NetApp HCI-Dokumentation

HCI

NetApp
October 11, 2024

Inhalt

NetApp HCI-Dokumentation

Mit den NetApp HCI Lösungen

Mit NetApp HCI können Sie Cloud-Services sowohl über diverse Public-Cloud-Provider als auch vor Ort bereitstellen. Mithilfe von NetApp HCI lassen sich Services ähnlich wie bei einem Cloud-Provider implementieren – komplett ohne Einbeziehung DER IT in einen Self-Service-Modus.

Weitere Informationen zu NetApp HCI Lösungen finden Sie in der "Dokumentation der NetApp HCI-Lösungen".

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"

Versionshinweise

Was ist neu in NetApp HCI

NetApp aktualisiert regelmäßig den NetApp HCI, um Ihnen neue Funktionen, Verbesserungen und Fehlerkorrekturen zu bieten. NetApp HCI 1.8P1 umfasst Element 12.2 für Storage-Cluster.

- Der NetApp HCI 1.8P1 Abschnitt beschreibt neue Funktionen und Aktualisierungen in NetApp HCI Version 1.8P1.
- Der Element 12.2 Abschnitt enthält eine Beschreibung der neuen Funktionen und Updates in NetApp Element 12.2.

NetApp HCI 1.8P1

NetApp HCI 1.8P1 bietet Verbesserungen bei Sicherheit und Stabilität.

Verbesserungen der NetApp HCI-Dokumentation

Sie können jetzt auf NetApp HCI-Upgrade-, Erweiterungs-, Überwachungs- und Konzeptinformationen in einem einfach zu navigierende Format zugreifen"Hier".

NetApp Element Plug-in für vCenter Server 4.5 Verfügbarkeit

Das NetApp Element Plug-in für vCenter Server 4.5 ist außerhalb der Management-Nodes 12.2 und NetApp HCI 1.8P1 Versionen verfügbar. Befolgen Sie zum Aktualisieren des Plug-ins die Anweisungen in der "NetApp HCI-Upgrades" Dokumentation.

Verbesserungen bei der NetApp Hybrid Cloud Control

Die NetApp Hybrid Cloud Control wurde für Version 1.8P1 verbessert. "Weitere Informationen .".

Element 12.2

NetApp HCI 1.8P1 umfasst Element 12.2 für Storage-Cluster. Element 12.2 bietet SolidFire Enterprise SDS, Softwareverschlüsselung im Ruhezustand, Wartungsmodus, erweiterte Sicherheit beim Volume-Zugriff, vollständig qualifizierten Domänennamen (FQDN)-Zugriff auf UIs, Firmware-Updates für Storage-Nodes und Sicherheitsupdates.

SolidFire Enterprise SDS

Bei Element 12.2 wird SolidFire Enterprise SDS (ESDS) eingeführt. SolidFire ESDS bietet die Vorteile der SolidFire Scale-Out-Technologie und NetApp Element Software Data Services auf der Hardware Ihrer Wahl, die der Referenzkonfiguration für SolidFire ESDS entspricht. "Weitere Informationen .".

Im Folgenden finden Sie neue Element API-Methoden im Zusammenhang mit SolidFire ESDS ("Element 12.2 API-Informationen für SolidFire ESDS" hat weitere Informationen):

- `GetLicenseKey`
- `SetLicenseKey`

Softwareverschlüsselung im Ruhezustand

Element 12.2 bietet eine Softwareverschlüsselung im Ruhezustand, die bei der Erstellung eines Storage-Clusters aktiviert werden kann (und bei der Erstellung eines SolidFire Enterprise SDS-Storage-Clusters standardmäßig aktiviert ist). Diese Funktion verschlüsselt alle auf den SSDs gespeicherten Daten in den Storage-Nodes und verursacht nur eine sehr geringe Beeinträchtigung der Client-I/O (~2 %) auf die Performance.

Folgende Element API-Methoden stehen im Zusammenhang mit der Softwareverschlüsselung im Ruhezustand (das "Referenzhandbuch für Element API" bietet weitere Informationen):

- `CreateCluster`

Wartungsmodus

Mit Element 12.2 wird ein Wartungsmodus eingeführt, sodass ein Storage-Node bei Wartungsarbeiten wie Software-Upgrades oder Host-Reparaturen offline geschaltet werden kann und eine vollständige Synchronisierung aller Daten verhindert wird. Wenn ein oder mehrere Nodes gewartet werden müssen, können Sie die I/O-Auswirkungen auf den Rest des Storage-Clusters minimieren, indem Sie vor Beginn den Wartungsmodus für diese Nodes aktivieren. Sie können den Wartungsmodus sowohl mit den Geräteknoten als auch mit den SolidFire ESDS-Knoten verwenden.

Verbesserte Sicherheit bei Volume-Zugriff

Sie können nun den Volume-Zugriff auf bestimmte Initiatoren beschränken, die auf der VLAN-Zuordnung (virtuelles Netzwerk) basieren. Sie können einem oder mehreren virtuellen Netzwerken neue oder vorhandene Initiatoren zuordnen und diesen Initiator auf iSCSI-Ziele beschränken, auf die über diese virtuellen Netzwerke zugegriffen werden kann.

Die folgenden aktualisierten Element API-Methoden beziehen sich auf diese Sicherheitsverbesserungen (das "Referenzhandbuch für Element API" enthält weitere Informationen):

- `CreateInitiators`
- `ModifyInitiators`
- `AddAccount`
- `ModifyAccount`

Fully Qualified Domain Name (FQDN)-Zugriff auf UIs

Element 12.2 unterstützt den Zugriff auf die Cluster-Webschnittstelle über FQDNs. Wenn Sie auf Element 12.2-Speicher-Clustern den FQDN für den Zugriff auf Webbenutzerschnittstellen wie die Element Web-UI, die UI pro Node oder die Management-Node-UI verwenden, müssen Sie zuerst eine Speichercluster-Einstellung hinzufügen, um den vom Cluster verwendeten FQDN zu identifizieren. Diese Einstellung ermöglicht es dem Cluster, eine Anmeldesitzung ordnungsgemäß umzuleiten und erleichtert eine bessere Integration in externe Dienste wie Schlüsselmanager und Identitätsanbieter für die Multi-Faktor-Authentifizierung. Für diese Funktion sind Management Services ab Version 2.15 erforderlich. "Weitere Informationen .".

Updates der Storage Node-Firmware

Element 12.2 umfasst Firmware-Updates für Storage-Nodes. "Weitere Informationen .".

Verbesserte Sicherheit

Element 12.2 behebt Sicherheitslücken bei Storage-Nodes und dem Management-Node. "Weitere Informationen ." Informationen zu diesen Sicherheitsverbesserungen.

Neue INTELLIGENTE Warnung für fehlerhafte Laufwerke

Element 12.2 führt jetzt regelmäßige Zustandsprüfungen für SolidFire-Appliance-Laufwerke unter Verwendung von INTELLIGENTEN Systemzustandsdaten von den Laufwerken durch. Ein Laufwerk, das die SMART-Health-Prüfung nicht erfolgreich abschließt, kann fast zum Ausfall führen. Wenn ein Laufwerk die INTELLIGENTE Integritätsprüfung nicht erfolgreich durchläuft, wird ein neuer Cluster-Fehler mit kritischem Schweregrad angezeigt: `Drive with serial: <serial number> in slot: <node slot><drive slot> has failed the SMART overall health check. To resolve this fault, replace the drive`

Weitere Informationen

- "Versionshinweise zu NetApp Hybrid Cloud Control and Management Services"
- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"
- "Unterstützte Firmware- und ESXi-Treiberversionen für NetApp HCI und Firmware-Versionen für NetApp HCI Storage Nodes"

Weitere Release-Informationen

Dort finden Sie Links zu den neuesten und früheren Versionshinweisen zu verschiedenen Komponenten der NetApp HCI und Element Storage-Umgebung.

Sie werden aufgefordert, sich mit Ihren Anmeldedaten für die NetApp Support Site anzumelden.

NetApp HCI

- "Versionshinweise zu NetApp HCI 1.8P1"
- "Versionshinweise zu NetApp HCI 1.8"
- "Versionshinweise zu NetApp HCI 1.7P1"

NetApp Element Software

- "Versionshinweise zu NetApp Element Software 12.2"
- "Versionshinweise zu NetApp Element Software 12.0"
- "Versionshinweise zu NetApp Element Software 11.8"
- "Versionshinweise zu NetApp Element Software 11.7"
- "Versionshinweise zu NetApp Element Software 11.5.1"
- "Versionshinweise zu NetApp Element Software 11.3P1"

Management Services

- "Versionshinweise Für Management Services"

NetApp Element Plug-in für vCenter Server

- "Versionshinweise zu vCenter Plug-in 5.1" *NEU*
- "Versionshinweise zu vCenter Plug-in 5.0"
- "Versionshinweise zu vCenter Plug-in 4.10"
- "Versionshinweise zu vCenter Plug-in 4.9"
- "Versionshinweise zu vCenter Plug-in 4.8"
- "Versionshinweise zu vCenter Plug-in 4.7"
- "Versionshinweise zu vCenter Plug-in 4.6"
- "Versionshinweise zu vCenter Plug-in 4.5"
- "Versionshinweise zu vCenter Plug-in 4.4"
- "Versionshinweise zu vCenter Plug-in 4.3"

Computing-Firmware

- "Versionshinweise Zum Computing-Firmware-Bundle 2.146"
- "Compute Firmware Bundle 2.27 – Versionshinweise"
- "Compute Firmware Bundle 12.2.109 – Versionshinweise"
- "Unterstützte Firmware- und ESXi-Treiberversionen" *NEU*

Storage-Firmware

- "Speicher-Firmware-Paket 2.146 – Versionshinweise"
- "Speicher-Firmware-Paket 2.99.2 – Versionshinweise"
- "Speicher-Firmware-Paket 2.76 Versionshinweise"
- "Versionshinweise zum Storage Firmware Bundle 2.27"
- "H610S BMC 3.84.07 – Versionshinweise"
- "Unterstützte Firmware- und ESXi-Treiberversionen" *NEU*

Konzepte

Produktübersicht über NetApp HCI

NetApp HCI wurde als Hybrid-Cloud-Infrastruktur für die Ansprüche von Unternehmen entwickelt, kombiniert Storage, Computing, Netzwerke und Hypervisor – und erweitert diese Ressourcen um Funktionen für Public und Private Clouds.

Die disaggregierte Hybrid-Cloud-Infrastruktur von NetApp ermöglicht eine unabhängige Skalierung von Computing- und Storage und passt sich mühelos an Workloads mit garantierter Performance an.

- Erfüllt Anforderungen einer Hybrid-Multi-Cloud
- Compute und Storage skalieren unabhängig voneinander
- Vereinfachte Orchestrierung von Datenservices in Hybrid-Multi-Clouds

Komponenten von NetApp HCI

Hier eine Übersicht über die verschiedenen Komponenten der NetApp HCI Umgebung:

- NetApp HCI stellt Storage- und Computing-Ressourcen bereit. Sie verwenden den **NetApp Deployment Engine** Assistenten zur Implementierung von NetApp HCI. Rechenknoten werden nach erfolgreicher Implementierung als ESXi-Hosts angezeigt und können in VMware vSphere Web Client gemanagt werden.
- **Managementservices** oder Mikroservices umfassen den Active IQ Collector, QoSSIOC für das vCenter Plug-in und den mNode Service; sie werden häufig als Service-Bundles aktualisiert. Ab Element 11.3 werden **Management Services** auf dem Management-Node gehostet, wodurch sich ausgewählte Software-Services außerhalb der Hauptversionen schneller aktualisieren lassen. Der **Management Node** (mNode) ist eine virtuelle Maschine, die parallel zu einem oder mehreren auf Element Software basierenden Speicherclustern läuft. Er dient als Upgrade und zur Bereitstellung von Systemservices wie Monitoring und Telemetrie, zum Management von Cluster-Ressourcen und -Einstellungen, zur Ausführung von Systemtests und Dienstprogrammen und zur Aktivierung des NetApp Support-Zugriffs zur Fehlerbehebung.

  Erfahren Sie mehr über "Management Services-Releases".

- **Mit NetApp Hybrid Cloud Control** können Sie NetApp HCI managen. Sie können Management Services aktualisieren, Ihr System erweitern, Protokolle erfassen und Ihre Installation mit NetApp SolidFire Active IQ überwachen. Sie melden sich bei NetApp Hybrid Cloud Control an, indem Sie die IP-Adresse des Management-Node nutzen.
- Das **NetApp Element Plug-in für vCenter Server** ist ein Web-basiertes Tool, das in die vSphere-Benutzeroberfläche integriert ist. Das Plug-in ist eine erweiterbare und skalierbare, benutzerfreundliche Schnittstelle für VMware vSphere, mit der Storage Cluster mit **NetApp Element Software** gemanagt und überwacht werden können. Das Plug-in stellt eine Alternative zur Element UI dar. Über die Plug-in-Benutzeroberfläche können Cluster ermittelt und konfiguriert sowie Storage von der Cluster-Kapazität gemanagt, überwacht und zugewiesen werden, um Datastores und virtuelle Datastores (für virtuelle Volumes) zu konfigurieren. Ein Cluster wird im Netzwerk als einzelne lokale Gruppe angezeigt, die Hosts und Administratoren durch virtuelle IP-Adressen repräsentiert wird. Sie können auch Cluster-Aktivitäten mit Echtzeitberichten überwachen, einschließlich Fehler- und Warnmeldungen für alle Ereignisse, die während der Ausführung verschiedener Vorgänge auftreten können.

Erfahren Sie mehr über "NetApp Element Plug-in für vCenter Server".

- Standardmäßig sendet NetApp HCI Performance- und Alarmstatistiken an den **NetApp SolidFire Active IQ** Service. Im Rahmen des normalen Support-Vertrags überwacht NetApp Support diese Daten und warnt Sie vor Performance-Engpässen oder potenziellen Systemproblemen. Sie müssen ein NetApp Support-Konto erstellen, wenn Sie noch kein Konto haben (auch wenn Sie ein bestehendes SolidFire Active IQ-Konto haben), damit Sie diesen Service nutzen können.

  Erfahren Sie mehr über "NetApp SolidFire Active IQ".

NetApp HCI-URLs

Im Folgenden finden Sie die allgemeinen URLs, die Sie mit NetApp HCI verwenden:

URL	Beschreibung
`https://[IPv4 address of Bond1G interface on a storage node]`	Rufen Sie den Assistenten für die NetApp-Bereitstellungsmodul auf, um NetApp HCI zu installieren und zu konfigurieren. "Weitere Informationen ."
<code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt; </code>	Sie haben Zugriff auf NetApp Hybrid Cloud Control, um Upgrades, Erweiterungen und Monitoring Ihrer NetApp HCI Installation und Update-Managementservices durchzuführen. "Weitere Informationen ."
`https://[IP address]:442`	Greifen Sie über die Node-Benutzeroberfläche auf Netzwerk- und Cluster-Einstellungen zu und nutzen Sie Systemtests und Dienstprogramme. "Weitere Informationen ."
`https://<ManagementNodeIP>:9443`	Registrieren Sie das vCenter Plug-in-Paket im vSphere Web Client.
`https://activeiq.solidfire.com`	Überwachen Sie Ihre Daten und erhalten Sie Warnmeldungen zu Performance-Engpässen oder potenziellen Systemproblemen.
`https://<ManagementNodeIP>/mnode`	Managementservices müssen mithilfe der REST-API-UI vom Managementknoten manuell aktualisiert werden.
`https://[storage cluster MVIP address]`	Zugreifen auf die Benutzeroberfläche der NetApp Element Software

Weitere Informationen

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

Benutzerkonten

Um auf Storage-Ressourcen in Ihrem System zuzugreifen, müssen Sie Benutzerkonten einrichten.

Benutzerkontenverwaltung

Über Benutzerkonten werden der Zugriff auf die Storage-Ressourcen in einem softwarebasierten Netzwerk von NetApp Element gesteuert. Mindestens ein Benutzerkonto ist erforderlich, bevor ein Volume erstellt werden kann.

Wenn Sie ein Volume erstellen, wird es einem Konto zugewiesen. Wenn Sie ein virtuelles Volume erstellt haben, ist das Konto der Speichercontainer.

Folgende Aspekte sollten zusätzlich berücksichtigt werden:

- Das Konto enthält die CHAP-Authentifizierung, die für den Zugriff auf die ihm zugewiesenen Volumes erforderlich ist.
- Einem Konto können bis zu 2000 Volumes zugewiesen sein, aber ein Volume kann nur zu einem Konto gehören.
- Benutzerkonten können über den Erweiterungspunkt für die NetApp Element-Verwaltung verwaltet werden.

Mit NetApp Hybrid Cloud Control lassen sich folgende Account-Typen erstellen und verwalten:

- Administratorkonten für das Storage-Cluster
- Autoritäre Benutzerkonten
- Volume-Konten, nur für den Storage Cluster spezifisch, auf dem sie erstellt wurden.

Konten für Storage-Cluster-Administratoren

In einem Storage-Cluster mit NetApp Element Software können zwei Arten von Administratorkonten vorhanden sein:

- **Primary Cluster Administrator Account**: Dieses Administratorkonto wird beim Erstellen des Clusters erstellt. Dieses Konto ist das primäre administrative Konto mit der höchsten Zugriffsebene auf das Cluster. Dieses Konto ist analog zu einem Root-Benutzer in einem Linux-System. Sie können das Kennwort für dieses Administratorkonto ändern.
- **Cluster-Administratorkonto**: Sie können einem Cluster-Administratorkonto eine begrenzte Anzahl von Administratorzugriff zur Ausführung bestimmter Aufgaben innerhalb eines Clusters gewähren. Die jedem Cluster-Administratorkonto zugewiesenen Zugangsdaten werden zur Authentifizierung von API- und Element-UI-Anforderungen innerhalb des Storage-Systems verwendet.

> Ein lokales (nicht-LDAP)-Cluster-Administratorkonto ist erforderlich, um über die UI pro Node auf aktive Knoten in einem Cluster zuzugreifen. Kontoanmeldeinformationen sind für den Zugriff auf einen Node, der noch nicht Teil eines Clusters ist, nicht erforderlich.

Sie können Cluster-Administratorkonten verwalten, indem Sie Cluster-Administratorkonten erstellen, löschen und bearbeiten, das Kennwort für den Cluster-Administrator ändern und LDAP-Einstellungen konfigurieren, um den Systemzugriff für Benutzer zu verwalten.

Weitere Informationen finden Sie im "SolidFire und Element Documentation Center".

Autoritäre Benutzerkonten

Autorisierte Benutzerkonten können sich gegen alle Storage-Ressourcen authentifizieren, die mit der NetApp Hybrid Cloud Control Instanz der Nodes und Cluster verbunden sind. Mit diesem Konto können Sie Volumes, Konten, Zugriffsgruppen und mehr über alle Cluster hinweg verwalten.

Maßgebliche Benutzerkonten werden über die obere rechte Menü-Option „Benutzermanagement“ in der NetApp Hybrid Cloud Control gemanagt.

Das "Autorisierende Storage-Cluster" ist das Storage-Cluster, das NetApp Hybrid Cloud Control zum Authentifizieren von Benutzern verwendet.

Bei der NetApp Hybrid Cloud Control können sich alle Benutzer, die auf dem autorisierenden Storage-Cluster erstellt wurden, anmelden. Benutzer, die auf anderen Storage Clustern erstellt wurden, können sich bei Hybrid Cloud Control nicht anmelden.

- Wenn der Management-Node nur über einen Storage-Cluster verfügt, dann ist er das autorisierende Cluster.
- Wenn der Management-Node zwei oder mehr Storage-Cluster umfasst, wird einem dieser Cluster als autorisierende Cluster zugewiesen. Nur Benutzer dieses Clusters können sich bei NetApp Hybrid Cloud Control anmelden.

Viele NetApp Hybrid Cloud Control Funktionen funktionieren zwar mit mehreren Storage-Clustern, jedoch bringen Authentifizierung und Autorisierung erforderliche Einschränkungen mit sich. Die Einschränkung der Authentifizierung und Autorisierung besteht darin, dass Benutzer aus dem autorisierenden Cluster Aktionen auf anderen Clustern ausführen können, die an NetApp Hybrid Cloud Control gebunden sind, auch wenn diese nicht in den anderen Storage-Clustern ausgeführt werden. Bevor Sie mit der Verwaltung mehrerer Storage-Cluster fortfahren, sollten Sie sicherstellen, dass die auf den Standards definierten Benutzer auf allen anderen Storage-Clustern mit denselben Berechtigungen definiert sind. Benutzer können über NetApp Hybrid Cloud Control gemanagt werden.

Volume-Konten

Volume-spezifische Konten gelten nur für den Storage Cluster, auf dem sie erstellt wurden. Mit diesen Konten können Sie Berechtigungen für bestimmte Volumes im Netzwerk festlegen, haben aber keine Auswirkungen außerhalb dieser Volumes.

Volume-Konten werden in der Tabelle „NetApp Hybrid Cloud Control Volumes“ gemanagt.

Weitere Informationen

- "Benutzerkonten verwalten"
- "Informationen zu Clustern"
- "Ressourcen-Seite zu NetApp HCI"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Documentation Center"

Datensicherung

Begriffe der NetApp HCI Datensicherung umfassen verschiedene Arten von Remote-Replizierung, Volume Snapshots, Volume-Klonen, Sicherungsdomänen und

Hochverfügbarkeit mit der Double Helix Technologie.

Die NetApp HCI Datensicherung umfasst folgende Konzepte:

- Typen der Remote-Replizierung
- Volume Snapshots zur Datensicherung
- Volume-Klone
- Backup- und Restore-Prozess – Übersicht für SolidFire Storage
- Sicherungsdomänen
- Hochverfügbarkeit mit Double Helix

Typen der Remote-Replizierung

Die Remote-Replikation von Daten kann folgende Formen annehmen:

- Synchrone und asynchrone Replizierung zwischen Clustern
- Reine Snapshot Replizierung
- Replizierung zwischen Element und ONTAP Clustern mit SnapMirror

Siehe "TR-4741: NetApp Element Software Remote Replication".

Synchrone und asynchrone Replizierung zwischen Clustern

Für Cluster mit NetApp Element Software ermöglicht Echtzeitreplizierung die schnelle Erstellung von Remote-Kopien von Volume-Daten.

Ein Storage-Cluster kann mit bis zu vier anderen Storage-Clustern gekoppelt werden. Sie können Volume-Daten für Failover- und Failback-Szenarien synchron oder asynchron von einem Cluster in einem Cluster-Paar replizieren.

Synchrone Replizierung

Die synchrone Replizierung repliziert die Daten kontinuierlich vom Quell-Cluster zum Ziel-Cluster und wird von Latenz, Paketverlust, Jitter und Bandbreite beeinträchtigt.

Synchrone Replizierung eignet sich für die folgenden Situationen:

- Replizierung mehrerer Systeme über kurze Entfernungen
- Ein Disaster-Recovery-Standort lokal an der Quelle
- Zeitkritische Applikationen und der Schutz von Datenbanken
- Business-Continuity-Applikationen, bei denen der sekundäre Standort als primärer Standort fungieren muss, wenn der primäre Standort ausfällt

Asynchrone Replizierung

Die asynchrone Replikation repliziert kontinuierlich Daten von einem Quellcluster zu einem Zielcluster, ohne auf die Bestätigungen aus dem Zielcluster zu warten. Während der asynchronen Replizierung werden Schreibvorgänge dem Client (Applikation) bestätigt, nachdem sie im Quell-Cluster durchgeführt wurden.

Asynchrone Replizierung eignet sich für die folgenden Situationen:

- Der Disaster-Recovery-Standort ist weit von der Quelle entfernt und die Applikation toleriert keine durch das Netzwerk verursachten Latenzen.
- Das Netzwerk, das die Quell- und Ziel-Cluster verbindet, weist Bandbreiteneinschränkungen auf.

Reine Snapshot Replizierung

Bei der Datensicherung nur mit Snapshots werden geänderte Daten zu einem bestimmten Zeitpunkt in ein Remote-Cluster repliziert. Es werden nur die Snapshots repliziert, die auf dem Quellcluster erstellt wurden. Aktive Schreibvorgänge vom Quell-Volume sind nicht.

Sie können die Häufigkeit der Snapshot Replikationen festlegen.

Die Snapshot Replizierung hat keine Auswirkungen auf die asynchrone oder synchrone Replizierung.

Replizierung zwischen Element und ONTAP Clustern mit SnapMirror

Mit der NetApp SnapMirror Technologie können Snapshots repliziert werden, die mit NetApp Element Software für Disaster Recovery-Zwecke in ONTAP erstellt wurden. In einer SnapMirror Beziehung stellt Element einen Endpunkt dar, und ONTAP ist der andere.

SnapMirror ist eine NetApp Snapshot™ Replizierungstechnologie für Disaster Recovery, die für das Failover von primärem Storage auf sekundärem Storage an einem externen Standort ausgelegt ist. Die SnapMirror Technologie erstellt ein Replikat bzw. eine Spiegelung der Arbeitsdaten im sekundären Storage, von dem aus Sie bei einem Ausfall am primären Standort weiterhin Daten bereitstellen können. Daten werden auf Volume-Ebene gespiegelt.

Die Beziehung zwischen dem Quell-Volume im primären Storage und dem Ziel-Volume im sekundären Storage wird als Datensicherungsbeziehung bezeichnet. Die Cluster werden als Endpunkte bezeichnet, in denen sich die Volumes befinden und die Volumes, die die replizierten Daten enthalten, müssen peed sein. Eine Peer-Beziehung ermöglicht einen sicheren Datenaustausch zwischen Clustern und Volumes.

SnapMirror wird nativ auf den NetApp ONTAP Controllern ausgeführt und ist in Element integriert, das auf NetApp HCI und SolidFire Clustern ausgeführt wird. Die Logik zur Steuerung von SnapMirror befindet sich in ONTAP Software. Daher müssen alle SnapMirror Beziehungen mindestens ein ONTAP System erfordern, um die Koordination durchzuführen. Benutzer managen die Beziehungen zwischen Element- und ONTAP-Clustern. Dies erfolgt hauptsächlich über die Element UI. Einige Managementaufgaben befinden sich jedoch im NetApp ONTAP System Manager. Benutzer können SnapMirror auch über die CLI und die API managen, die sowohl in ONTAP als auch in Element verfügbar sind.

Siehe "TR-4651: NetApp SolidFire SnapMirror Architektur und Konfiguration" (Anmeldung erforderlich).

Sie müssen die SnapMirror Funktion auf Cluster-Ebene manuell mit der Element Software aktivieren. Die SnapMirror Funktion ist standardmäßig deaktiviert und wird nicht automatisch im Rahmen einer neuen Installation oder eines Upgrades aktiviert.

Nach der Aktivierung von SnapMirror können Sie SnapMirror Beziehungen über die Registerkarte Datensicherung in der Element Software erstellen.

Volume Snapshots zur Datensicherung

Ein Volume Snapshot ist eine zeitpunktgenaue Kopie eines Volumes, mit der Sie später ein Volume auf diesen speziellen Zeitpunkt wiederherstellen können.

Während Snapshots einem Volume-Klon ähneln, sind Snapshots lediglich Replikate von Volume-Metadaten.

Sie können also nicht mounten oder darauf schreiben. Das Erstellen eines Volume-Snapshots nimmt ebenfalls nur eine geringe Menge an Systemressourcen und Platz in Anspruch, sodass die Snapshot-Erstellung schneller als das Klonen erfolgt.

Sie können Snapshots in einem Remote-Cluster replizieren und als Sicherungskopie des Volumes verwenden. Dadurch können Sie ein Rollback eines Volumes zu einem bestimmten Zeitpunkt mit dem replizierten Snapshot durchzuführen. Sie können auch einen Klon eines Volumes aus einem replizierten Snapshot erstellen.

Sie können ein Backup von Snapshots aus einem SolidFire Cluster auf einem externen Objektspeicher oder auf einem anderen SolidFire Cluster erstellen. Wenn Sie einen Snapshot in einem externen Objektspeicher sichern, müssen Sie über eine Verbindung zum Objektspeicher verfügen, der Lese-/Schreibvorgänge ermöglicht.

Sie können einen Snapshot eines einzelnen Volumes oder mehrerer zur Datensicherheit erstellen.

Volume-Klone

Ein Klon eines einzelnen oder mehrerer Volumes ist eine zeitpunktgenaue Kopie der Daten. Wenn Sie ein Volume klonen, erstellt das System einen Snapshot des Volume und erstellt dann eine Kopie der Daten, auf die der Snapshot verweist.

Dies ist ein asynchroner Prozess und die erforderliche Zeit hängt von der Größe des zum Klonen benötigten Volumes und der aktuellen Cluster-Last ab.

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

Backup- und Restore-Prozess – Übersicht für SolidFire Storage

Backups und Restores von Volumes mit anderen SolidFire Storage-Systemen sowie in sekundären Objektspeichern mit Amazon S3 oder OpenStack Swift möglich.

Sie können ein Volume unter folgender Adresse sichern:

- Ein SolidFire Storage-Cluster
- Ein Amazon S3-Objektspeicher
- OpenStack Swift Objektspeicher

Wenn Sie Volumes aus OpenStack Swift oder Amazon S3 wiederherstellen, benötigen Sie Manifest-Informationen aus dem ursprünglichen Backup-Prozess. Wenn Sie ein Volume wiederherstellen, das auf einem SolidFire Storage-System gesichert wurde, sind keine Manifest-Informationen erforderlich.

Sicherungsdomänen

Eine Sicherungsdomäne ist ein Node oder eine Gruppe von Nodes, die so gruppiert werden, dass ein Teil oder sogar alle Knoten ausfallen könnten, ohne dass die Datenverfügbarkeit beeinträchtigt wird. Sicherungsdomänen ermöglichen die automatische Selbstreparatur eines Storage-Clusters beim Verlust eines Chassis (Chassis-Affinität) oder einer gesamten Domäne (Chassis-Gruppe).

Ein Protection-Domain-Layout weist jeden Knoten einer bestimmten Protection-Domain zu.

Es werden zwei unterschiedliche Protection Domain Layouts unterstützt, sogenannte Protection Domain

Levels.

- Auf Node-Ebene befindet sich jeder Node in einer eigenen Sicherungsdomäne.
- Auf Chassis-Ebene befinden sich nur Nodes, die sich ein Chassis teilen, in derselben Schutzdomäne.
  - Das Layout auf Chassis-Ebene wird automatisch von der Hardware bestimmt, wenn der Node zum Cluster hinzugefügt wird.
  - In einem Cluster, in dem sich jeder Node in einem separaten Chassis befindet, sind diese beiden Ebenen funktional identisch.

Sie können das NetApp Element-Plug-in für vCenter Server manuell "Aktivieren Sie die Überwachung von Schutzdomänen" verwenden. Sie können einen Schutz-Domain-Schwellenwert basierend auf Node- oder Chassis-Domänen auswählen.

Wenn ein neues Cluster erstellt wird, sollten Storage-Nodes genutzt werden, die sich in einem gemeinsamen Chassis befinden, sollte mithilfe der Sicherungs-Domains-Funktion ein Design für Ausfallschutz auf Chassis-Ebene in Betracht gezogen werden.

Sie können ein benutzerdefiniertes Schutz-Domain-Layout definieren, in dem jeder Knoten einer und nur einer benutzerdefinierten Schutzdomäne zugeordnet ist. Standardmäßig wird jeder Knoten derselben benutzerdefinierten Standard-Schutzdomäne zugewiesen.

Siehe "SolidFire und Element 12.2 Documentation Center".

Hochverfügbarkeit mit Double Helix

Die Double Helix Datensicherung ist eine Replizierungsmethode, die mindestens zwei redundante Datenkopien auf alle Laufwerke innerhalb eines Systems verteilt. Der Ansatz „RAID-less“ ermöglicht es einem System, mehrere gleichzeitige Ausfälle auf allen Ebenen des Storage-Systems zu absorbieren und schnell zu reparieren.

Weitere Informationen

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

Cluster

Ein Cluster ist eine Gruppe von Nodes, die als Ganzes funktionieren und Storage- oder Computing-Ressourcen bereitstellen. Ab NetApp HCI 1.8 können Sie ein Storage-Cluster mit zwei Knoten haben. Ein Storage-Cluster wird im Netzwerk als einzelne logische Gruppe angezeigt und kann dann als Block-Storage genutzt werden.

Die Storage-Ebene in NetApp HCI wird durch NetApp Element bereitgestellt. Die Management-Ebene wird durch das NetApp Element Plug-in für vCenter Server bereitgestellt. Ein Storage-Node ist ein Server, der eine Sammlung von Laufwerken enthält, die über die Bond10G-Netzwerkschnittstelle miteinander kommunizieren. Jeder Storage Node ist mit zwei Netzwerken verbunden, Storage und Management, wobei jeder über zwei unabhängige Links verfügt, um für Redundanz und Performance zu sorgen. Jeder Node benötigt in jedem Netzwerk eine IP-Adresse. Sie können mit neuen Storage-Nodes ein Cluster erstellen oder einem vorhandenen Cluster Storage Nodes hinzufügen, um die Storage-Kapazität und Performance zu steigern.

Autorisierende Storage-Cluster

Der Storage-Cluster ist der Storage-Cluster, mit dem NetApp Hybrid Cloud Control Benutzer authentifizieren kann.

Wenn der Management-Node nur über einen Storage-Cluster verfügt, dann ist er das autorisierende Cluster. Wenn der Management-Node zwei oder mehr Storage-Cluster umfasst, wird einem dieser Cluster als autorisierende Cluster zugewiesen. Nur Benutzer dieses Clusters können sich bei NetApp Hybrid Cloud Control anmelden. Um herauszufinden, welcher Cluster der autoritative Cluster ist, können Sie die API verwenden `GET /mnode/about`. In der Antwort ist die IP-Adresse im `token_url` Feld die virtuelle Management-IP-Adresse (MVIP) des autoritativen Speicher-Clusters. Wenn Sie versuchen, sich bei NetApp Hybrid Cloud Control als Benutzer anzumelden, der sich nicht auf dem autorisierenden Cluster befindet, schlägt der Anmeldeversuch fehl.

Viele Funktionen von NetApp Hybrid Cloud Control wurden für den Einsatz mit mehreren Storage-Clustern entwickelt. Allerdings schränkteutig die Authentifizierung und Autorisierung sein. Die Authentifizierung und Autorisierung im Zusammenhang mit der Authentifizierung besteht darin, dass der Benutzer aus dem autorisierenden Cluster Aktionen auf anderen Clustern ausführen kann, die an NetApp Hybrid Cloud Control gebunden sind, auch wenn diese nicht Anwender in den anderen Storage-Clustern sind. Bevor Sie mit der Verwaltung mehrerer Storage-Cluster fortfahren, sollten Sie sicherstellen, dass die auf den Standards definierten Benutzer auf allen anderen Storage-Clustern mit denselben Berechtigungen definiert sind.

Benutzer können mit NetApp Hybrid Cloud Control managen.

Bevor Sie mit der Verwaltung mehrerer Storage-Cluster fortfahren, sollten Sie sicherstellen, dass die auf den Standards definierten Benutzer auf allen anderen Storage-Clustern mit denselben Berechtigungen definiert sind. Sie können "Benutzer managen" über die Benutzeroberfläche der Element Software (Element Web UI).

Weitere Informationen zum Arbeiten mit Management-Storage-Cluster-Assets für Nodes finden Sie unter"Erstellen und Managen von Storage-Cluster-Assets".

Ungenutzte Kapazität

Wenn ein neu hinzugefügter Node mehr als 50 % der gesamten Cluster-Kapazität beträgt, wird einige der Kapazitäten dieses Node unbrauchbar („ungenutzt“) gemacht, sodass die Kapazitätsregel eingehalten wird. Dies bleibt der Fall, bis mehr Storage-Kapazität hinzugefügt wird. Wenn ein sehr großer Node hinzugefügt wird, der auch die Kapazitätsregel nicht befolgt, kann der zuvor isolierte Node nicht mehr ungenutzt bleiben, während der neu hinzugefügte Node ungenutzt ist. Kapazität sollte immer paarweise hinzugefügt werden, um dies zu vermeiden. Wenn ein Node ungenutzt wird, ist ein geeigneter Cluster-Fehler zu werfen.

Storage-Cluster mit zwei Nodes

Ab NetApp HCI 1.8 können Sie ein Storage-Cluster mit zwei Storage-Nodes einrichten.

- Sie können bestimmte Node-Typen verwenden, um das Storage-Cluster mit zwei Nodes zu bilden. Siehe "Versionshinweise zu NetApp HCI 1.8".

  In einem Cluster mit zwei Nodes sind die Storage-Nodes auf Nodes mit 480-GB- und 960-GB-Laufwerken begrenzt, und die Nodes müssen denselben Modelltyp aufweisen.

- Storage-Cluster mit zwei Nodes eignen sich am besten für kleinere Implementierungen mit Workloads, die nicht von hohen Anforderungen an Kapazität und Performance abhängig sind.
- Neben zwei Storage-Nodes enthält ein Storage-Cluster mit zwei Nodes auch zwei **NetApp HCI Witness**

Nodes.

Weitere Informationen zu "Witness Nodes"

- Sie können ein zwei-Node-Storage-Cluster auf ein Storage-Cluster mit drei Nodes skalieren. Die Ausfallsicherheit durch drei-Node-Cluster wird erhöht, da sich Storage-Node-Ausfälle automatisch beheben lassen.
- Storage-Cluster mit zwei Nodes bieten dieselben Sicherheitsfunktionen und Funktionen wie herkömmliche Storage-Cluster mit vier Nodes.
- Storage-Cluster mit zwei Nodes nutzen dieselben Netzwerke wie Storage-Cluster mit vier Nodes. Die Netzwerke werden während der NetApp HCI-Implementierung mit dem NetApp Deployment Engine Wizard eingerichtet.

Storage Cluster Quorum

Element Software erstellt ein Storage-Cluster von ausgewählten Nodes, wobei eine replizierte Datenbank der Clusterkonfiguration erhalten bleibt. Zur Teilnahme am Cluster-Ensemble sind mindestens drei Nodes erforderlich, um das Quorum für die Cluster-Ausfallsicherheit zu erhalten. Witness Nodes werden in einem Cluster mit zwei Knoten verwendet, um sicherzustellen, dass genügend Speicherknoten vorhanden sind, um ein gültiges Ensemble-Quorum zu bilden. Für die Erstellung eines Ensembles sind Storage Nodes vor Witness Nodes vorzuziehen. Für das Ensemble mit mindestens drei Nodes, das ein Storage Cluster mit zwei Nodes beinhaltet, werden zwei Storage-Nodes und ein Witness-Node verwendet.

In einem Ensemble mit drei Nodes mit zwei Storage-Nodes und einem Witness-Node wird bei einem Ausfall eines Storage-Node ein eingeschränkter Zustand des Clusters ausgeführt. Von den beiden Zeugenknoten kann nur einer im Ensemble aktiv sein. Der zweite Witness Node kann dem Ensemble nicht hinzugefügt werden, da er die Backup-Rolle ausführt. Das Cluster bleibt im eingeschränkten Zustand, bis der Offline-Storage-Node wieder in den Online-Status wechselt oder ein Ersatz-Node dem Cluster hinzugefügt wird.

Wenn ein Witness Node ausfällt, schließt sich der verbleibende Witness Node dem Ensemble zu einem Dreiknotenensemble an. Sie können einen neuen Witness Node bereitstellen, um den fehlgeschlagenen Witness Node zu ersetzen.

