura è facoltativa se si desidera liberare CPU e memoria dopo aver espanso il cluster a due nodi a quattro o più nodi.

> Verificare che non vengano segnalati errori o guasti del cluster. Per informazioni sugli avvisi di sistema, fare clic su **Reporting > Avvisi** nell'estensione Gestione NetApp Element di vSphere.

Fasi

1. Da vSphere, accedere al punto di estensione della gestione NetApp Element dalla scheda **Collegamenti** o dal pannello laterale.

2. Selezionare **Gestione NetApp Element > cluster > nodi**.



3. Selezionare la casella di controllo del nodo di controllo che si desidera eliminare e fare clic su **azioni > Rimuovi**.
4. Confermare l'azione nel prompt.
5. Fare clic su **host e cluster**.
6. Accedere alla VM del nodo di controllo rimossa in precedenza.
7. Fare clic con il pulsante destro del mouse sulla macchina virtuale e spegnerla.
8. Fare clic con il pulsante destro del mouse sulla macchina virtuale spenta, quindi fare clic su **Delete from Disk** (Elimina da disco).
9. Confermare l'azione nel prompt.

Trova ulteriori informazioni

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

USA Rancher su NetApp HCI

Panoramica di Rancher on NetApp HCI

Rancher è uno stack software completo per i team che adottano i container. Rancher affronta le sfide operative e di sicurezza legate alla gestione di più cluster Kubernetes in diverse infrastrutture, fornendo al contempo ai team DevOps strumenti integrati per l'esecuzione di workload containerizzati.

L'implementazione di Rancher su NetApp HCI implementa il piano di controllo Rancher, noto anche come *server Rancher*, e consente di creare cluster Kubernetes on-premise. Implementa il piano di controllo Rancher utilizzando il NetApp Hybrid Cloud Control.

Dopo l'implementazione, utilizzando il piano di controllo Rancher, è possibile eseguire il provisioning, la gestione e il monitoraggio dei cluster Kubernetes utilizzati dai team di sviluppo e operazioni. I team di sviluppo e operazioni possono utilizzare Rancher per eseguire attività su cluster di utenti che risiedono su NetApp HCI, un provider di cloud pubblico o qualsiasi altra infrastruttura abilitata da Rancher.

Vantaggi di Rancher su NetApp HCI

- Facilità di installazione: Non è necessario imparare a installare e configurare Rancher. È possibile implementare un'implementazione basata su modelli, sviluppata congiuntamente da NetApp HCI e Rancher.
- Gestione del ciclo di vita: In un'implementazione manuale di Rancher, gli aggiornamenti per l'applicazione server Rancher o per il cluster RKE (Rancher Kubernetes Engine) non sono automatizzati. Rancher su NetApp HCI offre la possibilità di aggiornare il cluster di gestione, che include il server Rancher e RKE.

Cosa puoi fare con Rancher su NetApp HCI

Con Rancher su NetApp HCI, puoi:

- Implementa servizi tra cloud provider e cloud privato.
- Porta le app e i dati su un'architettura di cloud ibrido indipendentemente dalla posizione del cloud senza compromettere gli accordi sul livello di servizio.
- Accelera le applicazioni native del cloud.
- Centralizzare la gestione di più cluster (nuovi ed esistenti).
- Orchestrazione di applicazioni basate su Kubernetes nel cloud ibrido.

Opzione di supporto tecnico

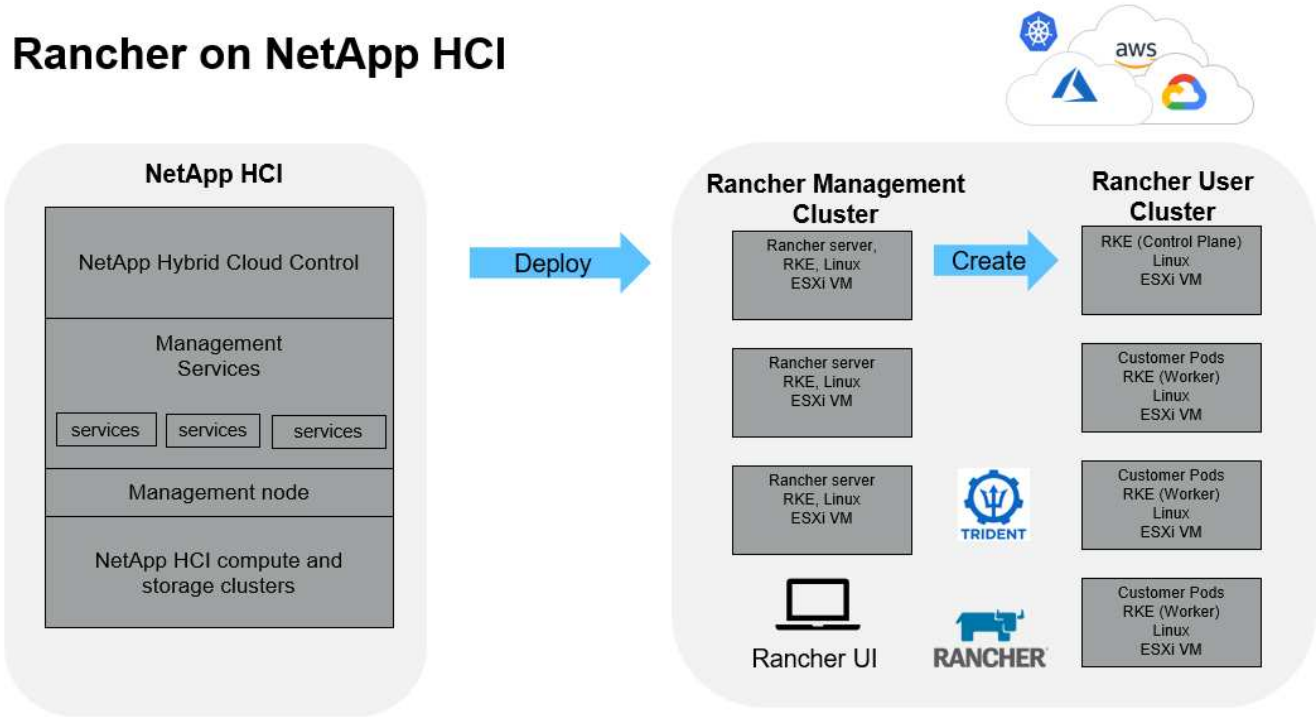
L'utilizzo di Rancher su NetApp HCI e Kubernetes software open-source include implementazione e utilizzo gratuiti. Le chiavi di licenza non sono richieste.

È possibile scegliere un'opzione NetApp Rancher Support per ottenere il supporto Enterprise Rancher basato su core.

> Il supporto Rancher non è incluso nel contratto NetApp Support Edge. Per le opzioni, contatta il reparto vendite NetApp o il tuo rivenditore. Se acquisti il supporto Rancher da NetApp, riceverai un'e-mail con le istruzioni.

Rancher su architettura e componenti NetApp HCI

Ecco una panoramica dei vari componenti di Rancher su NetApp HCI:



- **Controllo del cloud ibrido NetApp**: Questa interfaccia consente di implementare Rancher su software NetApp HCI e NetApp Element, richiesti per Rancher su NetApp HCI.

> È possibile utilizzare NetApp Hybrid Cloud Control anche per aggiornare i servizi di gestione, espandere il sistema, raccogliere i registri e monitorare l'installazione.

- **Servizi di gestione**: I servizi di gestione vengono eseguiti sul nodo di gestione e consentono di implementare Rancher su NetApp HCI utilizzando il controllo del cloud ibrido NetApp.
- **Cluster di gestione**: Rancher su NetApp HCI implementa tre macchine virtuali sul cluster di gestione Rancher, che è possibile vedere utilizzando il controllo del cloud ibrido NetApp, vCenter Server o l'interfaccia utente Rancher. Le macchine virtuali del cluster di gestione ospitano il server Rancher, Rancher Kubernetes Engine (RKE) e il sistema operativo Linux.

> Per ottenere le migliori performance e una maggiore sicurezza, prendere in considerazione l'utilizzo di un cluster Kubernetes dedicato per il server di gestione Rancher. Non è consigliabile eseguire i workload degli utenti sul cluster di gestione.

- **User Clusters**: I cluster di utenti Kubernetes a valle eseguono applicazioni e servizi. Qualsiasi cluster implementato da Rancher o importato in Rancher è un cluster utente.
- **Trident**: Un catalogo Trident è disponibile per Rancher su NetApp HCI e viene eseguito nei cluster di utenti. L'inclusione di questo catalogo semplifica l'implementazione di Trident nei cluster di utenti.

Trova ulteriori informazioni

- "Documentazione del rancher sull'architettura"

- "Pagina delle risorse NetApp HCI"

Rancher sui concetti di NetApp HCI

Scopri i concetti di base relativi a Rancher su NetApp HCI.

- **Server Rancher** o **piano di controllo**: Il piano di controllo Rancher, talvolta chiamato *server Rancher*, esegue il provisioning, la gestione e il monitoraggio dei cluster Kubernetes utilizzati dai team di sviluppo e operazioni.
- **Cataloghi**: I cataloghi sono repository GitHub o repository Helm Chart pieni di applicazioni pronte per l'implementazione. Rancher offre la possibilità di utilizzare un catalogo di grafici Helm che semplificano l'implementazione ripetuta delle applicazioni. Rancher include due tipi di cataloghi: Cataloghi globali integrati e cataloghi personalizzati. Trident viene implementato come catalogo. Vedere "Documentazione del rancher sui cataloghi".
- **Cluster di gestione**: Rancher su NetApp HCI implementa tre macchine virtuali nel cluster di gestione Rancher, che puoi vedere utilizzando Rancher, il controllo del cloud ibrido e il plug-in vCenter. Le macchine virtuali del cluster di gestione ospitano il server Rancher, Rancher Kubernetes Engine (RKE) e il sistema operativo Linux.
- **User Clusters**: Questi cluster Kubernetes downstream eseguono le tue applicazioni e i tuoi servizi. Nelle installazioni Kubernetes di Rancher, il cluster di gestione deve essere separato dai cluster degli utenti. Qualsiasi cluster implementato da Rancher o importato in Rancher da un utente Rancher viene considerato un cluster utente.
- **Modello di nodo Rancher**: Hybrid Cloud Control utilizza un modello di nodo Rancher per semplificare l'implementazione.

  Vedere "Documentazione del rancher sui modelli di nodo".

Software Trident e concetti di storage persistente

Trident, un'applicazione nativa di Kubernetes, viene eseguita direttamente all'interno di un cluster Kubernetes. Con Trident, gli utenti di Kubernetes (come sviluppatori, data scientist e amministratori di Kubernetes) possono creare, gestire e interagire con volumi di storage persistenti nel formato standard di Kubernetes con cui hanno già familiarità. Con Trident, le soluzioni NetApp sono in grado di soddisfare le richieste di volumi persistenti dei cluster Kubernetes.

Con Rancher, puoi utilizzare un volume persistente, che esiste indipendentemente da qualsiasi pod specifico e con la sua durata. L'utilizzo di Trident per gestire le richieste di rimborso dei volumi persistenti (PVC) isola gli sviluppatori che creano i pod dai dettagli di implementazione di livello inferiore dello storage a cui stanno accedendo.

Quando un'applicazione containerizzata emette una richiesta di richiesta di volume persistente (PVC), Trident esegue il provisioning dinamico dello storage in base ai parametri richiesti rispetto al livello di storage del software NetApp Element in NetApp HCI.

Un catalogo Trident è disponibile per Rancher su NetApp HCI e viene eseguito nei cluster di utenti. Come parte dell'implementazione di Rancher on NetApp HCI, un programma di installazione Trident è disponibile per impostazione predefinita nel catalogo Rancher. L'inclusione di questo catalogo semplifica l'implementazione di Trident nei cluster di utenti.

Vedere "Installare Trident con Rancher su NetApp HCI".

Per ulteriori informazioni, visitare il "Documentazione di Trident".

Trova ulteriori informazioni

- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"
- "Pagina delle risorse NetApp HCI"

Requisiti per Rancher su NetApp HCI

Prima di installare Rancher su NetApp HCI, assicurarsi che l'ambiente e il sistema NetApp HCI soddisfino questi requisiti.

> Se si implementa accidentalmente Rancher su NetApp HCI con informazioni errate (ad esempio un FQDN del server Rancher non corretto), non è possibile correggere l'implementazione senza rimuoverla e ridistribuirla. Sarà necessario rimuovere Rancher sull'istanza di NetApp HCI e quindi ridistribuire Rancher su NetApp HCI dall'interfaccia utente di controllo del cloud ibrido NetApp. Vedere "Rimuovere un'installazione di Rancher su NetApp HCI" per ulteriori informazioni.

Requisiti dei nodi

- Assicurati che il tuo sistema NetApp HCI disponga di almeno tre nodi di calcolo; questo è necessario per la piena resilienza. Rancher su NetApp HCI non è supportato nelle configurazioni solo storage.
- Assicurarsi che il datastore che si intende utilizzare per l'implementazione di Rancher su NetApp HCI disponga di almeno 60 GB di spazio libero.
- Assicurarsi che il cluster NetApp HCI utilizzi i servizi di gestione versione 2.17 o successiva.

Dettagli del nodo

Rancher su NetApp HCI implementa un cluster di gestione a tre nodi.

Tutti i nodi hanno le seguenti caratteristiche:

VCPU	RAM (GB)	Disco (GB)
2	8	20

Requisiti di rete

- Assicurarsi che la rete che si intende implementare Rancher sul cluster di gestione NetApp HCI disponga di un percorso verso la rete di gestione dei nodi.
- Rancher su NetApp HCI supporta gli indirizzi DHCP per il piano di controllo (server Rancher) e i cluster di utenti, ma si consiglia di utilizzare indirizzi IP statici per gli ambienti di produzione. Assicurarsi di aver allocato gli indirizzi IP statici necessari se si esegue l'implementazione in un ambiente di produzione.
  - Il server Rancher richiede tre indirizzi IP statici.
  - Ogni cluster di utenti richiede un numero di indirizzi IP statici pari a quello dei nodi nel cluster. Ad esempio, un cluster di utenti con quattro nodi richiede quattro indirizzi IP statici.

    - Se si prevede di utilizzare l'indirizzamento DHCP per il piano di controllo Rancher o i cluster di utenti, assicurarsi che la durata del lease DHCP sia di almeno 24 ore.
- Se è necessario utilizzare un proxy HTTP per abilitare l'accesso a Internet per Rancher su NetApp HCI, è necessario apportare una modifica pre-implementazione al nodo di gestione. Accedere al nodo di gestione utilizzando SSH e seguire la "istruzioni" Nella documentazione di Docker per aggiornare manualmente le impostazioni proxy per Docker.
- Se si attiva e si configura un server proxy durante l'implementazione, i seguenti intervalli di indirizzi IP e domini vengono aggiunti automaticamente alle impostazioni del server rancher noProxy:

```
127.0.0.0/8, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, .svc,
.cluster.local
```

- Assicurarsi che il nodo di gestione possa utilizzare il DNS per risolvere il nome host `<any IP address>.nip.io` A un indirizzo IP. Si tratta del provider DNS utilizzato durante l'implementazione; se il nodo di gestione non riesce a risolvere questo URL, l'implementazione non riesce.
- Assicurarsi di aver impostato i record DNS per ciascun indirizzo IP statico necessario.

Requisiti di VMware vSphere

- Assicurarsi che l'istanza di VMware vSphere in uso sia la versione 6.5, 6.7 o 7.0.
- È possibile utilizzare una configurazione di rete vSphere Standard Switch (VSS), ma in tal caso, assicurarsi che gli switch virtuali e gli host fisici utilizzati per le macchine virtuali Rancher possano accedere a tutti gli stessi gruppi di porte, nello stesso modo in cui si garantirebbe per le macchine virtuali normali.

Considerazioni sull'implementazione

Si consiglia di prendere in esame le seguenti considerazioni:

- Tipi di implementazioni
    - Implementazioni demo
    - Implementazioni in produzione
- FQDN del rancher

> Rancher su NetApp HCI non è resiliente agli errori dei nodi a meno che non si configuri un certo tipo di bilanciamento del carico di rete. Come soluzione semplice, creare una voce DNS round robin per i tre indirizzi IP statici riservati al server Rancher. Queste voci DNS devono essere risolte nell'FQDN del server Rancher che verrà utilizzato per accedere all'host del server Rancher, che serve l'interfaccia utente Web Rancher una volta completata l'implementazione.

Tipi di implementazioni

Puoi implementare Rancher su NetApp HCI nei seguenti modi:

- **Implementazioni demo**: Se DHCP è disponibile nell'ambiente di implementazione di destinazione e si desidera eseguire una dimostrazione della funzionalità Rancher on NetApp HCI, l'implementazione DHCP è più sensata.

  In questo modello di implementazione, l'interfaccia utente di Rancher è accessibile da ciascuno dei tre nodi

del cluster di gestione.

Se l'organizzazione non utilizza DHCP, è comunque possibile provarlo utilizzando quattro indirizzi IP statici allocati prima dell'implementazione, in modo simile a quanto si farebbe per un'implementazione in produzione.

- **Implementazioni in produzione**: Per le implementazioni in produzione o quando DHCP non è disponibile nell'ambiente di implementazione di destinazione, è necessario un po' più di lavoro di pre-implementazione. Il primo passo consiste nell'ottenere tre indirizzi IP consecutivi. Immettere il primo durante l'implementazione.

  Si consiglia di utilizzare il bilanciamento del carico L4 o la configurazione DNS round-robin per gli ambienti di produzione. Questo richiede un quarto indirizzo IP e una voce separata nella configurazione DNS.

  - **Bilanciamento del carico L4**: Questa è una tecnica in cui una macchina virtuale o un container che ospita un'applicazione come nginx è configurata per distribuire le richieste tra i tre nodi del cluster di gestione.
  - **Round-robin DNS**: Tecnica in cui viene configurato un singolo nome host nel sistema DNS che ruota le richieste tra i tre host che formano il cluster di gestione.

FQDN del rancher

L'installazione richiede l'assegnazione di un URL Rancher, che include il nome di dominio completo (FQDN, Fully Qualified Domain Name) dell'host in cui verrà servita l'interfaccia utente di Rancher al termine dell'installazione.

In tutti i casi, l'interfaccia utente di Rancher è accessibile nel browser tramite il protocollo https (porta 443).

Le implementazioni in produzione richiedono un FQDN configurato in grado di bilanciare il carico tra i nodi del cluster di gestione. Senza utilizzare FQDN e il bilanciamento del carico, l'ambiente non è resiliente ed è adatto solo per ambienti demo.

Porte richieste

Assicurarsi che l'elenco delle porte nella sezione "Porte per nodi server rancher su RKE" della sezione **nodi rancher** del funzionario "Documentazione del rancher" Sono aperti nella configurazione del firewall da e verso i nodi che eseguono il server Rancher.

URL richiesti

I seguenti URL devono essere accessibili dagli host in cui si trova il piano di controllo Rancher:

URL	Descrizione
https://charts.jetstack.io/	Integrazione di Kubernetes
https://releases.rancher.com/server-charts/stable	Download del software Rancher
https://entropy.ubuntu.com/	Servizio di entropia Ubuntu per la generazione di numeri casuali
https://raw.githubusercontent.com/vmware/cloud-init-vmware-guestinfo/v1.3.1/install.sh	Aggiunte di VMware guest
https://download.docker.com/linux/ubuntu/gpg	Chiave pubblica GPG Docker Ubuntu

URL	Descrizione
https://download.docker.com/linux/ubuntu	Link per il download di Docker
https://hub.docker.com/	Docker Hub per NetApp Hybrid Cloud Control

Implementare Rancher su NetApp HCI

Per utilizzare Rancher nel tuo ambiente NetApp HCI, devi prima implementare Rancher su NetApp HCI.

Prima di avviare l'implementazione, verificare lo spazio libero del datastore e altro "Requisiti per Rancher su NetApp HCI".

Il supporto Rancher non è incluso nel contratto NetApp Support Edge. Per le opzioni, contatta il reparto vendite NetApp o il tuo rivenditore. Se acquisti il supporto Rancher da NetApp, riceverai un'e-mail con le istruzioni.

Cosa succede quando si implementa Rancher su NetApp HCI?

L'implementazione prevede i seguenti passaggi, ciascuno descritto più avanti:

- Utilizza NetApp Hybrid Cloud Control per avviare l'implementazione.
- L'implementazione di Rancher crea un cluster di gestione che include tre macchine virtuali.

  A ciascuna macchina virtuale vengono assegnati tutti i ruoli Kubernetes per il piano di controllo e il lavoratore. Ciò significa che l'interfaccia utente di Rancher è disponibile su ciascun nodo.

- Viene installato anche il piano di controllo del rancher (o *server rancher*), utilizzando il modello di nodo NetApp HCI in Rancher per semplificare l'implementazione. Il piano di controllo Rancher funziona automaticamente con la configurazione utilizzata nel motore di implementazione NetApp, utilizzato per creare l'infrastruttura NetApp HCI.
- Dopo l'implementazione, riceverai un'e-mail da NetApp che ti fornirà la possibilità di iscriverti al supporto NetApp per le implementazioni Rancher su NetApp HCI.
- Dopo l'implementazione, i team Dev e Ops possono quindi implementare i propri cluster di utenti, in modo simile a qualsiasi implementazione di Rancher.

Fasi per implementare Rancher su NetApp HCI

- Accedi a NetApp Hybrid Cloud Control
- Implementare Rancher su NetApp HCI
- Verificare l'implementazione utilizzando vCenter Server

Accedi a NetApp Hybrid Cloud Control

Per iniziare l'implementazione, accedi a NetApp Hybrid Cloud Control.

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

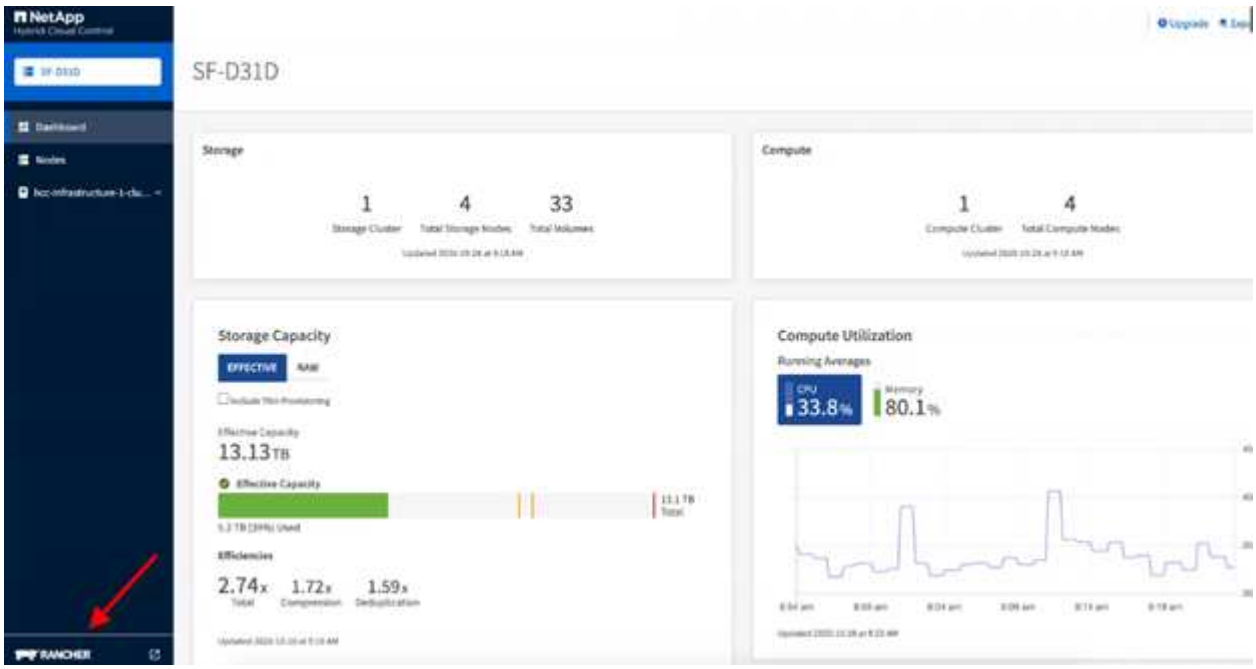
```
https://<ManagementNodeIP>
```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.

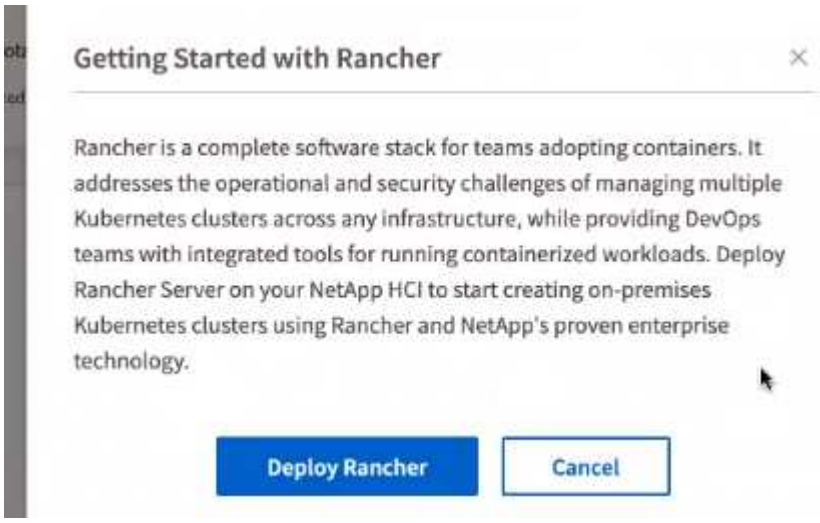
   Viene visualizzata l'interfaccia NetApp Hybrid Cloud Control.

Implementare Rancher su NetApp HCI

1. Da Hybrid Cloud Control, fare clic sull'icona **Rancher** in basso a sinistra nella barra di navigazione.

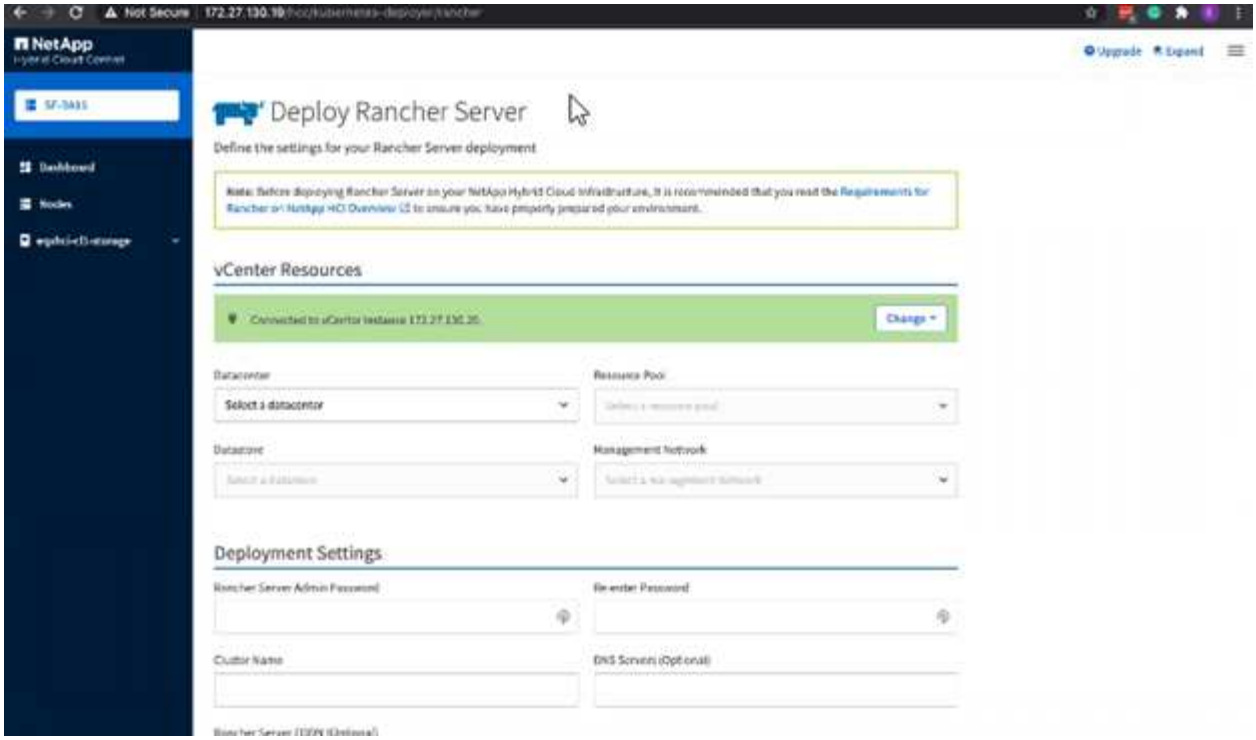


   Una finestra a comparsa mostra un messaggio sulla guida introduttiva a Rancher.



2. Fare clic su **Deploy Rancher**.

   Viene visualizzata l'interfaccia utente di Rancher.



Le credenziali vCenter vengono raccolte in base all'installazione di NetApp Deployment Engine.

3. Immettere le informazioni **risorse vCenter**. Alcuni campi sono descritti di seguito.
   - **Datacenter**: Seleziona un data center. Dopo aver selezionato il data center, tutti gli altri campi vengono precompilati, anche se è possibile modificarli.
   - **Datastore**: Selezionare un datastore sui nodi di storage NetApp HCI. Questo datastore deve essere resiliente e accessibile a tutti gli host VMware. Non selezionare un datastore locale accessibile solo a uno degli host.
   - **Rete di gestione**: Dovrebbe essere accessibile dalle stazioni di gestione e dalla rete di macchine virtuali in cui saranno ospitati i cluster di utenti.
4. Immettere le informazioni **Deployment Settings**:
   - **Server DNS**: Opzionale. Se si utilizza il bilanciamento del carico, immettere le informazioni sul server DNS interno.
   - **Rancher Server FQDN**: Per garantire che il server Rancher rimanga disponibile in caso di guasti al nodo, fornire un nome di dominio completo (FQDN) che il server DNS possa risolvere in uno degli indirizzi IP assegnati ai nodi del cluster Rancher Server. Questo FQDN con il prefisso "https" diventa l'URL Rancher che verrà utilizzato per accedere all'implementazione Rancher.

     Se non viene fornito alcun nome di dominio, verrà utilizzato il DNS con caratteri jolly e sarà possibile accedere al server Rancher utilizzando uno degli URL presentati al termine della distribuzione.
5. Immettere le informazioni **Advanced Settings**:
   - **Assign Static IP Addresses** (Assegna indirizzi IP statici): Se si attiva l'indirizzamento IP statico, fornire gli indirizzi IP iniziali per tre indirizzi IPv4 in sequenza, uno per ciascuna macchina virtuale del cluster di gestione. Rancher su NetApp HCI implementa tre macchine virtuali del cluster di gestione.
   - **Configura server proxy**:
6. Esaminare e selezionare la casella di controllo del Contratto di licenza con l'utente finale di Rancher.

7. Controllare e selezionare la casella di controllo per confermare le informazioni sul software Rancher.
8. Fare clic su **Deploy**.

   Una barra indica l'avanzamento dell'implementazione.

   > L'implementazione di Rancher potrebbe richiedere circa 15 minuti.

   Una volta completata l'implementazione, Rancher visualizza un messaggio sul completamento e fornisce un URL Rancher.

9. Annotare l'URL del rancher visualizzato alla fine dell'implementazione. Questo URL verrà utilizzato per accedere all'interfaccia utente di Rancher.

Verificare l'implementazione utilizzando vCenter Server

Nel client vSphere, è possibile visualizzare il cluster di gestione Rancher, che include le tre macchine virtuali.

> Una volta completata l'implementazione, non modificare la configurazione del cluster di macchine virtuali del server Rancher né rimuovere le macchine virtuali. Rancher su NetApp HCI si affida alla configurazione del cluster di gestione RKE implementata per funzionare normalmente.

Quali sono le prossime novità?

