Managen Sie NetApp HCI

HCI

NetApp
October 23, 2024

Inhalt

Managen Sie NetApp HCI

NetApp HCI Management-Überblick

Sie können den vollständig qualifizierten Domänennamen konfigurieren und Anmeldedaten für NetApp HCI, Benutzerkonten, Storage-Cluster, Volumes, Volume Access Groups managen. Initiatoren, Volume QoS-Richtlinien und der Management-Node

Hier sind die Punkte, mit denen Sie arbeiten können:

- "Konfigurieren Sie vollständig qualifizierten Domänennamen Web UI-Zugriff"
- "Ändern Sie die Anmeldedaten in NetApp HCI"
- "Aktualisieren der vCenter- und ESXi-Anmeldedaten"
- "Management von NetApp HCI Storage Assets"
- "Arbeiten Sie mit dem Management-Node"
- "Schaltet das NetApp HCI System aus oder ein"

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"

Konfigurieren Sie vollständig qualifizierten Domänennamen Web UI-Zugriff

Mit NetApp HCI mit Element Software 12.2 oder höher können Sie unter Verwendung des vollständig qualifizierten Domänennamens (FQDN) auf Webschnittstellen des Speicherclusters zugreifen. Wenn Sie den FQDN für den Zugriff auf Webbenutzerschnittstellen wie die Element-Web-UI, die Benutzeroberfläche per Node oder die Management-Node-Benutzeroberfläche verwenden möchten, müssen Sie zuerst eine Speichercluster-Einstellung hinzufügen, um den vom Cluster verwendeten FQDN zu identifizieren.

Sie können jetzt über den vollständig qualifizierten Domänennamen (FQDN) auf Webschnittstellen des Speicherclusters zugreifen. Wenn Sie den FQDN für den Zugriff auf Webbenutzerschnittstellen wie die Element-Web-UI, die Benutzeroberfläche per Node oder die Management-Node-Benutzeroberfläche verwenden möchten, müssen Sie zuerst eine Speichercluster-Einstellung hinzufügen, um den vom Cluster verwendeten FQDN zu identifizieren. Auf diese Weise kann der Cluster eine Anmeldesitzung ordnungsgemäß umleiten und die Integration in externe Services wie Schlüsselmanager und Identitätsanbieter für die Multi-Faktor-Authentifizierung verbessern.

Was Sie benötigen

- Diese Funktion erfordert Element 12.2 oder höher.
- Für die Konfiguration dieser Funktion mit NetApp Hybrid Cloud Control REST-APIs sind Management-Services 2.15 oder höher erforderlich.

- Für die Konfiguration dieser Funktion mit der NetApp Hybrid Cloud Control UI sind Management-Services ab 2.19 erforderlich.
- Zur Verwendung VON REST-APIs müssen Sie einen Management-Node mit Version 11.5 oder höher bereitgestellt haben.
- Sie benötigen vollqualifizierte Domain-Namen für den Management-Node und jeden Storage-Cluster, die korrekt zur Management Node-IP-Adresse und den einzelnen Storage-Cluster-IP-Adressen auflösen.

Über NetApp Hybrid Cloud Control und DIE REST-API können Sie den FQDN-Webbenutzerzugriff konfigurieren oder entfernen. Sie können auch Fehler bei falsch konfigurierten FQDNs beheben.

- Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control
- Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API
- Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control
- Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API
- Fehlerbehebung

Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie das Menüsymbol oben rechts auf der Seite aus.
4. Wählen Sie **Konfigurieren**.
5. Wählen Sie im Fenster **vollqualifizierte Domänennamen** die Option **Einrichtung** aus.
6. Geben Sie im daraufhin angezeigten Fenster die FQDNs für den Managementknoten und jeden Speichercluster ein.
7. Wählen Sie **Speichern**.

   Im Fensterbereich **Fully Qualified Domain Names** werden alle Speichercluster mit dem zugehörigen MVIP und FQDN aufgelistet.

   Nur verbundene Speichercluster mit dem FQDN-Satz werden im Fensterbereich **vollqualifizierte Domänennamen** aufgeführt.

Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API

Schritte

1. Stellen Sie sicher, dass die Element-Speicherknoten und der Managementknoten für die Netzwerkumgebung richtig DNS konfiguriert haben, damit FQDNs in der Umgebung aufgelöst werden können. Um DNS einzustellen, wechseln Sie zur Benutzeroberfläche für Speicherknoten pro Knoten und zum Managementknoten und wählen Sie dann **Netzwerkeinstellungen** > **Managementnetzwerk** aus.

a. UI pro Node für Storage-Nodes: `https://<storage_node_management_IP>:442`

b. UI pro Node für den Management-Node: `https://<management_node_IP>:442`

2. Ändern Sie die Storage-Cluster-Einstellungen mithilfe der Element API.

   a. Greifen Sie auf die Element API zu, und erstellen Sie mithilfe der die folgende Clusterschnittstelle `CreateClusterInterfacePreference` API-Methode, und fügen Sie den Cluster MVIP FQDN für den Vorzugswert ein:

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

        Hier ist beispielsweise der FQDN `storagecluster.my.org`:

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

3. Ändern Sie die Management-Node-Einstellungen mit der REST-API auf dem Management-Node:

   a. Rufen Sie die REST-API-UI für den Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/2/`. Beispiel:

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

   b. Wählen Sie **authorize** oder ein Schloss-Symbol aus und geben Sie den Benutzernamen und das Kennwort des Element Clusters ein.

   c. Geben Sie die Client-ID als ein `mnode-client`.

   d. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

   e. Schließen Sie das Fenster.

   f. Wählen Sie **GET /settings**.

   g. Wählen Sie **Probieren Sie es aus**.

   h. Wählen Sie **Ausführen**.

   i. Beachten Sie, ob der Proxy wie in angegeben verwendet wird `"use_proxy"` Von `true` Oder `false`.

   j. Wählen Sie **PUT /settings**.

   k. Wählen Sie **Probieren Sie es aus**.

   l. Geben Sie im Bereich Text anfordern den Management-Node FQDN als Wert für das ein `mnode_fqdn` Parameter. Geben Sie außerdem an, ob der Proxy verwendet werden soll (`true` Oder `false` Aus dem vorherigen Schritt) für das `use_proxy` Parameter.

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

m. Wählen Sie **Ausführen**.

Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control

Mit diesem Verfahren können Sie den FQDN-Webzugriff für den Managementknoten und die Speichercluster entfernen.

Schritte

1. Wählen Sie im Fenster **vollqualifizierte Domänennamen** die Option **Bearbeiten** aus.
2. Löschen Sie im resultierenden Fenster den Inhalt im Textfeld **FQDN**.
3. Wählen Sie **Speichern**.

   Das Fenster wird geschlossen, und der FQDN wird nicht mehr im Bereich **Fully Qualified Domain Names** aufgeführt.

Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API

Schritte

1. Ändern Sie die Storage-Cluster-Einstellungen mithilfe der Element API.

   a. Greifen Sie auf die Element API zu und löschen Sie mithilfe der die folgende Clusterschnittstelle `DeleteClusterInterfacePreference` API-Methode:

      - Name: `mvip_fqdn`

        Beispiel:

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

2. Ändern Sie die Management-Node-Einstellungen mit der REST-API auf dem Management-Node:

   a. Rufen Sie die REST-API-UI für den Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/2/`. Beispiel:

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

   b. Wählen Sie **authorize** oder ein Schloss-Symbol aus und geben Sie den Benutzernamen und das Kennwort des Element Clusters ein.

   c. Geben Sie die Client-ID als ein `mnode-client`.

   d. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

e. Schließen Sie das Fenster.

f. Wählen Sie **PUT /settings**.

g. Wählen Sie **Probieren Sie es aus**.

h. Geben Sie im Bereich des Anforderungskörpers keinen Wert für das ein `mnode_fqdn` Parameter. Geben Sie außerdem an, ob der Proxy verwendet werden soll (`true` Oder `false`) Für die `use_proxy` Parameter.

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

i. Wählen Sie **Ausführen**.

Fehlerbehebung

Wenn FQDNs falsch konfiguriert sind, können Sie Probleme beim Zugriff auf den Managementknoten, einen Speichercluster oder beide haben. Verwenden Sie die folgenden Informationen, um die Fehlerbehebung zu unterstützen.

Problem	Ursache	Auflösung
• Beim Versuch, entweder mit dem FQDN auf den Management-Node oder den Speicher-Cluster zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse nicht entweder beim Management-Node oder beim Storage-Cluster einloggen.	Der FQDN des Managementknoten und der FQDN des Speicherclusters sind beide falsch konfiguriert.	Verwenden Sie die REST-API-Anweisungen auf dieser Seite, um die FQDN-Einstellungen des Management-Nodes und Speicherclusters zu entfernen und erneut zu konfigurieren.
• Beim Versuch, auf den Speicher-Cluster-FQDN zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse nicht entweder beim Management-Node oder beim Storage-Cluster einloggen.	Der FQDN des Managementknoten ist richtig konfiguriert, der Speichercluster-FQDN ist jedoch falsch konfiguriert.	Mithilfe der REST-API-Anweisungen auf dieser Seite können Sie die FQDN-Einstellungen des Speicherclusters entfernen und erneut konfigurieren.

Problem	Ursache	Auflösung
• Beim Versuch, auf den Verwaltungsknoten FQDN zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse beim Management-Node und Storage-Cluster einloggen.	Der FQDN des Managementknoten ist falsch konfiguriert, der Speichercluster-FQDN ist jedoch korrekt konfiguriert.	Melden Sie sich bei NetApp Hybrid Cloud Control an, um die FQDN-Einstellungen des Managementknoten in der UI zu korrigieren, oder VERWENDEN Sie die REST-API-Anweisungen auf dieser Seite, um die Einstellungen zu korrigieren.

Weitere Informationen

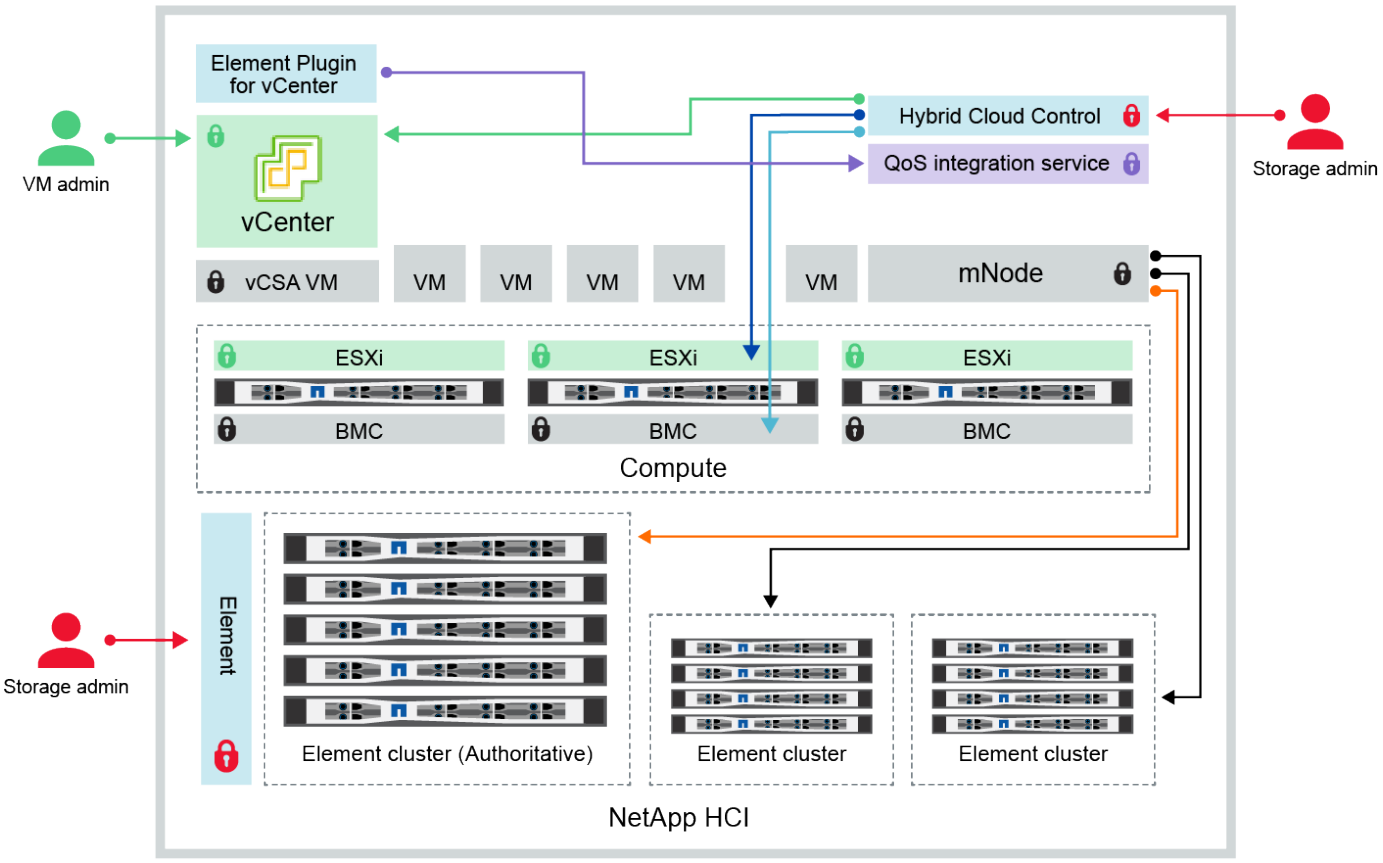
- "CreateClusterSchnittstellenPreference-API-Informationen in der SolidFire- und Element-Dokumentation"
- "Ressourcen-Seite zu NetApp HCI"
- "Dokumentation von SolidFire und Element Software"

Anmeldedaten in NetApp HCI und NetApp SolidFire ändern

Abhängig von den Sicherheitsrichtlinien im Unternehmen, die NetApp HCI oder NetApp SolidFire implementiert haben, gehört das Ändern von Anmeldedaten oder Passwörtern in der Regel zu den Sicherheitspraktiken. Bevor Sie Passwörter ändern, sollten Sie sich der Auswirkungen auf andere Softwarekomponenten in der Bereitstellung bewusst sein.

Wenn Sie die Anmeldedaten für eine Komponente einer NetApp HCI- oder NetApp SolidFire-Implementierung ändern, enthält die folgende Tabelle Anweisungen zu den Auswirkungen auf andere Komponenten.

Interaktionen von NetApp HCI-Komponenten:



- **Hybrid Cloud Control and administrator use VMware vSphere Single Sign-on credentials to log into vCenter**
- **Hybrid Cloud Control uses per-node 'root' account to communicate with VMware ESXi**
- **Hybrid Cloud Control uses per-node BMC credentials to communicate with BMC on compute nodes**
- **Element Plugin for VMware vCenter uses password to communicate with QoS service on mNode**
- **Administrator uses administrative Element storage credentials to log into Element UI and Hybrid Cloud Control**
- **mNode and services use Element certificates to communicate with authoritative storage cluster**
- **mNode and services use Element administrative credentials for additional storage clusters**

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Anmeldedaten für Element 	**Gilt für**: NetApp HCI und SolidFire Administratoren verwenden diese Anmeldedaten zur Anmeldung bei: • Element Benutzeroberfläche auf dem Element Storage-Cluster • Hybrid Cloud Control auf dem Management-Node (mNode) Wenn Hybrid Cloud Control mehrere Storage-Cluster managt, akzeptiert es nur die Admin-Anmeldeinformationen für die Storage-Cluster, bekannt als das *autorisierende Cluster*, für das der mNode ursprünglich eingerichtet wurde. Bei Storage-Clustern, die später zu Hybrid Cloud Control hinzugefügt werden, speichert der mNode die Anmeldedaten des Administrators sicher. Wenn Anmeldeinformationen für nachträglich hinzugefügte Speicher-Cluster geändert werden, müssen die Anmeldeinformationen auch im mnode mit der mNode-API aktualisiert werden.	• "Aktualisieren der Passwörter für den Storage-Cluster-Administrator". • Aktualisieren Sie die Anmeldedaten des Storage-Cluster-Administrators im mNode mithilfe des "Modifizierter clusteradmin API".
VSphere Single Sign On – Zugangsdaten 	**Gilt nur für**: NetApp HCI Administratoren verwenden diese Zugangsdaten, um sich beim VMware vSphere Client anzumelden. Wenn vCenter Teil der Installation von NetApp HCI ist, werden in der NetApp Deployment Engine die folgenden Anmeldedaten konfiguriert: • username@vsphere.local mit dem angegebenen Passwort, und • administrator@vsphere.local mit dem angegebenen Passwort. Wenn ein vorhandenes vCenter für die Implementierung von NetApp HCI verwendet wird, werden die Anmeldeinformationen für vSphere Single Sign-On von DEN IT-VMware-Administratoren gemanagt.	"Aktualisieren der vCenter- und ESXi-Anmeldedaten".

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Baseboard Management Controller (BMC) Zugangsdaten 	**Gilt nur für**: NetApp HCI Administratoren melden sich mithilfe dieser Anmeldedaten beim BMC der NetApp Computing-Nodes in einer NetApp HCI-Implementierung an. Das BMC bietet grundlegende Hardware-Überwachung und Funktionen der virtuellen Konsole. BMC-Anmeldeinformationen (auch als „*IPMI*“ bezeichnet) für jeden NetApp Computing-Node werden in NetApp HCI-Implementierungen sicher auf dem mNode gespeichert. NetApp Hybrid Cloud Control verwendet BMC-Anmeldeinformationen in einem Service-Konto, um während eines Upgrades der Computing-Node-Firmware mit dem BMC in den Computing-Nodes zu kommunizieren. Wenn die BMC-Anmeldedaten geändert werden, müssen auch die Anmeldeinformationen für die jeweiligen Computing-Nodes auf dem mnode aktualisiert werden, damit alle Hybrid Cloud Control-Funktionen erhalten bleiben.	• "Konfigurieren Sie IPMI für jeden Node in NetApp HCI". • Für H410C, H610C und H615C Nodes "Ändern Sie das Standard-IPMI-Passwort". • Für H410S und H610S Nodes "Ändern Sie das IPM-Standardpasswort". • "Ändern Sie BMC-Anmeldeinformationen auf dem Management-Node".
ESXi Anmeldedaten 	**Gilt nur für**: NetApp HCI Administratoren können sich über SSH oder die lokale DCUI mit einem lokalen Root-Konto bei ESXi Hosts anmelden. In NetApp HCI-Implementierungen ist der Benutzername „root“, und das Passwort wurde bei der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. ESXi Root-Anmeldedaten für jeden NetApp Computing-Node werden in NetApp HCI-Implementierungen sicher auf dem mnode gespeichert. NetApp Hybrid Cloud Control verwendet die Zugangsdaten in der Kapazität eines Service-Kontos, um direkt während Upgrades der Firmware des Computing-Nodes und Zustandsprüfungen mit ESXi Hosts zu kommunizieren. Wenn die ESXi-Root-Anmeldedaten von einem VMware-Administrator geändert werden, müssen die Anmeldeinformationen für die jeweiligen Computing-Nodes auf dem mnode aktualisiert werden, damit die Hybrid Cloud Control-Funktionalität erhalten bleibt.	"Anmeldedaten für vCenter- und ESXi-Hosts aktualisieren".

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Passwort für die QoS-Integration 	**Gilt für**: NetApp HCI und optional in SolidFire Nicht für interaktive Anmeldungen durch Administratoren verwendet. Die QoS-Integration zwischen VMware vSphere und Element Software wird durch folgende aktiviert: • Element Plug-in für vCenter Server und • QoS-Service auf dem mNode. Für die Authentifizierung verwendet der QoS-Service ein Passwort, das ausschließlich in diesem Zusammenhang verwendet wird. Das QoS-Passwort wird bei der Erstinstallation des Element Plug-in für vCenter Server angegeben oder während der NetApp HCI-Implementierung automatisch generiert. Keine Auswirkung auf andere Komponenten.	"Aktualisieren Sie die QoSSIOC-Anmeldeinformationen im NetApp Element-Plug-in für vCenter Server". Das SIOC-Passwort des NetApp Element-Plug-ins für vCenter-Server wird auch als *QoSSIOC-Passwort* bezeichnet. Lesen Sie den Element Plug-in for vCenter Server KB Artikel.
Anmeldedaten für vCenter Service Appliance 	**Gilt für**: NetApp HCI nur bei Einrichtung über die NetApp Deployment Engine Administratoren können sich bei den virtuellen Maschinen der vCenter Server Appliance anmelden. In NetApp HCI-Implementierungen ist der Benutzername „root“, und das Passwort wurde bei der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. Je nach der bereitgestellten VMware vSphere Version können sich auch bestimmte Administratoren in der vSphere Single Sign-On-Domäne bei der Appliance anmelden. Keine Auswirkung auf andere Komponenten.	Es sind keine Änderungen erforderlich.
Anmeldedaten für NetApp Management-Node-Admin 	**Gilt für**: NetApp HCI und optional in SolidFire Zur erweiterten Konfiguration und Fehlerbehebung können sich Administratoren bei Virtual Machines des NetApp Management Node anmelden. Je nach implementierter Management-Node-Version ist die Anmeldung über SSH nicht standardmäßig aktiviert. In NetApp HCI-Implementierungen wurden Benutzername und Passwort vom Benutzer während der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. Keine Auswirkung auf andere Komponenten.	Es sind keine Änderungen erforderlich.

Weitere Informationen

- "Ändern Sie das Standard-SSL-Zertifikat der Element Software"
- "Ändern Sie das IPMI-Passwort für Knoten"
- "Multi-Faktor-Authentifizierung aktivieren"
- "Erste Schritte mit externem Verschlüsselungsmanagement"
- "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt"

Aktualisieren der vCenter- und ESXi-Anmeldedaten

Wenn Sie Ihre Anmeldedaten in vCenter- und ESXi-Hosts ändern, müssen Sie die vollständigen Funktionen von NetApp Hybrid Cloud Control für Ihre NetApp HCI-Installation beibehalten. Auch müssen Sie diese Anmeldedaten im Asset-Service auf dem Management-Node aktualisieren.

Über diese Aufgabe

NetApp Hybrid Cloud Control kommuniziert mit vCenter und den einzelnen Computing-Nodes mit VMware vSphere ESXi, um Informationen zum Dashboard abzurufen und Rolling Upgrades von Firmware, Software und Treibern zu vereinfachen. NetApp Hybrid Cloud Control und seine zugehörigen Services auf dem Management-Node authentifizieren sich mit Anmeldeinformationen (Benutzername/Passwort) gegen VMware vCenter und ESXi.

Wenn die Kommunikation zwischen diesen Komponenten fehlschlägt, zeigen NetApp Hybrid Cloud Control und vCenter bei einem Authentifizierungsprobleme Fehlermeldungen an. Bei NetApp Hybrid Cloud Control wird ein rotes Fehlerbanner angezeigt, wenn es nicht mit der zugehörigen VMware vCenter Instanz in der NetApp HCI Installation kommunizieren kann. VMware vCenter zeigt ESXi Kontosperrmeldungen für einzelne ESXi Hosts dank NetApp Hybrid Cloud Control mit veralteten Zugangsdaten an.

Der Management-Node in NetApp HCI bezeichnet diese Komponenten mit den folgenden Namen:

- „Controller Assets“ sind vCenter Instanzen, die Ihrer NetApp HCI Installation zugeordnet sind.
- „Compute-Node-Ressourcen“ sind die ESXi-Hosts in Ihrer NetApp HCI Installation.

Bei der Erstinstallation von NetApp HCI mit der NetApp Deployment Engine speicherte der Management-Node die Anmeldeinformationen für den administrativen Benutzer, den Sie für vCenter angegeben haben, und das „Root“-Account-Passwort auf ESXi Servern.

Aktualisieren Sie das vCenter Passwort mithilfe der REST-API des Management-Node

Führen Sie die Schritte aus, um die Controller-Assets zu aktualisieren. Siehe "Vorhandene Controller-Assets können angezeigt oder bearbeitet werden".