Automatische Reparatur und Fehlerbehandlung in Storage-Clustern mit zwei Nodes

Wenn eine Hardwarekomponente in einem Node ausfällt, der Teil eines herkömmlichen Clusters ist, kann der Cluster Daten ausgleichen, die sich auf der Komponente befinden, die zu anderen verfügbaren Nodes im Cluster ausgefallen ist. Diese Funktion zur automatischen Fehlerbehebung ist in einem Storage-Cluster mit zwei Nodes nicht verfügbar, da dem Cluster mindestens drei physische Storage-Nodes zur automatischen Fehlerbehebung zur Verfügung stehen müssen. Wenn ein Node in einem Cluster mit zwei Nodes ausfällt, muss im Cluster mit zwei Nodes keine zweite Kopie der Daten neu gebootet werden. Neue Schreibvorgänge werden für Blockdaten im verbleibenden aktiven Storage-Node repliziert. Wenn der ausgefallene Node ersetzt und zum Cluster hinzugefügt wird, werden die Daten zwischen den beiden physischen Storage-Nodes gleichmäßig verteilt.

Storage Cluster mit drei oder mehr Nodes

Die Erweiterung von zwei Storage-Nodes auf drei Storage-Nodes erhöht die Ausfallsicherheit des Clusters. Diese Lösung ermöglicht automatische Reparatur bei Node- und Laufwerksausfällen, bietet jedoch keine zusätzliche Kapazität. Sie können die Erweiterung mithilfe der "UI für die NetApp Hybrid Cloud Control". Bei der Erweiterung von einem Cluster mit zwei Nodes auf ein Cluster mit drei Nodes kann die Kapazität ungenutzt

bleiben (siehe Ungenutzte Kapazität). Der UI-Assistent zeigt vor der Installation Warnungen zu ungenutzte Kapazität an. Ein einziger Zeuge-Knoten ist weiterhin verfügbar, um das Ensemble-Quorum bei Ausfall eines Speicherknoten zu erhalten, wobei ein zweiter Zeuge-Knoten im Standby-Modus. Wenn Sie ein Storage-Cluster mit drei Nodes auf ein Cluster mit vier Nodes erweitern, werden die Kapazität und die Performance erhöht. In einem Cluster mit vier Nodes sind Witness Nodes nicht mehr erforderlich, um das Cluster-Quorum zu bilden. Sie können das System auf bis zu 64 Computing-Nodes und 40 Storage-Nodes erweitern.

Weitere Informationen

- "NetApp HCI Storage Cluster mit zwei Nodes – TR-4823"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Knoten

Nodes sind Hardware- oder virtuelle Ressourcen, die in einem Cluster gruppiert werden, um Block-Storage- und Computing-Funktionen bereitzustellen.

NetApp HCI und Element Software definiert verschiedene Node-Rollen für ein Cluster. Die vier Arten von Node-Rollen sind **Management Node**, **Storage Node**, **Compute Node** und **NetApp HCI Witness Nodes**.

Management-Node

Der Management-Node (manchmal als mNode abgekürzt) interagiert mit einem Storage-Cluster, um Managementaktionen auszuführen, ist jedoch nicht Mitglied des Storage-Clusters. Managementknoten erfassen regelmäßig über API-Aufrufe Informationen über das Cluster und melden diese Informationen zur Remote-Überwachung an Active IQ (sofern aktiviert). Management-Nodes sind auch für die Koordinierung von Software-Upgrades der Cluster-Nodes verantwortlich.

Der Management-Node ist eine Virtual Machine (VM), die parallel mit einem oder mehreren auf Element Software basierenden Storage-Clustern ausgeführt wird. Neben Upgrades bietet es Systemservices wie Monitoring und Telemetrie, Management von Cluster-Ressourcen und -Einstellungen, Tests und Utilities sowie NetApp Support-Zugang zur Fehlerbehebung. Ab Element 11.3 fungiert der Management Node als Microservice-Host, wodurch sich ausgewählte Softwareservices schneller außerhalb der Hauptversionen aktualisieren lassen. Diese Microservices und Managementservices, wie Active IQ Collector, QoSSIOC für das vCenter Plug-in und der Management-Node-Service, werden häufig als Service-Bundles aktualisiert.

Storage-Nodes

NetApp HCI Storage-Nodes sind Hardware, die die Storage-Ressourcen für ein NetApp HCI System bereitstellen. Laufwerke im Node enthalten Block- und Metadatenspeicherplatz für den Daten-Storage und das Datenmanagement. Jeder Node enthält ein Factory Image der NetApp Element Software. NetApp HCI Storage Nodes können mit dem NetApp Element Management-Erweiterungspunkt gemanagt werden.

Computing Nodes

NetApp HCI Computing-Nodes sind Hardware, die Computing-Ressourcen wie CPU, Arbeitsspeicher und Netzwerk bereitstellt, die für die Virtualisierung bei der NetApp HCI Installation erforderlich sind. Da auf jedem Server VMware ESXi ausgeführt wird, muss das Management der Computing-Nodes von NetApp HCI (Hinzufügen oder Entfernen von Hosts) außerhalb des Plug-ins im Menü Hosts und Cluster in vSphere erfolgen. Unabhängig davon, ob es sich um ein Storage-Cluster mit vier Nodes oder ein Storage-Cluster mit zwei Nodes handelt, bleibt die Mindestanzahl an Computing-Nodes bei NetApp HCI Implementierungen

erhalten.

Witness Nodes

NetApp HCI Witness Nodes sind VMs, die auf Computing-Nodes parallel mit einem Element Software-basierten Storage-Cluster ausgeführt werden. Witness Nodes hosten keine Slice- oder Block-Services. Ein Witness Node ermöglicht bei Ausfall eines Storage-Nodes die Verfügbarkeit des Storage-Clusters. Sie können Witness Nodes auf dieselbe Weise managen und aktualisieren wie andere Storage Nodes. Ein Storage-Cluster kann bis zu vier Witness-Nodes enthalten. Ihr primärer Zweck ist es, sicherzustellen, dass genügend Clusterknoten vorhanden sind, um ein gültiges Ensemble-Quorum zu bilden.

Best Practice: Konfigurieren Sie die Witness Node VMs so konfigurieren Sie den lokalen Datastore des Computing-Nodes (Standardeinstellung: Nde) und konfigurieren Sie diese nicht auf Shared Storage, z. B. SolidFire Storage Volumes. Um eine automatische Migration der VMs zu verhindern, stellen Sie die Automatisierungsebene des Distributed Resource Scheduler (DRS) der Witness Node VM auf **deaktivierte** ein. Dadurch wird verhindert, dass beide Witness-Nodes auf demselben Computing-Node ausgeführt werden und eine Konfiguration mit einem Hochverfügbarkeitspaar (HA-Paar) erstellt wird.

Erfahren Sie mehr über "Ressourcenanforderungen Witness Node" und "Anforderungen an die IP-Adresse des Witness Node".

In einem Storage-Cluster mit zwei Nodes werden mindestens zwei Witness-Nodes für Redundanz bereitgestellt, falls ein Witness-Node ausfällt. Wenn der Installationsprozess von NetApp HCI Witness Nodes installiert, wird eine VM-Vorlage in VMware vCenter gespeichert, mit der Sie einen Witness-Node neu bereitstellen können, falls dieser versehentlich entfernt, verloren oder beschädigt wurde. Sie können auch die Vorlage verwenden, um einen Witness Node neu zu implementieren, wenn ein ausgefallener Computing-Node, der den Witness Node hostet, ersetzt werden muss. Anweisungen hierzu finden Sie im Abschnitt **Neuimplementierung Witness Nodes für zwei- und drei-Knoten-Speicher-Cluster** "Hier".

Weitere Informationen

- "NetApp HCI Storage Cluster mit zwei Nodes – TR-4823"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Storage

Wartungsmodus

Wenn Sie einen Storage Node für Wartungsarbeiten, wie z. B. Software-Upgrades oder Host-Reparaturen, offline schalten müssen, können Sie die Auswirkungen auf den Rest des Storage-Clusters durch Aktivierung des Wartungsmodus für diesen Node auf ein Minimum minimieren. Sie können den Wartungsmodus mit beiden Appliance-Nodes und SolidFire Enterprise SDS-Nodes verwenden.

Sie können einen Storage Node nur in den Wartungsmodus versetzen, wenn der Node in einem ordnungsgemäßen Zustand (keine Blockierung von Cluster-Fehlern) ist und das Storage Cluster einem Ausfall einzelner Nodes gegenüber tolerant ist. Sobald Sie den Wartungsmodus für einen gesunden und toleranten

Node aktivieren, wird der Node nicht sofort migriert. Er wird überwacht, bis die folgenden Bedingungen erfüllt sind:

- Für alle auf dem Node gehosteten Volumes ist ein Failover fehlgeschlagen
- Der Node hostet für ein Volume nicht mehr als primärer Node
- Jedem Failover eines Volumes wird ein temporärer Standby-Node zugewiesen

Nachdem diese Kriterien erfüllt sind, wird der Node in den Wartungsmodus versetzt. Wenn diese Kriterien innerhalb eines Zeitraums von 5 Minuten nicht erfüllt werden, wechselt der Node nicht in den Wartungsmodus.

Wenn Sie den Wartungsmodus für einen Storage-Node deaktivieren, wird der Node überwacht, bis die folgenden Bedingungen erfüllt sind:

- Alle Daten werden vollständig zum Node repliziert
- Alle blockierenden Cluster-Fehler werden behoben
- Alle temporären Standby-Node-Zuweisungen für die auf dem Node gehosteten Volumes wurden deaktiviert

Nachdem diese Kriterien erfüllt sind, wird der Node aus dem Wartungsmodus migriert. Wenn diese Kriterien nicht innerhalb einer Stunde erfüllt werden, kann der Node nicht in den Wartungsmodus wechseln.

Bei Verwendung der Element API werden die Status von Vorgängen im Wartungsmodus angezeigt:

- **Deaktiviert**: Es wurde keine Wartung angefordert.
- **FailedToRecover**: Der Knoten konnte nicht von der Wartung wiederherstellen.
- **RecoveringFromMaintenance**: Der Knoten wird gerade von der Wartung wiederhergestellt.
- **VorbereitungForMaintenance**: Es werden Maßnahmen ergriffen, damit ein Knoten die Wartung durchführen kann.
- **ReadyForMaintenance**: Der Knoten ist zur Wartung bereit.

Weitere Informationen

- "SolidFire und Element Documentation Center"

Volumes

Storage wird im NetApp Element System als Volumes bereitgestellt. Volumes sind Blockgeräte, auf die über das Netzwerk über iSCSI- oder Fibre Channel-Clients zugegriffen wird.

Das NetApp Element Plug-in für vCenter Server ermöglicht Ihnen das Erstellen, Anzeigen, Bearbeiten, Löschen, Klonen Sichern Sie Volumes für Benutzerkonten oder stellen Sie sie wieder her. Außerdem lassen sich Volumes in einem Cluster managen und Volumes in Volume-Zugriffsgruppen hinzufügen oder entfernen.

Persistente Volumes

Mithilfe persistenter Volumes können Management-Node-Konfigurationsdaten nicht lokal mit einer VM in einem bestimmten Storage-Cluster gespeichert werden, damit Daten auch bei Verlust oder Entfernung von Management-Nodes erhalten bleiben. Persistente Volumes sind eine optionale, jedoch empfohlene Management-Node-Konfiguration.

Wenn Sie einen Management-Node für NetApp HCI mithilfe der NetApp Deployment Engine implementieren, werden persistente Volumes automatisch aktiviert und konfiguriert.

Eine Option zum Aktivieren persistenter Volumes ist in den Installations- und Upgrade-Skripten bei der Implementierung eines neuen Management-Node enthalten. Persistente Volumes sind Volumes auf einem Element Software-basierten Storage-Cluster, die Konfigurationsinformationen für die Host-Management-Node-VM enthalten, die über den Lebenszyklus der VM hinaus bestehen bleiben. Wenn der Management-Node verloren geht, kann eine VM mit dem Ersatz-Management-Node eine Verbindung herstellen und Konfigurationsdaten für die verlorene VM wiederherstellen.

Wenn die Funktion persistenter Volumes während der Installation oder eines Upgrades aktiviert ist, erstellt automatisch mehrere Volumes mit NetApp-HCI – Pre-Pend auf den Namen des zugewiesenen Clusters. Diese Volumes können, wie jedes softwarebasierte Element Volume, je nach Ihren Vorliebe und Installation über die Web-UI in Element Software, das NetApp Element Plug-in für vCenter Server oder die API angezeigt werden. Persistente Volumes müssen mit einer iSCSI-Verbindung zum Management-Node in Betrieb sein, um die aktuellen Konfigurationsdaten beizubehalten, die für eine Recovery verwendet werden können.

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

Weitere Informationen

- "Volumes managen"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Volume-Zugriffsgruppen

Eine Volume-Zugriffsgruppe ist eine Sammlung von Volumes, auf die Benutzer entweder über iSCSI oder über Fibre Channel-Initiatoren zugreifen können.

Durch die Erstellung und Nutzung von Volume-Zugriffsgruppen können Sie den Zugriff auf eine Gruppe von Volumes steuern. Wenn Sie einen Satz von Volumes und einen Satz von Initiatoren einer Volume-Zugriffsgruppe zuordnen, gewährt die Zugriffsgruppe diesen Initiatoren Zugriff auf diese Gruppe von Volumes.

Volume-Zugriffsgruppen verfügen über die folgenden Grenzen:

- Maximal 128 Initiatoren pro Volume-Zugriffsgruppe.
- Maximal 64 Zugriffsgruppen pro Volume.
- Eine Zugriffsgruppe kann aus maximal 2000 Volumes bestehen.
- Ein IQN oder WWPN kann nur zu einer Volume-Zugriffsgruppe gehören.

Weitere Informationen

- "Management von Volume-Zugriffsgruppen"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Initiatoren

Initiatoren ermöglichen den Zugriff auf externe Clients auf Volumes in einem Cluster. Diese dienen als Einstiegspunkt für die Kommunikation zwischen Clients und Volumes. Sie können Initiatoren für CHAP-basierten Zugriff anstelle von kontenbasierten Speichervolumes verwenden. Wenn ein einzelner Initiator einer Volume-Zugriffsgruppe hinzugefügt wird, können die Mitglieder der Volume-Zugriffsgruppen auf alle der Gruppe hinzugefügten Storage Volumes zugreifen, ohne dass eine Authentifizierung erforderlich ist. Ein Initiator kann nur einer Zugriffsgruppe angehören.

Weitere Informationen

- "Verwalten von Initiatoren"
- "Volume-Zugriffsgruppen"
- "Management von Volume-Zugriffsgruppen"
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

NetApp HCI Lizenzierung

Wenn Sie NetApp HCI verwenden, werden je nach verwendetem System möglicherweise zusätzliche Lizenzen benötigt.

NetApp HCI und VMware vSphere Lizenzierung

Die VMware vSphere-Lizenzierung hängt von Ihrer Konfiguration ab:

Netzwerkoption	Lizenzierung
Option A: Zwei Kabel für Computing-Nodes mithilfe von VLAN-Tagging (alle Computing-Nodes)	Erfordert die Verwendung von vSphere Distributed Switch, für den eine Lizenz für VMware vSphere Enterprise Plus erforderlich ist
Option B: Sechs Kabel für Computing-Nodes mit getaggten VLANs (H410C 2RU 4-Node Computing-Node)	Bei dieser Konfiguration wird standardmäßig vSphere Standard Switch verwendet. Für die optionale Verwendung von vSphere Distributed Switch ist eine VMware Enterprise Plus-Lizenzierung erforderlich.
Option C: Sechs Kabel für Computing-Nodes mithilfe von nativen und getaggten VLANs (H410C, 2RU 4-Node Computing-Node)	Bei dieser Konfiguration wird standardmäßig vSphere Standard Switch verwendet. Für die optionale Verwendung von vSphere Distributed Switch ist eine VMware Enterprise Plus-Lizenzierung erforderlich.

NetApp HCI und ONTAP Select Lizenzierung

Falls Sie eine Version von ONTAP Select zur Verwendung in Verbindung mit einem erworbenen NetApp HCI System bereitgestellt wurden, gelten die folgenden zusätzlichen Einschränkungen:

- Die ONTAP Select Lizenz, die im Paket mit einem NetApp HCI Systemverkauf angeboten wird, darf nur in Verbindung mit den NetApp HCI Computing-Nodes verwendet werden.
- Der Storage für diese ONTAP Select Instanzen muss sich nur auf den NetApp HCI Storage-Nodes befinden.
- Die Verwendung von Computing-Nodes von Drittanbietern oder Storage-Nodes von Drittanbietern ist untersagt.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Maximale Konfigurationswerte für NetApp Hybrid Cloud Control

NetApp HCI umfasst NetApp Hybrid Cloud Control zur Vereinfachung von Computing-Lebenszyklus und Storage-Management. Die Lösung unterstützt Upgrades von Element Software auf Storage-Nodes für NetApp HCI und NetApp SolidFire Storage-Cluster sowie Firmware-Upgrades für NetApp HCI Computing-Nodes in NetApp HCI. Er ist standardmäßig auf den Management-Nodes in NetApp HCI verfügbar.

NetApp Hybrid Cloud Control kommuniziert nicht nur über die von NetApp bereitgestellten Hardware- und Software-Komponenten in einer NetApp HCI-Installation, sondern interagiert auch mit Komponenten anderer Anbieter in der Kundenumgebung wie VMware vCenter. NetApp stimmt die Funktionen von NetApp Hybrid Cloud Control und seine Interaktion mit diesen Drittanbieterkomponenten in der Kundenumgebung auf ein bestimmtes Maß ab. Für optimale Benutzerfreundlichkeit mit NetApp Hybrid Cloud Control empfiehlt NetApp, innerhalb verschiedener Konfigurationsmaxima zu bleiben.

Wenn Sie diese getesteten Grenzwerte überschreiten, treten möglicherweise Probleme mit NetApp Hybrid Cloud Control auf, z. B. eine langsamere Benutzeroberfläche, API-Antworten oder Funktionen, die nicht verfügbar sind. Wenn Sie NetApp für Produkt-Support mit NetApp Hybrid Cloud Control in Umgebungen einsetzen, die über die Konfigurationsmaxima hinausgehen, wird NetApp Support bitten, dass Sie die Konfiguration innerhalb der dokumentierten Konfigurationsmaxima ändern.

Konfigurationsmaxima

NetApp Hybrid Cloud Control unterstützt VMware vSphere-Umgebungen mit bis zu 100 ESXi-Hosts und 1000 virtuellen Maschinen (vergleichbar mit einer kleinen vCenter Server Appliance-Konfiguration).

NetApp HCI-Sicherheit

Beim Einsatz von NetApp HCI werden Ihre Daten durch branchenübliche Sicherheitsprotokolle gesichert.

Verschlüsselung für Storage-Nodes im Ruhezustand

NetApp HCI ermöglicht Ihnen die Verschlüsselung aller im Storage-Cluster gespeicherten Daten.

Alle Laufwerke in Storage-Nodes, die zu Verschlüsselung fähig sind, verwenden die AES-256-Bit-Verschlüsselung auf Laufwerksebene. Jedes Laufwerk verfügt über einen eigenen Verschlüsselungsschlüssel,

der beim ersten Initialized des Laufwerks erstellt wird. Wenn Sie die Verschlüsselungsfunktion aktivieren, wird ein Storage-Cluster-weites Passwort erstellt und Datenblöcke des Passworts werden dann auf alle Nodes im Cluster verteilt. Kein Single Node speichert das gesamte Passwort. Das Passwort wird dann verwendet, um den gesamten Zugriff auf die Laufwerke kennwortgeschützt zu machen. Sie benötigen das Passwort, um das Laufwerk zu entsperren. Da das Laufwerk alle Daten verschlüsselt, sind Ihre Daten jederzeit sicher.

Wenn Sie die Verschlüsselung im Ruhezustand aktivieren, werden die Performance und die Effizienz des Storage-Clusters nicht beeinträchtigt. Wenn Sie ein verschlüsselungsfähiges Laufwerk oder Node mit der Element API oder der Element UI aus dem Storage-Cluster entfernen, werden die Laufwerke im Ruhezustand deaktiviert. Zudem werden die Laufwerke sicher gelöscht, sodass die zuvor auf diesen Laufwerken gespeicherten Daten geschützt sind. Nachdem Sie das Laufwerk entfernt haben, können Sie das Laufwerk mit der API-Methode sicher löschen `SecureEraseDrives`. Wenn Sie ein Laufwerk oder einen Node aus dem Speicher-Cluster entfernen, bleiben die Daten durch das Cluster-weite Passwort und die individuellen Verschlüsselungsschlüssel des Laufwerks geschützt.

Informationen zum Aktivieren und Deaktivieren der Verschlüsselung im Ruhezustand finden Sie "Aktivieren und Deaktivieren der Verschlüsselung für ein Cluster" im SolidFire und Element Documentation Center.

Softwareverschlüsselung für Daten im Ruhezustand

Mithilfe der Softwareverschlüsselung können alle auf die SSDs in einem Storage-Cluster geschriebenen Daten verschlüsselt werden. Dies bietet eine primäre Verschlüsselungsschicht in SolidFire SDS-Nodes ohne Self-Encrypting Drives (SEDs).

Externes Verschlüsselungskeymanagement

Sie können Element Software für das Management der Storage-Cluster-Verschlüsselungen konfigurieren, indem Sie einen KMIP-konformen (Key Management Service) eines Drittanbieters verwenden. Wenn Sie diese Funktion aktivieren, wird der Schlüssel für den Zugriff auf das Passwort für den gesamten Laufwerkszugriff des Storage-Clusters von einem von Ihnen angegebenen KMS gemanagt. Element kann die folgenden wichtigen Managementservices nutzen:

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

Weitere Informationen zum Konfigurieren der externen Schlüsselverwaltung finden Sie unter "Erste Schritte mit External Key Management" im Dokumentationszentrum für SolidFire und Elemente.

Multi-Faktor-Authentifizierung

Multi-Faktor-Authentifizierung (MFA) ermöglicht es Benutzern, bei der Anmeldung mehrere Arten von Beweisen zur Authentifizierung bei der NetApp Element Web-UI oder der Storage-Node-UI vorzulegen. Sie können Element so konfigurieren, dass nur Multi-Faktor-Authentifizierung für Anmeldungen akzeptiert wird, die sich in Ihr vorhandenes Benutzerverwaltungssystem und Ihren Identitäts-Provider integrieren lassen. Sie können das Element so konfigurieren, dass es sich in einen vorhandenen SAML 2.0-Identitätsanbieter integrieren lässt, der mehrere Authentisierungsschemata wie Passwort- und Textnachricht, Passwort- und E-Mail-Nachricht oder andere Methoden durchsetzen kann.

Sie können Multi-Faktor-Authentifizierung mit gängigen SAML 2.0-kompatiblen Identitäts-Providern (IDPs) wie

Microsoft Active Directory Federation Services (ADFS) und Shibboleth kombinieren.

Informationen zur Konfiguration von MFA finden Sie unter "Aktivieren der Multi-Faktor-Authentifizierung" im SolidFire and Element Documentation Center.

FIPS 140-2 für HTTPS und Verschlüsselung von Daten im Ruhezustand

NetApp SolidFire Storage-Cluster und NetApp HCI Systeme unterstützen eine Verschlüsselung, die die Anforderungen des Federal Information Processing Standard (FIPS) 140-2 an kryptografische Module erfüllt. Sie können die Compliance mit FIPS 140-2 auf Ihrem NetApp HCI oder SolidFire Cluster sowohl für HTTPS-Kommunikation als auch für Laufwerkverschlüsselung aktivieren.

Wenn Sie den FIPS 140-2 Betriebsmodus auf dem Cluster aktivieren, aktiviert das Cluster das NetApp Cryptographic Security Module (NCSM) und nutzt die zertifizierte Verschlüsselung nach FIPS 140-2 Level 1 für die gesamte Kommunikation über HTTPS mit der NetApp Element UI und den API. Sie verwenden die `EnableFeature` Element API mit dem `fips` Parameter zur Aktivierung der FIPS 140-2-HTTPS-Verschlüsselung. Auf Storage-Clustern mit FIPS-kompatibler Hardware können Sie mithilfe der Element API mit dem `FipsDrives` Parameter auch die FIPS-Laufwerksverschlüsselung für Daten im Ruhezustand aktivieren `EnableFeature`.

Weitere Informationen zur Vorbereitung eines neuen Storage-Clusters für die Verschlüsselung nach FIPS 140-2 finden Sie unter "Erstellung eines Clusters, das FIPS-Laufwerke unterstützt".

Weitere Informationen zur Aktivierung von FIPS 140-2 auf einem vorhandenen, vorbereiteten Cluster finden Sie unter "Die API für das EnableFeature-Element".

Leistung und Servicequalität

Ein SolidFire Storage Cluster bietet QoS-Parameter (Quality of Service) für einzelne Volumes. Sie können die Cluster-Performance, die in ein- und Ausgaben pro Sekunde (IOPS) gemessen wird, mit drei konfigurierbaren Parametern garantieren, die QoS definieren: Das IOPS-Minimum, das IOPS-Maximum und die Burst-IOPS.

SolidFire Active IQ verfügt über eine Seite mit QoS-Empfehlungen zur optimalen Konfiguration und Einrichtung von QoS-Einstellungen.

Parameter für die Servicequalität

IOPS-Parameter werden folgendermaßen definiert:

- **Minimum IOPS** - die Mindestanzahl kontinuierlicher ein- und Ausgänge pro Sekunde (IOPS), die der Storage Cluster einem Volume zur Verfügung stellt. Die für ein Volume konfigurierten IOPS-Mindestwerte sind das garantierte Performance-Niveau für ein Volume. Die Performance sinkt nicht unter dieses Niveau.
- **Maximale IOPS** - die maximale Anzahl an anhaltenden IOPS, die der Storage Cluster einem Volume zur Verfügung stellt. Wenn Cluster-IOPS-Niveaus kritisch hoch sind, wird diese IOPS-Performance nicht überschritten.
- **Burst IOPS** - die maximale Anzahl von IOPS in einem kurzen Burst Szenario erlaubt. Wenn ein Volume unter dem IOPS-Maximum ausgeführt wurde, werden Burst Credits gesammelt. Wenn Performance-Level sehr hoch sind und auf ein Maximum geschoben werden, sind kurze Anstiegen von IOPS auf dem Volume zulässig.

Element Software verwendet Burst IOPS, wenn ein Cluster eine niedrige IOPS-Auslastung aufweist.

Ein einzelnes Volume kann Burst-IOPS anhäufen und die Gutschriften verwenden, um über ihren maximalen IOPS bis zu ihrem IOPS-Burst-Level für einen festgelegten „Burst-Zeitraum“ zu steigen. Ein Volume kann bis zu 60 Sekunden lang hochgehen, wenn das Cluster über die Kapazität verfügt, um die Burst-Kapazität aufzunehmen. Ein Volume kann für jede Sekunde, in der das Volume unter seinem maximalen IOPS-Limit ausgeführt wird, eine Sekunde Burst Credit (bis zu einem Maximum von 60 Sekunden) angesammelt werden.

Die IOPS-Burst-IOPS-Werte sind auf zwei Arten begrenzt:

- Ein Volume kann für einige Sekunden einen Spitzenwert über dem maximalen IOPS erzielen, der der Anzahl der Burst Credits entspricht, die es beim Volume gesammelt hat.
- Wenn ein Volume über die Einstellung für maximale IOPS platzt, ist es durch die Einstellung für Burst IOPS eingeschränkt. Daher überschreitet der IOPS-Burst niemals die Burst-IOPS-Einstellung für das Volume.

- **Effektive max. Bandbreite** - die maximale Bandbreite wird berechnet, indem die Anzahl der IOPS (basierend auf der QoS-Kurve) mit der I/O-Größe multipliziert wird.

  Beispiel: QoS-Parametereinstellungen für 100 Min IOPS, 1000 Max IOPS und 1500 Burst IOPS wirken sich auf die Performance-Qualität aus:

  - Workloads können ein Maximum von 1000 IOPS erreichen und halten, bis sich der Zustand von Workload-Engpässen für IOPS im Cluster bemerkbar macht. Die IOPS werden dann inkrementell reduziert, bis sich die IOPS auf allen Volumes innerhalb der designierten QoS-Bereiche befinden und die Konflikte für die Performance sinken.
  - Die Performance auf allen Volumes wird über den Mindestwert von 100 IOPS erreicht. Die Werte sinken nicht unter die Einstellung für Min IOPS, könnten aber bei Entlastung der Workloads über 100 IOPS bleiben.
  - Die Performance beträgt in einem kontinuierlichen Zeitraum niemals mehr als 1000 IOPS oder weniger als 100 IOPS. Die Performance von 1500 IOPS (Burst IOPS) ist zulässig, aber nur für die Volumes, die Burst Credits aufgesammelt haben, wenn sie unter dem IOPS-Maximum laufen und nur für kurze Zeit zulässig sind. Burst-Werte werden niemals aufrechterhalten.

QoS-Wertbegrenzungen

Hier sind die möglichen Mindest- und Höchstwerte für QoS.

Parameter	Mindestwert	Standard	4 4 KB	5 8 KB	6 16 KB	262KB
IOPS-Minimum	50	50	15.000	9,375*	5556*	385*
IOPS-Maximum	100	15.000	200,000**	125.000	74.074	5128
IOPS-Burst	100	15.000	200,000**	125.000	74,074	5128

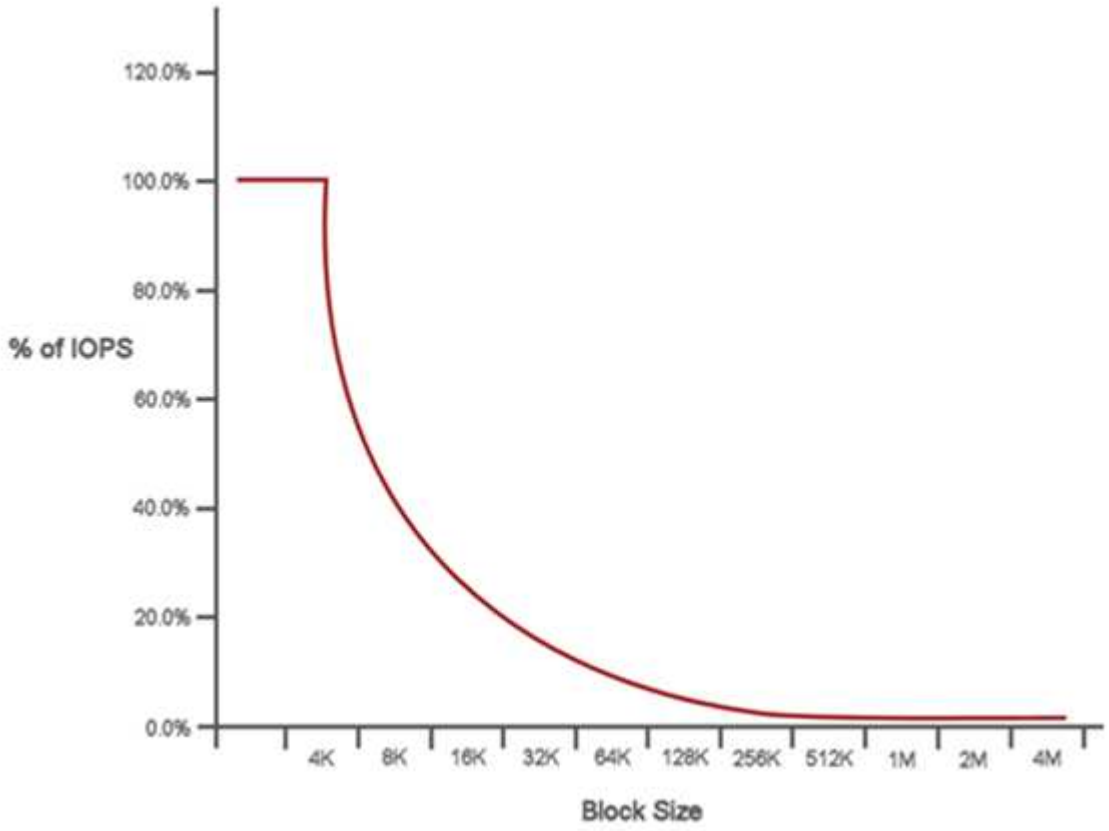
*Diese Schätzungen sind ungefähr. **Maximale IOPS und Burst IOPS können auf 200,000 gesetzt werden. Diese Einstellung ist jedoch nur erlaubt, die Performance eines Volumes effektiv zu nutzen. Die tatsächliche maximale Performance eines Volumes wird durch die Auslastung des Clusters und die Performance pro Node begrenzt.

QoS-Performance

Die QoS-Performance-Kurve zeigt die Beziehung zwischen Blockgröße und dem Prozentsatz der IOPS.

Die Blockgröße und die Bandbreite haben direkte Auswirkungen auf die Anzahl der IOPS, die eine Applikation erreichen kann. Element Software berücksichtigt die Blockgröße, die durch die Normalisierung der Blockgrößen auf 4 kb erhält. Je nach Workload kann das System die Blockgrößen erhöhen. Mit zunehmender Blockgröße erhöht das System die Bandbreite auf ein Niveau, das für die Verarbeitung größerer Blockgrößen erforderlich ist. Mit einer höheren Bandbreite verringert sich auch die Anzahl an IOPS, die das System erreichen kann.

Die QoS-Performance-Kurve zeigt die Beziehung zwischen zunehmenden Blockgrößen und dem sinkenden Prozentsatz an IOPS:



Wenn Blockgröße beispielsweise 4 kb und eine Bandbreite 4000 kbit/s beträgt, betragen die IOPS 1000. Bei einer Blockgröße von bis zu 8.000 USD erhöht sich die Bandbreite auf 5000 kBit/s und der IOPS-Wert sinkt auf 625. Unter Berücksichtigung der Blockgröße übernimmt das System dafür, dass Workloads mit niedrigerer Priorität, bei denen größere Blockgrößen zum Beispiel Backups und Hypervisor-Aktivitäten verwendet werden, nicht zu viele der Performance in Anspruch nehmen, die durch Datenverkehr mit höherer Priorität durch kleinere Blöcke benötigt wird.

QoS-Richtlinien (QoS

Mit einer QoS-Richtlinie können Sie standardisierte Quality-of-Service-Einstellungen erstellen und speichern, die auf viele Volumes angewendet werden können.

QoS-Richtlinien eignen sich am besten für Serviceumgebungen, beispielsweise mit Datenbank-, Applikations- oder Infrastrukturservern, die selten neu gestartet werden und den konstanten Zugriff auf den Storage benötigen. Einzelne Volume-QoS eignet sich am besten für lichtstarke VMs, z. B. virtuelle Desktops oder

spezielle VMs mit Kiosk-Typ. Diese können täglich neu gestartet, eingeschaltet oder mehrfach ausgeschaltet werden.

QoS- und QoS-Richtlinien sollten nicht gemeinsam eingesetzt werden. 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.

Der ausgewählte Cluster muss zur Verwendung von QoS-Richtlinien Element 10.0 oder höher sein. Anderenfalls sind QoS-Richtlinienfunktionen nicht verfügbar.

Weitere Informationen

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

Anforderungen und Vorbereitstellungs-Aufgaben zu erfüllen

Anforderungen für die NetApp HCI-Implementierung – Überblick

NetApp HCI verfügt über spezifische physische und Netzwerkanforderungen für den ordnungsgemäßen Betrieb im Datacenter. Stellen Sie sicher, dass Sie die folgenden Anforderungen und Empfehlungen implementieren, bevor Sie mit der Implementierung beginnen.

Bevor Sie die NetApp HCI Hardware erhalten, sollten Sie sicherstellen, dass Sie die Checklisten im Arbeitsbuch zur Vorabimplementierung von NetApp Professional Services ausfüllen. Dieses Dokument enthält eine Liste mit Aufgaben, die Sie bewältigen müssen, um Ihr Netzwerk und Ihre Umgebung auf eine erfolgreiche NetApp HCI-Bereitstellung vorzubereiten.

Im Folgenden finden Sie die Links zu den Anforderungen und Aufgaben vor der Implementierung:

- "Anforderungen an Netzwerk-Ports"
- "Netzwerk- und Switch-Anforderungen"
- "Anforderungen an die Netzwerkkabel"
- "Anforderungen an die IP-Adresse"
- "Netzwerkkonfiguration"
- "DNS- und Zeitdaueranforderungen"
- "Umweltanforderungen"
- "Sicherungsdomänen"
- "Ressourcenanforderungen von Witness Node für Storage Cluster mit zwei Nodes"

Weitere Informationen

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

Anforderungen an Netzwerk-Ports

Möglicherweise müssen Sie die folgenden Ports durch die Edge-Firewall Ihres Datacenters zulassen, damit Sie das System Remote managen, Clients außerhalb Ihres Datacenters die Verbindung zu Ressourcen ermöglichen und sicherstellen können, dass die internen Services ordnungsgemäß funktionieren. Einige dieser Ports, URLs oder IP-Adressen sind je nach Nutzung des Systems möglicherweise nicht erforderlich.

Alle Ports sind TCP, sofern nicht anders angegeben, und alle TCP-Ports müssen die Dreiwege-Handshake-Kommunikation zwischen dem NetApp-Supportserver, dem Verwaltungsknoten und den Knoten unterstützen, auf denen die Element-Software ausgeführt wird. Beispielsweise kommuniziert der Host auf einem Management-Knoten über TCP-Port 443 mit dem Host auf einem Speicher-Cluster-MVIP-Ziel, und der Ziel-

Host kommuniziert über einen beliebigen Port zurück zum Quellhost.