Dopo l'implementazione, è possibile eseguire le seguenti operazioni:

- "Completare le attività post-implementazione"
- "Installare Trident con Rancher su NetApp HCI"
- "Implementare cluster di utenti e applicazioni"
- "Gestire Rancher su NetApp HCI"
- "Monitor Rancher su NetApp HCI"

Trova ulteriori informazioni

- "Risoluzione dei problemi di implementazione del rancher"
- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"
- "Pagina delle risorse NetApp HCI"

Attività post-implementazione

Panoramica delle attività post-implementazione

Dopo aver implementato Rancher su NetApp HCI, dovresti continuare con le attività post-implementazione.

- "Garantire la parità del supporto Rancher"
- "Migliorare la resilienza delle macchine virtuali Rancher"
- "Configurare il monitoraggio"
- "Installare Trident"
- "Abilitare il supporto Trident per i cluster di utenti"

Trova ulteriori informazioni

- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Garantire la parità del supporto Rancher

Dopo aver implementato Rancher su NetApp HCI, è necessario assicurarsi che il numero di core di supporto Rancher acquistati corrisponda al numero di core CPU utilizzati per le VM di gestione Rancher e i cluster utente.

Se hai acquistato il supporto per rancher solo per una parte delle tue risorse di calcolo NetApp HCI, devi intervenire in VMware vSphere per garantire che Rancher su NetApp HCI e i suoi cluster di utenti gestiti siano eseguiti solo sugli host per i quali hai acquistato il supporto per rancher. Consultare la documentazione di VMware vSphere per informazioni su come garantire questo risultato confinando i carichi di lavoro di calcolo a host specifici.

Trova ulteriori informazioni

- "VSphere ha e DRS Affinity Rules"
- "Creare regole di affinità per VM"
- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Migliorare la resilienza delle macchine virtuali Rancher

Dopo aver implementato Rancher su NetApp HCI, l'ambiente vSphere conterrà tre nuovi nodi come macchine virtuali per ospitare l'ambiente Rancher. L'interfaccia utente Web di Rancher è disponibile da ciascuno di questi nodi. Per una resilienza completa, ciascuna

delle tre macchine virtuali e i dischi virtuali corrispondenti devono risiedere su un host fisico diverso dopo eventi come cicli di alimentazione e failover.

Per garantire che ciascuna macchina virtuale e le relative risorse rimangano su un host fisico diverso, è possibile creare regole di affinità anti-Affinity di VMware vSphere Distributed Resource Scheduler (DRS). Questo non è automatizzato come parte dell'implementazione di Rancher su NetApp HCI.

Per istruzioni su come configurare le regole di affinità DRS, consultare le seguenti risorse di documentazione VMware:

"Creare regole di affinità per VM"

"VSphere ha e DRS Affinity Rules"

Trova ulteriori informazioni

- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Abilitare il monitoraggio

Dopo aver implementato Rancher su NetApp HCI, è possibile attivare il monitoraggio dello storage Active IQ (per lo storage all-flash SolidFire e NetApp HCI) e il monitoraggio del calcolo NetApp HCI (solo per NetApp HCI), se non lo si è già fatto durante l'installazione o l'aggiornamento.

Per istruzioni su come attivare il monitoraggio, vedere "Abilitare il monitoraggio Active IQ e NetApp HCI".

Trova ulteriori informazioni

- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Installare Trident

Scopri come installare Trident dopo aver installato Rancher su NetApp HCI. Trident è un orchestrator dello storage, che si integra con Docker e Kubernetes, nonché con piattaforme basate su queste tecnologie, come Red Hat OpenShift, Rancher e IBM Cloud Private. L'obiettivo di Trident è rendere il provisioning, la connessione e il consumo dello storage trasparenti e privi di attrito per le applicazioni. Trident è un progetto open source completamente supportato gestito da NetApp. Trident ti consente di creare, gestire e interagire con volumi di storage persistenti nel formato standard di Kubernetes che conosci.

Per ulteriori informazioni su Trident, vedere "Documentazione di Trident".

Di cosa hai bisogno

- Rancher è stato installato su NetApp HCI.
- Hai implementato i tuoi cluster di utenti.
- Le reti cluster utente sono state configurate per Trident. Vedere "Abilitare il supporto Trident per i cluster di utenti" per istruzioni.
- Hai completato le fasi necessarie per la preparazione del nodo di lavoro per Trident. Vedere "Documentazione di Trident".

A proposito di questa attività

Il catalogo dei programmi di installazione Trident viene installato come parte dell'installazione di Rancher utilizzando NetApp Hybrid Cloud Control. In questa attività, si utilizza il catalogo del programma di installazione per installare e configurare Trident. Nell'ambito dell'installazione di Rancher, NetApp fornisce un modello di nodo. Se non si intende utilizzare il modello di nodo fornito da NetApp e si desidera eseguire il provisioning su RHEL o CentOS, potrebbero essere necessari ulteriori requisiti. Se si modifica il nodo di lavoro in RHEL o CentOS, è necessario soddisfare diversi prerequisiti. Vedere "Documentazione di Trident".

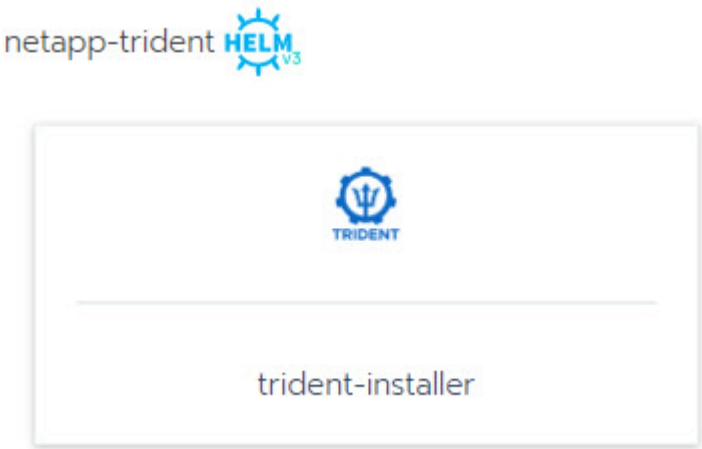
Fasi

1. Dall'interfaccia utente di Rancher, selezionare un progetto per il cluster utente.

   Per informazioni sui progetti e sugli spazi dei nomi, vedere "Documentazione del rancher".

2. Selezionare **Apps**, quindi **Launch**.

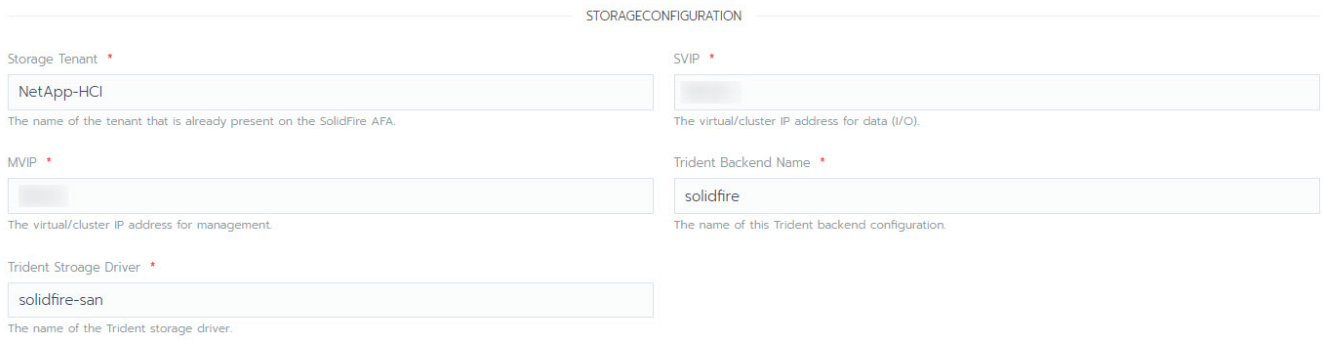
3. Nella pagina **Catalog**, selezionare il programma di installazione di Trident.



   Nella pagina visualizzata, selezionare la freccia **descrizioni dettagliate** per ulteriori informazioni sull'applicazione Trident e per trovare il collegamento a "Documentazione di Trident".

4. Selezionare la freccia **Opzioni di configurazione** e immettere le credenziali e le informazioni di

configurazione dello storage.

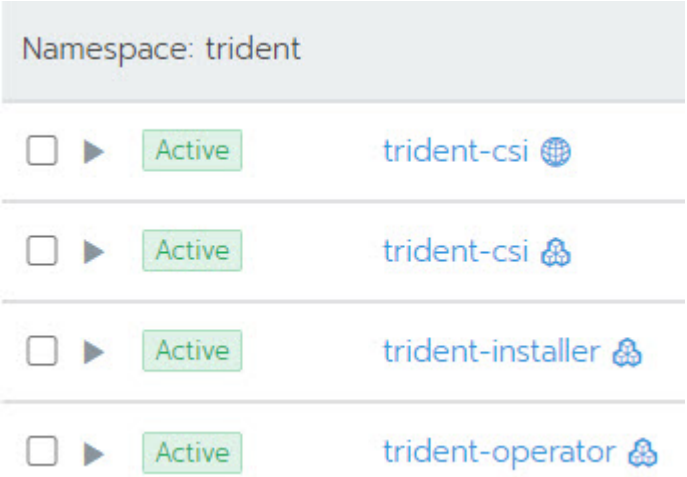


> Il tenant di storage predefinito è NetApp HCI. È possibile modificare questo valore. È anche possibile modificare il nome del backend. Tuttavia, non modificare il valore predefinito del driver dello storage, che è **solidfire-san**.

5. Selezionare **Launch** (Avvia).

   In questo modo viene installato il carico di lavoro Trident sullo spazio dei nomi **trident**.

6. Selezionare **risorse > carichi di lavoro** e verificare che lo spazio dei nomi **trident** includa i seguenti componenti:



7. (Facoltativo) selezionare **Storage** per visualizzare le classi di storage che è possibile utilizzare per i volumi persistenti.

> Le tre classi di storage sono **solidfire-gold**, **solidfire-silver** e **solidfire-bronze**. Per impostare una di queste classi di storage come predefinita, selezionare l'icona nella colonna **Default**.

Trova ulteriori informazioni

- "Abilitare il supporto Trident per i cluster di utenti"
- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"

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

Abilitare il supporto Trident per i cluster di utenti

Se l'ambiente NetApp HCI non dispone di un percorso tra le reti di gestione e di storage e si implementano cluster di utenti che richiedono il supporto di Trident, è necessario configurare ulteriormente le reti di cluster utente dopo l'installazione di Trident. Per ogni cluster di utenti, è necessario abilitare la comunicazione tra le reti di gestione e di storage. A tale scopo, modificare la configurazione di rete per ciascun nodo del cluster utente.

A proposito di questa attività

Per modificare la configurazione di rete per ciascun nodo del cluster utente, attenersi alla procedura generale riportata di seguito. Questi passaggi presuppongono che sia stato creato il cluster utente con il modello di nodo predefinito installato con Rancher su NetApp HCI.

> È possibile apportare queste modifiche come parte di un modello di nodo personalizzato da utilizzare per i cluster di utenti futuri.

Fasi

1. Implementare un cluster di utenti con il modello predefinito esistente.
2. Collegare la rete di storage al cluster utente.
   a. Aprire il client Web VMware vSphere per l'istanza vCenter connessa.
   b. Nell'albero di inventario di host e cluster, selezionare un nodo nel cluster utente appena distribuito.
   c. Modificare le impostazioni del nodo.
   d. Nella finestra di dialogo delle impostazioni, aggiungere una nuova scheda di rete.
   e. Nell'elenco a discesa **Nuova rete**, cercare una rete e selezionare **HCI_Internal_Storage_Data_Network**.
   f. Espandere la sezione scheda di rete e registrare l'indirizzo MAC del nuovo adattatore di rete.
   g. Fare clic su **OK**.
3. In Rancher, scaricare il file della chiave privata SSH per ciascun nodo del cluster utente.
4. Connettersi utilizzando SSH a un nodo del cluster utente, utilizzando il file di chiave privata scaricato per quel nodo:

   ```
   ssh -i <private key filename> <ip address>
   ```

5. In qualità di superutente, modificare e salvare `/etc/netplan/50-cloud-init.yaml` in modo che includa `ens224` simile all'esempio seguente. Sostituire `<MAC address>` Con l'indirizzo MAC registrato in precedenza:

```
network:
    ethernets:
        ens192:
            dhcp4: true
            match:
                macaddress: 00:50:56:91:1d:41
            set-name: ens192
        ens224:
            dhcp4: true
            match:
                macaddress: <MAC address>
            set-name: ens224
    version: 2
```

6. Utilizzare il seguente comando per riconfigurare la rete:

```
`netplan try`
```

7. Ripetere i passaggi da 4 a 6 per ogni nodo rimanente nel cluster utente.
8. Una volta riconfigurata la rete per ciascun nodo del cluster utente, è possibile implementare applicazioni nel cluster utente che utilizzano Trident.

Implementare cluster di utenti e applicazioni

Dopo aver implementato Rancher su NetApp HCI, è possibile configurare cluster di utenti e aggiungere applicazioni a tali cluster.

Implementare cluster di utenti

Dopo l'implementazione, i team Dev e Ops possono quindi implementare i propri cluster utente Kubernetes, in modo simile a qualsiasi implementazione Rancher, su cui possono implementare le applicazioni.

1. Accedere all'interfaccia utente di Rancher utilizzando l'URL fornito al termine dell'implementazione di Rancher.
2. Creare cluster di utenti. Consultare la documentazione di Rancher su "implementazione dei carichi di lavoro".
3. Eseguire il provisioning dei cluster di utenti in Rancher su NetApp HCI. Consultare la documentazione di Rancher su "Configurazione dei cluster Kubernetes in Rancher".

Implementare le applicazioni sui cluster di utenti

Analogamente a qualsiasi implementazione di Rancher, è possibile aggiungere applicazioni sui cluster Kubernetes.

Consultare la documentazione di Rancher su "implementazione di applicazioni tra cluster".

Trova ulteriori informazioni

- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"
- "Pagina delle risorse NetApp HCI"

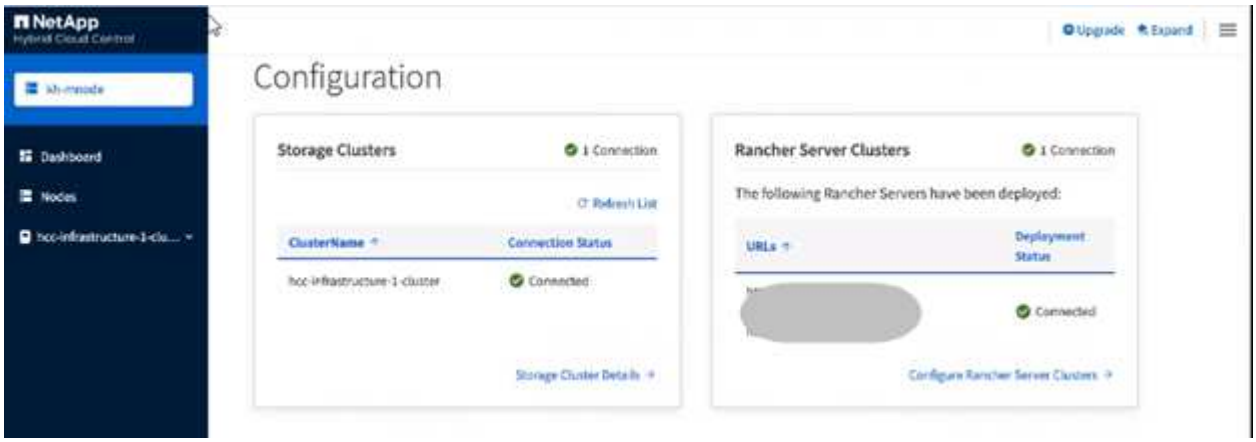
Gestire Rancher su NetApp HCI

Dopo aver implementato Rancher su NetApp HCI, è possibile visualizzare gli URL e lo stato del cluster del server Rancher. È anche possibile eliminare il server Rancher.

Identificare gli URL e lo stato del cluster di server Rancher

È possibile identificare gli URL del cluster di server Rancher e determinare lo stato del server.

1. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI o Element.
2. Dalla dashboard, selezionare l'icona Opzioni in alto a destra e selezionare **Configura**.



La pagina Rancher Server Clusters visualizza un elenco dei cluster di server Rancher implementati, l'URL associato e lo stato.

Trova ulteriori informazioni

- "Rimuovere Rancher"
- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"
- "Pagina delle risorse NetApp HCI"

Monitorare un rancher sull'implementazione di NetApp HCI

Esistono diversi modi per monitorare il server Rancher, i cluster di gestione e altri dettagli.

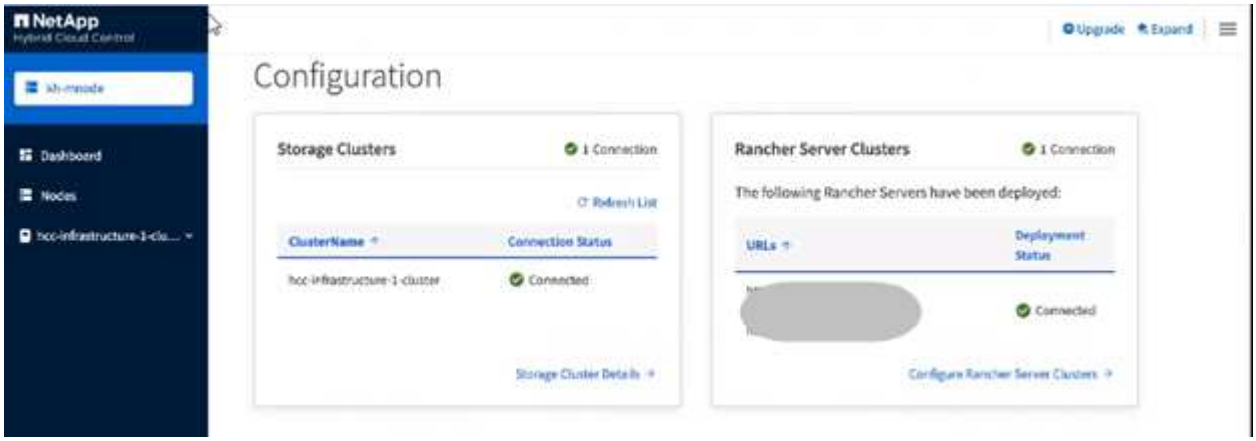
- NetApp Hybrid Cloud Control
- UI del rancher

- NetApp Active IQ
- Server vCenter

Monitorare Rancher utilizzando il NetApp Hybrid Cloud Control

Utilizzando NetApp Hybrid Cloud Control, è possibile visualizzare l'URL Rancher e lo stato del cluster del server Rancher. È inoltre possibile monitorare i nodi in cui Rancher è in esecuzione.

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, fare clic sull'icona Opzioni in alto a destra e selezionare **Configura**.



3. Per visualizzare le informazioni sui nodi, dalla dashboard di controllo del cloud ibrido, espandere il nome del cluster di storage e fare clic su **Nodes**.

Monitorare Rancher utilizzando l'interfaccia utente Rancher

Utilizzando l'interfaccia utente di Rancher, è possibile visualizzare informazioni su Rancher sui cluster di gestione NetApp HCI e sui cluster di utenti.

> Nell'interfaccia utente di Rancher, i cluster di gestione vengono definiti "cluster locali".

1. Accedere all'interfaccia utente di Rancher utilizzando l'URL fornito al termine dell'implementazione di Rancher.
2. Vedere "Monitoraggio in Rancher v2.5".

Monitorare il rancher utilizzando NetApp Active IQ

Grazie a NetApp Active IQ, è possibile visualizzare la telemetria di Rancher, ad esempio informazioni sull'installazione, nodi, cluster, stato, informazioni sullo spazio dei nomi, e molto altro ancora.

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dal menu in alto a destra, selezionare **NetApp Active IQ**.

Monitorare Rancher utilizzando vCenter Server

Con vCenter Server è possibile monitorare le macchine virtuali Rancher.

Trova ulteriori informazioni

- "Documentazione del rancher sull'architettura"
- "La terminologia di Kubernetes per Rancher"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Upgrade Rancher su NetApp HCI

Per aggiornare il software Rancher, è possibile utilizzare l'interfaccia utente di NetApp Hybrid Cloud Control (HCC) o L'API REST. HCC offre un semplice processo di aggiornamento dei componenti dell'implementazione di Rancher, tra cui il server Rancher, RKE (Rubernetes Engine) Rancher e il sistema operativo del nodo del cluster di gestione (per gli aggiornamenti di sicurezza). In alternativa, è possibile utilizzare l'API per automatizzare gli aggiornamenti.

Gli aggiornamenti sono disponibili per componente invece che per pacchetto cumulativo. Di conseguenza, alcuni aggiornamenti dei componenti, come il sistema operativo Ubuntu, sono disponibili con cadenza più rapida. Gli aggiornamenti interessano solo l'istanza del server Rancher e il cluster di gestione su cui è distribuito Rancher Server. Gli aggiornamenti al sistema operativo Ubuntu del nodo del cluster di gestione sono solo per patch di sicurezza critiche e non aggiornano il sistema operativo. I cluster di utenti non possono essere aggiornati da NetApp Hybrid Cloud Control.

Di cosa hai bisogno

- **Privilegi di amministratore**: Si dispone delle autorizzazioni di amministratore del cluster di storage per eseguire l'aggiornamento.
- **Servizi di gestione**: Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente.

> È necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente 2.17 o successivo per la funzionalità Rancher.

- **Porte di sistema**: Se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, si è assicurati che le porte necessarie siano aperte. Vedere "Porte di rete" per ulteriori informazioni.
- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare un'implementazione di Rancher:
  a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

  ```
  https://<ManagementNodeIP>
  ```

  b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.

c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.

d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

Opzioni di upgrade

Scegliere uno dei seguenti processi di aggiornamento:

- Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare un'implementazione di Rancher
- Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare un'implementazione di Rancher

Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare un'implementazione di Rancher

Utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control, puoi aggiornare uno qualsiasi di questi componenti nella tua implementazione di Rancher:

- Server del rancher
- Rancher Kubernetes Engine (RKE)
- Aggiornamenti di sicurezza del sistema operativo del nodo

Di cosa hai bisogno

- Una buona connessione a Internet. Gli aggiornamenti del sito dark (aggiornamenti in un sito senza connettività esterna) non sono disponibili.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare **Rancher**.
5. Selezionare il menu **azioni** del software che si desidera aggiornare.
   - Server del rancher
   - Rancher Kubernetes Engine (RKE)
   - Aggiornamenti di sicurezza del sistema operativo del nodo
6. Selezionare **Upgrade** per gli aggiornamenti del server Rancher o RKE o **Apply Upgrade** per gli aggiornamenti di sicurezza del sistema operativo Node.

> Per il sistema operativo del nodo, gli aggiornamenti automatici delle patch di sicurezza vengono eseguiti quotidianamente, ma il nodo non viene riavviato automaticamente. Applicando gli aggiornamenti, si riavvia ogni nodo per rendere effettive le modifiche di protezione.

Viene visualizzato un banner che indica che l'aggiornamento del componente è stato eseguito correttamente. Potrebbe esserci un ritardo di 2 minuti prima che l'interfaccia utente di NetApp Hybrid Cloud Control mostri il

numero di versione aggiornato.

Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare un'implementazione di Rancher

È possibile utilizzare le API per aggiornare uno qualsiasi di questi componenti nella distribuzione di Rancher:

- Server del rancher
- Rancher Kubernetes Engine (RKE)
- Sistema operativo Node (per gli aggiornamenti di sicurezza)

È possibile utilizzare uno strumento di automazione di propria scelta per eseguire le API o L'interfaccia utente REST API disponibile sul nodo di gestione.

Opzioni

- Upgrade di Rancher Server
- Aggiornare RKE
- Applicare gli aggiornamenti di sicurezza del sistema operativo del nodo

> Per il sistema operativo del nodo, gli aggiornamenti automatici delle patch di sicurezza vengono eseguiti quotidianamente, ma il nodo non viene riavviato automaticamente. Applicando gli aggiornamenti, si riavvia ogni nodo per rendere effettive le modifiche di protezione.

Upgrade di Rancher Server

Comandi API

1. Avviare la richiesta di aggiornamento delle versioni dell'elenco:

```
curl -X POST "https://<managementNodeIP>/k8sdeployer/1/upgrade/rancher-versions" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

> Puoi trovare il portatore `${TOKEN}` Utilizzato dal comando API quando si "autorizzare". Il portatore `${TOKEN}` è nella risposta di arricciamento.

2. Ottenere lo stato dell'attività utilizzando l'ID attività del comando precedente e copiare il numero di versione più recente dalla risposta:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Avviare la richiesta di upgrade del server Rancher:

```
curl -X PUT "https://<mNodeIP>/k8sdeployer/1/upgrade/rancher/<version
number>" -H "accept: application/json" -H "Authorization: Bearer"
```

4. Ottenere lo stato del task utilizzando l'ID del task dalla risposta del comando di upgrade:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

FASI DELL'INTERFACCIA UTENTE API REST

1. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra di autorizzazione.
3. Verificare la disponibilità del pacchetto di aggiornamento più recente:
   a. Dall'interfaccia utente API REST, eseguire **POST /upgrade/rancher-versions**.
   b. Dalla risposta, copiare l'ID attività.
   c. Eseguire **GET /task/{taskID}** con l'ID attività del passaggio precedente.
4. Dalla risposta **/task/{taskID}**, copiare l'ultimo numero di versione che si desidera utilizzare per l'aggiornamento.
5. Eseguire l'aggiornamento di Rancher Server:
   a. Dall'interfaccia utente API REST, eseguire **PUT /upgrade/rancher/{version}** con il numero di versione più recente del passaggio precedente.
   b. Dalla risposta, copiare l'ID attività.
   c. Eseguire **GET /task/{taskID}** con l'ID attività del passaggio precedente.

L'aggiornamento è stato completato correttamente quando `PercentComplete` indica `100` e. `results` indica il numero della versione aggiornata.

Aggiornare RKE

Comandi API

1. Avviare la richiesta di aggiornamento delle versioni dell'elenco:

```
curl -X POST "https://<mNodeIP>/k8sdeployer/1/upgrade/rke-versions" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

> Puoi trovare il portatore `${TOKEN}` Utilizzato dal comando API quando si "autorizzare". Il portatore `${TOKEN}` è nella risposta di arricciamento.

2. Ottenere lo stato dell'attività utilizzando l'ID attività del comando precedente e copiare il numero di versione più recente dalla risposta:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Avviare la richiesta di aggiornamento RKE

```
curl -X PUT "https://<mNodeIP>/k8sdeployer/1/upgrade/rke/<version
number>" -H "accept: application/json" -H "Authorization: Bearer"
```

4. Ottenere lo stato del task utilizzando l'ID del task dalla risposta del comando di upgrade:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

FASI DELL'INTERFACCIA UTENTE API REST

1. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra di autorizzazione.
3. Verificare la disponibilità del pacchetto di aggiornamento più recente:
   a. Dall'interfaccia utente API REST, eseguire **POST /upgrade/rke-versions**.
   b. Dalla risposta, copiare l'ID attività.
   c. Eseguire **GET /task/{taskID}** con l'ID attività del passaggio precedente.
4. Dalla risposta **/task/{taskID}**, copiare l'ultimo numero di versione che si desidera utilizzare per l'aggiornamento.

5. Eseguire l'aggiornamento RKE:
   a. Dall'interfaccia utente API REST, eseguire **PUT /upgrade/rke/{version}** con il numero di versione più recente del passaggio precedente.
   b. Copiare l'ID attività dalla risposta.
   c. Eseguire **GET /task/{taskID}** con l'ID attività del passaggio precedente.

L'aggiornamento è stato completato correttamente quando `PercentComplete` indica `100` e. `results` indica il numero della versione aggiornata.

Applicare gli aggiornamenti di sicurezza del sistema operativo del nodo

Comandi API

1. Avviare la richiesta di verifica degli aggiornamenti:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/upgrade/checkNodeUpdates"
-H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

> Puoi trovare il portatore `${TOKEN}` Utilizzato dal comando API quando si "autorizzare". Il portatore `${TOKEN}` è nella risposta di arricciamento.

2. Ottenere lo stato dell'attività utilizzando l'ID attività del comando precedente e verificare che sia disponibile un numero di versione più recente dalla risposta:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Applicare gli aggiornamenti del nodo:

```
curl -X POST "https://<mNodeIP>/k8sdeployer/1/upgrade/applyNodeUpdates"
-H "accept: application/json" -H "Authorization: Bearer"
```

> Per il sistema operativo del nodo, gli aggiornamenti automatici delle patch di sicurezza vengono eseguiti quotidianamente, ma il nodo non viene riavviato automaticamente. Applicando gli aggiornamenti, ogni nodo viene riavviato in sequenza per rendere effettive le modifiche di protezione.

4. Ottenere lo stato del task utilizzando l'ID del task dall'aggiornamento `applyNodeUpdates` risposta:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

FASI DELL'INTERFACCIA UTENTE API REST

1. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra di autorizzazione.
3. Verificare se è disponibile un pacchetto di aggiornamento:
   a. Dall'interfaccia utente API REST, eseguire **GET /upgrade/checkNodeUpdates**.
   b. Dalla risposta, copiare l'ID attività.
   c. Eseguire **GET /task/{taskID}** con l'ID attività del passaggio precedente.
   d. Dalla risposta **/task/{taskID}**, verificare che vi sia un numero di versione più recente di quello attualmente applicato ai nodi.
4. Applicare gli aggiornamenti del sistema operativo del nodo:

   > Per il sistema operativo del nodo, gli aggiornamenti automatici delle patch di sicurezza vengono eseguiti quotidianamente, ma il nodo non viene riavviato automaticamente. Applicando gli aggiornamenti, ogni nodo viene riavviato in sequenza per rendere effettive le modifiche di protezione.

   a. Dall'interfaccia utente API REST, eseguire **POST /upgrade/applyNodeUpdates**.
   b. Dalla risposta, copiare l'ID attività.
   c. Eseguire **GET /task/{taskID}** con l'ID attività del passaggio precedente.
   d. Dalla risposta **/task/{taskID}**, verificare che l'aggiornamento sia stato applicato.

L'aggiornamento è stato completato correttamente quando `PercentComplete` indica `100` e. `results` indica il numero della versione aggiornata.

Trova ulteriori informazioni

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

Rimuovere un'installazione di Rancher su NetApp HCI

Se Rancher viene distribuito accidentalmente su NetApp HCI con informazioni errate (ad esempio, un FQDN del server Rancher non corretto), è necessario rimuovere l'installazione e quindi ridistribuire. Per rimuovere l'installazione di Rancher sull'istanza di NetApp HCI, procedere come segue.

Questa azione non elimina i cluster di utenti.

È possibile conservare i cluster di utenti. In caso di conservazione, è possibile eseguire la migrazione in un'altra implementazione di Rancher. Se si desidera eliminare i cluster di utenti, è necessario eseguire questa operazione prima di eliminare il server Rancher; in caso contrario, l'eliminazione dei cluster di utenti dopo l'eliminazione del server Rancher risulta più difficile.