Aktualisieren Sie das ESXi-Passwort mithilfe der REST-API des Management-Node

Schritte

1. Eine Übersicht über DIE REST-API-Benutzeroberfläche der Management-Node finden Sie im "Übersicht über DIE REST-API-Benutzeroberfläche der Management-Node".
2. Greifen Sie auf die REST-API-UI für Managementservices auf dem Management-Node zu:

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

Ersetzen Sie <Management-Node-IP> durch die IPv4-Adresse des Management-Node im für NetApp HCI verwendeten Managementnetzwerk.

3. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den NetApp SolidFire Cluster-Administrator ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
4. Klicken Sie in DER REST API-Benutzeroberfläche auf **GET /Assets/Compute_Nodes**.

   Hierdurch werden die Datensätze von Computing-Node-Assets abgerufen, die im Management-Node gespeichert werden.

   Hier ist der direkte Link zu dieser API in der UI:

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

5. Klicken Sie auf **Probieren Sie es aus**.
6. Klicken Sie Auf **Ausführen**.
7. Ermitteln Sie im Antwortkörper die Datensätze der Computing-Node-Assets, die aktualisierte Anmeldedaten benötigen. Sie können die Eigenschaften „ip“ und „Host_Name“ verwenden, um die richtigen ESXi-Host-Datensätze zu finden.

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

   Im nächsten Schritt werden die Felder „Parent“ und „id“ im Datensatz „Compute Asset Record“ verwendet, um auf den zu aktualisienden Datensatz Bezug zu nehmen.

8. Konfiguration der spezifischen Computing-Node-Ressource:
   a. Klicken Sie auf **PUT /Assets/{Asset_id}/Compute-Nodes/{Compute_id}**.

      Hier ist der direkte Link zur API in der UI:

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

a. Klicken Sie auf **Probieren Sie es aus**.

b. Geben Sie die „Asset_id“ mit den „übergeordneten“ Informationen ein.

c. Geben Sie die „Compute_id“ mit der „id“-Information ein.

d. Ändern Sie den Anfraentext in der Benutzeroberfläche, um nur die Kennwortparameter und die Parameter für den Benutzernamen im Datensatz für die Rechnungsanteile zu aktualisieren:

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

e. Klicken Sie Auf **Ausführen**.

f. Überprüfen Sie, ob es sich bei der Antwort um HTTP 200 handelt, was bedeutet, dass die neuen Anmeldeinformationen im Datensatz der referenzierten Rechnungs-Anlage gespeichert wurden

9. Wiederholen Sie die vorherigen beiden Schritte für zusätzliche Computing-Node-Ressourcen, die mit einem neuen Passwort aktualisiert werden müssen.
10. Navigieren Sie zu https://<mNode_ip>/inventory/1/.

a. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:

i. Geben Sie den Benutzernamen und das Passwort für den NetApp SolidFire Cluster-Administrator ein.

ii. Geben Sie die Client-ID als ein `mnode-client`.

iii. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.

iv. Schließen Sie das Fenster.

b. Klicken Sie in DER REST API UI auf **GET /Installations**.

c. Klicken Sie auf **Probieren Sie es aus**.

d. Wählen Sie in der Dropdown-Liste Beschreibung aktualisieren die Option **true** aus.

e. Klicken Sie Auf **Ausführen**.

f. Überprüfen Sie, ob die Antwort HTTP 200 ist.

11. Warten Sie ca. 15 Minuten, bis die Meldung Kontosperrung in vCenter verschwindet.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Managen Sie NetApp HCI Storage

Management von NetApp HCI Storage – Überblick

Mit NetApp HCI lassen sich diese Storage-Ressourcen mithilfe von NetApp Hybrid Cloud Control managen.

- "Benutzerkonten erstellen und verwalten"
- "Hinzufügen und Managen von Storage-Clustern"
- "Erstellung und Management von Volumes"
- "Erstellung und Management von Volume-Zugriffsgruppen"
- "Erstellen und Verwalten von Initiatoren"
- "Erstellung und Management von QoS-Richtlinien für Volumes"

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Erstellen und managen Sie Benutzerkonten mit NetApp Hybrid Cloud Control

In Element-basierten Storage-Systemen können maßgebliche Cluster-Benutzer erstellt werden, um Login-Zugriff auf NetApp Hybrid Cloud Control zu ermöglichen. Dies hängt von den Berechtigungen ab, die Sie „Administrator“ oder „schreibgeschützten“ Benutzern gewähren möchten. Neben Cluster-Benutzern gibt es auch Volume-Konten, über die Clients eine Verbindung zu Volumes auf einem Storage-Node herstellen können.

Verwalten Sie die folgenden Kontoarten:

- Managen von autorisierenden Cluster-Konten
- Volume-Konten verwalten

Aktivieren Sie LDAP

Um LDAP für jedes Benutzerkonto verwenden zu können, müssen Sie zunächst LDAP aktivieren.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Klicken Sie im Dashboard auf das Symbol Optionen oben rechts und wählen Sie **Benutzerverwaltung**.
3. Klicken Sie auf der Seite Benutzer auf **LDAP konfigurieren**.
4. Definieren Sie Ihre LDAP-Konfiguration.
5. Wählen Sie den Authentifizierungstyp Suchen und Bind oder Direct Bind aus.
6. Bevor Sie die Änderungen speichern, klicken Sie oben auf der Seite auf **LDAP-Anmeldung testen**, geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, den Sie kennen, und klicken Sie auf **Test**.

7. Klicken Sie Auf **Speichern**.

Managen von autorisierenden Cluster-Konten

"Autoritäre Benutzerkonten" Werden bei NetApp Hybrid Cloud Control über die Option „Benutzerverwaltung“ rechts oben gemanagt. Mithilfe dieser Kontoarten können Sie sich gegen alle Storage-Ressourcen authentifizieren, die mit einer NetApp Hybrid Cloud Control Instanz von Nodes und Clustern verbunden sind. Mit diesem Konto können Sie Volumes, Konten, Zugriffsgruppen und mehr über alle Cluster hinweg verwalten.

Erstellen Sie ein autorisierende Cluster-Konto

Erstellen Sie ein Konto mit NetApp Hybrid Cloud Control.

Mithilfe dieses Kontos können Kunden sich bei der Hybrid Cloud Control, der UI pro Node für das Cluster und dem Storage-Cluster in der NetApp Element Software anmelden.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Klicken Sie im Dashboard auf das Symbol Optionen oben rechts und wählen Sie **Benutzerverwaltung**.
3. Wählen Sie **Benutzer Erstellen**.
4. Wählen Sie den Authentifizierungstyp von Cluster oder LDAP aus.
5. Führen Sie eine der folgenden Aktionen durch:
   - Wenn Sie LDAP ausgewählt haben, geben Sie den DN ein.

     Um LDAP zu verwenden, müssen Sie zunächst LDAP oder LDAPS aktivieren. Siehe Aktivieren Sie LDAP.

   - Wenn Sie Cluster als Auth-Typ ausgewählt haben, geben Sie einen Namen und ein Passwort für das neue Konto ein.
6. Wählen Sie entweder Administrator- oder schreibgeschützten Berechtigungen aus.

   Klicken Sie zum Anzeigen der Berechtigungen aus der NetApp Element-Software auf **ältere Berechtigungen anzeigen**. Wenn Sie eine Untergruppe dieser Berechtigungen auswählen, wird dem Konto Schreibberechtigung zugewiesen. Wenn Sie alle älteren Berechtigungen auswählen, wird dem Konto Administratorberechtigungen zugewiesen.

   Um sicherzustellen, dass alle untergeordneten Gruppen Berechtigungen erben, erstellen Sie im LDAP-Server eine DN-Organisationsadministratorgruppe. Alle untergeordneten Konten dieser Gruppe übernehmen diese Berechtigungen.

7. Aktivieren Sie das Kontrollkästchen unter „Ich habe die NetApp Endbenutzer-Lizenzvereinbarung gelesen und akzeptiere sie“.
8. Klicken Sie Auf **Benutzer Erstellen**.

Bearbeiten Sie ein autorisierende Cluster-Konto

Mit NetApp Hybrid Cloud Control können Sie die Berechtigungen oder das Passwort eines Benutzerkontos ändern.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Klicken Sie im Dashboard oben rechts auf das Symbol und wählen Sie **Benutzerverwaltung**.
3. Filtern Sie die Liste der Benutzerkonten optional durch Auswahl von **Cluster**, **LDAP** oder **IDP**.

   Wenn Sie Benutzer im Storage-Cluster mit LDAP konfiguriert haben, wird für diese Konten ein Benutzertyp mit „LDAP“ angezeigt. Wenn Benutzer auf dem Storage-Cluster mit IDP konfiguriert wurden, zeigen diese Konten einen Benutzertyp mit „IDP“.

4. Erweitern Sie in der Spalte **Aktionen** in der Tabelle das Menü für das Konto und wählen Sie **Bearbeiten**.
5. Nehmen Sie die erforderlichen Änderungen vor.
6. Wählen Sie **Speichern**.
7. Abmelden von NetApp Hybrid Cloud Control
8. "Aktualisieren Sie die Anmeldedaten" Die maßgebliche Cluster-Ressource, die die NetApp Hybrid Cloud Control API verwendet, ist die Lösung.

   > Die Benutzeroberfläche von NetApp Hybrid Cloud Control dauert möglicherweise bis zu 2 Minuten, um den Bestand zu aktualisieren. Um den Bestand manuell zu aktualisieren, greifen Sie auf den Rest API UI Inventory Service zu `https://<ManagementNodeIP>/inventory/1/` Und ausführen `GET /installations/{id}` Für den Cluster.

9. Melden Sie sich bei NetApp Hybrid Cloud Control an.

Löschen eines autorisierenden Benutzerkontos

Sie können ein oder mehrere Konten löschen, wenn sie nicht mehr benötigt werden. Sie können ein LDAP-Benutzerkonto löschen.

Sie können das primäre Administratorbenutzerkonto für das autorisierende Cluster nicht löschen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Klicken Sie im Dashboard oben rechts auf das Symbol und wählen Sie **Benutzerverwaltung**.
3. Erweitern Sie in der Spalte **Aktionen** in der Benutzertabelle das Menü für das Konto und wählen Sie **Löschen**.
4. Bestätigen Sie den Löschvorgang, indem Sie **Ja** wählen.

Volume-Konten verwalten

"Volume-Konten" Werden in der Tabelle NetApp Hybrid Cloud Control Volumes gemanagt. Diese Konten gelten nur für den Storage Cluster, auf dem sie erstellt wurden. Mit diesen Typen von Konten können Sie Berechtigungen für Volumes im gesamten Netzwerk festlegen, haben aber keine Auswirkungen außerhalb dieser Volumes.

Ein Volume-Konto enthält die CHAP-Authentifizierung, die für den Zugriff auf die ihm zugewiesenen Volumes erforderlich ist.

Erstellen eines Volume-Kontos

Erstellen Sie ein für dieses Volume spezifisches Konto.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Wählen Sie im Dashboard **Storage** > **Volumes** aus.
3. Wählen Sie die Registerkarte **Konten**.
4. Klicken Sie auf die Schaltfläche **Konto erstellen**.
5. Geben Sie einen Namen für das neue Konto ein.
6. Geben Sie im Abschnitt CHAP-Einstellungen die folgenden Informationen ein:
   - Initiatorschlüssel für CHAP-Node-Session-Authentifizierung
   - Zielschlüssel für CHAP-Knoten-Session-Authentifizierung

   Um ein Kennwort automatisch zu generieren, lassen Sie die Felder für Anmeldedaten leer.
7. Wählen Sie **Konto Erstellen**.

Bearbeiten eines Volume-Kontos

Sie können die CHAP-Informationen ändern und ändern, ob ein Konto aktiv oder gesperrt ist.

Das Löschen oder Sperren eines Kontos im Zusammenhang mit dem Managementknoten führt zu einem nicht zugänglichen Managementknoten.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Wählen Sie im Dashboard **Storage** > **Volumes** aus.
3. Wählen Sie die Registerkarte **Konten**.
4. Erweitern Sie in der Spalte **Aktionen** in der Tabelle das Menü für das Konto und wählen Sie **Bearbeiten**.
5. Nehmen Sie die erforderlichen Änderungen vor.
6. Bestätigen Sie die Änderungen, indem Sie **Ja** wählen.

Löschen Sie ein Volume-Konto

Löschen Sie ein Konto, das Sie nicht mehr benötigen.

Bevor Sie ein Volume-Konto löschen, löschen Sie zunächst alle Volumes, die dem Konto zugeordnet sind.

Das Löschen oder Sperren eines Kontos im Zusammenhang mit dem Managementknoten führt zu einem nicht zugänglichen Managementknoten.

Persistente Volumes, die mit Managementservices verbunden sind, werden einem neuen Konto bei der Installation oder bei einem Upgrade zugewiesen. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie die Volumes oder ihr zugehörigem Konto nicht. Wenn Sie diese Konten löschen, können Sie den Management-Node nicht mehr verwenden.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Wählen Sie im Dashboard **Storage** > **Volumes** aus.
3. Wählen Sie die Registerkarte **Konten**.
4. Erweitern Sie in der Spalte **Aktionen** in der Tabelle das Menü für das Konto und wählen Sie **Löschen**.
5. Bestätigen Sie den Löschvorgang, indem Sie **Ja** wählen.

Weitere Informationen

- "Informationen zu Accounts"
- "Arbeiten Sie mit Benutzerkonten"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Fügen Sie Storage-Cluster mit NetApp Hybrid Cloud Control hinzu und managen Sie sie

Sie können Storage-Cluster zur Bestandsaufnahme der Management-Node-Ressourcen hinzufügen, sodass sie mittels NetApp Hybrid Cloud Control (HCC) gemanagt werden können. Der erste während der Systemeinrichtung hinzugefügte Storage Cluster ist der Standard "Autorisierende Storage-Cluster", Aber zusätzliche Cluster können mit HCC UI hinzugefügt werden.

Nach dem Hinzufügen eines Speicher-Clusters können Sie die Cluster-Performance überwachen, die Anmeldeinformationen für das Storage-Cluster für die verwaltete Ressource ändern oder ein Storage-Cluster aus der Asset-Bestandsaufnahme des Management-Nodes entfernen, wenn dieses nicht mehr mit HCC verwaltet werden muss.

Ab Element 12.2 können Sie den verwenden "Wartungsmodus" Funktionsoptionen zum Aktivieren und Deaktivieren des Wartungsmodus für Ihre Storage-Cluster-Nodes

Was Sie benötigen

- **Clusteradministrator-Berechtigungen**: Sie haben Berechtigungen als Administrator auf dem "Autorisierende Storage-Cluster". Das autoritäre Cluster ist das erste Cluster, das während der Systemeinrichtung zur Inventarisierung der Managementknoten hinzugefügt wird.
- **Element Software**: Die NetApp Element Software 11.3 oder höher wird in Ihrer Speichercluster-Version ausgeführt.
- **Management-Node**: Sie haben einen Management-Node mit Version 11.3 oder höher bereitgestellt.
- **Management Services**: Sie haben Ihr Management Services Bundle auf Version 2.17 oder höher aktualisiert.

Optionen

- Fügen Sie einen Storage-Cluster hinzu
- Bestätigen des Storage-Cluster-Status
- Bearbeiten der Anmeldedaten für das Storage-Cluster
- Entfernen eines Storage-Clusters
- Aktivieren und deaktivieren Sie den Wartungsmodus

Fügen Sie einen Storage-Cluster hinzu

Mit NetApp Hybrid Cloud Control können Sie dem Inventory der Management-Node-Ressourcen ein Storage-Cluster hinzufügen. Auf diese Weise können Sie den Cluster mithilfe der HCC-Benutzeroberfläche verwalten und überwachen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an und stellen Sie die autorisierenden Anmeldedaten des Storage-Cluster-Administrators bereit.
2. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
3. Wählen Sie im Fensterbereich **Storage Cluster Storage Cluster Details** aus.
4. Wählen Sie **Storage-Cluster Hinzufügen**.
5. Geben Sie die folgenden Informationen ein:
   - Virtuelle IP-Adresse für das Storage-Cluster-Management

     Es können nur Remote-Storage-Cluster hinzugefügt werden, die derzeit nicht von einem Management-Node gemanagt werden.

   - Benutzername und Passwort für den Storage Cluster
6. Wählen Sie **Hinzufügen**.

   Nachdem Sie das Storage-Cluster hinzugefügt haben, kann der Cluster-Bestand bis zu 2 Minuten dauern, bis die neue Ergänzung angezeigt wird. Möglicherweise müssen Sie die Seite in Ihrem Browser aktualisieren, um die Änderungen anzuzeigen.

7. Wenn Sie Element ESDS-Cluster hinzufügen, geben Sie Ihren SSH-privaten Schlüssel und das SSH-Benutzerkonto ein oder laden Sie es hoch.

Bestätigen des Storage-Cluster-Status

Über die Benutzeroberfläche von NetApp Hybrid Cloud Control können Sie den Verbindungsstatus von Storage-Cluster-Ressourcen überwachen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an und stellen Sie die autorisierenden Anmeldedaten des Storage-Cluster-Administrators bereit.
2. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
3. Überprüfen Sie den Status von Speicherclustern im Inventar.
4. Wählen Sie im Fensterbereich **Storage Cluster Storage Cluster Details** für weitere Details.

Bearbeiten der Anmeldedaten für das Storage-Cluster

Der Benutzername und das Passwort des Storage-Clusters können Sie über die Benutzeroberfläche von NetApp Hybrid Cloud Control bearbeiten.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an und stellen Sie die autorisierenden Anmeldedaten des Storage-Cluster-Administrators bereit.
2. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
3. Wählen Sie im Fensterbereich **Storage Cluster Storage Cluster Details** aus.
4. Wählen Sie für den Cluster das Menü **Aktionen** aus und wählen Sie **Cluster-Anmeldeinformationen bearbeiten**.
5. Aktualisieren Sie den Benutzernamen und das Passwort des Storage-Clusters.
6. Wählen Sie **Speichern**.

Entfernen eines Storage-Clusters

Durch Entfernen eines Storage-Clusters aus NetApp Hybrid Cloud Control wird das Cluster aus der Inventar des Management-Node entfernt. Nachdem Sie ein Storage-Cluster entfernt haben, kann der Cluster nicht mehr von HCC gemanagt werden. Sie können ihn nur aufrufen, indem Sie direkt zur Management-IP-Adresse navigieren.

Sie können das autorisierende Cluster nicht aus dem Bestand entfernen. Um den autorisierenden Cluster zu ermitteln, gehen Sie zu **Benutzerverwaltung > Benutzer**. Der autoritative Cluster wird neben der Überschrift **Benutzer** aufgelistet.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an und stellen Sie die autorisierenden Anmeldedaten des Storage-Cluster-Administrators bereit.
2. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
3. Wählen Sie im Fensterbereich **Storage Cluster Storage Cluster Details** aus.
4. Wählen Sie für den Cluster das Menü **Aktionen** aus und wählen Sie **Storage Cluster entfernen**.

   Durch Klicken auf **Ja** wird der Cluster aus der Installation entfernt.

5. Wählen Sie **Ja**.

Aktivieren und deaktivieren Sie den Wartungsmodus

Das "Wartungsmodus" Optionen bieten die Möglichkeit Aktivieren Und Deaktivieren Wartungsmodus für einen Storage-Cluster-Node.

Was Sie benötigen

- **Element Software**: Die NetApp Element Software 12.2 oder höher wird in Ihrer Speichercluster-Version ausgeführt.
- **Management-Node**: Sie haben einen Management-Node mit Version 12.2 oder höher bereitgestellt.
- **Management Services**: Sie haben Ihr Management Services Bundle auf Version 2.19 oder höher aktualisiert.

- Sie haben Zugriff auf die Anmeldung auf Administratorebene.

Wartungsmodus aktivieren

Sie können das folgende Verfahren verwenden, um den Wartungsmodus für einen Storage-Cluster-Node zu aktivieren.

Es kann sich nur ein Node gleichzeitig im Wartungsmodus befinden.

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser. Beispiel:

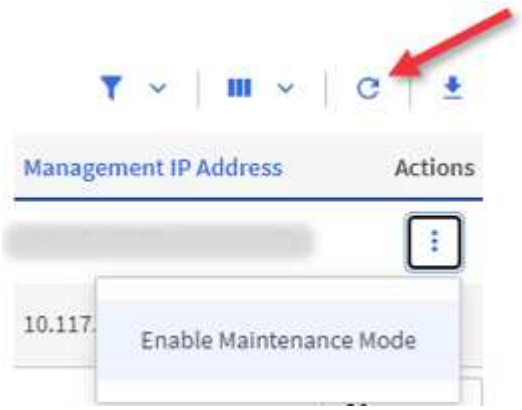
```
https://<ManagementNodeIP>
```

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des NetApp HCI-Storage-Cluster-Administrators bereitstellen.

   Die Funktionsoptionen für den Wartungsmodus sind auf der schreibgeschützten Ebene deaktiviert.

3. Wählen Sie im blauen Feld links die NetApp HCI-Installation aus.
4. Wählen Sie im linken Navigationsbereich **Knoten** aus.
5. Um Informationen zum Speicherbestand anzuzeigen, wählen Sie **Speicherung**.
6. Aktivieren des Wartungsmodus auf einem Storage-Node:

   Die Tabelle der Storage-Nodes wird automatisch alle zwei Minuten für Aktionen aktualisiert, die nicht von Benutzern initiiert wurden. Um sicherzustellen, dass Sie über den aktuellen Status verfügen, können Sie die Knoten-Tabelle aktualisieren, indem Sie das Aktualisierungssymbol oben rechts in der Knotentabelle verwenden.

   a. Wählen Sie unter **Actions** die Option **Wartungsmodus aktivieren** aus.

      Während **Wartungsmodus** aktiviert wird, sind Aktionen im Wartungsmodus für den ausgewählten Knoten und alle anderen Knoten im selben Cluster nicht verfügbar.

Nachdem **Aktivieren des Wartungsmodus** abgeschlossen ist, wird in der Spalte **Knotenstatus** ein Schraubenschlüsselsymbol und der Text „**Wartungsmodus**“ für den Knoten angezeigt, der sich im

Wartungsmodus befindet.

Wartungsmodus deaktivieren

Nachdem ein Knoten erfolgreich in den Wartungsmodus versetzt wurde, steht für diesen Knoten die Aktion **Wartungsmodus deaktivieren** zur Verfügung. Aktionen auf den anderen Nodes sind erst verfügbar, wenn der Wartungsmodus auf dem Node, der gerade gewartet wird, erfolgreich deaktiviert wurde.

Schritte

1. Wählen Sie für den Knoten im Wartungsmodus unter **Aktionen** die Option **Wartungsmodus deaktivieren** aus.

   Während **Wartungsmodus** deaktiviert wird, sind Aktionen im Wartungsmodus für den ausgewählten Knoten und alle anderen Knoten im selben Cluster nicht verfügbar.

   Nachdem **Wartungsmodus deaktivieren** abgeschlossen ist, wird in der Spalte **Knotenstatus aktiv** angezeigt.

   > Wenn sich ein Node im Wartungsmodus befindet, werden keine neuen Daten akzeptiert. Daher kann das Deaktivieren des Wartungsmodus länger dauern, da der Node die Daten wieder synchronisieren muss, bevor er den Wartungsmodus beenden kann. Je länger Sie im Wartungsmodus verbringen, desto länger kann es zum Deaktivieren des Wartungsmodus dauern.

Fehlerbehebung

Falls beim Aktivieren oder Deaktivieren des Wartungsmodus Fehler auftreten, wird oben in der Node-Tabelle ein Banner-Fehler angezeigt. Für weitere Informationen über den Fehler können Sie den auf dem Banner bereitgestellten Link **Details anzeigen** wählen, um zu zeigen, was die API zurückgibt.

Weitere Informationen

- "Erstellen und Managen von Storage-Cluster-Assets"
- "Seite „NetApp HCI Ressourcen“"

Erstellen und managen Sie Volumes mit NetApp Hybrid Cloud Control

Sie können ein Volume erstellen und das Volume einem bestimmten Konto zuordnen. Durch die Verknüpfung eines Volumes mit einem Konto erhält das Konto über die iSCSI-Initiatoren und CHAP-Anmeldeinformationen Zugriff auf das Volume.

Sie können die QoS-Einstellungen für ein Volume während der Erstellung festlegen.