Die folgenden Abkürzungen werden in der Tabelle verwendet:

- MIP: Management-IP-Adresse, eine Adresse pro Node
- SIP: Speicher-IP-Adresse, eine Adresse pro Knoten
- MVIP: Management der virtuellen IP-Adresse
- SVIP: Virtuelle Speicher-IP-Adresse

Quelle	Ziel	Port	Beschreibung
BMC/IPMI für Computing-Node	Management-Node	111 TCP/UDP	API-Kommunikation mit NetApp Hybrid Cloud Control
BMC/IPMI für Computing-Node	Management-Node	137-138 UDP	API-Kommunikation mit NetApp Hybrid Cloud Control
BMC/IPMI für Computing-Node	Management-Node	445	API-Kommunikation mit NetApp Hybrid Cloud Control
BMC/IPMI für Computing-Node	Management-Node	623 UDP	RMCP-Anschluss (Remote Management Control Protocol) Erforderlich für Upgrades der NetApp Hybrid Cloud Control Computing-Firmware
BMC/IPMI für Computing-Node	Management-Node	2049 TCP/UDP	API-Kommunikation mit NetApp Hybrid Cloud Control
ISCSI-Clients	Speicher-Cluster MVIP	443	(Optional) UI- und API-Zugriff
ISCSI-Clients	Speicher-Cluster SVIP	3260	ISCSI-Kommunikation des Clients
ISCSI-Clients	Storage-Node SIP	3260	ISCSI-Kommunikation des Clients
Management-Node	`sfsupport.solidfire.com`	22	Reverse-SSH-Tunnel für den Support-Zugriff
Management-Node	Storage-Node MIP	22	SSH-Zugriff für die Unterstützung
Management-Node	DNS-Server	53 TCP/UDP	DNS-Suche
Management-Node	BMC/IPMI für Computing-Node	139	API-Kommunikation mit NetApp Hybrid Cloud Control

Quelle	Ziel	Port	Beschreibung
Management-Node	Storage-Node MIP	442	UI- und API-Zugriff auf Upgrades von Storage-Node und Element Software
Management-Node	Storage-Node MVIP	442	UI- und API-Zugriff auf Upgrades von Storage-Node und Element Software
Management-Node	`23.32.54.122`, `216.240.21.15`	443	Upgrades für Element Software
Management-Node	Baseboard Management Controller (BMC)	443	Hardware-Überwachung und Bestandsverbindung (Redfish- und IPMI-Befehle)
Management-Node	BMC/IPMI für Computing-Node	443	HTTPS-Kommunikation mit NetApp Hybrid Cloud Control
Management-Node	`monitoring.solidfire.com`	443	Berichterstellung für den Storage-Cluster an Active IQ
Management-Node	Speicher-Cluster MVIP	443	UI- und API-Zugriff auf Upgrades von Storage-Node und Element Software
Management-Node	VMware vCenter	443	HTTPS-Kommunikation mit NetApp Hybrid Cloud Control
Management-Node	BMC/IPMI für Computing-Node	623 UDP	RMCP-Anschluss (Remote Management Control Protocol) Erforderlich für Upgrades der NetApp Hybrid Cloud Control Computing-Firmware
Management-Node	BMC/IPMI für Storage-Node	623 UDP	RMCP-Anschluss Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
Management-Node	VMware vCenter	5988-5989	HTTPS-Kommunikation mit NetApp Hybrid Cloud Control
Management-Node	Witness Node	9442	Konfigurations-API-Service pro Node

Quelle	Ziel	Port	Beschreibung
Management-Node	VCenter Server	9443	VCenter Plug-in-Registrierung: Der Port kann nach Abschluss der Registrierung geschlossen werden.
SNMP-Server	Speicher-Cluster MVIP	161 UDP	SNMP-Abfrage
SNMP-Server	Storage-Node MIP	161 UDP	SNMP-Abfrage
BMC/IPMI für Storage-Node	Management-Node	623 UDP	RMCP-Anschluss Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
Storage-Node MIP	DNS-Server	53 TCP/UDP	DNS-Suche
Storage-Node MIP	Management-Node	80	Upgrades für Element Software
Storage-Node MIP	S3/Swift-Endpunkt	80	(Optional) HTTP-Kommunikation an S3/Swift-Endpunkt für Backup und Recovery
Storage-Node MIP	NTP-Server	123 UDP	NTP
Storage-Node MIP	Management-Node	162 UDP	(Optional) SNMP-Traps
Storage-Node MIP	SNMP-Server	162 UDP	(Optional) SNMP-Traps
Storage-Node MIP	LDAP-Server	389 TCP/UDP	(Optional) LDAP-Suche
Storage-Node MIP	Management-Node	443	Upgrades für Element Software
Storage-Node MIP	Remote Storage Cluster MVIP	443	Kommunikation über die Verbindung des Remote-Replikationsclusters
Storage-Node MIP	Remote-Speicherknoten MIP	443	Kommunikation über die Verbindung des Remote-Replikationsclusters
Storage-Node MIP	S3/Swift-Endpunkt	443	(Optional) HTTPS-Kommunikation an S3/Swift-Endpunkt für Backup und Recovery
Storage-Node MIP	LDAPS-Server	636 TCP/UDP	LDAPS-Suche
Storage-Node MIP	Management-Node	10514 TCP/UDP, 514 TCP/UDP	Syslog-Weiterleitung
Storage-Node MIP	Syslog-Server	10514 TCP/UDP, 514 TCP/UDP	Syslog-Weiterleitung
Storage-Node MIP	Remote-Speicherknoten MIP	2181	Cluster-übergreifende Kommunikation für Remote-Replizierung

Quelle	Ziel	Port	Beschreibung
Storage-Node SIP	S3/Swift-Endpunkt	80	(Optional) HTTP-Kommunikation an S3/Swift-Endpunkt für Backup und Recovery
Storage-Node SIP	Compute-Knoten SIP	442	API für Computing-Nodes, Konfiguration und Validierung sowie Zugriff auf Softwareinventar
Storage-Node SIP	S3/Swift-Endpunkt	443	(Optional) HTTPS-Kommunikation an S3/Swift-Endpunkt für Backup und Recovery
Storage-Node SIP	Remote-Speicherknoten SIP	2181	Cluster-übergreifende Kommunikation für Remote-Replizierung
Storage-Node SIP	Storage-Node SIP	3260	ISCSI miteinander verbinden
Storage-Node SIP	Remote-Speicherknoten SIP	4000 bis 4020	Remote-Replizierung: Node-to-Node-Datentransfer
System Administrator-PC	Storage-Node MIP	80	(Nur NetApp HCI) Landing Page der NetApp Deployment Engine
System Administrator-PC	Management-Node	442	HTTPS-UI-Zugriff auf den Management-Node
System Administrator-PC	Storage-Node MIP	442	HTTPS-UI- und API-Zugriff auf Storage-Node, (nur NetApp HCI) Konfigurations- und Implementierungsüberwachung in der NetApp Deployment Engine
System Administrator-PC	Computing Node BMC/IPMI H410 und H600 Serie	443	HTTPS-UI- und API-Zugriff auf die Remote-Steuerung des Nodes
System Administrator-PC	Management-Node	443	HTTPS-UI- und API-Zugriff auf den Management-Node
System Administrator-PC	Speicher-Cluster MVIP	443	HTTPS-UI- und API-Zugriff auf das Storage-Cluster
System Administrator-PC	Storage Node BMC/IPMI H410 und H600 Series	443	HTTPS-UI- und API-Zugriff auf die Remote-Steuerung des Nodes

Quelle	Ziel	Port	Beschreibung
System Administrator-PC	Storage-Node MIP	443	Erstellung von HTTPS-Storage-Clustern, UI-Zugriff nach der Implementierung auf das Storage-Cluster
System Administrator-PC	Computing Node BMC/IPMI H410 und H600 Serie	623 UDP	RMCP-Anschluss Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
System Administrator-PC	Storage Node BMC/IPMI H410 und H600 Series	623 UDP	RMCP-Anschluss Dies ist erforderlich, um IPMI-fähige Systeme zu verwalten.
System Administrator-PC	Witness Node	8080	Witness Node pro Node Web-UI
VCenter Server	Speicher-Cluster MVIP	443	VCenter-Plug-in-API-Zugriff
VCenter Server	Management-Node	8443	(Optional) vCenter Plug-in QoSSIOC-Service.
VCenter Server	Speicher-Cluster MVIP	8444	Zugriff auf vCenter VASA Provider (nur VVols)
VCenter Server	Management-Node	9443	VCenter Plug-in-Registrierung: Der Port kann nach Abschluss der Registrierung geschlossen werden.

Weitere Informationen

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

Netzwerk- und Switch-Anforderungen

Die für NetApp HCI verwendeten Switches erfordern eine spezifische Konfiguration, um eine erfolgreiche Implementierung sicherzustellen. In der Switch-Dokumentation finden Sie spezifische Anweisungen zur Implementierung der folgenden Anforderungen an Ihre Umgebung.

Für eine NetApp HCI-Implementierung sind mindestens drei Netzwerksegmente erforderlich, eines für jeden der folgenden Verkehrstypen:

- Vereinfachtes
- VMware vMotion
- Storage/Daten

Je nach den Computing- und Storage-Node-Modellen der NetApp H-Series und der geplanten Verkabelungskonfiguration können diese Netzwerke physisch über separate Switches getrennt oder über VLANs voneinander getrennt werden. Bei den meisten Implementierungen müssen diese Netzwerke (und alle anderen zusätzlichen Virtual-Machine-Netzwerke) mit VLANs logisch voneinander getrennt werden.

Computing- und Storage-Nodes müssen vor, während und nach der Implementierung kommunizieren können. Wenn Sie getrennte Managementnetzwerke für Storage- und Computing-Nodes implementieren, stellen Sie sicher, dass diese Managementnetzwerke Netzwerkrouten zwischen ihnen haben. Diese Netzwerke müssen über Gateways verfügen, und es muss eine Route zwischen den Gateways vorhanden sein. Stellen Sie sicher, dass jedem neuen Node ein Gateway zugewiesen ist, um die Kommunikation zwischen den Nodes und Managementnetzwerken zu erleichtern.

NetApp HCI verfügt über folgende Switch-Anforderungen:

- Alle mit NetApp HCI-Nodes verbundenen Switch-Ports müssen als Spanning Tree Edge Ports konfiguriert werden.
  - Bei Cisco Switches, je nach Switch-Modell, Softwareversion und Porttyp, können Sie dies mit einem der folgenden Befehle ausführen:
    - `spanning-tree port type edge`
    - `spanning-tree port type edge trunk`
    - `spanning-tree portfast`
    - `spanning-tree portfast trunk`
  - Bei Mellanox-Switches können Sie dies mit dem Befehl tun `spanning-tree port type edge`.
- NetApp HCI-Nodes verfügen über redundante Ports für alle Netzwerkfunktionen, ausgenommen Out-of-Band-Management. Für eine optimale Ausfallsicherheit teilen Sie diese Ports auf zwei Switches mit redundanten Uplinks auf eine herkömmliche hierarchische Architektur oder eine Layer-2-Spine-and-Leaf-Architektur.
- Die Switches für Storage, Virtual Machine und vMotion-Datenverkehr müssen Geschwindigkeiten von mindestens 10 GbE pro Port unterstützen (bis zu 25 GbE pro Port werden unterstützt).
- Die Switches, die Managementdatenverkehr verarbeiten, müssen Geschwindigkeiten von mindestens 1 GbE pro Port unterstützen.
- Sie müssen Jumbo Frames auf den Switch Ports konfigurieren, die Storage und vMotion Traffic verarbeiten. Für eine erfolgreiche Installation müssen Hosts 9000-Byte-Pakete lückenlos versenden können.
- Die Netzwerklatenz zwischen allen Storage- und Computing-Nodes sollte 2 ms nicht überschreiten.

Alle NetApp HCI-Nodes bieten zusätzliche Out-of-Band-Managementfunktionen über einen dedizierten Management-Port. Die Nodes der NetApp H300S, H300E, H500S, H500E, H700S, H700E und H410C ermöglichen darüber hinaus den IPMI-Zugriff über Port A. als Best Practice sollten Sie das Remote-Management von NetApp HCI vereinfachen, indem Sie Out-of-Band-Management für alle Nodes in der Umgebung konfigurieren.

Weitere Informationen

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

Anforderungen an die Netzwerkkabel

Sie können die folgenden Richtlinien verwenden, um sicherzustellen, dass Sie über genügend der richtigen Art von Netzwerkkabel für die Größe Ihrer Bereitstellung verfügen. Für RJ45-Ports müssen Kabel nach Kategorie 5e oder Cat 6 verwendet werden.

- 2-Kabel-Computing-Node-Konfiguration: Jeder Computing-Node muss über zwei SFP+/SFP28-Schnittstellen mit einem 10/25-GbE-Netzwerk verbunden werden (optional ist ein zusätzliches Cat 5e/6-Kabel für Out-of-Band-Management erhältlich).
- Konfiguration mit Computing-Nodes mit sechs Kabeln: Jeder Computing-Node muss über vier SFP+/SFP28-Schnittstellen mit einem 10/25-GbE-Netzwerk und über zwei Cat 5e/6-Kabel mit einem 1/10-GbE-Netzwerk verbunden werden (ein zusätzliches Cat 5e/6-Kabel ist optional für Out-of-Band-Management).
- Jeder Storage Node muss über zwei SFP+/SFP28-Schnittstellen mit einem 10/25-GbE-Netzwerk und über zwei Cat 5e/6-Kabel mit einem 1/10-GbE-Netzwerk verbunden sein (ein zusätzliches Cat 5e/6-Kabel ist optional für Out-of-Band-Management).
- Stellen Sie sicher, dass die Netzwerkkabel, die Sie zum Anschließen des NetApp HCI-Systems an Ihr Netzwerk verwenden, lang genug sind, um Ihre Switches bequem zu erreichen.

Für eine Implementierung mit vier Storage-Nodes und drei Computing-Nodes (unter Verwendung der sechs-Kabel-Konfiguration) sind beispielsweise die folgende Anzahl an Netzwerkkabel erforderlich:

- (14) Cat 5e/6-Kabel mit RJ45-Anschlüssen (plus sieben Kabel für IPMI-Datenverkehr, falls gewünscht)
- (20) Twinax-Kabel mit SFP28/SFP+ Anschlüssen

Dies ist auf folgende Gründe zurückzuführen:

- Vier Storage-Nodes benötigen acht (8) Cat 5e/6-Kabel und acht (8) Twinax-Kabel.
- Für drei Computing-Nodes bei der 6-Kabel-Konfiguration sind sechs (6) Cat 5e/6-Kabel und zwölf (12) Twinax-Kabel erforderlich.

> In einer Konfiguration mit sechs Kabeln sind zwei Ports für VMware ESXi reserviert und von der NetApp Deployment Engine eingerichtet und gemanagt. Über die Element TUI oder die Element Web GUI können diese dedizierten ESXi Ports nicht aufgerufen oder gemanagt werden.

Weitere Informationen

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

Anforderungen an die IP-Adresse

NetApp HCI verfügt über spezifische IP-Adressanforderungen, die von der Größe der Implementierung abhängen. Zu beachten ist, dass die anfänglichen IP-Adressen, die Sie jedem Node zugewiesen haben, bevor Sie die NetApp Deployment Engine zur Implementierung des Systems verwenden, temporär sind und nicht wiederverwendet werden können. Sie müssen eine zweite permanente Gruppe nicht verwendeter IP-

Adressen festlegen, die Sie während der endgültigen Bereitstellung zuweisen können.

Anzahl der pro NetApp HCI Implementierung benötigten IP-Adressen

Das NetApp HCI-Storage-Netzwerk und das Management-Netzwerk sollten jeweils separate, zusammenhängende Bereiche der IP-Adressen verwenden. In der folgenden Tabelle können Sie ermitteln, wie viele IP-Adressen Sie für Ihre Implementierung benötigen:

Systemkomponente	Management-Netzwerk-IP-Adressen erforderlich	Erforderliche Storage-Netzwerk-IP-Adressen	VMotion Netzwerk-IP-Adressen erforderlich	Insgesamt pro Komponente benötigte IP-Adressen
Computing-Node	1	2	1	4
Storage-Node	1	1		2
Storage-Cluster	1	1		2
VMware vCenter	1			1
Management-Node	1	1		2
Witness Node	1	1		2 pro Witness Node (für jeden Storage-Cluster mit zwei oder drei Nodes werden zwei Witness-Nodes implementiert)

IP-Adressen, die von NetApp HCI reserviert werden

NetApp HCI behält sich die folgenden IP-Adressbereiche für Systemkomponenten vor. Vermeiden Sie bei der Planung Ihres Netzwerks die Verwendung dieser IP-Adressen:

IP-Adressbereich	Beschreibung
10.0.0.0/24	Overlay-Netzwerk Docker
10.0.1.0/24	Overlay-Netzwerk Docker
10.255.0.0/16	Docker Swarm Ingress-Netzwerk
169.254.100.1/22	Docker Bridge-Netzwerk
169.254.104.0/22	Docker Bridge-Netzwerk

Weitere Informationen

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

Netzwerkkonfiguration

Netzwerkkonfiguration

NetApp HCI kann mehrere verschiedene Netzwerkverkabelungen und VLAN-Konfigurationen nutzen. Es ist wichtig, Ihre Netzwerkkonfiguration zu planen, um eine erfolgreiche Bereitstellung sicherzustellen.

Erforderliche Netzwerksegmente

NetApp HCI erfordert mindestens drei Netzwerksegmente: Management-, Storage- und Virtualisierungsverkehr (einschließlich Virtual Machines und VMware vMotion Traffic). Ebenso lässt sich der Datenverkehr von Virtual Machines und vMotion trennen. Diese Netzwerksegmente bestehen in der Regel als logisch getrennte VLANs in der NetApp HCI-Netzwerkinfrastruktur.

Die Verbindung von Computing- und Storage-Nodes mit diesen Netzwerken hängt davon ab, wie das Netzwerk entworfen und die Nodes verkabeln. Die Beispielnetzwerke in diesem Handbuch gehen von den folgenden Netzwerken aus:

Netzwerkname	VLAN-ID
Vereinfachtes	100
Storage	105
VMotion	107
Virtual Machines	200, 201

Damit Ihre NetApp HCI Nodes automatisch erkannt und konfiguriert werden können, müssen Sie über ein Netzwerksegment verfügen, das auf allen Switch-Ports, die für die SFP+/SFP28-Schnittstellen auf den Nodes verwendet werden, als nicht getaggt oder natives VLAN verfügbar ist. Dadurch wird Layer-2-Kommunikation zwischen allen Nodes für die Erkennung und Implementierung ermöglicht. Ohne natives VLAN müssen die SFP+/SFP28 Schnittstellen aller Nodes manuell mit einer VLAN- und IPv4-Adresse konfiguriert werden, damit sie erkannt werden können. In den Beispielen für die Netzwerkkonfiguration in diesem Dokument wird dafür das Managementnetzwerk (VLAN-ID 100) verwendet.

Die NetApp Deployment Engine ermöglicht die schnelle Konfiguration von Netzwerken für Computing- und Storage-Nodes bei der ersten Implementierung. Sie können bestimmte integrierte Management-Komponenten wie vCenter und den Management-Node in ihr eigenes Netzwerksegment platzieren. Diese Netzwerksegmente müssen Routing ermöglichen, damit vCenter und der Management Node mit Storage- und Computing-Managementnetzwerken kommunizieren können. In den meisten Implementierungen verwenden diese Komponenten dasselbe Managementnetzwerk (in diesem Beispiel VLAN-ID 100).

Sie konfigurieren Virtual-Machine-Netzwerke mit vCenter. Das standardmäßige Netzwerk der virtuellen Maschine (Portgruppe „VM_Network“) in NetApp HCI-Bereitstellungen ist ohne VLAN-ID konfiguriert. Wenn Sie mehrere getaggte virtuelle Maschinennetzwerke verwenden möchten (VLAN-IDs 200 und 201 im vorhergehenden Beispiel), müssen Sie diese in die erste Netzwerkplanung einbeziehen.

Netzwerkkonfiguration und Verkabelung

Sie können eine Netzwerkkonfiguration mit zwei Kabeln für die Compute-Nodes H410C verwenden und so die Kabelführung vereinfachen. Diese Konfiguration verwendet zwei SFP+/SFP28 Schnittstellen sowie eine optionale (aber empfohlene) RJ45-Schnittstelle für IPMI-Kommunikation. Diese Nodes können auch eine sechs-Kabel-Konfiguration mit zwei RJ45- und vier SFP28/SFP+-Schnittstellen verwenden.

Die H410S und H610S Storage-Nodes unterstützen eine Netzwerktopologie mit vier Netzwerk-Ports (Ports A bis D).

Computing-Nodes unterstützen je nach Hardwareplattform drei Netzwerktopologien:

Konfigurationsoption	Verkabelung für H410C Nodes	Verkabelung für H610C Nodes	Verkabelung für H615C Nodes
Option A	Zwei Kabel mit den Anschlüssen D und E	Zwei Kabel mit den Anschlüssen C und D	Zwei Kabel mit den Anschlüssen A und B
Option B	Sechs Kabel mit den Anschlüssen A bis F	Nicht verfügbar	Nicht verfügbar
Option C	Ähnlich wie Option B, jedoch mit nativen VLANs (oder „Zugriffs-Ports“) auf dem Switch für Management-, Storage- und vMotion-Netzwerke		

Nodes, die nicht über die richtige Anzahl der verbundenen Kabel verfügen, können nicht an der Bereitstellung teilnehmen. Ein Computing-Node in einer Konfiguration mit sechs Kabeln kann beispielsweise nicht implementiert werden, wenn nur die Ports D und E verbunden sind.

Sie können die NetApp HCI-Netzwerkkonfiguration nach der Implementierung anpassen, um den Infrastrukturanforderungen gerecht zu werden. Wenn Sie jedoch NetApp HCI-Ressourcen erweitern, beachten Sie, dass neue Nodes über dieselbe Kabelkonfiguration wie die vorhandenen Computing- und Storage-Nodes verfügen müssen.

Wenn die NetApp Deployment Engine ausfällt, weil Ihr Netzwerk keine Jumbo Frames unterstützt, können Sie eine der folgenden Problemumgehungen ausführen:

- Verwenden Sie eine statische IP-Adresse, und legen Sie eine MTU (Maximum Transmission Unit) von 9000 Byte im Bond10G-Netzwerk manuell fest.
- Konfigurieren Sie das Dynamic Host Configuration Protocol, um für eine MTU-Schnittstelle mit 9000 Byte im Bond10G-Netzwerk zu werben.

Optionen für die Netzwerkkonfiguration

- "Netzwerkkonfigurationsoption A"
- "Netzwerkkonfigurationsoption B"
- "Netzwerkkonfigurationsoption C"

Weitere Informationen

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

Netzwerkkonfiguration

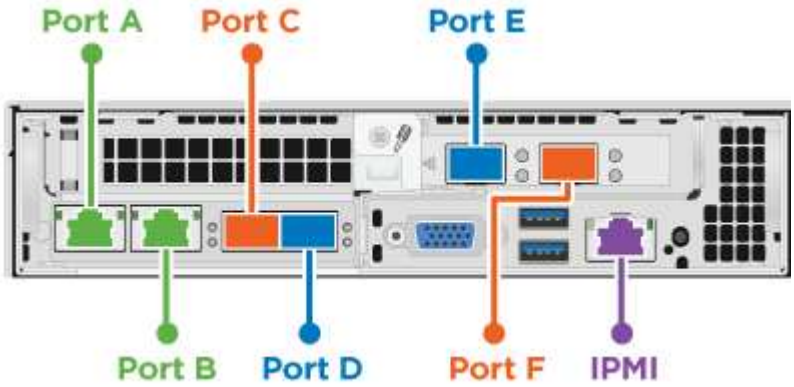
NetApp HCI kann mehrere verschiedene Netzwerkverkabelungen und VLAN-Konfigurationen nutzen. Bei der ersten Konfiguration, Option A, werden für jeden Computing-Node zwei Netzwerkkabel verwendet.

Konfigurationsoption A: Zwei Kabel für Computing-Nodes

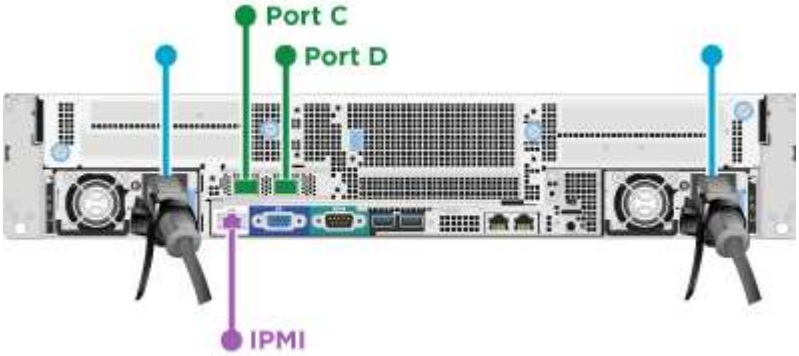
Die Compute-Nodes NetApp H410C, H610C und H615C unterstützen zwei Netzwerkkabel für die Konnektivität zu allen NetApp HCI-Netzwerken. Diese Konfiguration erfordert, dass der Storage, vMotion und alle Netzwerke virtueller Maschinen VLAN Tagging verwenden. Alle Computing- und Storage-Nodes müssen dasselbe VLAN-ID-Schema verwenden. Bei dieser Konfiguration kommen vSphere Distributed Switches zum Einsatz, für die eine Lizenzierung von VMware vSphere Enterprise Plus erforderlich ist.

In der NetApp HCI-Dokumentation werden Buchstaben für die Netzwerkanschlüsse auf der Rückseite der H-Serie-Knoten verwendet.

Im Folgenden sind die Netzwerk-Ports und Standorte auf dem H410C Storage-Node aufgeführt:



Die Netzwerk-Ports und die Standorte auf dem H610C Computing-Node:



Die Netzwerk-Ports und die Standorte auf dem H615C Computing-Node:

Bei dieser Konfiguration werden auf jedem Node die folgenden Netzwerk-Ports verwendet:

Knoten	Verwendete Netzwerkports
H410C	D und E

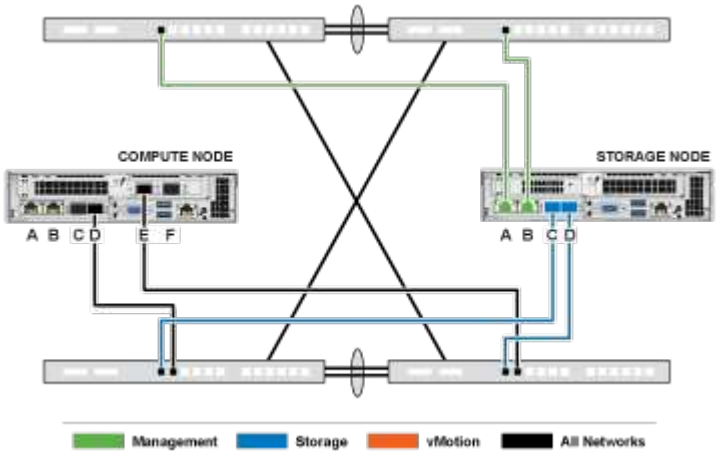
Knoten	Verwendete Netzwerkports
H610C	C und D
H615C	A und B

VLAN-Konfiguration

Als Best Practice sollten Sie die erforderlichen Netzwerksegmente auf allen Switch-Ports konfigurieren, die die Nodes verwenden. Beispiel:

Netzwerkname	VLAN-ID	Switch-Port-Konfiguration
Vereinfachtes	100	Nativ
Storage	105	Getaggt
VMotion	107	Getaggt
Virtual Machines	200, 201	Getaggt

Die folgende Abbildung zeigt die empfohlene Verkabelungskonfiguration für H410C Computing-Nodes mit zwei Kabeln und H410S Storage-Nodes mit vier Kabeln. Alle Switch-Ports in diesem Beispiel teilen sich dieselbe Konfiguration.



Beispiel für Switch-Befehle

Mit den folgenden Beispielbefehlen können Sie alle Switch-Ports konfigurieren, die für NetApp HCI-Nodes verwendet werden. Diese Befehle basieren auf einer Cisco Konfiguration, erfordern jedoch möglicherweise nur kleine Änderungen für Mellanox Switches. In der Switch-Dokumentation finden Sie die spezifischen Befehle, die Sie zur Implementierung dieser Konfiguration benötigen. Ersetzen Sie den Schnittstellennamen, die Beschreibung und das VLAN durch die Werte für Ihre Umgebung.

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

Einige Switches erfordern möglicherweise die Einbeziehung des nativen VLANs in die Liste zulässiger VLANs. Informationen zu Ihrem spezifischen Switch-Modell und der Software-Version finden Sie in der Dokumentation.

Weitere Informationen

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

Netzwerkkonfiguration

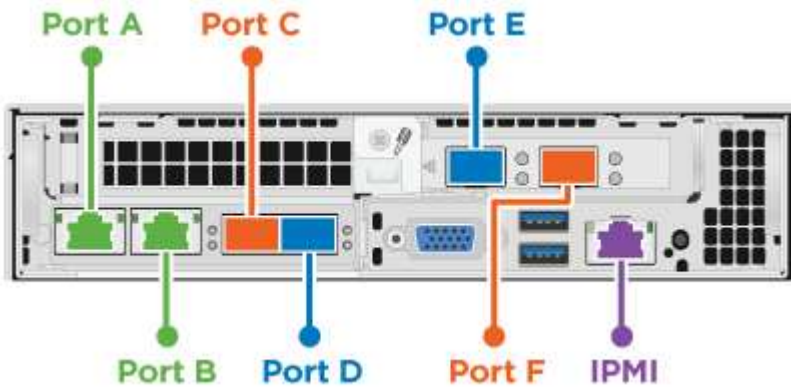
NetApp HCI kann mehrere verschiedene Netzwerkverkabelungen und VLAN-Konfigurationen nutzen. Bei der ersten Konfiguration, Option B, werden für jeden Computing-Node sechs Netzwerkkabel verwendet.

Konfigurationsoption B: Sechs Kabel für Computing-Nodes

Als sekundäre Netzwerkkonfigurationsoption unterstützen die H410C Computing-Nodes den Einsatz von sechs Netzwerkkabel für die Verbindung mit allen NetApp HCI-Netzwerken. Diese Konfiguration erfordert, dass der Storage, vMotion und alle Netzwerke virtueller Maschinen VLAN Tagging verwenden. Sie können diese Konfiguration mit vSphere Standard Switches oder vSphere Distributed Switches (wofür eine Lizenzierung von VMware vSphere Enterprise Plus erforderlich ist) verwenden.

In der NetApp HCI-Dokumentation werden Buchstaben für die Netzwerkanschlüsse auf der Rückseite der H-Serie-Knoten verwendet.

Die Netzwerk-Ports und die Standorte auf dem H410C Computing-Node:



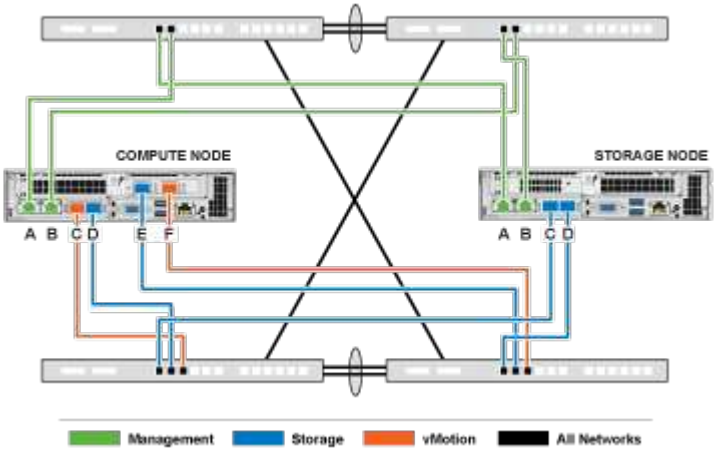
VLAN-Konfiguration

Wenn Sie Computing-Nodes mithilfe von sechs Kabeln und Storage-Nodes mithilfe von vier Kabeln implementieren. Als Best Practice sollten Sie die erforderlichen Netzwerksegmente für alle Switch-Ports, die die Nodes verwenden, konfigurieren. Beispiel:

Netzwerkname	VLAN-ID	Switch-Port-Konfiguration
Vereinfachtes	100	Nativ
Storage	105	Getaggt
VMotion	107	Getaggt

Netzwerkname	VLAN-ID	Switch-Port-Konfiguration
Virtual Machines	200, 201	Getaggt

Die folgende Abbildung zeigt die empfohlene Verkabelungskonfiguration für Compute-Nodes mit sechs Kabeln und Storage-Nodes mit vier Kabeln. Alle Switch-Ports in diesem Beispiel teilen sich dieselbe Konfiguration.



Beispiel für Switch-Befehle

Mit den folgenden Beispielbefehlen können Sie alle Switch-Ports konfigurieren, die für NetApp HCI-Nodes verwendet werden. Diese Befehle basieren auf einer Cisco Konfiguration, erfordern jedoch möglicherweise nur kleine Änderungen für Mellanox Switches. In der Switch-Dokumentation finden Sie die spezifischen Befehle, die Sie zur Implementierung dieser Konfiguration benötigen. Ersetzen Sie den Schnittstellennamen, die Beschreibung und das VLAN durch die Werte für Ihre Umgebung.

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

Einige Switches erfordern möglicherweise die Einbeziehung des nativen VLANs in die Liste zulässiger VLANs. Informationen zu Ihrem spezifischen Switch-Modell und der Software-Version finden Sie in der Dokumentation.

Weitere Informationen

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

Netzwerkkonfiguration

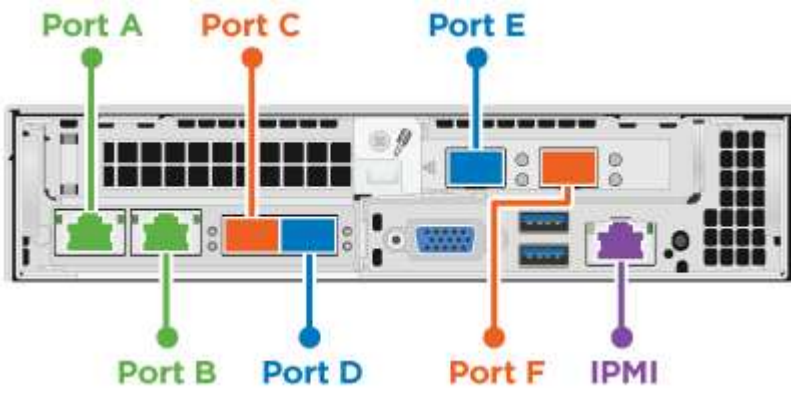
NetApp HCI kann mehrere verschiedene Netzwerkverkabelungen und VLAN-Konfigurationen nutzen. Bei der dritten Konfiguration, Option C, werden sechs Netzwerkkabel für jeden Computing-Node mit nativen VLANs verwendet.

Konfigurationsoption C: Sechs Kabel für Computing-Nodes mit nativen VLANs

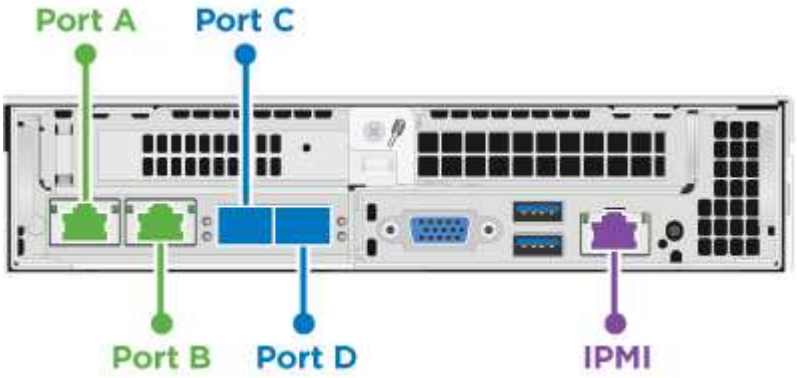
Sie können NetApp HCI bereitstellen, ohne getaggte VLANs für Storage- und Virtualisierungsdatenverkehr zu verwenden. Stattdessen sind Sie auf die Switch-Konfiguration zum Trennen der Netzwerksegmente angewiesen. Sie können diese Konfiguration mit vSphere Standard Switches oder vSphere Distributed Switches (wofür eine Lizenzierung von VMware vSphere Enterprise Plus erforderlich ist) verwenden.

In der NetApp HCI-Dokumentation werden Buchstaben für die Netzwerkanschlüsse auf der Rückseite der H-Serie-Knoten verwendet.

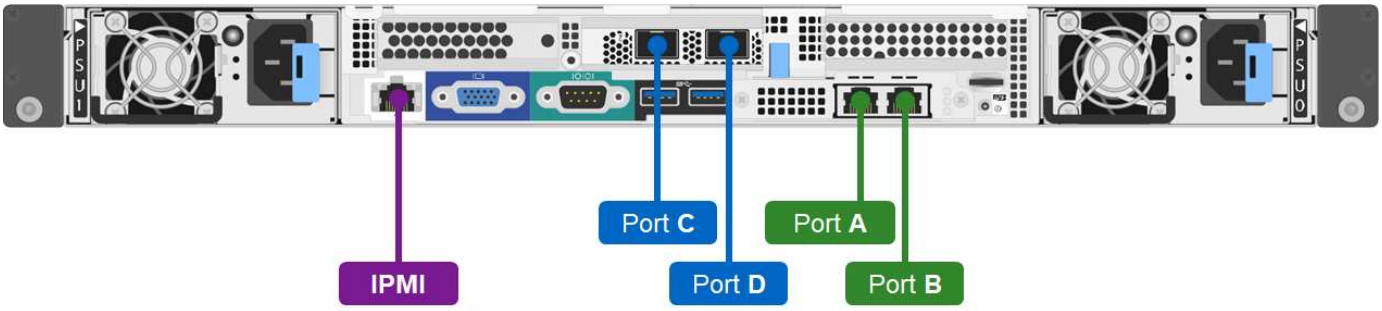
Im Folgenden sind die Netzwerk-Ports und Standorte auf dem H410C Storage-Node aufgeführt:



Im Folgenden sind die Netzwerk-Ports und Standorte auf dem H410S Storage-Node aufgeführt:



Im Folgenden sind die Netzwerk-Ports und Standorte auf dem H610S Storage-Node aufgeführt:



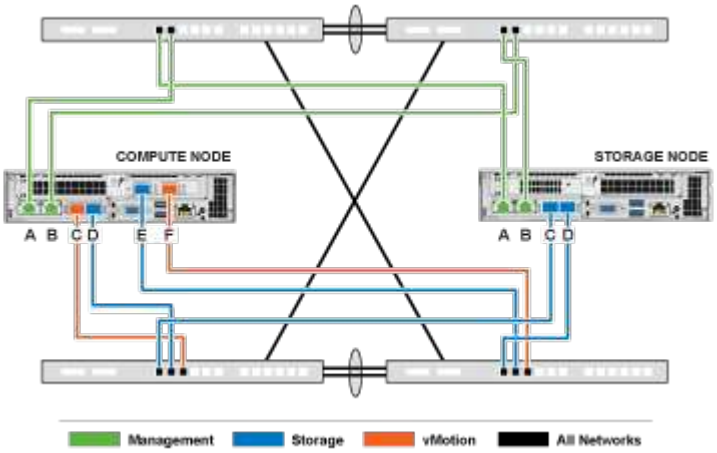
VLAN-Konfiguration für die Nodes H410C, H410S und H610S

Diese Topologieoption verwendet die folgende VLAN-Konfiguration auf den Nodes H410C, H410S und H610S:

Verwendete Node-Ports	Netzwerkname	VLAN-ID	Konfiguration des verbundenen Switch-Ports
Ports A und B auf Computing- und Storage-Nodes	Vereinfachtes	100	Nativ
Die Ports D und E auf Computing-Nodes	Storage	105	Nativ
Die Ports C und D auf Storage-Nodes	Storage	105	Nativ
Die Ports C und F auf Computing-Nodes	VMotion	107	Nativ
Die Ports C und F auf Computing-Nodes	Virtual Machines	200, 201	Getaggt

Achten Sie darauf, die Switch-Ports bei der Implementierung dieser Konfiguration sorgfältig zu konfigurieren. Konfigurationsfehler in dieser Netzwerktopologie können zu Problemen mit der Bereitstellung führen, die sich nur schwer diagnostizieren lassen.

Die folgende Abbildung zeigt die Übersicht über die Netzwerkkonfiguration für diese Topologieoption. Im Beispiel werden einzelne Switch-Ports mit dem entsprechenden Netzwerksegment als natives Netzwerk konfiguriert.



Beispiel für Switch-Befehle

Mit den folgenden Switch-Befehlen können Sie die für die NetApp HCI-Nodes verwendeten Switch-Ports konfigurieren. Diese Befehle basieren auf einer Cisco Konfiguration, erfordern jedoch möglicherweise nur minimale Änderungen für Mellanox Switches. In der Switch-Dokumentation finden Sie die spezifischen Befehle, die Sie zur Implementierung dieser Konfiguration benötigen.

Sie können die folgenden Beispielbefehle verwenden, um die für das Managementnetzwerk verwendeten Switch-Ports zu konfigurieren. Ersetzen Sie den Schnittstellennamen, die Beschreibung und das VLAN durch die Werte für Ihre Konfiguration.

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

Sie können die folgenden Beispielbefehle verwenden, um die für das Speichernetzwerk verwendeten Switch-Ports zu konfigurieren. Ersetzen Sie den Schnittstellennamen, die Beschreibung und das VLAN durch die Werte für Ihre Konfiguration.

```
mtu 9216
switchport access vlan 105
spanning-tree port type edge
```

Sie können die folgenden Beispielbefehle verwenden, um die für das vMotion- und Virtual Machine-Netzwerk verwendeten Switch-Ports zu konfigurieren. Ersetzen Sie den Schnittstellennamen, die Beschreibung und das VLAN durch die Werte für Ihre Konfiguration.

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

Einige Switches erfordern möglicherweise die Einbeziehung des nativen VLANs in die Liste zulässiger VLANs. Informationen zu Ihrem spezifischen Switch-Modell und der Software-Version finden Sie in der Dokumentation.