Opzioni

- Rimuovere Rancher su NetApp HCI utilizzando il controllo del cloud ibrido NetApp (Consigliato)
- Rimuovere Rancher su NetApp HCI utilizzando l'API REST

Rimuovere Rancher su NetApp HCI utilizzando il controllo del cloud ibrido NetApp

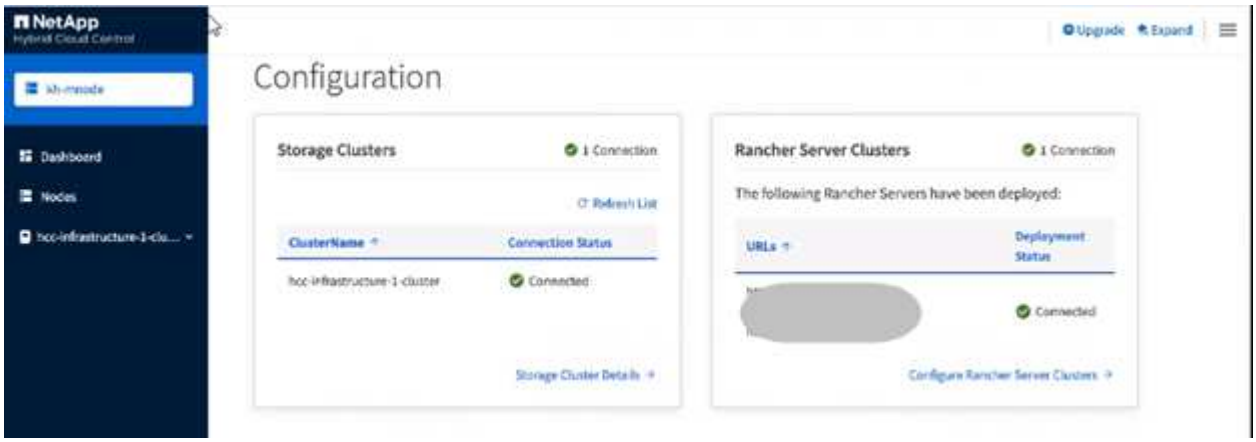
È possibile utilizzare l'interfaccia utente Web di NetApp Hybrid Cloud Control per rimuovere le tre macchine virtuali configurate durante l'implementazione per ospitare il server Rancher.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Dalla dashboard, fare clic sul menu in alto a destra.
4. Selezionare **Configura**.



5. Nel riquadro **Rancher Server Clusters**, fare clic su **Configure Rancher Server Clusters**.
6. Selezionare il menu **Actions** per l'installazione di Rancher che si desidera rimuovere.

Facendo clic su **Delete** (Elimina), viene immediatamente rimosso il rancher sul cluster di gestione NetApp HCI.

7. Selezionare **Delete** (Elimina).

Rimuovere Rancher su NetApp HCI utilizzando l'API REST

È possibile utilizzare l'API REST di NetApp Hybrid Cloud Control per rimuovere le tre macchine virtuali configurate durante l'implementazione per ospitare il server Rancher.

Fasi

1. Inserire l'indirizzo IP del nodo di gestione seguito da `/k8sdeployer/api/`:

```
https://[IP address]/k8sdeployer/api/
```

2. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e immettere le credenziali di amministratore del cluster per le autorizzazioni per l'utilizzo delle API.
   a. Inserire il nome utente e la password del cluster.
   b. Selezionare **corpo richiesta** dall'elenco a discesa tipo se il valore non è già selezionato.
   c. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
   d. Non inserire un valore per il client secret.
   e. Fare clic su **autorizzare** per avviare una sessione.
   f. Chiudere la finestra.
3. Chiudere la finestra di dialogo **Available Authorisations** (autorizzazioni disponibili).
4. Fare clic su **POST/Destroy**.
5. Fare clic su **Provalo**.
6. Nella casella di testo del corpo della richiesta, immettere l'FQDN del server Rancher come `serverURL` valore.
7. Fare clic su **Execute** (Esegui).

   Dopo alcuni minuti, le macchine virtuali del server Rancher non dovrebbero più essere visibili nell'elenco host e cluster di vSphere Client. Dopo la rimozione, puoi utilizzare il controllo del cloud ibrido NetApp per ridistribuire Rancher su NetApp HCI.

Ulteriori informazioni

- "Risoluzione dei problemi di implementazione del rancher"
- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Manutenzione dell’hardware della serie H.

Panoramica sulla manutenzione dell’hardware della serie H.

Per garantire il funzionamento ottimale del sistema, è necessario eseguire attività di manutenzione dell’hardware, come la sostituzione di nodi difettosi, la sostituzione di dischi guasti nei nodi di storage e così via.

Di seguito sono riportati i collegamenti alle attività di manutenzione dell’hardware:

- "Sostituire lo chassis 2U serie H."
- "Sostituire le unità di alimentazione CC nei nodi H615C e H610S"
- "Sostituire i DIMM nei nodi di calcolo"
- "Sostituire le unità per i nodi di storage"
- "Sostituire i nodi H410C"
- "Sostituire i nodi H410S"
- "Sostituire i nodi H610C e H615C"
- "Sostituire i nodi H610S"
- "Sostituire le unità di alimentazione"
- "Sostituire gli switch SN2010, SN2100 e SN2700"
- "Sostituire il nodo di storage in un cluster a due nodi"

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Plug-in NetApp Element per server vCenter"
- "*TR-4820: Guida rapida alla pianificazione delle reti NetApp HCI*"
- "NetApp Configuration Advisor" 5.8.1 o successivo tool di convalida della rete

Sostituire lo chassis 2U serie H.

Se lo chassis presenta un guasto alla ventola o un problema di alimentazione, sostituirlo il prima possibile. Le fasi della procedura di sostituzione dello chassis dipendono dalla configurazione NetApp HCI e dalla capacità del cluster, che richiedono un’attenta considerazione e pianificazione. Contattare il supporto NetApp per ricevere assistenza e per ordinare uno chassis sostitutivo.

A proposito di questa attività

Prima di sostituire il telaio, considerare quanto segue:

- Il rack dispone di spazio aggiuntivo per un nuovo chassis?
- Uno chassis dell’implementazione dispone di slot di nodo inutilizzati?
- Se il rack dispone di spazio aggiuntivo, è possibile spostare ciascuno dei nodi dallo chassis guasto al

nuovo chassis, uno alla volta? Tenere presente che questo processo potrebbe richiedere tempo.

- Il cluster di storage può rimanere online quando si rimuovono i nodi che fanno parte dello chassis guasto?
- Le macchine virtuali (VM) e il cluster ESXi sono in grado di gestire il carico di lavoro quando si rimuovono i nodi di calcolo che fanno parte dello chassis guasto?

Opzioni di sostituzione

Scegliere una delle seguenti opzioni:Sostituire lo chassis quando è disponibile ulteriore spazio inutilizzato nel rack
Sostituire lo chassis quando non è disponibile spazio aggiuntivo inutilizzato nel rack

Sostituire lo chassis quando è disponibile ulteriore spazio inutilizzato nel rack

Se il rack dispone di spazio aggiuntivo, è possibile installare il nuovo chassis e spostare i nodi uno alla volta nel nuovo chassis. Se uno degli chassis installati dispone di slot di nodo inutilizzati, è possibile spostare i nodi dallo chassis guasto agli slot inutilizzati uno alla volta, quindi rimuovere lo chassis guasto. Prima di eseguire la procedura, assicurarsi che le lunghezze dei cavi siano sufficienti e che le porte dello switch siano disponibili.

> I passaggi per lo spostamento dei nodi di calcolo sono diversi dai passaggi per lo spostamento dei nodi di storage. Prima di spostarli, assicurarsi che i nodi siano chiusi correttamente. Dopo aver spostato tutti i nodi dallo chassis guasto, rimuovere lo chassis dal rack e restituirlo a NetApp.

Installare il nuovo telaio

È possibile installare il nuovo chassis nello spazio rack disponibile e spostare i nodi in esso.

Di cosa hai bisogno

- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o di un'altra protezione antistatica.
- Si dispone del telaio sostitutivo.
- Si dispone di un ascensore o di due o più persone per eseguire le fasi.
- Hai un cacciavite Phillips n. 1.

Fasi

1. Protezione antistatica.
2. Disimballare lo chassis sostitutivo. Conservare la confezione per quando si restituisce lo chassis guasto a NetApp.
3. Inserire le guide spedite insieme al telaio.
4. Far scorrere lo chassis sostitutivo nel rack.

   > Durante l'installazione del telaio, utilizzare sempre personale sufficiente o un sollevatore.

5. Fissare lo chassis al rack con le viti a testa zigrinata per il montaggio anteriore e serrare le viti con il cacciavite.

Spostare un nodo di calcolo

Prima di spostare un nodo di calcolo sul nuovo chassis o su uno chassis esistente che dispone di slot aggiuntivi inutilizzati, è necessario migrare le macchine virtuali (VM), arrestare correttamente il nodo ed etichettare i cavi inseriti nel nodo.

Assicurarsi di disporre di una protezione antistatica quando si sposta il nodo.

Fasi

1. Prendere nota del numero di serie del nodo riportato sull'adesivo sul retro del nodo.
2. In VMware vSphere Web Client, selezionare **host e cluster**, selezionare un nodo (host), quindi selezionare **Monitor > hardware Status > Sensors**.
3. Nella sezione **Sensori**, cercare il numero di serie annotato dall'adesivo sul retro del nodo.
4. Una volta trovato il numero di serie corrispondente, migrare le macchine virtuali su un altro host disponibile.

   Consultare la documentazione VMware per le fasi della migrazione.

5. Fare clic con il pulsante destro del mouse sul nodo e selezionare **alimentazione > Arresta il sistema**. A questo punto, è possibile rimuovere fisicamente il nodo dallo chassis.
6. Etichettare il nodo e tutti i cavi sul retro del nodo.
7. Rimuovere il nodo dal telaio tirando verso il basso la maniglia della camma sul lato destro di ciascun nodo ed estraendolo con entrambe le maniglie della camma.
8. Reinstallare il nodo nel nuovo chassis spingendo il nodo fino a quando non si sente uno scatto. Le etichette collegate al nodo prima della rimozione sono la guida per l'utente. Il nodo si accende automaticamente quando viene installato correttamente.

   Assicurarsi di supportare il nodo da sotto quando lo si installa. Non esercitare una forza eccessiva mentre si spinge il nodo nel telaio.

   Se si esegue l'installazione nel nuovo chassis, assicurarsi di installare il nodo nello slot originale dello chassis.

9. Ricollegare i cavi alle stesse porte sul retro del nodo. Le etichette presenti sui cavi quando sono stati scollegati sono di aiuto.

   Assicurarsi di non forzare i cavi nelle porte per evitare di danneggiare i cavi, le porte o entrambi.

10. Verificare che il nodo di calcolo (host) sia elencato nel cluster ESXi in VMware vSphere Web Client.
11. Eseguire questi passaggi per tutti i nodi di calcolo nello chassis guasto.

Spostare un nodo di storage

Prima di spostare i nodi di storage nel nuovo chassis, è necessario rimuovere i dischi, arrestare correttamente i nodi ed etichettare tutti i componenti.

Fasi

1. Identificare il nodo che si intende rimuovere come segue:
   a. Annotare il numero di serie del nodo dall'etichetta sul retro del nodo.
   b. Nel client Web VMware vSphere, selezionare **Gestione NetApp Element** e copiare l'indirizzo IP MVIP.
   c. Utilizzare l'indirizzo IP MVIP in un browser Web per accedere all'interfaccia utente del software NetApp Element con il nome utente e la password configurati nel motore di implementazione NetApp.

d. Selezionare **Cluster > Nodes** (cluster > nodi).

e. Abbinare il numero di serie annotato con il numero di serie (codice di matricola) elencato.

f. Annotare l'ID del nodo.

2. Dopo aver identificato il nodo, allontanare le sessioni iSCSI dal nodo utilizzando la seguente chiamata API: `wget --no-check-certificate -q --user=<USER> --password=<PASS> -O - --post-data '{ "method":"MovePrimariesAwayFromNode", "params":{"nodeID":<NODEID>} }' https://<MVIP>/json-rpc/8.0`MVIP è l'indirizzo IP MVIP, NODEID è l'ID del nodo, USER è il nome utente configurato nel motore di implementazione NetApp quando si imposta NetApp HCI e PASS è la password configurata nel motore di implementazione NetApp quando si imposta NetApp HCI.

3. Selezionare **Cluster > Drives** per rimuovere i dischi associati al nodo.

> Prima di rimuovere il nodo, attendere che le unità rimosse vengano visualizzate come disponibili.

4. Selezionare **Cluster > Nodes > Actions > Remove** (cluster > nodi > azioni > Rimuovi) per rimuovere il nodo.

5. Utilizzare la seguente chiamata API per arrestare il nodo: `wget --no-check-certificate -q --user=<USER> --password=<PASS> -O - --post-data '{ "method":"Shutdown", "params":{"option":"halt", "nodes":[ <NODEID>]} }' https://<MVIP>/json-rpc/8.0`MVIP è l'indirizzo IP MVIP, NODEID è l'ID del nodo, USER è il nome utente configurato nel motore di implementazione NetApp quando si imposta NetApp HCI e PASS è la password configurata nel motore di implementazione NetApp quando si imposta NetApp HCI. Una volta spento il nodo, è possibile rimuoverlo fisicamente dallo chassis.

6. Rimuovere le unità dal nodo nello chassis come indicato di seguito:

   a. Rimuovere il pannello.

   b. Etichettare i dischi.

   c. Aprire la maniglia della camma ed estrarre con cautela ciascuna unità con entrambe le mani.

   d. Posizionare i dischi su una superficie piana antistatica.

7. Rimuovere il nodo dal telaio come indicato di seguito:

   a. Etichettare il nodo e i cavi ad esso collegati.

   b. Tirare verso il basso la maniglia della camma sul lato destro di ciascun nodo ed estrarre il nodo utilizzando entrambe le maniglie della camma.

8. Reinstallare il nodo nello chassis spingendo il nodo fino a quando non si sente uno scatto. Le etichette collegate al nodo prima della rimozione sono la guida per l'utente.

> Assicurarsi di supportare il nodo da sotto quando lo si installa. Non esercitare una forza eccessiva mentre si spinge il nodo nel telaio.

> Se si esegue l'installazione nel nuovo chassis, assicurarsi di installare il nodo nello slot originale dello chassis.

9. Installare i dischi nei rispettivi slot nel nodo premendo la maniglia della camma su ciascun disco fino a quando non scatta in posizione.

10. Ricollegare i cavi alle stesse porte sul retro del nodo. Le etichette applicate ai cavi quando vengono scollegati saranno di aiuto.

> Assicurarsi di non forzare i cavi nelle porte per evitare di danneggiare i cavi, le porte o entrambi.

11. Una volta acceso il nodo, aggiungerlo al cluster.

> Potrebbero essere necessari fino a 2 minuti per l'aggiunta e la visualizzazione del nodo in **nodi > attivo**.

12. Aggiungere i dischi.
13. Eseguire questa procedura per tutti i nodi di storage nello chassis.

Sostituire lo chassis quando non è disponibile spazio aggiuntivo inutilizzato nel rack

Se il rack non dispone di spazio aggiuntivo e se nessuno degli chassis dell'implementazione dispone di slot di nodo inutilizzati, è necessario determinare quali elementi possono rimanere in linea, se necessario, prima di eseguire la procedura di sostituzione.

A proposito di questa attività

Prima di sostituire lo chassis, tenere in considerazione i seguenti punti:

- Il cluster di storage può rimanere online senza i nodi di storage nello chassis guasto? Se la risposta è no, è necessario arrestare tutti i nodi (sia di calcolo che di storage) nell'implementazione di NetApp HCI. Se la risposta è sì, è possibile arrestare solo i nodi di storage nello chassis guasto.
- Le macchine virtuali e il cluster ESXi possono rimanere online senza i nodi di calcolo nello chassis guasto? Se la risposta è no, è necessario arrestare o migrare le macchine virtuali appropriate per poter arrestare i nodi di calcolo nello chassis guasto. Se la risposta è sì, è possibile arrestare solo i nodi di calcolo nello chassis guasto.

Chiudere un nodo di calcolo

Prima di spostare il nodo di calcolo nel nuovo chassis, è necessario migrare le macchine virtuali, spegnerle correttamente ed etichettare i cavi inseriti nel nodo.

Fasi

1. Prendere nota del numero di serie del nodo riportato sull'adesivo sul retro del nodo.
2. In VMware vSphere Web Client, selezionare **host e cluster**, selezionare un nodo (host), quindi selezionare **Monitor > hardware Status > Sensors**.
3. Nella sezione **Sensori**, cercare il numero di serie annotato dall'adesivo sul retro del nodo.
4. Una volta trovato il numero di serie corrispondente, migrare le macchine virtuali su un altro host disponibile.

   > Consultare la documentazione VMware per le fasi della migrazione.

5. Fare clic con il pulsante destro del mouse sul nodo e selezionare **alimentazione > Arresta il sistema**. A questo punto, è possibile rimuovere fisicamente il nodo dallo chassis.

Chiudere un nodo di storage

Vedere la procedura qui.

Rimuovere il nodo

Rimuovere con attenzione il nodo dallo chassis ed etichettare tutti i componenti. I passaggi per rimuovere fisicamente il nodo sono gli stessi per i nodi di storage e di calcolo. Per un nodo di storage, rimuovere l'unità prima di rimuovere il nodo.

Fasi

1. Per un nodo di storage, rimuovere le unità dal nodo nello chassis come segue:
   a. Rimuovere il pannello.
   b. Etichettare i dischi.
   c. Aprire la maniglia della camma ed estrarre con cautela ciascuna unità con entrambe le mani.
   d. Posizionare i dischi su una superficie piana antistatica.
2. Rimuovere il nodo dal telaio come indicato di seguito:
   a. Etichettare il nodo e i cavi ad esso collegati.
   b. Tirare verso il basso la maniglia della camma sul lato destro di ciascun nodo ed estrarre il nodo utilizzando entrambe le maniglie della camma.
3. Eseguire questa procedura per tutti i nodi che si desidera rimuovere. A questo punto, è possibile rimuovere lo chassis guasto.

Sostituire il telaio

Se il rack non dispone di spazio aggiuntivo, disinstallare lo chassis guasto e sostituirlo con il nuovo chassis.

Fasi

1. Protezione antistatica.
2. Disimballare lo chassis sostitutivo e conservarlo su una superficie piana. Conservare la confezione per quando si restituisce l'unità guasta a NetApp.
3. Rimuovere lo chassis guasto dal rack e posizionarlo su una superficie piana.

   Utilizzare una manodopera o un sollevatore sufficienti durante lo spostamento di un telaio.

4. Rimuovere le guide.
5. Installare le nuove guide fornite con il telaio sostitutivo.
6. Far scorrere lo chassis sostitutivo nel rack.
7. Fissare lo chassis al rack con le viti a testa zigrinata per il montaggio anteriore e serrare le viti con il cacciavite.
8. Installare i nodi nel nuovo chassis come segue:
   a. Reinstallare il nodo nello slot originale dello chassis spingendo il nodo fino a udire uno scatto. Le etichette che hai collegato al nodo prima della rimozione lo aiutano a guidare l'utente.

      Assicurarsi di supportare il nodo da sotto quando lo si installa. Non esercitare una forza eccessiva mentre si spinge il nodo nel telaio.

b. Per i nodi di storage, installare i dischi nei rispettivi slot nel nodo premendo la maniglia CAM su ciascun disco fino a quando non scatta in posizione.

c. Ricollegare i cavi alle stesse porte sul retro del nodo. Le etichette applicate ai cavi quando vengono scollegati sono di ausilio.

> Assicurarsi di non forzare i cavi nelle porte per evitare di danneggiare i cavi, le porte o entrambi.

9. Assicurarsi che i nodi siano online come segue:

Opzione	Fasi
Se tutti i nodi (storage e calcolo) sono stati reinstallati nell'implementazione di NetApp HCI	a. In VMware vSphere Web Client, verificare che i nodi di calcolo (host) siano elencati nel cluster ESXi. b. Nel plug-in Element per il server vCenter, verificare che i nodi di storage siano elencati come attivi.
Se sono stati reinstallati solo i nodi nello chassis guasto	a. In VMware vSphere Web Client, verificare che i nodi di calcolo (host) siano elencati nel cluster ESXi. b. Nel plug-in Element per il server vCenter, selezionare **Cluster > Nodes > Pending**. c. Selezionare il nodo e scegliere **Aggiungi**. > Potrebbero essere necessari fino a 2 minuti per l'aggiunta e la visualizzazione del nodo in **nodi > attivo**. d. Selezionare **Drives** (unità). e. Dall'elenco Available (disponibili), aggiungere le unità. f. Eseguire questa procedura per tutti i nodi di storage reinstallati.

10. Verificare che i volumi e gli archivi dati siano disponibili e accessibili.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire le unità di alimentazione CC nei nodi H615C e H610S

I nodi H615C e H610S supportano due alimentatori da –48 V a –60 V CC. Queste unità sono disponibili come add-on opzionali quando si ordinano nodi H615C o H610S. È possibile utilizzare queste istruzioni per rimuovere le unità di alimentazione CA nello chassis e sostituirle con unità di alimentazione CC oppure per sostituire un'unità di alimentazione CC difettosa con una nuova.

Di cosa hai bisogno

- Se si sostituisce un alimentatore CC difettoso, è stata fornita un'unità di alimentazione CC sostitutiva.
- Se si stanno sostituendo le unità di alimentazione CA dello chassis con unità CC, si è preso in considerazione il downtime per la procedura.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o si sono prese altre precauzioni antistatiche.
- Hai garantito che i requisiti di alimentazione siano soddisfatti:
  - Tensione di alimentazione: –(48-60) V CC
  - Consumo di corrente: 37 a (massimo)
  - Requisiti per l'interruttore: Interruttore da 40 A.
- Hai garantito che i materiali nel tuo ambiente siano conformi alle specifiche RoHS.
- Hai garantito che i requisiti dei cavi siano soddisfatti:
  - Un cavo nero UL 10 AWG, massimo 2 m (intrecciato) [–(48-60) V CC]
  - Un cavo rosso UL 10 AWG, massimo 2 m (intrecciato) [ritorno V CC]
  - Un cavo UL 10 AWG, massimo 2 m verde/giallo, verde con striscia gialla, trefolo (messa a terra di sicurezza)

A proposito di questa attività

La procedura si applica ai seguenti modelli di nodi:

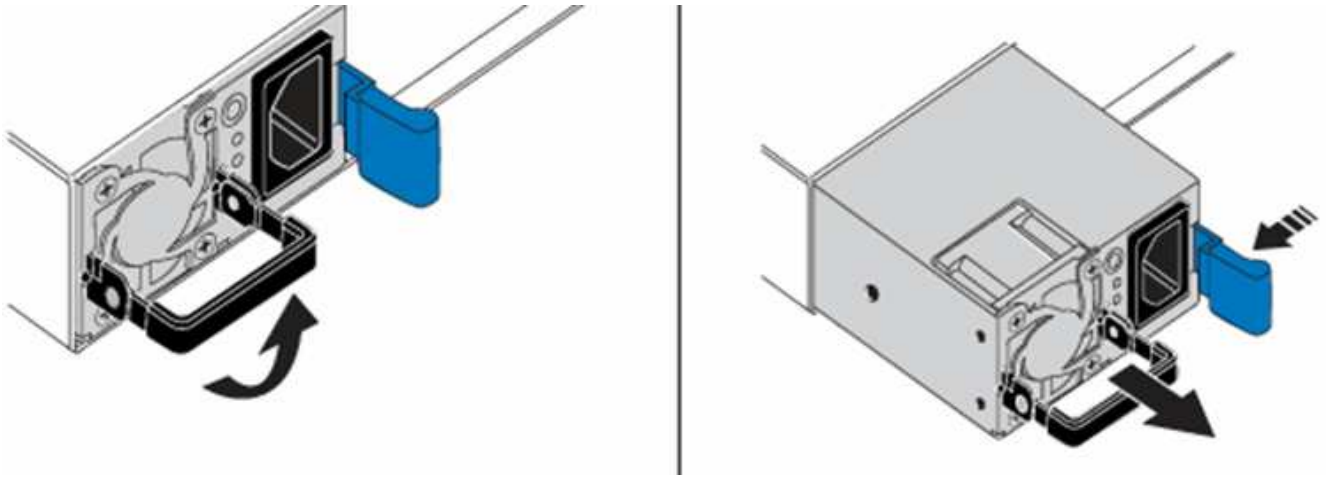
- Uno chassis di calcolo H615C per unità rack (1U)
- Chassis storage 1U H610S

> Nel caso di H615C e H610S, i termini "nodo" e "chassis" sono utilizzati in modo intercambiabile perché nodo e chassis non sono componenti separati, a differenza del caso di chassis 2U a quattro nodi.

> Non è possibile combinare unità di alimentazione CA e CC nell'installazione.

Fasi

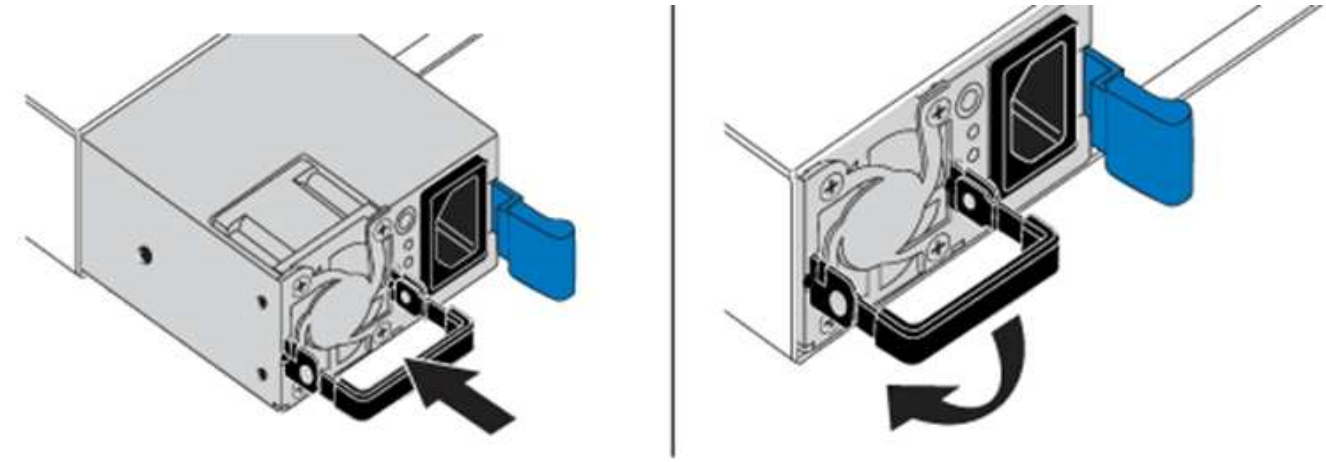
1. Spegnere le unità di alimentazione e scollegare i cavi di alimentazione. Se si sostituisce un alimentatore CC difettoso, spegnere la fonte di alimentazione e rimuovere tutti i cavi inseriti nel connettore blu.
2. Sollevare la maniglia della camma e premere il fermo blu per estrarre l'alimentatore.



L'illustrazione è un esempio. La posizione dell'alimentatore nello chassis e il colore del pulsante di rilascio variano a seconda del tipo di chassis in uso.

Assicurarsi di utilizzare entrambe le mani per sostenere il peso dell'alimentatore.

3. Allineare con entrambe le mani i bordi dell'alimentatore con l'apertura del telaio, spingere delicatamente l'unità nel telaio utilizzando la maniglia della camma fino a bloccarla in posizione e riportare la maniglia della camma in posizione verticale.



4. Collegare le unità di alimentazione CC. Assicurarsi che la fonte di alimentazione sia spenta durante il cablaggio dell'alimentatore CC e della fonte di alimentazione.
   a. Inserire i cavi nero, rosso e verde/giallo nei connettori blu.
   b. Inserire il connettore blu nelle unità di alimentazione CC e nella fonte di alimentazione.

5. Accendere le unità di alimentazione CC.

> I LED dell'alimentatore sono accesi quando l'alimentatore CC è in linea. Le spie LED verdi indicano che le unità di alimentazione funzionano correttamente.

6. Restituire l'unità difettosa a NetApp seguendo le istruzioni riportate nella confezione.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire i DIMM nei nodi di calcolo

È possibile sostituire un modulo DIMM (Dual Inline Memory Module) guasto nei nodi di calcolo NetApp HCI invece di sostituire l'intero nodo.

Di cosa hai bisogno

- Prima di iniziare questa procedura, dovresti aver contattato il supporto NetApp e aver ricevuto una parte di ricambio. Durante l'installazione della sostituzione verrà fornito supporto. Se non l'hai già fatto, contatta "Supporto".
- Hai pianificato il downtime del sistema, perché devi spegnere o spegnere e riaccendere il nodo e avviare il nodo in NetApp Safe Mode per accedere all'interfaccia utente del terminale (TUI).

A proposito di questa attività

Questa procedura si applica ai seguenti modelli di nodi di calcolo:

- Nodi H410C. Un nodo H410C viene inserito in uno chassis NetApp HCI 2U.
- Nodo H610C. Nel telaio è integrato un nodo H610C.
- Nodo H615C. Nel telaio è integrato un nodo H615C.

> I nodi H410C e H615C includono DIMM di diversi vendor. Assicurarsi di non combinare DIMM di vendor diversi in un unico chassis.

> I termini "chassis" e "nodo" sono utilizzati in modo intercambiabile nel caso di H610C e H615C, perché il nodo e lo chassis non sono componenti separati.

Di seguito sono riportati i passaggi necessari per sostituire i DIMM nei nodi di calcolo:

- Preparare la sostituzione del DIMM
- Sostituire il modulo DIMM dal telaio

Preparare la sostituzione del DIMM

Quando si verificano problemi con il DIMM, VMware ESXi visualizza avvisi, ad esempio `Memory Configuration Error`, `Memory Uncorrectable ECC`, `Memory Transition to Critical`, e. `Memory Critical Overtemperature`. Anche se gli avvisi scompaiono dopo qualche istante, il problema hardware potrebbe persistere. Eseguire la diagnosi e risolvere il problema del DIMM guasto. È possibile ottenere informazioni sul DIMM guasto da vCenter Server. Se sono necessarie ulteriori informazioni rispetto a quelle disponibili da vCenter Server, è necessario eseguire il check dell'hardware nell'interfaccia telefonica utente (TUI).

Fasi

1. Identificare lo slot che ha registrato l'errore come segue:
   a. Per H615C, procedere come indicato di seguito:
      i. Accedere all'interfaccia utente BMC.
      ii. Selezionare **Log & Report** > **IPMI Event Log**.
      iii. Nel registro eventi, individuare l'errore di memoria e identificare lo slot in cui viene registrato l'errore.

   b. Per H410C, procedere come indicato di seguito:
      i. Accedere all'interfaccia utente BMC.
      ii. Selezionare **Server Health** > **Health Event Log**.
      iii. Nel registro eventi, individuare l'errore di memoria e identificare lo slot in cui viene registrato l'errore.

2. Eseguire la procedura per identificare il codice del produttore del modulo DIMM.

> I nodi H410C e H615C includono DIMM di diversi produttori. Non utilizzare tipi di DIMM diversi nello stesso chassis. Identificare il produttore del modulo DIMM guasto e ordinare un modulo sostitutivo dello stesso tipo.

   a. Accedere a BMC per avviare la console sul nodo.
   b. Premere **F2** sulla tastiera per accedere al menu **Customize System/View Logs** (Personalizza sistema/Visualizza registri).

c. Inserire la password quando richiesto.

> La password deve corrispondere a quella configurata nel motore di implementazione NetApp al momento della configurazione di NetApp HCI.

a. Dal menu System Customization (Personalizzazione sistema), premere la freccia verso il basso per passare a Troubleshooting Options (Opzioni di risoluzione dei problemi), quindi premere **Invio**.

b. Dal menu Troubleshooting Mode Options (Opzioni modalità di risoluzione dei problemi), utilizzare la

freccia su o giù per attivare la shell ESXi e SSH, che sono disabilitati per impostazione predefinita.

c. Premere due volte il tasto <Esc> per uscire dalle opzioni di risoluzione dei problemi.

d. Eseguire `smbiosDump` utilizzare una delle seguenti opzioni:

Opzione	Fasi
Opzione A.	i. Connettersi all'host ESXi (nodo di calcolo) utilizzando l'indirizzo IP dell'host e le credenziali root definite. ii. Eseguire `smbiosDump` comando. Vedere il seguente esempio di output: `Memory Device:#30 Location: "P1-DIMMA1" Bank: "P0_Node0_Channel0_Dimm0" Manufacturer:"Samsung" Serial: "38EB8380" Asset Tag: "P1-DIMMA1_AssetTag (date:18/15)" Part Number: "M393A4K40CB2-CTD" Memory Array: #29 Form Factor: 0x09(DIMM) Type: 0x1a (DDR4) Type Detail: 0x0080 (Synchronous) Data Width: 64 bits (+8 ECC bits) Size: 32 GB`
Opzione B	i. Premere **Alt + F1** per inserire la shell e accedere al nodo per eseguire il comando.