Folgende Möglichkeiten zum Managen von Volumes in NetApp Hybrid Cloud Control:

- Erstellen eines Volumes
- Wenden Sie eine QoS-Richtlinie auf ein Volume an
- Bearbeiten Sie ein Volume
- Volumes klonen
- Hinzufügen von Volumes zu einer Volume-Zugriffsgruppe

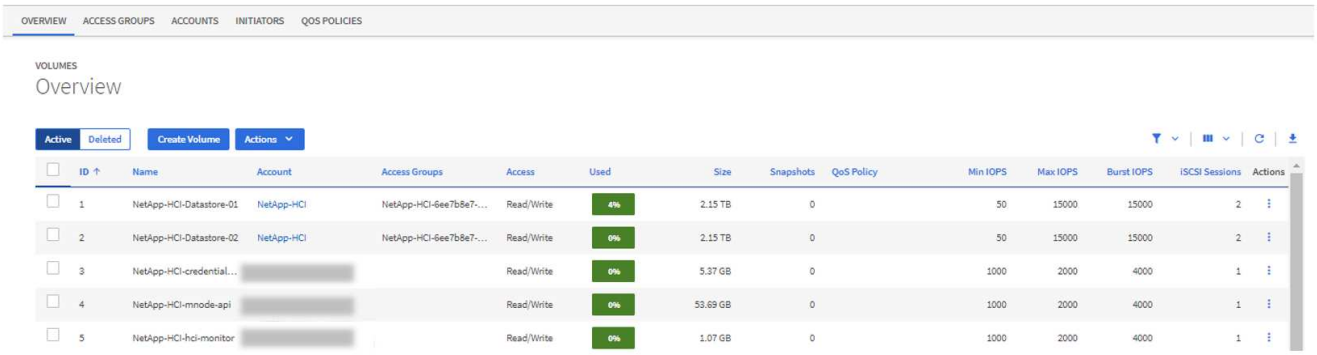
- Löschen Sie ein Volume
- Wiederherstellen eines gelöschten Volumes
- Löschen Sie ein gelöschtes Volume

Erstellen eines Volumes

Mit NetApp Hybrid Cloud Control können Sie ein Storage-Volume erstellen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie die Registerkarte **Bände** > **Übersicht**.



4. Wählen Sie **Lautstärke Erstellen**.
5. Geben Sie einen Namen für das neue Volume ein.
6. Geben Sie die Gesamtgröße des Volumes ein.

> Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mit Größen erstellen, die in GB oder gib gemessen wurden: 1 GB = 1 000 000 000 Byte 1 gib = 1 073 741 824 Byte

7. Wählen Sie eine Blockgröße für das Volume aus.
8. Wählen Sie aus der Liste **Konto** das Konto aus, das Zugriff auf das Volume haben soll.

   Wenn kein Konto vorhanden ist, klicken Sie auf **Neues Konto erstellen**, geben Sie einen neuen Kontonamen ein und klicken Sie auf **Konto erstellen**. Das Konto wird erstellt und mit dem neuen Volumen in der **Konto** Liste verknüpft.

> Wenn mehr als 50 Konten vorhanden sind, wird die Liste nicht angezeigt. Beginnen Sie mit der Eingabe, und die automatische Vervollständigung zeigt Werte an, die Sie auswählen können.

9. Um die Servicequalität für das Volume zu konfigurieren, führen Sie einen der folgenden Schritte aus:
   - Legen Sie unter **Quality of Service Settings** benutzerdefinierte Mindest-, Maximum- und Burst-Werte für IOPS fest oder verwenden Sie die Standard-QoS-Werte.
   - Wählen Sie eine vorhandene QoS-Richtlinie aus, indem Sie die Option **Quality of Service Policy**

zuweisen aktivieren und eine vorhandene QoS-Richtlinie aus der Ergebnisliste auswählen.

- Erstellen und Zuweisen einer neuen QoS-Richtlinie durch Aktivieren der Option **Quality of Service Policy** zuweisen und Klicken auf **Neue QoS-Richtlinie erstellen**. Geben Sie im daraufhin angezeigten Fenster einen Namen für die QoS-Richtlinie ein, und geben Sie anschließend QoS-Werte ein. Klicken Sie anschließend auf **Quality of Service Policy**.

Volumes mit einem IOPS-Wert von max oder Burst über 20,000 IOPS erfordern möglicherweise eine hohe Warteschlangentiefe oder mehrere Sitzungen, um diesen IOPS-Level auf einem einzelnen Volume zu erreichen.

10. Klicken Sie Auf **Volume Erstellen**.

Wenden Sie eine QoS-Richtlinie auf ein Volume an

Mithilfe von NetApp Hybrid Cloud Control können Sie eine QoS-Richtlinie auf vorhandene Storage-Volumes anwenden. Wenn Sie stattdessen benutzerdefinierte QoS-Werte für ein Volume festlegen müssen, ist dies möglich Bearbeiten Sie ein Volume. Informationen zum Erstellen einer neuen QoS-Richtlinie finden Sie unter "Erstellung und Management von QoS-Richtlinien für Volumes".

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie ein oder mehrere Volumes aus, die einer QoS-Richtlinie zugeordnet werden sollen.
5. Klicken Sie oben in der Tabelle Volumes auf die Dropdown-Liste **Aktionen** und wählen Sie **QoS-Richtlinie anwenden**.
6. Wählen Sie im resultierenden Fenster eine QoS-Richtlinie aus der Liste aus und klicken Sie auf **QoS-Richtlinie anwenden**.

> Wenn Sie QoS-Richtlinien für ein Volume verwenden, können Sie durch benutzerdefinierte QoS festlegen, dass die QoS-Richtlinie, die mit dem Volume verbunden ist, entfernt wird. Benutzerdefinierte QoS-Werte überschreiben QoS-Richtlinienwerte für Volume-QoS-Einstellungen.

Bearbeiten Sie ein Volume

Mit NetApp Hybrid Cloud Control lassen sich Volume-Attribute wie QoS-Werte, Volume-Größe und die Maßeinheit bearbeiten, mit der Byte-Werte berechnet werden. Außerdem haben Sie die Möglichkeit, den Kontozugriff für die Replizierungsnutzung zu ändern oder den Zugriff auf das Volume zu beschränken.

Über diese Aufgabe

Sie können die Größe eines Volume ändern, wenn unter den folgenden Bedingungen genügend Speicherplatz auf dem Cluster vorhanden ist:

- Normale Betriebsbedingungen.
- Volume-Fehler oder -Ausfälle werden gemeldet.
- Das Volume ist zu klonen.
- Das Volume wird neu synchronisiert.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Erweitern Sie in der Spalte **Aktionen** in der Tabelle Volumes das Menü für die Lautstärke und wählen Sie **Bearbeiten**.
5. Nehmen Sie die Änderungen nach Bedarf vor:

   a. Ändern Sie die Gesamtgröße des Volumes.

   Sie können die Volume-Größe vergrößern, aber nicht verkleinern. Sie können die Größe eines Volumes nur in einem einzigen Größenänderungs-Vorgang anpassen. Speicherbereinigung und Software-Upgrades unterbrechen die Größenänderung nicht.

   Wenn Sie die Volume-Größe für die Replikation anpassen, erhöhen Sie zuerst die Größe des Volumes, das als Replikationsziel zugewiesen wurde. Anschließend können Sie die Größe des Quellvolumens anpassen. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

   Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mit Größen erstellen, die in GB oder gib gemessen wurden: 1 GB = 1 000 000 000 Byte 1 gib = 1 073 741 824 Byte

   b. Wählen Sie eine andere Zugriffsebene für Konten aus:

   - Schreibgeschützt
   - Lese-/Schreibzugriff
   - Gesperrt
   - Replizierungsziel

   c. Wählen Sie das Konto aus, das Zugriff auf das Volume haben soll.

   Beginnen Sie mit der Eingabe, und die automatische Vervollständigung zeigt mögliche Werte an, die Sie auswählen können.

   Wenn kein Konto vorhanden ist, klicken Sie auf **Neues Konto erstellen**, geben Sie einen neuen Kontonamen ein und klicken Sie auf **Erstellen**. Der Account wird erstellt und dem vorhandenen Volume zugeordnet.

   d. Ändern Sie die Servicequalität mit einer der folgenden Aktionen:

   i. Wählen Sie eine vorhandene Richtlinie aus.

   ii. Legen Sie unter „Benutzerdefinierte Einstellungen“ die Mindest-, Höchst- und Burst-Werte für IOPS fest oder verwenden Sie die Standardwerte.

   Wenn Sie QoS-Richtlinien für ein Volume verwenden, können Sie durch benutzerdefinierte QoS festlegen, dass die QoS-Richtlinie, die mit dem Volume verbunden ist, entfernt wird. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen außer Kraft gesetzt.

Wenn Sie IOPS-Werte ändern, sollten Sie sich Dutzende oder Hunderte erhöhen. Eingabewerte erfordern gültige ganze Zahlen. Konfigurieren Sie Volumes mit einem extrem hohen Burst-Wert. So kann das System gelegentlich umfangreiche sequenzielle Workloads von großen Blöcken schneller verarbeiten und zugleich die anhaltenden IOPS für ein Volume einschränken.

6. Wählen Sie **Speichern**.

Volumes klonen

Sie können einen Klon eines einzelnen Storage Volumes erstellen oder eine Gruppe von Volumes klonen, um eine zeitpunktgenaue Kopie der Daten zu erstellen. Wenn Sie ein Volume klonen, erstellt das System einen Snapshot des Volume und erstellt dann eine Kopie der Daten, auf die der Snapshot verweist.

Bevor Sie beginnen

- Mindestens ein Cluster muss hinzugefügt und ausgeführt werden.
- Mindestens ein Volume wurde erstellt.
- Ein Benutzerkonto wurde erstellt.
- Der verfügbare nicht bereitgestellte Speicherplatz muss der Volume-Größe entsprechen oder größer sein.

Über diese Aufgabe

Das Cluster unterstützt bis zu zwei aktuell laufende Klonanforderungen pro Volume und bis zu 8 aktive Volume-Klonvorgänge gleichzeitig. Anforderungen, die über diese Grenzen hinausgehen, werden zur späteren Verarbeitung in die Warteschlange gestellt.

Das Klonen von Volumes ist ein asynchroner Prozess. Die erforderliche Zeit hängt von der Größe des Klonens des Volumes und der aktuellen Cluster-Last ab.

Geklonte Volumes übernehmen keine Zugriffsgruppenmitgliedschaft für Volumes vom Quell-Volume.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie die Registerkarte **Volumes** > **Übersicht** aus.
4. Wählen Sie jedes Volume aus, das Sie klonen möchten.
5. Klicken Sie oben in der Tabelle Volumes auf die Dropdown-Liste **Aktionen** und wählen Sie **Klonen**.
6. Gehen Sie im daraufhin angezeigten Fenster wie folgt vor:

    a. Geben Sie ein Präfix für den Volume-Namen ein (optional).

    b. Wählen Sie den Zugriffstyp aus der Liste **Zugriff** aus.

    c. Wählen Sie ein Konto aus, das dem neuen Volume-Klon zugeordnet werden soll (standardmäßig ist **aus Volume kopieren** ausgewählt, das dasselbe Konto verwendet, das das ursprüngliche Volume verwendet).

    d. Wenn kein Konto vorhanden ist, klicken Sie auf **Neues Konto erstellen**, geben Sie einen neuen Kontonamen ein und klicken Sie auf **Konto erstellen**. Der Account wird erstellt und dem Volume zugeordnet.

Verwenden Sie beschreibende Best Practices für die Benennung. Dies ist besonders wichtig, wenn in Ihrer Umgebung mehrere Cluster oder vCenter Server verwendet werden.

Wenn Sie die Volume-Größe eines Klons erhöhen, führt dies zu einem neuen Volume mit zusätzlichem freien Speicherplatz am Ende des Volumes. Je nachdem, wie Sie das Volume verwenden, müssen Sie möglicherweise Partitionen erweitern oder neue Partitionen im freien Speicherplatz erstellen, um es zu nutzen.

a. Klicken Sie Auf **Volumes Klonen**.

Der Zeitaufwand zum Abschluss eines Klonvorgangs wird von der Volume-Größe und der aktuellen Cluster-Last beeinflusst. Aktualisieren Sie die Seite, wenn das geklonte Volume nicht in der Liste der Volumes angezeigt wird.

Hinzufügen von Volumes zu einer Volume-Zugriffsgruppe

Sie können einer Volume-Zugriffsgruppe ein einzelnes Volume oder eine Gruppe von Volumes hinzufügen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie ein oder mehrere Volumes aus, die einer Volume-Zugriffsgruppe zugeordnet werden sollen.
5. Klicken Sie oben in der Tabelle Volumes auf die Dropdown-Liste **Aktionen** und wählen Sie **zur Zugriffsgruppe hinzufügen**.
6. Wählen Sie im resultierenden Fenster eine Zugriffsgruppe für Volumes aus der Liste **Volume Access Group** aus.
7. Klicken Sie Auf **Volumen Hinzufügen**.

Löschen Sie ein Volume

Ein oder mehrere Volumes können aus einem Element Storage-Cluster gelöscht werden.

Über diese Aufgabe

Gelöschte Volumes werden nicht sofort vom System gelöscht, sie bleiben etwa acht Stunden lang verfügbar. Nach acht Stunden werden sie gereinigt und sind nicht mehr verfügbar. Wenn Sie ein Volume wiederherstellen, bevor das System es bereinigt, wird das Volume wieder online geschaltet und die iSCSI-Verbindungen werden wiederhergestellt.

Wenn ein Volume, das zum Erstellen eines Snapshots verwendet wird, gelöscht wird, werden die zugehörigen Snapshots inaktiv. Wenn die gelöschten Quell-Volumes gelöscht werden, werden auch die zugehörigen inaktiven Snapshots aus dem System entfernt.

Persistente Volumes, die mit Managementservices verbunden sind, werden bei der Installation oder bei einem Upgrade einem neuen Konto erstellt und zugewiesen. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie die Volumes oder ihr zugehörigem Konto nicht. Wenn Sie diese Volumes löschen, kann der Management-Node nicht mehr verwendet werden.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie ein oder mehrere zu löschende Volumes aus.
5. Klicken Sie oben in der Tabelle Volumes auf die Dropdown-Liste **Aktionen** und wählen Sie **Löschen**.
6. Bestätigen Sie im daraufhin angezeigten Fenster die Aktion, indem Sie auf **Ja** klicken.

Wiederherstellen eines gelöschten Volumes

Nach dem Löschen eines Storage Volume können Sie ihn weiterhin wiederherstellen, falls dies vor acht Stunden nach dem Löschen erfolgt.

Gelöschte Volumes werden nicht sofort vom System gelöscht, sie bleiben etwa acht Stunden lang verfügbar. Nach acht Stunden werden sie gereinigt und sind nicht mehr verfügbar. Wenn Sie ein Volume wiederherstellen, bevor das System es bereinigt, wird das Volume wieder online geschaltet und die iSCSI-Verbindungen werden wiederhergestellt.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie **Gelöscht**.
5. Erweitern Sie in der Spalte **Aktionen** der Tabelle Volumes das Menü für die Lautstärke und wählen Sie **Wiederherstellen**.
6. Bestätigen Sie den Vorgang, indem Sie **Ja** wählen.

Löschen Sie ein gelöschtes Volume

Nach dem Löschen von Storage Volumes bleiben diese für ungefähr acht Stunden verfügbar. Nach acht Stunden werden sie automatisch gereinigt und sind nicht mehr verfügbar. Wenn Sie die acht Stunden nicht warten möchten, können Sie sie löschen

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände** > **Übersicht**.
4. Wählen Sie **Gelöscht**.
5. Wählen Sie ein oder mehrere Volumes aus, die gelöscht werden sollen.
6. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie mehrere Volumen ausgewählt haben, klicken Sie oben in der Tabelle auf den Schnellfilter **Löschen**.
   - Wenn Sie ein einzelnes Volume ausgewählt haben, erweitern Sie in der Spalte **Aktionen** der

Volumetabelle das Menü für die Lautstärke und wählen Sie **Löschen**.

7. Erweitern Sie in der Spalte **Aktionen** der Tabelle Volumes das Menü für die Lautstärke und wählen Sie **Löschen**.
8. Bestätigen Sie den Vorgang, indem Sie **Ja** wählen.

Weitere Informationen

- "Informationen zu Volumes"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Erstellung und Management von Volume-Zugriffsgruppen

Sie können neue Volume-Zugriffsgruppen erstellen, den Namen, zugehörige Initiatoren oder zugehörige Volumes von Zugriffsgruppen ändern oder vorhandene Volume-Zugriffsgruppen mithilfe von NetApp Hybrid Cloud Control löschen.

Was Sie benötigen

- Sie haben Administratoranmeldedaten für dieses NetApp HCI-System.
- Sie haben Ihre Managementservices auf mindestens Version 2.15.28 aktualisiert. Das NetApp Hybrid Cloud Control Storage-Management ist in früheren Service-Bundle-Versionen nicht verfügbar.
- Stellen Sie sicher, dass Sie über ein logisches Benennungsschema für Volume-Zugriffsgruppen verfügen.

Fügen Sie eine Zugriffsgruppe für Volumes hinzu

Mit NetApp Hybrid Cloud Control können Sie einem Storage-Cluster eine Volume-Zugriffsgruppe hinzufügen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Zugriffsgruppen** aus.
5. Klicken Sie auf die Schaltfläche **Zugriffsgruppe erstellen**.
6. Geben Sie im daraufhin angezeigten Dialogfeld einen Namen für die Zugriffsgruppe des neuen Volumes ein.
7. (Optional) Wählen Sie im Abschnitt **Initiatoren** einen oder mehrere Initiatoren aus, die der neuen Zugriffsgruppe zugeordnet werden sollen.

   Wenn Sie einen Initiator der Volume-Zugriffsgruppe zuordnen, kann dieser Initiator ohne Authentifizierung auf jedes Volume in der Gruppe zugreifen.

8. (Optional) Wählen Sie im Abschnitt **Volumes** ein oder mehrere Volumes aus, die in diese Zugriffsgruppe aufgenommen werden sollen.
9. Wählen Sie **Zugriffsgruppe Erstellen**.

Bearbeiten Sie eine Zugriffsgruppe für Volumes

Sie können die Eigenschaften einer vorhandenen Volume-Zugriffsgruppe mit NetApp Hybrid Cloud Control bearbeiten. Sie können den Namen, zugeordnete Initiatoren oder zugehörige Volumes einer Zugriffsgruppe ändern.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Zugriffsgruppen** aus.
5. Erweitern Sie in der Spalte **Aktionen** der Tabelle der Zugriffsgruppen das Optionsmenü für die Zugriffsgruppe, die Sie bearbeiten müssen.
6. Wählen Sie im Optionsmenü die Option **Bearbeiten**.
7. Nehmen Sie alle erforderlichen Änderungen am Namen, den zugehörigen Initiatoren oder den zugehörigen Volumes vor.
8. Bestätigen Sie Ihre Änderungen, indem Sie **Speichern** wählen.
9. Überprüfen Sie in der Tabelle **Access Groups**, ob die Zugriffsgruppe Ihre Änderungen widerspiegelt.

Löschen Sie eine Zugriffsgruppe für Volumes

Sie können eine Volume-Zugriffsgruppe mithilfe von NetApp Hybrid Cloud Control entfernen und gleichzeitig die mit dieser Zugriffsgruppe verknüpften Initiatoren aus dem System entfernen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Zugriffsgruppen** aus.
5. Erweitern Sie in der Spalte **Aktionen** der Zugriffstabelle das Optionsmenü für die zu löschende Zugriffsgruppe.
6. Wählen Sie im Optionsmenü die Option **Löschen** aus.
7. Wenn Sie die Initiatoren, die der Zugriffsgruppe zugeordnet sind, nicht löschen möchten, deaktivieren Sie das Kontrollkästchen **Initiatoren löschen in dieser Zugriffsgruppe**.
8. Bestätigen Sie den Löschvorgang, indem Sie **Ja** auswählen.

Weitere Informationen

- "Erfahren Sie mehr über Volume Access Groups"
- "Hinzufügen eines Initiators zu einer Volume-Zugriffsgruppe"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Erstellen und Verwalten von Initiatoren

Verwenden Sie können "Initiatoren" Für CHAP-basierten und nicht kontenbasierten Zugriff auf Volumes. Sie können Initiatoren erstellen und löschen und ihnen freundliche Alias geben, um die Administration und den Zugriff auf Volumes zu vereinfachen. Wenn Sie einer Volume-Zugriffsgruppe einen Initiator hinzufügen, ermöglicht dieser Initiator den Zugriff auf alle Volumes in der Gruppe.

Was Sie benötigen

- Sie haben Cluster-Administrator-Anmeldedaten.
- Sie haben Ihre Managementservices auf mindestens Version 2.17 aktualisiert. Das NetApp Hybrid Cloud Control Initiator-Management ist in früheren Service-Bundle-Versionen nicht verfügbar.

Optionen

- Erstellen eines Initiators
- Fügen Sie Initiatoren zu einer Volume-Zugriffsgruppe hinzu
- Ändern eines Initiator-Alias
- Löschen Sie Initiatoren

Erstellen eines Initiators

Sie können iSCSI- oder Fibre Channel-Initiatoren erstellen und diese optional Aliase zuweisen.

Über diese Aufgabe

Das akzeptierte Format eines Initiator-IQN lautet `iqn.yyyy-mm` Wobei y und m Ziffern sind, gefolgt von Text, der nur Ziffern, Kleinbuchstaben, einen Punkt enthalten darf (`.`), Doppelpunkt (`:`) Oder Strich (`-`). Ein Beispiel für das Format:

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

Das akzeptierte Format eines Fibre Channel Initiator-WWPN `:Aa:bB:CC:dd:11:22:33:44` Oder `AabBCCdd11223344`. Ein Beispiel für das Format:

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

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Initiatoren** aus.
5. Wählen Sie die Schaltfläche **Initiatoren erstellen**.

Option	Schritte
Erstellen Sie einen oder mehrere Initiatoren	a. Geben Sie im Feld **IQN/WWPN** den IQN oder WWPN für den Initiator ein. b. Geben Sie im Feld **Alias** einen Anzeigenamen für den Initiator ein. c. (Optional) Wählen Sie **Initiator hinzufügen**, um neue Initiatorfelder zu öffnen, oder verwenden Sie stattdessen die Option Bulk create. d. Wählen Sie **Initiatoren Erstellen** Aus.
Initiatoren für Massenvorgänge erstellen	a. Wählen Sie **Bulk Add IQNs/WWPNs** aus. b. Geben Sie eine Liste von IQNs oder WWPNs in das Textfeld ein. Jeder IQN oder WWPN muss Komma oder Speicherplatz getrennt oder in seiner eigenen Zeile sein. c. Wählen Sie **IQNs/WWPNs hinzufügen**. d. (Optional) Fügen Sie jedem Initiator eindeutige Aliase hinzu. e. Entfernen Sie jeden Initiator aus der Liste, der in der Installation möglicherweise bereits vorhanden ist. f. Wählen Sie **Initiatoren Erstellen** Aus.

Fügen Sie Initiatoren zu einer Volume-Zugriffsgruppe hinzu

Sie können Initiatoren zu einer Volume-Zugriffsgruppe hinzufügen. Wenn Sie einer Volume-Zugriffsgruppe einen Initiator hinzufügen, ermöglicht der Initiator den Zugriff auf alle Volumes in dieser Volume-Zugriffsgruppe.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Initiatoren** aus.
5. Wählen Sie einen oder mehrere Initiatoren aus, die Sie hinzufügen möchten.
6. Wählen Sie **Aktionen > zur Zugriffsgruppe hinzufügen**.
7. Wählen Sie die Zugriffsgruppe aus.
8. Bestätigen Sie Ihre Änderungen, indem Sie **Initiator hinzufügen** wählen.

Ändern eines Initiator-Alias

Sie können den Alias eines bestehenden Initiators ändern oder einen Alias hinzufügen, wenn einer noch nicht vorhanden ist.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Initiatoren** aus.
5. Erweitern Sie in der Spalte **Aktionen** das Optionsmenü für den Initiator.
6. Wählen Sie **Bearbeiten**.
7. Nehmen Sie alle erforderlichen Änderungen am Alias vor oder fügen Sie einen neuen Alias hinzu.
8. Wählen Sie **Speichern**.