Weitere Informationen

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

DNS- und Zeitdaueranforderungen

Vor der Bereitstellung müssen Sie DNS-Datensätze (Domain Name System) für Ihr NetApp HCI-System vorbereiten und NTP-Serverinformationen erfassen. Für eine erfolgreiche Bereitstellung ist für NetApp HCI ein DNS-Server mit den richtigen DNS-Einträgen und ein NTP-Server erforderlich.

Vor der Bereitstellung von NetApp HCI folgende Vorbereitungen für DNS und Server treffen:

- Erstellen Sie alle erforderlichen DNS-Einträge für Hosts (z. B. einzelne Rechner- oder Speicherknoten) und dokumentieren Sie, wie die Host-Einträge mit den jeweiligen IP-Adressen übereinstimmen. Während der Bereitstellung müssen Sie Ihrem Storage-Cluster ein Präfix zuweisen, das auf jeden Host angewendet wird. Um Verwirrung zu vermeiden, sollten Sie bei der Auswahl eines Präfixes Ihre DNS-Benennungspläne im Auge behalten.
- Wenn Sie NetApp HCI mit einer neuen VMware vSphere Installation unter Verwendung eines vollständig qualifizierten Domain-Namens implementieren, müssen Sie einen PTR-Datensatz (Pointer) und einen Adressdatensatz (A) für vCenter Server auf einem beliebigen DNS-Server erstellen, der vor der Bereitstellung verwendet wird.
- Wenn Sie NetApp HCI mit einer neuen vSphere Installation mit ausschließlich IP-Adressen implementieren, müssen Sie für vCenter keine neuen DNS-Einträge erstellen.
- NetApp HCI erfordert einen gültigen NTP-Server für die Zeiterfassung. Sie können einen öffentlich

verfügbaren Zeitserver verwenden, wenn Sie keinen in Ihrer Umgebung haben.

- Stellen Sie sicher, dass alle Storage- und Computing-Node-Uhren miteinander synchronisiert sind und dass die Uhren der Geräte, die Sie zum Anmelden bei NetApp HCI verwenden, mit den NetApp HCI-Nodes synchronisiert werden.

Weitere Informationen

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

Umweltanforderungen

Stellen Sie sicher, dass das für die Installation von NetApp HCI verwendete Rack von Steckdosen mit Strom versorgt wird und dass Ihr Rechenzentrum ausreichend gekühlt für die Größe Ihrer NetApp HCI-Installation sorgt.

Detaillierte Informationen zu den Funktionen der einzelnen Komponenten von NetApp HCI finden Sie im NetApp HCI "Datenblatt" .

Der Compute-Node H410C arbeitet nur mit Netzspannung (200-240 V AC). Sie müssen sicherstellen, dass die Stromanforderungen erfüllt sind, wenn Sie einer vorhandenen NetApp HCI-Installation H410C Nodes hinzufügen.

Weitere Informationen

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

Sicherungsdomänen

Die NetApp Element Software unterstützt die Funktionalität von Sicherungsdomänen, die das Datenlayout auf den Storage-Nodes optimiert, um die bestmögliche Datenverfügbarkeit zu erzielen. Um diese Funktion einzusetzen, sollten Sie die Storage-Kapazität gleichmäßig auf drei oder mehr NetApp H-Series Chassis verteilen, um die Storage-Zuverlässigkeit zu optimieren. In diesem Szenario aktiviert der Storage Cluster automatisch die Sicherungsdomänen.

Weitere Informationen

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

Ressourcenanforderungen von Witness Node für Storage Cluster mit zwei Nodes

NetApp HCI unterstützt eine Mindestinstallationsgröße von zwei Storage-Nodes und zwei

Computing-Nodes. Wenn Sie NetApp HCI mit einem Storage Cluster mit zwei oder drei Nodes installieren, müssen Sie die Ressourcenanforderungen der NetApp HCI Witness Nodes und der Virtual Machine (VM) kennen.

Wenn ein Storage-Cluster zwei oder drei Nodes verwendet, wird außerdem neben jedem Storage Cluster ein Paar Witness-Nodes implementiert. Witness-Nodes verfügen über die folgenden VM-Ressourcenanforderungen:

Ressource	Anforderungen
VCPU	4
Speicher	12GB
Festplattengröße	67GB

NetApp HCI unterstützt nur bestimmte Storage-Node-Modelle in Storage-Clustern mit zwei oder drei Nodes. Weitere Informationen finden Sie in den Versionshinweisen für Ihre NetApp HCI-Version.

Best Practice: Konfigurieren Sie die Witness Node VMs so konfigurieren Sie den lokalen Datastore des Computing-Nodes (Standardeinstellung: Nde) und konfigurieren Sie diese nicht auf Shared Storage, z. B. SolidFire Storage Volumes. Um eine automatische Migration der VMs zu verhindern, stellen Sie die Automatisierungsebene des Distributed Resource Scheduler (DRS) der Witness Node VM auf **deaktivierte** ein. Dadurch wird verhindert, dass beide Witness-Nodes auf demselben Computing-Node ausgeführt werden und eine Konfiguration mit einem Hochverfügbarkeitspaar (HA-Paar) erstellt wird.

Wenn der Installationsprozess von NetApp HCI Witness Nodes installiert, wird eine VM-Vorlage in VMware vCenter gespeichert, mit der Sie einen Witness-Node neu bereitstellen können, falls dieser versehentlich entfernt, verloren oder beschädigt wurde. Sie können auch die Vorlage verwenden, um einen Witness Node neu zu implementieren, wenn ein ausgefallener Computing-Node, der den Witness Node hostet, ersetzt werden muss. Anweisungen hierzu finden Sie im Abschnitt **Neuimplementierung Witness Nodes für zwei- und drei-Knoten-Speicher-Cluster** "Hier".

Weitere Informationen

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

Legen Sie los – mit NetApp HCI

Übersicht über die Installation und Implementierung von NetApp HCI

Befolgen Sie diese Anweisungen zur Installation und Implementierung von NetApp HCI. Diese Anweisungen enthalten Links zu weiteren Details.

Hier eine Übersicht über das Verfahren:

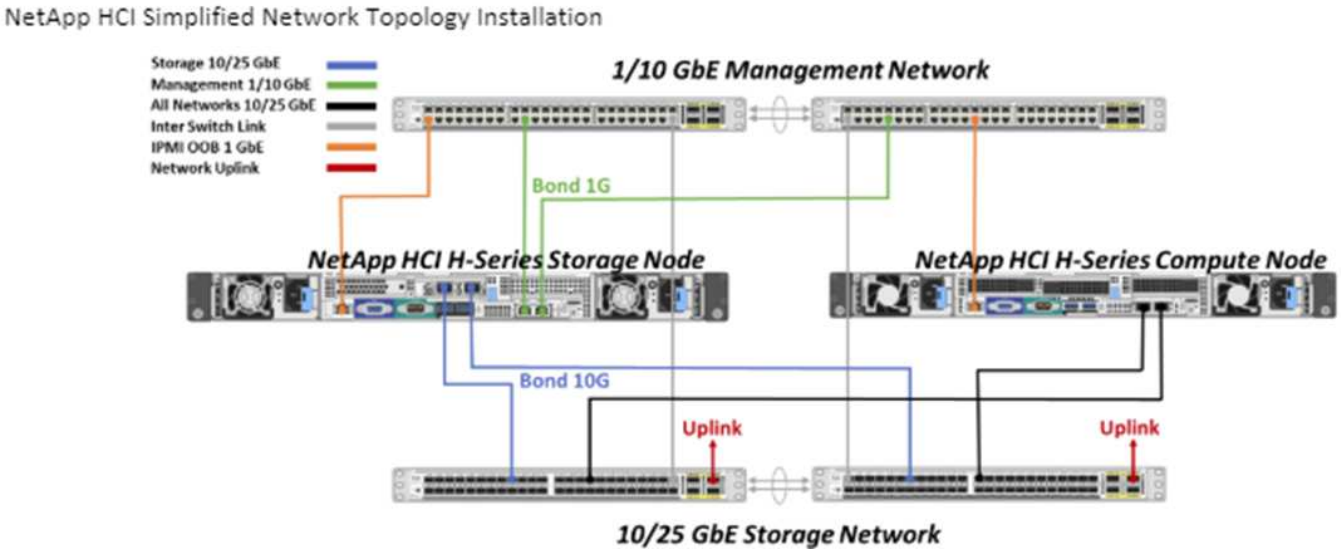
- Installation vorbereiten
- Validieren der Netzwerkbereitschaft mit NetApp Active IQ Config Advisor
- Arbeiten Sie mit Ihrem NetApp Team zusammen
- Installieren Sie die NetApp HCI Hardware
- Führen Sie nach dem Installieren der Hardware optionale Aufgaben aus
- Implementierung von NetApp HCI mit der NetApp Deployment Engine (nde)
- Managen Sie NetApp HCI mit dem vCenter Plug-in
- Monitoring oder Upgrade von NetApp HCI mit der Hybrid Cloud Control

Installation vorbereiten

Bevor Sie mit der Installation beginnen, füllen Sie die Checkliste zur Bestandsaufnahme zum *NetApp HCI Installation Discovery Workbook* aus, die Sie vor dem Erhalt der Hardware erhalten haben.

Bereiten Sie das Netzwerk und die Installationsstandorte vor

Es folgt eine vereinfachte Installation der NetApp HCI-Netzwerktopologie:



Hierbei handelt es sich um eine vereinfachte Netzwerktopologie für einen einzelnen Storage Node und einen einzelnen Computing-Node. Der minimale Cluster für NetApp HCI ist zwei Storage- und zwei Compute-Nodes.

Ihre Netzwerktopologie kann sich von den hier gezeigten unterscheiden. Dies ist nur ein Beispiel.

Für die Verbindung zu allen NetApp HCI-Netzwerken verwendet dieses Setup zwei Netzwerkkabel an den Computing-Nodes.

Lesen Sie diese Ressourcen:

- Verwenden Sie das Arbeitsbuch zur Ermittlung der NetApp HCI-Installation_, um Ihr Netzwerk vor der Installation zu konfigurieren.
- Weitere Informationen und andere unterstützte Konfigurationen finden Sie unter "*TR-4820: Quick Planning Guide für NetApp HCI-Netzwerke*" und "*Installations- und Setup-Anleitung für NetApp HCI*" .
- Informationen zu NetApp HCI-Konfigurationen, die kleiner als vier Storage-Nodes sind, finden Sie unter "*TR-4823: NetApp HCI 2-Node Storage Cluster*".
- Details zur Konfiguration des Link Aggregation Control Protocol (LACP) auf den Switch-Ports, die für jeden der Speicher-Nodes verwendet werden, finden Sie unter "Konfigurieren Sie LCAP, um eine optimale Storage-Performance zu erzielen".

Mit diesem Setup wird der gesamte Datenverkehr auf zwei physische, redundante Ports konsolidiert, die Verkabelung reduziert und die Netzwerkkonfiguration optimiert. Diese Konfiguration erfordert, dass der Storage, vMotion und alle Netzwerksegmente von Virtual Machines VLAN-Tagging verwenden. Das Managementnetzwerk kann natives oder getaggtes VLAN verwenden. Natives VLAN ist jedoch der bevorzugte Modus, sodass die NetApp Deployment Engine (nde) Netzwerkressourcen automatisiert zuweisen kann (Zero Conf).

Dieser Modus erfordert vSphere Distributed Switches (VdS), für die eine Lizenzierung von VMware vSphere Enterprise Plus erforderlich ist.

Netzwerkanforderungen bevor Sie beginnen

Hier sind die wichtigsten Voraussetzungen.

Informationen zu den Voraussetzungen finden Sie unter "Anforderungen für die NetApp HCI-Implementierung – Überblick".

- Bond1G ist eine logische Schnittstelle, die 1-GbE-Netzwerk-Ports auf Storage-Nodes und eine Management-Schnittstelle auf Computing-Nodes kombiniert. Dieses Netzwerk wird für nde API Traffic verwendet. Alle Nodes müssen über die Managementoberfläche im selben L2-Netzwerk kommunizieren können.
- Bond10G ist eine logische Schnittstelle, die 10/25-GbE-Ports kombiniert und von nde für Beaconing und Inventar verwendet wird. Alle Nodes müssen über die Bond10G-Schnittstelle mit nicht fragmentierten Jumbo Frames kommunizieren können.
- Nde benötigt mindestens eine manuell zugewiesene IP-Adresse auf der Bond1G-Schnittstelle auf einem Storage-Node. Nde wird von diesem Node ausgeführt.
- Alle Nodes verfügen über temporäre IP-Adressen, die durch die nde Erkennung zugewiesen werden. Diese erfolgt durch die automatische private IP-Adresse (APIPA).

Während des nde-Prozesses werden allen Nodes permanente IP-Adressen zugewiesen und alle APIPA-zugewiesenen temporären IPs werden freigegeben.

- Nde benötigt für das Management separate Netzwerke, iSCSI und vMotion, die im Switch-Netzwerk

vorkonfiguriert sind.

Validieren der Netzwerkbereitschaft mit NetApp Active IQ Config Advisor

Installieren Sie NetApp Active IQ Config Advisor 5.8.1 oder höher, um die Netzwerkbereitschaft für NetApp HCI zu gewährleisten. Dieses Netzwerkvalidierungstool befindet sich unter anderem "NetApp Support Tools". Mit diesem Tool können Sie Konnektivität, VLAN-IDs, Anforderungen an die IP-Adresse, Switch-Konnektivität und vieles mehr validieren.

Weitere Informationen finden Sie unter "Validieren Sie Ihre Umgebung mit Active IQ Config Advisor"

Arbeiten Sie mit Ihrem NetApp Team zusammen

Ihr NetApp Team überprüft mithilfe des NetApp Active IQ Config Advisor-Berichts und des *Discovery Workbook*, ob Ihre Netzwerkumgebung bereit ist.

Installieren Sie die NetApp HCI Hardware

NetApp HCI kann in unterschiedlichen Konfigurationen installiert werden:

- H410C Compute-Nodes: Konfiguration mit zwei Kabeln oder Konfiguration mit sechs Kabeln
- H610C Computing-Node: Konfiguration mit zwei Kabeln
- H615C Computing-Node: Konfiguration mit zwei Kabeln
- H410S Storage-Node
- H610S Storage-Node

Vorsichtsmaßnahmen und Details finden Sie unter "Hardware der H-Serie installieren".

Schritte

1. Installieren Sie die Schienen und das Gehäuse.
2. Installieren Sie Nodes im Chassis und installieren Sie Laufwerke für Storage-Nodes. (Gilt nur, wenn Sie H410C und H410S in einem NetApp Chassis der H-Serie installieren.)
3. Installieren Sie die Schalter.
4. Verkabeln Sie den Computing-Node.
5. Storage-Node verkabeln.
6. Schließen Sie die Stromkabel an.
7. Schalten Sie die NetApp HCI-Knoten ein.

Führen Sie nach dem Installieren der Hardware optionale Aufgaben aus

Nach der Installation der NetApp HCI Hardware sollten Sie einige optionale, jedoch empfohlene Aufgaben ausführen.

Management von Storage-Kapazität über das gesamte Chassis hinweg

Stellen Sie sicher, dass die Storage-Kapazität gleichmäßig auf alle Chassis mit Storage-Nodes verteilt wird.

Konfigurieren Sie IPMI für jeden Node

Nachdem die NetApp HCI Hardware im Rack montiert, verkabelt und hochgefahren wurde, können Sie für jeden Node den IPMI-Zugriff (Intelligent Platform Management Interface) konfigurieren. Weisen Sie jedem IPMI-Port eine IP-Adresse zu und ändern Sie das Standard-IPMI-Kennwort des Administrators, sobald Sie Remote-IPMI-Zugriff auf den Node haben.

Siehe "IPMI konfigurieren".

Implementierung von NetApp HCI mit der NetApp Deployment Engine (nde)

Die nde Benutzeroberfläche ist die Software-Wizard-Schnittstelle, die zur Installation von NetApp HCI verwendet wird.

Starten Sie die nde UI

NetApp HCI verwendet eine IPv4-Adresse des Storage-Node-Managementnetzwerks zum ersten Zugriff auf die nde. Als Best Practice wird empfohlen, eine Verbindung vom ersten Storage Node herzustellen.

Voraussetzungen

- Sie haben die IP-Adresse des SpeicherNode-Managementnetzwerks bereits manuell oder über DHCP zugewiesen.
- Sie müssen physischen Zugriff auf die NetApp HCI Installation haben.

Schritte

1. Wenn Sie die anfängliche Storage-Node-Management-Netzwerk-IP nicht kennen, verwenden Sie die Terminal User Interface (TUI), die über Tastatur und Monitor auf dem Storage-Node oder zugegriffen wird"Verwenden Sie einen USB-Stick".

   Weitere Informationen finden Sie unter "*Zugriff auf die NetApp Deployment Engine*".

2. Wenn Sie die IP-Adresse von einem Webbrowser aus kennen, stellen Sie eine Verbindung mit der Bond1G-Adresse des primären Knotens über HTTP, nicht mit HTTPS her.

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

Implementieren Sie NetApp HCI mit der nde-UI

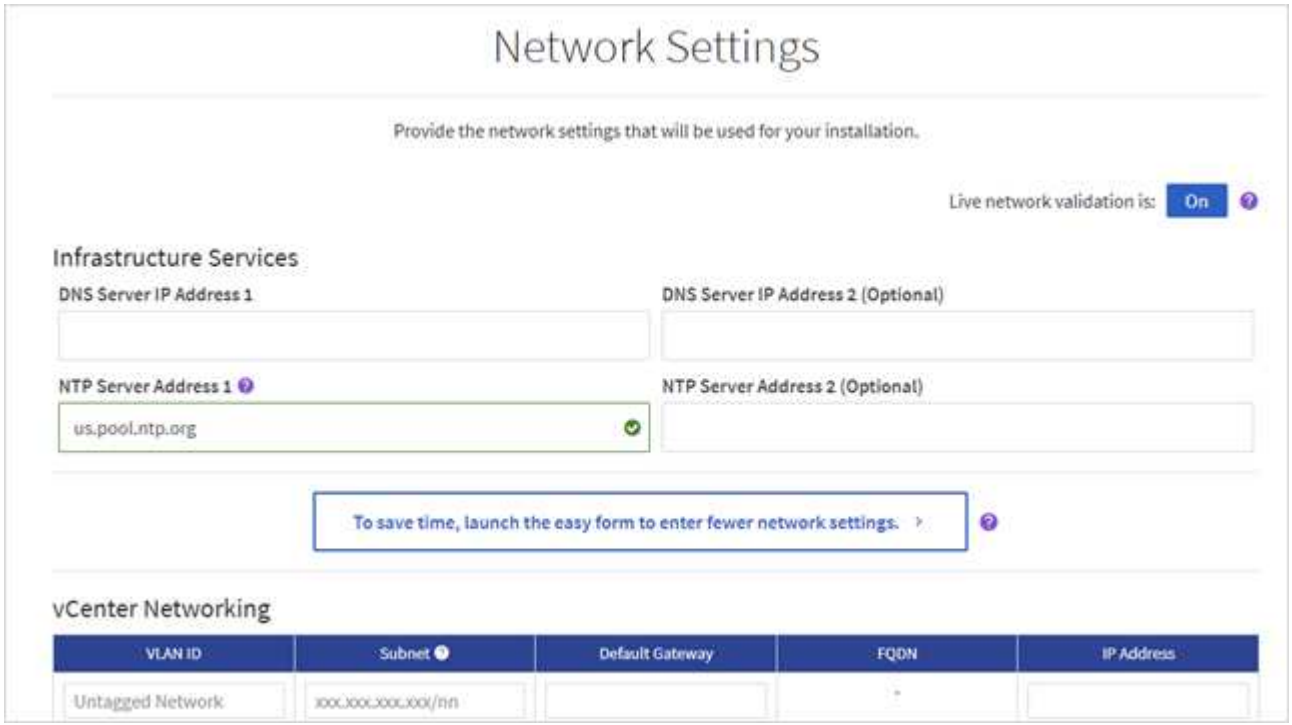
1. Akzeptieren Sie in der nde die Voraussetzungen, prüfen Sie die Nutzung von Active IQ und akzeptieren Sie Lizenzvereinbarungen.
2. Optional können Sie die Data-Fabric-Fileservices durch ONTAP Select aktivieren und die ONTAP Select-Lizenz akzeptieren.
3. Konfigurieren Sie eine neue vCenter-Implementierung. Wählen Sie **Configure using a Fully Qualified Domain Name** aus, und geben Sie sowohl den vCenter Server Domain Name als auch die DNS Server IP-Adresse ein.

   Es wird dringend empfohlen, den FQDN-Ansatz für die vCenter-Installation zu verwenden.

4. Überprüfen Sie, ob die Bestandsbewertung aller Knoten erfolgreich abgeschlossen wurde.

   Der Storage-Node, auf dem die nde ausgeführt wird, wird bereits geprüft.

5. Wählen Sie alle Knoten aus und wählen Sie **Weiter**.
6. Netzwerkeinstellungen konfigurieren. Die zu verwendenden Werte finden Sie im Arbeitsbuch zur Bestandsaufnahme *NetApp HCI Installation*.
7. Wählen Sie das blaue Feld aus, um die einfache Form zu starten.



8. Im Formular „Netzwerkeinstellungen leicht“:
   a. Geben Sie den Namensvorfix ein. (Weitere Informationen finden Sie in den Systemdetails im Arbeitsbuch zur Bestandsaufnahme *NetApp HCI Installation*.)
   b. Wählen Sie **Nein** für werden Sie VLAN-IDs zuweisen? (Sie weisen sie später auf der Seite „Netzwerkeinstellungen“ zu.)
   c. Geben Sie die Subnetz-CIDR-, Standard-Gateway- und IP-Adresse für die Management-, vMotion- und iSCI-Netzwerke gemäß Ihrer Arbeitsmappe ein. (Diese Werte finden Sie im Abschnitt „IP-Zuweisungsmethode“ des Arbeitsbuchs zur Ermittlung der NetApp HCI-Installation_.)
   d. Wählen Sie **auf Netzwerkeinstellungen anwenden**.
9. Mitglied werden "VCenter vorhanden"(optional).
10. Notieren Sie die Seriennummern der Knoten im Arbeitsbuch zur Ermittlung der NetApp HCI-Installation_.
11. Geben Sie eine VLAN-ID für das vMotion Netzwerk und jedes Netzwerk an, das VLAN-Tagging erfordert. Siehe *NetApp HCI Installationsanleitung*.
12. Laden Sie Ihre Konfiguration als CSV-Datei herunter.
13. Wählen Sie **Bereitstellung Starten**.
14. Kopieren Sie die angezeigte URL, und speichern Sie sie.

Die Implementierung dauert etwa 45 Minuten.

Überprüfen Sie die Installation mithilfe des vSphere Web Client

1. Starten Sie den vSphere Web Client und melden Sie sich mit den während der nde Verwendung angegebenen Anmeldeinformationen an.

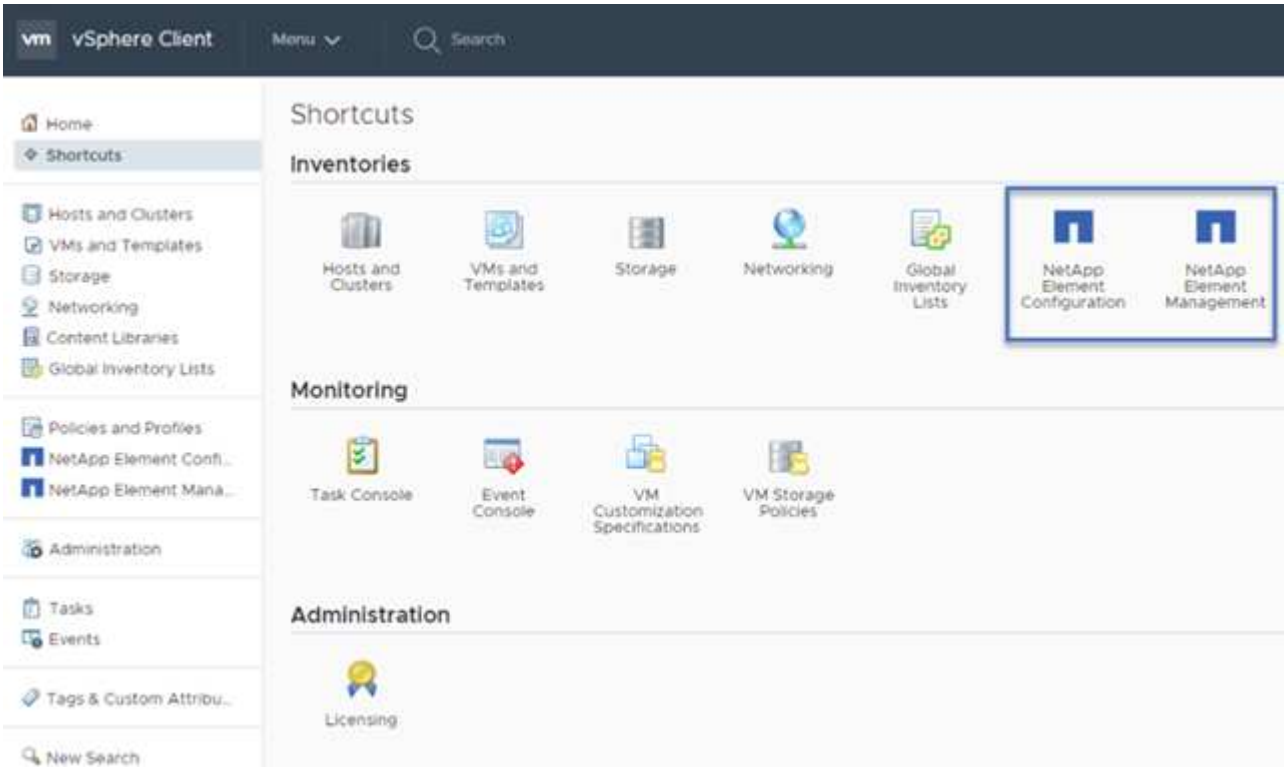
   Sie müssen an den Benutzernamen anhängen `@vsphere.local`.

2. Vergewissern Sie sich, dass keine Alarme vorhanden sind.
3. Überprüfen Sie, ob die vCenter, mNode und ONTAP Select (optional) Appliances ohne Warnsymbole ausgeführt werden.
4. Beobachten Sie, dass die zwei Standard-Datastores (NetApp-HCI-Datastore_01 & 02) erstellt werden.
5. Wählen Sie jeden Datenspeicher aus, und stellen Sie sicher, dass alle Computing-Nodes auf der Registerkarte Hosts aufgeführt sind.
6. Validierung von vMotion und Datastore-02
   a. Migrieren Sie den vCenter Server auf NetApp-HCI-Datastore-02 (nur Storage vMotion).
   b. Migrieren Sie vCenter Server zu allen Computing-Nodes (nur Compute vMotion).
7. Wechseln Sie zum NetApp Element Plug-in für vCenter Server, und stellen Sie sicher, dass das Cluster sichtbar ist.
8. Stellen Sie sicher, dass auf dem Dashboard keine Meldungen angezeigt werden.

Managen Sie NetApp HCI mit dem vCenter Plug-in

Nach der Installation von NetApp HCI können Sie Cluster, Volumes, Datastores, Protokolle, Zugriffsgruppen konfigurieren. Initiatoren und Quality of Service (QoS)-Richtlinien mithilfe des NetApp Element Plug-ins für vCenter Server.

Weitere Informationen finden Sie unter "*NetApp Element Plug-in für vCenter Server Dokumentation*".



Monitoring oder Upgrade von NetApp HCI mit der Hybrid Cloud Control

Sie können das System optional mit NetApp HCI Hybrid Cloud Control überwachen, aktualisieren oder erweitern.

Sie melden sich bei NetApp Hybrid Cloud Control an, indem Sie die IP-Adresse des Management-Node nutzen.

Hybrid Cloud Control bietet folgende Möglichkeiten:

- "Überwachen Sie die NetApp HCI-Installation"
- "Führen Sie ein Upgrade Ihres NetApp HCI Systems durch"
- "Erweitern Sie Ihre NetApp HCI Storage- oder Computing-Ressourcen"

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 Benutzeroberfläche von NetApp Hybrid Cloud Control wird angezeigt.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "NetApp HCI Installations- und Setup-Anleitung"
- "TR-4820: Quick Planning Guide für NetApp HCI-Netzwerke"
- "NetApp Element Plug-in für vCenter Server-Handbuch"
- "NetApp Configuration Advisor" Netzwerkvalidierungstool 5.8.1 oder höher
- "NetApp SolidFire Active IQ Dokumentation"

Hardware der H-Serie installieren

Bevor NetApp HCI zum Einsatz kommt, sollten die Storage- und Computing-Nodes ordnungsgemäß installiert werden.

Eine visuelle Darstellung der Anweisungen finden Sie im"Poster".

- Workflow-Diagramme
- Installation vorbereiten
- Installieren Sie die Schienen
- Installieren Sie den Node/das Chassis

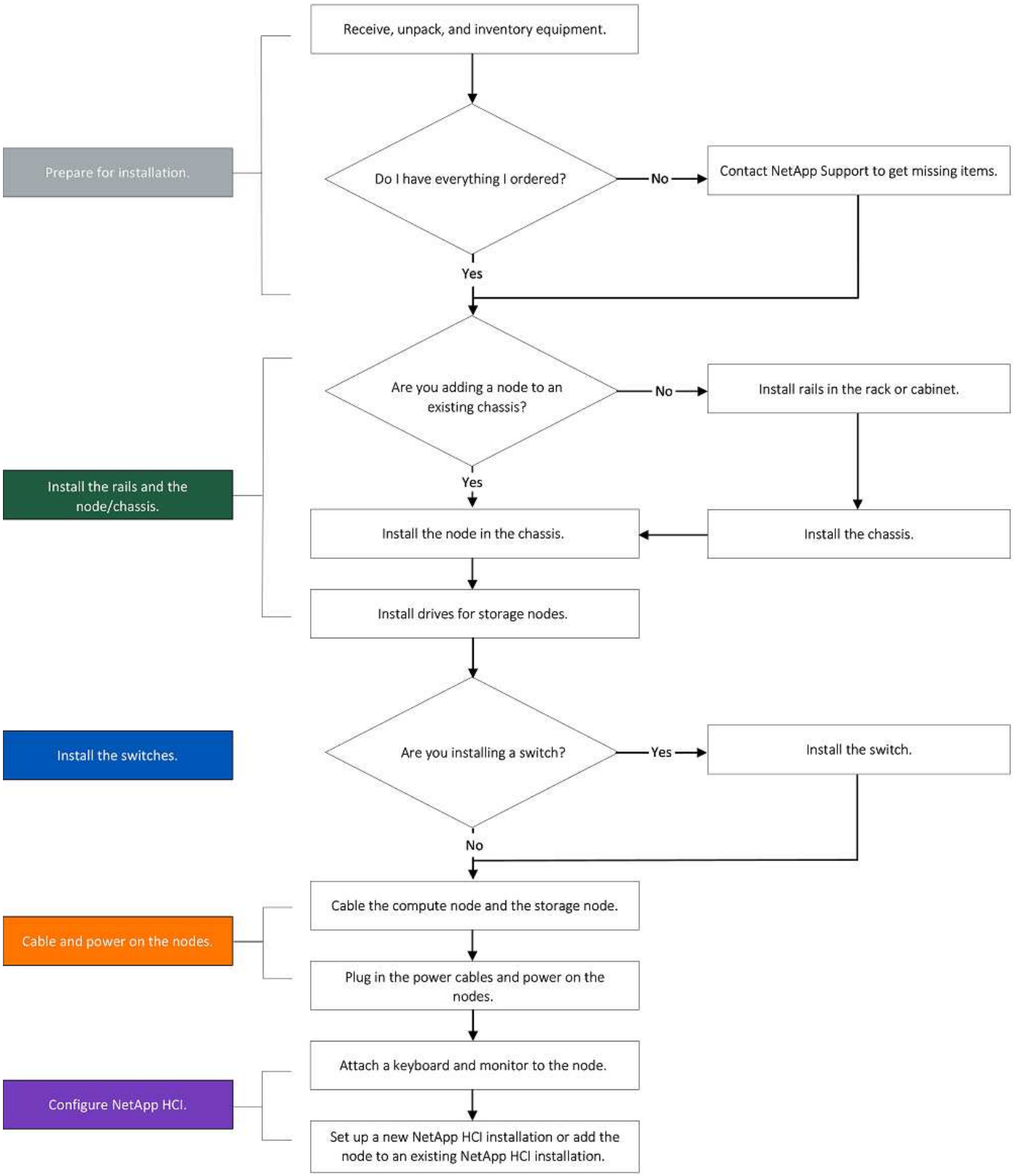
- Installieren Sie die Schalter
- Die Nodes verkabeln
- Schalten Sie die Nodes ein
- Konfigurieren Sie NetApp HCI
- Ausführung von Aufgaben nach der Konfiguration

Workflow-Diagramme

Die Workflow-Diagramme hier bieten einen allgemeinen Überblick über die Installationsschritte. Die Schritte variieren je nach Modell der H-Serie leicht.

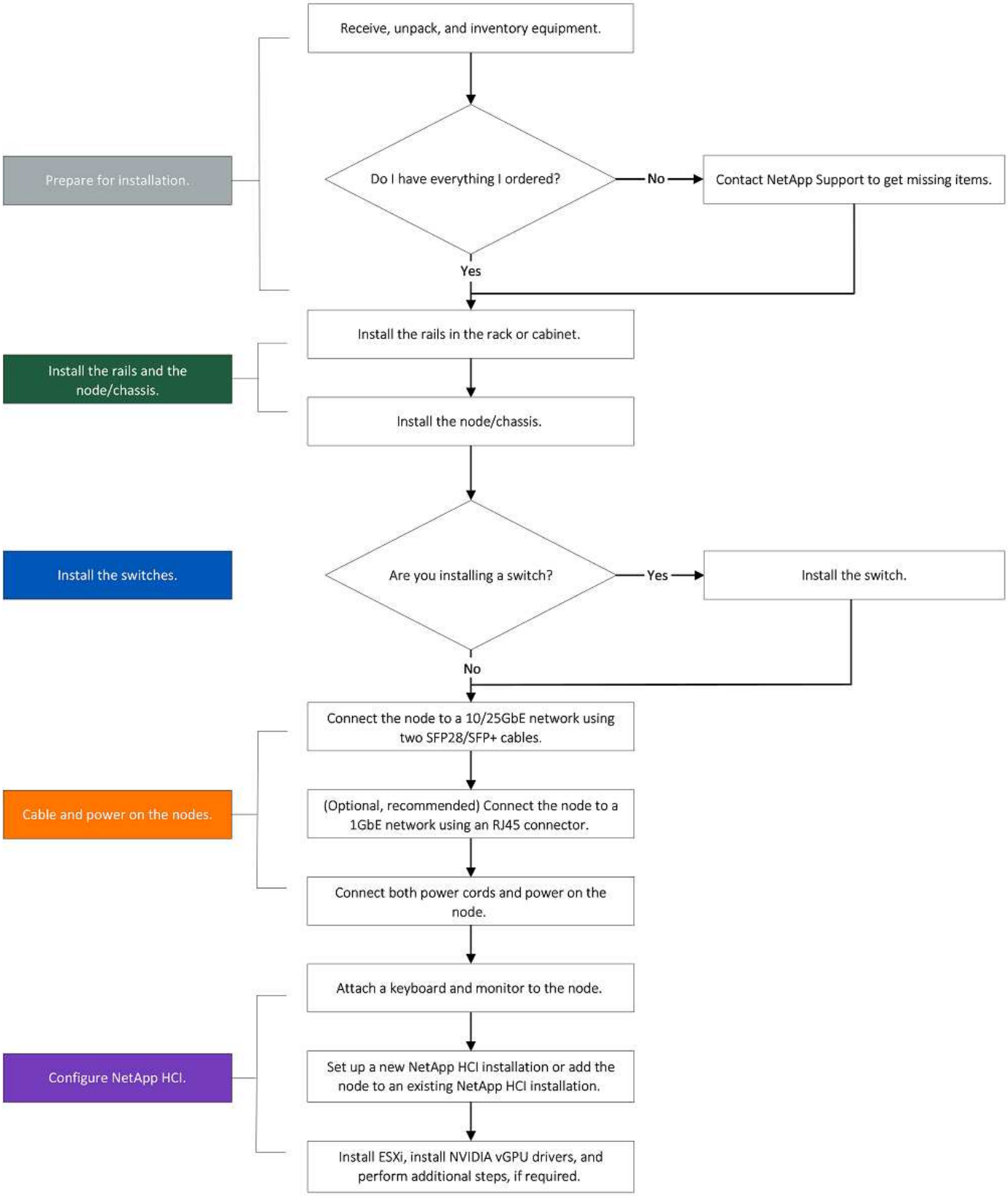
- H410C und H410S
- H610C und H615C
- [H610S]

H410C und H410S



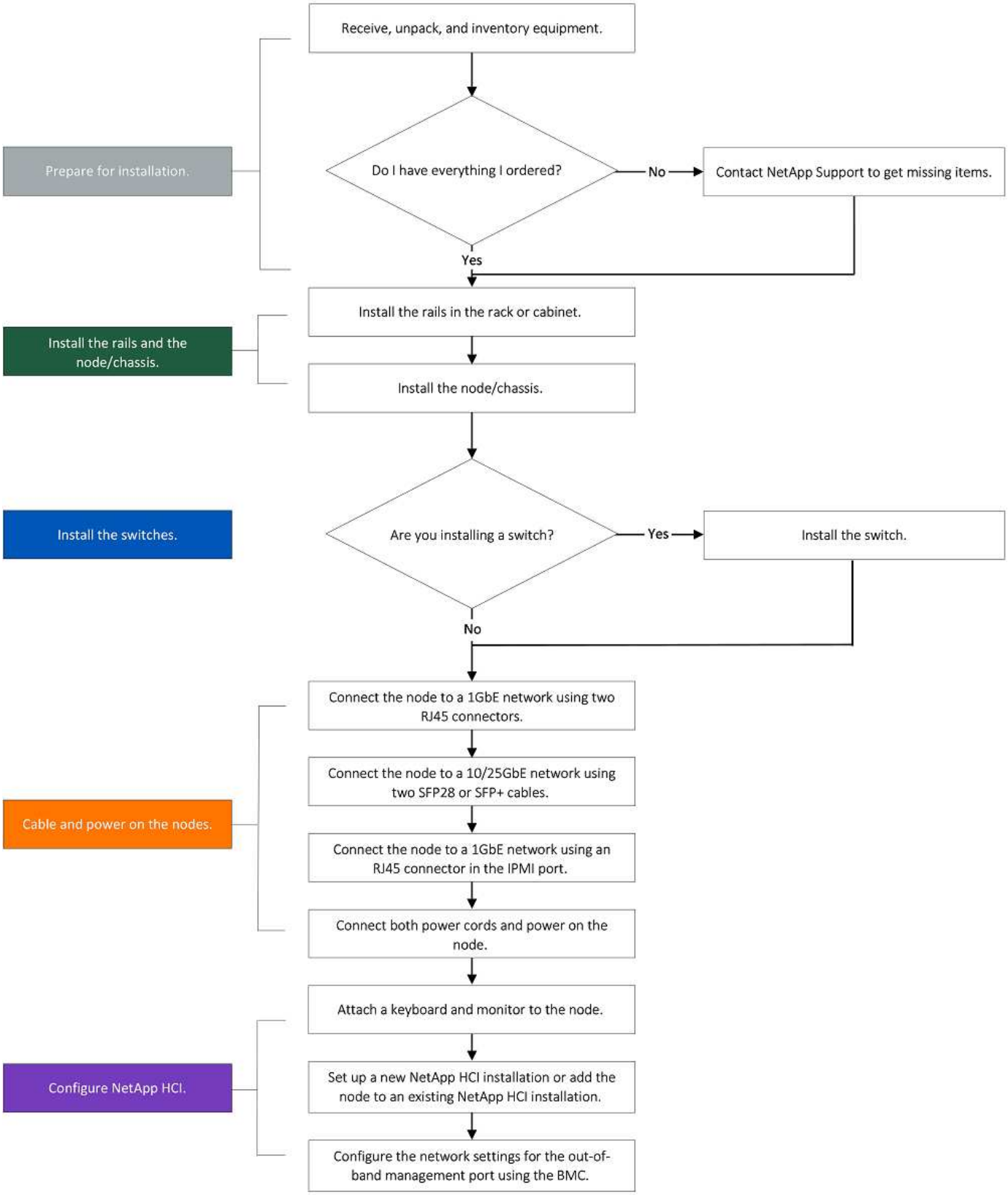
H610C und H615C

Die Begriffe „Node“ und „Chassis“ werden bei H610C und H615C gemeinsam verwendet, da Node und Chassis keine separaten Komponenten sind wie bei einem 2-HE-Chassis mit vier Nodes.