3. Contatta il supporto NetApp per ricevere assistenza sui passi successivi. Il supporto NetApp richiede le seguenti informazioni per elaborare la sostituzione di una parte:
   - Numero di serie del nodo
   - Nome del cluster
   - Dettagli del registro eventi di sistema dall'interfaccia utente BMC
   - Output da `smbiosDump` comando

Sostituire il modulo DIMM dal telaio

Prima di rimuovere e sostituire fisicamente il modulo DIMM guasto nel telaio, assicurarsi di aver eseguito tutte le operazioni "fasi preparatorie".

I DIMM devono essere sostituiti negli stessi slot da cui sono stati rimossi.

Fasi

1. Accedere al nodo accedendo a vCenter Server.
2. Fare clic con il pulsante destro del mouse sul nodo che segnala l'errore e selezionare l'opzione per impostare il nodo in modalità di manutenzione.
3. Migrare le macchine virtuali (VM) su un altro host disponibile.

   Consultare la documentazione VMware per le fasi della migrazione.

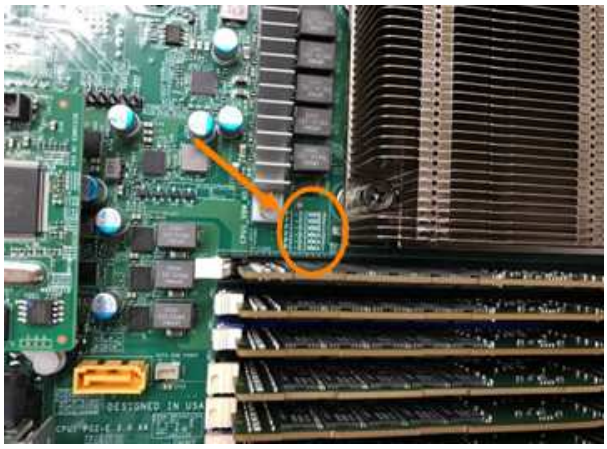
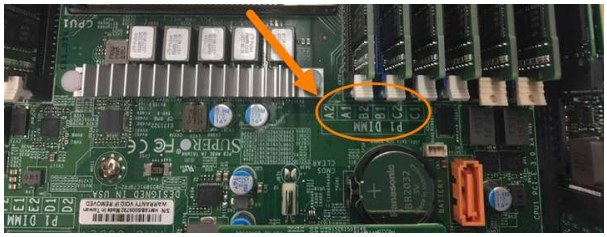
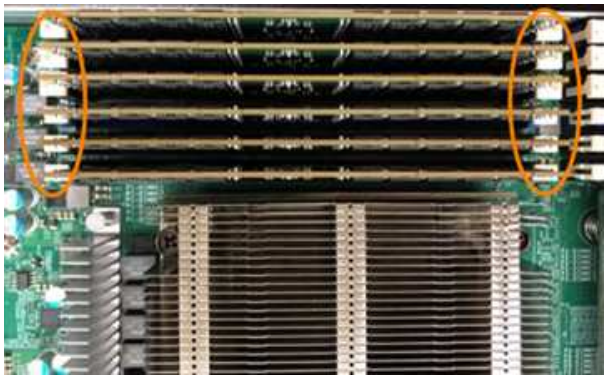
4. Spegnere lo chassis o il nodo.

   Per uno chassis H610C o H615C, spegnere lo chassis. Per i nodi H410C in uno chassis 2U a quattro nodi, spegnere solo il nodo con il DIMM guasto.

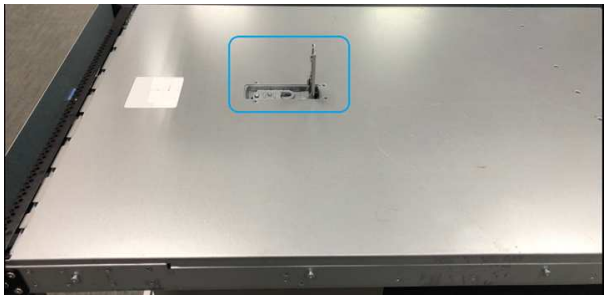
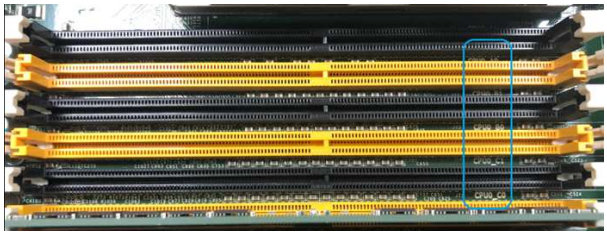
5. Rimuovere i cavi di alimentazione e di rete, estrarre con cautela il nodo o lo chassis dal rack e posizionarlo su una superficie piana e antistatica.

   Prendere in considerazione l'utilizzo di fascette per cavi.

6. Applicare una protezione antistatica prima di aprire il coperchio dello chassis per sostituire il DIMM.
7. Eseguire i passaggi relativi al modello di nodo:

Modello di nodo	Fasi
H410C	a. Individuare il DIMM guasto facendo corrispondere il numero/ID dello slot annotato in precedenza con la numerazione sulla scheda madre. Di seguito sono riportate immagini di esempio che mostrano i numeri degli slot DIMM sulla scheda madre:   b. Spingere i due fermi verso l'esterno ed estrarre con cautela il modulo DIMM. Ecco un'immagine di esempio che mostra i fermi di fissaggio:  c. Installare correttamente il modulo DIMM sostitutivo. Quando si inserisce correttamente il DIMM nello slot, i due fermi si bloccano in posizione. Assicurarsi di toccare solo le estremità posteriori del DIMM. Se si premono altre parti del DIMM, l'hardware potrebbe danneggiarsi.
	Installare il nodo nello chassis NetApp HCI,

Modello di nodo	Fasi
H610C	a. Sollevare il coperchio come mostrato nell'immagine seguente:  b. Allentare le quattro viti di bloccaggio blu sul retro del nodo. Di seguito è riportato un esempio di immagine che mostra la posizione delle due viti di bloccaggio; le altre due si trovano sull'altro lato del nodo:  c. Rimuovere entrambi gli spazi vuoti della scheda PCI. d. Rimuovere la GPU e il coperchio del flusso d'aria. e. Individuare il DIMM guasto facendo corrispondere il numero/ID dello slot annotato in precedenza con la numerazione sulla scheda madre. Di seguito è riportato un esempio di immagine che mostra la posizione dei numeri degli slot DIMM sulla scheda madre:

Modello di nodo	Fasi
H615C	a. Sollevare il coperchio come mostrato nell'immagine seguente:  b. Rimuovere la GPU (se nel nodo H615C è installata la GPU) e il coperchio del flusso d'aria.  c. Individuare il DIMM guasto facendo corrispondere il numero/ID dello slot annotato in precedenza con la numerazione sulla scheda madre. Di seguito è riportato un esempio di immagine che mostra la posizione dei numeri degli slot DIMM sulla scheda madre:  d. Spingere i due fermi verso l'esterno ed estrarre con cautela il modulo DIMM. e. Installare correttamente il modulo DIMM sostitutivo. Quando si inserisce correttamente il DIMM nello slot, i due fermi si bloccano in posizione. Assicurarsi di toccare solo le estremità posteriori del DIMM. Se si premono altre parti del DIMM, l'hardware potrebbe danneggiarsi.
	Riposizionare il coperchio del flusso d'aria.

8. Inserire i cavi di alimentazione e di rete. Assicurarsi che tutti i LED delle porte si accendano.
9. Premere il pulsante di accensione nella parte anteriore del nodo se non si accende automaticamente quando viene installato.
10. Una volta visualizzato il nodo in vSphere, fare clic con il pulsante destro del mouse sul nome e uscire dalla modalità di manutenzione.
11. Verificare le informazioni sull'hardware come indicato di seguito:
    a. Accedere all'interfaccia utente del BMC (Baseboard Management Controller).
    b. Selezionare **sistema > informazioni hardware** e controllare i DIMM elencati.
    f. Rimettere il coperchio sul nodo.
    g. Installare lo chassis H610C nel rack, assicurandosi che scatti quando lo si inserisce in posizione.

Cosa succederà

Una volta ripristinato il normale funzionamento del nodo, in vCenter, selezionare la scheda Summary (Riepilogo) per verificare che la capacità di memoria sia quella prevista.

Se il DIMM non è installato correttamente, il nodo funziona normalmente ma con una capacità di memoria inferiore al previsto.

Dopo la procedura di sostituzione del modulo DIMM, è possibile eliminare gli avvisi e gli errori nella scheda hardware Status (Stato hardware) di vCenter. È possibile eseguire questa operazione se si desidera cancellare la cronologia degli errori relativi all'hardware sostituito. "Scopri di più".

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire le unità per i nodi di storage

Se un disco è difettoso o se il livello di usura del disco scende al di sotto di una soglia, sostituirlo. Gli allarmi nell'interfaccia utente del software Element e nel client Web VMware vSphere avvisano l'utente quando un disco si guasta o sta per guastarsi. È possibile sostituire a caldo un disco guasto.

A proposito di questa attività

Questa procedura serve per sostituire i dischi nei nodi di storage H410S e H610S. La rimozione di un disco porta il disco offline. Tutti i dati presenti sul disco vengono rimossi e migrati su altri dischi del cluster. La migrazione dei dati ad altri dischi attivi nel sistema può richiedere da alcuni minuti a un'ora, a seconda dell'utilizzo della capacità e dell'i/o attivo nel cluster.

Best practice per la gestione dei dischi

Attenersi alle seguenti Best practice per la gestione dei dischi:

- Tenere l'unità nella busta ESD fino a quando non si è pronti per l'installazione.
- Aprire il sacchetto ESD manualmente o tagliare la parte superiore con un paio di forbici.
- Indossare sempre un braccialetto antistatico collegato a terra su una superficie non verniciata dello chassis.

- Utilizzare sempre entrambe le mani durante la rimozione, l'installazione o il trasporto di un disco.
- Non forzare mai un disco nello chassis.
- Utilizzare sempre imballaggi approvati per la spedizione delle unità.
- Non impilare i dischi l'uno sull'altro.

Best practice per l'aggiunta e la rimozione di dischi

Attenersi alle seguenti Best practice per aggiungere dischi al cluster e rimuovere dischi dal cluster:

- Aggiungi tutti i dischi a blocchi e assicurati che la sincronizzazione dei blocchi sia completa prima di aggiungere i dischi slice.
- Per il software Element 10.x e versioni successive, aggiungere tutti i dischi a blocchi contemporaneamente. Assicurarsi di non eseguire questa operazione per più di tre nodi alla volta.
- Per il software Element 9.x e versioni precedenti, aggiungere tre dischi alla volta per sincronizzarli completamente prima di aggiungere il gruppo successivo di tre.
- Rimuovere il disco slice e assicurarsi che la sincronizzazione slice sia completa prima di rimuovere i dischi a blocchi.
- Rimuovere tutti i dischi a blocchi da un singolo nodo alla volta. Assicurarsi che la sincronizzazione di tutti i blocchi sia completa prima di passare al nodo successivo.

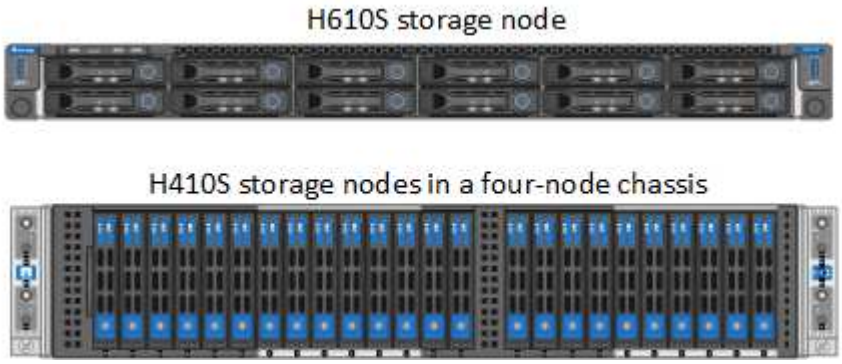
Fasi

1. Rimuovere l'unità dal cluster utilizzando l'interfaccia utente del software NetApp Element o il punto di estensione della gestione NetApp Element nel plug-in Element per il server vCenter.

Opzione	Fasi
Utilizzo dell'interfaccia utente di Element	a. Dall'interfaccia utente di Element, selezionare **Cluster > Drives**. b. Fare clic su **Failed** (guasto) per visualizzare l'elenco dei dischi guasti. c. Annotare il numero di slot del disco guasto. Queste informazioni sono necessarie per individuare il disco guasto nello chassis. d. Fare clic su **azioni** per l'unità che si desidera rimuovere. e. Fare clic su **Rimuovi**. È ora possibile rimuovere fisicamente il disco dallo chassis.

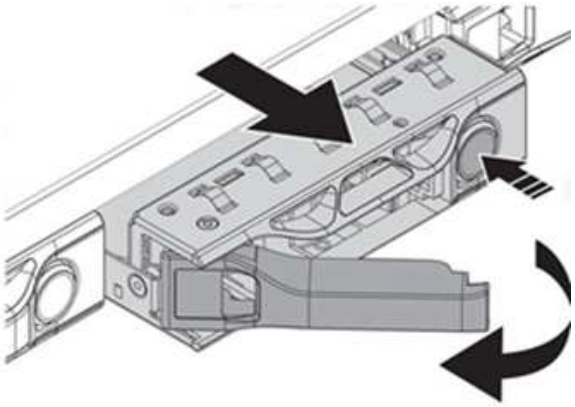
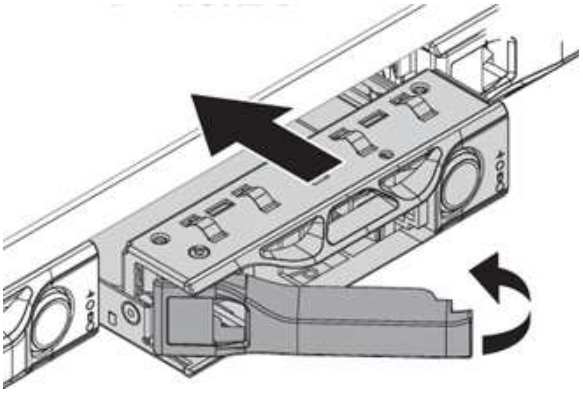
Opzione	Fasi
Utilizzo del plug-in Element per l'interfaccia utente del server vCenter	a. Dal punto di estensione della gestione NetApp Element del client Web vSphere, selezionare **Gestione NetApp Element > cluster**. b. Se vengono aggiunti due o più cluster, assicurarsi che il cluster che si intende utilizzare per l'attività sia selezionato nella barra di navigazione. c. Selezionare **All** dall'elenco a discesa per visualizzare l'elenco completo dei dischi. d. Selezionare la casella di controllo per ciascun disco che si desidera rimuovere. e. Selezionare **Rimuovi unità**. f. Confermare l'azione. Se la capacità non è sufficiente per rimuovere i dischi attivi prima di rimuovere un nodo, viene visualizzato un messaggio di errore quando si conferma la rimozione del disco. Dopo aver risolto l'errore, è possibile rimuovere fisicamente il disco dal telaio.

2. Sostituire l'unità dal telaio:
   a. Disimballare l'unità sostitutiva e posizionarla su una superficie piana e priva di scariche elettrostatiche vicino al rack. Conservare il materiale di imballaggio per quando si restituisce il disco guasto a NetApp. Di seguito è riportato il punto di vista frontale dei nodi di storage H610S e H410S con i dischi:



   b. Eseguire le operazioni in base al modello di nodo:

Modello di nodo	Fasi
H410S	i. Identificare il nodo facendo corrispondere il numero di serie (codice di matricola) con il numero annotato dall'interfaccia utente dell'elemento. Il numero di serie è riportato su un adesivo sul retro di ciascun nodo. Una volta identificato il nodo, è possibile utilizzare le informazioni relative agli slot per identificare lo slot in cui si trova l'unità guasta. I dischi sono disposti in ordine alfabetico da A a D e da 0 a 5. ii. Rimuovere il pannello. iii. Premere il pulsante di rilascio sul disco guasto:  Quando si preme il pulsante di rilascio, la maniglia della camma sulle molle dell'unità si apre parzialmente e l'unità si rilascia dalla scheda intermedia. iv. Aprire la maniglia della camma ed estrarre con cautela l'unità con entrambe le mani. v. Posizionare l'unità su una superficie piana antistatica. vi. Inserire l'unità sostitutiva nello slot completamente nello chassis con entrambe le mani. vii. Premere la maniglia della camma fino a farla scattare in posizione. viii. Reinstallare il pannello. ix. Informare il supporto NetApp in merito alla sostituzione del disco. Il supporto NetApp fornirà istruzioni per la restituzione del disco guasto.

Modello di nodo	Fasi
H610S	i. Far corrispondere il numero di slot del disco guasto dell'interfaccia utente Element con il numero sullo chassis. Il LED sul disco guasto è acceso in ambra. ii. Rimuovere il pannello. iii. Premere il pulsante di rilascio e rimuovere il disco guasto come mostrato nell'illustrazione seguente:  Assicurarsi che la maniglia del vassoio sia completamente aperta prima di provare a far scorrere l'unità fuori dal telaio. iv. Estrarre l'unità e posizionarla su una superficie piana e priva di elettricità statica. v. Premere il pulsante di rilascio sull'unità sostitutiva prima di inserirla nell'alloggiamento. Le molle della maniglia del vassoio dell'unità si aprono.  vi. Inserire l'unità sostitutiva senza esercitare una forza eccessiva. Quando l'unità è inserita completamente, si sente uno scatto. vii. Chiudere con cautela la maniglia del vassoio dell'unità. Reinstallare il pannello. Informare il supporto NetApp in merito alla

3. Aggiungere nuovamente il disco al cluster utilizzando l'interfaccia utente Element o il punto di estensione di gestione NetApp Element nel plug-in Element per il server vCenter.

> Quando si installa un nuovo disco in un nodo esistente, il disco viene automaticamente registrato come **Available** nell'interfaccia utente Element. È necessario aggiungere l'unità al cluster prima che possa partecipare al cluster.

Opzione	Fasi
Utilizzo dell'interfaccia utente di Element	a. Dall'interfaccia utente di Element, selezionare **Cluster > Drives**. b. Selezionare **Available** per visualizzare l'elenco dei dischi disponibili. c. Selezionare l'icona Actions (azioni) per l'unità che si desidera aggiungere e selezionare **Add** (Aggiungi).
Utilizzo del plug-in Element per l'interfaccia utente del server vCenter	a. Dal punto di estensione della gestione NetApp Element del client Web vSphere, selezionare **Gestione NetApp Element > cluster > unità**. b. Dall'elenco a discesa Available (disponibile), selezionare l'unità e scegliere **Add** (Aggiungi). c. Confermare l'azione.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire i nodi H410C

È necessario sostituire un nodo di calcolo in caso di guasto della CPU, altri problemi della scheda madre o in caso di mancata accensione. Le istruzioni si applicano ai nodi H410C. Se si dispone di un nodo di calcolo H410C che esegue il sistema operativo Bootstrap NetApp HCI versione 1.6P1 o successiva, non è necessario sostituire il nodo in caso di guasto del DIMM di memoria; è necessario sostituire solo il DIMM guasto. Se i DIMM nel nodo non presentano guasti, è possibile utilizzarli nel nodo sostitutivo.

> Il nodo sostitutivo deve avere la stessa versione del sistema operativo NetApp HCI Bootstrap degli altri nodi di calcolo nell'installazione di NetApp HCI.
>
> NetApp consiglia di utilizzare il motore di implementazione NetApp per aggiungere un nodo di calcolo sostitutivo. Se non è possibile utilizzare il motore di distribuzione NetApp per l'installazione ESXi, consultare l'articolo della Knowledge base di NetApp "Come installare ESXi sul nodo di calcolo NetApp HCI manualmente".

Di cosa hai bisogno

- Hai determinato che il nodo di calcolo deve essere sostituito.
- Si dispone di un nodo di calcolo sostitutivo. Per ordinare un nodo sostitutivo, contattare il supporto NetApp. Il nodo di calcolo viene spedito con il sistema operativo Bootstrap installato. I nodi vengono spediti dalla fabbrica con la versione più recente del sistema operativo Bootstrap. Potrebbe essere necessario eseguire il processo di ripristino dell'immagine di fabbrica (RTFI) sul nodo nei seguenti scenari:
  - L'installazione corrente di NetApp HCI esegue una versione del sistema operativo Bootstrap precedente alla versione più recente. In questo caso, il processo RTFI esegue il downgrade del nuovo nodo alla versione del sistema operativo in esecuzione nell'installazione di NetApp HCI.
  - Il nodo sostitutivo fornito esegue una versione del sistema operativo di bootstrap precedente alla versione più recente e l'installazione di NetApp HCI in cui viene sostituito il nodo esegue già la versione più recente. In questo caso, il processo RTFI aggiornerà la versione del sistema operativo sul nuovo nodo alla versione più recente. Vedere "Come utilizzare RTFI con una chiave USB (accesso richiesto)" e. "Come RTFI utilizzando BMC (accesso richiesto)".
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o si sono prese altre precauzioni antistatiche.
- Ciascun cavo collegato al nodo di calcolo è etichettato.

A proposito di questa attività

Gli allarmi di VMware vSphere Web Client avvisano l'utente in caso di guasto di un nodo. Il numero di serie del nodo guasto di VMware vSphere Web Client deve corrispondere al numero di serie riportato sull'etichetta sul retro del nodo.

Quando si sostituisce un nodo di calcolo H410C, considerare quanto segue:

- È possibile combinare il nodo di calcolo H410C con i nodi di calcolo e storage NetApp HCI esistenti nello stesso chassis e cluster.
- Il nodo di calcolo H410C funziona solo con tensione di linea elevata (200-240 VCA). Quando si aggiungono nodi H410C a un sistema NetApp HCI esistente, è necessario assicurarsi che i requisiti di alimentazione siano soddisfatti.

Panoramica dei passaggi

Di seguito viene riportata una panoramica generale delle fasi di questa procedura:
Fase 1: Prepararsi a sostituire il nodo di calcolo
Fase 2: Sostituire il nodo di calcolo nel telaio
7 e versioni successive
Fase 4: Aggiungere il nodo di calcolo al cluster
Fase 5: Implementare nuovamente i nodi di controllo per cluster storage a due e tre nodi

Di seguito sono riportate alcune attività aggiuntive che potrebbero essere necessarie se il sistema dispone delle condizioni specifiche a cui sono applicabili:

- "Rimuovere i nodi di controllo per liberare le risorse di calcolo"
- Modificare la password se si riceve un nodo sostitutivo con una password BMC non standard
- Aggiornare il firmware BMC sul nodo

Fase 1: Prepararsi a sostituire il nodo di calcolo

È necessario migrare le macchine virtuali (VM) ospitate sul nodo in un host disponibile e rimuovere il nodo guasto dal cluster. Si dovrebbero ottenere dettagli sul nodo guasto, come il numero di serie e le informazioni di rete.

Fasi

1. In VMware vSphere Web Client, eseguire la procedura per migrare le macchine virtuali su un altro host disponibile.

   Consultare la documentazione VMware per le fasi della migrazione.

2. Eseguire la procedura per rimuovere il nodo dall'inventario. La procedura dipende dalla versione di NetApp HCI installata:

Numero di versione di NetApp HCI	Fasi
NetApp HCI 1.3 e versioni successive	a. Selezionare il nodo guasto e selezionare **Monitor > hardware Status > Sensors**. b. Annotare il numero di serie del nodo guasto. In questo modo, è possibile identificare il nodo nello chassis facendo corrispondere il numero di serie riportato sull'etichetta sul retro del nodo con il numero di serie annotato. c. Fare clic con il pulsante destro del mouse sul nodo guasto e selezionare **connessione > Disconnetti**. d. Selezionare **Sì** per confermare l'azione. e. Fare clic con il pulsante destro del mouse sul nodo guasto e selezionare **Rimuovi dall'inventario**. f. Selezionare **Sì** per confermare l'azione.
Versioni di NetApp HCI precedenti alla 1.3	a. Fare clic con il pulsante destro del mouse sul nodo e selezionare **Rimuovi dall'inventario**. b. Selezionare il nodo guasto e selezionare **Monitor > hardware Status > Sensors**. c. Notare il numero di serie del nodo 0, che è il numero di serie del nodo guasto. In questo modo, è possibile identificare il nodo nello chassis facendo corrispondere il numero di serie riportato sull'etichetta sul retro del nodo con il numero di serie annotato. d. Con il nodo guasto selezionato, selezionare **Manage > Networking > VMkernel adapter** (Gestisci > rete > adattatori VMkernel) e copiare i quattro indirizzi IP elencati. È possibile riutilizzare queste informazioni quando si eseguono le fasi iniziali della configurazione di rete in VMware ESXi.

Fase 2: Sostituire il nodo di calcolo nel telaio

Dopo aver rimosso il nodo guasto dal cluster, è possibile rimuovere il nodo dallo chassis e installare il nodo sostitutivo.

Assicurarsi di disporre di una protezione antistatica prima di eseguire la procedura riportata di seguito.

Fasi

1. Protezione antistatica.
2. Disimballare il nuovo nodo e impostarlo su una superficie piana vicino allo chassis. Conservare il materiale di imballaggio per quando si restituisce il nodo guasto a NetApp.
3. Etichettare ciascun cavo inserito nella parte posteriore del nodo che si desidera rimuovere. Dopo aver installato il nuovo nodo, inserire nuovamente i cavi nelle porte originali.
4. Scollegare tutti i cavi dal nodo.
5. Se si desidera riutilizzare i DIMM, rimuoverli.
6. Tirare verso il basso la maniglia della camma sul lato destro del nodo ed estrarre il nodo utilizzando entrambe le maniglie della camma. La maniglia della camma da tirare verso il basso è dotata di una freccia che indica la direzione di spostamento. L'altra maniglia CAM non si sposta ed è lì per aiutare a estrarre il nodo.

   Supportare il nodo con entrambe le mani quando lo si tira fuori dallo chassis.

7. Posizionare il nodo su una superficie piana. È necessario imballare il nodo e restituirlo a NetApp.
8. Installare il nodo sostitutivo.
9. Spingere il nodo fino a quando non si sente uno scatto.

   Assicurarsi di non esercitare una forza eccessiva quando si fa scorrere il nodo nel telaio.

   Assicurarsi che il nodo si accenda. Se non si accende automaticamente, premere il pulsante di accensione nella parte anteriore del nodo.

10. Se in precedenza sono stati rimossi i DIMM dal nodo guasto, inserirli nel nodo sostitutivo.

    È necessario sostituire i DIMM negli stessi slot da cui sono stati rimossi nel nodo guasto.

11. Ricollegare i cavi alle porte da cui sono stati precedentemente scollegati. Le etichette applicate ai cavi quando sono stati scollegati sono di aiuto.

    Se le prese d'aria sul retro del telaio sono bloccate da cavi o etichette, possono verificarsi guasti prematuri dei componenti dovuti al surriscaldamento. Non forzare i cavi nelle porte, poiché si potrebbero danneggiare i cavi, le porte o entrambe.

    Assicurarsi che il nodo sostitutivo sia cablato nello stesso modo degli altri nodi nello chassis.

Passaggio 3: Rimuovere la risorsa del nodo di calcolo in NetApp HCI 1,7 e versioni successive

In NetApp HCI 1.7 e versioni successive, dopo aver sostituito fisicamente il nodo, è necessario rimuovere la risorsa del nodo di calcolo utilizzando le API del nodo di gestione. Per utilizzare le API REST, il cluster di storage deve eseguire il software NetApp Element 11.5 o versione successiva e dovrebbe essere stato implementato un nodo di gestione con versione 11.5 o successiva.

Fasi

1. Inserire l'indirizzo IP del nodo di gestione seguito da /mnode: `https://[IP address]/mnode`
2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e immettere le credenziali di amministratore del cluster per le autorizzazioni per l'utilizzo delle API.
   a. Inserire il nome utente e la password del cluster.
   b. Selezionare corpo richiesta dall'elenco a discesa tipo se il valore non è già selezionato.
   c. Inserire l'ID client come mnode-client se il valore non è già stato compilato. Non inserire un valore per il client secret.
   d. Selezionare **autorizzare** per avviare una sessione.

   > Se si ottiene il `Auth Error TypeError: Failed to fetch` Messaggio di errore dopo aver tentato di autorizzare, potrebbe essere necessario accettare il certificato SSL per l'MVIP del cluster. Copiare l'indirizzo IP nell'URL token, incollarlo in un'altra scheda del browser e autorizzare di nuovo. Se si tenta di eseguire un comando dopo la scadenza del token, viene visualizzato `Error: UNAUTHORIZED` errore. Se ricevi questa risposta, autorizzi di nuovo.

3. Chiudere la finestra di dialogo Available Authorization (autorizzazioni disponibili).
4. Selezionare **GET/Assets**.
5. Selezionare **Provalo**.
6. Selezionare **Esegui**. Scorrere verso il basso nel corpo della risposta fino alla sezione Compute (calcolo) e copiare i valori padre e id per il nodo di calcolo guasto.
7. Selezionare **DELETE/assets/{asset_id}/compute-nodes/{compute_id}**.
8. Selezionare **Provalo**. Inserire i valori di origine e id ottenuti al punto 7.
9. Selezionare **Esegui**.

Fase 4: Aggiungere il nodo di calcolo al cluster

È necessario aggiungere nuovamente il nodo di calcolo al cluster. La procedura varia a seconda della versione di NetApp HCI in esecuzione.

NetApp HCI 1.6P1 e versioni successive

È possibile utilizzare NetApp Hybrid Cloud Control solo se l'installazione di NetApp HCI viene eseguita sulla versione 1.6P1 o successiva.

Di cosa hai bisogno

- Assicurarsi che l'istanza di vSphere utilizzata da NetApp HCI disponga di licenze vSphere Enterprise Plus se si sta espandendo un'implementazione con Virtual Distributed Switch.

- Assicurarsi che nessuna delle istanze vCenter o vSphere in uso con NetApp HCI disponga di licenze scadute.
- Assicurarsi di disporre di indirizzi IPv4 liberi e inutilizzati sullo stesso segmento di rete dei nodi esistenti (ciascun nuovo nodo deve essere installato sulla stessa rete dei nodi esistenti del suo tipo).
- Assicurarsi di disporre delle credenziali dell'account amministratore vCenter.
- Assicurarsi che ogni nuovo nodo utilizzi la stessa topologia di rete e lo stesso cablaggio dei cluster di calcolo o di storage esistenti.
- "Gestire gli iniziatori e i gruppi di accesso ai volumi" per il nuovo nodo di calcolo.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

```
https://<ManagementNodeIP>
```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Nel riquadro di espansione dell'installazione, selezionare **Espandi**.
4. Accedere al motore di implementazione NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI locale.

   Non è possibile accedere utilizzando le credenziali Lightweight Directory Access Protocol.

5. Nella pagina di benvenuto, selezionare **Sì**.
6. Nella pagina End User License (licenza per l'utente finale), eseguire le seguenti operazioni:
   a. Leggi il contratto di licenza con l'utente finale di VMware.
   b. Se si accettano i termini, selezionare **Accetto** alla fine del testo del contratto.
7. Selezionare **continua**.
8. Nella pagina vCenter, attenersi alla seguente procedura:
   a. Immettere un indirizzo FQDN o IP e le credenziali di amministratore per l'istanza di vCenter associata all'installazione di NetApp HCI.
   b. Selezionare **continua**.
   c. Selezionare un data center vSphere esistente a cui aggiungere il nuovo nodo di calcolo oppure selezionare **Create New Datacenter** (Crea nuovo data center) per aggiungere i nuovi nodi di calcolo a un nuovo data center.

      Se si seleziona Create New Datacenter (Crea nuovo data center), il campo Cluster viene compilato automaticamente.

   d. Se è stato selezionato un data center esistente, selezionare un cluster vSphere a cui associare i nuovi nodi di calcolo.