Löschen Sie Initiatoren

Sie können einen oder mehrere Initiatoren löschen. Wenn Sie einen Initiator löschen, wird dieser vom System aus einer zugehörigen Volume-Zugriffsgruppe entfernt. Verbindungen, die den Initiator verwenden, bleiben gültig, bis die Verbindung zurückgesetzt wird.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
2. Erweitern Sie im Dashboard im linken Navigationsmenü den Namen Ihres Storage-Clusters.
3. Wählen Sie **Bände**.
4. Wählen Sie die Registerkarte **Initiatoren** aus.
5. Einen oder mehrere Initiatoren löschen:
   a. Wählen Sie einen oder mehrere Initiatoren aus, die Sie löschen möchten.
   b. Wählen Sie **Aktionen > Löschen**.
   c. Bestätigen Sie den Löschvorgang und wählen Sie **Ja**.

Weitere Informationen

- "Weitere Informationen zu Initiatoren"
- "Erfahren Sie mehr über Volume Access Groups"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Erstellung und Management von QoS-Richtlinien für Volumes

Mit einer QoS-Richtlinie (Quality of Service) können Sie eine standardisierte Quality-of-Service-Einstellung erstellen und speichern, die auf viele Volumes angewendet werden kann. Der ausgewählte Cluster muss zur Verwendung von QoS-Richtlinien Element 10.0 oder höher sein. Anderenfalls sind QoS-Richtlinienfunktionen nicht verfügbar.

Weitere Informationen zur Verwendung finden Sie unter NetApp HCI Concepts "QoS-Richtlinien (QoS" Anstelle einzelner Volumes "QoS".

Mithilfe von NetApp Hybrid Cloud Control lassen sich QoS-Richtlinien erstellen und managen, indem folgende Aufgaben ausgeführt werden:

- Erstellen einer QoS-Richtlinie
- Wenden Sie eine QoS-Richtlinie auf ein Volume an
- Ändern der QoS-Richtlinienzuweisung eines Volumes
- Bearbeiten einer QoS-Richtlinie
- Löschen einer QoS-Richtlinie

Erstellen einer QoS-Richtlinie

Sie können QoS-Richtlinien erstellen und auf Volumes anwenden, die eine vergleichbare Performance aufweisen sollten.

Wenn Sie QoS-Richtlinien verwenden, verwenden Sie keine benutzerdefinierte QoS für ein Volume. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen überschrieben und angepasst.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Klicken Sie auf die Registerkarte **QoS Policies**.
5. Klicken Sie Auf **Create Policy**.
6. Geben Sie den **Policy Name** ein.

   Verwenden Sie beschreibende Best Practices für die Benennung. Dies ist besonders wichtig, wenn in Ihrer Umgebung mehrere Cluster oder vCenter Server verwendet werden.

7. Geben Sie die Werte für IOPS-Minimum, IOPS-Maximum und IOPS-Burst ein.
8. Klicken Sie auf **QoS-Richtlinie erstellen**.

   Für die Richtlinie wird eine System-ID generiert, und die Richtlinie wird auf der Seite QoS Policies mit ihren zugewiesenen QoS-Werten angezeigt.

Wenden Sie eine QoS-Richtlinie auf ein Volume an

Mithilfe von NetApp Hybrid Cloud Control kann einer vorhandenen QoS-Richtlinie ein Volume zugewiesen werden.

Was Sie benötigen

Die QoS-Richtlinie, die Sie zuweisen möchten, war Erstellt.

Über diese Aufgabe

Dieser Task beschreibt, wie eine QoS-Richtlinie einem einzelnen Volume durch Ändern der entsprechenden Einstellungen zugewiesen wird. Die neueste Version von NetApp Hybrid Cloud Control bietet keine Massenzuordnungsoption für mehr als ein Volume. Bis die Funktion für die Massen-Zuweisung in einer

zukünftigen Version verfügbar ist, können Sie QoS-Richtlinien über die Element Web-UI oder das vCenter Plug-in in Bulk zuweisen.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Klicken Sie auf das Menü **Aktionen** neben dem Volumen, den Sie ändern möchten.
5. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
6. Aktivieren Sie im Dialogfeld **QoS-Richtlinie zuweisen** und wählen Sie die QoS-Richtlinie aus der Dropdown-Liste aus, die auf das ausgewählte Volume angewendet werden soll.

   Durch die Zuweisung von QoS werden alle zuvor angewandten QoS-Werte für Volumes außer Kraft gesetzt.

7. Klicken Sie Auf **Speichern**.

   Das aktualisierte Volume mit der zugewiesenen QoS-Richtlinie wird auf der Übersichtsseite angezeigt.

Ändern der QoS-Richtlinienzuweisung eines Volumes

Sie können die Zuweisung einer QoS-Richtlinie aus einem Volume entfernen oder eine andere QoS-Richtlinie oder benutzerdefinierte QoS auswählen.

Was Sie benötigen

Das Volume, das Sie ändern möchten, ist Zugewiesen Eine QoS-Richtlinie

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Klicken Sie auf das Menü **Aktionen** neben dem Volumen, den Sie ändern möchten.
5. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
6. Führen Sie im Dialogfeld einen der folgenden Schritte aus:
   - Deaktivieren Sie **Assign QoS Policy** und ändern Sie die **Min IOPS**, **Max IOPS** und **Burst IOPS**-Werte für die QoS einzelner Volumes.

     Wenn QoS-Richtlinien deaktiviert sind, verwendet das Volume Standard-QoS-IOPS-Werte, sofern nichts anderes geändert wurde.

   - Wählen Sie in der Dropdown-Liste eine andere QoS-Richtlinie aus, die auf das ausgewählte Volume angewendet werden soll.
7. Klicken Sie Auf **Speichern**.

   Das aktualisierte Volume wird auf der Seite Übersicht angezeigt.

Bearbeiten einer QoS-Richtlinie

Sie können den Namen einer vorhandenen QoS-Richtlinie ändern oder die mit der Richtlinie verknüpften Werte bearbeiten. Das Ändern von Performance-Werten für die QoS-Richtlinie wirkt sich auf die QoS aller mit der Richtlinie verknüpften Volumes aus.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Klicken Sie auf die Registerkarte **QoS Policies**.
5. Klicken Sie auf das Menü **Aktionen** neben der QoS-Richtlinie, die Sie ändern möchten.
6. Klicken Sie Auf **Bearbeiten**.
7. Ändern Sie im Dialogfeld **QoS-Richtlinie bearbeiten** einen oder mehrere der folgenden Optionen:
   - **Name**: Der benutzerdefinierte Name für die QoS-Richtlinie.
   - **Minimum IOPS**: Die Mindestzahl an IOPS für das Volume garantiert. Standard = 50.
   - **Maximale IOPS**: Die maximale Anzahl von IOPS für das Volume zulässig. Standard = 15,000.
   - **Burst IOPS**: Die maximale Anzahl an IOPS über einen kurzen Zeitraum für das Volume zulässig. Standard = 15,000.
8. Klicken Sie Auf **Speichern**.

   Die aktualisierte QoS-Richtlinie wird auf der Seite QoS-Richtlinien angezeigt.

Klicken Sie auf den Link in der Spalte **aktive Volumes**, um eine Richtlinie anzuzeigen, in der eine gefilterte Liste der Volumes angezeigt wird, die dieser Richtlinie zugeordnet sind.

Löschen einer QoS-Richtlinie

Die QoS-Richtlinie kann gelöscht werden, wenn sie nicht mehr benötigt wird. Wenn Sie eine QoS-Richtlinie löschen, erhalten alle mit der Richtlinie zugewiesenen Volumes die QoS-Werte, die zuvor von der Richtlinie definiert wurden, jedoch als individuelle Volume-QoS. Jede Zuordnung zur Richtlinie „Gelöschte QoS“ wird entfernt.

Schritte

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
2. Erweitern Sie im Dashboard das Menü für Ihr Speichercluster.
3. Wählen Sie **Storage > Volumes**.
4. Klicken Sie auf die Registerkarte **QoS Policies**.
5. Klicken Sie auf das Menü **Aktionen** neben der QoS-Richtlinie, die Sie ändern möchten.
6. Klicken Sie Auf **Löschen**.
7. Bestätigen Sie die Aktion.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Arbeiten Sie mit dem Management-Node

Übersicht über Management-Nodes

Sie können den Management-Node (mNode) verwenden, um Systemdienste zu verwenden, Cluster-Assets und -Einstellungen zu managen, Systemtests und Dienstprogramme auszuführen, Active IQ für das System-Monitoring zu konfigurieren und den NetApp Support-Zugriff zur Fehlerbehebung zu aktivieren.

> Als Best Practice wird nur ein Management Node mit einer VMware vCenter Instanz verknüpft, sodass nicht dieselben Storage- und Computing-Ressourcen oder vCenter Instanzen in mehreren Management Nodes definiert werden müssen.

Für Cluster mit Element Softwareversion 11.3 oder höher können Sie mit dem Management-Node über eine von zwei Schnittstellen arbeiten:

- Mit der Management-Node-UI (`https://[mNode IP]:442`) Können Sie Änderungen an Netzwerk- und Clustereinstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.
- Mit der integrierten REST API UI (`https://[mNode IP]/mnode`) Können Sie APIs ausführen oder verstehen, die mit den Management-Knoten-Services verbunden sind, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

Installation oder Wiederherstellung eines Management-Node:

- "Installieren Sie einen Management-Node"
- "Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)"
- "Wiederherstellung eines Management-Node"

Zugriff auf den Management-Node:

- "Zugriff auf den Management-Node (UI oder REST-API)"

Ändern Sie das Standard-SSL-Zertifikat:

- "Ändern Sie das Standard-SSL-Zertifikat für den Management-Node"

Führen Sie Aufgaben mit der Management-Node-UI durch:

- "Übersicht über die Management-Node-UI"

Aufgaben mit den MANAGEMENT-Node-REST-APIs:

- "Übersicht über DIE REST-API-UI für den Management-Node"

Deaktivieren oder aktivieren Sie Remote-SSH-Funktionen oder starten Sie mit NetApp Support eine Remote-Support-Tunnelsitzung, um Unterstützung bei der Fehlerbehebung zu bieten:

- "Aktivieren von Remote-Verbindungen mit NetApp Support"

- "Verwalten der SSH-Funktionalität auf dem Management-Node"

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Installation oder Wiederherstellung eines Management-Node

Installieren Sie einen Management-Node

Sie können den Management-Node für Ihr Cluster, auf dem die NetApp Element Software ausgeführt wird, manuell installieren. Verwenden Sie dabei das entsprechende Image für Ihre Konfiguration.

Dieses Handbuch richtet sich an NetApp HCI-Administratoren, die die NetApp Deployment Engine nicht zur Installation von Management-Nodes verwenden.

Was Sie benötigen

- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Ihre Installation verwendet IPv4. Der Management-Node 11.3 unterstützt IPv6 nicht.

  Wenn IPv6 unterstützt werden soll, können Sie den Management-Node 11.1 verwenden.

- Sie sind berechtigt, Software von der NetApp Support Site herunterzuladen.
- Sie haben den für Ihre Plattform korrekten Managementknoten-Image-Typ identifiziert:

Plattform	Bildtyp der Installation
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

- (Management-Node 12.0 und höher mit Proxy-Server) Sie haben die Version 2.16 von NetApp Hybrid Cloud Control auf Managementservices aktualisiert, bevor Sie einen Proxy-Server konfigurieren.

Über diese Aufgabe

Der Element 12.2 Management-Node ist ein optionales Upgrade. Bei bestehenden Implementierungen wird dieser Bedarf nicht benötigt.

Bevor Sie dieses Verfahren befolgen, sollten Sie ein Verständnis von haben "Persistente Volumes" Und ob du sie nutzen willst oder nicht. Persistente Volumes sind optional, aber im Falle eines VM-Verlusts empfohlen für die Wiederherstellung von Daten aus der Management-Node-Konfiguration.

Schritte

1. und implementieren Sie die VM

2. und konfigurieren Sie das Netzwerk
3. Konfigurieren Sie die Zeitsynchronisierung
4. Richten Sie den Management-Node ein
5. Controller-Assets konfigurieren
6. (Nur NetApp HCI) Konfigurieren der Ressourcen der Computing-Nodes

Laden Sie ISO oder OVA herunter, und implementieren Sie die VM

1. Laden Sie die OVA oder ISO für Ihre Installation im herunter "NetApp HCI" Auf der NetApp Support Site:
   a. Wählen Sie **Letzte Version herunterladen** und akzeptieren Sie die EULA.
   b. Wählen Sie das Management-Node-Image aus, das Sie herunterladen möchten.
2. Wenn Sie die OVA heruntergeladen haben, gehen Sie wie folgt vor:
   a. OVA bereitstellen.
   b. Wenn sich Ihr Storage-Cluster in einem separaten Subnetz vom Management-Node (eth0) befindet und Sie persistente Volumes verwenden möchten, fügen Sie der VM im Storage-Subnetz einen zweiten NIC (Network Interface Controller) hinzu (z. B. eth1) oder stellen Sie sicher, dass das Managementnetzwerk zum Storage-Netzwerk weiterleiten kann.
3. Wenn Sie die ISO heruntergeladen haben, führen Sie die folgenden Schritte aus:
   a. Erstellen Sie aus Ihrem Hypervisor eine neue 64-Bit-Virtual Machine mit der folgenden Konfiguration:
      - Sechs virtuelle CPUs
      - 24 GB RAM
      - Speicheradaptertyp auf LSI Logic Parallel eingestellt

        Der Standard für Ihren Management-Node ist möglicherweise LSI Logic SAS. Überprüfen Sie im Fenster **New Virtual Machine** die Konfiguration des Speicheradapters, indem Sie **Hardware anpassen** > **Virtual Hardware** wählen. Ändern Sie bei Bedarf LSI Logic SAS in **LSI Logic Parallel**.

      - 400 GB virtuelle Festplatte, Thin Provisioning
      - Eine virtuelle Netzwerkschnittstelle mit Internetzugang und Zugriff auf den Speicher MVIP.
      - Eine virtuelle Netzwerkschnittstelle mit Managementnetzwerk-Zugriff auf das Storage-Cluster. Wenn sich Ihr Storage-Cluster in einem separaten Subnetz vom Management-Node (eth0) befindet und Sie persistente Volumes verwenden möchten, fügen Sie der VM im Storage-Subnetz (eth1) einen zweiten NIC (Network Interface Controller) hinzu oder stellen Sie sicher, dass das Managementnetzwerk zum Speichernetzwerk umgeleitet werden kann.

        Schalten Sie die virtuelle Maschine nicht vor dem Schritt ein, der später in diesem Verfahren angezeigt wird.

   b. Verbinden Sie die ISO mit der virtuellen Maschine, und starten Sie sie am .iso-Installations-Image.

      Wenn Sie einen Management-Node mithilfe des Images installieren, kann dies zu einer Verzögerung von 30 Sekunden führen, bevor der Startbildschirm angezeigt wird.

4. Schalten Sie die virtuelle Maschine für den Managementknoten ein, nachdem die Installation abgeschlossen ist.

Erstellen Sie den Management-Node-Administrator, und konfigurieren Sie das Netzwerk

1. Erstellen Sie über die Terminal User Interface (TUI) einen Management Node Admin User.

   Um durch die Menüoptionen zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste. Um durch die Tasten zu navigieren, drücken Sie Tab. Um von den Schaltflächen zu den Feldern zu wechseln, drücken Sie Tab. Um zwischen Feldern zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste.

2. Konfigurieren Sie das Management-Node-Netzwerk (eth0).

   Wenn Sie eine zusätzliche NIC benötigen, um den Speicherdatenverkehr zu isolieren, lesen Sie die Anweisungen zum Konfigurieren einer anderen NIC: "Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)".

Konfigurieren Sie die Zeitsynchronisierung

1. Stellen Sie sicher, dass die Zeit zwischen dem Management-Node und dem Storage-Cluster mit NTP synchronisiert wird:

   Ab Element 12.3 werden die Teilschritte a bis (e) automatisch ausgeführt. Für Management-Node 12.3 fahren Sie mit fort Unterschritt (f) Um die Konfiguration der Zeitsynchronisation abzuschließen.

   a. Melden Sie sich über SSH oder die vom Hypervisor bereitgestellte Konsole beim Management-Node an.

   b. NTPD stoppen:

      ```
      sudo service ntpd stop
      ```

   c. Bearbeiten Sie die NTP-Konfigurationsdatei `/etc/ntp.conf`:

      i. Kommentieren Sie die Standardserver (`server 0.gentoo.pool.ntp.org`) Durch Hinzufügen von a `#` Vor jedem.

      ii. Fügen Sie für jeden Standardserver, den Sie hinzufügen möchten, eine neue Zeile hinzu. Die Standardzeitserver müssen die gleichen NTP-Server sein, die auf dem Speicher-Cluster verwendet werden, die Sie in A verwenden "Später Schritt".

      ```
      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. Speichern Sie die Konfigurationsdatei nach Abschluss.

d. Erzwingen einer NTP-Synchronisierung mit dem neu hinzugefügten Server.

```
sudo ntpd -gq
```

e. NTPD neu starten.

```
sudo service ntpd start
```

f. Zeitsynchronisierung mit Host über den Hypervisor deaktivieren (im Folgenden ein VMware-Beispiel):

> Wenn Sie den mNode in einer anderen Hypervisor-Umgebung als VMware bereitstellen, zum Beispiel vom .iso-Image in einer OpenStack-Umgebung, finden Sie in der Hypervisor-Dokumentation die entsprechenden Befehle.

i. Periodische Zeitsynchronisierung deaktivieren:

```
vmware-toolbox-cmd timesync disable
```

ii. Den aktuellen Status des Dienstes anzeigen und bestätigen:

```
vmware-toolbox-cmd timesync status
```

iii. Überprüfen Sie in vSphere das `Synchronize guest time with host` Das Kontrollkästchen ist in den VM-Optionen nicht aktiviert.

> Aktivieren Sie diese Option nicht, wenn Sie zukünftige Änderungen an der VM vornehmen.

> Bearbeiten Sie NTP nicht, nachdem Sie die Konfiguration zur Zeitsynchronisation abgeschlossen haben, da es sich auf das NTP beim Ausführen des auswirkt "Setup-Befehl" Auf dem Management-Node.

Richten Sie den Management-Node ein

1. Konfigurieren und Ausführen des Management-Node-Setup-Befehls:

> Sie werden aufgefordert, Passwörter in einer sicheren Eingabeaufforderung einzugeben. Wenn sich Ihr Cluster hinter einem Proxy-Server befindet, müssen Sie die Proxy-Einstellungen konfigurieren, damit Sie ein öffentliches Netzwerk erreichen können.

```
sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

a. Ersetzen Sie den Wert in [ ] Klammern (einschließlich der Klammern) für jeden der folgenden erforderlichen Parameter:

> Die gekürzte Form des Befehlsnamens ist in Klammern ( ) und kann durch den vollständigen Namen ersetzt werden.

- **--mnode_admin_user (-mu) [username]**: Der Benutzername für das Administrator-Konto des Management-Node. Dies ist wahrscheinlich der Benutzername für das Benutzerkonto, mit dem Sie sich beim Management-Node anmelden.
- **--Storage_mvip (-SM) [MVIP-Adresse]**: Die virtuelle Management-IP-Adresse (MVIP) des Speicherclusters, auf dem Element Software ausgeführt wird. Konfigurieren Sie den Management-Node mit demselben Storage-Cluster, das Sie während verwendet haben "Konfiguration von NTP-Servern".
- **--Storage_username (-su) [username]**: Der Benutzername des Speicherclusters für den vom angegebenen Cluster `--storage_mvip` Parameter.
- **--Telemetrie_Active (-t) [true]**: Den Wert TRUE beibehalten, der die Datenerfassung zur Analyse durch Active IQ ermöglicht.

b. (Optional): Fügen Sie dem Befehl Active IQ-Endpunkt-Parameter hinzu:

- **--Remote_Host (-rh) [AIQ_Endpunkt]**: Der Endpunkt, an dem Active IQ Telemetriedaten zur Verarbeitung gesendet werden. Wenn der Parameter nicht enthalten ist, wird der Standardendpunkt verwendet.

c. (Empfohlen): Fügen Sie die folgenden persistenten Volume-Parameter hinzu. Ändern oder löschen Sie das Konto und die Volumes, die für die Funktion „persistente Volumes“ erstellt wurden, nicht, oder die Managementfunktion kann verloren gehen.

- **--use_persistent_Volumes (-pv) [true/false, default: False]**: Aktivieren oder deaktivieren Sie persistente Volumes. Geben Sie den Wert TRUE ein, um die Funktion persistenter Volumes zu aktivieren.
- **--persistent_Volumes_Account (-pva) [Account_Name]**: Wenn `--use_persistent_volumes` Ist auf „true“ gesetzt. Verwenden Sie diesen Parameter, und geben Sie den Namen des Speicherkontos ein, der für persistente Volumes verwendet wird.

> Verwenden Sie einen eindeutigen Kontonamen für persistente Volumes, der sich von jedem vorhandenen Kontonamen im Cluster unterscheidet. Es ist von zentraler Bedeutung, dass das Konto für persistente Volumes getrennt von der übrigen Umgebung bleibt.

- **--persistent_Volumes_mvip (-pvm) [mvip]**: Geben Sie die virtuelle Management-IP-Adresse (MVIP) des Storage-Clusters ein, auf dem Element Software ausgeführt wird, die mit persistenten Volumes verwendet wird. Dies ist nur erforderlich, wenn vom Management-Node mehrere Storage-Cluster gemanagt werden. Wenn nicht mehrere Cluster verwaltet werden, wird der Standard-Cluster MVIP verwendet.

d. Proxy-Server konfigurieren:

- **--use_Proxy (-up) [true/false, default: False]**: Aktivieren oder deaktivieren Sie die Verwendung des Proxy. Dieser Parameter ist erforderlich, um einen Proxyserver zu konfigurieren.
- **--Proxy_Hostname_or_ip (-pi) [Host]**: Der Proxy-Hostname oder die IP. Dies ist erforderlich, wenn Sie einen Proxy verwenden möchten. Wenn Sie dies angeben, werden Sie zur Eingabe aufgefordert `--proxy_port`.
- **--Proxy_username (-pu) [username]**: Der Proxy-Benutzername. Dieser Parameter ist optional.
- **--Proxy_password (-pp) [password]**: Das Proxy-Passwort. Dieser Parameter ist optional.
- **--Proxy_Port (-pq) [Port, Standard: 0]**: Der Proxy-Port. Wenn Sie dies angeben, werden Sie aufgefordert, den Proxy-Hostnamen oder die IP einzugeben (`--proxy_hostname_or_ip`).
- **--Proxy_SSH_Port (-ps) [Port, Standard: 443]**: Der SSH-Proxy-Port. Standardmäßig ist der Port 443.

e. (Optional) Verwenden Sie die Parameterhilfe, wenn Sie zusätzliche Informationen über die einzelnen Parameter benötigen:
   - **--help (-h)**: Gibt Informationen über jeden Parameter zurück. Parameter werden basierend auf der ursprünglichen Implementierung als erforderlich oder optional definiert. Die Parameteranforderungen für Upgrades und Neuimplementierungen können variieren.

f. Führen Sie die aus `setup-mnode` Befehl.

Controller-Assets konfigurieren

1. Suchen Sie die Installations-ID:
   a. Melden Sie sich in einem Browser bei DER REST API-UI für den Management-Node an:
   b. Wechseln Sie zum Speicher-MVIP und melden Sie sich an. Durch diese Aktion wird das Zertifikat für den nächsten Schritt akzeptiert.
   c. Öffnen Sie die REST API-UI für den Bestandsdienst auf dem Managementknoten:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   d. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   e. Wählen Sie in DER REST API UI **GET /Installations** aus.
   f. Wählen Sie **Probieren Sie es aus**.
   g. Wählen Sie **Ausführen**.
   h. Kopieren Sie aus dem Code 200 Response Body den und speichern Sie den `id` Für die Installation in einem späteren Schritt.

      Die Installation verfügt über eine Basiskonfiguration, die während der Installation oder eines Upgrades erstellt wurde.

2. (Nur NetApp HCI) Suchen Sie das Hardware-Tag für Ihren Computing-Node in vSphere:
   a. Wählen Sie den Host im vSphere Web Client Navigator aus.

b. Wählen Sie die Registerkarte **Monitor** aus und wählen Sie **Hardwarezustand**.

c. Die Node-BIOS-Hersteller und die Modellnummer werden aufgelistet. Kopieren und speichern Sie den Wert für `tag` Zur Verwendung in einem späteren Schritt.

3. Fügen Sie dem Management-Node bekannte Ressourcen ein vCenter Controller Asset zum NetApp HCI Monitoring (nur NetApp HCI Installationen) und zur Hybrid Cloud Control (für alle Installationen) hinzu:

a. Rufen Sie die mNode-Service-API-UI auf dem Management-Node auf, indem Sie die Management-Node-IP-Adresse, gefolgt von eingeben `/mnode`:

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

b. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:

i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

ii. Geben Sie die Client-ID als ein `mnode-client`.

iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

iv. Schließen Sie das Fenster.

c. Wählen Sie **POST /Assets/{Asset_id}/Controllers** aus, um eine Unterressource des Controllers hinzuzufügen.

> Sie sollten eine neue NetApp HCC-Rolle in vCenter erstellen, um eine Controller-Unterressource hinzuzufügen. Diese neue NetApp HCC-Rolle beschränkt die Management Node Services-Ansicht auf reine NetApp Ressourcen. Siehe "Erstellen einer NetApp HCC-Rolle in vCenter".

d. Wählen Sie **Probieren Sie es aus**.

e. Geben Sie im Feld **Asset_id** die ID der übergeordneten Basis ein, die Sie in die Zwischenablage kopiert haben.

f. Geben Sie die erforderlichen Nutzlastwerte mit dem Typ ein `vCenter` Und vCenter Zugangsdaten.

g. Wählen Sie **Ausführen**.

(Nur NetApp HCI) Konfigurieren der Ressourcen der Computing-Nodes

1. (Nur für NetApp HCI) Hinzufügen einer Computing-Node-Ressource zu den bekannten Management-Node-Assets:

a. Wählen Sie **POST /Assets/{Asset_id}/Compute-Nodes** aus, um eine Compute-Node-Unterressource mit Anmeldeinformationen für die Compute-Node-Ressource hinzuzufügen.

b. Wählen Sie **Probieren Sie es aus**.

c. Geben Sie im Feld **Asset_id** die ID der übergeordneten Basis ein, die Sie in die Zwischenablage kopiert haben.

d. Geben Sie in der Nutzlast die erforderlichen Nutzlastwerte ein, die auf der Registerkarte „Modell“ definiert sind. Eingabe `ESXi Host` Als `type` Und geben Sie die Hardware-Tag-Nummer ein, die Sie während eines vorherigen Schritts für gespeichert haben `hardware_tag`.

e. Wählen Sie **Ausführen**.

Weitere Informationen

- "Persistente Volumes"
- "Fügen Sie dem Management-Node Computing- und Controller-Ressourcen hinzu"
- "Konfigurieren Sie eine Speicher-NIC"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)

Wenn Sie eine zusätzliche NIC für den Speicher verwenden, können Sie SSH in den Management-Knoten einlegen oder die vCenter-Konsole verwenden und einen Curl-Befehl ausführen, um eine getaggte oder nicht getaggte Netzwerkschnittstelle einzurichten.

Bevor Sie beginnen

- Sie kennen Ihre eth0-IP-Adresse.
- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node 11.3 oder höher implementiert.

Konfigurationsoptionen

Wählen Sie die für Ihre Umgebung relevante Option:

- Konfigurieren Sie einen Speicher Network Interface Controller (NIC) für eine nicht getaggte Netzwerkschnittstelle
- Konfigurieren Sie einen Speicher Network Interface Controller (NIC) für eine getaggte Netzwerkschnittstelle

Konfigurieren Sie einen Speicher Network Interface Controller (NIC) für eine nicht getaggte Netzwerkschnittstelle

Schritte

1. Öffnen Sie eine SSH oder vCenter Konsole.
2. Ersetzen Sie die Werte in der folgenden Befehlsvorlage und führen Sie den Befehl aus:

> Werte werden durch dargestellt `$` Für jeden der erforderlichen Parameter für die neue Storage-Netzwerk-Schnittstelle. Der `cluster` Das Objekt in der folgenden Vorlage ist erforderlich und kann für die Umbenennung des Management-Node-Host-Namens verwendet werden. `--insecure` Oder `-k` Optionen sollten nicht in Produktionsumgebungen verwendet werden.