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

H610S

Die Begriffe „Node“ und „Chassis“ werden bei H610C und H615C gemeinsam verwendet, da Node und Chassis keine separaten Komponenten sind wie bei einem 2-HE-Chassis mit vier Nodes.


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

Installation vorbereiten

Überprüfen Sie vor der Installation die gelieferten Hardware und wenden Sie sich an den NetApp Support, wenn Teile fehlen.

Stellen Sie sicher, dass Sie an Ihrem Installationsstandort die folgenden Elemente installiert haben:

- Rack-Platz für das System.

Node-Typ	Rack-Fläche
H410C und H410S Nodes	Zwei Höheneinheiten (2 HE)
H610C Node	2U
H615C und H610S Nodes	Eine Höheneinheit (1 HE)

- SFP28/SFP+ Direct-Attach-Kabel oder Transceiver
- CAT5e oder höhere Kabel mit RJ45-Stecker
- Ein Schalter für Tastatur, Video, Maus (KVM), um das System zu konfigurieren
- USB-Stick (optional)

Die Hardware, die an Sie geliefert wird, hängt davon ab, was Sie bestellen. Eine neue 2-HE-Bestellung mit vier Nodes umfasst das Chassis, die Blende, den Schienen-Kit, Laufwerke für Storage-Nodes, Storage- und Computing-Nodes und Netzkabel (zwei pro Chassis). Wenn Sie H610S Storage-Nodes bestellen, werden die Laufwerke im Chassis installiert.

Achten Sie beim Einbau der Hardware darauf, dass Sie das gesamte Verpackungsmaterial und die Verpackung aus dem Gerät entfernen. Dadurch wird verhindert, dass die Knoten überhitzt und heruntergefahren werden.

Installieren Sie die Schienen

Die Hardwarebestellung, die Ihnen zugestellt wurde, enthält eine Reihe von Gleitschienen. Sie benötigen einen Schraubendreher, um die Schieneninstallation abzuschließen. Die Installationsschritte variieren für jedes Node-Modell entsprechend.

Installieren Sie die Hardware von der Unterseite des Racks bis zur Oberseite, um zu verhindern, dass das Gerät umkippeln kann. Wenn Ihr Rack Stabilisatoren beinhaltet, müssen Sie diese vor der Installation der Hardware installieren.

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

H410C und H410S

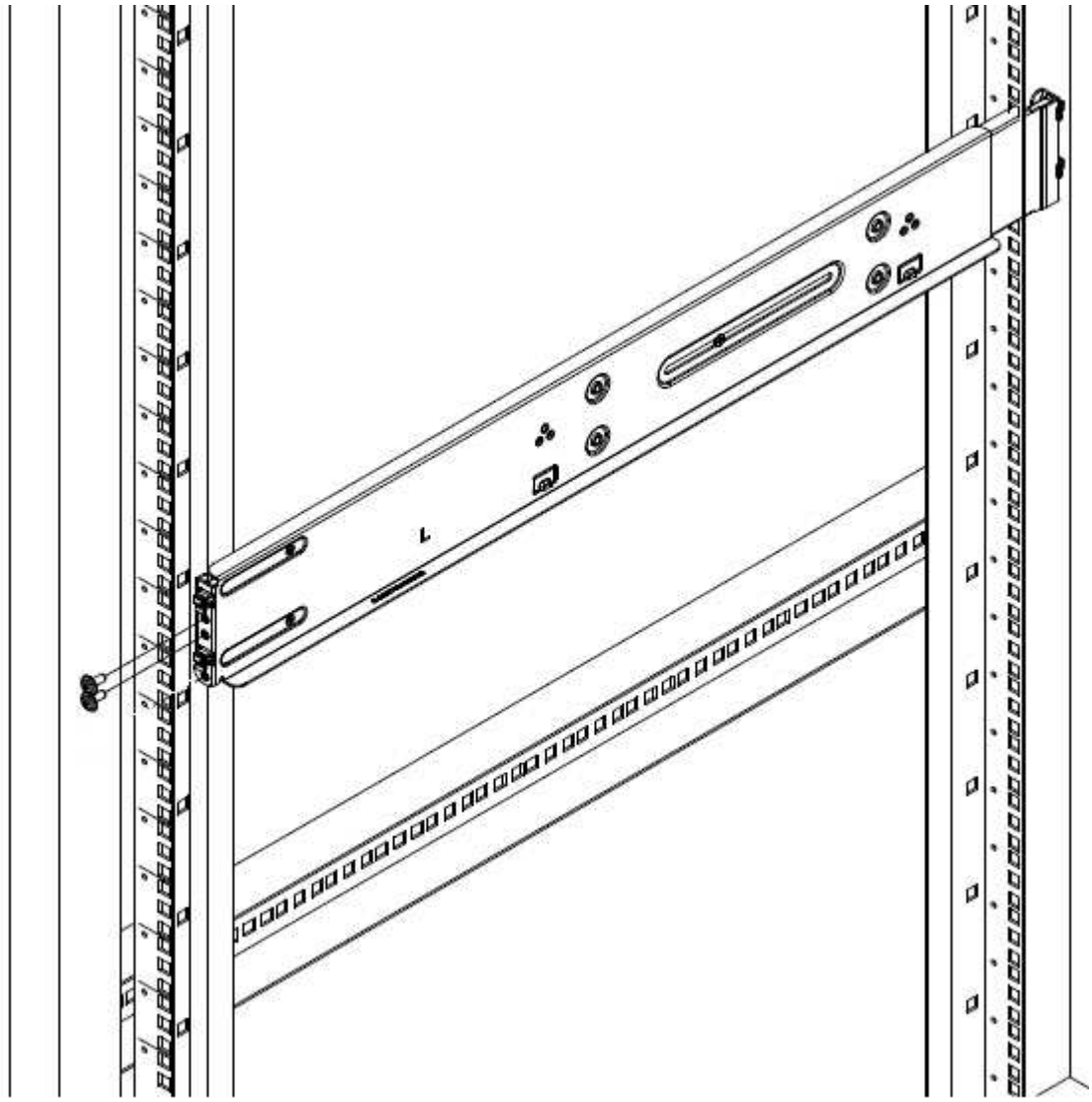
H410C und H410S Nodes sind in einem 2-HE-Chassis mit vier Nodes installiert. Das Chassis wird mit zwei Adaptersätzen ausgeliefert. Wenn Sie das Gehäuse in einem Rack mit runden Löchern einsetzen möchten, verwenden Sie die Adapter für ein Rack mit runden Löchern. Die Schienen für H410C und H410S Nodes passen ein Rack zwischen 29 Zoll und 33.5 Zoll Tiefe. Wenn die Schiene vollständig zusammengeschraubt ist,

ist sie 28 Zoll lang, und die vorderen und hinteren Abschnitte der Schiene werden zusammen mit nur einer Schraube gehalten.

Wenn Sie das Gehäuse auf einer vollständig versetzten Schiene installieren, können die vorderen und hinteren Abschnitte der Schiene voneinander getrennt sein.

Schritte

1. Richten Sie die Vorderseite der Schiene an den Löchern an der vorderen Stange des Racks aus.
2. Schieben Sie die Haken an der Vorderseite der Schiene in die Löcher an der vorderen Stange des Racks und dann nach unten, bis die federbelasteten Stangen in die Rack-Löcher einrasten.
3. Befestigen Sie die Schiene mit Schrauben am Rack. Hier sehen Sie eine Abbildung der linken Schiene, die an der Vorderseite des Racks befestigt ist:

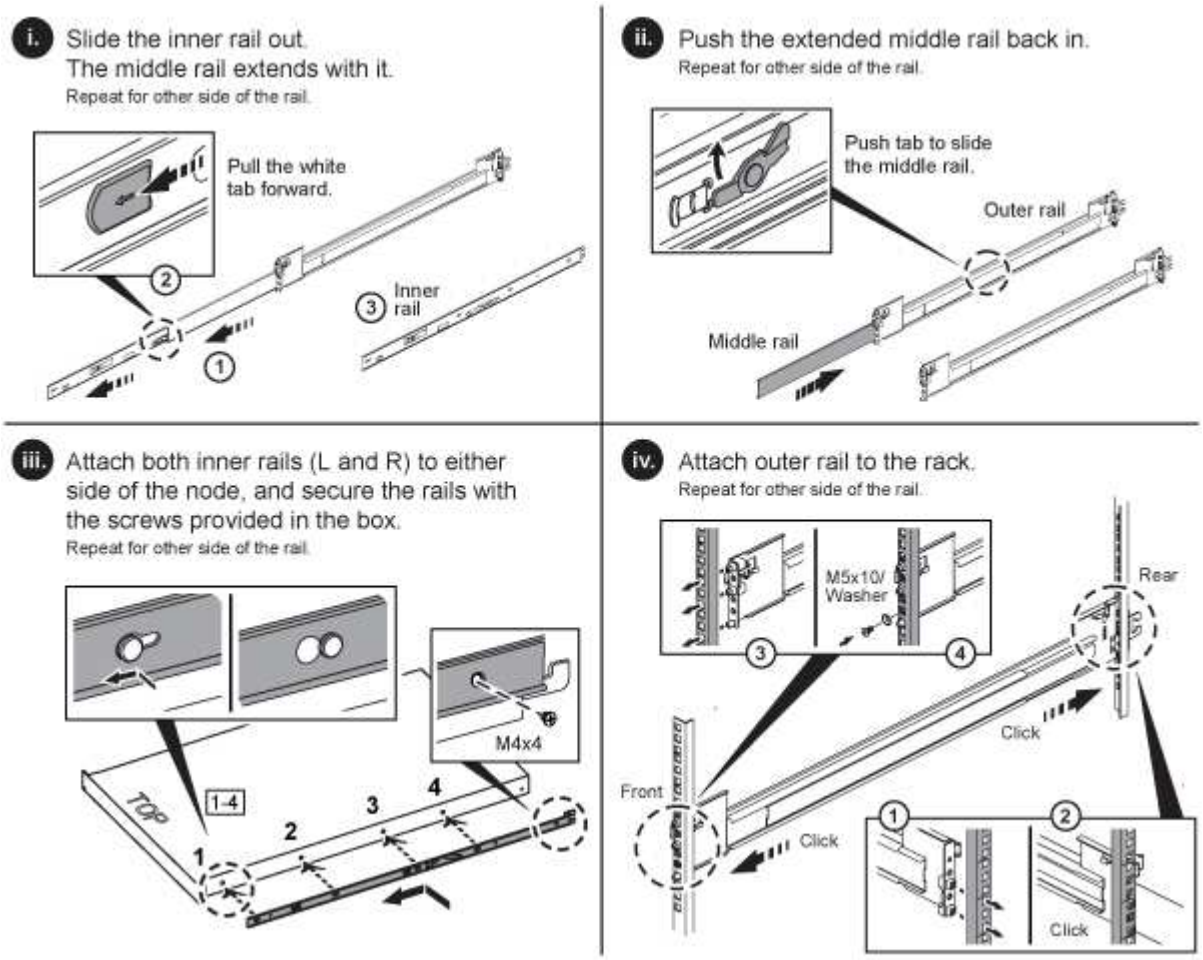


4. Ziehen Sie den hinteren Teil der Schiene auf die hintere Stange des Racks.
5. Richten Sie die Haken an der Rückseite der Schiene an den entsprechenden Löchern am hinteren Pfosten aus, um sicherzustellen, dass sich Vorder- und Rückseite der Schiene auf der gleichen Ebene befinden.
6. Montieren Sie die Rückseite der Schiene am Rack und befestigen Sie die Schiene mit Schrauben.

7. Führen Sie alle oben genannten Schritte für die andere Seite des Racks aus.

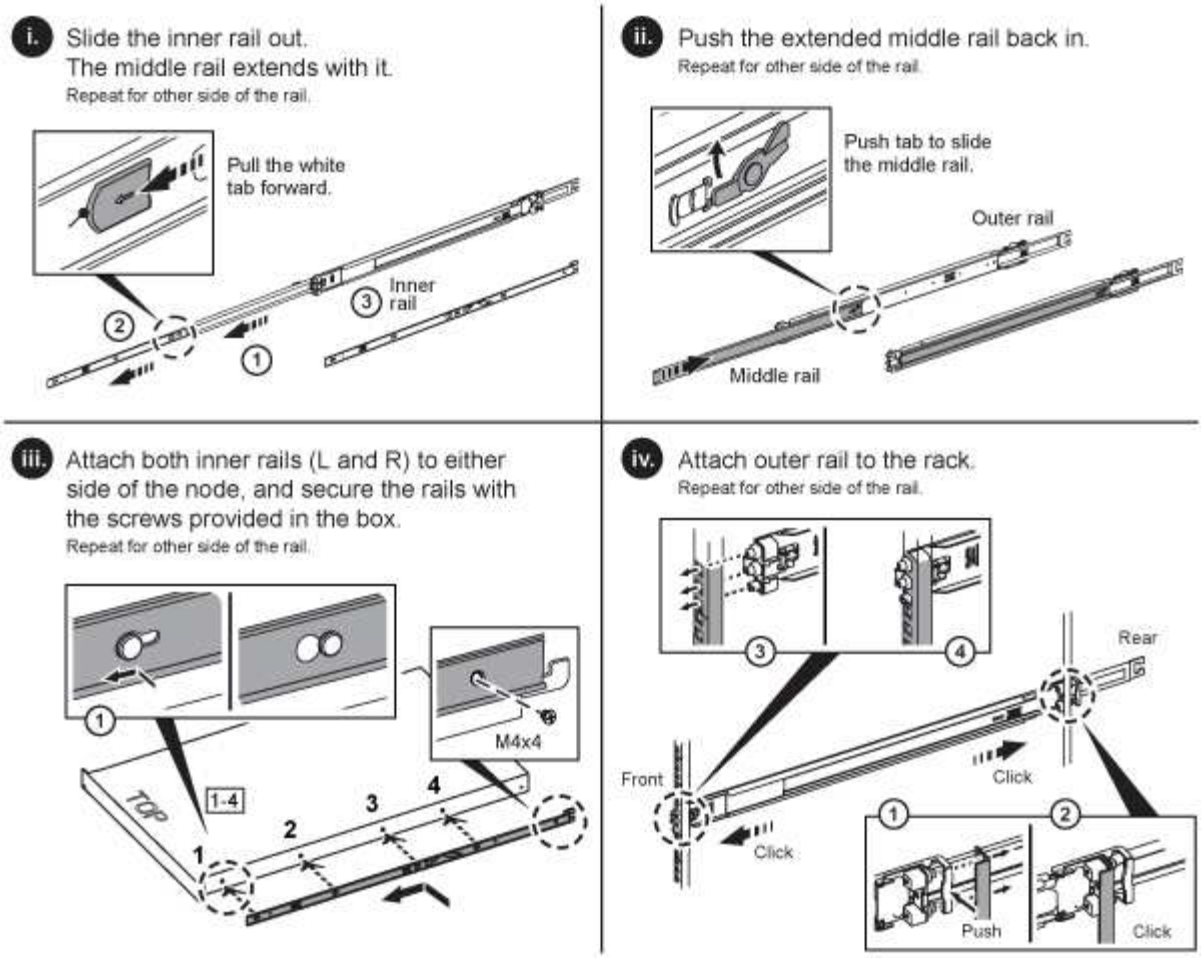
H610C

Folgende Abbildung zeigt die Installation von Schienen für einen H61OC Computing-Node:



H610S und H615C

Folgende Abbildung zeigt die Installation von Rails für einen H610S Storage-Node oder einen H615C Computing-Node:



Auf dem H610S und H615C gibt es linke und rechte Schienen. Positionieren Sie die Schraubenbohrung nach unten, so dass die H610S/H615C Rändelschraube das Gehäuse an der Schiene befestigen kann.

Installieren Sie den Node/das Chassis

Sie installieren den H410C Computing-Node und H410S Storage-Node in einem 2-HE-Chassis mit vier Nodes. Installieren Sie für H610C, H615C und H610S das Chassis/Node direkt auf den Schienen im Rack.

Ab NetApp HCI 1.8 können Sie ein Storage-Cluster mit zwei oder drei Storage-Nodes einrichten.

Entfernen Sie das gesamte Verpackungsmaterial und die Verpackung vom Gerät. So wird verhindert, dass die Nodes überhitzt und heruntergefahren werden.

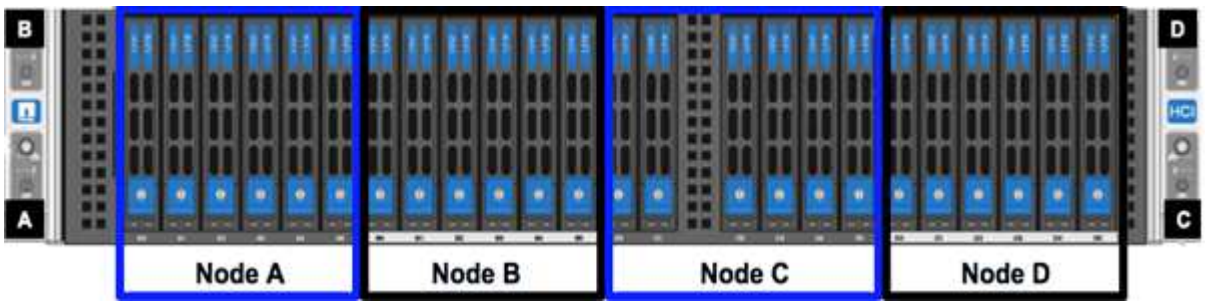
- H410C und H410S Nodes
- H610C Node/Chassis
- H610S und H615C Node/Chassis

H410C und H410S Nodes

Schritte

1. Installieren Sie die H410C und H410S Nodes im Chassis. Dies ist ein Beispiel aus der Rückansicht eines Chassis mit vier installierten Nodes:

2. Installieren Sie Laufwerke für H410S Storage-Nodes.



H610C Node/Chassis

Bei H610C werden die Begriffe „Node“ und „Chassis“ austauschbar, da Node und Chassis keine separaten Komponenten sind, anders als bei einem 2-HE-Chassis mit vier Nodes.

Hier sehen Sie eine Abbildung zur Installation des Node/Chassis im Rack:

H610S und H615C Node/Chassis

Bei H615C und H610S werden die Begriffe „Node“ und „Chassis“ austauschbar verwendet, da Node und Chassis keine separaten Komponenten sind, anders als bei einem 2-HE-Chassis mit vier Nodes.

Hier sehen Sie eine Abbildung zur Installation des Node/Chassis im Rack:

Installieren Sie die Schalter

Wenn Sie Mellanox SN2010-, SN2100- und SN2700-Switches in Ihrer NetApp HCI-Installation verwenden möchten, befolgen Sie die hier angegebenen Anweisungen, um die Switches zu installieren und zu verkabeln:

- "Mellanox-Hardware-Benutzerhandbuch"
- "TR-4836: NetApp HCI mit Mellanox SN2100 und SN2700 Switch-Verkabelungshandbuch (Anmeldung erforderlich)"

Die Nodes verkabeln

Wenn Sie einer vorhandenen NetApp HCI Installation Nodes hinzufügen, stellen Sie sicher, dass die Verkabelung und Netzwerkkonfiguration der fügen Nodes mit der vorhandenen Installation identisch sind.

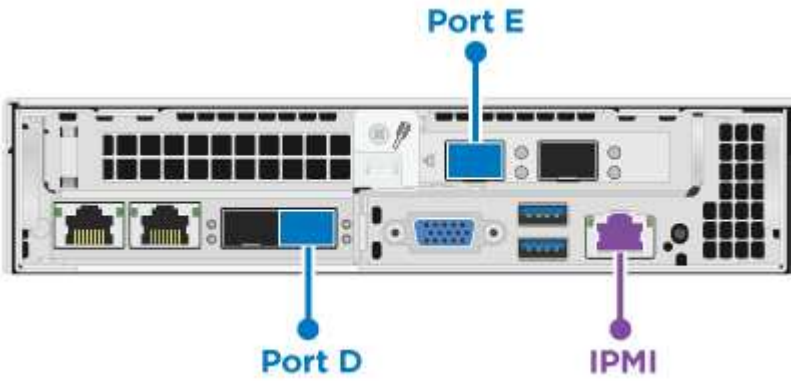
Stellen Sie sicher, dass die Luftzirkulation an der Rückseite des Gehäuses nicht durch Kabel oder Etiketten blockiert ist. Dies kann zu vorzeitigen Komponentenausfällen aufgrund von Überhitzung führen.

- H410C Computing-Node und H410S Storage-Node
- H610C Computing-Node
- H615C Computing-Node
- H610S Storage-Node

H410C Computing-Node und H410S Storage-Node

Sie haben zwei Optionen zur Verkabelung des Node H410C: Verwenden Sie zwei Kabel oder sechs Kabel.

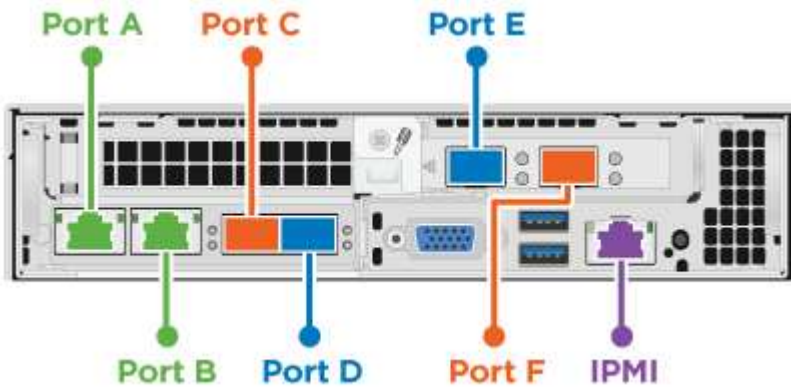
Hier ist die Konfiguration mit zwei Kabeln:



Verbinden Sie für die Ports D und E zwei SFP28/SFP+-Kabel oder Transceiver für gemeinsame Verwaltung, virtuelle Maschinen und Speicherkonnektivität.

(Optional, empfohlen) Verbinden Sie ein CAT5e-Kabel mit dem IPMI-Port, um bandexterne Verwaltungsverbindungen herzustellen.

Die sechs Kabel-Konfiguration ist hier:



Verbinden Sie für die Anschlüsse A und B zwei CAT5e- oder höhere Kabel in den Anschlüssen A und B

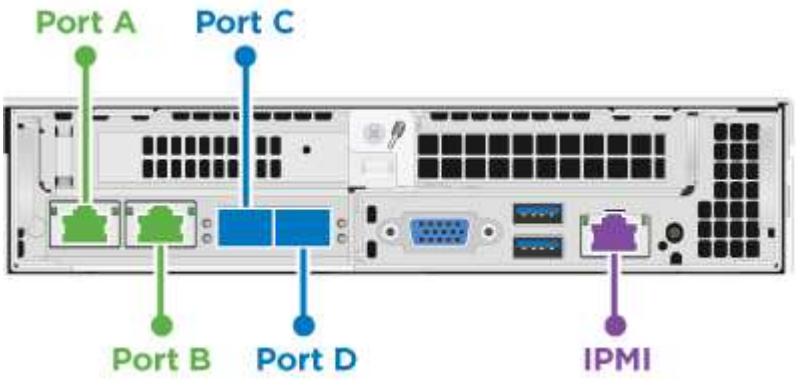
für die Verwaltungskonnektivität.

Verbinden Sie für die Anschlüsse C und F zwei SFP28/SFP+-Kabel oder Transceiver für die Anbindung virtueller Maschinen.

Verbinden Sie für die Anschlüsse D und E zwei SFP28/SFP+-Kabel oder Transceiver für die Speicherkonnektivität.

(Optional, empfohlen) Verbinden Sie ein CAT5e-Kabel mit dem IPMI-Port, um bandexterne Verwaltungsverbindungen herzustellen.

Hier ist die Verkabelung für den H410S-Node:



Verbinden Sie für die Anschlüsse A und B zwei CAT5e- oder höhere Kabel in den Anschlüssen A und B für die Verwaltungskonnektivität.

Verbinden Sie für die Anschlüsse C und D zwei SFP28/SFP+-Kabel oder Transceiver für die Speicherkonnektivität.

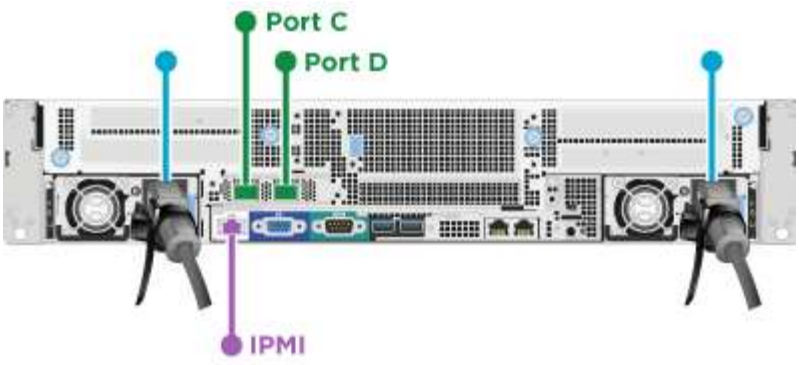
(Optional, empfohlen) Verbinden Sie ein CAT5e-Kabel mit dem IPMI-Port, um bandexterne Verwaltungsverbindungen herzustellen.

Schließen Sie nach dem Kabel der Nodes die Netzkabel an die beiden Netzteile pro Chassis an und stecken Sie sie in eine 240-V-PDU oder eine Steckdose.

H610C Computing-Node

Hier ist die Verkabelung für den H610C-Knoten:

H610C Nodes werden nur in der Konfiguration mit zwei Kabeln implementiert. Stellen Sie sicher, dass alle VLANs an den Ports C und D. vorhanden sind



Bei den Ports C und D verbinden Sie den Node über zwei SFP28/SFP+-Kabel mit einem 10/25-GbE-Netzwerk.

(Optional, empfohlen) Verbinden Sie den Knoten mit einem 1-GbE-Netzwerk über einen RJ45-Anschluss am IPMI-Port.

Schließen Sie beide Stromkabel an den Knoten an, und schließen Sie die Stromkabel an eine 200-240 V Steckdose an.

H615C Computing-Node

Hier ist die Verkabelung für den Knoten H615C:

H615C Nodes werden nur in der Konfiguration mit zwei Kabeln implementiert. Stellen Sie sicher, dass alle VLANs sich auf den Ports A und B befinden

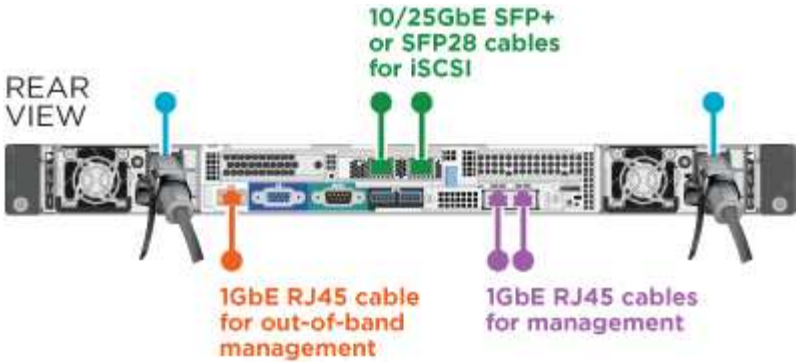
Bei den Ports A und B verbinden Sie den Node über zwei SFP28/SFP+-Kabel mit einem 10 GbE-Netzwerk.

(Optional, empfohlen) Verbinden Sie den Knoten mit einem 1-GbE-Netzwerk über einen RJ45-Anschluss am IPMI-Port.

Schließen Sie beide Stromkabel an den Knoten an, und schließen Sie die Stromkabel an eine 110-140V-Steckdose an.

H610S Storage-Node

Hier ist die Verkabelung für den H610S-Node:



Verbinden Sie den Knoten über zwei RJ45-Anschlüsse am IPMI-Port mit einem 1-GbE-Netzwerk.

Verbinden Sie den Node über zwei SFP28- oder SFP+-Kabel mit einem 10 GbE-Netzwerk.

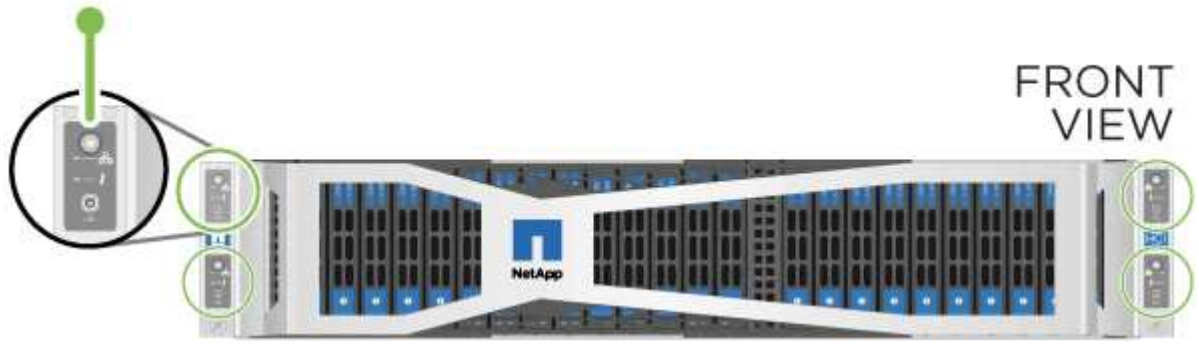
Verbinden Sie den Knoten über einen RJ45-Anschluss im IPMI-Port mit einem 1-GbE-Netzwerk.

Schließen Sie beide Stromkabel an den Node an.

Schalten Sie die Nodes ein

Das Booten der Nodes dauert etwa sechs Minuten.

Die folgende Abbildung zeigt den ein/aus-Schalter am NetApp HCI 2U-Gehäuse:



Folgende Abbildung zeigt den ein/aus-Schalter am H610C Node:

Folgende Abbildung zeigt den ein/aus-Schalter auf den H615C und H610S Nodes:

Konfigurieren Sie NetApp HCI

Wählen Sie eine der folgenden Optionen:

- Neue NetApp HCI Installation
- Erweiterung einer vorhandenen NetApp HCI Installation

Neue NetApp HCI Installation

Schritte

1. Konfigurieren Sie eine IPv4-Adresse im Managementnetzwerk (Bond1G) auf einem NetApp HCI Storage Node.

   Wenn Sie im Managementnetzwerk DHCP verwenden, können Sie eine Verbindung mit der DHCP-übernommenen IPv4-Adresse des Storage-Systems herstellen.

   a. Schließen Sie eine Tastatur, ein Video, eine Maus (KVM) an die Rückseite eines Speicherknoten an.

   b. Konfigurieren Sie die IP-Adresse, die Subnetzmaske und die Gateway-Adresse für Bond1G in der Benutzeroberfläche. Sie können auch eine VLAN-ID für das Bond1G-Netzwerk konfigurieren.

2. Navigieren Sie über einen unterstützten Webbrowser (Mozilla Firefox, Google Chrome oder Microsoft Edge) zu der NetApp Deployment Engine, indem Sie eine Verbindung zu der IPv4-Adresse herstellen, die Sie in Schritt 1 konfiguriert haben.
3. Verwenden Sie die Benutzeroberfläche der NetApp Deployment Engine (UI), um NetApp HCI zu konfigurieren.

   Alle anderen NetApp HCI-Nodes werden automatisch erkannt.

Erweiterung einer vorhandenen NetApp HCI Installation

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser.
2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des NetApp HCI-Storage-Cluster-Administrators bereitstellen.
3. Befolgen Sie die Schritte im Assistenten, um Ihre NetApp HCI-Installation um Storage- und/oder Computing-Nodes hinzuzufügen.

   Um H410C Computing-Nodes hinzuzufügen, muss die vorhandene Installation NetApp HCI 1.4 oder höher ausführen. Um H615C Computing-Nodes hinzuzufügen, muss die vorhandene Installation NetApp HCI 1.7 oder höher ausführen.

Die neu installierten NetApp HCI Nodes im selben Netzwerk werden automatisch erkannt.

Ausführung von Aufgaben nach der Konfiguration

Abhängig vom Typ Ihres Node müssen Sie möglicherweise nach der Installation der Hardware und der Konfiguration von NetApp HCI weitere Schritte durchführen.

- H610C Node
- H615C und H610S Nodes

H610C Node

Installieren Sie die GPU-Treiber in ESXi für jeden installierten H610C Node und validieren Sie deren Funktionalität.

H615C und H610S Nodes

Schritte

1. Verwenden Sie einen Webbrowser, und navigieren Sie zur standardmäßigen BMC-IP-Adresse: `192.168.0.120`
2. Melden Sie sich mit Benutzername `root` und Passwort `calvin`an.
3. Navigieren Sie im Bildschirm Knotenverwaltung zu **Einstellungen > Netzwerkeinstellungen** und konfigurieren Sie die Netzwerkparameter für den Out-of-Band-Management-Port.

Wenn Ihr H615C Node GPUs in ihm hat, installieren Sie GPU-Treiber in ESXi für jeden installierten H615C Node und validieren Sie seine Funktionalität.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "NetApp Element Plug-in für vCenter Server"
- "*TR-4820: Quick Planning Guide für NetApp HCI-Netzwerke*"
- "NetApp Configuration Advisor" Netzwerkvalidierungstool 5.8.1 oder höher

Konfigurieren Sie LACP, um eine optimale Storage-Performance zu erzielen

Um eine optimale NetApp HCI-Storage-Cluster-Performance zu erzielen, sollten Sie das Link Aggregation Control Protocol (LACP) auf den Switch-Ports konfigurieren, die für jeden Storage-Node verwendet werden.

Was Sie benötigen

- Sie haben die Switch-Ports, die mit den 10/25-GbE-Schnittstellen der NetApp HCI Storage-Nodes verbunden sind, als LACP-Port-Channel konfiguriert.
- Sie haben die LACP-Timer auf den Switches eingestellt, die Speicherdatenverkehr auf „fast Mode (1s)“ setzen, um eine optimale Failover-Erkennungszeit zu erreichen. Während der Implementierung werden die Bond1G-Schnittstellen auf allen Storage-Nodes automatisch für den aktiv/Passiv-Modus konfiguriert.

- Sie haben Cisco Virtual PortChannel (vPC) oder die entsprechende Switch-Stack-Technologie für die Switches konfiguriert, die das Storage-Netzwerk bedienen. Die Switch-Stack-Technologie erleichtert die Konfiguration von LACP- und Port-Kanälen und bietet eine Loop-freie Topologie zwischen Switches und den 10/25-GbE-Ports auf den Storage-Nodes.

Schritte

1. Folgen Sie den Empfehlungen Ihres Switch-Anbieters, um LACP auf den für NetApp H-Series Storage-Nodes verwendeten Switch-Ports zu aktivieren.
2. Vor der Implementierung von NetApp HCI muss der Bond-Modus auf allen Storage-Nodes in der On-Node-Benutzeroberfläche (auch bekannt als Terminal User Interface, TUI) auf LACP eingestellt werden.

Weitere Informationen

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

Validieren Sie Ihre Umgebung mit Active IQ Config Advisor

Bevor Sie die NetApp HCI Hardware in Racks und die Installation von NetApp HCI durchführen, müssen Sie überprüfen, ob Ihre Umgebung den NetApp HCI Netzwerkanforderungen entspricht. Active IQ Config Advisor führt Überprüfungen in Ihrer Umgebung durch, indem Netzwerk-, Switch- und VMware vSphere-Konfigurationen validiert werden. Das Tool generiert einen Bericht, den Sie zur Behebung von Problemen verwenden können. Der Bericht kann an Ihren Professional Services Engineer übergeben werden, um eine Installation vorzubereiten und zu planen.

Installation von Active IQ Config Advisor

Laden Sie Active IQ Config Advisor auf einem PC mit Zugriff auf die NetApp HCI-Netzwerke herunter, und installieren Sie sie.

Schritte

1. Wählen Sie in einem Webbrowser im NetApp Support-Menü die Option **Tools** aus, suchen Sie nach Active IQ Config Advisor und laden Sie das Tool herunter.

   NetApp Support-Website › Tools.

   Nachdem Sie der Endbenutzer-Lizenzvereinbarung (Endbenutzer License Agreement, EULA) zugestimmt haben, wird die Download-Seite angezeigt. Microsoft Windows-, Linux- und Mac-Binärdateien sind im Fenster **Client Tool** verfügbar.

2. Führen Sie die ausführbare Datei aus.
3. Wählen Sie eine Sprache aus, und wählen Sie **OK**.
4. Wählen Sie **Weiter**.
5. Lesen Sie die EULA und wählen Sie **Ich stimme zu**.
6. Wählen Sie **Installieren**.
7. Stellen Sie sicher, dass **Run Active IQ Config Advisor** ausgewählt ist, und wählen Sie **Finish**.

Nach kurzer Verzögerung öffnet sich die Active IQ Config Advisor-Benutzeroberfläche in einem neuen Browser-Fenster oder einer neuen Registerkarte.

Verwenden Sie Active IQ Config Advisor

Active IQ Config Advisor wird in einem Browser-Fenster ausgeführt, sammelt Informationen über Ihr Netzwerk und Ihre Umgebung und erstellt einen Bericht, mit dem Sie sämtliche Netzwerk- oder Konfigurationsprobleme, die die NetApp HCI-Implementierung beeinträchtigen könnten, beheben können.

Was Sie benötigen

Sie haben Active IQ Config Advisor auf einem Gerät installiert, das auf das Management-Netzwerk, die VMware vCenter Server-Netzwerke (wenn Sie eine vorhandene VMware Installation beitreten) und die Switches für NetApp HCI zugreifen kann.

Wenn Sie Mellanox-Switches verwenden und NetApp Professional Services sie im Rahmen der Implementierung konfigurieren, müssen Sie keine Switch-Informationen bereitstellen.

Über diese Aufgabe

Active IQ Config Advisor führt nur schreibgeschützte Überprüfungen durch, um Daten zu erfassen. Es wurde keine Konfiguration im Rahmen der Sammlung geändert.

Schritte

1. Öffnen Sie Active IQ Config Advisor.

   Config Advisor wird mit dem Fenster **Grundeinstellungen** in einem Webbrowser angezeigt. Hier können Sie globale Erfassungseinstellungen festlegen und die Erfassungsergebnisse verschlüsseln.

2. Geben Sie eine Passphrase im Abschnitt **Verschlüsselungseinstellungen** ein, um das Sammlungsprojekt zu verschlüsseln.

   So wird sichergestellt, dass nur Sie dieses Sammlungsprojekt nach der Erstellung laden können.

3. Identifizieren Sie diesen Sammlungsbericht wie Ihren eigenen, indem Sie Ihren Namen und Ihre E-Mail-Adresse im Abschnitt **Benutzerverifizierung** eingeben.
4. Wählen Sie **Speichern**.
5. Wählen Sie **Neue Datenerfassung erstellen**.
6. Wählen Sie im Dropdown-Menü **Sammlungsart** die Option **lösungsbasiert** aus.
7. Wählen Sie im Dropdown-Menü **Profil** die Option **NetApp HCI Pre Deployment** aus.
8. Wählen Sie für jeden Gerätetyp in der Spalte **Typ** im Dropdown-Menü **Aktionen** die Anzahl dieses Geräts in Ihrem NetApp HCI-Netzwerk aus.