      Se NetApp HCI non riconosce le impostazioni di rete del cluster selezionato, assicurarsi che il mapping vmkernel e vmnic per le reti di gestione, storage e vMotion sia impostato sui valori predefiniti di implementazione.

e. Selezionare **continua**.

9. Nella pagina delle credenziali ESXi, immettere una password radice ESXi per il nodo di calcolo o i nodi che si desidera aggiungere. Utilizzare la stessa password creata durante la distribuzione iniziale di NetApp HCI.
10. Selezionare **continua**.
11. Se è stato creato un nuovo cluster di data center vSphere, nella pagina topologia di rete, selezionare una topologia di rete che corrisponda ai nuovi nodi di calcolo che si stanno aggiungendo.

> È possibile selezionare l'opzione a due cavi solo se i nodi di calcolo utilizzano la topologia a due cavi e l'implementazione NetApp HCI esistente è configurata con ID VLAN.

12. Nella pagina inventario disponibile, selezionare il nodo che si desidera aggiungere all'installazione di NetApp HCI esistente.

> Per alcuni nodi di calcolo, potrebbe essere necessario abilitare EVC al livello più elevato supportato dalla versione di vCenter prima di poterli aggiungere all'installazione. Utilizzare il client vSphere per abilitare EVC per questi nodi di calcolo. Una volta attivata, aggiornare la pagina **Inventory** e provare ad aggiungere nuovamente i nodi di calcolo.

13. Selezionare **continua**.
14. Facoltativo: Se è stato creato un nuovo cluster di data center vSphere, nella pagina Impostazioni di rete, importare le informazioni di rete da un'implementazione NetApp HCI esistente selezionando la casella di controllo **Copia impostazione da un cluster esistente**. In questo modo vengono inserite le informazioni predefinite relative al gateway e alla subnet per ciascuna rete.
15. Nella pagina Network Settings (Impostazioni di rete), alcune informazioni di rete sono state rilevate dalla distribuzione iniziale. Il nuovo nodo di calcolo è elencato in base al numero di serie e si consiglia di assegnarvi nuove informazioni di rete. Per il nuovo nodo di calcolo, attenersi alla seguente procedura:
    a. Se NetApp HCI ha rilevato un prefisso di denominazione, copiarlo dal campo prefisso di denominazione rilevato e inserirlo come prefisso per il nuovo nome host univoco aggiunto nel campo **Nome host**.
    b. Nel campo **Management IP Address** (Indirizzo IP di gestione), immettere un indirizzo IP di gestione per il nodo di calcolo all'interno della subnet della rete di gestione.
    c. Nel campo vMotion IP Address (Indirizzo IP vMotion), immettere un indirizzo IP vMotion per il nodo di calcolo che si trova all'interno della subnet di rete vMotion.
    d. Nel campo iSCSI A - IP Address (Indirizzo IP iSCSI A), immettere un indirizzo IP per la prima porta iSCSI del nodo di calcolo che si trova nella subnet di rete iSCSI.
    e. Nel campo iSCSI B - IP Address (Indirizzo IP - iSCSI B), immettere un indirizzo IP per la seconda porta iSCSI del nodo di calcolo che si trova all'interno della subnet di rete iSCSI.
16. Selezionare **continua**.
17. Nella pagina Review della sezione Network Settings (Impostazioni di rete), il nuovo nodo viene visualizzato in grassetto. Se è necessario apportare modifiche alle informazioni contenute in una qualsiasi sezione, attenersi alla seguente procedura:
    a. Selezionare **Modifica** per la sezione.
    b. Al termine delle modifiche, fare clic su Continue (continua) nelle pagine successive per tornare alla pagina Review (esamina).
18. Facoltativo: Se non si desidera inviare statistiche del cluster e informazioni di supporto ai server SolidFire

Active IQ ospitati da NetApp, deselezionare la casella di controllo finale. In questo modo si disattiva il monitoraggio diagnostico e dello stato di salute in tempo reale per NetApp HCI. La disattivazione di questa funzione elimina la possibilità per NetApp di supportare e monitorare in modo proattivo NetApp HCI per rilevare e risolvere i problemi prima che la produzione venga compromessa.

19. Selezionare **Aggiungi nodi**. È possibile monitorare l'avanzamento mentre NetApp HCI aggiunge e configura le risorse.
20. Facoltativo: Verificare che il nuovo nodo di calcolo sia visibile in vCenter.

NetApp HCI 1.4 P2, 1.4 e 1.3

Se l'installazione di NetApp HCI esegue la versione 1.4P2, 1.4 o 1.3, è possibile utilizzare il motore di implementazione NetApp per aggiungere il nodo al cluster.

Di cosa hai bisogno

- Assicurarsi che l'istanza di vSphere utilizzata da NetApp HCI disponga di licenze vSphere Enterprise Plus se si sta espandendo un'implementazione con Virtual Distributed Switch.
- Assicurarsi che nessuna delle istanze vCenter o vSphere in uso con NetApp HCI disponga di licenze scadute.
- Assicurarsi di disporre di indirizzi IPv4 liberi e inutilizzati sullo stesso segmento di rete dei nodi esistenti (ciascun nuovo nodo deve essere installato sulla stessa rete dei nodi esistenti del suo tipo).
- Assicurarsi di disporre delle credenziali dell'account amministratore vCenter.
- Assicurarsi che ogni nuovo nodo utilizzi la stessa topologia di rete e lo stesso cablaggio dei cluster di calcolo o di storage esistenti.

Fasi

1. Individuare l'indirizzo IP di gestione di uno dei nodi di storage esistenti: `http://<storage_node_management_IP_address>/`
2. Accedere al motore di implementazione NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI locale.

   Non è possibile accedere utilizzando le credenziali Lightweight Directory Access Protocol.

3. Selezionare **espandere l'installazione**.
4. Nella pagina di benvenuto, selezionare **Sì**.
5. Nella pagina End User License (licenza per l'utente finale), eseguire le seguenti operazioni:
   a. Leggi il contratto di licenza con l'utente finale di VMware.
   b. Se si accettano i termini, selezionare **Accetto** alla fine del testo del contratto.
6. Selezionare **continua**.
7. Nella pagina vCenter, attenersi alla seguente procedura:
   a. Immettere un indirizzo FQDN o IP e le credenziali di amministratore per l'istanza di vCenter associata all'installazione di NetApp HCI.
   b. Selezionare **continua**.
   c. Selezionare un data center vSphere esistente al quale aggiungere il nuovo nodo di calcolo.
   d. Selezionare un cluster vSphere a cui associare il nuovo nodo di calcolo.

> Se si aggiunge un nodo di calcolo con una generazione di CPU diversa dalla generazione di CPU dei nodi di calcolo esistenti e la compatibilità vMotion avanzata (EVC) è disattivata sull'istanza vCenter di controllo, è necessario attivare EVC prima di procedere. Ciò garantisce la funzionalità vMotion al termine dell'espansione.

   e. Selezionare **continua**.

8. Nella pagina credenziali ESXi, creare le credenziali di amministratore ESXi per il nodo di calcolo che si desidera aggiungere. Utilizzare le stesse credenziali master create durante la distribuzione iniziale di NetApp HCI.
9. Selezionare **continua**.
10. Nella pagina inventario disponibile, selezionare il nodo che si desidera aggiungere all'installazione di NetApp HCI esistente.

> Per alcuni nodi di calcolo, potrebbe essere necessario abilitare EVC al livello più elevato supportato dalla versione di vCenter prima di poterli aggiungere all'installazione. Utilizzare il client vSphere per abilitare EVC per questi nodi di calcolo. Una volta attivata, aggiornare la pagina Inventory e provare ad aggiungere nuovamente i nodi di calcolo.

11. Selezionare **continua**.
12. Nella pagina Impostazioni di rete, attenersi alla seguente procedura:
    a. Verificare le informazioni rilevate dall'implementazione iniziale.
    b. Ogni nuovo nodo di calcolo viene elencato in base al numero di serie e si devono assegnare nuove informazioni di rete. Per ogni nuovo nodo di storage, attenersi alla seguente procedura:
        i. Se NetApp HCI ha rilevato un prefisso di denominazione, copiarlo dal campo prefisso di denominazione rilevato e inserirlo come prefisso per il nuovo nome host univoco aggiunto nel campo Nome host.
        ii. Nel campo Management IP Address (Indirizzo IP di gestione), immettere un indirizzo IP di gestione per il nodo di calcolo all'interno della subnet della rete di gestione.
        iii. Nel campo vMotion IP Address (Indirizzo IP vMotion), immettere un indirizzo IP vMotion per il nodo di calcolo che si trova all'interno della subnet di rete vMotion.
        iv. Nel campo iSCSI A - IP Address (Indirizzo IP iSCSI A), immettere un indirizzo IP per la prima porta iSCSI del nodo di calcolo che si trova nella subnet di rete iSCSI.
        v. Nel campo iSCSI B - IP Address (Indirizzo IP - iSCSI B), immettere un indirizzo IP per la seconda porta iSCSI del nodo di calcolo che si trova all'interno della subnet di rete iSCSI.
    c. Selezionare **continua**.
13. Nella pagina Review della sezione Network Settings (Impostazioni di rete), il nuovo nodo viene visualizzato in grassetto. Se si desidera apportare modifiche alle informazioni di qualsiasi sezione, attenersi alla seguente procedura:
    a. Selezionare **Modifica** per la sezione.
    b. Una volta apportate le modifiche, selezionare **continua** nelle pagine successive per tornare alla pagina di revisione.
14. Facoltativo: Se non si desidera inviare statistiche del cluster e informazioni di supporto ai server Active IQ ospitati da NetApp, deselezionare la casella di controllo finale. In questo modo si disattiva il monitoraggio diagnostico e dello stato di salute in tempo reale per NetApp HCI. La disattivazione di questa funzione elimina la possibilità per NetApp di supportare e monitorare in modo proattivo NetApp HCI per rilevare e risolvere i problemi prima che la produzione venga compromessa.

15. Selezionare **Aggiungi nodi**. È possibile monitorare l'avanzamento mentre NetApp HCI aggiunge e configura le risorse.
16. Facoltativo: Verificare che il nuovo nodo di calcolo sia visibile in vCenter.

NetApp HCI 1.2, 1.1 e 1.0

Dopo aver sostituito fisicamente il nodo, è necessario aggiungerlo nuovamente al cluster VMware ESXi ed eseguire diverse configurazioni di rete in modo da poter utilizzare tutte le funzionalità disponibili.

> Per eseguire questa procedura, è necessario disporre di una console o di una tastiera, di un video o di un mouse (KVM).

Fasi

1. Installare e configurare VMware ESXi versione 6.0.0 come segue:
   a. Sulla console remota o sullo schermo KVM, selezionare **Power Control > Set Power Reset** (controllo alimentazione > Imposta ripristino alimentazione). In questo modo il nodo viene riavviato.
   b. Nella finestra del menu di avvio visualizzata, selezionare **Installazione ESXi** premendo il tasto freccia giù.

      > Questa finestra rimane aperta per soli cinque secondi. Se non si effettua la selezione entro cinque secondi, riavviare nuovamente il nodo.

   c. Premere **Invio** per avviare il processo di installazione.
   d. Completare la procedura di installazione guidata.

      > Quando viene richiesto di selezionare il disco su cui installare ESXi, selezionare il secondo disco nell'elenco selezionando il tasto freccia giù. Quando viene richiesto di inserire una password root, è necessario inserire la stessa password configurata nel motore di implementazione NetApp quando si configura NetApp HCI.

   e. Al termine dell'installazione, premere **Invio** per riavviare il nodo.

      > Per impostazione predefinita, il nodo viene riavviato con il sistema operativo NetApp HCI Bootstrap. Per utilizzare VMware ESXi, è necessario eseguire una configurazione unica sul nodo.

2. Configurare VMware ESXi sul nodo come segue:
   a. Nella finestra di accesso dell'interfaccia utente del terminale del sistema operativo NetApp HCI Bootstrap, immettere le seguenti informazioni:
      i. Nome utente: Elemento
      ii. Password: CatchTheFire!
   b. Premere il tasto freccia giù per selezionare **OK**.
   c. Premere **Invio** per accedere.
   d. Nel menu principale, utilizzare il tasto freccia giù per selezionare **tunnel di supporto > Apri tunnel di supporto**.
   e. Nella finestra visualizzata, inserire le informazioni sulla porta.

> Per queste informazioni, contatta il supporto NetApp. Il supporto NetApp effettua l'accesso al nodo per impostare il file di configurazione di avvio e completare l'attività di configurazione.

f. Riavviare il nodo.

3. Configurare la rete di gestione come segue:
   a. Accedere a VMware ESXi inserendo le seguenti credenziali:
      i. Nome utente: Root
      ii. Password: La password impostata al momento dell'installazione di VMware ESXi.

      > La password deve corrispondere a quella configurata nel motore di implementazione NetApp al momento della configurazione di NetApp HCI.

   b. Selezionare **Configure Management Network** (Configura rete di gestione) e premere **Invio**.
   c. Selezionare **schede di rete** e premere **Invio**.
   d. Selezionare **vmnic2** e **vmnic3**, quindi premere **Invio**.
   e. Selezionare **IPv4 Configuration** (Configurazione IPv4) e premere la barra spaziatrice sulla tastiera per selezionare l'opzione di configurazione statica.
   f. Inserire l'indirizzo IP, la subnet mask e le informazioni del gateway predefinito, quindi premere **Invio**. È possibile riutilizzare le informazioni copiate prima di rimuovere il nodo. L'indirizzo IP immesso corrisponde all'indirizzo IP della rete di gestione precedentemente copiato.
   g. Premere **Esc** per uscire dalla sezione Configure Management Network (Configura rete di gestione).
   h. Selezionare **Sì** per applicare le modifiche.
4. Configurare la rete in modo che il nodo sia sincronizzato con gli altri nodi del cluster come segue:

Plug-in Element per vCenter 5.0 e versioni successive

A partire da Element Plug-in per vCenter 5.0, aggiungere il nodo (host) al data center.

a. In VMware vSphere Web Client, selezionare **Inventory > Hosts and Clusters** (inventario > host e cluster).

b. Fare clic con il pulsante destro del mouse sul data center e selezionare **Add host** (Aggiungi host).

   La procedura guidata consente di aggiungere l'host.

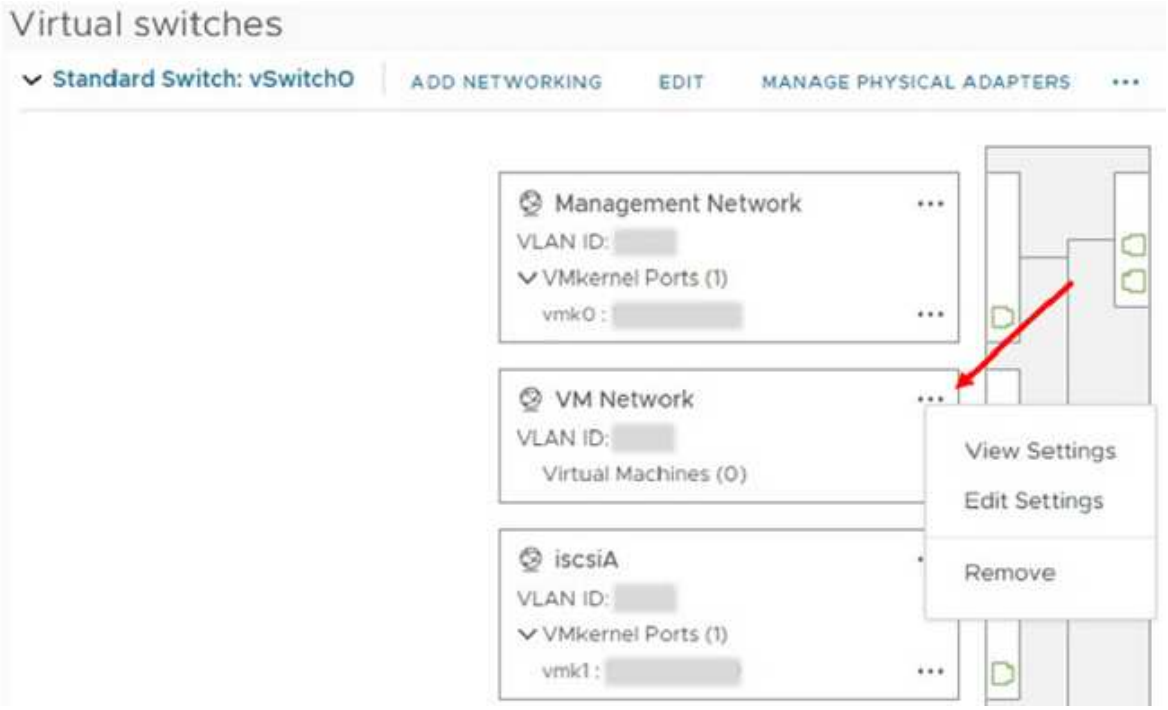
   > Quando viene richiesto di inserire il nome utente e la password, utilizzare le seguenti credenziali: Nome utente: Password root: La password configurata nel motore di implementazione NetApp al momento della configurazione di NetApp HCI

   L'aggiunta del nodo al cluster potrebbe richiedere alcuni minuti. Al termine del processo, il nodo appena aggiunto viene elencato nel cluster.

c. Selezionare il nodo, quindi selezionare **Configure > Networking > Virtual switches** (Configura > rete > Switch virtuali) ed eseguire la seguente procedura:

   i. Espandere **vSwitch0**.

   ii. Nella figura visualizzata, selezionare la rete della macchina virtuale ··· Icona seguita da **Rimuovi**.



   iii. Confermare l'azione.

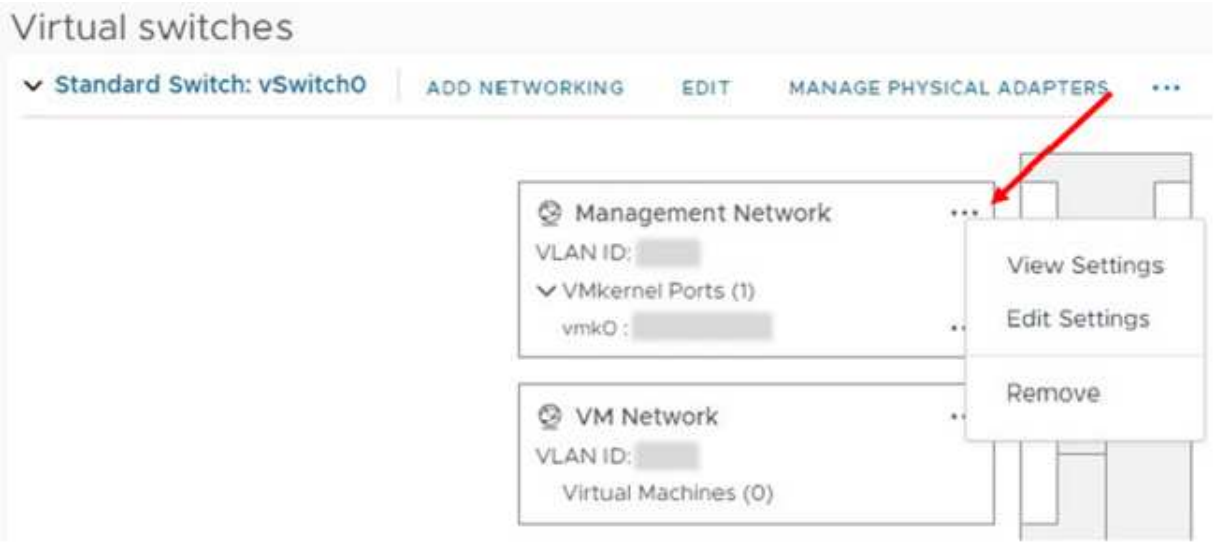
   iv. Selezionare **EDIT** nell'intestazione vSwitch0.

   v. Nella finestra vSwitch0 - Modifica impostazioni, selezionare **Teaming and failover**.

   vi. Verificare che vmnic3 sia presente nell'elenco degli adattatori di standby e selezionare **OK**.

d. Nella figura visualizzata, selezionare la rete di gestione ··· Icona seguita da **Modifica**

impostazioni.

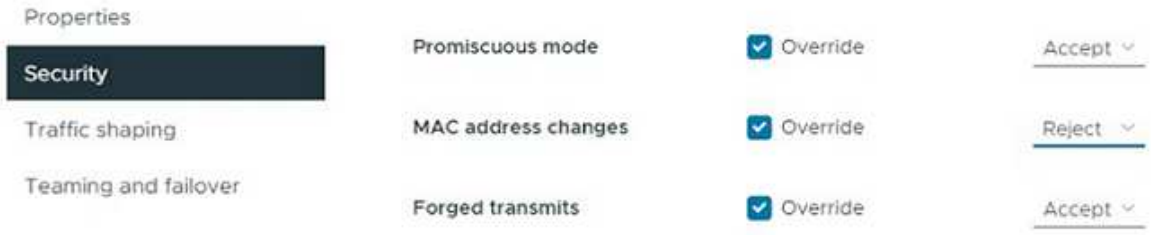


   i. Nella finestra Management Network - Edit settings (rete di gestione - Modifica impostazioni), selezionare **Teaming and failover** (raggruppamento e failover).
   ii. Verificare che vmnic3 sia presente nell'elenco degli adattatori di standby e selezionare **OK**.

e. Selezionare **Add Networking** (Aggiungi rete) nell'intestazione vSwitch0 e immettere i seguenti dettagli nella finestra visualizzata:
   i. Per il tipo di connessione, selezionare **Virtual Machine Port Group for a Standard Switch** (Gruppo di porte macchina virtuale per uno switch standard) e selezionare **Next** (Avanti).
   ii. Per il dispositivo di destinazione, selezionare **nuovo switch standard** e selezionare **Avanti**.
   iii. In Create a Standard Switch (Crea uno switch standard), spostare vmnic0 e vmnic4 su Active adapter (adattatori attivi) e selezionare **Next** (Avanti).
   iv. In Connection settings (Impostazioni di connessione), verificare che la rete VM sia l'etichetta di rete e, se necessario, inserire l'ID VLAN.
   v. Selezionare **Avanti**.
   vi. Esaminare la schermata Ready to complete (Pronto per il completamento) e selezionare **Finish** (fine).

f. Espandere vSwitch1 e selezionare **EDIT** per modificare le impostazioni come segue:
   i. In Proprietà, impostare MTU su 9000 e selezionare **OK**.

g. Nella figura visualizzata, selezionare la rete della macchina virtuale ··· Icona seguita da **Modifica**.
   i. Selezionare **Security** (protezione) ed effettuare le seguenti selezioni:



ii. Selezionare **Teaming and failover**, quindi selezionare la casella di controllo **Override**.

iii. Spostare vmnic0 sugli adattatori di standby.

iv. Selezionare **OK**.

h. Selezionare **ADD NETWORKING** (AGGIUNGI RETE) nell'intestazione vSwitch1 e immettere i seguenti dettagli nella finestra Add Networking (Aggiungi rete):

i. Per il tipo di connessione, selezionare **VMkernel Network Adapter** e selezionare **Avanti**.

ii. Per il dispositivo di destinazione, selezionare l'opzione per utilizzare uno switch standard esistente, selezionare vSwitch1 e selezionare **Avanti**.

iii. In Crea uno switch standard, spostare vmnic1 e vmnic5 su Active adapter e selezionare **Avanti**.

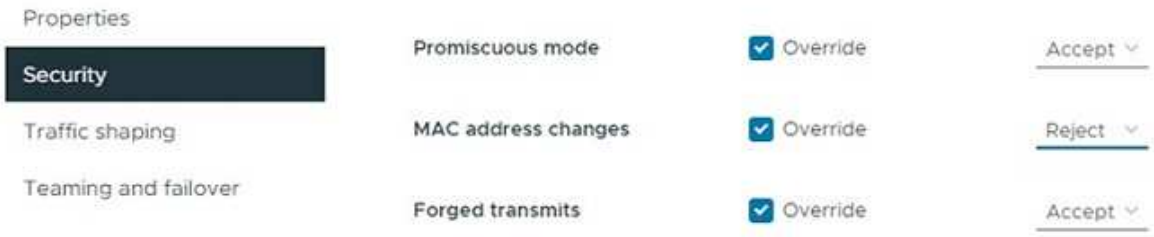
iv. In Port properties (Proprietà porta), modificare l'etichetta di rete in vMotion, selezionare la casella di controllo per il traffico vMotion in Enable Services (attiva servizi) e selezionare **Next** (Avanti).

v. In IPv4 settings (Impostazioni IPv4), fornire le informazioni IPv4 e selezionare **Next** (Avanti).

vi. Se si è pronti per procedere, selezionare **fine**.

i. Nel grafico visualizzato, selezionare vMotion ··· Icona seguita da **Modifica**.

i. Selezionare **Security** (protezione) ed effettuare le seguenti selezioni:



ii. Selezionare **Teaming and failover**, quindi selezionare la casella di controllo **Override**.

iii. Spostare vmnic4 sugli adattatori di standby.

iv. Selezionare **OK**.

j. Selezionare **ADD NETWORKING** (AGGIUNGI RETE) nell'intestazione vSwitch1 e immettere i seguenti dettagli nella finestra Add Networking (Aggiungi rete):

i. Per il tipo di connessione, selezionare **VMkernel Network Adapter** e selezionare **Avanti**.

ii. Per il dispositivo di destinazione, selezionare **nuovo switch standard** e selezionare **Avanti**.

iii. In Crea uno switch standard, spostare vmnic1 e vmnic5 su Active adapter e selezionare **Avanti**.

iv. In Port properties (Proprietà porta), modificare l'etichetta di rete in iSCSI-B e selezionare **Next** (Avanti).

v. In IPv4 settings (Impostazioni IPv4), fornire le informazioni IPv4 e selezionare **Next** (Avanti).

vi. Se si è pronti per procedere, selezionare **fine**.

k. Espandere **vSwitch2** e selezionare **EDIT**:

i. In Proprietà, impostare MTU su 9000 e selezionare **OK**.

l. Nella figura visualizzata, selezionare iSCSI-B. ··· Icona seguita da **Modifica**.

i. Selezionare **Security** (protezione) ed effettuare le seguenti selezioni:

ii. Selezionare **Teaming and failover**, quindi selezionare la casella di controllo **Override**.

iii. Spostare vmnic1 sugli adattatori inutilizzati.

iv. Selezionare **OK**.

m. Selezionare **ADD NETWORKING** (AGGIUNGI RETE) nell'intestazione vSwitch1 e immettere i seguenti dettagli nella finestra Add Networking (Aggiungi rete):

i. Per il tipo di connessione, selezionare **VMkernel Network Adapter** e selezionare **Avanti**.

ii. Per il dispositivo di destinazione, selezionare l'opzione per utilizzare uno switch standard esistente, selezionare vSwitch2 e selezionare **Avanti**.

iii. In Port properties (Proprietà porta), modificare l'etichetta di rete in iSCSI-A e selezionare **Next** (Avanti).

iv. In IPv4 settings (Impostazioni IPv4), fornire le informazioni IPv4 e selezionare **Next** (Avanti).

v. Se si è pronti per procedere, selezionare **fine**.

n. Nella figura visualizzata, selezionare iSCSI-A. ··· Icona seguita da **Modifica**.

i. Selezionare **Security** (protezione) ed effettuare le seguenti selezioni:

ii. Selezionare **Teaming and failover**, quindi selezionare la casella di controllo **Override**.

iii. Spostare vmnic5 sugli adattatori inutilizzati utilizzando l'icona a forma di freccia.

iv. Selezionare **OK**.

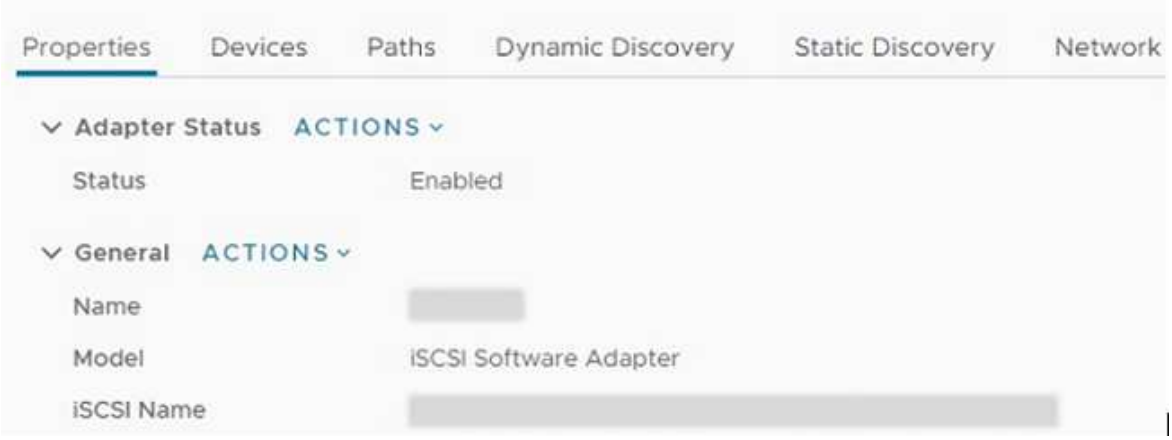
o. Dopo aver selezionato il nodo appena aggiunto e aperto la scheda Configure (Configura), selezionare **Storage > Storage Adapter** (Storage > Storage Adapter) ed eseguire la seguente procedura:

i. Selezionare l'elenco **ADD SOFTWARE ADAPTER** (AGGIUNGI SCHEDA SOFTWARE).

ii. Selezionare **Add iSCSI adapter** (Aggiungi adattatore iSCSI) e selezionare **OK**.

iii. In Storage Adapter (adattatori storage), selezionare l'adattatore iSCSI

iv. In Proprietà > Generale, copiare il nome iSCSI.



> Il nome iSCSI è necessario quando si crea l'iniziatore.

p. Eseguire le seguenti operazioni nel plug-in NetApp SolidFire vCenter:
   i. Selezionare l'istanza di destinazione.
   ii. Selezionare **Gestione**.
   iii. Selezionare il cluster di destinazione.
   iv. Selezionare **Gestione > iniziatori**.
   v. Selezionare **Crea iniziatore**.
   vi. Inserire l'indirizzo IQN copiato in precedenza nel campo IQN/WWPN.
   vii. Selezionare **OK**.
   viii. Selezionare il nuovo iniziatore.
   ix. Selezionare **elenco azioni > azioni in blocco** e selezionare **Aggiungi a gruppo di accesso**.
   x. Selezionare il gruppo di accesso di destinazione e scegliere **Aggiungi**.

q. In VMware vSphere Web Client, in Storage Adapter, selezionare l'adattatore iSCSI ed eseguire le seguenti operazioni:
   i. Selezionare **Dynamic Discovery > Add** (rilevamento dinamico > Aggiungi).
   ii. Inserire l'indirizzo IP SVIP nel campo Server iSCSI.

   > Per ottenere l'indirizzo IP SVIP, selezionare **Gestione NetApp Element** e copiare l'indirizzo IP SVIP. Lasciare il numero di porta predefinito così com'è. Dovrebbe essere 3260.

   iii. Selezionare **OK**.
   iv. Selezionare **Network Port Binding** e selezionare **ADD**.
   v. Selezionare iSCSI-A e iSCSI-B, quindi selezionare **OK**
   vi. Selezionare **RIPETERE LA SCANSIONE DELL'ADATTATORE**.
   vii. Selezionare **RIPETERE LA SCANSIONE DELLO STORAGE**. Cercare nuovi volumi VMFS e selezionare **OK**.
   viii. Una volta completata la nuova scansione, verificare se i volumi nel cluster e negli archivi dati sono visibili sul nuovo nodo di calcolo (host).

Plug-in Element per vCenter 4.10 e versioni precedenti

Per Element Plug-in per vCenter 4.10 e versioni precedenti, aggiungere il nodo (host) al cluster.

a. In VMware vSphere Web Client, selezionare **host e cluster**.

b. Fare clic con il pulsante destro del mouse sul cluster a cui si desidera aggiungere il nodo e selezionare **Add host** (Aggiungi host).

   La procedura guidata consente di aggiungere l'host.