```
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"
}
'
```

Konfigurieren Sie einen Speicher Network Interface Controller (NIC) für eine getaggte Netzwerkschnittstelle

Schritte

1. Öffnen Sie eine SSH oder vCenter Konsole.
2. Ersetzen Sie die Werte in der folgenden Befehlsvorlage und führen Sie den Befehl aus:

> Werte werden durch dargestellt `$` Für jeden der erforderlichen Parameter für die neue Storage-Netzwerk-Schnittstelle. Der `cluster` Das Objekt in der folgenden Vorlage ist erforderlich und kann für die Umbenennung des Management-Node-Host-Namens verwendet werden. `--insecure` Oder `-k` Optionen sollten nicht in Produktionsumgebungen verwendet werden.

```
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"
}
'
```

Weitere Informationen

- "Fügen Sie dem Management-Node Computing- und Controller-Ressourcen hinzu"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Wiederherstellung eines Management-Node

Sie können den Management-Node für Ihren Cluster, auf dem die NetApp Element Software ausgeführt wird, manuell wiederherstellen und neu bereitstellen, wenn der vorherige Management-Node persistente Volumes verwendete.

Sie können eine neue OVA implementieren und ein Neuimplementierung-Skript ausführen, um Konfigurationsdaten aus einem zuvor installierten Management Node, auf dem Version 11.3 und höher ausgeführt wird, zu übertragen.

Was Sie benötigen

- Auf dem vorherigen Management-Node wurde die NetApp Element Softwareversion 11.3 oder höher mit ausgeführt "Persistente Volumes" Funktionalität eingebunden.
- Sie kennen die MVIP und SVIP des Clusters, der die persistenten Volumes enthält.
- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Ihre Installation verwendet IPv4. Der Management-Node 11.3 unterstützt IPv6 nicht.
- Sie sind berechtigt, Software von der NetApp Support Site herunterzuladen.
- Sie haben den für Ihre Plattform korrekten Managementknoten-Image-Typ identifiziert:

Plattform	Bildtyp der Installation
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

Schritte

1. und implementieren Sie die VM
2. Konfigurieren des Netzwerks
3. Konfigurieren Sie die Zeitsynchronisierung
4. Konfigurieren Sie den Management-Node

Laden Sie ISO oder OVA herunter, und implementieren Sie die VM

1. Laden Sie die OVA oder ISO für Ihre Installation im herunter "NetApp HCI" Auf der NetApp Support Site:
   a. Klicken Sie auf **Letzte Version herunterladen** und akzeptieren Sie die EULA.
   b. Wählen Sie das Management-Node-Image aus, das Sie herunterladen möchten.
2. Wenn Sie die OVA heruntergeladen haben, gehen Sie wie folgt vor:
   a. OVA bereitstellen.
   b. Wenn sich Ihr Storage-Cluster in einem separaten Subnetz vom Management-Node (eth0) befindet und Sie persistente Volumes verwenden möchten, fügen Sie der VM im Storage-Subnetz einen zweiten NIC (Network Interface Controller) hinzu (z. B. eth1) oder stellen Sie sicher, dass das Managementnetzwerk zum Storage-Netzwerk weiterleiten kann.
3. Wenn Sie die ISO heruntergeladen haben, führen Sie die folgenden Schritte aus:
   a. Erstellen Sie aus Ihrem Hypervisor eine neue 64-Bit-Virtual Machine mit der folgenden Konfiguration:
      - Sechs virtuelle CPUs
      - 24 GB RAM
      - 400 GB virtuelle Festplatte, Thin Provisioning
      - Eine virtuelle Netzwerkschnittstelle mit Internetzugang und Zugriff auf den Speicher MVIP.
      - Eine virtuelle Netzwerkschnittstelle mit Managementnetzwerk-Zugriff auf das Storage-Cluster. Wenn sich Ihr Storage-Cluster in einem separaten Subnetz vom Management-Node (eth0) befindet und Sie persistente Volumes verwenden möchten, fügen Sie der VM im Storage-Subnetz (eth1)

einen zweiten NIC (Network Interface Controller) hinzu oder stellen Sie sicher, dass das Managementnetzwerk zum Speichernetzwerk umgeleitet werden kann.

> Schalten Sie die virtuelle Maschine nicht vor dem Schritt ein, der später in diesem Verfahren angezeigt wird.

b. Verbinden Sie die ISO mit der virtuellen Maschine, und starten Sie sie am .iso-Installations-Image.

> Wenn Sie einen Management-Node mithilfe des Images installieren, kann dies zu einer Verzögerung von 30 Sekunden führen, bevor der Startbildschirm angezeigt wird.

4. Schalten Sie die virtuelle Maschine für den Managementknoten ein, nachdem die Installation abgeschlossen ist.

Konfigurieren des Netzwerks

1. Erstellen Sie über die Terminal User Interface (TUI) einen Management Node Admin User.

> Um durch die Menüoptionen zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste. Um durch die Tasten zu navigieren, drücken Sie Tab. Um von den Schaltflächen zu den Feldern zu wechseln, drücken Sie Tab. Um zwischen Feldern zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste.

2. Konfigurieren Sie das Management-Node-Netzwerk (eth0).

> Wenn Sie eine zusätzliche NIC benötigen, um den Speicherdatenverkehr zu isolieren, lesen Sie die Anweisungen zum Konfigurieren einer anderen NIC: "Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)".

Konfigurieren Sie die Zeitsynchronisierung

1. Stellen Sie sicher, dass die Zeit zwischen dem Management-Node und dem Storage-Cluster mit NTP synchronisiert wird:

> Ab Element 12.3 werden die Teilschritte a bis (e) automatisch ausgeführt. Für Management-Node 12.3 fahren Sie mit fort Unterschritt (f) Um die Konfiguration der Zeitsynchronisation abzuschließen.

1. Melden Sie sich über SSH oder die vom Hypervisor bereitgestellte Konsole beim Management-Node an.
2. NTPD stoppen:

```
sudo service ntpd stop
```

3. Bearbeiten Sie die NTP-Konfigurationsdatei `/etc/ntp.conf`:
   a. Kommentieren Sie die Standardserver (`server 0.gentoo.pool.ntp.org`) Durch Hinzufügen von a `#` Vor jedem.
   b. Fügen Sie für jeden Standardserver, den Sie hinzufügen möchten, eine neue Zeile hinzu. Die Standardzeitserver müssen die gleichen NTP-Server sein, die auf dem Speicher-Cluster verwendet

werden, die Sie in A verwenden "Später Schritt".

```
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. Speichern Sie die Konfigurationsdatei nach Abschluss.

4. Erzwingen einer NTP-Synchronisierung mit dem neu hinzugefügten Server.

```
sudo ntpd -gq
```

5. NTPD neu starten.

```
sudo service ntpd start
```

6. Zeitsynchronisierung mit Host über den Hypervisor deaktivieren (im Folgenden ein VMware-Beispiel):

> Wenn Sie den mNode in einer anderen Hypervisor-Umgebung als VMware bereitstellen, zum Beispiel vom .iso-Image in einer OpenStack-Umgebung, finden Sie in der Hypervisor-Dokumentation die entsprechenden Befehle.

a. Periodische Zeitsynchronisierung deaktivieren:

```
vmware-toolbox-cmd timesync disable
```

b. Den aktuellen Status des Dienstes anzeigen und bestätigen:

```
vmware-toolbox-cmd timesync status
```

c. Überprüfen Sie in vSphere das `Synchronize guest time with host` Das Kontrollkästchen ist in den VM-Optionen nicht aktiviert.

> Aktivieren Sie diese Option nicht, wenn Sie zukünftige Änderungen an der VM vornehmen.

> Bearbeiten Sie NTP nicht, nachdem Sie die Konfiguration zur Zeitsynchronisation abgeschlossen haben, da es sich auf das NTP beim Ausführen des auswirkt Befehl „Neuimplementierung“ Auf dem Management-Node.

Konfigurieren Sie den Management-Node

1. Erstellen eines temporären Zielverzeichnisses für den Inhalt des Management Services-Pakets:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Laden Sie das Management-Services-Bundle (Version 2.15.28 oder höher) herunter, das zuvor auf dem vorhandenen Management-Node installiert wurde, und speichern Sie es im `/sf/etc/mnode/` Verzeichnis.
3. Extrahieren Sie das heruntergeladene Bundle mit dem folgenden Befehl und ersetzen Sie den Wert in [ ] Klammern (einschließlich der Klammern) durch den Namen der Bundle-Datei:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle
file]
```

4. Extrahieren Sie die resultierende Datei in das `/sf/etc/mnode-archive` Verzeichnis:

```
tar -C /sf/etc/mnode/mnode-archive -xvf
/sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. Eine Konfigurationsdatei für Konten und Volumes erstellen:

```
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. Ersetzen Sie den Wert in [ ] Klammern (einschließlich der Klammern) für jeden der folgenden erforderlichen Parameter:

      - **[mvip IP-Adresse]**: Die Management-virtuelle IP-Adresse des Storage-Clusters. Konfigurieren Sie den Management-Node mit demselben Storage-Cluster, das Sie während verwendet haben "Konfiguration von NTP-Servern".
      - **[Kontoname des persistenten Volumes]**: Der Name des Kontos, der mit allen persistenten Volumes in diesem Speicher-Cluster verknüpft ist.

6. Konfigurieren und Ausführen des Befehls „Management Node Neuimplementierung“, um eine Verbindung zu persistenten Volumes zu herstellen, die im Cluster gehostet werden, und um Services mit früheren Management-Node-Konfigurationsdaten zu starten:

> Sie werden aufgefordert, Passwörter in einer sicheren Eingabeaufforderung einzugeben. Wenn sich Ihr Cluster hinter einem Proxy-Server befindet, müssen Sie die Proxy-Einstellungen konfigurieren, damit Sie ein öffentliches Netzwerk erreichen können.

```
sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

a. Ersetzen Sie den Wert in [ ]-Klammern (einschließlich der Klammern) durch den Benutzernamen für das Administratorkonto für den Managementknoten. Dies ist wahrscheinlich der Benutzername für das Benutzerkonto, mit dem Sie sich beim Management-Node anmelden.

> Sie können den Benutzernamen hinzufügen oder dem Skript erlauben, Sie zur Eingabe der Informationen zu auffordern.

b. Führen Sie die aus `redeploy-mnode` Befehl. Das Skript zeigt eine Erfolgsmeldung an, wenn die erneute Implementierung abgeschlossen ist.

c. Wenn Sie unter Verwendung des vollständig qualifizierten Domain-Namens (FQDN) des Systems auf Element oder NetApp HCI-Webschnittstellen (z. B. der Management-Node oder NetApp Hybrid Cloud Control) zugreifen, "Konfigurieren Sie die Authentifizierung für den Management-Node neu".

> SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Nodes mit Management-Services 2.18 und höher standardmäßig deaktiviert. Wenn Sie zuvor die SSH-Funktion auf dem Management-Node aktiviert hatten, müssen Sie möglicherweise auch "Deaktivieren Sie SSH erneut" Auf dem wiederhergestellten Management-Node.

Weitere Informationen

- "Persistente Volumes"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Greifen Sie auf den Management-Node zu

Ab der NetApp Element Softwareversion 11.3 enthält der Managementknoten zwei UIs: Eine Benutzeroberfläche für die Verwaltung VON REST-basierten Diensten und eine UI pro Node zum Verwalten von Netzwerk- und Clustereinstellungen sowie Betriebssystemtests und -Dienstprogrammen.

Für Cluster mit Element Softwareversion 11.3 oder höher können Sie eine von zwei Schnittstellen verwenden:

- Mithilfe der Management-Node-UI (`https:// [mNode IP}:442`) Können Sie Änderungen an Netzwerk- und Clustereinstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.
- Über die integrierte REST-API-UI (`https://[mNode IP}/mnode`) Können Sie APIs ausführen oder verstehen, die mit den Management-Knoten-Services verbunden sind, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

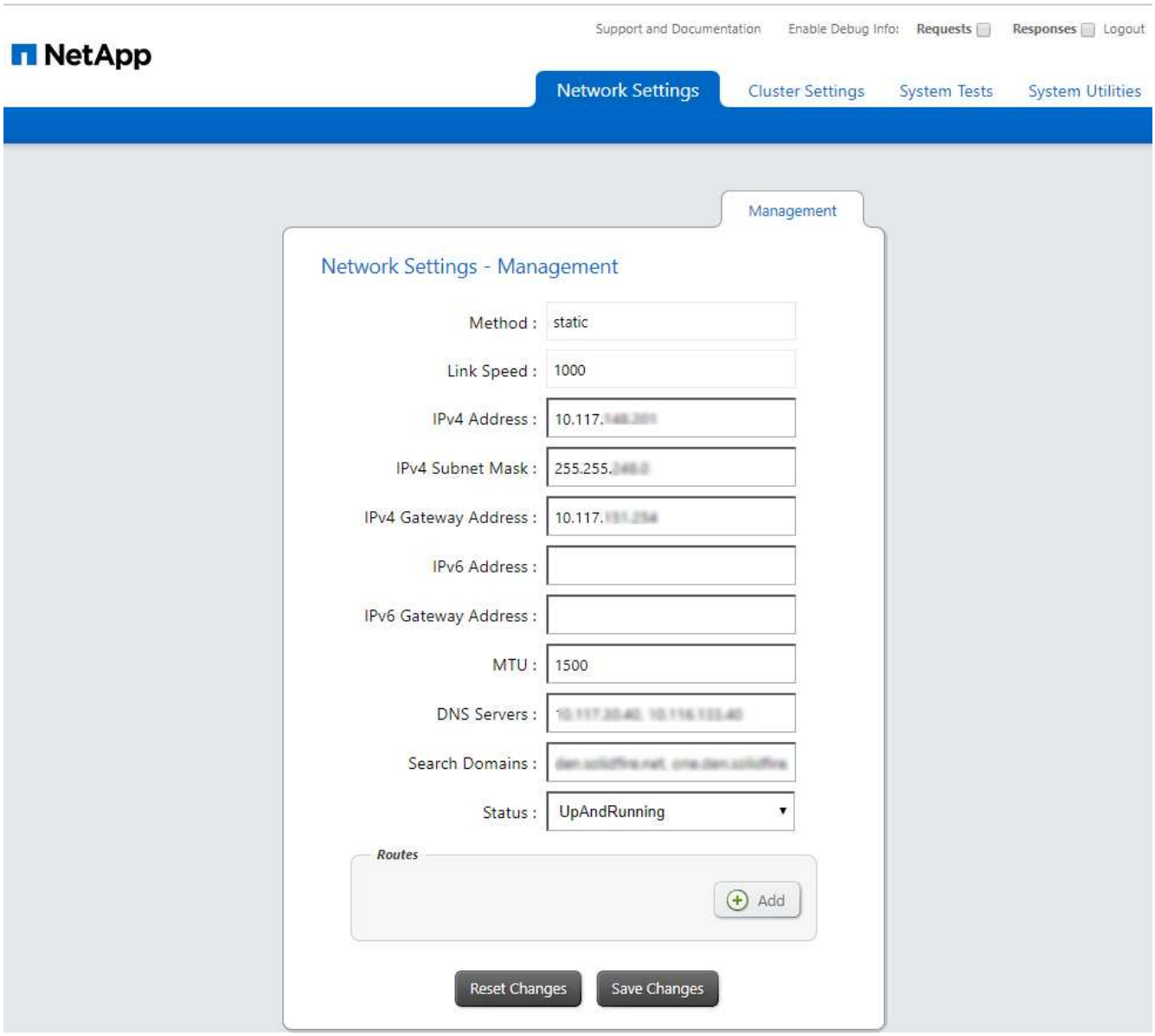
Greifen Sie über die UI auf den Management-Node zu

Über die UI pro Node können Sie auf Netzwerk- und Cluster-Einstellungen zugreifen und Systemtests und Dienstprogramme verwenden.

Schritte

1. Greifen Sie auf die UI pro Node für den Management-Node zu, indem Sie die IP-Adresse des Management-Knotens eingeben, gefolgt von :442

```
https://[IP address]:442
```



2. Geben Sie bei der entsprechenden Eingabeaufforderung den Benutzernamen und das Passwort für den Management-Node ein.

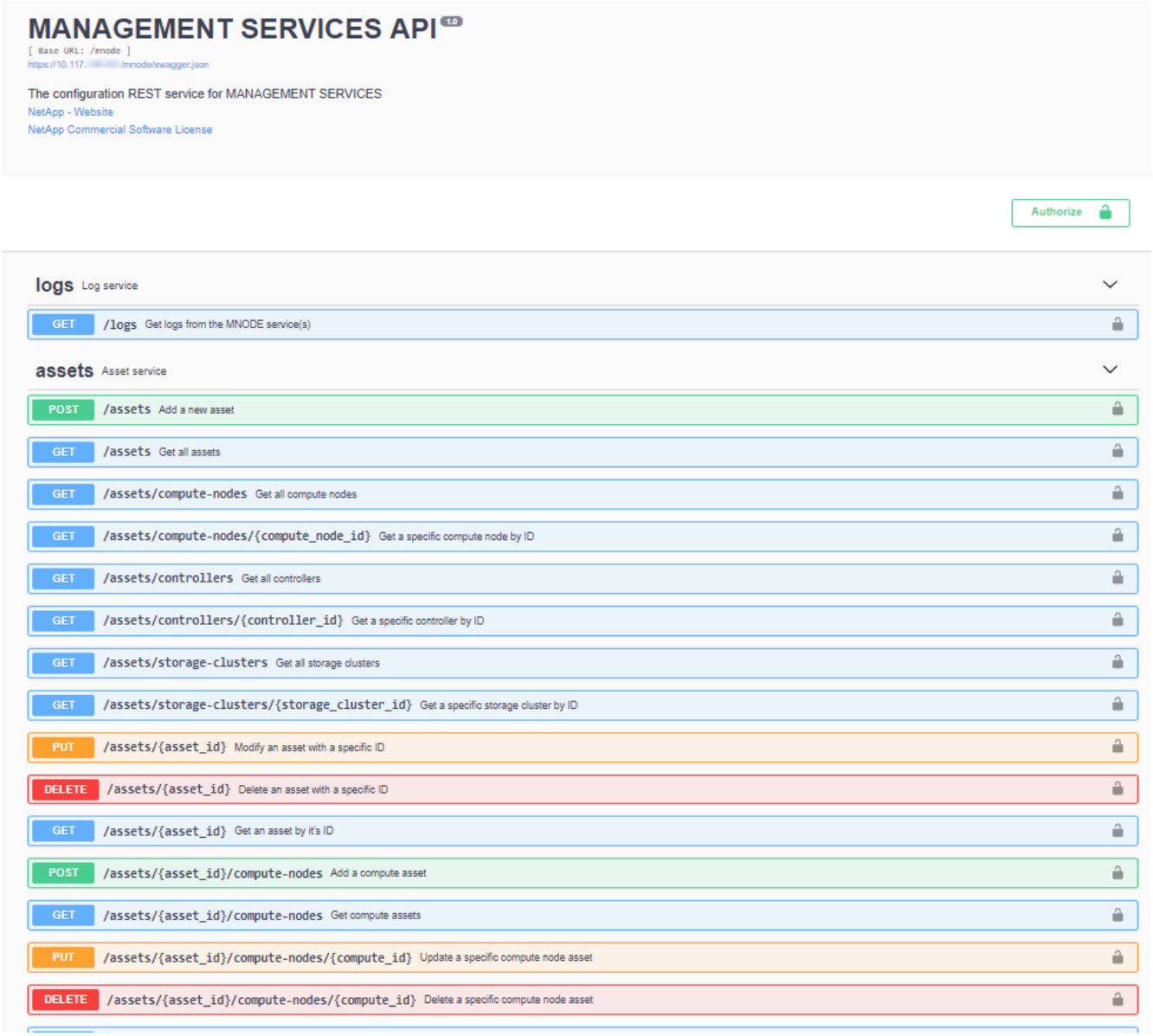
Greifen Sie auf DIE REST-API-UI für den Management-Node zu

Über DIE REST-API-UI erhalten Sie den Zugriff auf ein Menü mit Service-bezogenen APIs, die Managementservices auf dem Management-Node steuern.