   Wenn Sie beispielsweise drei Cisco Switches haben, wählen Sie 3 aus dem Dropdown-Menü * Aktionen* in dieser Zeile aus. Es werden drei Zeilen angezeigt, eine für jeden Cisco Switch, den Sie identifiziert haben.

   Wenn Sie Mellanox-Switches verwenden und NetApp Professional Services sie im Rahmen der Implementierung konfigurieren, müssen Sie keine Switch-Informationen bereitstellen.

9. Geben Sie bei allen Switches die Management-IP-Adresse und die Administratoranmeldeinformationen ein.

10. Führen Sie für alle VMware vCenter Server, die Sie identifiziert haben, einen der folgenden Schritte aus:
    - Wenn Sie einen neuen vCenter-Server bereitstellen, geben Sie die für den Server geplante IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) an.
    - Wenn Sie einem vorhandenen vCenter-Server beitreten, geben Sie die IP-Adresse oder FQDN und die Administratoranmeldeinformationen für den Server an.
11. Optional: Wenn Sie Informationen für Switches hinzugefügt haben, geben Sie die Anzahl der Computing- und Storage-Nodes im Abschnitt **Switch Validation** ein.
12. Wählen Sie die Konfiguration der Compute Node-Verkabelung aus, die Sie im Abschnitt * Compute Node Network* verwenden möchten.
13. Geben Sie die einzelnen Switch-Ports und alle VLAN-Tags ein, die Sie für Management-, vMotion- und Speichernetzwerke für alle Switches im Abschnitt * Compute Node Network* verwenden möchten.
14. Geben Sie individuelle Switch-Ports und alle VLAN-Tags ein, die Sie für die Verwaltung und Speichernetzwerke für alle Switches im Abschnitt **Storage Node Network** verwenden möchten.
15. Geben Sie im Abschnitt **Netzwerkeinstellungsüberprüfung** die IP-Adressen und Gateway-IP-Adresse für das Managementnetzwerk ein, gefolgt von Listen von Servern für DNS, NTP und vCenter Server (wenn Sie einen neuen vCenter Server mit NetApp HCI bereitstellen).

    In diesem Abschnitt kann Active IQ Config Advisor sicherstellen, dass das Managementnetzwerk zur Verwendung verfügbar ist. Außerdem wird sichergestellt, dass Dienste wie DNS und NTP ordnungsgemäß funktionieren.

16. Wählen Sie **Validieren**, um sicherzustellen, dass alle eingegebenen IP-Adressinformationen und Anmeldeinformationen gültig sind.
17. Wählen Sie **Speichern oder Sammeln**.

    Dadurch wird der Erfassungsprozess gestartet, und Sie können den Fortschritt sehen, während die Sammlung zusammen mit einem Echtzeit-Protokoll der Erfassungsbefehle ausgeführt wird. In der Spalte **Progress** werden für jede Sammelaufgabe farbcodierte Fortschrittsbalken angezeigt.

    Die Fortschrittsbalken zeigen den Status in folgenden Farben an:

    - **Grün**: Die Sammlung ist ohne Befehlsfehler beendet. Sie können die Bereitstellungsrisiken und -Empfehlungen sehen, indem Sie im Menü **Aktionen** das Symbol **Ansicht & Analyse** auswählen.
    - **Gelb**: Die Sammlung hat einige Befehlsfehler abgeschlossen. Sie können die Bereitstellungsrisiken und -Empfehlungen sehen, indem Sie im Menü **Aktionen** das Symbol **Ansicht & Analyse** auswählen.
    - **Rot**: Die Sammlung ist fehlgeschlagen. Sie müssen die Fehler beheben und die Sammlung erneut ausführen.
18. Optional: Wenn die Sammlung abgeschlossen ist, können Sie das binokulare Symbol für eine beliebige Erfassungszeile auswählen, um die ausgeführten Befehle und die erfassten Daten anzuzeigen.
19. Wählen Sie die Registerkarte **Anzeigen & Analysieren**.

    Auf dieser Seite finden Sie einen allgemeinen Integritätsbericht Ihrer Umgebung. Sie können einen Abschnitt des Kreisdiagramms auswählen, um weitere Details zu diesen spezifischen Prüfungen oder Beschreibungen von Problemen zu erhalten, sowie Empfehlungen zur Behebung von Problemen, die eine erfolgreiche Bereitstellung beeinträchtigen könnten. Sie können diese Probleme selbst lösen oder Hilfe von den NetApp Professional Services anfordern.

20. Wählen Sie **Export**, um den Sammelbericht als PDF- oder Microsoft Word-Dokument zu exportieren.

> Die Dokumente zu PDF und Microsoft Word enthalten Informationen zur Switch-Konfiguration Ihrer Implementierung. NetApp Professional Services verwendet diese zur Überprüfung der Netzwerkeinstellungen.

21. Senden Sie die exportierte Berichtsdatei an Ihren NetApp Professional Services Vertreter.

Weitere Informationen

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

Konfigurieren Sie IPMI für jeden Node

Nachdem die NetApp HCI Hardware im Rack montiert, verkabelt und hochgefahren wurde, können Sie für jeden Node den IPMI-Zugriff (Intelligent Platform Management Interface) konfigurieren. Weisen Sie jedem IPMI-Port eine IP-Adresse zu und ändern Sie das Standard-IPMI-Administratorpasswort, sobald Sie Remote-IPMI-Zugriff auf den Node haben.

Voraussetzungen

Nachdem Sie bestätigt haben, dass Ihre Umgebung zur Unterstützung von NetApp HCI bereit ist und potenzielle Probleme beheben kann, müssen Sie vor der Implementierung einige abschließende Aufgaben erledigen.

- Ein erfolgreicher Bericht von Active IQ Config Advisor ist sichergestellt.
- Sammeln aller relevanten Informationen über Ihr Netzwerk, die aktuelle oder geplante VMware-Infrastruktur und die geplanten Benutzeranmeldeinformationen.
- Rack, Kabel und Strom an der NetApp HCI Installation.

Weisen Sie die IP-Adresse des IPMI-Ports manuell zu

Das Dynamic Host Configuration Protocol (DHCP) ist standardmäßig für den IPMI-Port jedes NetApp HCI-Knotens aktiviert. Wenn Ihr IPMI-Netzwerk DHCP nicht verwendet, können Sie dem IPMI-Port manuell eine statische IPv4-Adresse zuweisen.

Was Sie benötigen

Stellen Sie sicher, dass Sie über einen Switch oder einen Monitor und eine Tastatur verfügen, mit dem Sie auf das BIOS jedes Knotens zugreifen können.

Über diese Aufgabe

Verwenden Sie die Pfeiltasten, um im BIOS zu navigieren. Wählen Sie eine Registerkarte oder Option durch Drücken `Enter`von . Kehren Sie mit der Taste zurück zu den vorherigen Bildschirmen `ESC`.

Schritte

1. Schalten Sie den Node ein.

2. Rufen Sie das BIOS auf, indem Sie die Taste drücken `Del`.
3. Wählen Sie die Registerkarte IPMI aus.
4. Wählen Sie **BMC-Netzwerkkonfiguration** und drücken Sie `Enter`.
5. Wählen Sie **Ja** und drücken Sie `Enter`.
6. Wählen Sie **Konfigurationsadresse Quelle** und drücken Sie `Enter`.
7. Wählen Sie **statisch** und drücken Sie `Enter`.
8. Wählen Sie **Station IP-Adresse** aus, und geben Sie eine neue IP-Adresse für den IPMI-Port ein. Drücken Sie, `Enter` wenn Sie fertig sind.
9. Wählen Sie **Subnetzmaske** aus, und geben Sie eine neue Subnetzmaske für den IPMI-Port ein. Drücken Sie, `Enter` wenn Sie fertig sind.
10. Wählen Sie **Gateway-IP-Adresse** aus, und geben Sie eine neue Gateway-IP-Adresse für den IPMI-Port ein. Drücken Sie, `Enter` wenn Sie fertig sind.
11. Schließen Sie ein Ende eines Ethernet-Kabels an den IPMI-Port und das andere Ende an einen Switch an.

    Der IPMI-Port für diesen Node ist bereit zur Verwendung.
12. Wiederholen Sie dieses Verfahren für alle anderen NetApp HCI-Nodes mit IPMI-Ports, die nicht konfiguriert sind.

Ändern Sie das Standard-IPMI-Passwort für die Nodes H410C und H410S

Sie sollten das Standardpasswort für das IPMI-Administratorkonto auf jedem Computing- und Storage-Node ändern, sobald Sie den IPMI-Netzwerkport konfigurieren.

Was Sie benötigen

Sie haben die IPMI-IP-Adresse für jeden Computing- und Storage-Node konfiguriert.

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der das IPMI-Netzwerk erreichen kann, und navigieren Sie zu der IPMI-IP-Adresse für den Knoten.
2. Geben Sie den Benutzernamen und das Kennwort `ADMIN` in die Anmeldeaufforderung ein `ADMIN`.
3. Wählen Sie nach der Anmeldung die Registerkarte **Konfiguration** aus.
4. Wählen Sie **Benutzer**.
5. Wählen Sie den `ADMIN` Benutzer aus und wählen Sie **Benutzer ändern**.
6. Aktivieren Sie das Kontrollkästchen **Passwort ändern**.
7. Geben Sie ein neues Passwort in die Felder **Passwort** und **Passwort bestätigen** ein.
8. Wählen Sie **Ändern**, und wählen Sie dann **OK**.
9. Wiederholen Sie dieses Verfahren für alle anderen NetApp HCI H410C- und H410S-Nodes mit Standard-IPMI-Passwörtern.

Ändern des Standard-IPMI-Passworts für H610C, H615C und H610S Nodes

Sie sollten das Standardpasswort für das IPMI-Administratorkonto auf jedem Computing- und Storage-Node ändern, sobald Sie den IPMI-Netzwerkport konfigurieren.

Was Sie benötigen

Sie haben die IPMI-IP-Adresse für jeden Computing- und Storage-Node konfiguriert.

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der das IPMI-Netzwerk erreichen kann, und navigieren Sie zu der IPMI-IP-Adresse für den Knoten.
2. Geben Sie den Benutzernamen und das Kennwort `calvin` in die Anmeldeaufforderung ein `root`.
3. Wählen Sie nach der Anmeldung das Menünavigationssymbol oben links auf der Seite aus, um das Seitenleiste-Fach zu öffnen.
4. Wählen Sie **Einstellungen**.
5. Wählen Sie **Benutzerverwaltung**.
6. Wählen Sie den **Administrator**-Benutzer aus der Liste aus.
7. Aktivieren Sie das Kontrollkästchen **Passwort ändern**.
8. Geben Sie ein neues, starkes Passwort in die Felder **Passwort** und **Passwort bestätigen** ein.
9. Wählen Sie unten auf der Seite **Speichern**.
10. Wiederholen Sie dieses Verfahren für alle anderen NetApp HCI H610C, H615C oder H610S Nodes mit Standard-IPMI-Passwörtern.

Weitere Informationen

- "NetApp SolidFire Active IQ Dokumentation"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Implementieren Sie NetApp HCI

Rufen Sie die NetApp Deployment Engine auf

Rufen Sie die NetApp Deployment Engine auf

Um NetApp HCI bereitzustellen, müssen Sie über die IPv4-Adresse, die der Bond1G-Schnittstelle zugewiesen ist, auf die NetApp Deployment Engine auf einem der Storage-Nodes der NetApp H-Series zugreifen. Dies ist die logische Schnittstelle, die Ports A und B für Storage-Nodes kombiniert. Dieser Storage-Node wird zum controlling-Storage-Node für den Implementierungsprozess. Sie müssen je nach Umgebung entweder die IPv4-Adresse konfigurieren oder sie von einem der Storage-Nodes abrufen.

Sie können nur über die Bond1G-Schnittstelle eines Storage-Node auf die NetApp Deployment Engine zugreifen. Die logische Schnittstelle, die Ports C und D für Storage-Nodes kombiniert, wird unter Verwendung der Bond10G-Schnittstelle nicht unterstützt.

Nutzen Sie eine der folgenden Methoden, die Ihrer Netzwerkumgebung am besten für den Zugriff auf die NetApp Deployment Engine beschreibt:

Szenario	Methode
Sie verfügen in Ihrer Umgebung nicht über DHCP	"Zugriff auf die NetApp Deployment Engine in Umgebungen ohne DHCP"
In Ihrer Umgebung ist DHCP vorhanden	"Greifen Sie in Umgebungen mit DHCP auf die NetApp Deployment Engine zu"
Sie möchten alle IP-Adressen manuell zuweisen	"Weisen Sie IP-Adressen manuell dem Zugriff auf die NetApp Deployment Engine zu"

Weitere Informationen

- "Konfigurieren Sie vollständig qualifizierten Domänennamen Web UI-Zugriff"

Zugriff auf die NetApp Deployment Engine in Umgebungen ohne DHCP

Wenn DHCP im Netzwerk nicht verwendet wird, müssen Sie eine statische IPv4-Adresse auf der Bond1G-Schnittstelle eines der Storage-Nodes (auch bekannt als kontrollierende Storage-Node) festlegen, über die Sie auf die NetApp Deployment Engine zugreifen können. Die NetApp Deployment Engine auf dem steuernden Storage-Node erkennt und kommuniziert mit anderen Computing- und Storage-Nodes mithilfe von IPv4-Adressen, die auf den Bond10G-Schnittstellen aller Nodes automatisch konfiguriert wurden. Sie sollten diese Methode verwenden, es sei denn, Ihr Netzwerk hat spezielle Anforderungen.

Was Sie benötigen

- Sie oder Ihr Netzwerkadministrator haben die Aufgaben im Dokument Installations- und Setup-Anleitung ausgeführt.

- Sie haben physischen Zugriff auf die NetApp HCI-Nodes.
- Alle NetApp HCI-Nodes sind eingeschaltet.
- DHCP ist für die NetApp HCI-Netzwerke nicht aktiviert, und die NetApp HCI-Nodes haben keine IP-Adressen von DHCP-Servern erhalten.
- Das NetApp HCI Management-Netzwerk ist als natives VLAN auf den Bond1G- und Bond10G-Schnittstellen aller Nodes konfiguriert.

Schritte

1. Stecken Sie ein KVM in die Rückseite eines der NetApp HCI Storage-Nodes (dieser Node wird der steuernde Storage-Node).
2. Konfigurieren Sie die IP-Adresse, die Subnetzmaske und die Gateway-Adresse für Bond1G in der Benutzeroberfläche. Sie können bei Bedarf auch eine VLAN-ID für das Bond1G-Netzwerk konfigurieren.

   Sie können diese IPv4-Adresse während der Implementierung mit der NetApp Deployment Engine später nicht mehr verwenden.

3. Öffnen Sie einen Webbrowser auf einem Computer, der auf das NetApp HCI-Managementnetzwerk zugreifen kann.
4. Navigieren Sie zu der IP-Adresse, die Sie dem steuernden Speicher-Node zugewiesen haben. Beispiel:

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

   Dies führt Sie zur Benutzeroberfläche der NetApp Deployment Engine.

Weitere Informationen

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

Greifen Sie in Umgebungen mit DHCP auf die NetApp Deployment Engine zu

In Umgebungen, in denen Server automatisch eine IPv4-Konfiguration von DHCP beziehen, können Sie mithilfe der IPv4-Adresse, die der Bond1G-Schnittstelle auf einem der Storage-Nodes zugewiesen ist, auf die NetApp Deployment Engine zugreifen. Sie können einen USB-Stick verwenden, um die IPv4-Adresse von einem der Speicherknoten abzurufen. Die NetApp Deployment Engine erkennt automatisch andere Computing- und Storage-Nodes, die über DHCP zugewiesene IPv4-Adressen verwenden. Sie sollten diese Methode nur verwenden, wenn Ihr Netzwerk besondere Anforderungen hat.

Was Sie benötigen

- Sie oder Ihr Netzwerkadministrator haben die Aufgaben im Dokument Installations- und Setup-Anleitung ausgeführt.
- Sie haben physischen Zugriff auf die NetApp HCI-Nodes.
- Alle NetApp HCI-Nodes sind eingeschaltet.

- DHCP ist in den NetApp HCI Management- und Storage-Netzwerken aktiviert.
- Der DHCP-Adressenpool ist groß genug für zwei IPv4-Adressen pro NetApp HCI-Node.

> Damit die NetApp HCI-Implementierung erfolgreich ist, müssen alle Nodes in der Implementierung entweder über DHCP-übernommene oder automatisch konfigurierte IPv4-Adressen verfügen (Sie können keine Methoden für die IPv4-Adresszuweisung kombinieren).

Über diese Aufgabe

Wenn DHCP nur für das Speichernetzwerk (Bond10G-Schnittstellen) verwendet wird, sollten Sie die unter Link beschriebenen Schritte verwenden"Zugriff auf die NetApp Deployment Engine in Umgebungen ohne DHCP", um auf die NetApp-Bereitstellungs-Engine zuzugreifen.

Schritte

1. Warten Sie mehrere Minuten, bis die Nodes IP-Adressen anfordern.
2. Wählen Sie einen Speicherknoten aus, und legen Sie einen USB-Stick in den Knoten ein. Lassen Sie es für mindestens fünf Sekunden.
3. Entfernen Sie den USB-Stick, und stecken Sie ihn in den Computer ein.
4. Öffnen Sie die `readme.html` Datei. Dies führt Sie zur Benutzeroberfläche der NetApp Deployment Engine.

Weitere Informationen

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

Weisen Sie IP-Adressen manuell dem Zugriff auf die NetApp Deployment Engine zu

Sie können auf allen NetApp HCI-Nodes manuell statische IPv4-Adressen den Bond1G- und Bond10G-Schnittstellen zuweisen, um auf die NetApp Deployment Engine zuzugreifen und NetApp HCI zu implementieren. Sie sollten diese Methode nur verwenden, wenn Ihr Netzwerk besondere Anforderungen hat.

Was Sie benötigen

- Sie oder Ihr Netzwerkadministrator haben die Aufgaben im Dokument Installations- und Setup-Anleitung ausgeführt.
- Sie haben physischen Zugriff auf die NetApp HCI-Nodes.
- Alle NetApp HCI-Nodes sind eingeschaltet.
- DHCP ist für die NetApp HCI-Netzwerke nicht aktiviert, und die NetApp HCI-Nodes haben keine IP-Adressen von DHCP-Servern erhalten. HINWEIS: Alle IP-Adressen, die Sie vor der Implementierung des Systems manuell mit der NetApp Deployment Engine zuweisen, sind temporär und können nicht wiederverwendet werden. Wenn Sie IP-Adressen manuell zuweisen möchten, müssen Sie einen zweiten permanenten Satz nicht verwendeter IP-Adressen festlegen, den Sie während der endgültigen Bereitstellung zuweisen können.

Über diese Aufgabe

In dieser Konfiguration verwenden Computing- und Storage-Nodes statische IPv4-Adressen, um während der Implementierung mit anderen Nodes zu erkennen und zu kommunizieren. Diese Konfiguration wird nicht empfohlen.

Schritte

1. Stecken Sie ein KVM in die Rückseite eines der NetApp HCI Storage-Nodes (dieser Node wird der steuernde Storage-Node).
2. Konfigurieren Sie die IP-Adresse, die Subnetzmaske und die Gateway-Adresse für Bond1G und Bond10G in der Benutzeroberfläche. Sie können bei Bedarf auch eine VLAN-ID für jedes Netzwerk konfigurieren.
3. Wiederholen Sie Schritt 2 für die übrigen Storage- und Computing-Nodes.
4. Öffnen Sie einen Webbrowser auf einem Computer, der auf das NetApp HCI-Managementnetzwerk zugreifen kann.
5. Navigieren Sie zur Bond1G-IP-Adresse, die Sie dem steuernden Storage-Node zugewiesen haben. Beispiel:

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

   Dies führt Sie zur Benutzeroberfläche der NetApp Deployment Engine.

Weitere Informationen

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

Starten Sie die Implementierung

Bevor Sie mit der NetApp HCI-Bereitstellung fortfahren können, müssen Sie die Endbenutzer-Lizenzvereinbarungen lesen und verstehen.

Schritte

1. Wählen Sie auf der Seite **Willkommen bei NetApp HCI erste Schritte**.
2. Gehen Sie auf der Seite **Voraussetzungen** wie folgt vor:
   a. Stellen Sie sicher, dass jede Voraussetzung erfüllt ist, und aktivieren Sie zur Bestätigung jedes zugehörigen Kontrollkästchens.
   b. Wählen Sie **Weiter**.
3. Gehen Sie auf der Seite **Endbenutzer-Lizenzen** wie folgt vor:
   a. Lesen Sie die Endbenutzer-Lizenzvereinbarung für NetApp
   b. Wenn Sie die Bedingungen akzeptieren, wählen Sie am Ende des Vertragstextes **Ich akzeptiere** aus.
   c. Lesen Sie die VMware-Endbenutzer-Lizenzvereinbarung.
   d. Wenn Sie die Bedingungen akzeptieren, wählen Sie am Ende des Vertragstextes **Ich akzeptiere** aus.
   e. Wählen Sie **Weiter**.

Weitere Informationen

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

Konfigurieren Sie VMware vSphere

Konfiguration von VMware vSphere

NetApp HCI verwendet die vCenter Server- und ESXi-Komponenten von VMware vSphere. VCenter Server dient zur Verwaltung und Überwachung des auf jedem Rechenknoten installierten VMware ESXi-Hypervisors. Sie können eine neue vSphere Implementierung installieren und konfigurieren, die auch das NetApp Element Plug-in für vCenter Server installiert, oder eine vorhandene vSphere Implementierung einbinden und erweitern.

Beachten Sie bei der Installation einer neuen vSphere Implementierung die folgenden Einschränkungen:

- Die NetApp Deployment Engine installiert die neue vCenter Server Appliance mit der kleinen Implementierungsoption.
- Die vCenter Server-Lizenz ist eine temporäre Evaluierungslizenz. Um den Betrieb nach Ablauf des Evaluierungszeitraums fortgeführt zu haben, müssen Sie einen neuen Lizenzschlüssel von VMware erhalten und diesen in die vCenter Server-Lizenzbestandsliste einfügen.

> Wenn Ihre vSphere Inventarkonfiguration einen Ordner verwendet, um das NetApp HCI Cluster im vCenter Datacenter zu speichern, schlagen einige Vorgänge, wie z. B. die Erweiterung von NetApp HCI Computing-Ressourcen, fehl. Stellen Sie sicher, dass sich das NetApp HCI-Cluster direkt im Datacenter in der Inventurstruktur des vSphere Web-Clients befindet und nicht in einem Ordner gespeichert ist. Weitere Informationen finden Sie im NetApp Knowledgebase Artikel.

Wenn Sie einen neuen vCenter Server installieren, können Sie während der Netzwerkkonfiguration einen vSphere Standard-Switch oder einen vSphere Distributed Switch (VDS) installieren. Ein VDS ermöglicht nach der NetApp HCI-Implementierung ein vereinfachtes, zentralisiertes Management der Netzwerkkonfiguration für Virtual Machines. Die Funktionen der Cloud-Datenservices auf NetApp HCI erfordern ein VDS; die Standard-Switches von vSphere werden für Cloud-Datenservices nicht unterstützt.

Weitere Informationen

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

Konfigurieren einer neuen VMware vSphere Umgebung

Sie können im Rahmen des NetApp HCI-Installationsprozesses eine neue vSphere Umgebung implementieren, indem Sie einige der Netzwerkinformationen bereitstellen, die vSphere verwenden sollte. Wenn Sie vSphere mit einer IP-Adresse konfigurieren, kann die Adresse nach der Installation nicht mehr geändert werden.

Was Sie benötigen

Sie haben die Netzwerkinformationen für die geplante vSphere Umgebung erhalten.

Schritte

1. Wählen Sie **Configure a New vSphere Deployment**.

2. Wählen Sie die Version von vSphere aus, die während der Bereitstellung installiert werden soll.
3. Konfiguration der neuen vSphere Umgebung mit einer der folgenden Optionen:

Option	Schritte
Verwenden Sie einen Domain-Namen (empfohlen).	a. Wählen Sie **Configure using a Fully Qualified Domain Name** aus. b. Geben Sie den vCenter Server-Domänennamen in das Feld **vCenter Server Fully Qualified Domain Name** ein. c. Geben Sie die IP-Adresse des DNS-Servers in das Feld * DNS-Server-IP-Adresse* ein. d. Wählen Sie **Weiter**.
Verwenden Sie eine IP-Adresse.	a. Wählen Sie **Konfigurieren mit einer IP-Adresse**. b. Wählen Sie **Weiter**.

Weitere Informationen

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

Schließen Sie sich einer vorhandenen VMware vSphere Implementierung an

Konfigurieren Sie NetApp HCI, um die Vorteile einer vorhandenen vSphere-Bereitstellung zu nutzen, indem Sie die Netzwerkinformationen und -Anmeldeinformationen des vCenter Servers bereitstellen.

Was Sie benötigen

- Wenn Sie einer vorhandenen vSphere 6.7-Bereitstellung beitreten, stellen Sie sicher, dass vCenter Server Version 6.7 Update 1 ausführt.
- Wenn Sie einer vorhandenen vSphere 6.5-Implementierung beitreten, stellen Sie sicher, dass vCenter Server Version 6.5 Update 2 oder höher ausführt.
- Holen Sie sich die Netzwerkdetails und die Anmeldedaten des Administrators für Ihre vorhandene vSphere Implementierung.

Über diese Aufgabe

Wenn Sie mehrere vCenter Server-Systeme verbinden, die über den vCenter Linked Mode verbunden sind, erkennt NetApp HCI nur eines der vCenter Server Systeme.

Die Verwendung des NetApp Element-Plug-ins für vCenter Server zur Verwaltung von Clusterressourcen von anderen vCenter-Servern aus "VCenter Linked Mode"ist auf lokale Storage-Cluster beschränkt.

Schritte

1. Wählen Sie **Join and Extend an einer vorhandenen vSphere-Bereitstellung** aus.

2. Geben Sie den Domainnamen oder die IP-Adresse in das Feld **vCenter Server Domain Name oder IP address** ein. Wenn Sie einen Domänennamen eingeben, müssen Sie auch die IP-Adresse eines aktiven DNS-Servers in das angezeigte Feld **DNS Server IP Address** eingeben.
3. Geben Sie die Anmeldeinformationen eines vSphere-Administrators in den Feldern **Benutzername und Passwort** ein.
4. Wählen Sie **Weiter**.

Weitere Informationen

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

NetApp HCI-Anmeldedaten werden konfiguriert

Während der Implementierung definieren Sie einen Satz von Zugangsdaten, die in der neu implementierten VMware vSphere Umgebung, den NetApp HCI Computing- und Storage-Ressourcen und dem Management-Node verwendet werden sollen. Wenn Sie NetApp HCI in einer vorhandenen vSphere Umgebung implementieren, werden diese Anmeldedaten nicht auf den vorhandenen vCenter Server angewendet.

Über diese Aufgabe

Beachten Sie folgende Punkte zu den in der NetApp HCI Deployment Engine festgelegten Anmeldedaten:

- **NetApp Hybrid Cloud Control (HCC) oder Element UI**: Um sich bei der erfolgreichen Implementierung bei NetApp HCC oder der Element User Interface anzumelden, verwenden Sie den in diesem Implementierungsschritt angegebenen Benutzernamen und das Passwort.
- **VMware vCenter**: Um sich bei vCenter anzumelden (falls im Rahmen der Bereitstellung installiert), verwenden Sie den Benutzernamen mit dem Suffix `@vsphere.local` oder dem integrierten `Administrator@vsphere.local` Benutzerkonto und das in diesem Bereitstellungsschritt angegebene Passwort.
- **VMware ESXi**: Um sich bei ESXi auf den Compute-Nodes anzumelden, verwenden Sie den Benutzernamen `root` und das gleiche Passwort, das in diesem Bereitstellungsschritt angegeben wurde.

Bei der Interaktion mit VMware vCenter Instanzen nutzt NetApp Hybrid Cloud Control eine der folgenden Komponenten:

- Das integrierte `Administrator@vsphere.local` Benutzerkonto auf der vCenter-Instanz, das im Rahmen der Bereitstellung installiert wurde.
- Die vCenter Zugangsdaten, über die die NetApp HCI Implementierung mit einem vorhandenen VMware vCenter Server verbunden wurde.

Schritte

1. Geben Sie auf der Seite **Anmeldeinformationen** einen Benutzernamen in das Feld **Benutzername** ein.
2. Geben Sie im Feld **Passwort** ein Passwort ein. Das Passwort muss den Kennwortkriterien entsprechen, die im Feld **Passwort muss enthalten** angezeigt werden.
3. Bestätigen Sie das Passwort im Feld **Passwort erneut eingeben**.
4. Wählen Sie **Weiter**.

Weitere Informationen

- "Unterstützte Firmware- und ESXi-Treiberversionen für NetApp HCI und Firmware-Versionen für NetApp HCI Storage Nodes"
- Informationen zum späteren Aktualisieren der vCenter- und ESXi-Anmeldeinformationen finden Sie unter "Aktualisieren der vCenter- oder ESXi-Anmeldedaten".

Wählen Sie eine Netzwerktopologie aus

Bei der Verkabelung von NetApp HCI-Knoten haben Sie die Möglichkeit, unterschiedliche Netzwerkkabelkonfigurationen je nach Ihren Anforderungen zu verwenden. Für jeden Computing-Node können Sie alle sechs Netzwerkports mit unterschiedlichen Traffic-Typen verwenden, die jedem Port-Paar zugewiesen sind. Alternativ können Sie zwei Ports verwenden, wobei alle Arten von Datenverkehr den Ports zugewiesen sind. Storage-Nodes verwenden die standardmäßige Konfiguration mit vier Kabeln. Ihre Auswahl beeinflusst, welche Compute-Nodes im Inventar ausgewählt werden können.

Was Sie benötigen

Bei Auswahl der zwei-Kabel-Netzwerktopologie für Computing-Nodes sollten folgende Anforderungen berücksichtigt werden:

- Sie haben eine VMware vSphere Enterprise Plus-Lizenz, die Sie nach Abschluss der Bereitstellung anwenden können.
- Sie haben überprüft, ob die Konfiguration Ihres Netzwerks und Ihrer Netzwerk-Switches korrekt ist.
- Für Storage- und vMotion-Netzwerke ist VLAN-Tagging für alle Computing- und Storage-Nodes erforderlich.

Schritte

1. Wählen Sie auf der Seite **Netzwerktopologie** eine Computing-Node-Topologie aus, die sich an die von Ihnen installierte Compute-Nodes für NetApp HCI eignet:
   - **6 Kabeloption**: Die Option mit sechs Kabeln bietet für jeden Verkehrstyp (Verwaltung, virtuelle Maschine und Speicher) dedizierte Ports. Optional können Sie vSphere Distributed Switch (VDS) aktivieren. Durch Aktivieren von VDS wird ein verteilter Switch konfiguriert, der ein vereinfachtes, zentralisiertes Management der Netzwerkkonfiguration für Virtual Machines nach Abschluss der NetApp HCI-Implementierung ermöglicht. Wenn Sie diese Option aktivieren, müssen Sie nach der Bereitstellung über eine vSphere Enterprise Plus-Lizenz verfügen.
   - **2 Kabeloption**: Die zwei-Kabel-Option kombiniert Management, virtuelle Maschine und Speicherverkehr auf zwei verbundenen Ports. Für diese Verkabelungsoption ist VDS erforderlich, und sie wird automatisch aktiviert. Sie müssen eine vSphere Enterprise Plus-Lizenz nach der Bereitstellung anwenden können.
2. Bei einigen Kabeloptionen werden mehrere Ansichten auf der Rückseite der verschiedenen Node-Hardware angezeigt. Gehen Sie durch die Ansichten auf der Rückseite, um zu sehen, wie die Netzwerkkabel für das spezifische Node-Modell und die Kabeloption angeschlossen werden.
3. Wenn Sie fertig sind, wählen Sie **Weiter**.

Weitere Informationen

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

HCI Storage Nodes"

Bestandsauswahl

Bestandsauswahl und Knotenkompatibilität

Bei der Auswahl von Nodes für Ihre Implementierung gelten einige Einschränkungen für die Node-Konfigurationen, die in derselben Implementierung kombiniert werden können.

Kompatibilität von Storage-Nodes

NetApp HCI unterstützt Storage-Nodes und -Laufwerke mit SED (Self-Encrypting Drive) und FIPS 140-2-2-Laufwerksverschlüsselung. Bei der Implementierung oder Erweiterung von NetApp HCI können Sie Nodes mit unterschiedlichen Verschlüsselungsstufen kombinieren. NetApp HCI unterstützt jedoch in dieser Situation nur die grundlegendste Form der Verschlüsselung. Wenn beispielsweise ein Storage-Node gemischt wird, der für FIPS-Verschlüsselung geeignet ist und Nodes nur die SED-Verschlüsselung unterstützen, wird bei dieser Konfiguration die SED-Verschlüsselung unterstützt, die FIPS-Laufwerksverschlüsselung ist jedoch nicht.

Das Hinzufügen von Storage-Nodes, die für eine FIPS-Laufwerksverschlüsselung zum Storage-Cluster sorgen, aktiviert die FIPS-Laufwerksverschlüsselungsfunktion nicht automatisch. Nach der Implementierung oder Erweiterung einer Installation mit FIPS-fähigen Nodes muss die FIPS-Laufwerksverschlüsselung manuell aktiviert werden. Anweisungen dazu finden Sie im Benutzerhandbuch zur Element Software.

Auf allen Storage-Nodes muss dieselbe kleinere Version der Element Software ausgeführt werden, um in derselben Implementierung kompatibel zu sein. Beispielsweise können Sie keinen Storage-Node mit Element 11.3.1 und anderen Storage-Nodes mit Element 11.5 nicht kombinieren.

Je nach Hardware-Konfiguration des Node werden H410S Storage-Nodes möglicherweise in der Bestandsliste mit der Bezeichnung H300S, H500S oder H700S Storage-Nodes angezeigt.

NetApp HCI unterstützt nur bestimmte Storage-Node-Modelle in Storage-Clustern mit zwei Nodes. Weitere Informationen finden Sie unter "Storage-Cluster mit zwei Nodes" oder in den Versionshinweisen für Ihre NetApp HCI-Version.

Bei Storage-Cluster mit zwei Nodes sind die Storage-Node-Typen auf Nodes mit 480-GB- und 960-GB-Laufwerken beschränkt.

Kompatibilität von Computing-Nodes

Computing-Nodes müssen die folgenden Anforderungen erfüllen, um als Inventar ausgewählt werden zu können:

- Die CPU-Generationen in allen Computing-Nodes müssen mit der richtigen VMware vMotion Funktion übereinstimmen. Nachdem Sie einen Computing-Node aus dem Inventar ausgewählt haben, können Sie keine Computing-Nodes mit unterschiedlichen CPU-Generationen auswählen.
- Computing-Nodes können nicht mit GPU-fähigen Compute-Nodes im selben Compute-Cluster kombiniert werden. Wenn Sie einen GPU-fähigen Computing-Node auswählen, werden die aus CPU-Computing-Nodes nicht wählbar und umgekehrt.
- Die auf dem Computing-Node ausgeführte Softwareversion muss mit der Haupt- und Unterversion der NetApp Deployment Engine, die die Implementierung hostet, übereinstimmen. Wenn dies nicht der Fall ist,

müssen Sie mit dem RTFI-Prozess ein neues Image des Computing-Nodes erstellen. Anweisungen finden Sie in den NetApp Knowledgebase-Artikeln zu RTFI.

- Für den Rechenknoten muss die auf der Seite Netzwerktopologie ausgewählte Verkabelungskonfiguration in der Liste **Compute Nodes** ausgewählt sein.
- Die Netzwerkverkabelungskonfigurationen für Computing-Nodes desselben Modells müssen innerhalb eines einzelnen Computing-Clusters übereinstimmen.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element Software Documentation Center"

Wählen Sie Inventar aus

Auf der Seite **Inventar** erkennt die NetApp Deployment Engine automatisch verfügbare Computing- und Storage-Nodes und ermöglicht es Ihnen, alle NetApp HCI-Ressourcen zur Implementierung auszuwählen und hinzuzufügen. Wenn ein Node die Implementierungsanforderungen nicht erfüllt, kann er nicht ausgewählt werden. Die Probleme werden als Fehler angezeigt. Sie können den Cursor über den Fehler in der Zeile des Knotens positionieren, um eine Erklärung anzuzeigen. Wenn Sie auf der Seite „Inventar“ den Node auswählen, der die NetApp Deployment Engine hostet, wird automatisch ausgewählt. Sie können die Auswahl nicht aufheben.

Was Sie benötigen

Jumbo-Frames müssen aktiviert sein, um eine ordnungsgemäße Inventarerkennung zu gewährleisten. Wenn im Inventar keine Nodes oder nur eine Untermenge von Nodes angezeigt werden, überprüfen Sie, ob die für NetApp HCI Nodes verwendeten Switch Ports (alle SFP+/SFP28-Schnittstellen) mit Jumbo Frames konfiguriert sind.

Schritte

1. Zeigen Sie auf der Seite **Inventar** die Liste der verfügbaren Knoten an.

   Wenn das System keine Bestandsliste erkennt, wird ein Fehler angezeigt. Beheben Sie den Fehler, bevor Sie fortfahren. Wenn Ihr System DHCP für die Zuweisung von IP-Adressen verwendet, werden die Storage- und Computing-Ressourcen möglicherweise nicht sofort im Inventar angezeigt.

2. Optional: Wenn eine Ressource nicht sofort im Bestand angezeigt wird oder wenn Sie einen Fehler beheben und den Bestand aktualisieren müssen, wählen Sie **Bestand aktualisieren**. Möglicherweise müssen Sie den Bestand mehrmals aktualisieren.
3. Optional: So filtern Sie den Bestand nach Node-Attributen wie Node-Typ:
   a. Wählen Sie **Filter** in der Kopfzeile der Listen **Compute Nodes** oder **Storage Nodes** aus.
   b. Wählen Sie aus den Dropdown-Listen Kriterien aus.
   c. Geben Sie unter den Dropdown-Listen Informationen ein, um die Kriterien zu erfüllen.
   d. Wählen Sie **Filter Hinzufügen**.
   e. Löschen Sie einzelne Filter, indem Sie **X** neben einem aktiven Filter auswählen, oder deaktivieren Sie alle Filter, indem Sie **X** über der Filterliste auswählen.
4. Wählen Sie aus der Liste **Compute Nodes** alle mit Ihrem System gelieferten Computing-Nodes aus.

Sie müssen mindestens zwei Computing-Nodes auswählen, um mit der Implementierung fortzufahren.

5. Wählen Sie aus der Liste **Storage Nodes** alle Storage Nodes aus, die mit Ihrem System geliefert wurden.

   Sie müssen mindestens zwei Storage-Nodes auswählen, um mit der Implementierung fortzufahren.

6. Optional: Wenn ein Auswahlfeld für Storage-Nodes gekennzeichnet ist, überschreitet dieser Storage-Node 33 % der gesamten Storage Cluster-Kapazität. Gehen Sie wie folgt vor:
   - Löschen Sie das Auswahlfeld für den markierten Speicherknoten.
   - Wählen Sie zusätzliche Storage-Nodes aus, um die Storage-Cluster-Kapazität gleichmäßig auf die Nodes zu verteilen.
7. Wählen Sie **Weiter**.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Netzwerkeinstellungen konfigurieren

NetApp HCI stellt eine Seite mit Netzwerkeinstellungen mit einem einfachen Formular zur Vereinfachung der Netzwerkkonfiguration bereit. Wenn Sie das einfache Formular ausfüllen, füllt NetApp HCI automatisch einen Großteil der restlichen Informationen auf der Seite mit den Netzwerkeinstellungen aus. Sie können dann die endgültigen Netzwerkeinstellungen eingeben und überprüfen, ob die Netzwerkkonfiguration korrekt ist, bevor Sie fortfahren. Sie müssen das Formular nicht vollständig ausfüllen.