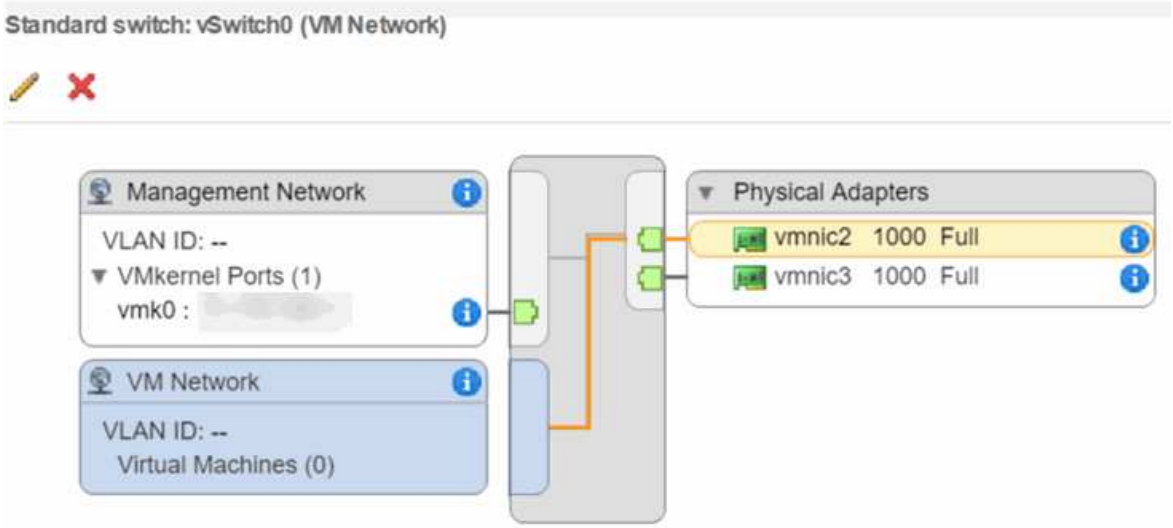
   > Quando viene richiesto di inserire il nome utente e la password, utilizzare le seguenti credenziali: Nome utente: Password root: La password configurata nel motore di implementazione NetApp al momento della configurazione di NetApp HCI

   L'aggiunta del nodo al cluster potrebbe richiedere alcuni minuti. Al termine del processo, il nodo appena aggiunto viene elencato nel cluster.

c. Selezionare il nodo, quindi selezionare **Manage > Networking > Virtual switches** (Gestisci > rete > Switch virtuali) ed eseguire la seguente procedura:

   i. Selezionare **vSwitch0**. Nella tabella visualizzata dovrebbe essere visualizzato solo vSwitch0.

   ii. Nella figura visualizzata, selezionare **VM Network** e fare clic su **X** per rimuovere il gruppo di porte di rete della macchina virtuale.



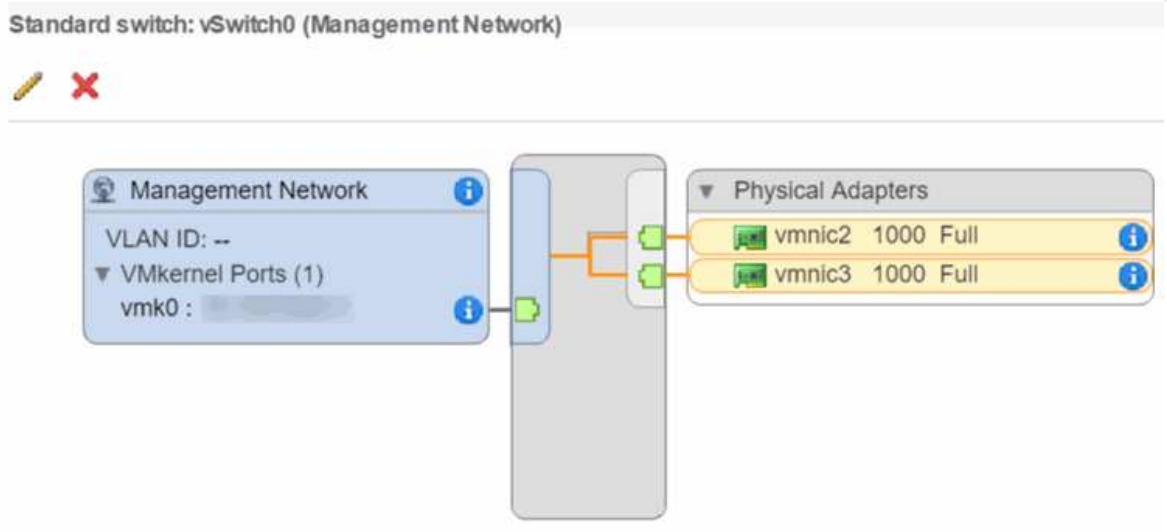
   iii. Confermare l'azione.

   iv. Selezionare **vSwitch0**, quindi selezionare l'icona a forma di matita per modificare le impostazioni.

   v. Nella finestra vSwitch0 - Modifica impostazioni, selezionare **Teaming and failover**.

   vi. Assicurarsi che vmnic3 sia elencato sotto Standby adapter (adattatori di standby) e selezionare **OK**.

   vii. Nella figura visualizzata, selezionare **Management Network** (rete di gestione) e selezionare l'icona a forma di matita per modificare le impostazioni.



viii. Nella finestra Management Network - Edit settings (rete di gestione - Modifica impostazioni), selezionare **Teaming and failover** (raggruppamento e failover).

ix. Spostare vmnic3 su Standby Adapter utilizzando l'icona a forma di freccia e selezionare **OK**.

d. Dal menu a discesa Actions (azioni), selezionare **Add Networking** (Aggiungi rete) e immettere i seguenti dettagli nella finestra visualizzata:

   i. Per il tipo di connessione, selezionare **Virtual Machine Port Group for a Standard Switch** (Gruppo di porte macchina virtuale per uno switch standard) e selezionare **Next** (Avanti).

   ii. Per il dispositivo di destinazione, selezionare l'opzione per aggiungere un nuovo switch standard e selezionare **Avanti**.

   iii. Selezionare **+**.

   iv. Nella finestra Add Physical Adapters to Switch (Aggiungi adattatori fisici allo switch), selezionare vmnic0 e vmnic4, quindi selezionare **OK**. Vmnic0 e vmnic4 sono ora elencati in Active adapter.

   v. Selezionare **Avanti**.

   vi. In Connection settings (Impostazioni di connessione), verificare che VM Network sia l'etichetta di rete e selezionare **Next** (Avanti).

   vii. Se si è pronti per procedere, selezionare **fine**. VSwitch1 viene visualizzato nell'elenco degli switch virtuali.

e. Selezionare **vSwitch1** e selezionare l'icona a forma di matita per modificare le impostazioni come segue:

   i. In Proprietà, impostare MTU su 9000 e selezionare **OK**. Nella figura visualizzata, selezionare **VM Network**, quindi fare clic sull'icona a forma di matita per modificare le impostazioni come segue:

f. Selezionare **Security** (protezione) ed effettuare le seguenti selezioni:

i. Selezionare **Teaming and failover**, quindi selezionare la casella di controllo **Override**.
ii. Spostare vmnic0 su Standby Adapter utilizzando l'icona a forma di freccia.
iii. Selezionare **OK**.

g. Con vSwitch1 selezionato, dal menu a discesa Actions (azioni), selezionare **Add Networking** (Aggiungi rete) e inserire i seguenti dettagli nella finestra visualizzata:
   i. Per il tipo di connessione, selezionare **VMkernel Network Adapter** e selezionare **Avanti**.
   ii. Per il dispositivo di destinazione, selezionare l'opzione per utilizzare uno switch standard esistente, selezionare vSwitch1 e selezionare **Avanti**.
   iii. In Port properties (Proprietà porta), modificare l'etichetta di rete in vMotion, selezionare la casella di controllo per il traffico vMotion in Enable Services (attiva servizi) e selezionare **Next** (Avanti).
   iv. In IPv4 settings (Impostazioni IPv4), fornire le informazioni IPv4 e selezionare **Next** (Avanti). L'indirizzo IP immesso corrisponde all'indirizzo IP vMotion copiato in precedenza.
   v. Se si è pronti per procedere, selezionare **fine**.

h. Nella figura visualizzata, selezionare vMotion e selezionare l'icona a forma di matita per modificare le impostazioni nel modo seguente:
   i. Selezionare **Security** (protezione) ed effettuare le seguenti selezioni:

   ii. Selezionare **Teaming and failover**, quindi selezionare la casella di controllo **Override**.
   iii. Spostare vmnic4 su Standby Adapter utilizzando l'icona a forma di freccia.
   iv. Selezionare **OK**.

i. Con vSwitch1 selezionato, dal menu a discesa Actions (azioni), selezionare **Add Networking** (Aggiungi rete) e inserire i seguenti dettagli nella finestra visualizzata:
   i. Per il tipo di connessione, selezionare **VMkernel Network Adapter** e selezionare **Avanti**.
   ii. Per il dispositivo di destinazione, selezionare l'opzione per aggiungere un nuovo switch standard e selezionare **Avanti**.
   iii. Selezionare **+**.

iv. Nella finestra Add Physical Adapters to Switch (Aggiungi adattatori fisici allo switch), selezionare vmnic1 e vmnic5, quindi selezionare **OK**. Vmnic1 e vmnic5 sono ora elencati in Active adapter.

v. Selezionare **Avanti**.

vi. In Port properties (Proprietà porta), modificare l'etichetta di rete in iSCSI-B e selezionare **Next** (Avanti).

vii. In IPv4 settings (Impostazioni IPv4), fornire le informazioni IPv4 e selezionare **Next** (Avanti). L'indirizzo IP immesso corrisponde all'indirizzo IP iSCSI-B copiato in precedenza.

viii. Se si è pronti per procedere, selezionare **fine**. VSwitch2 viene visualizzato nell'elenco degli switch virtuali.

j. Selezionare **vSwitch2** e selezionare l'icona a forma di matita per modificare le impostazioni come segue:

i. In Proprietà, impostare MTU su 9000 e selezionare **OK**.

k. Nella figura visualizzata, selezionare **iSCSI-B** e selezionare l'icona a forma di matita per modificare le impostazioni come segue:

i. Selezionare **Security** (protezione) ed effettuare le seguenti selezioni:

ii. Selezionare **Teaming and failover**, quindi selezionare la casella di controllo **Override**.

iii. Spostare vmnic1 sugli adattatori inutilizzati utilizzando l'icona a forma di freccia.

iv. Selezionare **OK**.

l. Dal menu a discesa Actions (azioni), selezionare **Add Networking** (Aggiungi rete) e immettere i seguenti dettagli nella finestra visualizzata:

i. Per il tipo di connessione, selezionare **VMkernel Network Adapter** e selezionare **Avanti**.

ii. Per il dispositivo di destinazione, selezionare l'opzione per utilizzare uno switch standard esistente, selezionare vSwitch2 e selezionare **Avanti**.

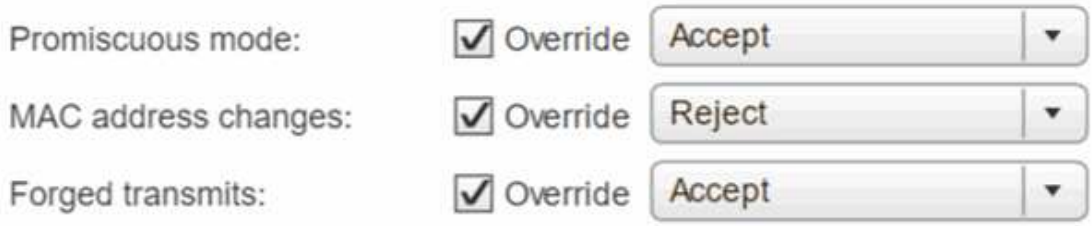
iii. In Port properties (Proprietà porta), modificare l'etichetta di rete in iSCSI-A e selezionare **Next** (Avanti).

iv. In IPv4 settings (Impostazioni IPv4), fornire le informazioni IPv4 e selezionare **Next** (Avanti). L'indirizzo IP immesso corrisponde all'indirizzo IP iSCSI-A copiato in precedenza.

v. Se si è pronti per procedere, selezionare **fine**.

m. Nella figura visualizzata, selezionare **iSCSI-A** e selezionare l'icona a forma di matita per modificare le impostazioni come segue:

i. Selezionare **Security** (protezione) ed effettuare le seguenti selezioni:



ii. Selezionare **Teaming and failover**, quindi selezionare la casella di controllo **Override**.

iii. Spostare vmnic5 sugli adattatori inutilizzati utilizzando l'icona a forma di freccia.

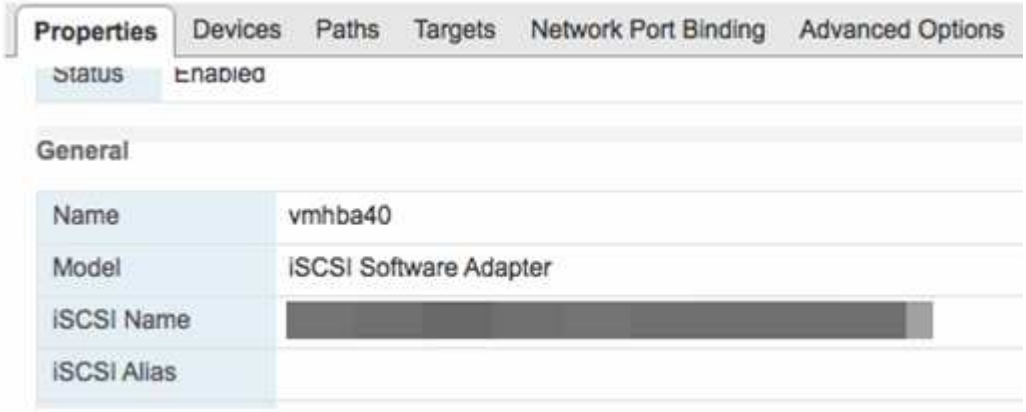
iv. Selezionare **OK**.

n. Con il nodo appena aggiunto selezionato e la scheda Manage (Gestisci) aperta, selezionare **Storage > Storage Adapter** (Storage > Storage Adapter) ed eseguire la seguente procedura:

i. Selezionare **+** e selezionare **Software iSCSI Adapter**.

ii. Per aggiungere l'adattatore iSCSI, selezionare **OK** nella finestra di dialogo.

iii. In Storage Adapter (adattatori storage), selezionare iSCSI Adapter (adattatore iSCSI) e, nella scheda Properties (Proprietà), copiare iSCSI Name (Nome iSCSI).



Il nome iSCSI è necessario quando si crea l'iniziatore.

o. Eseguire le seguenti operazioni nel plug-in NetApp SolidFire vCenter:

i. Selezionare **Gestione > iniziatori > Crea**.

ii. Selezionare **Crea un singolo iniziatore**.

iii. Inserire l'indirizzo IQN copiato in precedenza nel campo IQN/WWPN.

iv. Selezionare **OK**.

v. Selezionare **azioni in blocco** e selezionare **Aggiungi a gruppo di accesso al volume**.

vi. Selezionare **NetApp HCI**, quindi **Aggiungi**.

p. In VMware vSphere Web Client, in Storage Adapter, selezionare l'adattatore iSCSI ed eseguire le seguenti operazioni:

i. In Dettagli adattatore, selezionare **destinazioni > rilevamento dinamico > Aggiungi**.

ii. Inserire l'indirizzo IP SVIP nel campo Server iSCSI.

> Per ottenere l'indirizzo IP SVIP, selezionare **Gestione NetApp Element** e copiare l'indirizzo IP SVIP. Lasciare il numero di porta predefinito così com'è. Dovrebbe essere 3260.

iii. Selezionare **OK**. Viene visualizzato un messaggio che consiglia di eseguire una nuova scansione dell'adattatore di storage.

iv. Selezionare l'icona di riscan (scansione).

v. In Dettagli scheda di rete, selezionare **Network Port Binding** e selezionare **+**.

vi. Selezionare le caselle di controllo iSCSI-B e iSCSI-A, quindi fare clic su OK. Viene visualizzato un messaggio che consiglia di eseguire una nuova scansione dell'adattatore di storage.

vii. Selezionare l'icona di riscan (scansione). Una volta completata la riscan, verificare se i volumi nel cluster sono visibili sul nuovo nodo di calcolo (host).

Fase 5: Implementare nuovamente i nodi di controllo per cluster storage a due e tre nodi

Dopo aver sostituito fisicamente il nodo di calcolo guasto, è necessario ridistribuire la VM del nodo di controllo NetApp HCI se il nodo di calcolo guasto ospitava il nodo di controllo. Queste istruzioni si applicano solo ai nodi di calcolo che fanno parte di un'installazione NetApp HCI con cluster di storage a due o tre nodi.

Di cosa hai bisogno

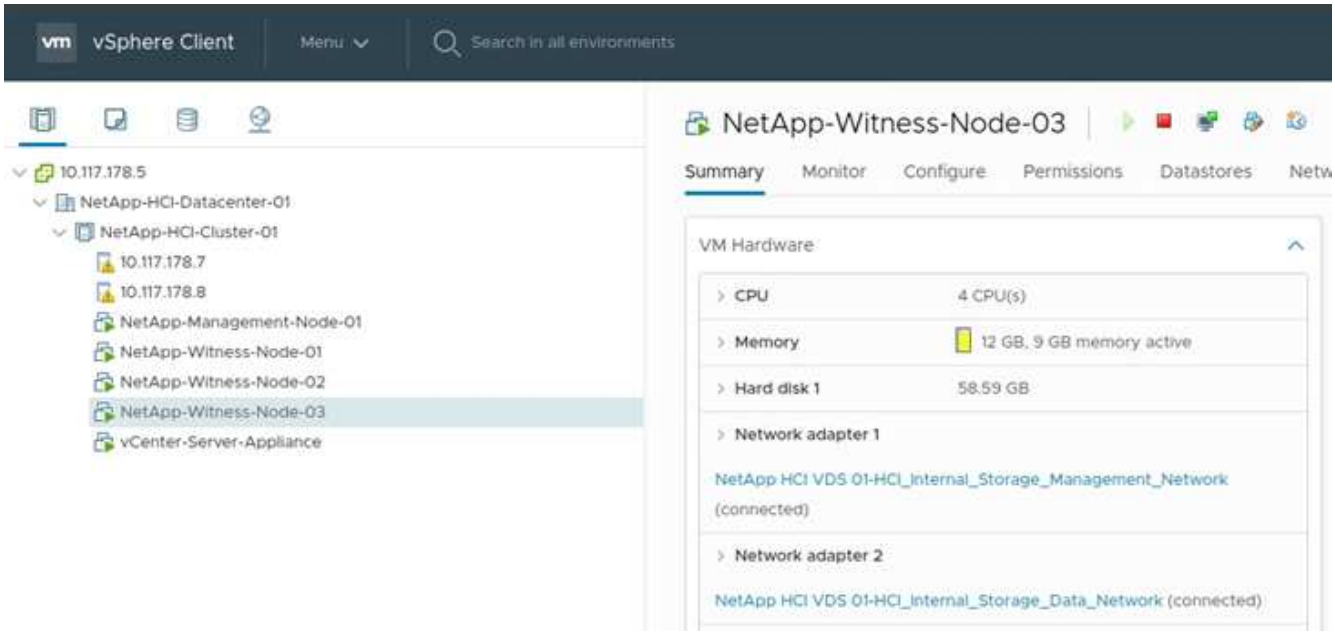
- Raccogliere le seguenti informazioni:
  - Nome del cluster di storage
  - Subnet mask, indirizzo IP del gateway, server DNS e informazioni di dominio per la rete di gestione
  - Subnet mask per la rete di storage
- Assicurarsi di disporre dell'accesso al cluster di storage per poter aggiungere i nodi di controllo al cluster.
- Considerare le seguenti condizioni per decidere se rimuovere il nodo di controllo esistente da VMware vSphere Web Client o dal cluster di storage:
  - Se si desidera utilizzare lo stesso nome della macchina virtuale per il nuovo nodo di controllo, eliminare tutti i riferimenti al nodo di controllo precedente da vSphere.
  - Se si desidera utilizzare lo stesso nome host sul nuovo nodo di controllo, rimuovere prima il nodo di controllo precedente dal cluster di storage.

> Non è possibile rimuovere il nodo di controllo precedente se il cluster non dispone di due soli nodi di storage fisici (e nessun nodo di controllo). In questo scenario, aggiungere il nuovo nodo di controllo al cluster prima di rimuovere quello precedente. È possibile rimuovere il nodo di controllo dal cluster utilizzando il punto di estensione Gestione NetApp Element.

Quando è necessario ridistribuire i nodi di controllo?

È necessario ridistribuire i nodi di controllo nei seguenti scenari:

- È stato sostituito un nodo di calcolo guasto che fa parte di un'installazione di NetApp HCI, che ha un cluster di storage a due o tre nodi e il nodo di calcolo guasto ospitava una macchina virtuale del nodo di controllo.
- È stata eseguita la procedura di ripristino dell'immagine di fabbrica (RTFI) sul nodo di calcolo.
- La VM del nodo di controllo è danneggiata.
- La VM del nodo di controllo è stata accidentalmente rimossa da ESXi. La macchina virtuale viene configurata utilizzando il modello creato come parte dell'implementazione iniziale utilizzando NetApp Deployment Engine. Ecco un esempio dell'aspetto di una macchina virtuale Witness Node:



> Se il modello di macchina virtuale è stato eliminato, contattare il supporto NetApp per ottenere l'immagine Witness Node .ova e ridistribuirla. È possibile scaricare il modello da "qui (accesso richiesto)". Tuttavia, è necessario coinvolgere il supporto per ottenere indicazioni sulla configurazione.

Fasi

1. In VMware vSphere Web Client, selezionare **host e cluster**.
2. Fare clic con il pulsante destro del mouse sul nodo di calcolo che ospiterà la macchina virtuale del nodo di controllo e selezionare **Nuova macchina virtuale**.
3. Selezionare **Deploy from template** (implementa dal modello) e selezionare **Next** (Avanti).
4. Seguire i passaggi della procedura guidata:
   a. Selezionare **Data Center**, individuare il modello di macchina virtuale e selezionare **Avanti**.
   b. Immettere un nome per la macchina virtuale nel seguente formato: NetApp-Witness-Node- n.

      > il numero deve essere sostituito con un numero.

   c. Lasciare la selezione predefinita per la posizione della macchina virtuale così com'è e selezionare **Avanti**.

d. Lasciare la selezione predefinita per la risorsa di calcolo di destinazione così com'è e selezionare **Avanti**.

e. Selezionare l'archivio dati locale e selezionare **Avanti**. Lo spazio libero nell'archivio dati locale varia a seconda della piattaforma di calcolo.

f. Selezionare **Power on virtual machine after creation** (accensione macchina virtuale dopo la creazione) dall'elenco delle opzioni di implementazione e selezionare **Next** (Avanti).

g. Rivedere le selezioni e selezionare **fine**.

5. Configurare la rete di gestione e storage e le impostazioni del cluster per il nodo di controllo come segue:

   a. In VMware vSphere Web Client, selezionare **host e cluster**.

   b. Fare clic con il pulsante destro del mouse sul nodo di controllo e accenderlo se non è già acceso.

   c. Nella vista Summary (Riepilogo) del nodo di controllo, selezionare **Launch Web Console** (Avvia console Web).

   d. Attendere che il nodo di controllo del mirroring avvii il menu con lo sfondo blu.

   e. Selezionare un punto qualsiasi all'interno della console per accedere al menu.

   f. Configurare la rete di gestione come segue:

      i. Premere il tasto freccia giù per selezionare Network (rete), quindi premere **Invio** per OK.

      ii. Selezionare **Network config**, quindi premere **Invio** per OK.

      iii. Selezionare **net0**, quindi premere **Invio** per OK.

      iv. Premere **Tab** fino a visualizzare il campo IPv4, quindi, se applicabile, eliminare l'IP esistente nel campo e immettere le informazioni IP di gestione per il nodo di controllo. Controllare anche la subnet mask e il gateway.

      > Non verrà applicato alcun tag VLAN a livello di host della macchina virtuale; il tagging verrà gestito in vSwitch.

      v. Premere **Tab** per selezionare OK, quindi premere **Invio** per salvare le modifiche. Dopo la configurazione della rete di gestione, viene visualizzata nuovamente la schermata Network (rete).

   g. Configurare la rete di storage come segue:

      i. Premere il tasto freccia giù per selezionare Network (rete), quindi premere **Invio** per OK.

      ii. Selezionare **Network config**, quindi premere **Invio** per OK.

      iii. Selezionare **net1**, quindi premere **Invio** per OK.

      iv. Premere **Tab** fino a visualizzare il campo IPv4, quindi, se applicabile, eliminare l'IP esistente nel campo e immettere le informazioni IP di storage per il nodo di controllo.

      v. Premere **Tab** per selezionare OK, quindi premere **Invio** per salvare le modifiche.

      vi. Impostare MTU su 9000.

      > Se MTU non viene impostato prima di aggiungere il nodo di controllo del mirroring al cluster, vengono visualizzati avvisi del cluster per le impostazioni MTU non coerenti. Questo può impedire l'esecuzione della garbage collection e causare problemi di performance.

      vii. Premere **Tab** per selezionare OK, quindi premere **Invio** per salvare le modifiche. Dopo la configurazione della rete di storage, viene visualizzata nuovamente la schermata Network (rete).

h. Configurare le impostazioni del cluster come segue:

   i. Premere **Tab** per selezionare Annulla, quindi premere **Invio**.

   ii. Selezionare **Cluster Settings** (Impostazioni cluster), quindi premere **Invio** per OK.

   iii. Premere **Tab** per selezionare Change Settings (Modifica impostazioni), quindi premere **Invio** per Change Settings (Modifica impostazioni).

   iv. Premere **Tab** per accedere al campo Nome host e immettere il nome host.

   v. Premere il tasto freccia giù per accedere al campo Cluster (cluster) e immettere il nome del cluster di storage.

   vi. Premere il tasto **Tab** per selezionare il pulsante OK, quindi premere **Invio**.

6. Aggiungere il nodo di controllo al cluster di storage come segue:

   a. Dal client Web vSphere, accedere al punto di estensione della gestione NetApp Element dalla scheda **Collegamenti** o dal pannello laterale.

   b. Selezionare **Gestione NetApp Element > cluster**.

   c. Selezionare la sottoscheda **Nodes**.

   d. Selezionare **Pending** dall'elenco a discesa per visualizzare l'elenco dei nodi. Il nodo di controllo deve essere visualizzato nell'elenco dei nodi in sospeso.

   e. Selezionare la casella di controllo del nodo da aggiungere e selezionare **Aggiungi nodo**. Una volta completata l'azione, il nodo viene visualizzato nell'elenco dei nodi attivi per il cluster.

Modificare la password se si riceve un nodo sostitutivo con una password BMC non standard

Alcuni nodi sostitutivi potrebbero essere forniti con password non standard per l'interfaccia utente del BMC (Baseboard Management Controller). Se si riceve un nodo sostitutivo con una password BMC non standard, è necessario modificare la password predefinita, ADMIN.

Fasi

1. Identificare se è stato ricevuto un nodo sostitutivo con una password BMC non standard:

   a. Cercare un adesivo sotto la porta IPMI sul retro del nodo sostitutivo ricevuto. Se si individua un adesivo sotto la porta IPMI, significa che è stato ricevuto un nodo con una password BMC non standard. Vedere la seguente immagine di esempio:

   b. Annotare la password.

2. Accedere all'interfaccia utente BMC utilizzando la password univoca riportata sull'adesivo.

3. Selezionare **Factory Default**, quindi selezionare il pulsante di opzione **Remove current settings and set the user defaults to ADMIN/ADMIN** (Rimuovi impostazioni correnti e imposta le impostazioni utente predefinite su ADMIN/ADMIN*):

4. Selezionare **Restore** (Ripristina).

5. Disconnettersi e quindi effettuare nuovamente l'accesso per confermare che le credenziali sono state modificate.

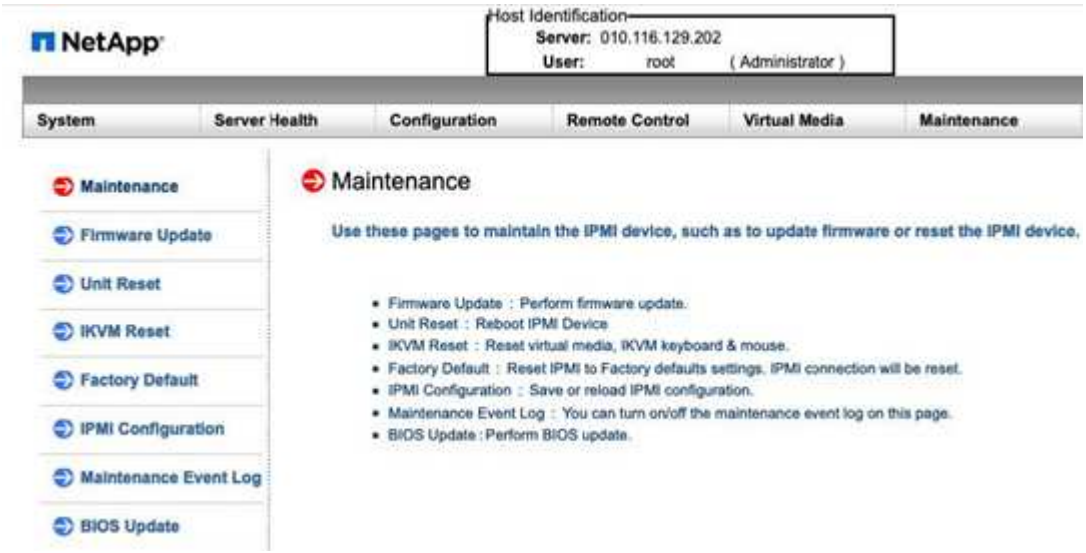
Aggiornare il firmware BMC sul nodo

Dopo aver sostituito il nodo di calcolo, potrebbe essere necessario aggiornare la versione del firmware. È possibile scaricare il file del firmware più recente dal menu a discesa di "Sito di supporto NetApp (accesso richiesto)".

Fasi

1. Accedere all'interfaccia utente del BMC (Baseboard Management Controller).
2. Selezionare **manutenzione > aggiornamento firmware**.

3. Dalla console BMC, selezionare **manutenzione**.



4. Dalla scheda Maintenance (manutenzione), selezionare **firmware Update** (aggiornamento firmware) dalla barra di navigazione a sinistra dell'interfaccia utente e selezionare **Enter Update Mode** (Immetti modalità di aggiornamento).

5. Selezionare **Sì** nella finestra di dialogo di conferma.
6. Selezionare **Sfoglia** per selezionare l'immagine del firmware da caricare, quindi selezionare **carica firmware**. Il caricamento del firmware da una posizione esterna alla diretta vicinanza del nodo potrebbe causare tempi di caricamento prolungati e possibili timeout.
7. Consentire i controlli di preservazione della configurazione e selezionare **Avvia aggiornamento**. L'aggiornamento richiede circa 5 minuti. Se il tempo di caricamento supera i 60 minuti, annullare il caricamento e trasferire il file su una macchina locale nelle vicinanze del nodo. In caso di timeout della sessione, è possibile che vengano visualizzati diversi avvisi durante il tentativo di accesso all'area di aggiornamento del firmware dell'interfaccia utente BMC. Se si annulla l'aggiornamento, si viene reindirizzati alla pagina di accesso.
8. Al termine dell'aggiornamento, selezionare **OK** e attendere il riavvio del nodo. Effettuare l'accesso dopo l'aggiornamento e selezionare **sistema** per verificare che la versione di **Revisione firmware** corrisponda alla versione caricata.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire i nodi H410S

Sostituire un nodo di storage in caso di guasto del modulo DIMM (Dual Inline Memory Module), guasto della CPU, problemi della scheda Radian, altri problemi della scheda madre o in caso di mancata accensione. Gli allarmi di VMware vSphere Web Client avvisano l'utente quando un nodo di storage è guasto. Utilizzare l'interfaccia utente del software NetApp Element per ottenere il numero di serie (codice di matricola) del nodo guasto. Queste informazioni sono necessarie per individuare il nodo guasto nello chassis.