Schritte

1. Um auf die REST-API-UI für Managementservices zuzugreifen, geben Sie die Management-Node-IP-Adresse gefolgt von ein `/mnode`:

```
https://[IP address]/mnode
```



2. Klicken Sie auf **autorisieren** oder auf ein Schlosssymbol und geben Sie Cluster Admin-Anmeldeinformationen ein, um APIs zu verwenden.

Weitere Informationen

- "Active IQ- und NetApp HCI-Monitoring aktivieren"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Ändern Sie das Standard-SSL-Zertifikat für den Management-Node

Sie können das Standard-SSL-Zertifikat und den privaten Schlüssel des Management-Node mithilfe der NetApp Element-API ändern.

Wenn Sie einen Verwaltungsknoten konfigurieren, erstellt er ein eindeutiges, selbstsigniertes SSL-Zertifikat (Secure Sockets Layer) und einen privaten Schlüssel, der für die gesamte HTTPS-Kommunikation über die Element-Benutzeroberfläche, die Benutzeroberfläche pro Knoten oder APIs verwendet wird. Die Element

Software unterstützt selbstsignierte Zertifikate sowie Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt und verifiziert werden.

Sie können die folgenden API-Methoden verwenden, um mehr Informationen über das Standard-SSL-Zertifikat zu erhalten und Änderungen vorzunehmen.

- **GetNodeSSLZertifikat**

  Sie können das verwenden "GetNodeSSLCertificate-Methode" So rufen Sie Informationen zum derzeit installierten SSL-Zertifikat ab, einschließlich aller Zertifikatdetails.

- **SetNodeSSLZertifikat**

  Sie können das verwenden "SetNodeSSLCertificate-Methode" Zum Festlegen der Cluster- und Node-SSL-Zertifikate auf das von Ihnen zur Verfügung gestellt Zertifikat und den privaten Schlüssel. Das System überprüft das Zertifikat und den privaten Schlüssel, um zu verhindern, dass ein ungültiges Zertifikat angewendet wird.

- **RemoveNodeSSLZertifikat**

  Das "RemoveNodeSSLCertificate-Methode" Entfernt das derzeit installierte SSL-Zertifikat und den privaten Schlüssel. Das Cluster generiert dann ein neues selbstsigniertes Zertifikat und einen privaten Schlüssel.

Weitere Informationen

- "Ändern Sie das Standard-SSL-Zertifikat der Element Software"
- "Welche Anforderungen gelten für das Festlegen benutzerdefinierter SSL-Zertifikate in der Element Software?"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Arbeiten Sie mit der Management-Node-UI

Übersicht über die Management-Node-UI

Mit der Management-Node-UI (`https://<mNodeIP>:442`) Können Sie Änderungen an Netzwerk- und Clustereinstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.

Aufgaben, die Sie mit der Management-Node-UI durchführen können:

- "Konfigurieren Sie die Meldungsüberwachung auf NetApp HCI"
- "Ändern und Testen der Netzwerk-, Cluster- und Systemeinstellungen des Management-Node"
- "Führen Sie Systemdienstprogramme vom Management-Node aus"

Weitere Informationen

- "Greifen Sie auf den Management-Node zu"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Konfigurieren Sie die Meldungsüberwachung auf NetApp HCI

Sie können die Einstellungen konfigurieren, um Meldungen auf Ihrem NetApp HCI System zu überwachen.

Die NetApp HCI-Alarmüberwachung leitet Warnungen des NetApp HCI Storage-Cluster-Systems an vCenter Server weiter, sodass Sie alle Warnmeldungen für NetApp HCI über die Schnittstelle des vSphere Web-Clients anzeigen können.

1. Öffnen Sie die Management-Node-UI pro Node (`https://[IP address]:442`).
2. Klicken Sie auf die Registerkarte * Warnmonitor*.
3. Konfigurieren der Optionen für die Überwachung von Warnmeldungen.

Optionen für die Überwachung von Warnmeldungen

Optionen	Beschreibung
Führen Sie Alarmüberwachungstests Aus	Führt die Systemtests des Monitorsystems aus, um Folgendes zu überprüfen: • NetApp HCI und VMware vCenter Konnektivität • Paarung von NetApp HCI und VMware vCenter über vom QoSSIOC-Service bereitgestellte Datenspeicherinformationen • Aktuelle NetApp HCI Alarm- und vCenter-Alarmlisten
Sammeln Von Warnungen	Aktiviert oder deaktiviert die Weiterleitung von NetApp HCI Storage-Warnmeldungen an vCenter. Sie können das Ziel-Storage-Cluster aus der Dropdown-Liste auswählen. Die Standardeinstellung für diese Option ist `Enabled`.
Sammeln Von Best Practice-Warnungen	Aktiviert oder deaktiviert die Weiterleitung von Best Practice-Warnmeldungen zu NetApp HCI Storage an vCenter. Warnmeldungen zu Best Practices sind Fehler, die durch eine suboptimale Systemkonfiguration ausgelöst werden. Die Standardeinstellung für diese Option ist `Disabled`. Bei deaktivierter NetApp HCI Storage Best Practice werden in vCenter keine Warnungen angezeigt.

Optionen	Beschreibung
Support-Daten an AIQ senden	Steuert den Datenfluss von VMware vCenter zu NetApp SolidFire Active IQ. Folgende Optionen stehen zur Verfügung: • Aktiviert: Alle vCenter Alarme, NetApp HCI Storage-Alarme und Support-Daten werden an NetApp SolidFire Active IQ gesendet. So kann NetApp die NetApp HCI Installation proaktiv unterstützen und überwachen, damit mögliche Probleme erkannt und gelöst werden können, bevor das System beeinträchtigt wird. • Deaktiviert: An NetApp SolidFire Active IQ werden keine vCenter Warnmeldungen, NetApp HCI Storage-Alarme oder Support-Daten gesendet. Wenn Sie die **Send Data to AIQ** Option mithilfe der NetApp Deployment Engine deaktiviert haben, sollten Sie dies tun "Telemetrie aktivieren" Verwenden Sie die REST API des Management-Node erneut, um den Service von dieser Seite aus zu konfigurieren.
Compute-Node-Daten an AIQ senden	Steuert den Datenfluss von den Computing-Nodes zu NetApp SolidFire Active IQ. Folgende Optionen stehen zur Verfügung: • Aktiviert: Support- und Überwachungsdaten über die Computing-Nodes werden an NetApp SolidFire Active IQ übertragen, um eine proaktive Unterstützung der Computing-Node-Hardware zu ermöglichen. • Deaktiviert: Support und Monitoring von Daten über die Computing-Nodes werden nicht an NetApp SolidFire Active IQ übertragen. Wenn Sie die **Send Data to AIQ** Option mithilfe der NetApp Deployment Engine deaktiviert haben, sollten Sie dies tun "Telemetrie aktivieren" Verwenden Sie die REST API des Management-Node erneut, um den Service von dieser Seite aus zu konfigurieren.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Ändern und Testen der Netzwerk-, Cluster- und Systemeinstellungen des Management-Node

Sie können die Einstellungen für das Management-Node-Netzwerk, das Cluster und das System ändern und testen.

- Aktualisieren der Netzwerkeinstellungen für den Management-Node
- Aktualisiert die Cluster-Einstellungen des Management-Node
- Testen Sie die Einstellungen für den Management-Node

Aktualisieren der Netzwerkeinstellungen für den Management-Node

Auf der Registerkarte „Netzwerkeinstellungen“ der Benutzeroberfläche für Management-Node pro Node können Sie die Felder für die Netzwerkschnittstelle des Managementknoten ändern.

1. Öffnen Sie die Management-Node-UI pro Node.
2. Klicken Sie auf die Registerkarte **Netzwerkeinstellungen**.
3. Die folgenden Informationen anzeigen oder eingeben:
   a. **Methode**: Wählen Sie eine der folgenden Methoden, um die Schnittstelle zu konfigurieren:
      - `loopback`: Verwenden Sie, um die IPv4-Loopback-Schnittstelle zu definieren.
      - `manual`: Verwenden Sie, um Schnittstellen zu definieren, für die keine Konfiguration erfolgt standardmäßig.
      - `dhop`: Nutzung, um eine IP-Adresse über DHCP zu erhalten.
      - `static`: Zur Definition von Ethernet-Schnittstellen mit statisch zugewiesenen IPv4-Adressen.
   b. **Verbindungsgeschwindigkeit**: Die Geschwindigkeit, die von der virtuellen NIC ausgehandelt wird.
   c. **IPv4-Adresse**: Die IPv4-Adresse für das eth0-Netzwerk.
   d. **IPv4-Subnetzmaske**: Adressenunterteilungen des IPv4-Netzwerks.
   e. **IPv4 Gateway-Adresse**: Router-Netzwerkadresse zum Senden von Paketen aus dem lokalen Netzwerk.
   f. **IPv6-Adresse**: Die IPv6-Adresse für das eth0-Netzwerk.
   g. **IPv6 Gateway-Adresse**: Router-Netzwerkadresse zum Senden von Paketen aus dem lokalen Netzwerk.

      Die IPv6-Optionen werden für Version 11.3 oder höher des Management-Node nicht unterstützt.

   h. **MTU**: Größte Paketgröße, die ein Netzwerkprotokoll übertragen kann. Muss größer als oder gleich 1500 sein. Wenn Sie eine zweite Speicher-NIC hinzufügen, sollte der Wert 9000 sein.
   i. **DNS Server**: Netzwerkschnittstelle für die Clusterkommunikation.
   j. **Domänen suchen**: Suche nach zusätzlichen MAC-Adressen, die dem System zur Verfügung stehen.
   k. **Status**: Mögliche Werte:
      - `UpAndRunning`

- `Down`
- `Up`

l. **Routen**: Statische Routen zu bestimmten Hosts oder Netzwerken über die zugehörige Schnittstelle werden die Routen konfiguriert.

Aktualisiert die Cluster-Einstellungen des Management-Node

Auf der Registerkarte Cluster-Einstellungen der Benutzeroberfläche pro Node für den Managementknoten können Sie die Felder für die Cluster-Schnittstelle ändern, wenn sich der Status eines Node im Status „verfügbar“, „Ausstehend“, „Pendingaktiv“ und „aktiv“ befindet.

1. Öffnen Sie die Management-Node-UI pro Node.
2. Klicken Sie auf die Registerkarte **Cluster-Einstellungen**.
3. Die folgenden Informationen anzeigen oder eingeben:
   - **Rolle**: Rolle, die der Management-Knoten im Cluster hat. Möglicher Wert: `Management`.
   - **Version**: Element Software Version läuft auf dem Cluster.
   - **Standardschnittstelle**: Standard-Netzwerkschnittstelle für die Kommunikation mit dem Cluster, auf dem die Element-Software ausgeführt wird.

Testen Sie die Einstellungen für den Management-Node

Nachdem Sie die Einstellungen für das Änderungsmanagement und das Netzwerk für den Management-Node geändert und die Änderungen übernommen haben, können Sie Tests durchführen, um die durchgeführten Änderungen zu validieren.

1. Öffnen Sie die Management-Node-UI pro Node.
2. Klicken Sie in der Management-Knoten-UI auf **Systemtests**.
3. Führen Sie eine der folgenden Aktionen durch:
   a. Um zu überprüfen, ob die von Ihnen konfigurierten Netzwerkeinstellungen für das System gültig sind, klicken Sie auf **Netzwerk-Konfiguration testen**.
   b. Um die Netzwerkverbindung zu allen Knoten im Cluster sowohl auf 1G- als auch 10G-Schnittstellen mit ICMP-Paketen zu testen, klicken Sie auf **Ping testen**.
4. Folgendes anzeigen oder eingeben:
   - **Hosts**: Geben Sie eine kommagetrennte Liste von Adressen oder Host-Namen von Geräten an, die ping werden sollen.
   - **Versuche**: Geben Sie an, wie oft das System den Ping-Test wiederholen soll. Standard: 5.
   - **Paketgröße**: Geben Sie die Anzahl der Bytes an, die in das ICMP-Paket gesendet werden sollen, das an jede IP gesendet wird. Die Anzahl der Bytes muss kleiner sein als die in der Netzwerkkonfiguration angegebene maximale MTU.
   - **Timeout ms**: Geben Sie die Anzahl der Millisekunden an, die auf jede einzelne Ping-Antwort warten soll. Standard: 500 ms.
   - **Total Timeout sec**: Geben Sie die Zeit in Sekunden an, die der Ping auf eine Systemantwort warten soll, bevor Sie den nächsten Ping-Versuch starten oder den Prozess beenden. Standard: 5.
   - **Fragmentierung verbieten**: Aktivieren Sie das DF-Flag (nicht fragmentieren) für die ICMP-Pakete.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Führen Sie Systemdienstprogramme vom Management-Node aus

Sie können die UI pro Node für den Management-Node verwenden, um Cluster-Supportpakete zu erstellen oder zu löschen, die Node-Konfigurationseinstellungen zurückzusetzen oder das Netzwerk neu zu starten.

Schritte

1. Öffnen Sie die Management-Node-UI pro Node mithilfe der Anmeldedaten für den Management-Node-Administrator.
2. Klicken Sie Auf **Systemdienstprogramme**.
3. Klicken Sie auf die Schaltfläche für das Dienstprogramm, das Sie ausführen möchten:
   a. **Control Power**: Startet neu, schaltet den Knoten aus oder schaltet den Knoten ab. Geben Sie eine der folgenden Optionen an.

      Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

      - **Aktion**: Optionen beinhalten `Restart` Und `Halt` (Ausschalten).
      - **Wartezeit**: Jede zusätzliche Zeit, bevor der Knoten wieder online kommt.

   b. **Cluster Support Bundle erstellen**: Erstellt das Cluster Support Bundle zur Unterstützung der NetApp Support diagnostischen Evaluierungen von einem oder mehreren Knoten in einem Cluster. Legen Sie die folgenden Optionen fest:
      - **Paketname**: Eindeutiger Name für jedes erstellte Supportpaket. Wenn kein Name angegeben wird, werden „Supportbundle“ und der Node-Name als Dateiname verwendet.
      - **MVIP**: Das MVIP des Clusters. Bundles werden von allen Nodes im Cluster gesammelt. Dieser Parameter ist erforderlich, wenn der Parameter Nodes nicht angegeben wird.
      - **Knoten**: Die IP-Adressen der Knoten, aus denen Pakete gesammelt werden. Geben Sie die Knoten, aus denen Pakete gesammelt werden sollen, entweder Knoten oder MVIP, jedoch nicht beides an. Dieser Parameter ist erforderlich, wenn MVIP nicht angegeben wird.
      - **Benutzername**: Der Cluster Admin Benutzername.
      - **Passwort**: Das Cluster-Admin-Passwort.
      - **Unvollständigkeit zulassen**: Lässt das Skript weiter laufen, wenn Bündel nicht von einem oder mehreren Knoten gesammelt werden können.
      - **Extra Args**: Dieser Parameter wird dem zugeführt `sf_make_support_bundle` Skript: Dieser Parameter sollte nur auf Anfrage des NetApp Support verwendet werden.

   c. **Alle Support-Pakete löschen**: Löscht alle aktuellen Support-Bundles auf dem Management-Knoten.
   d. **Reset Node**: Setzt den Management Node auf ein neues Installations-Image zurück. Dadurch werden alle Einstellungen außer der Netzwerkkonfiguration in den Standardzustand geändert. Legen Sie die folgenden Optionen fest:
      - **Build**: Die URL zu einem Remote Element Software-Image, auf das der Knoten zurückgesetzt wird.
      - **Optionen**: Spezifikationen für die Ausführung der Reset-Vorgänge. Details werden vom NetApp Support zur Verfügung gestellt, falls erforderlich.

Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

e. **Netzwerk neu starten**: Startet alle Netzwerkdienste auf dem Management-Knoten neu.

Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Arbeiten mit DER REST-API des Management-Node

Übersicht über DIE REST-API-UI für den Management-Node

Über die integrierte REST-API-UI (`https://<ManagementNodeIP>/mnode`) Können Sie APIs ausführen oder verstehen, die mit den Management-Knoten-Services verbunden sind, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

Aufgaben, die Sie mit REST-APIs durchführen können:

Autorisierung

- "Autorisierung zur Verwendung VON REST-APIs"

Konfiguration der Ressourcen

- "Active IQ- und NetApp HCI-Monitoring aktivieren"
- "Konfigurieren Sie einen Proxy-Server für den Management-Node"
- "Konfiguration von NetApp Hybrid Cloud Control für mehrere vCenter"
- "Fügen Sie dem Management-Node Computing- und Controller-Ressourcen hinzu"
- "Erstellen und Managen von Storage-Cluster-Assets"

Asset Management

- "Vorhandene Controller-Assets können angezeigt oder bearbeitet werden"
- "Erstellen und Managen von Storage-Cluster-Assets"
- "Entfernen Sie ein Asset vom Management-Node"
- "VERWENDEN Sie die REST API, um NetApp HCI-Protokolle zu sammeln"
- "Überprüfen Sie die Betriebssystem- und Servicestversionen der Management-Nodes"
- "Abrufen von Protokollen von Managementservices"

Weitere Informationen

- "Greifen Sie auf den Management-Node zu"
- "NetApp Element Plug-in für vCenter Server"

- "Seite „NetApp HCI Ressourcen“"

Autorisierung zur Verwendung VON REST-APIs

Sie müssen autorisieren, bevor Sie APIs für Managementservices in der REST API-UI verwenden können. Dazu erhalten Sie ein Zugriffstoken.

Um ein Token zu erhalten, geben Sie Cluster-Admin-Anmeldedaten und eine Client-ID an. Jedes Token dauert etwa zehn Minuten. Nachdem ein Token abgelaufen ist, können Sie erneut eine Genehmigung für ein neues Access Token erteilen.

Während der Installation und Implementierung des Management-Node werden Autorisierungsfunktionen für Sie eingerichtet. Der Token-Service basiert auf dem Storage-Cluster, das Sie während des Setups definiert haben.

Bevor Sie beginnen

- Auf Ihrer Cluster-Version sollte die NetApp Element Software 11.3 oder höher ausgeführt werden.
- Sie sollten einen Management-Node mit Version 11.3 oder höher implementiert haben.

API-Befehl

```
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`
```

SCHRITTE DER REST API-UI

1. Greifen Sie auf die REST-API-UI für den Service zu, indem Sie beispielsweise die Management-Node-IP-Adresse gefolgt vom Dienstnamen eingeben `/mnode/`:

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

2. Klicken Sie Auf **Autorisieren**.

   Alternativ können Sie auf ein Sperrsymbol neben einer beliebigen Service-API klicken.

3. Gehen Sie wie folgt vor:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Geben Sie keinen Wert für das Clientgeheimnis ein.
   d. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
4. Schließen Sie das Dialogfeld * Verfügbare Berechtigungen*.

   Wenn Sie versuchen, einen Befehl auszuführen, nachdem das Token abgelaufen ist, wird ein angezeigt `401 Error: UNAUTHORIZED` Meldung wird angezeigt. Wenn Sie dies sehen, autorisieren Sie erneut.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Active IQ- und NetApp HCI-Monitoring aktivieren

Das Active IQ-Storage-Monitoring für das Computing-Monitoring von NetApp HCI und NetApp HCI lässt sich aktivieren, falls dies bei der Installation oder einem Upgrade nicht bereits geschehen war. Wenn Sie die Telemetrie mithilfe der NetApp HCI Deployment Engine deaktiviert haben, müssen Sie dieses Verfahren möglicherweise verwenden.

Der Active IQ Collector Service leitet Konfigurationsdaten und softwarebasierte Element Cluster-Performance-Kennzahlen an NetApp Active IQ weiter, um historische Berichte zu erstellen und Performance-Monitoring nahezu in Echtzeit zu ermöglichen. Der NetApp HCI Monitoring Service ermöglicht die Weiterleitung von Storage-Cluster-Fehlern an vCenter zur Alarmbenachrichtigung.

Bevor Sie beginnen

- Im Storage Cluster wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.
- Sie haben Internetzugang. Der Active IQ Collector Service kann nicht von dunklen Standorten verwendet werden, die keine externe Verbindung haben.

Schritte

1. Holen Sie sich die Basis-Asset-ID für die Installation:
   a. Öffnen Sie die REST API-UI für den Bestandsdienst auf dem Managementknoten:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Klicken Sie auf **autorisieren** und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Fenster.
   c. Klicken Sie in DER REST API UI auf **GET /Installations**.
   d. Klicken Sie auf **Probieren Sie es aus**.
   e. Klicken Sie Auf **Ausführen**.
   f. Kopieren Sie aus dem Text Code 200 Antwort den `id` Für die Installation.

```
{
  "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",
```

Die Installation verfügt über eine Basiskonfiguration, die während der Installation oder eines Upgrades erstellt wurde.

2. Telemetrie aktivieren:
   a. Rufen Sie die mNode-Service-API-UI auf dem Management-Node auf, indem Sie die Management-Node-IP-Adresse, gefolgt von eingeben `/mnode`:

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

   b. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Fenster.
   c. Konfigurieren der BasisinAssets:
      i. Klicken Sie auf **PUT /Assets/{Asset_id}**.
      ii. Klicken Sie auf **Probieren Sie es aus**.
      iii. Geben Sie die folgende in die JSON-Nutzlast ein:

```
{
"telemetry_active": true
"config": {}
}
```

      iv. Geben Sie die Basis-ID des vorherigen Schritts in **Asset_ID** ein.
      v. Klicken Sie Auf **Ausführen**.

      Der Active IQ Service wird automatisch neu gestartet, sobald die Assets geändert werden. Das Ändern von Anlagen führt zu einer kurzen Verzögerung, bevor Einstellungen angewendet werden.

3. Wenn dies noch nicht der Fall ist, fügen Sie dem Management-Node bekannte Assets, die als Management-Node bekannt sind, eine vCenter-Controller-Ressource für das NetApp HCI-Monitoring (nur NetApp HCI-Installationen) und Hybrid Cloud Control (für alle Installationen) hinzu:

   Für NetApp HCI Monitoring Services ist ein Controller-Asset erforderlich.

   a. Klicken Sie auf **POST /Assets/{Asset_id}/Controllers**, um eine Unterressource des Controllers hinzuzufügen.
   b. Klicken Sie auf **Probieren Sie es aus**.
   c. Geben Sie im Feld **Asset_id** die ID der übergeordneten Basis ein, die Sie in die Zwischenablage kopiert haben.
   d. Geben Sie die erforderlichen Nutzlastwerte mit ein `type` Als `vCenter` Und vCenter Zugangsdaten.

```
{
"username": "string",
"password": "string",
"ip": "string",
"type": "vCenter",
"host_name": "string",
"config": {}
}
```

   `ip` Ist die vCenter IP-Adresse.

   e. Klicken Sie Auf **Ausführen**.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Konfiguration von NetApp Hybrid Cloud Control für mehrere vCenter

Sie können NetApp Hybrid Cloud Control so konfigurieren, dass Assets von zwei oder mehr vCenters gemanagt werden, die nicht den verknüpften Modus verwenden.

Sie sollten diesen Prozess nach der Erstinstallation verwenden, wenn Sie Assets für eine kürzlich skalierte Installation hinzufügen müssen oder wenn Ihre Konfiguration nicht automatisch neue Assets hinzugefügt wurde. Mithilfe dieser APIs können Sie Ressourcen hinzufügen, die zu Ihrer Installation hinzugefügt wurden.

Was Sie benötigen

- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.

Schritte

1. "Fügen Sie neue vCenters als Controller Assets hinzu" Für die Konfiguration des Management-Node.

2. "Hinzufügen neuer Computing-Nodes als Computing-Ressourcen" Für die Konfiguration des Management-Node.