Was Sie benötigen

- Sie haben folgende Informationen erhalten:
  - Das geplante Benennungspräfix für die Hosts und das Storage-Cluster
  - Alle geplanten Subnetzmaske, gestartet die IP-Adresse, das Standard-Gateway und VLAN-IDs für die Management-, iSCSI- und vMotion-Netzwerke
  - Die IP-Adresse, das Standard-Gateway, die VLAN-IDs und die Subnetzmaskeninformationen für jede geplante VMware vCenter-Bereitstellung
  - Die NTP-Serveradresse (Network Time Protocol) für NetApp HCI
  - Die IP-Adressdaten des DNS-Servers für NetApp HCI
- Wenn Sie einen vSphere Distributed Switch bereitstellen, können Sie nach Abschluss der Bereitstellung eine vSphere Enterprise Plus-Lizenz anwenden.
- Wenn Sie Node-Ports während der Konfiguration der Terminal User Interface (TUI) VLAN-IDs zugewiesen haben, haben Sie diese Ports während der Netzwerkkonfiguration mit derselben VLAN-ID konfiguriert. Sie müssen keine getaggten Host-Ports als Access-Ports oder native VLANs auf den verbundenen Switch-Ports konfigurieren.
- Sie haben überprüft, ob die Netzwerk-Switch-Konfiguration korrekt ist. Falsche Switch-Konfigurationen (z. B. falsche VLANs oder MTU-Größe) verursachen Implementierungsfehler.

Über diese Aufgabe

Wenn Sie die Netzwerktopologie mit zwei Kabeln für Computing-Nodes ausgewählt haben, müssen Sie für vMotion und Storage-Netzwerke für alle Computing- und Storage-Nodes in der Bereitstellung VLAN-IDs verwenden (für die Managementnetzwerke sind optionale IDs).

> Wenn Sie vor der Implementierung Host-seitiges VLAN-Tagging erfordern, wenn Sie VLAN-IDs auf Computing- und Storage-Nodes konfiguriert haben, damit sie durch die NetApp Deployment Engine erkannt werden können, stellen Sie sicher, dass Sie bei der Konfiguration der Netzwerkeinstellungen in der NetApp Deployment Engine die richtigen VLANs verwenden.

Wenn Sie einen Speicher-Cluster mit zwei oder drei Knoten bereitstellen, können Sie die IP-Adressinformationen für Witness Nodes auf der Seite **Network Settings** nach der Verwendung des einfachen Formulars ausfüllen.

Schritte

1. Optional: Um die Live-Validierung von Netzwerkinformationen zu deaktivieren, die Sie auf dieser Seite eingeben, schalten Sie den Schalter **Live Network validation is** auf **aus** um.
2. Geben Sie im Abschnitt **Infrastrukturdienste** der Seite **Netzwerkeinstellungen** die DNS- und NTP-Serverinformationen für NetApp HCI in die folgenden Felder ein:

Feld	Beschreibung
DNS Server IP-Adresse 1	Die IP-Adresse des primären DNS-Servers für NetApp HCI. Wenn Sie auf der Seite vCenter Configuration einen DNS-Server angegeben haben, ist dieses Feld ausgefüllt und schreibgeschützt.
DNS Server IP-Adresse 2 (optional)	Eine optionale IP-Adresse eines sekundären DNS-Servers für NetApp HCI.
* NTP-Server-Adresse 1*	Die IP-Adresse oder der vollqualifizierte Domain-Name des primären NTP-Servers für diese Infrastruktur.
NTP-Serveradresse 2 (optional)	Eine optionale IP-Adresse oder ein vollständig qualifizierter Domain-Name des sekundären NTP-Servers für diese Infrastruktur.

3. Wählen Sie **um Zeit zu sparen, starten Sie das einfache Formular**, um weniger Netzwerkeinstellungen einzugeben.

   Das Dialogfeld **Network Settings Easy Form** wird angezeigt.

4. Geben Sie im Feld **Naming Prefix** ein Präfix für die Benennung ein.

   Das Namenspräfix wird auf den Namen jedes Hosts und den Namen des Storage-Clusters angewendet. Präfixe für die Benennung haben folgende Merkmale:

   - Nur mit einem Buchstaben beginnen
   - Kann Buchstaben, Zahlen und Bindestriche enthalten
   - Darf nicht mehr als 55 Zeichen enthalten

5. Wählen Sie eine der folgenden Optionen für das Zuweisen von VLAN-IDs aus.

   Wenn Sie das Formular verwenden, wählen Sie **Clear** neben einer Zeile aus, um die Eingabe aus einer

Zeile von Feldern zu löschen.

> Wenn Sie VLAN-IDs zuweisen, konfigurieren Sie VLAN-Tags, die NetApp HCI für den Netzwerkverkehr gelten. Sie müssen Ihr natives VLAN nicht als VLAN-ID eingeben. Um das native VLAN für ein Netzwerk zu verwenden, lassen Sie das entsprechende Feld leer.

Option	Schritte
Weisen Sie VLAN-IDs zu	a. Wählen Sie **Ja** für die Option **wird VLAN-IDs** zugewiesen. b. Geben Sie in der Spalte **VLAN ID** ein VLAN-Tag ein, das für jeden Netzwerkdatenverkehr verwendet werden soll, den Sie einem VLAN zuweisen möchten. Sowohl beim Computing-vMotion-Datenverkehr als auch beim iSCSI-Datenverkehr muss eine nicht gemeinsam genutzte VLAN-ID verwendet werden. c. Wählen Sie **Weiter**. d. Geben Sie in der Spalte **Subnetz** Subnetzdefinitionen im CIDR-Format für jeden Netzwerkdatenverkehr in jedem Netzwerk ein, z. B. 192.168.1.0/24. e. Geben Sie in der Spalte **Default Gateway** die IP-Adresse des Standard-Gateways für jeden Netzwerkdatenverkehr in jedem Netzwerk ein. f. Geben Sie in der Spalte **Starting IP** die erste nutzbare IP-Adresse für jedes Netzwerk-Subnetz in jedem Netzwerk ein.
Weisen Sie keine VLAN-IDs zu	a. Wählen Sie **Nein** für die Option **wird VLAN-IDs** zugewiesen. b. Geben Sie in der Spalte **Subnetz** Subnetzdefinitionen im CIDR-Format für jeden Netzwerkdatenverkehr in jedem Netzwerk ein, z. B. 192.168.1.0/24. c. Geben Sie in der Spalte **Default Gateway** die IP-Adresse des Standard-Gateways für jeden Netzwerkdatenverkehr in jedem Netzwerk ein. d. Geben Sie in der Spalte **Starting IP** die erste nutzbare IP-Adresse für jeden Netzwerkdatenverkehr in jedem Netzwerk ein.

6. Wählen Sie **auf Netzwerkeinstellungen anwenden**.
7. Wählen Sie zur Bestätigung * Ja* aus.

   Dies füllt die Seite **Netzwerkeinstellungen** mit den Einstellungen aus, die Sie in der einfachen Form

eingegeben haben. NetApp HCI validiert die von Ihnen eingegebenen IP-Adressen. Sie können diese Validierung mit der Schaltfläche Live Network Validation deaktivieren deaktivieren deaktivieren deaktivieren deaktivieren.

8. Überprüfen Sie, ob die automatisch ausgefüllten Daten korrekt sind.
9. Wählen Sie **Weiter**.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Konfiguration prüfen und implementieren

Sie können die von Ihnen bereitgestellten Informationen vor Beginn der Implementierung überprüfen. Sie können auch fehlerhafte oder unvollständige Informationen korrigieren, bevor Sie fortfahren.

Während der Implementierung erstellt der Management-Node-Installationsprozess Volumes, deren Namen mit im Element Storage-Cluster beginnen `NetApp-HCI-`, und ein SolidFire-Konto, das mit dem Namen beginnt `tenant_`. Löschen Sie diese Volumes oder Konten nicht; dies führt zu einem Verlust der Verwaltungsfunktionalität.

Schritte

1. Optional: Wählen Sie das Symbol **Download**, um Installationsinformationen im CSV-Format herunterzuladen.

   Sie können diese Datei speichern und später auf sie verweisen, um Informationen zur Konfiguration zu erhalten.

2. Erweitern Sie die einzelnen Abschnitte und prüfen Sie die Informationen. Um alle Abschnitte gleichzeitig zu erweitern, wählen Sie **Alle erweitern**.
3. Optional: So nehmen Sie Änderungen an den Informationen in einem beliebigen angezeigten Abschnitt vor:
   a. Wählen Sie im entsprechenden Abschnitt die Option **Bearbeiten** aus.
   b. Nehmen Sie die erforderlichen Änderungen vor.
   c. Wählen Sie **Weiter**, bis Sie die Seite **Bewertung** erreichen. Ihre vorherigen Einstellungen werden auf jeder Seite gespeichert.
   d. Wiederholen Sie die Schritte 2 und 3, um alle weiteren erforderlichen Änderungen vorzunehmen.
4. Wenn Sie keine Cluster-Statistiken und Support-Informationen an von NetApp gehostete SolidFire Active IQ Server senden möchten, deaktivieren Sie das endgültige Kontrollkästchen.

   Hierdurch wird der Zustand und die Diagnoseüberwachung in Echtzeit für NetApp HCI deaktiviert. Wenn diese Funktion deaktiviert wird, ist es für NetApp nicht mehr möglich, NetApp HCI proaktiv zu unterstützen und zu überwachen, um Probleme zu erkennen und zu beheben, bevor die Produktion beeinträchtigt wird.

5. Wenn alle Informationen korrekt sind, wählen Sie **Bereitstellung starten**.

Ein Dialogfeld wird angezeigt. Bei Problemen mit der Netzwerkverbindung oder bei einem Stromausfall während des letzten Einrichtungsvorgangs oder bei Verlust der Browsersitzung können Sie die im Dialogfeld angezeigte URL kopieren und verwenden, um zur letzten Seite zum Setup-Fortschritt zu wechseln.

6. Überprüfen Sie die Informationen im Dialogfeld und wählen Sie **in Zwischenablage kopieren** aus, um die URL in die Zwischenablage zu kopieren.
7. Speichern Sie die URL in einer Textdatei auf Ihrem Computer.
8. Wenn Sie bereit sind, mit der Bereitstellung fortzufahren, wählen Sie **OK**.

   Die Bereitstellung beginnt und eine Fortschrittsseite wird angezeigt. Schließen Sie das Browser-Fenster nicht oder navigieren Sie von der Fortschrittsseite weg, bis die Bereitstellung abgeschlossen ist. Wenn Ihre Browser-Sitzung aus irgendeinem Grund verloren gegangen ist, können Sie die zuvor kopierte URL aufrufen (und alle angezeigten Sicherheitswarnungen akzeptieren), um wieder Zugriff auf die Seite mit dem endgültigen Setup-Fortschritt zu erhalten.

   Wenn die Bereitstellung fehlschlägt, speichern Sie Fehlermeldungen, und wenden Sie sich an den NetApp Support.

   Nach Abschluss der Implementierung werden die Computing-Nodes möglicherweise mehr als ein Mal neu gestartet, bevor sie bereit für den Service sind.

Nachdem Sie fertig sind

Starten Sie die Verwendung von NetApp HCI, indem Sie **vSphere starten** wählen.

- Bei NetApp HCI-Installationen mit vSphere 6.7 startet dieser Link die HTML5 vSphere Webschnittstelle. Bei Installationen mit vSphere 6.5 wird über diesen Link die Adobe Flash vSphere Webschnittstelle gestartet.
- In Konfigurationen mit zwei oder drei Storage-Nodes konfiguriert die nde die Witness-Nodes so, dass der lokale Datastore auf den Computing-Nodes verwendet wird. Daher zeigt Ihr vSphere Client zwei Warnungen zur Datastore-Nutzung auf Disk* an. Um fortzufahren, wählen Sie in jeder Warnung den Link **auf Grün zurücksetzen** aus.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Aufgaben nach der Implementierung

Aufgaben nach der Implementierung

Je nach Ihrer Auswahl während des Implementierungsprozesses müssen Sie einige abschließende Aufgaben ausführen, bevor das NetApp HCI System betriebsbereit ist. Hierzu zählen die Aktualisierung von Firmware und Treibern und das Vornehmen erforderlicher Änderungen der Konfiguration.

- "Unterstützte Netzwerkänderungen"
- "Deaktivieren Sie den Smartd-Dienst auf NetApp HCI-Compute-Nodes"
- "Deaktivieren Sie den Befehl „lacp-individual“ bei konfigurierten Switches"
- "Erstellen einer NetApp HCC-Rolle in vCenter"
- "Halten Sie VMware vSphere auf dem neuesten Stand"
- "Installieren von GPU-Treibern für Compute-Nodes mit GPU-Aktivierung"
- "Konfigurieren Sie vollständig qualifizierten Domänennamen Web UI-Zugriff"
- "Zugriff auf NetApp Hybrid Cloud Control"
- "Verringern Sie den Verschleiß der Boot-Medien in einem NetApp HCI Computing-Node"

Weitere Informationen

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

Unterstützte Netzwerkänderungen

Nachdem Sie NetApp HCI implementiert haben, können Sie eingeschränkte Änderungen an der Standard-Netzwerkkonfiguration vornehmen. Bestimmte Einstellungen sind jedoch für einen reibungslosen Betrieb und eine ordnungsgemäße Netzwerkerkennung erforderlich. Eine Änderung dieser Einstellungen führt zu unerwartetem Verhalten und kann eine Erweiterung von Computing- und Storage-Ressourcen verhindern.

Nach der Implementierung des Systems können Sie je nach Ihren Netzwerkanforderungen die folgenden Änderungen an der Standardkonfiguration von VMware vSphere vornehmen:

- VSwitch-Namen ändern
- Ändern Sie die Namen der Portgruppen
- Fügen Sie weitere Portgruppen hinzu und entfernen Sie sie
- Ändern Sie die Failover-Reihenfolge der vmnic-Schnittstelle für alle zusätzlichen Portgruppen, die Sie hinzugefügt haben

Die Compute-Nodes H300E, H500E, H700E und H410C

NetApp HCI erwartet die folgende Netzwerkkonfiguration für die Nodes H300E, H500E, H700E und H410C.

Im Folgenden finden Sie eine Konfiguration mit sechs Schnittstellen mit VMware vSphere Distributed Switching (VDS). Diese Konfiguration wird nur unterstützt, wenn sie mit VMware vSphere Distributed Switches verwendet wird. Sie erfordert eine Lizenzierung von VMware vSphere Enterprise Plus.

Netzwerkfunktion	vmkernel	Vmnic (physische Schnittstelle)
Vereinfachtes	vmk0	Vmnic2 (Port A), vmnic3 (Port B)
ISCSI-A	vmk1	Vmnic5 (Port E)
ISCSI-B	vmk2	Vmnic1 (Port D)
VMotion	vmk3	Vmnic4 (Port C), vmnic0 (Port F)

Im Folgenden finden Sie eine Konfiguration mit sechs Schnittstellen und VMware vSphere Standard Switching (VSS). Bei dieser Konfiguration kommen VMware vSphere Standard Switches (VSS) zum Einsatz.

Netzwerkfunktion	vmkernel	Vmnic (physische Schnittstelle)
Vereinfachtes	vmk0	Vmnic2 (Port A), vmnic3 (Port B)
ISCSI-A	vmk2	Vmnic1 (Port E)
ISCSI-B	vmk3	Vmnic5 (Port D)
VMotion	vmk1	Vmnic4 (Port C), vmnic0 (Port F)

Die folgende Konfiguration umfasst zwei Schnittstellen. Diese Konfiguration wird nur unterstützt, wenn sie mit VMware vSphere Distributed Switches (VDS) verwendet wird, und erfordert eine Lizenzierung von VMware vSphere Enterprise Plus.

Netzwerkfunktion	vmkernel	Vmnic (physische Schnittstelle)
Vereinfachtes	vmk0	Vmnic1 (Port D), vmnic5 (Port E)
ISCSI-A	vmk1	Vmnic1 (Port E)
ISCSI-B	vmk2	Vmnic5 (Port D)
VMotion	vmk3	Vmnic1 (Port C), vmnic5 (Port F)

H610C Computing-Nodes

NetApp HCI erwartet die folgende Netzwerkkonfiguration für H610C Nodes.

Diese Konfiguration wird nur unterstützt, wenn sie mit VMware vSphere Distributed Switches (VDS) verwendet wird, und erfordert eine Lizenzierung von VMware vSphere Enterprise Plus.

Die Ports A und B werden auf dem H610C nicht verwendet.

Netzwerkfunktion	vmkernel	Vmnic (physische Schnittstelle)
Vereinfachtes	vmk0	Vmnic2 (Port C), vmnic3 (Port D)
ISCSI-A	vmk1	Vmnic3 (Port D)
ISCSI-B	vmk2	Vmnic2 (Port C)
VMotion	vmk3	Vmnic2 (Port C), vmnic3 (Port D)

H615C Computing-Nodes

NetApp HCI erwartet die folgende Netzwerkkonfiguration für H615C Nodes.

Diese Konfiguration wird nur unterstützt, wenn sie mit VMware vSphere Distributed Switches (VDS) verwendet wird, und erfordert eine Lizenzierung von VMware vSphere Enterprise Plus.

Netzwerkfunktion	vmkernel	Vmnic (physische Schnittstelle)
Vereinfachtes	vmk0	Vmnic0 (Port A), vmnic1 (Port B)
ISCSI-A	vmk1	Vmnic0 (Port B)

Netzwerkfunktion	vmkernel	Vmnic (physische Schnittstelle)
ISCSI-B	vmk2	Vmnic1 (Port A)
VMotion	vmk3	Vmnic0 (Port A), vmnic1 (Port B)

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Deaktivieren Sie den Smartd-Dienst auf NetApp HCI-Compute-Nodes

Standardmäßig fragt der `smartd` Dienst regelmäßig die Laufwerke in den Compute-Nodes ab. Nach der Implementierung von NetApp HCI sollten Sie diesen Service auf allen Computing-Nodes deaktivieren.

Schritte

1. Melden Sie sich mithilfe von SSH oder einer lokalen Konsolensitzung mithilfe der Root-Anmeldedaten bei VMware ESXi auf dem Computing-Node an.
2. Stoppen Sie den laufenden `smartd` Dienst:

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

3. Verhindern Sie, dass der `smartd` Dienst beim Booten startet:

```
chkconfig smartd off
```

4. Wiederholen Sie diese Schritte auf den übrigen Computing-Nodes in Ihrer Installation.

Weitere Informationen

- "Schalten Sie den smartd-Service in VMware ESXi aus"
- "VMware KB-Artikel 2133286"

Deaktivieren Sie den Befehl „lacp-individual“ bei konfigurierten Switches

Standardmäßig bleiben der Mellanox-Switch `lacp-individual`-Befehl und der Cisco-Switch- `lacp suspend-individual`Befehl nach der Implementierung konfiguriert. Dieser Befehl ist nach der Installation nicht erforderlich. Wenn er weiterhin konfiguriert bleibt, kann er bei der Fehlerbehebung oder beim Neustart eines Switch zu Problemen mit dem Volume-Zugriff führen. Nach der Implementierung sollten Sie jede Mellanox-Switch- und Cisco-Switch-Konfiguration

überprüfen und den Befehl oder `lacp suspend-individual` entfernen `lacp-individual`.

Schritte

1. Öffnen Sie mithilfe von SSH eine Sitzung für den Switch.
2. Zeigt die laufende Konfiguration an:

   ```
   show running-config
   ```

3. Überprüfen Sie die Switch-Konfigurationsausgabe für den `lacp-individual` Befehl oder `lacp suspend-individual`.

   > Das ist die `xxx-xxx` vom Benutzer angegebene(n) Schnittstellennummer(n). Falls erforderlich, können Sie auf die Schnittstellennummer zugreifen, indem Sie die Schnittstellen der Multi-Chassis Link Aggregation Group anzeigen: `show mlag interfaces`

   a. Überprüfen Sie bei einem Mellanox-Switch, ob die Ausgabe die folgende Zeile enthält:

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

   b. Überprüfen Sie bei einem Cisco-Switch, ob der Ausgang die folgende Zeile enthält:

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

4. Wenn der Befehl vorhanden ist, entfernen Sie ihn aus der Konfiguration.
   a. Für einen Mellanox Switch:

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

   b. Bei einem Cisco-Switch:
      `no interface mlag-port-channel xxx-xxx lacp suspend-individual enable force`
5. Wiederholen Sie diese Schritte für jeden Switch in Ihrer Konfiguration.

Weitere Informationen

- "Der Storage-Node wird während der Fehlerbehebung heruntergefahren"

Erstellen einer NetApp HCC-Rolle in vCenter

Es wird empfohlen, eine NetApp-HCC-Rolle in vCenter zu erstellen, um nach der Installation vCenter-Assets (Controller) oder Rechenknoten (Nodes) manuell zum Management-Node hinzuzufügen oder vorhandene Controller oder Nodes zu ändern.

Diese NetApp HCC-Rolle beschränkt Ihre Management-Node-Services-Ansicht auf reine NetApp Ressourcen.

Über diese Aufgabe

- Dieses Verfahren beschreibt die in Version 6.7 von vSphere verfügbaren Schritte. Ihre vSphere Benutzeroberfläche kann sich je nach installierter Version von der Beschreibung leicht unterscheiden. Weitere Hilfe finden Sie in der Dokumentation zu VMware vCenter.

- An "Erstellen einer neuen NetApp HCC-Rolle"richten Sie zunächst ein neues Benutzerkonto in vCenter ein, erstellen eine NetApp-HCC-Rolle und weisen dann die Benutzerberechtigungen zu.
- Bei NetApp ESXi Host-Konfigurationen sollten Sie das von nde erstellte Benutzerkonto auf die neue NetApp HCC-Rolle aktualisieren:
  - Verwenden Sie"Diese Option", wenn Ihr NetApp ESXi-Host nicht in einem vCenter-Host-Cluster vorhanden ist
  - Verwenden Sie"Diese Option", wenn Ihr NetApp ESXi-Host innerhalb eines vCenter-Host-Clusters existiert
- Sie können "Konfigurieren Sie ein Controller-Asset"dies auf dem Management-Node bereits tun.
- Verwenden Sie die neue NetApp-HCC-Rolle für "Fügen Sie eine Ressource oder einen Computing-Node hinzu"den Management-Node.

Erstellen einer neuen NetApp HCC-Rolle

Richten Sie in vCenter ein neues Benutzerkonto ein, erstellen Sie eine NetApp HCC-Rolle und weisen Sie dann die Benutzerberechtigungen zu.

Richten Sie ein neues Benutzerkonto in vCenter ein

Führen Sie folgende Schritte aus, um ein neues Benutzerkonto in vCenter einzurichten:

Schritte

1. Melden Sie sich beim vSphere Web Client als gleichwertig an `administrator@vsphere.local`.
2. Wählen Sie im Menü die Option **Verwaltung**.
3. Wählen Sie im Abschnitt **Single Sign On** die Option **Benutzer** und **Gruppen** aus.
4. Wählen Sie in der Liste **Domain** oder Ihre LDAP-Domain aus `vsphere.local`.
5. Wählen Sie **Benutzer Hinzufügen**.
6. Füllen Sie das Formular **Benutzer hinzufügen** aus.

Neue NetApp HCC-Rolle in vCenter erstellen

Führen Sie folgende Schritte aus, um eine neue NetApp HCC-Rolle in vCenter zu erstellen:

Schritte

1. Wählen Sie **Rolle bearbeiten** aus, und weisen Sie die erforderlichen Berechtigungen zu.
2. Wählen Sie im linken Navigationsbereich **Global**.
3. Wählen Sie **Diagnose** und **Lizenzen**.
4. Wählen Sie im linken Navigationsbereich **Hosts** aus.
5. Wählen Sie **Wartung**, **Leistung**, **Konfiguration der Speicherpartition** und **Firmware**.
6. Speichern unter `NetApp Role`.

Weisen Sie vCenter Benutzerberechtigungen zu

Führen Sie die folgenden Schritte aus, um die Benutzerberechtigungen der neuen NetApp HCC-Rolle in vCenter zuzuweisen.

Schritte

1. Wählen Sie im Menü die Option **Hosts** und **Cluster** aus.
2. Wählen Sie im linken Navigationsbereich eine der folgenden Optionen aus:
   - VCenter auf oberster Ebene
   - Ihr gewünschtes vCenter, wenn Sie sich im verknüpften Modus befinden.

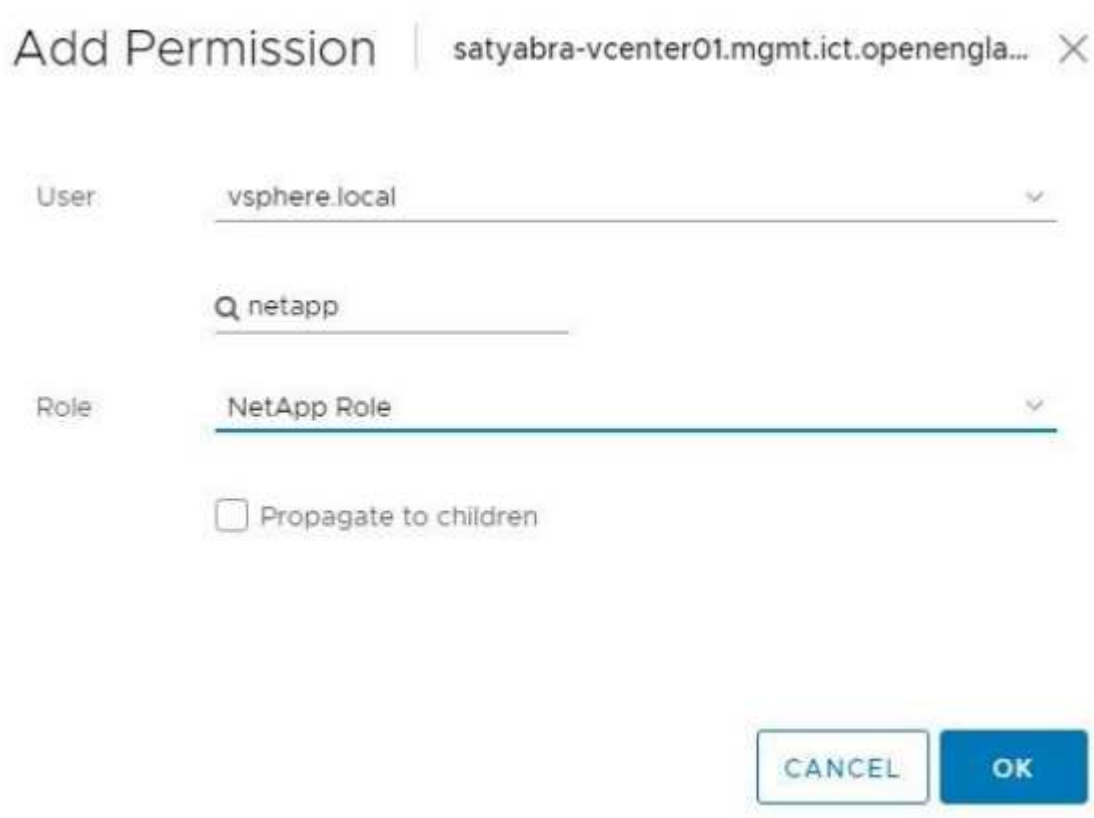
   Die Verwendung des NetApp Element-Plug-ins für vCenter Server zur Verwaltung von Clusterressourcen von anderen vCenter-Servern aus "VCenter Linked Mode"ist auf lokale Storage-Cluster beschränkt.

3. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
4. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie oder Ihre LDAP-Domäne aus `vsphere.local`
   b. Verwenden Sie die Suche, um den neuen Benutzer zu suchen, den Sie in erstellt Richten Sie ein neues Benutzerkonto in vCenter einhaben.
   c. Wählen Sie `NetApp Role`.

   Do * NOT* select **propagieren auf Kinder**.



Weisen Sie dem Rechenzentrum Benutzerberechtigungen zu

Führen Sie die folgenden Schritte aus, um dem Rechenzentrum in vCenter die Benutzerberechtigungen zuzuweisen.

Schritte

1. Wählen Sie im linken Fensterbereich **Datacenter** aus.
2. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
3. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie oder Ihre LDAP-Domäne aus `vsphere.local`.
   b. Verwenden Sie die Suche, um den neuen HCC-Benutzer zu suchen, den Sie in erstellt Richten Sie ein neues Benutzerkonto in vCenter einhaben.
   c. Wählen Sie `ReadOnly role`.

   Do * NOT* select **propagieren auf Kinder**.

Weisen Sie NetApp HCI-Datastores Benutzerberechtigungen zu

Führen Sie die folgenden Schritte aus, um den NetApp HCI-Datastores in vCenter die Benutzerberechtigungen zuzuweisen.

Schritte

1. Wählen Sie im linken Fensterbereich **Datacenter** aus.
2. Erstellen Sie einen neuen Speicherordner. Klicken Sie mit der rechten Maustaste auf **Datacenter** und wählen Sie **Speicherordner erstellen**.
3. Übertragen Sie alle NetApp HCI-Datastores vom Storage-Cluster und lokal auf den Computing-Node in den neuen Speicherordner.
4. Wählen Sie den neuen Speicherordner aus.
5. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
6. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie oder Ihre LDAP-Domäne aus `vsphere.local`.
   b. Verwenden Sie die Suche, um den neuen HCC-Benutzer zu suchen, den Sie in erstellt Richten Sie ein neues Benutzerkonto in vCenter einhaben.
   c. Wählen Sie `Administrator role`
   d. Wählen Sie **auf Kinder übertragen**.

Weisen Sie einem NetApp Host-Cluster Benutzerberechtigungen zu

Führen Sie die folgenden Schritte durch, um die Benutzerberechtigungen einem NetApp Host-Cluster in vCenter zuzuweisen.

Schritte

1. Wählen Sie im linken Navigationsbereich das NetApp Host-Cluster aus.
2. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
3. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

a. Wählen Sie oder Ihre LDAP-Domäne aus `vsphere.local`.

b. Verwenden Sie die Suche, um den neuen HCC-Benutzer zu suchen, den Sie in erstellt Richten Sie ein neues Benutzerkonto in vCenter einhaben.

c. Oder `Administrator` auswählen `NetApp Role`.

d. Wählen Sie **auf Kinder übertragen**.

NetApp ESXi Hostkonfigurationen

Bei NetApp ESXi Hostkonfigurationen sollten Sie das von der nde erstellte Benutzerkonto auf die neue NetApp HCC-Rolle aktualisieren.

Der NetApp ESXi-Host ist nicht in einem vCenter-Host-Cluster vorhanden

Wenn der NetApp ESXi-Host nicht in einem vCenter-Host-Cluster vorhanden ist, können Sie das folgende Verfahren verwenden, um die NetApp HCC-Rolle und Benutzerberechtigungen in vCenter zuzuweisen.

Schritte

1. Wählen Sie im Menü die Option **Hosts** und **Cluster** aus.
2. Wählen Sie im linken Navigationsbereich den NetApp ESXi Host aus.
3. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
4. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie oder Ihre LDAP-Domäne aus `vsphere.local`.

   b. Verwenden Sie die Suche, um den neuen Benutzer zu suchen, den Sie in erstellt Richten Sie ein neues Benutzerkonto in vCenter einhaben.

   c. Oder `Administrator` auswählen `NetApp Role`.

5. Wählen Sie **auf Kinder übertragen**.

Der NetApp ESXi-Host ist in einem vCenter-Host-Cluster vorhanden

Wenn ein NetApp ESXi Host innerhalb eines vCenter Host Clusters mit ESXi Hosts anderer Anbieter vorhanden ist, können Sie im folgenden Verfahren die NetApp HCC-Rolle und die Benutzerberechtigungen in vCenter zuweisen.

1. Wählen Sie im Menü die Option **Hosts** und **Cluster** aus.
2. Erweitern Sie im linken Navigationsbereich den gewünschten Host-Cluster.
3. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
4. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie oder Ihre LDAP-Domäne aus `vsphere.local`.

   b. Verwenden Sie die Suche, um den neuen Benutzer zu suchen, den Sie in erstellt Richten Sie ein neues Benutzerkonto in vCenter einhaben.

c. Wählen Sie `NetApp Role`.

Do * NOT* select **propagieren auf Kinder**.

5. Wählen Sie im linken Navigationsbereich einen NetApp ESXi Host aus.
6. Wählen Sie im rechten Navigationsbereich die Option **Berechtigungen** aus.
7. Klicken Sie auf das Symbol **+**, um den neuen Benutzer hinzuzufügen.

   Fügen Sie im Fenster **Berechtigung hinzufügen** folgende Details hinzu:

   a. Wählen Sie oder Ihre LDAP-Domäne aus `vsphere.local`.
   b. Verwenden Sie die Suche, um den neuen Benutzer zu suchen, den Sie in erstellt Richten Sie ein neues Benutzerkonto in vCenter einhaben.
   c. Oder `Administrator` auswählen `NetApp Role`.
   d. Wählen Sie **auf Kinder übertragen**.
8. Wiederholen Sie diesen Vorgang für verbleibende NetApp ESXi Hosts im Host-Cluster.

Die Controller-Ressource ist bereits auf dem Management-Node vorhanden

Wenn auf dem Verwaltungsknoten bereits ein Controller-Asset vorhanden ist, führen Sie die folgenden Schritte aus, um den Controller mithilfe vonzu konfigurieren `PUT /assets /{asset_id} /controllers /{controller_id}`.

Schritte

1. Zugriff auf die mNode-Service-API-UI auf dem Management-Node:

   `https://<ManagementNodeIP>/mnode`

2. Wählen Sie **autorisieren** aus, und geben Sie die Anmeldeinformationen ein, um auf die API-Aufrufe zuzugreifen.
3. Wählen Sie diese Option, `GET /assets` um die übergeordnete ID zu erhalten.
4. Wählen Sie `PUT /assets /{asset_id} /controllers /{controller_id}`.
   a. Geben Sie die im Account-Setup erstellten Anmeldeinformationen in den Text der Anforderung ein.

Fügen Sie dem Management-Node eine Ressource oder einen Computing-Node hinzu

Wenn Sie nach der Installation manuell ein neues Asset oder einen Compute-Node (und BMC-Assets) hinzufügen müssen, verwenden Sie das neue HCC-Benutzerkonto, das Sie in erstellt Richten Sie ein neues Benutzerkonto in vCenter einhaben. Weitere Informationen finden Sie unter "Fügen Sie dem Management-Node Computing- und Controller-Ressourcen hinzu".

Weitere Informationen

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

Halten Sie VMware vSphere auf dem neuesten Stand

Nach der Bereitstellung von NetApp HCI sollten Sie VMware vSphere Lifecycle Manager verwenden, um die neuesten Sicherheits-Patches für die Version von VMware vSphere, die mit NetApp HCI verwendet wird, anzuwenden.

Stellen Sie mithilfe der "Interoperabilitäts-Matrix-Tool" sicher, dass alle Softwareversionen kompatibel sind. "Dokumentation zu VMware vSphere Lifecycle Manager"Weitere Informationen finden Sie im.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Installieren von GPU-Treibern für Compute-Nodes mit GPU-Aktivierung

Compute-Nodes mit NVIDIA-GPUs (Graphics Processing Units) wie dem H610C müssen NVIDIA-Softwaretreiber in VMware ESXi installiert sein, damit sie von der höheren Verarbeitungsleistung profitieren können. Nach der Implementierung von Computing-Nodes mit GPUs müssen die folgenden Schritte auf jedem GPU-fähigen Compute-Node ausgeführt werden, um die GPU-Treiber in ESXi zu installieren.

Schritte

1. Öffnen Sie einen Browser, und navigieren Sie zum NVIDIA Lizenzportal unter folgender URL:

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

2. Laden Sie je nach Umgebung eines der folgenden Treiberpakete auf Ihren Computer herunter:

VSphere Version	Treiberpaket
VSphere 6.5	`NVIDIA-GRID-vSphere-6.5-410.92-410.91-412.16.zip`
VSphere 6.7	`NVIDIA-GRID-vSphere-6.7-410.92-410.91-412.16.zip`

3. Extrahieren Sie das Treiberpaket auf Ihrem Computer.

   Die resultierende .VIB-Datei ist die unkomprimierte Treiberdatei.