Di cosa hai bisogno

- Hai determinato che il nodo di storage deve essere sostituito.
- Si dispone di un nodo storage sostitutivo.

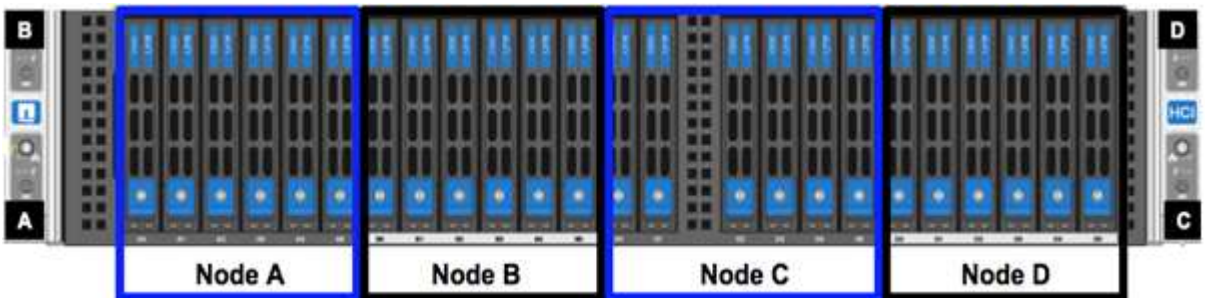
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o si sono prese altre precauzioni antistatiche.
- Ciascun cavo collegato al nodo di storage è etichettato.

A proposito di questa attività

La procedura di sostituzione si applica ai nodi di storage H410S in uno chassis NetApp HCI a due unità rack (2U) e quattro nodi.

Ecco la vista posteriore di uno chassis a quattro nodi con nodi H410S:

Di seguito viene mostrata la vista frontale di uno chassis a quattro nodi con nodi H410S, che mostra gli alloggiamenti corrispondenti a ciascun nodo:



Panoramica dei passaggi

Di seguito viene riportata una panoramica generale delle fasi di questa procedura:Preparare la sostituzione del nodo di storage
Sostituire il nodo di storage nello chassis
Aggiungere il nodo storage al cluster

Preparare la sostituzione del nodo di storage

Prima di installare il nodo sostitutivo, rimuovere correttamente il nodo di storage guasto dal cluster. È possibile eseguire questa operazione senza causare alcuna interruzione del servizio. Il numero di serie del nodo di storage guasto deve essere ottenuto dall'interfaccia utente dell'elemento e deve corrispondere al numero di serie riportato sull'etichetta sul retro del nodo.

> In caso di guasti ai componenti in cui il nodo è ancora in linea e funzionante, ad esempio un errore del modulo DIMM (Dual Inline Memory Module), è necessario rimuovere le unità dal cluster prima di rimuovere il nodo guasto.

Fasi

1. Se si verifica un errore DIMM, rimuovere dal cluster le unità associate al nodo che si intende sostituire. Prima di rimuovere il nodo, è possibile utilizzare l'interfaccia utente del software NetApp Element o il punto di estensione della gestione NetApp Element nel plug-in Element per il server vCenter.
2. Rimuovere i nodi utilizzando l'interfaccia utente del software NetApp Element o il punto di estensione della

gestione NetApp Element nel plug-in Element per il server vCenter:

Opzione	Fasi
Utilizzo dell'interfaccia utente di Element	a. Dall'interfaccia utente di Element, selezionare **Cluster > Nodes**. b. Annotare il numero di serie (codice di matricola) del nodo difettoso. Queste informazioni devono corrispondere al numero di serie riportato sull'adesivo sul retro del nodo. c. Dopo aver preso nota del numero di serie, rimuovere il nodo dal cluster come segue: d. Selezionare **azioni** per il nodo che si desidera rimuovere. e. Selezionare **Rimuovi**. È ora possibile rimuovere fisicamente il nodo dallo chassis.
Utilizzo del plug-in Element per l'interfaccia utente del server vCenter	a. Dal punto di estensione della gestione NetApp Element del client Web vSphere, selezionare **Gestione NetApp Element > cluster**. b. Selezionare la sottoscheda **Nodes**. c. Dalla vista attiva, selezionare la casella di controllo per ciascun nodo che si desidera rimuovere, quindi selezionare **azioni > Rimuovi**. d. Confermare l'azione. Tutti i nodi rimossi da un cluster vengono visualizzati nell'elenco dei nodi in sospeso.

Sostituire il nodo di storage nello chassis

Installare il nodo sostitutivo nello stesso slot dello chassis da cui si rimuove il nodo difettoso. Utilizzare il numero di serie annotato dall'interfaccia utente e abbinarlo al numero di serie sul retro del nodo.

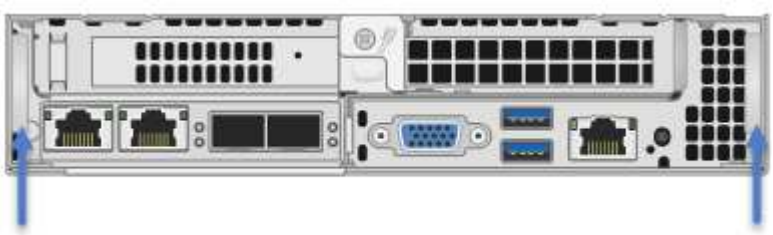
> Assicurarsi di disporre di una protezione antistatica prima di eseguire la procedura riportata di seguito.

Fasi

1. Disimballare il nuovo nodo storage e impostarlo su una superficie piana vicino allo chassis. Conservare il materiale di imballaggio per quando si restituisce il nodo guasto a NetApp.
2. Etichettare ciascun cavo inserito nella parte posteriore del nodo di storage che si desidera rimuovere. Dopo aver installato il nuovo nodo di storage, inserire i cavi nelle porte originali.
3. Scollegare tutti i cavi dal nodo di storage.
4. Tirare verso il basso la maniglia della camma sul lato destro del nodo ed estrarre il nodo utilizzando entrambe le maniglie della camma. La maniglia della camma da tirare verso il basso è dotata di una freccia

che indica la direzione di spostamento. L'altra maniglia CAM non si sposta ed è lì per aiutare a estrarre il nodo.

Supportare il nodo con entrambe le mani quando lo si tira fuori dallo chassis.



5. Posizionare il nodo su una superficie piana.
6. Installare il nodo sostitutivo.
7. Spingere il nodo fino a quando non si sente uno scatto.

   Assicurarsi di non esercitare una forza eccessiva quando si fa scorrere il nodo nel telaio.

8. Ricollegare i cavi alle porte da cui sono stati precedentemente scollegati. Le etichette applicate ai cavi quando sono stati scollegati sono di aiuto.

   Se le prese d'aria sul retro del telaio sono bloccate da cavi o etichette, possono verificarsi guasti prematuri dei componenti dovuti al surriscaldamento. Non forzare i cavi nelle porte, poiché si potrebbero danneggiare i cavi, le porte o entrambe.

   Assicurarsi che il nodo sostitutivo sia cablato nello stesso modo degli altri nodi nello chassis.

9. Premere il pulsante nella parte anteriore del nodo per accenderlo.

Aggiungere il nodo storage al cluster

È necessario aggiungere nuovamente il nodo di storage al cluster. La procedura varia a seconda della versione di NetApp HCI in esecuzione.

Di cosa hai bisogno

- Gli indirizzi IPv4 liberi e inutilizzati si trovano sullo stesso segmento di rete dei nodi esistenti (ogni nuovo nodo deve essere installato sulla stessa rete dei nodi esistenti del suo tipo).
- Si dispone di uno dei seguenti tipi di account cluster di storage SolidFire:
  - L'account Administrator nativo creato durante la distribuzione iniziale
  - Un account utente personalizzato con autorizzazioni Cluster Admin, Drives, Volumes e Node
- Il nuovo nodo è stato cablato e acceso.
- Si dispone dell'indirizzo IPv4 di gestione di un nodo di storage già installato. L'indirizzo IP si trova nella scheda **Gestione NetApp Element > cluster > nodi** del plug-in NetApp Element per vCenter Server.
- Il nuovo nodo utilizza la stessa topologia di rete e lo stesso cablaggio dei cluster di storage esistenti.

  Assicurarsi che la capacità dello storage sia suddivisa in modo uniforme in tutti gli chassis per ottenere la massima affidabilità.

NetApp HCI 1.6P1 e versioni successive

È possibile utilizzare NetApp Hybrid Cloud Control solo se l'installazione di NetApp HCI viene eseguita sulla versione 1.6P1 o successiva.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

```
https://<ManagementNodeIP>/manager/login
```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Nel riquadro di espansione dell'installazione, selezionare **Espandi**.
4. Accedere al motore di implementazione NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI locale.

   Non è possibile accedere utilizzando le credenziali Lightweight Directory Access Protocol.

5. Nella pagina di benvenuto, selezionare **No**.
6. Selezionare **continua**.
7. Nella pagina inventario disponibile, selezionare il nodo di storage che si desidera aggiungere all'installazione di NetApp HCI esistente.
8. Selezionare **continua**.
9. Nella pagina Network Settings (Impostazioni di rete), alcune informazioni di rete sono state rilevate dalla distribuzione iniziale. Ogni nuovo nodo di storage viene elencato in base al numero di serie e si devono assegnare nuove informazioni di rete. Attenersi alla seguente procedura:
   a. Se NetApp HCI ha rilevato un prefisso di denominazione, copiarlo dal campo prefisso di denominazione rilevato e inserirlo come prefisso per il nuovo nome host univoco aggiunto nel campo Nome host.
   b. Nel campo Management IP Address (Indirizzo IP di gestione), immettere un indirizzo IP di gestione per il nuovo nodo di storage all'interno della subnet della rete di gestione.
   c. Nel campo Storage (iSCSI) IP Address (Indirizzo IP storage (iSCSI)), inserire un indirizzo IP iSCSI per il nuovo nodo di storage all'interno della subnet di rete iSCSI.
   d. Selezionare **continua**.

   NetApp HCI potrebbe impiegare del tempo per convalidare gli indirizzi IP immessi. Il pulsante continua diventa disponibile al termine della convalida dell'indirizzo IP.

10. Nella pagina Review della sezione Network Settings (Impostazioni di rete), i nuovi nodi vengono visualizzati in grassetto. Se è necessario apportare modifiche alle informazioni contenute in qualsiasi sezione, attenersi alla seguente procedura:
    a. Selezionare **Modifica** per la sezione.
    b. Una volta apportate le modifiche, selezionare **continua** nelle pagine successive per tornare alla pagina di revisione.
11. Facoltativo: Se non si desidera inviare statistiche del cluster e informazioni di supporto ai server Active IQ ospitati da NetApp, deselezionare la casella di controllo finale. In questo modo si disattiva il monitoraggio

diagnostico e dello stato di salute in tempo reale per NetApp HCI. La disattivazione di questa funzione elimina la possibilità per NetApp di supportare e monitorare in modo proattivo NetApp HCI per rilevare e risolvere i problemi prima che la produzione venga compromessa.

12. Selezionare **Aggiungi nodi**. È possibile monitorare l'avanzamento mentre NetApp HCI aggiunge e configura le risorse.
13. Facoltativo: Verificare che i nuovi nodi di storage siano visibili in VMware vSphere Web Client.

NetApp HCI 1.4 P2, 1.4 e 1.3

Se l'installazione di NetApp HCI esegue la versione 1.4P2, 1.4 o 1.3, è possibile utilizzare il motore di implementazione NetApp per aggiungere il nodo al cluster.

Fasi

1. Individuare l'indirizzo IP di gestione di uno dei nodi di storage esistenti: `http://<storage_node_management_IP_address>/`
2. Accedere al motore di implementazione NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI locale.

   > Non è possibile accedere utilizzando le credenziali Lightweight Directory Access Protocol.

3. Selezionare **espandere l'installazione**.
4. Nella pagina di benvenuto, selezionare **No**.
5. Fare clic su **continua**.
6. Nella pagina inventario disponibile, selezionare il nodo di storage da aggiungere all'installazione di NetApp HCI.
7. Selezionare **continua**.
8. Nella pagina Impostazioni di rete, attenersi alla seguente procedura:
   a. Verificare le informazioni rilevate dall'implementazione iniziale. Ogni nuovo nodo di storage viene elencato in base al numero di serie e si devono assegnare nuove informazioni di rete. Per ogni nuovo nodo di storage, attenersi alla seguente procedura:
      i. Se NetApp HCI ha rilevato un prefisso di denominazione, copiarlo dal campo prefisso di denominazione rilevato e inserirlo come prefisso per il nuovo nome host univoco aggiunto nel campo Nome host.
      ii. Nel campo Management IP Address (Indirizzo IP di gestione), immettere un indirizzo IP di gestione per il nuovo nodo di storage all'interno della subnet della rete di gestione.
      iii. Nel campo Storage (iSCSI) IP Address (Indirizzo IP storage (iSCSI)), inserire un indirizzo IP iSCSI per il nuovo nodo di storage all'interno della subnet di rete iSCSI.
   b. Selezionare **continua**.
   c. Nella pagina Review della sezione Network Settings (Impostazioni di rete), il nuovo nodo viene visualizzato in grassetto. Se si desidera apportare modifiche alle informazioni di qualsiasi sezione, attenersi alla seguente procedura:
      i. Selezionare **Modifica** per la sezione.
      ii. Una volta apportate le modifiche, selezionare **continua** nelle pagine successive per tornare alla pagina di revisione.
9. Facoltativo: Se non si desidera inviare statistiche del cluster e informazioni di supporto ai server Active IQ ospitati da NetApp, deselezionare la casella di controllo finale. In questo modo si disattiva il monitoraggio

diagnostico e dello stato di salute in tempo reale per NetApp HCI. La disattivazione di questa funzione elimina la possibilità per NetApp di supportare e monitorare in modo proattivo NetApp HCI per rilevare e risolvere i problemi prima che la produzione venga compromessa.

10. Selezionare **Aggiungi nodi**. È possibile monitorare l'avanzamento mentre NetApp HCI aggiunge e configura le risorse.
11. Facoltativo: Verificare che i nuovi nodi di storage siano visibili in VMware vSphere Web Client.

NetApp HCI 1.2, 1.1 e 1.0

Quando si installa il nodo, l'interfaccia utente terminale (TUI) visualizza i campi necessari per configurare il nodo. Prima di aggiungere il nodo al cluster, è necessario immettere le informazioni di configurazione necessarie per il nodo.

> È necessario utilizzare l'interfaccia telefonica utente (TUI) per configurare le informazioni di rete statiche e le informazioni del cluster. Se si utilizza la gestione out-of-band, è necessario configurarla sul nuovo nodo.

Per eseguire queste operazioni, è necessario disporre di una console o di una tastiera, di un video, di un mouse (KVM) e delle informazioni di rete e del cluster necessarie per configurare il nodo.

Fasi

1. Collegare una tastiera e un monitor al nodo. La TUI viene visualizzata sul terminale tty1 con la scheda Network Settings (Impostazioni di rete).
2. Utilizzare la navigazione a schermo per configurare le impostazioni di rete Bond1G e Bond10G per il nodo. Inserire le seguenti informazioni per Bond1G:
   - Indirizzo IP. È possibile riutilizzare l'indirizzo IP di gestione dal nodo guasto.
   - Subnet mask. In caso contrario, l'amministratore di rete può fornire queste informazioni.
   - Indirizzo del gateway. In caso contrario, l'amministratore di rete può fornire queste informazioni. Inserire le seguenti informazioni per Bond10G:
   - Indirizzo IP. È possibile riutilizzare l'indirizzo IP dello storage dal nodo guasto.
   - Subnet mask. In caso contrario, l'amministratore di rete può fornire queste informazioni.
3. Invio `s` per salvare le impostazioni, quindi immettere `y` per accettare le modifiche.
4. Invio `c` Per accedere alla scheda Cluster.
5. Utilizzare la navigazione sullo schermo per impostare il nome host e il cluster per il nodo.

   > Se si desidera modificare il nome host predefinito con il nome del nodo rimosso, è necessario farlo ora.

   > Si consiglia di utilizzare lo stesso nome per il nuovo nodo del nodo sostituito per evitare confusione in futuro.

6. Invio `s` per salvare le impostazioni. L'appartenenza al cluster passa da disponibile a in sospeso.
7. Nel plug-in NetApp Element per vCenter Server, selezionare **Gestione NetApp Element > cluster > nodi**.
8. Selezionare **Pending** dall'elenco a discesa per visualizzare l'elenco dei nodi disponibili.
9. Selezionare il nodo che si desidera aggiungere e selezionare **Aggiungi**.

Potrebbero essere necessari fino a 2 minuti per l'aggiunta del nodo al cluster e la visualizzazione in nodi > attivo.

L'aggiunta delle unità contemporaneamente può causare interruzioni. Per le Best practice relative all'aggiunta e alla rimozione di dischi, vedere "Questo articolo della Knowledge base" (accesso richiesto).

10. Selezionare **Drives** (unità).
11. Selezionare **Available** dall'elenco a discesa per visualizzare le unità disponibili.
12. Selezionare le unità che si desidera aggiungere e selezionare **Aggiungi**.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire i nodi H610C e H615C

È necessario sostituire uno chassis per riparare i guasti dei nodi di calcolo relativi alla CPU, alla scheda madre o se non si accende. Se nel nodo di calcolo H610C è presente un modulo DIMM guasto che esegue il sistema operativo NetApp HCI Bootstrap versione 1.6 o successiva, è possibile sostituire il modulo DIMM senza sostituire lo chassis. Per i nodi H615C, non è necessario sostituire lo chassis in caso di guasto di un DIMM; è possibile sostituire solo il DIMM guasto.

Per H610C e H615C, i termini "nodo" e "chassis" sono utilizzati in modo intercambiabile, perché il nodo e lo chassis non sono componenti separati.

NetApp consiglia di utilizzare il motore di implementazione NetApp per aggiungere un nodo di calcolo sostitutivo. Se non è possibile utilizzare il motore di distribuzione NetApp per l'installazione ESXi, consultare l'articolo della Knowledge base di NetApp "Come installare ESXi sul nodo di calcolo NetApp HCI manualmente".

Di cosa hai bisogno

- È stato verificato che il nodo non funziona correttamente.
- Si dispone di uno chassis sostitutivo. Per ordinare un prodotto sostitutivo, contattare il supporto NetApp.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o di un'altra protezione antistatica.
- Ciascun cavo collegato al telaio è etichettato.

A proposito di questa attività

Gli allarmi di VMware vSphere Web Client avvisano l'utente in caso di guasto di un host. Il numero di serie dell'host guasto di VMware vSphere Web Client deve corrispondere al numero di serie riportato sull'etichetta sul retro del nodo.

Fase 1: Preparare la sostituzione del nodo

Prima di sostituire il nodo, è necessario migrare le macchine virtuali (VM) ospitate sul nodo in un host

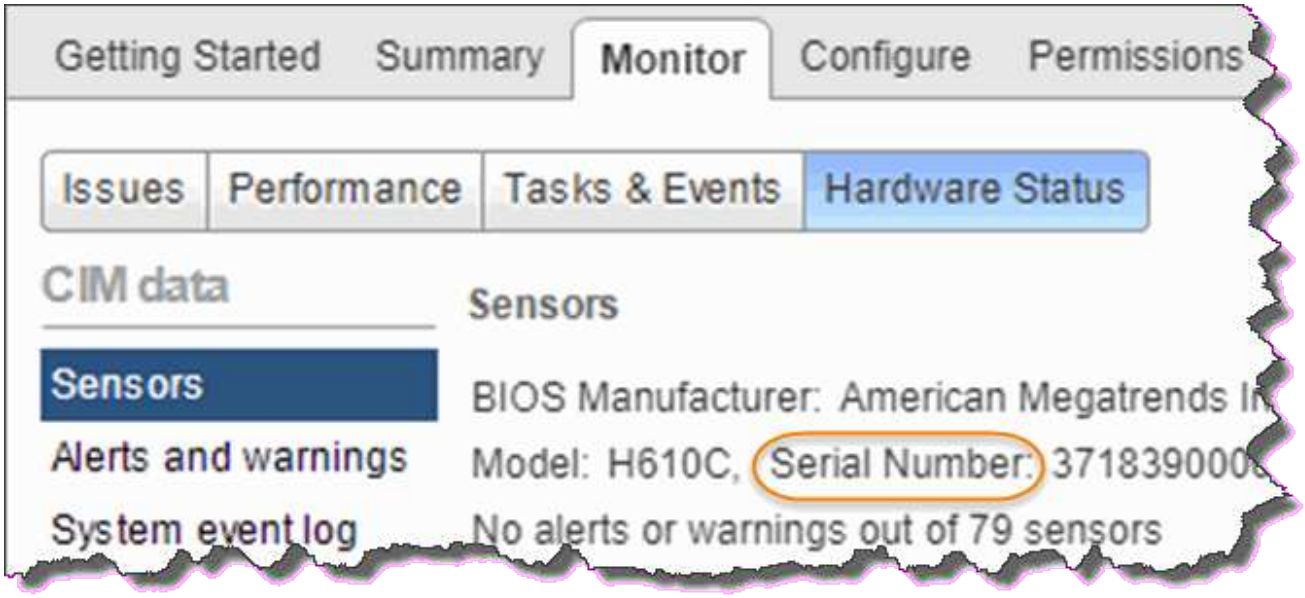
disponibile e rimuovere il nodo dal cluster. È necessario registrare i dettagli del nodo, ad esempio il numero di serie e le informazioni di rete. La migrazione delle macchine virtuali e la registrazione dei dettagli del nodo si applicano anche in caso di guasti ai componenti in cui il nodo è ancora in linea e funzionante, ad esempio un guasto del modulo DIMM (Dual Inline Memory Module).

Fasi

1. In VMware vSphere Web Client, eseguire la procedura per migrare le macchine virtuali su un altro host disponibile.

   Consultare la documentazione VMware per le fasi della migrazione.

2. Selezionare il nodo guasto e selezionare **Monitor > hardware Status > Sensors**.
3. Annotare il numero di serie del nodo guasto. La seguente schermata è solo un esempio:



   Per identificare lo chassis, è necessario disporre del numero di serie corrispondente a quello indicato sull'adesivo sul retro del nodo.

4. Fare clic con il pulsante destro del mouse sul nodo guasto e selezionare **connessione > Disconnetti**.
5. Selezionare **Sì** per confermare l'azione.
6. Fare clic con il pulsante destro del mouse sul nodo guasto e selezionare **Rimuovi dall'inventario**.
7. Fare clic su **Sì** per confermare l'azione.

Fase 2: Sostituire il nodo

Dopo aver rimosso il nodo guasto dal cluster, è possibile rimuovere lo chassis guasto e installare lo chassis sostitutivo.

Assicurarsi di disporre di una protezione antistatica prima di eseguire la procedura riportata di seguito.

Fasi

1. Disimballare il nuovo chassis e impostarlo su una superficie piana. Conservare il materiale di imballaggio

per quando si restituisce lo chassis guasto a NetApp.

2. Etichettare ciascun cavo inserito nella parte posteriore dello chassis che si desidera rimuovere. Dopo aver installato il nuovo chassis, inserire nuovamente i cavi nelle porte originali.
3. Scollegare tutti i cavi dal retro dello chassis.
4. Rimuovere il telaio svitando le viti a testa zigrinata sulle linguette di montaggio. È necessario imballare e restituire lo chassis guasto a NetApp.
5. Far scorrere il telaio sostitutivo sulle guide.

   Assicurarsi di non esercitare una forza eccessiva quando si fa scorrere il telaio sulle guide.

6. Solo per H615C. Rimuovere i DIMM dal telaio guasto e inserirli nel telaio sostitutivo.

   Sostituire i DIMM negli stessi slot da cui sono stati rimossi nel nodo guasto.

7. Rimuovere le due unità di alimentazione su entrambi i lati dello chassis guasto e inserirle nello chassis sostitutivo.
8. Ricollegare i cavi alle porte da cui sono stati precedentemente scollegati. Le etichette aggiunte ai cavi quando vengono scollegati saranno di aiuto.

   Se le prese d'aria sul retro del telaio sono bloccate da cavi o etichette, possono verificarsi guasti prematuri dei componenti dovuti al surriscaldamento. Non forzare i cavi nelle porte, poiché si potrebbero danneggiare i cavi, le porte o entrambe.

9. Accendere lo chassis.

Passaggio 3: Aggiungere il nodo al cluster

È necessario configurare NetApp HCI in modo che utilizzi il nuovo nodo di calcolo.

Di cosa hai bisogno

- L'istanza vSphere in uso da NetApp HCI dispone di licenze vSphere Enterprise Plus se si aggiunge il nodo a un'implementazione con Virtual Distributed Switch.
- Nessuna delle istanze vCenter o vSphere in uso con NetApp HCI dispone di licenze scadute.
- Gli indirizzi IPv4 liberi e inutilizzati si trovano sullo stesso segmento di rete dei nodi esistenti (il nuovo nodo deve essere installato sulla stessa rete dei nodi esistenti del suo tipo).
- Le credenziali dell'account amministratore vCenter sono pronte.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI.
3. Nel riquadro di espansione dell'installazione, selezionare **Espandi**.

   Il browser apre NetApp Deployment Engine.

4. Accedere al motore di implementazione NetApp fornendo le credenziali di amministratore del cluster di storage NetApp HCI locale.

> Non è possibile accedere utilizzando le credenziali Lightweight Directory Access Protocol.

5. Nella pagina di benvenuto, selezionare **Sì**.
6. Nella pagina End User License (licenza per l'utente finale), eseguire le seguenti operazioni:
   a. Leggi il contratto di licenza con l'utente finale di VMware.
   b. Se si accettano i termini, selezionare **Accetto** alla fine del testo del contratto.
7. Fare clic su continua.
8. Nella pagina vCenter, attenersi alla seguente procedura:
   a. Immettere un indirizzo FQDN o IP e le credenziali di amministratore per l'istanza di vCenter associata all'installazione di NetApp HCI.
   b. Selezionare **continua**.
   c. Selezionare un data center vSphere esistente a cui aggiungere i nuovi nodi di calcolo oppure selezionare Create New Datacenter (Crea nuovo data center) per aggiungere i nuovi nodi di calcolo a un nuovo data center.

> Se si seleziona Create New Datacenter (Crea nuovo data center), il campo Cluster viene compilato automaticamente.

   d. Se è stato selezionato un data center esistente, selezionare un cluster vSphere a cui associare i nuovi nodi di calcolo.

> Se NetApp HCI non riconosce le impostazioni di rete del cluster selezionato per l'espansione, assicurarsi che il mapping vmkernel e vmnic per le reti di gestione, storage e vMotion sia impostato sui valori predefiniti di implementazione.

   e. Selezionare **continua**.
9. Nella pagina delle credenziali ESXi, immettere una password radice ESXi per il nodo di calcolo o i nodi che si desidera aggiungere. Utilizzare la stessa password creata durante la distribuzione iniziale di NetApp HCI.
10. Selezionare **continua**.
11. Se è stato creato un nuovo cluster di data center vSphere, nella pagina topologia di rete, selezionare una topologia di rete che corrisponda ai nuovi nodi di calcolo che si stanno aggiungendo.

> È possibile selezionare l'opzione a due cavi solo se i nodi di calcolo utilizzano la topologia a due cavi e l'implementazione NetApp HCI esistente è configurata con ID VLAN.

12. Nella pagina inventario disponibile, selezionare il nodo da aggiungere all'installazione di NetApp HCI esistente.

> Per alcuni nodi di calcolo, potrebbe essere necessario abilitare EVC al livello più elevato supportato dalla versione di vCenter prima di poterli aggiungere all'installazione. Utilizzare il client vSphere per abilitare EVC per questi nodi di calcolo. Una volta attivata, aggiornare la pagina Inventory e provare ad aggiungere nuovamente i nodi di calcolo.

13. Selezionare **continua**.
14. Facoltativo: Se è stato creato un nuovo cluster di data center vSphere, nella pagina Impostazioni di rete, importare le informazioni di rete da un'implementazione NetApp HCI esistente selezionando la casella di controllo **Copia impostazione da un cluster esistente**. In questo modo vengono inserite le informazioni predefinite relative al gateway e alla subnet per ciascuna rete.
15. Nella pagina Network Settings (Impostazioni di rete), alcune informazioni di rete sono state rilevate dalla distribuzione iniziale. Ogni nuovo nodo di calcolo viene elencato in base al numero di serie e si devono assegnare nuove informazioni di rete. Per ogni nuovo nodo di calcolo, attenersi alla seguente procedura:
    a. Se NetApp HCI ha rilevato un prefisso di denominazione, copiarlo dal campo prefisso di denominazione rilevato e inserirlo come prefisso per il nuovo nome host univoco aggiunto nel campo Nome host.
    b. Nel campo Management IP Address (Indirizzo IP di gestione), immettere un indirizzo IP di gestione per il nodo di calcolo all'interno della subnet della rete di gestione.
    c. Nel campo vMotion IP Address (Indirizzo IP vMotion), immettere un indirizzo IP vMotion per il nodo di calcolo che si trova all'interno della subnet di rete vMotion.
    d. Nel campo iSCSI A - IP Address (Indirizzo IP iSCSI A), immettere un indirizzo IP per la prima porta iSCSI del nodo di calcolo che si trova nella subnet di rete iSCSI.
    e. Nel campo iSCSI B - IP Address (Indirizzo IP - iSCSI B), immettere un indirizzo IP per la seconda porta iSCSI del nodo di calcolo che si trova all'interno della subnet di rete iSCSI.
16. Selezionare **continua**.
17. Nella pagina Review della sezione Network Settings (Impostazioni di rete), il nuovo nodo viene visualizzato in grassetto. Se è necessario apportare modifiche alle informazioni contenute in qualsiasi sezione, attenersi alla seguente procedura:
    a. Selezionare **Modifica** per la sezione.
    b. Una volta apportate le modifiche, selezionare **continua** nelle pagine successive per tornare alla pagina di revisione.
18. Facoltativo: Se non si desidera inviare statistiche del cluster e informazioni di supporto ai server SolidFire Active IQ ospitati da NetApp, deselezionare la casella di controllo finale. In questo modo si disattiva il monitoraggio diagnostico e dello stato di salute in tempo reale per NetApp HCI. La disattivazione di questa funzione elimina la possibilità per NetApp di supportare e monitorare in modo proattivo NetApp HCI per rilevare e risolvere i problemi prima che la produzione venga compromessa.
19. Selezionare **Aggiungi nodi**. È possibile monitorare l'avanzamento mentre NetApp HCI aggiunge e configura le risorse.
20. Facoltativo: Verificare che i nuovi nodi di calcolo siano visibili in vCenter.

Fase 4: Installare i driver della GPU

I nodi di calcolo con unità di elaborazione grafica NVIDIA (GPU), come il nodo H610C, necessitano dei driver software NVIDIA installati in VMware ESXi per poter sfruttare la maggiore potenza di elaborazione. Per installare i driver della GPU, il nodo di calcolo deve disporre di una scheda GPU.

Fasi

1. Aprire un browser e accedere al portale delle licenze NVIDIA al seguente URL: `https://nvid.nvidia.com/dashboard/`
2. Scaricare la versione del pacchetto di driver sul computer, a seconda dell'ambiente in uso.

   L'esempio seguente mostra la versione del pacchetto di driver per vSphere 6,0, 6,5 e 6,7:

Versione di vSphere	Pacchetto di driver
VSphere 6.0	NVIDIA-GRID-vSphere-6.0-390.94-390.96-392.05.zip
VSphere 6.5	NVIDIA-GRID-vSphere-6.5-410.92-410.91-412.16.zip
VSphere 6.7	NVIDIA-GRID-vSphere-6.7-410.92-410.91-412.16.zip

3. Estrarre il pacchetto di driver sul computer. Il file .VIB risultante è il file del driver non compresso.
4. Copiare il file del driver .VIB dal computer a ESXi in esecuzione sul nodo di calcolo. L'utility SCP (Secure Copy Protocol) è disponibile nella maggior parte delle distribuzioni Linux o come utility scaricabile per tutte le versioni di Windows.