> Möglicherweise müssen Sie es "Ändern der BMC-Zugangsdaten für Computing-Nodes" Um ein aufzulösen `Hardware ID not available` Oder `Unable to Detect` Der Fehler wird unter NetApp Hybrid Cloud Control gemeldet.

3. Aktualisieren Sie die BestandsdienstAPI auf dem Managementknoten:

```
https://<ManagementNodeIP>/inventory/1/
```

> Alternativ können Sie 2 Minuten warten, bis der Bestand in der Benutzeroberfläche von NetApp Hybrid Cloud Control aktualisiert wird.

   a. Klicken Sie auf **autorisieren** und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Fenster.
   b. Klicken Sie in DER REST API UI auf **GET /Installations**.
   c. Klicken Sie auf **Probieren Sie es aus**.
   d. Klicken Sie Auf **Ausführen**.
   e. Kopieren Sie als Antwort die Installations-Asset-ID (`"id"`).
   f. Klicken Sie in DER REST API-UI auf **GET /Installations/{id}**.
   g. Klicken Sie auf **Probieren Sie es aus**.
   h. Stellen Sie „Aktualisieren“ auf fest `True`.
   i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.
   j. Klicken Sie Auf **Ausführen**.
4. Aktualisieren Sie den Browser NetApp Hybrid Cloud Control, um die Änderungen anzuzeigen.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Fügen Sie dem Management-Node Computing- und Controller-Ressourcen hinzu

Über DIE REST API UI lassen sich Compute- und Controller-Ressourcen zur Management-Node-Konfiguration hinzufügen.

Möglicherweise müssen Sie ein Asset hinzufügen, wenn Sie vor Kurzem Ihre Installation skaliert haben und neue Ressourcen nicht automatisch zu Ihrer Konfiguration hinzugefügt wurden. Mithilfe dieser APIs können Sie Ressourcen hinzufügen, die zu Ihrer Installation hinzugefügt wurden.

Was Sie benötigen

- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.
- Das ist schon "Neue NetApp HCC-Rolle in vCenter erstellt" Begrenzung der Management-Node-Services-Ansicht auf reine NetApp Ressourcen
- Sie verfügen über die vCenter-Management-IP-Adresse und die zugehörigen Anmeldedaten.
- Sie haben die Management-IP-Adresse und die Root-Anmeldedaten des Computing-Nodes (ESXi).
- Sie verfügen über die Hardware- (BMC) Management-IP-Adresse und Administrator-Anmeldeinformationen.

Über diese Aufgabe

(Nur NetApp HCI) Wenn nach der Skalierung Ihres NetApp HCI-Systems keine Computing-Nodes in der Hybrid Cloud Control (HCC) angezeigt werden, können Sie mithilfe der einen Compute-Node hinzufügen `POST /assets/{asset_id}/compute-nodes` Beschrieben in diesem Verfahren.

Wenn Sie Computing-Knoten manuell hinzufügen, stellen Sie sicher, dass Sie auch die BMC-Assets hinzufügen. Andernfalls wird ein Fehler zurückgegeben.

Schritte

1. Holen Sie sich die Basis-Asset-ID für die Installation:
   a. Öffnen Sie die REST API-UI für den Bestandsdienst auf dem Managementknoten:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als ein `mnode-client`.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Fenster.
   c. Wählen Sie in DER REST API UI **GET /Installations** aus.
   d. Wählen Sie **Probieren Sie es aus**.
   e. Wählen Sie **Ausführen**.
   f. Kopieren Sie aus dem Text Code 200 Antwort den `id` Für die Installation.

```
{
  "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",
```

Die Installation verfügt über eine Basiskonfiguration, die während der Installation oder eines Upgrades erstellt wurde.

g. Wählen Sie in DER REST-API-UI **GET /installations/{id}** aus.
h. Wählen Sie **Probieren Sie es aus**.
i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.
j. Wählen Sie **Ausführen**.
k. Kopieren Sie aus der Antwort die Cluster-Controller-ID und speichern Sie sie (`"controllerId"`) Für den Einsatz in einem späteren Schritt.

2. (Nur für Computing-Nodes) Suchen Sie die Hardware-Tag-Nummer für Ihren Compute-Node In vSphere.
3. Um einer vorhandenen Basisressource ein Controller Asset (vCenter), einen Computing Node (ESXi) oder eine Hardware (BMC) hinzuzufügen, wählen Sie eine der folgenden Optionen aus:

Option	Beschreibung
POST /Assets/{Asset_id}/Controller	a. Öffnen Sie die MNODE-Service-REST-API-UI auf dem Management-Node: `https://<ManagementNodeIP>/mnode` i. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus: A. Geben Sie den Benutzernamen und das Passwort für den Cluster ein. B. Geben Sie die Client-ID als ein `mnode-client`. C. Wählen Sie **autorisieren**, um eine Sitzung zu starten. D. Schließen Sie das Fenster. b. Wählen Sie **POST /Assets/{Asset_id}/Controllers** aus. c. Wählen Sie **Probieren Sie es aus**. d. Geben Sie die übergeordnete Basis-Asset-ID in das Feld **Asset_id** ein. e. Fügen Sie die erforderlichen Werte der Nutzlast hinzu. f. Wählen Sie **Ausführen**.

Option	Beschreibung
POST /Assets/{Asset_id}/Compute-Nodes	a. Öffnen Sie die MNODE-Service-REST-API-UI auf dem Management-Node: `https://<ManagementNodeIP>/mnode` i. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus: A. Geben Sie den Benutzernamen und das Passwort für den Cluster ein. B. Geben Sie die Client-ID als ein `mnode-client`. C. Wählen Sie **autorisieren**, um eine Sitzung zu starten. D. Schließen Sie das Fenster. b. Wählen Sie **POST /Assets/{Asset_id}/Compute-Nodes** aus. c. Wählen Sie **Probieren Sie es aus**. d. Geben Sie im Feld **Asset_id** die übergeordnete Basis-Asset-ID ein, die Sie in einem früheren Schritt kopiert haben. e. Führen Sie in der Nutzlast folgende Schritte aus: i. Geben Sie die Management-IP für den Node im ein `ip` Feld. ii. Für `hardwareTag`Geben Sie den Hardware-Tag-Wert ein, den Sie in einem früheren Schritt gespeichert haben. iii. Geben Sie bei Bedarf andere Werte ein. f. Wählen Sie **Ausführen**.

Option	Beschreibung
POST /Assets/{Asset_id}/Hardware-Nodes	a. Öffnen Sie die MNODE-Service-REST-API-UI auf dem Management-Node: `https://<ManagementNodeIP>/mnode` i. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus: A. Geben Sie den Benutzernamen und das Passwort für den Cluster ein. B. Geben Sie die Client-ID als ein `mnode-client`. C. Wählen Sie **autorisieren**, um eine Sitzung zu starten. D. Schließen Sie das Fenster. b. Wählen Sie **POST /Assets/{Asset_id}/Hardware-Nodes** aus. c. Wählen Sie **Probieren Sie es aus**. d. Geben Sie die übergeordnete Basis-Asset-ID in das Feld **Asset_id** ein. e. Fügen Sie die erforderlichen Werte der Nutzlast hinzu. f. Wählen Sie **Ausführen**.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

So finden Sie ein Hardware-Tag für einen Compute-Node

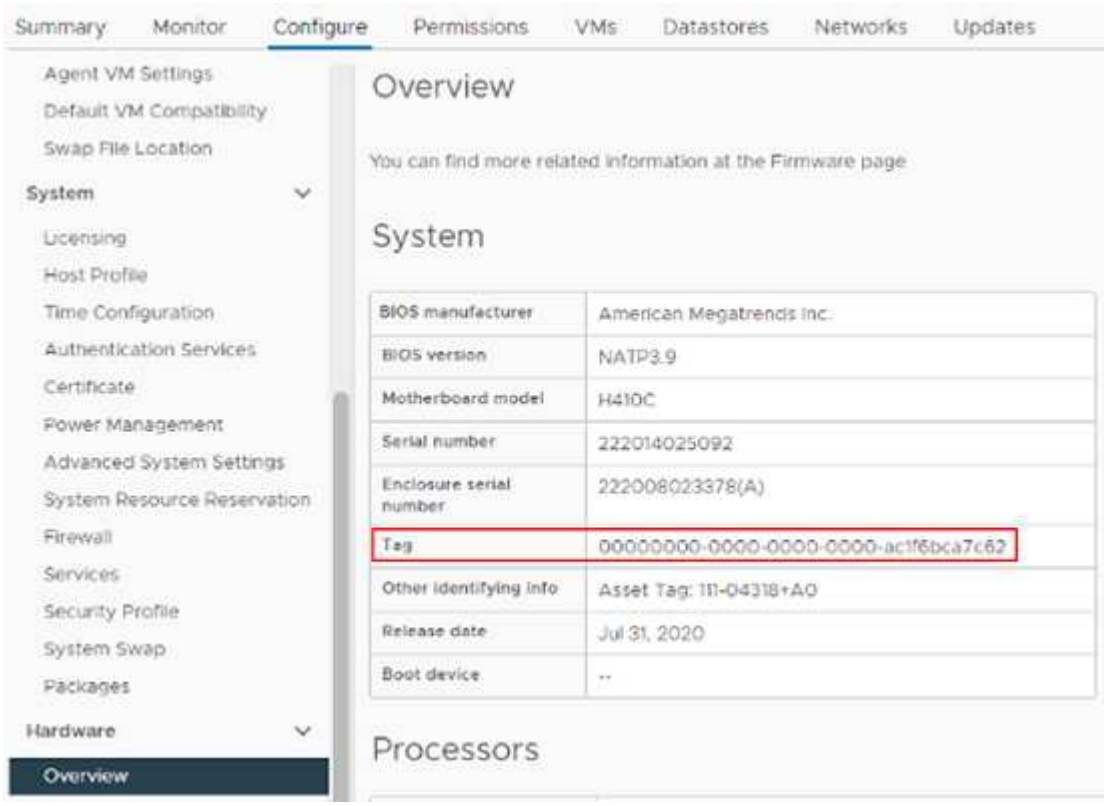
Mithilfe der REST API-Benutzeroberfläche müssen Sie die Hardware-Tag-Nummer zur Konfiguration der Managementknoten hinzufügen.

VMware vSphere 8.0 und 7.0

Suchen Sie in VMware vSphere Web Client 8.0 und 7.0 das Hardware-Tag für einen Computing-Knoten.

Schritte

1. Wählen Sie den Host im vSphere Web Client Navigator aus.
2. Wählen Sie die Registerkarte **Konfigurieren** aus.
3. Wählen Sie in der Seitenleiste die Option **Hardware** > **Übersicht**. Überprüfen Sie, ob die Hardware-Tag-Nummer im aufgeführt ist `System` Tabelle:



4. Kopieren und speichern Sie den Wert für **Tag**.
5. Fügen Sie Ihre Computing- und Controller-Ressourcen dem Management-Node hinzu.

VMware vSphere 6.7 und 6.5

Suchen Sie in VMware vSphere Web Client 6.7 und 6.5 das Hardware-Tag für einen Computing-Knoten.

Schritte

1. Wählen Sie den Host im vSphere Web Client Navigator aus.
2. Wählen Sie die Registerkarte **Monitor** aus und wählen Sie **Hardwarezustand**.
3. Überprüfen Sie, ob das Tag mit dem BIOS-Hersteller und der Modellnummer aufgelistet ist.

4. Kopieren und speichern Sie den Wert für **Tag**.
5. Fügen Sie Ihre Computing- und Controller-Ressourcen dem Management-Node hinzu.

Erstellen und Managen von Storage-Cluster-Assets

Sie können dem Managementknoten neue Storage-Cluster-Assets hinzufügen, die gespeicherten Zugangsdaten für bekannte Storage-Cluster-Assets bearbeiten und Storage-Cluster-Assets über DIE REST-API vom Managementknoten löschen.

Was Sie benötigen

- Stellen Sie sicher, dass auf Ihrer Speichercluster-Version die NetApp Element-Software 11.3 oder höher ausgeführt wird.
- Stellen Sie sicher, dass Sie einen Management-Node mit Version 11.3 oder höher bereitgestellt haben.

Optionen für das Storage Cluster Asset Management

Wählen Sie eine der folgenden Optionen:

- Rufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab
- Fügen Sie eine neue Storage-Cluster-Ressource hinzu
- Bearbeiten Sie die gespeicherten Anmeldedaten für eine Storage-Cluster-Ressource
- Löschen einer Speichercluster-Ressource

Rufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab

Sie können die REST API verwenden, um die Installations-ID und die ID des Storage-Clusters zu erhalten. Sie benötigen die Installations-ID, um eine neue Storage Cluster-Ressource hinzuzufügen, und die Cluster-ID, um eine bestimmte Storage-Cluster-Ressource zu ändern oder zu löschen.

Schritte

1. Greifen Sie auf die REST-API-UI für den Bestandsdienst zu, indem Sie die IP-Adresse des Management-Node gefolgt von eingeben `/inventory/1/`:

```
https://<ManagementNodeIP>/inventory/1/
```

2. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Klicken Sie auf **GET /Installations**.
4. Klicken Sie auf **Probieren Sie es aus**.
5. Klicken Sie Auf **Ausführen**.

   Die API gibt eine Liste aller bekannten Installationen zurück.

6. Speichern Sie aus dem Code 200 Response Body den Wert im `id` Feld, das Sie in der Liste der Installationen finden können. Dies ist die Installations-ID. Beispiel:

```
"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. Rufen Sie die REST-API-UI für den Storage-Service auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

8. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
9. Klicken Sie auf **GET /Clusters**.
10. Klicken Sie auf **Probieren Sie es aus**.
11. Geben Sie die Installations-ID ein, die Sie zuvor in gespeichert haben `installationId` Parameter.
12. Klicken Sie Auf **Ausführen**.

    Die API gibt eine Liste aller bekannten Storage-Cluster in dieser Installation zurück.

13. Suchen Sie aus dem Code 200 Response Body den richtigen Storage Cluster und speichern Sie den Wert im Cluster `storageId` Feld. Dies ist die Storage-Cluster-ID.

Fügen Sie eine neue Storage-Cluster-Ressource hinzu

Mithilfe der REST API können Sie dem Management-Node-Bestand eine oder mehrere neue Storage-Cluster-Ressourcen hinzufügen. Wenn Sie eine neue Storage-Cluster-Ressource hinzufügen, wird diese automatisch beim Management-Node registriert.

Was Sie benötigen

- Sie haben die kopiert Storage Cluster-ID und Installations-ID Für jeden Storage-Cluster, den Sie hinzufügen möchten.
- Wenn Sie mehr als einen Storage-Node hinzufügen, haben Sie die Einschränkungen von gelesen und verstanden "Autorisierende Cluster" Unterstützung für mehrere Storage-Cluster.

> Alle im autoritären Cluster definierten Benutzer werden als Benutzer auf allen anderen Clustern definiert, die an die Instanz von Hybrid Cloud Control gebunden sind.

Schritte

1. Rufen Sie die REST-API-UI für den Storage-Service auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/storage/1/`:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

2. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Klicken Sie auf **POST /Cluster**.
4. Klicken Sie auf **Probieren Sie es aus**.
5. Geben Sie im Feld **Text anfordern** die Informationen des neuen Speicherclusters in die folgenden Parameter ein:

   ```
   {
     "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
     "mvip": "10.0.0.1",
     "password": "admin",
     "userId": "admin"
   }
   ```

Parameter	Typ	Beschreibung
`installationId`	Zeichenfolge	Die Installation, in der der neue Speicher-Cluster hinzugefügt werden soll. Geben Sie die Installations-ID ein, die Sie zuvor in diesen Parameter gespeichert haben.
`mvip`	Zeichenfolge	Die virtuelle IPv4-Management-IP-Adresse (MVIP) des Speicherclusters.
`password`	Zeichenfolge	Das Passwort, das für die Kommunikation mit dem Storage-Cluster verwendet wird.
`userId`	Zeichenfolge	Die Benutzer-ID für die Kommunikation mit dem Speicher-Cluster (der Benutzer muss über Administratorrechte verfügen).

6. Klicken Sie Auf **Ausführen**.

   Die API gibt ein Objekt mit Informationen über die neu hinzugefügte Storage-Cluster-Ressource zurück, z. B. Informationen über Name, Version und IP-Adresse.

Bearbeiten Sie die gespeicherten Anmeldedaten für eine Storage-Cluster-Ressource

Sie können die gespeicherten Anmeldeinformationen bearbeiten, die der Management-Node zur Anmeldung bei einem Storage-Cluster verwendet. Der von Ihnen gewählte Benutzer muss über einen Cluster-Admin-Zugriff verfügen.

Vergewissern Sie sich, dass Sie die Schritte in befolgt haben Rufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab Bevor Sie fortfahren.

Schritte

1. Rufen Sie die REST-API-UI für den Storage-Service auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/storage/1/`:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

2. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Klicken Sie auf **PUT /Clusters/{storageId}**.
4. Klicken Sie auf **Probieren Sie es aus**.

5. Fügen Sie die Storage-Cluster-ID ein, die Sie zuvor in kopiert haben `storageId` Parameter.
6. Ändern Sie im Feld **Text anfordern** einen oder beide der folgenden Parameter:

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

Parameter	Typ	Beschreibung
`password`	Zeichenfolge	Das Passwort, das für die Kommunikation mit dem Storage-Cluster verwendet wird.
`userId`	Zeichenfolge	Die Benutzer-ID für die Kommunikation mit dem Speicher-Cluster (der Benutzer muss über Administratorrechte verfügen).

7. Klicken Sie Auf **Ausführen**.

Löschen einer Speichercluster-Ressource

Sie können eine Storage-Cluster-Ressource löschen, wenn das Storage-Cluster nicht mehr in Betrieb ist. Wenn Sie eine Storage-Cluster-Ressource entfernen, wird diese automatisch vom Management-Node registriert.

Vergewissern Sie sich, dass Sie die Schritte in befolgt haben Rufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab Bevor Sie fortfahren.

Schritte

1. Rufen Sie die REST-API-UI für den Storage-Service auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Klicken Sie auf **DELETE /Clusters/{storageId}**.
4. Klicken Sie auf **Probieren Sie es aus**.
5. Geben Sie die Storage-Cluster-ID ein, die Sie zuvor in kopiert haben `storageId` Parameter.
6. Klicken Sie Auf **Ausführen**.

Bei Erfolg gibt die API eine leere Antwort zurück.

Weitere Informationen

- "Autorisierende Cluster"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Vorhandene Controller-Assets können angezeigt oder bearbeitet werden

Sie können Informationen zu vorhandenen VMware vCenter Controllern in der Management-Node-Konfiguration über DIE REST-API anzeigen und bearbeiten. Controller sind VMware vCenter Instanzen, die bei Ihrer NetApp HCI Installation auf dem Management-Node registriert sind.

Bevor Sie beginnen

- Stellen Sie sicher, dass auf Ihrer Cluster-Version NetApp Element 11.3 oder höher ausgeführt wird.
- Stellen Sie sicher, dass Sie einen Management-Node mit Version 11.3 oder höher bereitgestellt haben.

Zugriff auf DIE REST-API für Managementservices

Schritte

1. Rufen Sie die REST-API-UI für Managementservices auf, indem Sie die IP-Adresse des Management-Node gefolgt von eingeben `/vcenter/1/`:

   ```
   https://<ManagementNodeIP>/vcenter/1/
   ```

2. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.

Anzeigen gespeicherter Informationen zu vorhandenen Controllern

Sie können vorhandene vCenter Controller, die beim Management-Node registriert sind, auflisten und gespeicherte Informationen über sie mithilfe der REST-API anzeigen.

Schritte

1. Klicken Sie auf **GET /Compute/Controllers**.
2. Klicken Sie auf **Probieren Sie es aus**.
3. Klicken Sie Auf **Ausführen**.

   Die API gibt eine Liste aller bekannten vCenter-Controller sowie die IP-Adresse, Controller-ID, Hostname und Benutzer-ID zurück, die für die Kommunikation mit jedem Controller verwendet wurden.

4. Wenn Sie den Verbindungsstatus eines bestimmten Controllers möchten, kopieren Sie die Controller-ID von `id` Feld dieses Controllers in der Zwischenablage und siehe Den Status eines vorhandenen Controllers anzeigen.

Den Status eines vorhandenen Controllers anzeigen

Sie können den Status aller vorhandenen vCenter Controller anzeigen, die beim Management-Node registriert sind. Die API gibt einen Status zurück, der angibt, ob NetApp Hybrid Cloud Control sich sowohl mit dem vCenter Controller verbinden kann als auch mit dem Grund für diesen Status.

Schritte

1. Klicken Sie auf **GET /Compute/Controllers/{Controller_id}/Status**.
2. Klicken Sie auf **Probieren Sie es aus**.
3. Geben Sie die Controller-ID ein, die Sie zuvor in kopiert haben `controller_id` Parameter.
4. Klicken Sie Auf **Ausführen**.

   Die API gibt einen Status dieses bestimmten vCenter-Controllers zurück, zusammen mit einem Grund für diesen Status.

Bearbeiten Sie die gespeicherten Eigenschaften eines Controllers

Sie können den gespeicherten Benutzernamen oder das gespeicherte Passwort für einen der vorhandenen vCenter Controller bearbeiten, die beim Management-Node registriert sind. Sie können die gespeicherte IP-Adresse eines vorhandenen vCenter-Controllers nicht bearbeiten.

Schritte

1. Klicken Sie auf **PUT /Compute/Controllers/{Controller_id}**.
2. Geben Sie die Controller-ID eines vCenter Controllers in ein `controller_id` Parameter.
3. Klicken Sie auf **Probieren Sie es aus**.
4. Ändern Sie einen der folgenden Parameter im Feld **Text anfordern**:

Parameter	Typ	Beschreibung
`userId`	Zeichenfolge	Ändern Sie die Benutzer-ID, die für die Kommunikation mit dem vCenter Controller verwendet wird (der Benutzer muss über Administratorrechte verfügen).
`password`	Zeichenfolge	Ändern Sie das Passwort, das für die Kommunikation mit dem vCenter Controller verwendet wird.

5. Klicken Sie Auf **Ausführen**.

   Die API gibt aktualisierte Controller-Informationen zurück.

Weitere Informationen

- "Fügen Sie dem Management-Node Computing- und Controller-Ressourcen hinzu"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Entfernen Sie ein Asset vom Management-Node

Wenn ein Computing-Node physisch ersetzt oder aus dem NetApp HCI-Cluster entfernt werden muss, müssen die Computing-Node-Ressource mithilfe der Management-Node-APIs entfernt werden.

Was Sie benötigen

- Im Storage Cluster wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.

Schritte

1. Geben Sie die Management-Node-IP-Adresse gefolgt von ein `/mnode/1/`:

   ```
   https://<ManagementNodeIP>/mnode/1/
   ```

2. Klicken Sie auf **autorisieren** oder auf ein Schlosssymbol und geben Sie Cluster Admin-Anmeldeinformationen ein, um APIs zu verwenden.
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Wählen Sie **Text anfordern** aus der Dropdown-Liste Typ aus, wenn der Wert nicht bereits ausgewählt ist.
   c. Geben Sie die Client-ID als ein `mnode-client` Wenn der Wert nicht bereits ausgefüllt ist.
   d. Geben Sie keinen Wert für das Clientgeheimnis ein.
   e. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
   f. Schließen Sie das Fenster.
3. Schließen Sie das Dialogfeld * Verfügbare Berechtigungen*.
4. Klicken Sie auf **GET/Assets**.
5. Klicken Sie auf **Probieren Sie es aus**.
6. Klicken Sie Auf **Ausführen**.
7. Scrollen Sie im Antwortkörper nach unten zum Abschnitt **Computing**, und kopieren Sie den `parent` Und `id` Werte für den fehlgeschlagenen Rechenknoten.
8. Klicken Sie auf **DELETE/Assets/{Asset_id}/Compute-Nodes/{Compute_id}**.
9. Klicken Sie auf **Probieren Sie es aus**.
10. Geben Sie das ein `parent` Und `id` Werte, die Sie in einem vorherigen Schritt kopiert haben.
11. Klicken Sie Auf **Ausführen**.

Konfigurieren Sie einen Proxyserver

Wenn Ihr Cluster hinter einem Proxy-Server liegt, müssen Sie die Proxy-Einstellungen so

konfigurieren, dass Sie ein öffentliches Netzwerk erreichen können.

Für Telemetrie-Kollektoren und Reverse-Tunnel-Verbindungen wird ein Proxy-Server verwendet. Sie können einen Proxy-Server mithilfe der REST API-UI aktivieren und konfigurieren, falls Sie während der Installation oder dem Upgrade noch keinen Proxy-Server konfiguriert haben. Sie können auch vorhandene Proxy-Server-Einstellungen ändern oder einen Proxy-Server deaktivieren.

Der Befehl zum Konfigurieren von Updates für einen Proxy-Server und gibt dann die aktuellen Proxy-Einstellungen für den Management-Node zurück. Die Proxy-Einstellungen werden von Active IQ, dem NetApp HCI Monitoring-Service, der von der NetApp Deployment Engine implementiert wird, und anderen Element Software Utilities verwendet, die auf dem Management-Node installiert sind. Hierzu gehören auch der Tunnel zur Reverse-Unterstützung für NetApp Support.

Bevor Sie beginnen

- Sie sollten Host- und Anmeldeinformationen für den Proxyserver kennen, den Sie konfigurieren.
- Stellen Sie sicher, dass auf Ihrer Cluster-Version NetApp Element 11.3 oder höher ausgeführt wird.
- Stellen Sie sicher, dass Sie einen Management-Node mit Version 11.3 oder höher bereitgestellt haben.
- (Management-Node 12.0 und höher) vor der Konfiguration eines Proxy-Servers haben Sie die NetApp Hybrid Cloud Control auf die Managementservices Version 2.16 aktualisiert.

Schritte

1. Greifen Sie auf die REST-API-UI auf dem Management-Node zu, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode`:

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

2. Klicken Sie auf **autorisieren** oder auf ein Schloss-Symbol, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Klicken Sie auf **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Klicken Sie auf **PUT /settings**.
4. Klicken Sie auf **Probieren Sie es aus**.
5. Um einen Proxyserver zu aktivieren, müssen Sie festlegen `use_proxy` Um wahr zu sein. Geben Sie die IP- oder Host-Namen und Proxy-Port-Ziele ein.

   Der Proxy-Benutzername, das Proxy-Passwort und der SSH-Port sind optional und sollten bei Nichtverwendung weggelassen werden.