   Nell'esempio seguente vengono illustrati i comandi per ESXi 6,0, 6,5 e 6,7. I comandi presuppongono che il driver si trovi nella directory $HOME/NVIDIA/ESX6.x/ sull'host di gestione:

Opzione	Descrizione
ESXi 6.0	scp@HOME/NVIDIA/ESX6.0/NVIDIA**.vib root <ESXi_IP_ADDR>:/.
ESXi 6.5	casa/NVIDIA/ESX6.5/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.
ESXi 6.7	casa/NVIDIA/ESX6.7/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.

5. Attenersi alla seguente procedura per accedere come root all'host ESXi e installare NVIDIA vGPU manager in ESXi.
   a. Eseguire il seguente comando per accedere all'host ESXi come utente root:
      `ssh root@<ESXi_IP_ADDRESS>`
   b. Eseguire il seguente comando per verificare che non siano installati driver NVIDIA GPU:
      `nvidia-smi`Questo comando dovrebbe restituire il messaggio `nvidia-smi: not found`.
   c. Eseguire i seguenti comandi per attivare la modalità di manutenzione sull'host e installare NVIDIA vGPU Manager dal file VIB:
      `esxcli system maintenanceMode set --enable true`
      `esxcli software vib install -v /NVIDIA**.vib`Viene visualizzato il messaggio `Operation finished successfully`.
   d. Eseguire il seguente comando e verificare che tutti gli otto driver GPU siano elencati nell'output del comando:
      `nvidia-smi`
   e. Eseguire il seguente comando per verificare che il pacchetto NVIDIA vGPU sia stato installato e caricato correttamente:

```
vmkload_mod -l | grep nvidia`Il comando dovrebbe restituire un output simile
al seguente: `nvidia 816 13808
```

f. Eseguire i seguenti comandi per uscire dalla modalità di manutenzione e riavviare l'host:
```
esxcli system maintenanceMode set -enable false
reboot -f
```

6. Ripetere i passaggi 4-6 per tutti gli altri nodi di calcolo appena implementati con GPU NVIDIA.
7. Eseguire le seguenti operazioni seguendo le istruzioni riportate nel sito della documentazione NVIDIA:
   a. Installare il server di licenza NVIDIA.
   b. Configurare le macchine virtuali guest per il software NVIDIA vGPU.
   c. Se si utilizzano desktop compatibili con vGPU in un contesto di infrastruttura di desktop virtuale (VDI), configurare VMware Horizon View per il software NVIDIA vGPU.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire i nodi H610S

Potrebbe essere necessario sostituire lo chassis se la ventola, l'unità di elaborazione centrale (CPU) o il modulo DIMM (Dual Inline Memory Module) si guasta o se si verificano problemi di surriscaldamento o problemi durante il processo di avvio. Il LED ambra lampeggiante nella parte anteriore dello chassis indica la possibile necessità di sostituire lo chassis. Prima di procedere, contatta il supporto NetApp.

> Vedere "Articolo della Knowledge base" Per informazioni sui requisiti di installazione per i nodi H610S. I nodi storage H610S nuovi e spare potrebbero avere requisiti di installazione aggiuntivi in base alla versione software Element esistente del cluster di storage. Per ulteriori informazioni, contatta il supporto NetApp.

> I termini "nodo" e "chassis" sono utilizzati in modo intercambiabile nel caso di H610S, che è uno chassis a un'unità rack (1U).

Best practice per l'aggiunta e la rimozione di dischi

Attenersi alle seguenti Best practice per aggiungere dischi al cluster:

- Aggiungi tutti i dischi a blocchi e assicurati che la sincronizzazione dei blocchi sia completa prima di aggiungere i dischi slice.
- Per il software Element 10.x e versioni successive, aggiungere tutti i dischi a blocchi contemporaneamente. Assicurarsi di non eseguire questa operazione per più di tre nodi alla volta.
- Per il software Element 9.x e versioni precedenti, aggiungere tre dischi alla volta per sincronizzarli completamente prima di aggiungere il gruppo successivo di tre.
- Rimuovere il disco slice e assicurarsi che la sincronizzazione slice sia completa prima di rimuovere i dischi a blocchi.

- Rimuovere tutti i dischi a blocchi da un singolo nodo alla volta. Assicurarsi che la sincronizzazione di tutti i blocchi sia completa prima di passare al nodo successivo.

Di cosa hai bisogno

- Hai contattato il supporto NetApp. Se stai ordinando un prodotto sostitutivo, dovresti avere un caso aperto con il supporto NetApp.
- Il nodo sostitutivo è stato ottenuto.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o di un'altra protezione antistatica.
- Se è necessario eseguire la procedura di ripristino dell'immagine di fabbrica (RTFI), è stata ottenuta la chiave USB. Il supporto NetApp può aiutarti a decidere se eseguire il processo RTFI.
- Si dispone di una tastiera e di un monitor.
- Il nodo guasto è stato rimosso correttamente dal cluster.
- In caso di guasto di un DIMM, sono state rimosse le unità prima di rimuovere il nodo dal cluster.

A proposito di questa attività

Gli allarmi di VMware vSphere Web Client avvisano l'utente in caso di guasto di un host. Il numero di serie dell'host guasto di VMware vSphere Web Client deve corrispondere al numero di serie riportato sull'etichetta sul retro del nodo.

Fasi

1. Individuare il codice di matricola nella parte anteriore dello chassis guasto.

2. Verificare che il numero di serie sul codice di matricola corrisponda al numero del caso NetApp Support al momento dell'ordine dello chassis sostitutivo.
3. Collegare la tastiera e il monitor al retro dello chassis guasto.
4. Verificare il numero di serie del nodo guasto con il supporto NetApp.
5. Spegnere lo chassis.
6. Etichettare le unità nella parte anteriore e i cavi nella parte posteriore con le rispettive posizioni, in modo da poterle riposizionare nelle stesse posizioni dopo la sostituzione.

Vedere la seguente immagine per il posizionamento delle unità nello chassis:

7. Rimuovere i cavi.
8. Rimuovere il telaio svitando le viti a testa zigrinata sulle linguette di montaggio. È necessario imballare e restituire lo chassis guasto a NetApp.
9. Installare il telaio sostitutivo.
10. Rimuovere con cautela le unità dallo chassis guasto e inserirle nello chassis sostitutivo.

    Inserire le unità negli stessi slot in cui si trovavano prima di rimuoverle.

11. Rimuovere le unità di alimentazione dallo chassis guasto e inserirle nello chassis sostitutivo.
12. Inserire i cavi di alimentazione e di rete nelle porte originali.
13. I ricetrasmettitori SFP (Small Form-factor Pluggable) potrebbero essere inseriti nelle porte 10 GbE del nodo sostitutivo. Rimuoverli prima di collegare via cavo le porte 10GbE.

    Se lo switch non riconosce i cavi, consultare la documentazione del fornitore dello switch.

14. Accendere lo chassis premendo il pulsante di accensione sulla parte anteriore. L'avvio del nodo richiede circa cinque minuti e 30 secondi.
15. Eseguire la procedura di configurazione.
    - Se il nodo H610S fa parte di un'installazione NetApp HCI, utilizzare il controllo del cloud ibrido NetApp per configurare la risorsa di storage. Vedere "Espandere le risorse di storage NetApp HCI".
    - Se il nodo H610S fa parte di un'installazione di storage all-flash SolidFire, configurare il nodo utilizzando l'interfaccia utente del software NetApp Element. Contattare il supporto NetApp per assistenza.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire le unità di alimentazione

Ogni chassis include due alimentatori per la ridondanza dell'alimentazione. Se un alimentatore è difettoso, sostituirlo il prima possibile per assicurarsi che lo chassis disponga di una fonte di alimentazione ridondante.

Di cosa hai bisogno

- L'alimentatore è guasto.
- Si dispone di un alimentatore sostitutivo.
- Hai verificato che il secondo alimentatore funziona.

- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o si sono prese altre precauzioni antistatiche.

A proposito di questa attività

La procedura di sostituzione si applica ai seguenti modelli di nodi:

- Due unità rack (2U), chassis NetApp HCI a quattro nodi
- Chassis di calcolo 2U H610C
- Uno chassis di calcolo H615C per unità rack (1U)
- Chassis storage 1U H610S

> Nel caso di H610C, H615C e H610S, i termini "nodo" e "chassis" sono utilizzati in modo intercambiabile perché nodo e chassis non sono componenti separati, a differenza del caso di chassis 2U a quattro nodi.

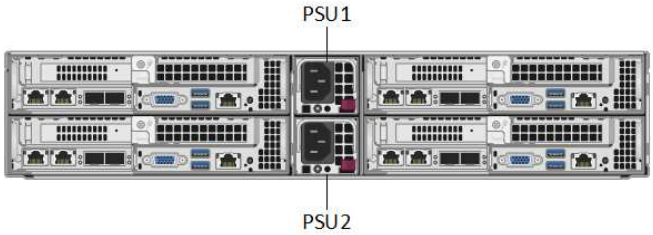
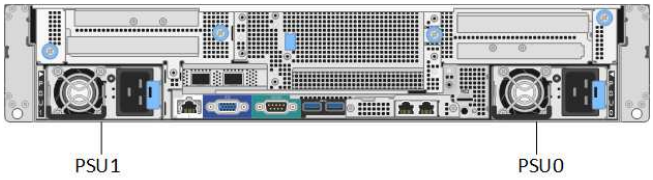
Gli allarmi di VMware vSphere Web Client forniscono informazioni sull'unità di alimentazione guasta, riferendosi a PS1 o PS2. In uno chassis NetApp HCI 2U a quattro nodi, PS1 si riferisce all'unità nella riga superiore dello chassis e PS2 all'unità nella riga inferiore dello chassis. È possibile sostituire l'unità di alimentazione difettosa mentre lo chassis è acceso e funzionante, purché l'unità di alimentazione ridondante funzioni.

Fasi

1. Individuare l'unità di alimentazione difettosa nel telaio. Il LED sull'unità guasta è di colore ambra.

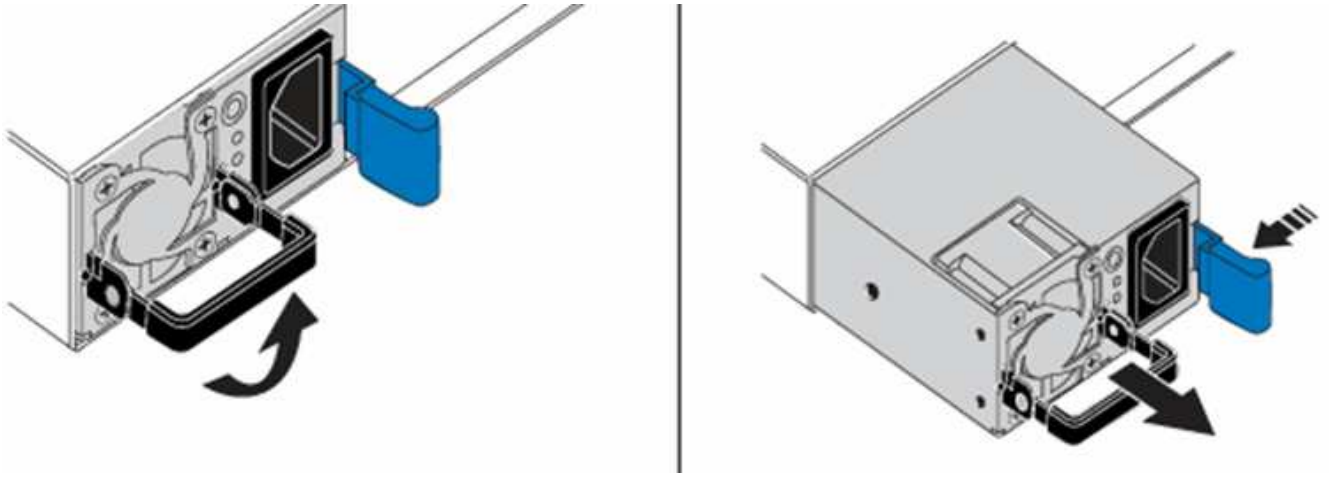
   > Le unità di alimentazione si trovano in modo diverso a seconda del tipo di chassis.

   Vedere le immagini riportate di seguito per le posizioni degli alimentatori:

Modello	Ubicazione delle unità di alimentazione
Chassis storage NetApp HCI 2U a quattro nodi	 I nodi nello chassis potrebbero essere diversi a seconda del tipo di nodi (storage o calcolo) in uso.
Chassis H610C	

Modello	Ubicazione delle unità di alimentazione
Chassis H615C	
Chassis H610S	

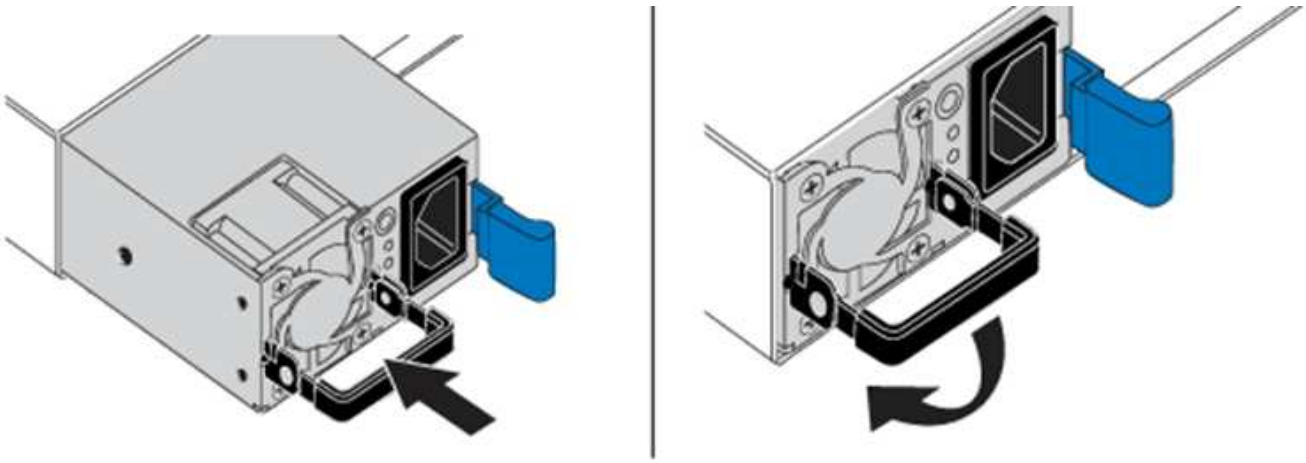
2. Scollegare il cavo di alimentazione dall'unità di alimentazione.
3. Sollevare la maniglia della camma e premere il fermo blu per estrarre l'alimentatore.



L'illustrazione è un esempio. La posizione dell'alimentatore nello chassis e il colore del pulsante di rilascio variano a seconda del tipo di chassis in uso.

Assicurarsi di utilizzare entrambe le mani per sostenere il peso dell'alimentatore.

4. Allineare con entrambe le mani i bordi dell'alimentatore con l'apertura del telaio, spingere delicatamente l'unità nel telaio utilizzando la maniglia della camma fino a bloccarla in posizione e riportare la maniglia della camma in posizione verticale.



5. Collegare il cavo di alimentazione.
6. Restituire l'unità difettosa a NetApp seguendo le istruzioni riportate nella confezione.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire gli switch SN2010, SN2100 e SN2700

È possibile sostituire uno switch serie SN2000 guasto senza interruzioni seguendo le Best practice e le procedure fornite da NetApp.

Di cosa hai bisogno

- Assicurarsi che Putty sia installato sul laptop e che l'output venga acquisito. Guarda questo video per scoprire come configurare Putty per acquisire la sessione di output.

[] | *https://img.youtube.com/vi/2LZfWH8HffA/maxresdefault.jpg*

- Assicurarsi di eseguire NetApp Config Advisor prima e dopo la sostituzione. Questo può aiutare a identificare altri problemi prima dell'inizio della manutenzione. Scaricare e installare Config Advisor, quindi accedere alla Guida di avvio rapido da "qui (accesso richiesto)".
- Procurarsi un cavo di alimentazione, gli attrezzi manuali di base e le etichette.
- Assicurarsi di aver pianificato una finestra di manutenzione di due o quattro ore.
- Acquisire familiarità con le porte dello switch riportate di seguito:

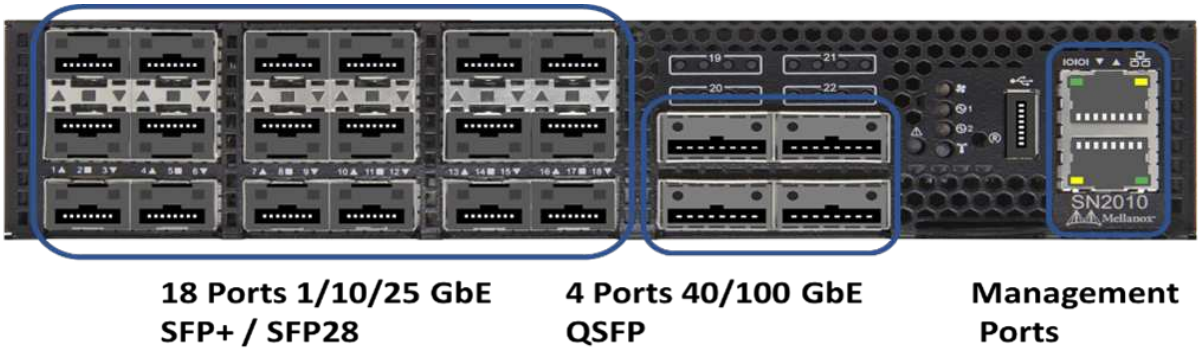


Figura 1. Porta e mascherina dello switch SN2010

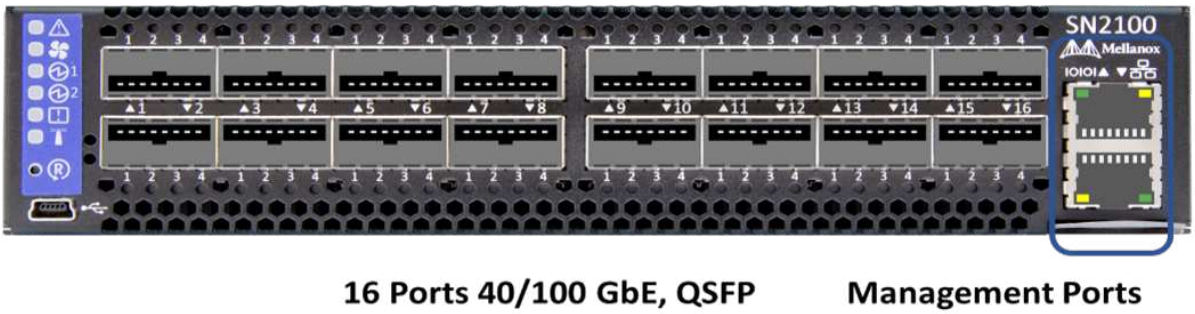


Figura 2. Porta e mascherina dello switch SN2100

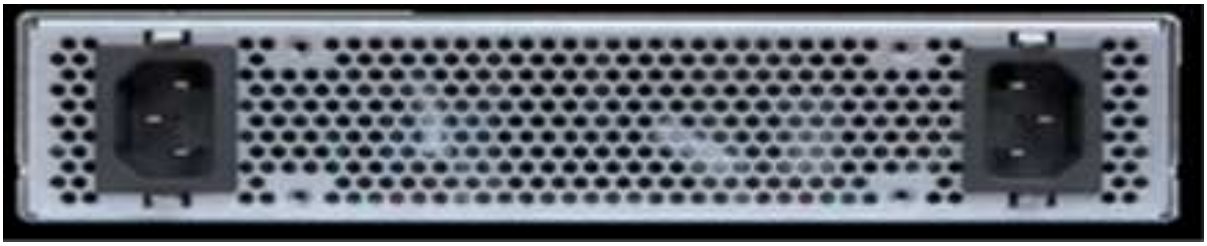


Figura 3. Switch SN2010 e SN2100 posteriore

Figura 4. Switch SN2700 anteriore e posteriore

A proposito di questa attività

Eseguire i passaggi descritti in questa procedura nell'ordine riportato di seguito. In questo modo si garantisce che il downtime sia minimo e che lo switch sostitutivo sia preconfigurato prima della sostituzione dello switch.

> Contatta il supporto NetApp se hai bisogno di assistenza.

Di seguito viene riportata una panoramica delle fasi della procedura:Prepararsi a sostituire l'interruttore difettoso
Creare il file di configurazione
Rimuovere l'interruttore difettoso e installare quello sostitutivo
Verificare la versione del sistema operativo sullo switch
Configurare lo switch sostitutivo
Completare la sostituzione

Prepararsi a sostituire l'interruttore difettoso

Prima di sostituire lo switch difettoso, procedere come segue.

Fasi

1. Verificare che lo switch sostitutivo sia dello stesso modello dello switch guasto.
2. Etichettare tutti i cavi collegati allo switch guasto.
3. Identificare il file server esterno in cui sono salvati i file di configurazione dello switch.
4. Assicurarsi di aver ottenuto le seguenti informazioni:
    a. Interfaccia utilizzata per la configurazione iniziale: Porta RJ-45 o interfaccia terminale seriale.
    b. Credenziali necessarie per l'accesso allo switch: Indirizzo IP della porta di gestione dello switch non difettoso e dello switch guasto.
    c. Le password per l'accesso all'amministrazione.

Creare il file di configurazione

È possibile configurare uno switch utilizzando i file di configurazione creati. Scegliere una delle seguenti opzioni per creare il file di configurazione per lo switch.

Opzione	Fasi

Creare il file di configurazione di backup dallo switch difettoso	1. Connettersi allo switch in remoto utilizzando SSH come illustrato nell'esempio seguente:
	`ssh admin@<switch_IP_address`
	2. Accedere alla modalità di configurazione come illustrato nell'esempio seguente:
	`switch > enable`
	`switch # configure terminal`
	3. Individuare i file di configurazione disponibili come mostrato nell'esempio seguente:
	`switch (config) #`
	`switch (config) # show configuration files`
	4. Salvare il file di configurazione BIN attivo su un server esterno:
	`switch (config) # configuration upload my-filename scp://myusername@my-server/path/to/my/<file>`

Opzione	Fasi

Creare il file di configurazione di backup modificando il file da un altro switch	1. Connettersi allo switch in remoto utilizzando SSH come illustrato nell'esempio seguente:
	`ssh admin@<switch_IP_address`
	2. Accedere alla modalità di configurazione come illustrato nell'esempio seguente:
	`switch > enable`
	`switch # configure terminal`
	3. Caricare un file di configurazione basato su testo dallo switch a un server esterno, come illustrato nell'esempio seguente:
	`switch (config) #`
	`switch (config) # configuration text file my-filename upload scp://root@my-server/root/tmp/my-filename`
	4. Modificare i seguenti campi nel file di testo in modo che corrispondano allo switch guasto:
	`## Network interface configuration`
	`##`
	`no interface mgmt0 dhcp`
	`interface mgmt0 ip address XX.XXX.XX.XXX /22`
	`##`
	`## Other IP configuration`
	`##`
	`hostname oldhostname`

Rimuovere l'interruttore difettoso e installare quello sostitutivo

Eseguire la procedura per rimuovere lo switch difettoso e installare il prodotto sostitutivo.

Fasi

1. Individuare i cavi di alimentazione sullo switch difettoso.
2. Etichettare e scollegare i cavi di alimentazione dopo il riavvio dello switch.
3. Etichettare e scollegare tutti i cavi dallo switch difettoso e fissarli per evitare di danneggiarli durante la sostituzione dello switch.
4. Rimuovere lo switch dal rack.
5. Installare lo switch sostitutivo nel rack.
6. Collegare i cavi di alimentazione e i cavi delle porte di gestione.

> L'interruttore si accende automaticamente quando viene applicata l'alimentazione CA. Non è presente alcun pulsante di accensione. Potrebbero essere necessari fino a cinque minuti prima che il LED di stato del sistema diventi verde.

7. Connettersi allo switch utilizzando la porta di gestione RJ-45 o l'interfaccia terminale seriale.

Verificare la versione del sistema operativo sullo switch

Verificare la versione del software del sistema operativo sullo switch. La versione dello switch difettoso e quella dello switch integro devono corrispondere.

Fasi

1. Connettersi allo switch in remoto utilizzando SSH.
2. Accedere alla modalità di configurazione.
3. Eseguire `show version` comando. Vedere il seguente esempio:

```
SFPS-HCI-SW02-A (config) #show version
Product name:      Onyx
Product release:   3.7.1134
Build ID:          #1-dev
Build date:        2019-01-24 13:38:57
Target arch:       x86_64
Target hw:         x86_64
Built by:          jenkins@e4f385ab3f49
Version summary:   X86_64 3.7.1134 2019-01-24 13:38:57 x86_64

Product model:     x86onie
Host ID:           506B4B3238F8
System serial num: MT1812X24570
System UUID:       27fe4e7a-3277-11e8-8000-506b4b891c00

Uptime:            307d 3h 6m 33.344s
CPU load averages: 2.40 / 2.27 / 2.21
Number of CPUs:    4
System memory:     3525 MB used / 3840 MB free / 7365 MB total
Swap:              0 MB used / 0 MB free / 0 MB total
```

4. Se le versioni non corrispondono, aggiornare il sistema operativo. Vedere "Guida all'aggiornamento del software Mellanox" per ulteriori informazioni.

Configurare lo switch sostitutivo

Eseguire la procedura per configurare lo switch sostitutivo. Vedere "Gestione della configurazione Mellanox" per ulteriori informazioni.

Fasi

1. Scegli tra le opzioni che più ti riguardano:

Opzione	Fasi

Dal file di configurazione BIN	1. Recuperare il file DI configurazione BIN come mostrato nell'esempio seguente:
	`switch (config) # configuration fetch scp://myusername@my-server/path/to/my/<file>`
	2. Caricare il file di configurazione BIN recuperato nella fase precedente, come mostrato nell'esempio seguente:
	`switch (config) # configuration switch-to my-filename`
	3. Tipo `yes` per confermare il riavvio.

Opzione	Fasi

Dal file di testo	1. Ripristinare le impostazioni predefinite dello switch:
	`switch (config) # reset factory keep-basic`
	2. Applicare il file di configurazione basato su testo:
	`switch (config) # configuration text file my-filename apply`
	3. Caricare un file di configurazione basato su testo dallo switch a un server esterno, come illustrato nell'esempio seguente:
	`switch (config) #`
	`switch (config) # configuration text file my-filename upload scp://root@my-server/root/tmp/my-filename`
	Non è necessario riavviare il sistema quando si applica il file di testo.

Completare la sostituzione

Eseguire i passaggi per completare la procedura di sostituzione.

Fasi

1. Inserire i cavi utilizzando le etichette come guida.
2. Eseguire NetApp Config Advisor. Accedere alla Guida di avvio rapido da "qui (accesso richiesto)".
3. Verificare l'ambiente di storage.
4. Restituire lo switch difettoso a NetApp.

Trova ulteriori informazioni

- "Pagina delle risorse NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Sostituire il nodo di storage in un cluster a due nodi

Prima di sostituire un nodo di storage che fa parte di un cluster a due nodi, è necessario aggiungere un terzo nodo di storage (che richiede un nuovo set di indirizzi IP), consentire il completamento della sincronizzazione, quindi rimuovere il nodo difettoso. Il cluster rimane in stato degradato fino a quando un nodo sostitutivo non si unisce al cluster.

Di cosa hai bisogno

- Si dispone di nuovi indirizzi IP di gestione e IP di storage.
- È stato verificato che il cluster visualizza `ClusterCannotSync` avvisa dopo che il nodo è offline. Ciò garantisce che il cluster esegua una risincronizzazione completa quando il nuovo nodo viene aggiunto di nuovo al cluster. Questo avviso viene visualizzato circa sei minuti dopo che il nodo di storage non è in linea.
- Hai contattato il supporto NetApp. Se stai ordinando un prodotto sostitutivo, dovresti avere un caso aperto con il supporto NetApp.
- Il nodo sostitutivo è stato ottenuto.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o di un'altra protezione antistatica.

A proposito di questa attività

Gli allarmi di VMware vSphere Web Client avvisano l'utente in caso di guasto di un host. Il numero di serie dell'host guasto di VMware vSphere Web Client deve corrispondere al numero di serie riportato sull'etichetta sul retro del nodo.

Fasi

1. Rimuovere fisicamente il nodo difettoso dal rack. I passaggi dipendono dal tipo di nodo di storage in uso. Vedere "Sostituire i nodi H410S" e. "Sostituire i nodi H610S".

   Non rimuovere il nodo dal cluster a questo punto.

2. Installare il nodo sostitutivo nello stesso slot.
3. Collegare il nodo.
4. Accendere il nodo.
5. Collegare una tastiera e un monitor al nodo.
6. Eseguire la procedura di configurazione:
   a. Configurare l'indirizzo IP IPMI/BMC.
   b. Configurare il nuovo nodo con i nuovi indirizzi IP di gestione e di storage e il nome del cluster.
7. Una volta aggiunto il nodo al cluster, aggiungere i dischi.
8. Al termine della sincronizzazione, rimuovere i dischi guasti e il nodo guasto dal cluster.
9. Utilizza NetApp Hybrid Cloud Control per configurare il nuovo nodo di storage aggiunto. Vedere "Espandere le risorse di storage NetApp HCI".

Trova ulteriori informazioni

- "Centro di documentazione NetApp HCI"
- "Centro di documentazione software SolidFire ed Element"

Versioni precedenti della documentazione di NetApp HCI

La documentazione relativa alle versioni precedenti di NetApp HCI è disponibile nel caso in cui non si utilizzi la versione più recente.

- "NetApp HCI 1.8P1"
- "NetApp HCI 1.8 e versioni precedenti"

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per Ansible role for Compute Upgrades"
- "Avviso per Ember OS 12.3.1"
- "Avviso per Ember OS 12.3"
- "Avviso per il nodo di gestione 12.3.1"
- "Avviso per il nodo di gestione 12.3"
- "Avviso per NetApp HCI 1.9P1"
- "Avviso per NetApp HCI 1.9"
- "Avviso per Storage firmware Bundle 2.146"
- "Avviso per Compute firmware Bundle 2.146"
- "Avviso per Storage firmware Bundle 2.99.2"
- "Avviso per Compute firmware Bundle 2.76"
- "Avviso per Storage firmware Bundle 2.76"
- "Avviso per Compute firmware Bundle 2.27"
- "Avviso per Storage firmware Bundle 2.27"

- "Avviso per l'ISO del firmware di calcolo"
- "Avviso per H610S BMC"
- "Avviso per i servizi di gestione 2.24.40 (plug-in NetApp Element per VMware vCenter Server 5,2.12)"
- "Avviso per i servizi di gestione 2.23.64 (plug-in NetApp Element per VMware vCenter Server 5.1.12)"
- "Avviso per i servizi di gestione 2.22.7 (plug-in NetApp Element per vCenter Server 5.0.37)"
- "Avviso per i servizi di gestione 2.21.61 (plug-in NetApp Element per vCenter Server 4.10.12)"
- "Avviso per i servizi di gestione 2.20.69 (plug-in NetApp Element per vCenter Server 4.9.14)"
- "Avviso per i servizi di gestione 2.19.48 (plug-in NetApp Element per vCenter Server 4.8.34)"
- "Avviso per i servizi di gestione 2.18.91 (plug-in NetApp Element per vCenter Server 4.7.10)"
- "Avviso per i servizi di gestione 2.17.56 (plug-in NetApp Element per vCenter Server 4.6.32)"
- "Avviso per i servizi di gestione 2.17.52 (plug-in NetApp Element per vCenter Server 4.6.29)"
- "Avviso per i servizi di gestione 2.16 (plug-in NetApp Element per vCenter Server 4.6.29)"
- "Avviso per i servizi di gestione 2.14 (plug-in NetApp Element per vCenter Server 4.5.42)"
- "Avviso per i servizi di gestione 2.13 (plug-in NetApp Element per vCenter Server 4.5.42)"
- "Avviso per i servizi di gestione 2.11 (plug-in NetApp Element per vCenter Server 4.4.72)"
- "Avviso per NetApp HCI 1.8"