```
{
"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. Klicken Sie Auf **Ausführen**.

Je nach Umgebung müssen Sie möglicherweise Ihren Management Node neu booten.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Überprüfen Sie die Betriebssystem- und Servicestversionen der Management-Nodes

Sie können die Versionsnummern des Management-Node-Betriebssystems, des Managementservices-Pakets und der einzelnen Services, die auf dem Management-Node ausgeführt werden, mithilfe der REST-API im Management-Node überprüfen.

Was Sie benötigen

- Auf dem Cluster wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.

Optionen

- API-Befehle
- SCHRITTE DER REST API-UI

API-Befehle

- Hier erhalten Sie Versionsinformationen zum Management-Node OS, zum Management-Services-Bundle und zum Management-Node-API-Service (mNode-API), der auf dem Management-Node ausgeführt wird:

```
curl -X GET "https://<ManagementNodeIP>/mnode/about" -H  "accept:
application/json"
```

- Abrufen der Versionsinformationen zu den einzelnen auf dem Management-Node ausgeführten Services:

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running"
-H  "accept: */*" -H  "Authorization: Bearer ${TOKEN}"
```

Ihr könnt den Träger finden `${TOKEN}` Wird von dem API-Befehl verwendet, wenn Sie "Autorisieren". Der Träger `${TOKEN}` Ist in der Curl-Antwort.

SCHRITTE DER REST API-UI

1. Rufen Sie die REST-API-UI für den Service auf, indem Sie die Management-Node-IP-Adresse, gefolgt von, eingeben `/mnode/`:

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

2. Führen Sie einen der folgenden Schritte aus:
   - Hier erhalten Sie Versionsinformationen zum Management-Node OS, zum Management-Services-Bundle und zum Management-Node-API-Service (mNode-API), der auf dem Management-Node ausgeführt wird:
     i. Wählen Sie **GET /about** aus.
     ii. Wählen Sie **Probieren Sie es aus**.
     iii. Wählen Sie **Ausführen**.

     Die Bundle-Version der Managementservices (`"mnode_bundle_version"`), Version des Management-Node-Betriebssystems (`"os_version"`) Und der Version der Management-Node-API (`"version"`) Sind im Antwortkörper angegeben.
   - Abrufen der Versionsinformationen zu den einzelnen auf dem Management-Node ausgeführten Services:
     i. Wählen Sie **GET /Services**.
     ii. Wählen Sie **Probieren Sie es aus**.
     iii. Wählen Sie den Status als **läuft** aus.
     iv. Wählen Sie **Ausführen**.

     Die Dienste, die auf dem Management-Knoten ausgeführt werden, werden im Response Body angezeigt.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Abrufen von Protokollen von Managementservices

Sie können mithilfe der REST API Protokolle von den Services abrufen, die auf dem Management-Node ausgeführt werden. Sie können Protokolle aus allen öffentlichen Diensten abrufen oder bestimmte Dienste angeben und Abfrageparameter verwenden, um die Rückgabeergebnisse besser zu definieren.

Was Sie benötigen

- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.

Schritte

1. Öffnen Sie die REST-API-UI auf dem Managementknoten.
   - Ab Management Services 2.21.61:

     ```
     https://<ManagementNodeIP>/mnode/4/
     ```

   - Für Managementservices ab Version 2.20.69:

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

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als mNode-Client ein, wenn der Wert nicht bereits gefüllt ist.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **GET /logs**.
4. Wählen Sie **Probieren Sie es aus**.
5. Geben Sie die folgenden Parameter an:
   - `Lines`: Geben Sie die Anzahl der Zeilen ein, die das Protokoll zurückgeben soll. Bei diesem Parameter handelt es sich um eine Ganzzahl, die standardmäßig auf 1000 gesetzt ist.

     Vermeiden Sie es, den gesamten Verlauf des Protokollinhalts anzufragen, indem Sie Zeilen auf 0 setzen.

   - `since`: Fügt einen ISO-8601-Zeitstempel für den Startpunkt der Service-Protokolle hinzu.

     Machen Sie einen vernünftigen Rahmen `since` Parameter beim Sammeln von Protokollen mit größeren Zeitpfannen.

   - `service-name`: Geben Sie einen Dienstnamen ein.

     Verwenden Sie die `GET /services` Befehl zum Auflisten von Services auf dem Management-Node.

   - `stopped`: Auf eingestellt `true` Um Protokolle von angehalten Diensten abzurufen.
6. Wählen Sie **Ausführen**.
7. Wählen Sie im Antwortkörper **Download** aus, um die Protokollausgabe zu speichern.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Managen von Supportverbindungen

Starten Sie eine Remote NetApp Support Sitzung

Wenn Sie technischen Support für Ihr NetApp HCI System benötigen, kann sich der NetApp Support per Fernzugriff mit Ihrem System verbinden. Um eine Sitzung zu starten und Remote-Zugriff zu erhalten, kann der NetApp Support eine Reverse Secure Shell-(SSH)-Verbindung zu Ihrer Umgebung öffnen.

Sie können einen TCP-Port für eine SSH-Reverse-Tunnel-Verbindung mit NetApp Support öffnen. Über diese Verbindung kann sich NetApp Support beim Management Node einloggen.

Bevor Sie beginnen

- Für Managementservices ab Version 2.18 ist die Möglichkeit für den Remote-Zugriff auf dem Management-Node standardmäßig deaktiviert. Informationen zum Aktivieren der Fernzugriffsfunktionen finden Sie unter "Verwalten der SSH-Funktionalität auf dem Management-Node".
- Wenn sich der Managementknoten hinter einem Proxyserver befindet, sind die folgenden TCP-Ports in der Datei sshd.config erforderlich:

TCP-Port	Beschreibung	Verbindungsrichtung
443	API-Aufrufe/HTTPS zur Umkehrung der Port-Weiterleitung über offenen Support-Tunnel zur Web-UI	Management-Node zu Storage-Nodes
22	SSH-Login-Zugriff	Management-Node zu Storage-Nodes oder von Storage-Nodes zum Management-Node

Schritte

- Melden Sie sich bei Ihrem Management-Knoten an und öffnen Sie eine Terminalsitzung.
- Geben Sie an einer Eingabeaufforderung Folgendes ein:

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- Um den Remote Support-Tunnel zu schließen, geben Sie Folgendes ein:

```
rst --killall
```

- (Optional) Deaktivieren "Remote-Zugriffsfunktion" Ein weiteres Jahr in der

> SSH bleibt aktiviert, wenn Sie ihn nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Node durch Updates und Upgrades bestehen, bis sie manuell deaktiviert ist.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Verwalten der SSH-Funktionalität auf dem Management-Node

Sie können den Status der SSH-Funktion auf dem Management-Node (mNode) mithilfe der REST-API deaktivieren, neu aktivieren oder bestimmen. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Knoten, die Management-Services 2.18 oder höher ausführen, standardmäßig deaktiviert.

Ab Management Services 2.20.69 können Sie die SSH-Funktion auf dem Management-Node über die NetApp Hybrid Cloud Control UI aktivieren und deaktivieren.

Was Sie benötigen

- **NetApp Hybrid Cloud Control Berechtigungen**: Sie haben Berechtigungen als Administrator.
- **Cluster Administrator Berechtigungen**: Sie haben Berechtigungen als Administrator auf dem Speicher-Cluster.
- **Element Software**: Auf Ihrem Cluster läuft die NetApp Element Software 11.3 oder höher.
- **Management-Node**: Sie haben einen Management-Node mit Version 11.3 oder höher bereitgestellt.
- **Aktualisierungen von Managementservices**:
  - Um die NetApp Hybrid Cloud Control UI zu verwenden, haben Sie Ihr aktualisiert "Management Services-Bundle" Auf Version 2.20.69 oder höher.
  - Um die REST API-UI zu verwenden, haben Sie das aktualisiert "Management Services-Bundle" Auf Version 2.17.

Optionen

- Deaktivieren oder aktivieren Sie die SSH-Funktion auf dem Management-Node mithilfe der NetApp Hybrid Cloud Control UI

Nach der Durchführung können Sie eine der folgenden Aufgaben ausführen "Authentifizierung":

- Deaktiviert bzw. aktiviert die SSH-Funktion auf dem Management-Node mithilfe von APIs
- Ermitteln des Status der SSH-Funktion auf dem Management-Node mithilfe von APIs

Deaktivieren oder aktivieren Sie die SSH-Funktion auf dem Management-Node mithilfe der NetApp Hybrid Cloud Control UI

Sie können die SSH-Funktion auf dem Management-Node deaktivieren oder neu aktivieren. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Knoten, die Management-Services 2.18 oder höher ausführen, standardmäßig deaktiviert. Durch Deaktivieren von SSH werden vorhandene SSH-Client-Sessions nicht zum Management-Node beendet oder getrennt. Wenn Sie SSH deaktivieren und sich zu einem späteren Zeitpunkt erneut aktivieren, können Sie dazu die Benutzeroberfläche von NetApp Hybrid Cloud Control verwenden.

Um den Support-Zugriff über SSH für ein Storage-Cluster zu aktivieren oder zu deaktivieren, müssen Sie die verwenden "Seite „Cluster-Einstellungen für Element UI“".

Schritte

1. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.
2. Schalten Sie im Bildschirm **Support Access for Management Node** den Switch ein, um den Management-Node SSH zu aktivieren.
3. Nach Abschluss der Fehlerbehebung schalten Sie im Bildschirm **Support Access for Management Node** den Switch ein, um SSH des Management-Node zu deaktivieren.

Deaktiviert bzw. aktiviert die SSH-Funktion auf dem Management-Node mithilfe von APIs

Sie können die SSH-Funktion auf dem Management-Node deaktivieren oder neu aktivieren. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Knoten, die Management-Services 2.18 oder höher ausführen, standardmäßig deaktiviert. Durch Deaktivieren von SSH werden vorhandene SSH-Client-Sessions nicht zum Management-Node beendet oder getrennt. Wenn Sie SSH deaktivieren und sich für eine spätere erneute Aktivierung entscheiden, können Sie dies über dieselbe API tun.

API-Befehl

Für Management Services 2.18 oder höher:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Für Managementservices ab Version 2.17:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Ihr könnt den Träger finden `${TOKEN}` Wird von dem API-Befehl verwendet, wenn Sie "Autorisieren". Der Träger `${TOKEN}` Ist in der Curl-Antwort.

SCHRITTE DER REST API-UI

1. Rufen Sie die REST-API-UI für den API-Service des Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/`:

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

2. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie in DER REST API-Benutzeroberfläche **PUT /settings/ssh** aus.

a. Klicken Sie auf **Probieren Sie es aus**.

b. Legen Sie den Parameter **Enabled** auf fest `false` Um SSH oder zu deaktivieren `true` Um die zuvor deaktivierte SSH-Funktion wieder zu aktivieren.

c. Klicken Sie Auf **Ausführen**.

Ermitteln des Status der SSH-Funktion auf dem Management-Node mithilfe von APIs

Sie können ermitteln, ob die SSH-Funktion auf dem Management-Node mithilfe einer Management-Node-Service-API aktiviert ist. SSH ist auf Management-Nodes, auf denen Management-Services 2.18 oder höher ausgeführt werden, standardmäßig deaktiviert.

API-Befehl

Für Management Services 2.18 oder höher:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Für Managementservices ab Version 2.17:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Ihr könnt den Träger finden `${TOKEN}` Wird von dem API-Befehl verwendet, wenn Sie "Autorisieren". Der Träger `${TOKEN}` Ist in der Curl-Antwort.

SCHRITTE DER REST API-UI

1. Rufen Sie die REST-API-UI für den API-Service des Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/`:

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

2. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:

   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.

   b. Geben Sie die Client-ID als ein `mnode-client`.

   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

   d. Schließen Sie das Fenster.

3. Wählen Sie in DER REST API UI **GET /settings/ssh** aus.

   a. Klicken Sie auf **Probieren Sie es aus**.

   b. Klicken Sie Auf **Ausführen**.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Schaltet das NetApp HCI System aus oder ein

Ausschalten oder Einschalten des NetApp HCI Systems

Sie können Ihr NetApp HCI System ausschalten oder einschalten, wenn Sie einen geplanten Ausfall haben, Hardware-Wartungsarbeiten durchführen oder das System erweitern müssen. Verwenden Sie die folgenden Aufgaben, um das NetApp HCI System auszuschalten oder es bei Bedarf auszuschalten.

Unter verschiedenen Umständen müssen Sie Ihr NetApp HCI System ausschalten, z. B.:

- Geplante Ausfallzeiten
- Austausch des Chassis-Lüfters
- Firmware-Upgrades
- Erweiterung von Storage- oder Computing-Ressourcen

Im Folgenden finden Sie eine Übersicht über die Aufgaben, die Sie zum Ausschalten eines NetApp HCI Systems ausführen müssen:

- Schalten Sie alle virtuellen Maschinen außer dem VMware vCenter Server (vCSA) aus.
- Schalten Sie alle ESXi-Server außer dem ein, der die vCSA hostet.
- Schalten Sie die vCSA aus.
- Schalten Sie das NetApp HCI Storage-System aus.

Im Folgenden finden Sie eine Übersicht über die Aufgaben, die Sie zum Einschalten eines NetApp HCI Systems ausführen müssen:

- Schalten Sie alle physischen Storage-Nodes ein.
- Schalten Sie alle physischen Computing-Nodes ein.
- Schalten Sie die vCSA ein.
- Überprüfen Sie das System und schalten Sie zusätzliche Virtual Machines ein.

Weitere Informationen

- "Unterstützte Firmware- und ESXi-Treiberversionen für NetApp HCI und Firmware-Versionen für NetApp HCI Storage Nodes"

Schalten Sie Computing-Ressourcen für ein NetApp HCI System aus

Um NetApp HCI Computing-Ressourcen auszuschalten, müssen Sie einzelne VMware ESXi-Hosts sowie die VMware vCenter Server Appliance in einer bestimmten Reihenfolge ausschalten.

Schritte

1. Melden Sie sich bei der vCenter-Instanz an, die das NetApp HCI-System steuert, und bestimmen Sie den ESXi-Rechner, der die virtuelle vCenter Server-Appliance (vCSA) hostet.
2. Nachdem Sie den ESXi-Host ermittelt haben, auf dem vCSA ausgeführt wird, schalten Sie alle anderen virtuellen Maschinen außer vCSA wie folgt aus:
   a. Wählen Sie eine virtuelle Maschine aus.
   b. Klicken Sie mit der rechten Maustaste, und wählen Sie **ein/aus > Gastbetriebssystem herunterfahren** aus.
3. Schalten Sie alle ESXi-Hosts aus, die nicht der ESXi-Host sind, auf dem die vCSA ausgeführt wird.
4. Schalten Sie die vCSA aus.

   Dadurch wird die vCenter-Sitzung beendet, da die vCSA während des Ausschaltvorgangs die Verbindung getrennt. Alle virtuellen Maschinen sollten jetzt heruntergefahren werden, wenn nur ein ESXi Host eingeschaltet ist.
5. Melden Sie sich bei dem ausgeführten ESXi-Host an.
6. Vergewissern Sie sich, dass alle virtuellen Maschinen auf dem Host ausgeschaltet sind.
7. Fahren Sie den ESXi-Host herunter.

   Dadurch werden alle offenen iSCSI-Sitzungen mit dem NetApp HCI-Storage-Cluster getrennt.

Weitere Informationen

- "Unterstützte Firmware- und ESXi-Treiberversionen für NetApp HCI und Firmware-Versionen für NetApp HCI Storage Nodes"

Schalten Sie die Storage-Ressourcen für ein NetApp HCI System aus

Wenn Sie Storage-Ressourcen für NetApp HCI ausschalten, müssen Sie den verwenden `Shutdown` Element API-Methode zum ordnungsgemäßen Anhalten der Storage-Nodes

Schritte

Nachdem Sie die Computing-Ressourcen heruntergefahren haben, verwenden Sie einen Webbrowser, um alle Nodes des NetApp HCI Storage-Clusters abzuschalten.

1. Melden Sie sich beim Storage-Cluster an und vergewissern Sie sich, dass Sie mit dem richtigen MVIP verbunden sind.
2. (Optional) Stellen Sie sicher, dass alle I/O-Vorgänge von den Hosts angehalten wurden:
   a. Legen Sie die I/O-Vorgänge auf der Hostseite still, indem Sie die entsprechenden Befehle für die verwendeten Hypervisoren verwenden.
   b. Wählen Sie in der Cluster-Benutzeroberfläche **Reporting** > **Übersicht** aus. Im Diagramm „Cluster Input/Output“ sollte keine Aktivität stattfinden.
   c. Nachdem alle I/O-Vorgänge angehalten wurden, warten Sie 20 Minuten, bevor Sie das Cluster herunterfahren.
3. Vergewissern Sie sich, dass die Anzahl der iSCSI-Sitzungen null ist.
4. Navigieren Sie zu **Cluster > Nodes > aktiv**, und notieren Sie die Knoten-IDs für alle aktiven Knoten im Cluster.

5. Um den NetApp HCI Storage-Cluster auszuschalten, öffnen Sie einen Webbrowser und verwenden Sie folgende URL, um den Abschalungs- und Stopp-Vorgang von zu starten `{MVIP}` Ist die Management-IP-Adresse des NetApp HCI Storage-Systems und des `nodes=[]` Array enthält die Knoten-IDs, die Sie in Schritt 4 aufgezeichnet haben. Beispiel:

```
https://{MVIP}/json-rpc/1.0?method=Shutdown&nodes=[1,2,3,4]&option=halt
```

   Sie können den Befehl in einem Inkognito-Fenster ausführen, um zu vermeiden, dass er später von der gespeicherten URL aus erneut ausgeführt wird.

6. Geben Sie den Benutzernamen und das Passwort des Cluster-Administrators ein.
7. Überprüfen Sie, ob der API-Anruf erfolgreich zurückgegeben wird, indem Sie überprüfen, ob alle Storage-Cluster-Nodes in enthalten sind `successful` Abschnitt des API-Ergebnisses.

   Sie haben alle NetApp HCI Storage-Nodes erfolgreich ausgeschaltet.

8. Schließen Sie den Browser oder die Registerkarte, um zu vermeiden, dass Sie die Schaltfläche „Zurück“ auswählen und den API-Aufruf wiederholen.

   Wenn Sie das Cluster neu starten, müssen Sie bestimmte Schritte durchführen, um zu überprüfen, ob alle Nodes online sind:

   1. Stellen Sie sicher, dass alle kritischen Schweregrad und `volumesOffline` Clusterfehler wurden behoben.
   2. Warten Sie 10 bis 15 Minuten, bis sich das Cluster absetzen lässt.
   3. Starten Sie, um die Hosts für den Zugriff auf die Daten aufzurufen.

   Wenn Sie beim Einschalten der Knoten mehr Zeit einplanen und überprüfen möchten, ob sie nach der Wartung ordnungsgemäß sind, wenden Sie sich an den technischen Support, um Hilfe bei der Verzögerung der Datensynchronisierung zu erhalten, um unnötige bin-Synchronisierung zu vermeiden.

Weitere Informationen

- "Unterstützte Firmware- und ESXi-Treiberversionen für NetApp HCI und Firmware-Versionen für NetApp HCI Storage Nodes"

Schalten Sie Storage-Ressourcen für ein NetApp HCI System ein

Nachdem der geplante Ausfall abgeschlossen ist, können Sie NetApp HCI einschalten.

Schritte

1. Schalten Sie alle Storage-Nodes entweder mit dem physischen ein-/aus-Schalter oder dem BMC ein.
2. Wenn Sie den BMC verwenden, melden Sie sich bei jedem Knoten an und navigieren Sie zu **Fernbedienung > Energiekontrolle > Power On Server**.
3. Wenn alle Storage-Nodes online sind, melden Sie sich beim NetApp HCI Storage-System an und überprüfen Sie, ob alle Nodes funktionsfähig sind.

Weitere Informationen

- "Unterstützte Firmware- und ESXi-Treiberversionen für NetApp HCI und Firmware-Versionen für NetApp HCI Storage Nodes"

Schalten Sie Computing-Ressourcen für ein NetApp HCI System ein

Nach Abschluss des geplanten Ausfalls können Sie die Computing-Ressourcen für ein NetApp HCI System einschalten.

Schritte

1. Schalten Sie die Computing-Nodes in denselben Schritten ein, die Sie zum Einschalten der Storage-Nodes ausgeführt haben.
2. Wenn alle Computing-Nodes betriebsbereit sind, melden Sie sich beim ESXi-Host an, auf dem die vCSA ausgeführt wurde.
3. Melden Sie sich beim Computing-Host an und überprüfen Sie, ob alle NetApp HCI-Datenspeicher sichtbar sind. Bei einem typischen NetApp HCI-System sollten Sie alle lokalen ESXi-Datastores und mindestens die folgenden gemeinsamen Datastores sehen:

```
NetApp-HCI-Datastore-[01,02]
```

1. Wenn der gesamte Storage zugänglich ist, schalten Sie die vCSA und alle anderen erforderlichen virtuellen Maschinen wie folgt ein:
   a. Wählen Sie die virtuellen Maschinen im Navigator aus, wählen Sie alle virtuellen Maschinen aus, die Sie einschalten möchten, und klicken Sie auf die Schaltfläche **Einschalten**.
2. Nachdem Sie die virtuellen Maschinen eingeschaltet haben, warten Sie ca. 5 Minuten, und navigieren Sie anschließend über einen Webbrowser zur IP-Adresse oder FQDN der vCSA-Applikation.

   Wenn Sie nicht lange genug warten, wird eine Meldung angezeigt, die besagt, dass der vSphere Client-Webserver initialisiert wird.

3. Melden Sie sich nach der Initialisierung des vSphere Clients an, und stellen Sie sicher, dass alle ESXi Hosts und Virtual Machines online sind.

Weitere Informationen

- "Unterstützte Firmware- und ESXi-Treiberversionen für NetApp HCI und Firmware-Versionen für NetApp HCI Storage Nodes"