4. Kopieren Sie die `.VIB` Treiberdatei vom Computer in ESXi, die auf dem Compute-Node ausgeführt wird. Bei den folgenden Beispielbefehlen für jede Version wird davon ausgegangen, dass sich der Treiber im `$HOME/NVIDIA/ESX6.x/` Verzeichnis auf dem Managementhost befindet. Das SCP Utility ist in den meisten Linux Distributionen jederzeit verfügbar oder als Download-Dienstprogramm für alle Windows Versionen erhältlich:

ESXi-Version	Beschreibung
ESXi 6.5	`scp $HOME/NVIDIA/ESX6.5/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.`
ESXi 6.7	`scp $HOME/NVIDIA/ESX6.7/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.`

5. Verwenden Sie die folgenden Schritte, um sich als Root-Protokoll auf dem ESXi Host einzuloggen und den NVIDIA vGPU-Manager in ESXi zu installieren.
   a. Führen Sie den folgenden Befehl aus, um sich beim ESXi-Host als Root-Benutzer anzumelden:

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

   b. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob derzeit keine NVIDIA-GPU-Treiber installiert sind:

      ```
      nvidia-smi
      ```

      Dieser Befehl sollte die Meldung zurückgeben `nvidia-smi: not found`.

   c. Führen Sie die folgenden Befehle aus, um den Wartungsmodus auf dem Host zu aktivieren und den NVIDIA vGPU-Manager aus der VIB-Datei zu installieren:

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

      Sie sollten die Nachricht sehen `Operation finished successfully`.

   d. Führen Sie den folgenden Befehl aus, und überprüfen Sie, ob alle acht GPU-Treiber in der Befehlsausgabe aufgeführt sind:

      ```
      nvidia-smi
      ```

   e. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das NVIDIA vGPU-Paket ordnungsgemäß installiert und geladen wurde:

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

      Der Befehl sollte eine Ausgabe wie die folgende zurückgeben: `nvidia 816 13808`

   f. Führen Sie den folgenden Befehl aus, um den Host neu zu starten:

```
reboot -f
```

g. Führen Sie den folgenden Befehl aus, um den Wartungsmodus zu beenden:

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

6. Wiederholen Sie die Schritte 4-6 für alle anderen neu implementierten Computing-Nodes mit NVIDIA-GPUs.
7. Führen Sie die folgenden Aufgaben anhand der Anweisungen auf der NVIDIA-Dokumentationswebsite durch:
   a. Installieren Sie den NVIDIA Lizenzserver.
   b. Konfigurieren Sie die Virtual Machine-Gastsysteme für die NVIDIA vGPU-Software.
   c. Wenn Sie vGPU-fähige Desktops im Kontext einer Virtual Desktop Infrastructure (VDI) verwenden, konfigurieren Sie die VMware Horizon View für NVIDIA vGPU-Software.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Konfigurieren Sie vollständig qualifizierten Domänennamen Web UI-Zugriff

Mit NetApp HCI mit Element 12.2 oder höher können Sie mithilfe des vollständig qualifizierten Domänennamens (FQDN) auf Webschnittstellen des Speicher-Clusters 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 für den Management-Node pro Node: `https://<ManagementNodeIP>:442`
2. Ändern Sie die Storage-Cluster-Einstellungen mithilfe der Element API.
   a. Greifen Sie auf die Element API zu, und erstellen Sie die folgende Einstellung für die Clusterschnittstelle mit der `CreateClusterInterfacePreference` API-Methode, und fügen Sie den Cluster-MVIP-FQDN für den Präferenzwert ein:
      - Name: `mvip_fqdn`

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

  Der FQDN lautet hier beispielsweise `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 Management-Node-IP-Adresse gefolgt von eingeben `/mnode/2/`. Beispiel:

      ```
      https://<ManagementNodeIP>/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 `mnode-client`ein.
   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 `true` oder `false` angegeben verwendet wird `"use_proxy"`.
   j. Wählen Sie **PUT /settings**.
   k. Wählen Sie **Probieren Sie es aus**.
   l. Geben Sie im Bereich „Anforderungskörper“ den FQDN des Verwaltungsknotens als Wert für den Parameter ein `mnode_fqdn`. Geben Sie außerdem an, ob der Proxy verwendet werden soll (`true`oder `false` vom vorherigen Schritt) für den `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 mit der API-Methode auf die Element API zu und löschen Sie die folgende Einstellung für die Cluster-Schnittstelle `DeleteClusterInterfacePreference`:

      - 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 Management-Node-IP-Adresse gefolgt von eingeben `/mnode/2/`. Beispiel:

```
https://<ManagementNodeIP>/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 `mnode-client`ein.

   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 „Anforderungskörper“ keinen Wert für den Parameter ein `mnode_fqdn`. Geben Sie auch an, ob der Proxy verwendet werden soll (`true`oder `false`) für den `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.
• 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

- "CreateClusterInterface API-Informationen im SolidFire and Element Documentation Center"
- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Zugriff auf NetApp Hybrid Cloud Control

Mit NetApp Hybrid Cloud Control können Sie NetApp HCI managen. Sie können Management-Services und andere Komponenten von NetApp HCI aktualisieren und die

Installation erweitern und überwachen. Sie melden sich bei NetApp Hybrid Cloud Control an, indem Sie die IP-Adresse des Management-Node nutzen.

Was Sie benötigen

- **Cluster Administrator Berechtigungen**: Sie haben Berechtigungen als Administrator auf dem Speicher-Cluster.
- **Management Services**: Sie haben Ihre Management Services auf mindestens Version 2.1.326 aktualisiert. NetApp Hybrid Cloud Control ist in früheren Service-Bundle-Versionen nicht verfügbar. Informationen zur aktuellen Service-Bundle-Version finden Sie im "Versionshinweise Für Management Services".

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 Benutzeroberfläche von NetApp Hybrid Cloud Control wird angezeigt.

> Wenn Sie sich mit unzureichenden Berechtigungen angemeldet haben, wird eine Meldung „nicht laden“ auf allen Seiten der HCC-Ressourcen angezeigt, und die Ressourcen stehen nicht zur Verfügung.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Verringern Sie den Verschleiß der Boot-Medien in einem NetApp HCI Computing-Node

Wenn Sie Flash-Speicher oder NVDIMM-Boot-Medien mit einem NetApp HCI-Computing-Node verwenden, wird durch die Beibehaltung der Systemprotokolle auf diesem Medium häufig auf diese Medien geschrieben. In diesem Fall kann der Flash-Speicher eventuell verschlechtert werden. Verwenden Sie die Anweisungen im folgenden KB-Artikel, um die Host-Protokollierung und die Core Dump-Datei auf einen freigegebenen Speicherort zu verschieben. So können Sie verhindern, dass das Boot-Medium im Laufe der Zeit abfällt, und vermeiden Sie vollständige Fehler auf der Boot-Festplatte.

"So wird der Verschleiß des Boot-Laufwerks eines NetApp HCI Computing-Node reduziert"

Weitere Informationen

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

Managen Sie NetApp HCI

NetApp HCI Management-Überblick

Anmeldeinformationen für NetApp HCI, Benutzerkonten, Storage-Cluster, Volumes, Volume-Zugriffsgruppen, Initiatoren, Volume-QoS-Richtlinien und den Management-Node können gemanagt werden.

Hier sind die Punkte, mit denen Sie arbeiten können:

- "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"

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 Benutzeroberfläche der REST-API des Verwaltungsknotens finden Sie unter "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. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, 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 `mnode-client`ein.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
4. Wählen Sie in der REST-API-UI **GET /Assets/Compute_Nodes** aus.

   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. Wählen Sie **Probieren Sie es aus**.
6. Wählen Sie **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. Wählen Sie **PUT /Assets/{Asset_id}/Compute-Nodes/{Compute_id}** aus.

      Hier ist der direkte Link zur API in der UI:

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

   a. Wählen Sie **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. Wählen Sie **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. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, 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 `mnode-client`ein.

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

iv. Schließen Sie das Fenster.

b. Wählen Sie in DER REST API-Benutzeroberfläche **GET /Installations** aus.

c. Wählen Sie **Probieren Sie es aus**.

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

e. Wählen Sie **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

- "SolidFire und Element 12.2 Documentation Center"
- "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. Wählen Sie im Dashboard oben rechts das Options-Symbol aus und wählen Sie **Benutzerverwaltung**.
3. Wählen Sie auf der Seite Benutzer die Option **LDAP konfigurieren** aus.
4. Definieren Sie Ihre LDAP-Konfiguration.
5. Wählen Sie den Authentifizierungstyp Suchen und Bind oder Direct Bind aus.
6. Bevor Sie die Änderungen speichern, wählen Sie **LDAP-Anmeldung testen** oben auf der Seite, geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, den Sie kennen, und wählen Sie **Test**.
7. Wählen Sie **Speichern**.

Managen von autorisierenden Cluster-Konten

"Autoritäre Benutzerkonten" Werden über das Menü Benutzerverwaltung oben rechts in NetApp Hybrid Cloud Control verwaltet. 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. Wählen Sie im Dashboard oben rechts das Optionensymbol aus, und wählen Sie dann **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.

   Um die Berechtigungen aus der NetApp Element-Software anzuzeigen, wählen Sie **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. Wählen Sie **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. Wählen Sie im Dashboard das Symbol oben rechts aus und wählen Sie **Benutzerverwaltung**.
3. Filtern Sie die Liste der Benutzerkonten optional durch Auswahl von **Cluster**, **LDAP** oder **IDP**.

   Wenn Sie Benutzer auf dem Storage-Cluster mit LDAP konfiguriert haben, wird für diese Konten der Benutzertyp „LDAP“ angezeigt. Wenn Sie Benutzer auf dem Storage-Cluster mit IDP konfiguriert haben, wird für diese Konten der Benutzertyp „IDP“ angezeigt.

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" Für die autoritative Cluster-Ressource, die die NetApp Hybrid Cloud Control API verwendet.

   Die Benutzeroberfläche von NetApp Hybrid Cloud Control dauert möglicherweise bis zu 15 Minuten, um den Bestand zu aktualisieren. Um die Bestandsaufnahme manuell zu aktualisieren, greifen Sie auf den REST-API-UI-Bestandsdienst `https://<ManagementNodeIP>/inventory/1/` zu und führen Sie `GET /installations/{id}` für das Cluster aus.

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. Wählen Sie im Dashboard das Symbol oben rechts aus 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" Das Management erfolgt in der NetApp Tabelle „Hybrid Cloud Control Volumes“. 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 Speicher-Cluster, der während des System-Setups hinzugefügt wurde"Autorisierende Storage-Cluster", ist der Standard, aber weitere Cluster können über die HCC-Benutzeroberfläche 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 mit den Leistungsoptionen den "Wartungsmodus"Wartungsmodus für Ihre Storage-Cluster-Nodes aktivieren und deaktivieren.

Was Sie benötigen

- **Cluster Administrator-Berechtigungen**: Sie haben Berechtigungen als Administrator auf der "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 15 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 die Auswahl von **Ja** wird der Cluster aus der Installation entfernt.

5. Wählen Sie **Ja**.

Aktivieren und deaktivieren Sie den Wartungsmodus

Mit diesen "Wartungsmodus" Funktionsoptionen stehen Ihnen die Funktionsoptionen Aktivierenund Deaktivieren der Wartungsmodus für einen Storage-Cluster-Node zur Verfügung.

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:

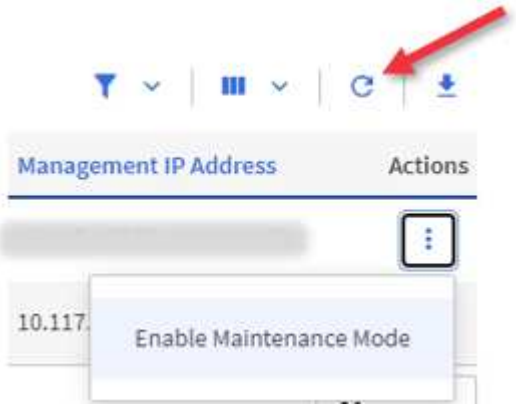
   ```
   https://<ManagementNodeIP>
   ```

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:

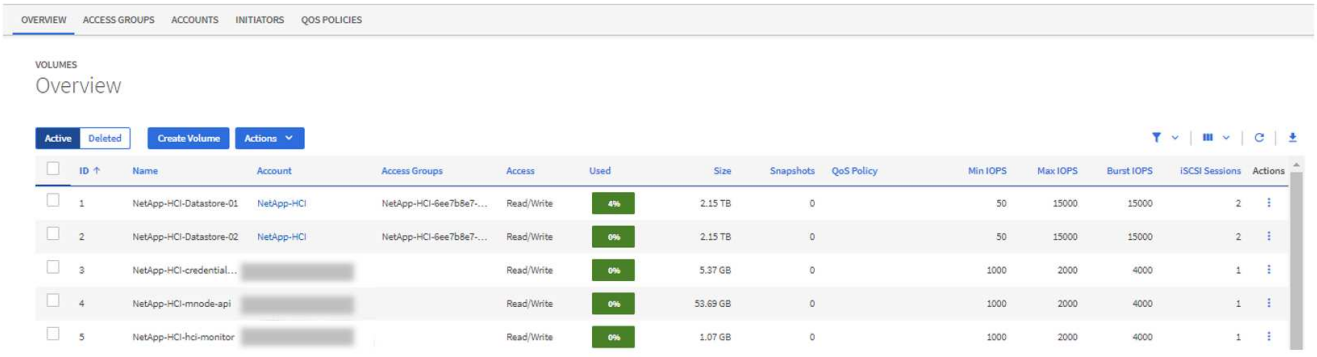
- Erstellen eines Volumes
- Wenden Sie eine QoS-Richtlinie auf ein Volume an
- Bearbeiten Sie ein Volume
- Volumes klonen
- Löschen Sie ein Volume
- Wiederherstellen eines gelöschten Volumes
- Löschen Sie ein gelöschtes Volume

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 in der Liste Konto das Konto aus, das Zugriff auf das Volume haben soll.

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

   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 festzulegen, führen Sie einen der folgenden Schritte aus:
   a. Wählen Sie eine vorhandene QoS-Richtlinie aus.
   b. Legen Sie unter QoS-Einstellungen die angepassten Werte für „Minimum“, „Maximum“ und „Burst“ für IOPS fest, oder verwenden Sie die QoS-Standardwerte.

      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. Wählen Sie **Lautstärke Erstellen**.

Wenden Sie eine QoS-Richtlinie auf ein Volume an

Sie können mithilfe von NetApp Hybrid Cloud Control eine QoS-Richtlinie auf ein vorhandenes Storage-Volume anwenden.

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. Ändern Sie die Servicequalität mit einer der folgenden Aktionen:

   a. Wählen Sie eine vorhandene Richtlinie aus.
   b. 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. Die benutzerdefinierte QoS überschreibt QoS-Richtlinienwerte für Volume-QoS-Einstellungen.

Wenn Sie die IOPS-Werte ändern, erhöhen Sie sich um Dutzende oder Hunderte. 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**.

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, wählen Sie **Neues Konto erstellen**, geben Sie einen neuen Kontonamen ein und wählen Sie **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.

Was Sie benötigen

- 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, und klicken Sie auf die Schaltfläche **Clone**, die angezeigt wird.
5. Führen Sie einen der folgenden Schritte aus:
   - Um ein einzelnes Volume zu klonen, führen Sie folgende Schritte aus:
     i. Geben Sie im Dialogfeld **Clone Volume** einen Volume-Namen für den Volume-Klon ein.

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

     ii. Wählen Sie eine Kontozugriffsebene aus:
        - Schreibgeschützt
        - Lese-/Schreibzugriff
        - Gesperrt
        - Replizierungsziel

     iii. Wählen Sie eine Größe in GB oder gib für den Volume-Klon aus.

        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.

     iv. Wählen Sie ein Konto aus, das dem Volume-Klon zugeordnet werden soll.

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

     v. Wählen Sie **Clone Volumes** Aus.
   - So klonen Sie mehrere Volumes:
     i. Geben Sie im Dialogfeld **Clone Volumes** ein optionales Präfix für die Volume Clones in das Feld **New Volume Name Präfix** ein.
     ii. Wählen Sie einen neuen Zugriffstyp für die Volume-Klone aus, oder kopieren Sie den Zugriffstyp von den aktiven Volumes.
     iii. Wählen Sie ein neues Konto aus, das mit den Volume-Klonen verknüpft werden soll, oder kopieren Sie die Kontenzuordnung aus den aktiven Volumes.

iv. Wählen Sie **Clone Volumes** Aus.

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.

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. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie mehrere Volumes ausgewählt haben, wählen Sie oben in der Tabelle den Schnellfilter **Löschen** aus.
   - Wenn Sie ein einzelnes Volume ausgewählt haben, erweitern Sie in der Spalte **actions** der Tabelle Volumes das Menü für das Volume und wählen **Delete**.
6. Bestätigen Sie den Löschvorgang, indem Sie **Ja** auswählen.

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, wählen Sie oben in der Tabelle den Schnellfilter **Löschen** aus.
   - 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"
- "Arbeiten mit Volumes"
- "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 ein Upgrade Ihrer Managementservices auf mindestens Version 2.15.28 durchgeführt. 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

Sie können für CHAP-basierten statt kontenbasierten Zugriff auf Volumes verwenden"Initiatoren". 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 Initiators IQN ist `iqn.yyyy-mm`, wobei y und m Ziffern sind, gefolgt von Text, der nur Ziffern, Kleinbuchstaben, einen Punkt, (`.`Doppelpunkt (:`oder Strich enthalten darf(`-`. Ein Beispiel für das Format:

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

Das akzeptierte Format eines Fibre Channel-Initiators WWPN ist `: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.

Option	Schritte
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 statt einzelner Volumes finden Sie unter NetApp HCI Concepts Content "QoS-Richtlinien (QoS""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. Wählen Sie die Registerkarte **QoS Policies**.
5. Wählen Sie **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. Wählen Sie **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 möchtenErstellt, war .

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. Wählen Sie das Menü **Aktionen** neben dem Volumen, das 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. Wählen Sie **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. Wählen Sie das Menü **Aktionen** neben dem Volumen, das 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. Wählen Sie **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. Wählen Sie die Registerkarte **QoS Policies**.
5. Wählen Sie das Menü **Aktionen** neben der QoS-Richtlinie, die Sie ändern möchten.
6. Wählen Sie **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. Wählen Sie **Speichern**.

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

Sie können den Link in der Spalte **Active Volumes** für eine Policy auswählen, um eine gefilterte Liste der Volumes anzuzeigen, die dieser Policy zugewiesen 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. Wählen Sie die Registerkarte **QoS Policies**.
5. Wählen Sie das Menü **Aktionen** neben der QoS-Richtlinie, die Sie ändern möchten.
6. Wählen Sie **Löschen**.
7. Bestätigen Sie die Aktion.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "NetApp SolidFire und Element Documentation Center (Version des Documentation Center)"

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.

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

- Mit dem Management Node UI (`https:// [mNode IP}:442`) können Sie Änderungen an Netzwerk- und Cluster-Einstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.
- Mit der integrierten REST-API-UI (`https://[mNode IP}/mnode`) können Sie APIs in Bezug auf die Management-Node-Services ausführen oder verstehen, 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

- (Verwaltungsknoten 12.0 und 12.2 mit Proxyserver) Sie haben NetApp Hybrid Cloud Control auf Verwaltungsdienste Version 2.16 aktualisiert, bevor Sie einen Proxyserver 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 wissen, "Persistente Volumes"ob Sie diese verwenden möchten oder nicht. Persistente Volumes sind optional, jedoch im Falle eines Datenverlusts bei der Management-Node-Konfiguration empfohlen.

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 von der Seite auf der NetApp Support-Website herunter "NetApp HCI":
   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, führen Sie die folgenden Schritte aus:
   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 mit der folgenden Konfiguration eine neue 64-Bit-VM aus Ihrem Hypervisor:
      - 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 VM nicht ein, bevor Sie den Schritt angeben, der später in diesem Verfahren ausgeführt werden soll.

   b. Verbinden Sie die ISO mit der VM 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 VM nach Abschluss der Installation für den Management-Node ein.

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. Wenn im Netzwerk ein DHCP-Server (Dynamic Host Configuration Protocol) vorhanden ist, der IPs mit einer MTU (Maximum Transmission Unit) von weniger als 1500 Byte zuweist, müssen Sie die folgenden Schritte durchführen:

   a. Versetzen Sie den Management-Node vorübergehend in ein vSphere-Netzwerk ohne DHCP, z. B. iSCSI,.

   b. Starten Sie die VM neu, oder starten Sie das VM-Netzwerk neu.

   c. Konfigurieren Sie über TUI die korrekte IP-Adresse im Managementnetzwerk mit einer MTU größer oder gleich 1500 Bytes.

   d. Weisen Sie der VM das richtige VM-Netzwerk erneut zu.

   Ein DHCP, der IPs mit einer MTU unter 1500 Byte zuweist, kann Sie verhindern, dass Sie das Management-Node-Netzwerk konfigurieren oder die Management-Node-UI verwenden.

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

   Wenn Sie eine zusätzliche NIC zur Isolierung des Speicherverkehrs benötigen, 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. Fahren Sie für Management-Knoten 12.3 mit fortUnterschritt (f), um die Konfiguration der Zeitsynchronisierung 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 Standard-Server (`server 0.gentoo.pool.ntp.org`), indem Sie vor jedem einen hinzufügen `#`.

   b. Fügen Sie für jeden Standardzeitserver, 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 verwenden werden"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, ob das `Synchronize guest time with host` Kontrollkästchen in den VM-Optionen deaktiviert ist.

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

> Bearbeiten Sie NTP nach Abschluss der Zeitsynchronisierung nicht, da es sich auf den NTP auswirkt, wenn Sie auf dem Management-Node ausführen"Setup-Befehl".

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 dem gleichen Storage-Cluster, den Sie während verwendet haben"Konfiguration von NTP-Servern".
      - **--Storage_username (-su) [username]**: Der Benutzername des Speicher-Cluster-Administrators für den durch den Parameter angegebenen Cluster `--storage_mvip`.
      - **--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` auf true gesetzt ist, 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 IP (`--proxy_hostname_or_ip`) einzugeben.
- **--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 den `setup-mnode` Befehl aus.

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. Gehen Sie zum Speicher-MVIP und melden Sie sich an. Dadurch 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 `mnode-client`ein.
      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 Antworttext von Code 200 den, und speichern Sie ihn `id` für die Installation, um ihn in einem späteren Schritt zu verwenden.

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` die 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. Greifen Sie auf die mnode Service API UI auf dem Management Node zu, indem Sie die Management Node IP-Adresse gefolgt von `/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 `mnode-client`ein.
      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.

      > Es wird empfohlen, eine neue NetApp-HCC-Rolle in vCenter zu 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 und den vCenter-Anmeldedaten ein `vCenter`.
   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. Geben Sie als `type` ein und geben Sie das Hardware-Tag ein `ESXi Host`, das Sie in einem vorherigen Schritt für gespeichert `hardware_tag` haben.

e. Wählen Sie **Ausführen**.

Weitere Informationen

- "Persistente Volumes"
- "Fügen Sie dem Management-Node eine Ressource 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.

Was Sie benötigen

- 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:

> Die Werte werden `$` für jeden der erforderlichen Parameter für Ihre neue Storage-Netzwerkschnittstelle angezeigt. Das `cluster` Objekt in der folgenden Vorlage ist erforderlich und kann zur Umbenennung des Host-Namens des Management-Node 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:

> Die Werte werden `$` für jeden der erforderlichen Parameter für Ihre neue Storage-Netzwerkschnittstelle angezeigt. Das `cluster` Objekt in der folgenden Vorlage ist erforderlich und kann zur Umbenennung des Host-Namens des Management-Node 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 eine Ressource 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 Ihrem vorherigen Management-Node wurde die NetApp Element-Softwareversion 11.3 oder höher ausgeführt, wobei "Persistente Volumes"die Funktionen aktiviert waren.
- 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 von der Seite auf der NetApp Support-Website herunter "NetApp HCI":
   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, führen Sie die folgenden Schritte aus:
   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 zur Isolierung des Speicherverkehrs benötigen, 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. Fahren Sie für Management-Knoten 12.3 mit fortUnterschritt (f), um die Konfiguration der Zeitsynchronisierung 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 Standard-Server (`server 0.gentoo.pool.ntp.org`), indem Sie vor jedem einen hinzufügen `#`.

   b. Fügen Sie für jeden Standardzeitserver, 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 verwenden werden"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, ob das `Synchronize guest time with host` Kontrollkästchen in den VM-Optionen deaktiviert ist.

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

> Bearbeiten Sie NTP nach Abschluss der Zeitsynchronisierung nicht, da es sich auf den NTP auswirkt, wenn Sie auf dem Management-Node ausführenBefehl „Neuimplementierung“.

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 dem gleichen Storage-Cluster, den 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 den `redeploy-mnode` Befehl aus. Das Skript zeigt eine Erfolgsmeldung an, wenn die erneute Implementierung abgeschlossen ist.

c. Wenn Sie über den vollständig qualifizierten Domänennamen (FQDN) des Systems auf Element- oder NetApp HCI-Webschnittstellen ("Konfigurieren Sie die Authentifizierung für den Management-Node neu"z. B. den Verwaltungsknoten oder die NetApp-Hybrid-Cloud-Steuerung) zugreifen, .

> Wenn Sie die SSH-Funktion auf dem Management-Node zuvor deaktiviert haben, müssen Sie "Deaktivieren Sie SSH erneut"auf dem wiederhergestellten Management-Node die entsprechende Option ausführen. Die SSH-Funktion "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support"ist standardmäßig auf dem Management-Node aktiviert.

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:

- Mit Hilfe der Management Node UI (`https:// [mNode IP}:442`) können Sie Änderungen an Netzwerk- und Cluster-Einstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.
- Mit der integrierten REST API UI (`https://[mNode IP}/mnode`) können Sie APIs im Zusammenhang mit den Management-Node-Services ausführen oder verstehen, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

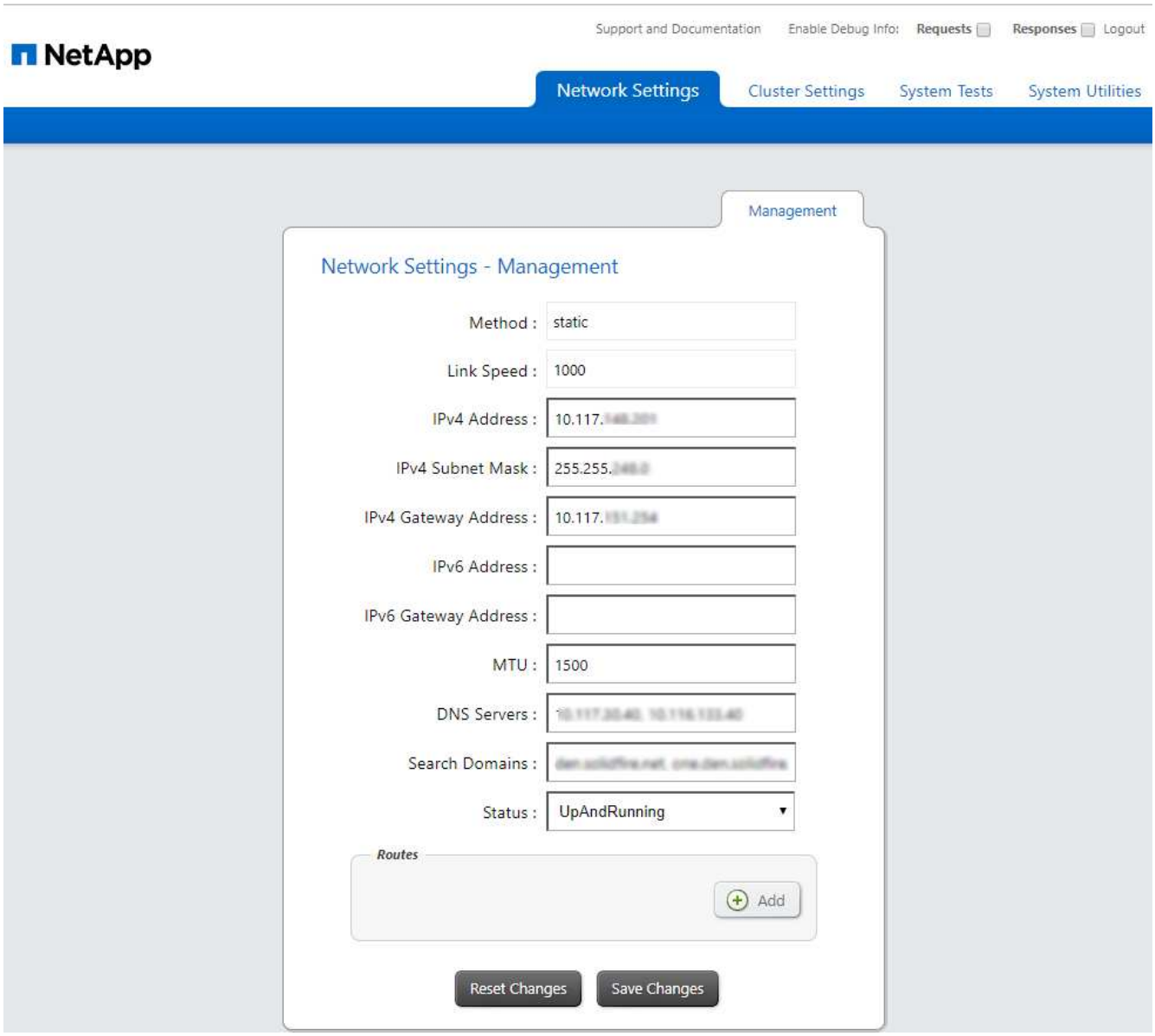
Greifen Sie über die UI auf den Management-Node zu

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.

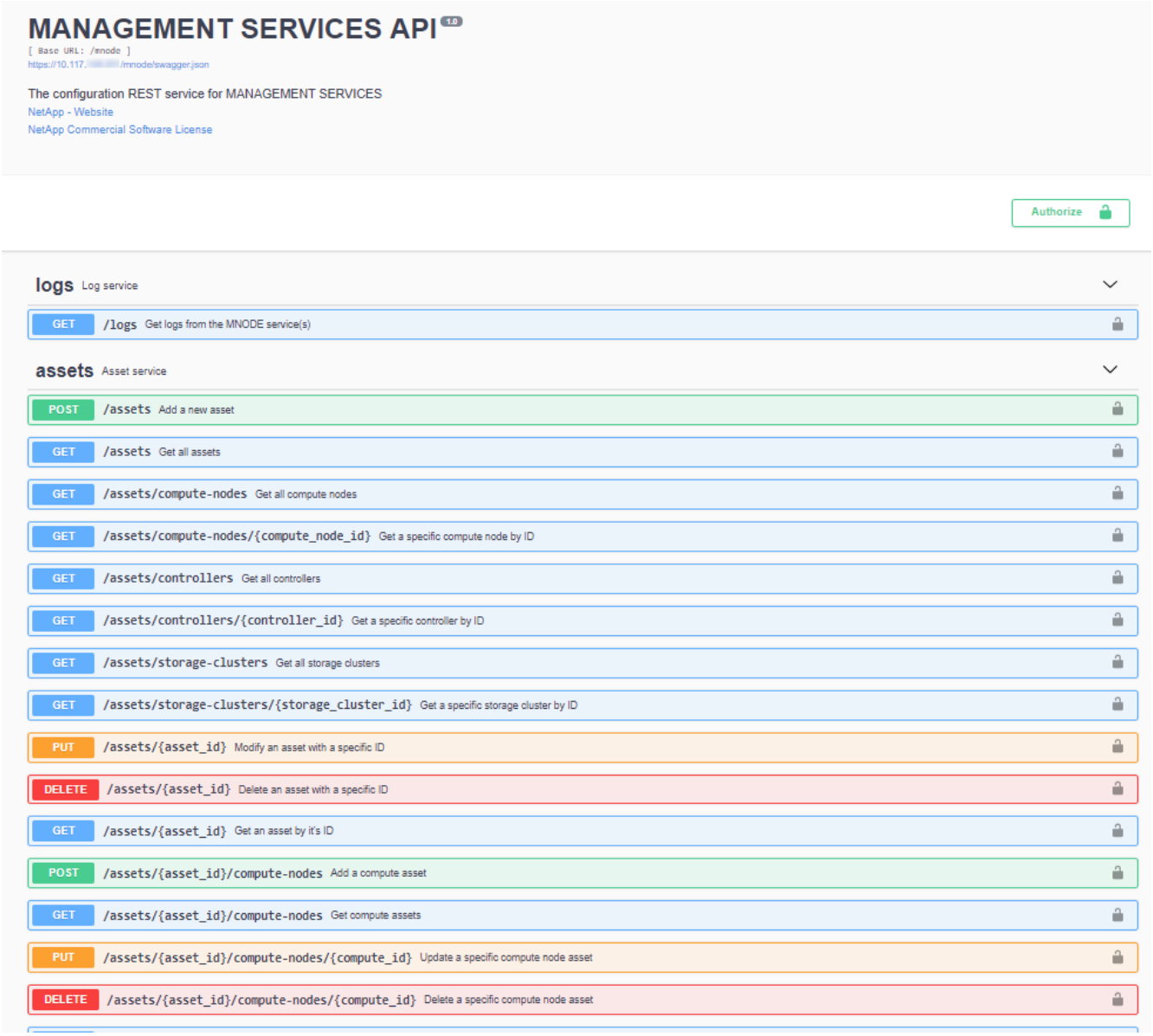
Greifen Sie auf DIE REST-API-UI für den Management-Node zu

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 Managementdienste zuzugreifen, geben Sie die Management-Node-IP-Adresse gefolgt von `/mnode`:

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



2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus und geben Sie Cluster-Administrator-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**

  Mit dem können "GetNodeSSLCertificate-Methode" Sie Informationen über das derzeit installierte SSL-Zertifikat einschließlich aller Zertifikatdetails abrufen.

- **SetNodeSSLZertifikat**

  Sie können mit dem die "SetNodeSSLCertificate-Methode" SSL-Zertifikate für das Cluster und pro Knoten auf das von Ihnen zur Verfügung gestellt Zertifikat und den privaten Schlüssel festlegen. Das System überprüft das Zertifikat und den privaten Schlüssel, um zu verhindern, dass ein ungültiges Zertifikat angewendet wird.

- **RemoveNodeSSLZertifikat**

  Dadurch "RemoveNodeSSLCertificate-Methode" werden das derzeit installierte SSL-Zertifikat und der private Schlüssel entfernt. 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 dem Management Node UI (`https://<ManagementNodeIP>:442`) können Sie Änderungen an Netzwerk- und Cluster-Einstellungen 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. Wählen Sie die Registerkarte **Alert Monitor**.
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 Option **Daten an AIQ senden** mit der NetApp-Bereitstellungsmodul deaktiviert haben, müssen Sie "Telemetrie aktivieren"die REST-API des Verwaltungsknotens erneut verwenden, um den Dienst 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 Option **Daten an AIQ senden** mit der NetApp-Bereitstellungsmodul deaktiviert haben, müssen Sie "Telemetrie aktivieren"die REST-API des Verwaltungsknotens erneut verwenden, um den Dienst 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. Wählen Sie die Registerkarte **Netzwerkeinstellungen** aus.
3. Die folgenden Informationen anzeigen oder eingeben:
   a. **Methode**: Wählen Sie eine der folgenden Methoden, um die Schnittstelle zu konfigurieren:
      - `loopback`: Zur Definition der IPv4-Loopback-Schnittstelle.
      - `manual`: Verwenden Sie diese Option, um Schnittstellen zu definieren, für die standardmäßig keine Konfiguration erfolgt.
      - `dhop`: Verwendung, 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. Wählen Sie die Registerkarte **Cluster-Einstellungen** aus.
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. Wählen Sie in der Management-Knoten-UI **System-Tests** aus.
3. Führen Sie eine der folgenden Aktionen durch:
   a. Um zu überprüfen, ob die von Ihnen konfigurierten Netzwerkeinstellungen für das System gültig sind, wählen Sie **Netzwerk-Konfiguration testen**.
   b. Um die Netzwerkverbindung zu allen Knoten im Cluster sowohl auf 1G- als auch 10G-Schnittstellen mit ICMP-Paketen zu testen, wählen Sie **Test Ping** aus.
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. Wählen Sie **System Utilities**.
3. Wählen Sie die Schaltfläche für das Dienstprogramm aus, 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 sind `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 Skript zugeführt `sf_make_support_bundle`. 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

Mit der integrierten REST API UI (`https://<ManagementNodeIP>/mnode`) können Sie APIs im Zusammenhang mit den Management-Node-Services ausführen oder verstehen, 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.

Was Sie benötigen

- 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 die Management-Node-IP-Adresse gefolgt vom Service-Namen eingeben, z. B. `/mnode/`:

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

2. Wählen Sie **Autorisieren** Aus.

   Alternativ können Sie das Sperrsymbol neben einer beliebigen Service-API auswählen.

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 `mnode-client`ein.
   c. Geben Sie keinen Wert für das Clientgeheimnis ein.
   d. Wählen Sie **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 eine `401 Error: UNAUTHORIZED` Meldung 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.

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.
- Sie haben Internetzugang. Der Active IQ Collector Service kann nicht von dunklen Seiten verwendet werden.

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 `mnode-client`ein.
      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 Antworttext von Code 200 die `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. Greifen Sie auf die mnode Service API UI auf dem Management Node zu, indem Sie die Management Node IP-Adresse gefolgt von `/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 `mnode-client`ein.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Fenster.
   c. Konfigurieren der BasisinAssets:
      i. Wählen Sie **PUT /Assets/{Asset_id}** aus.
      ii. Wählen Sie **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. Wählen Sie **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. Wählen Sie **POST /Assets/{Asset_id}/Controllers** aus, um eine Unterressource des Controllers 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 die erforderlichen Nutzlastwerte mit AS `vCenter`- und vCenter-Anmeldedaten ein `type`.

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

   `ip` Ist die vCenter-IP-Adresse.

   e. Wählen Sie **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" Zur Konfiguration des Management-Node.

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

> Unter Umständen müssen Sie "Ändern der BMC-Zugangsdaten für Computing-Nodes"einen oder `Unable to Detect` den in NetApp Hybrid-Cloud-Steuerung angezeigten Fehler beheben `Hardware ID not available`.

3. Aktualisieren Sie die BestandsdienstAPI auf dem Managementknoten:

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

> Alternativ können Sie 15 Minuten warten, bis der Bestand in der Benutzeroberfläche von NetApp Hybrid Cloud Control aktualisiert wird.

   a. 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 `mnode-client`ein.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Fenster.
   b. Wählen Sie in DER REST API UI **GET /Installations** aus.
   c. Wählen Sie **Probieren Sie es aus**.
   d. Wählen Sie **Ausführen**.
   e. Kopieren Sie aus der Antwort die Installations-Asset(`"id"`-ID).
   f. Wählen Sie in DER REST-API-UI **GET /installations/{id}** aus.
   g. Wählen Sie **Probieren Sie es aus**.
   h. Setzen Sie die Aktualisierung auf `True`.
   i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.
   j. Wählen Sie **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.
- Sie müssen "Neue NetApp HCC-Rolle in vCenter erstellt"die Ansicht der Management-Node-Services auf reine NetApp-Ressourcen beschränken.
- 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 dem Skalieren des NetApp HCI-Systems keine Compute-Nodes in Hybrid Cloud Control (HCC) angezeigt werden, können Sie einen Compute-Node hinzufügen, wie `POST /assets/{asset_id}/compute-nodes` in diesem Verfahren beschrieben.

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 `mnode-client`ein.
      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 Antworttext von Code 200 die `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 (`"controllerId"`) und speichern Sie sie zur Verwendung 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 `mnode-client`ein. 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 `mnode-client`ein. 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 in das Feld ein `ip`. ii. Geben Sie für `hardwareTag` den Wert des Hardware-Tags 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 `mnode-client`ein. 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

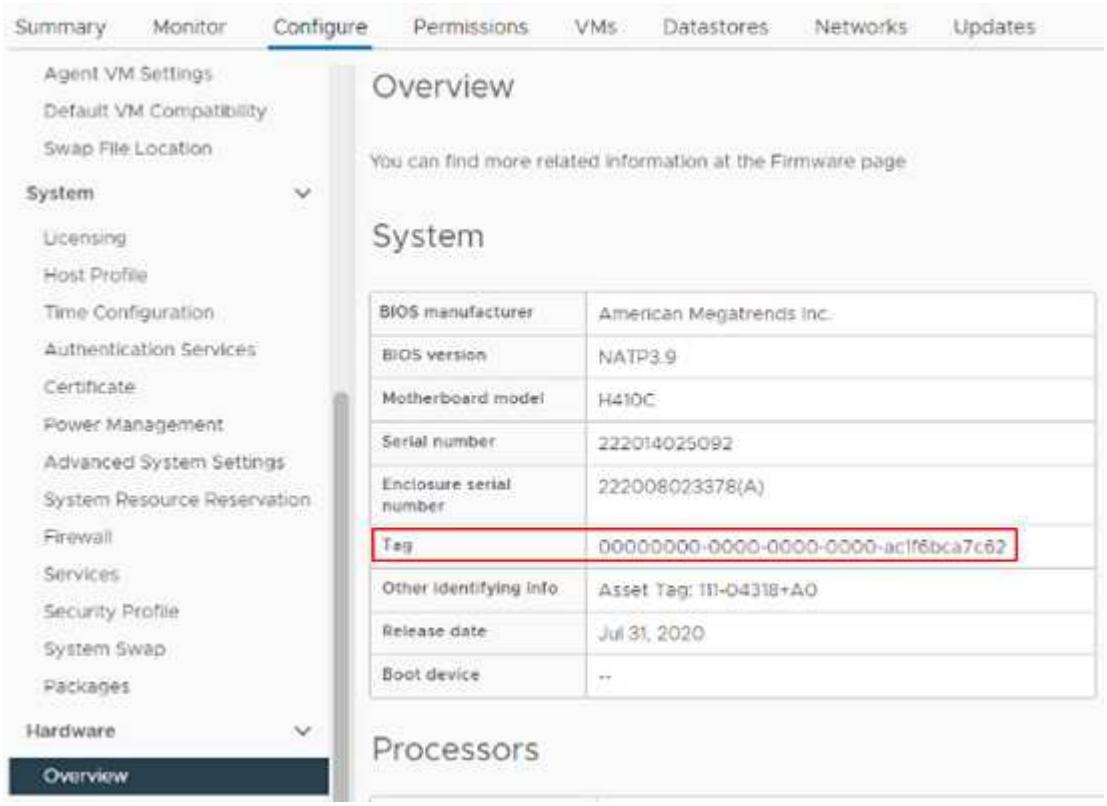
Mithilfe der REST API-Benutzeroberfläche müssen Sie die Hardware-Tag-Nummer zur Konfiguration der Managementknoten hinzufügen.

VMware vSphere 7.0

Suchen Sie die Hardware-Tag-Nummer für einen Compute-Knoten in VMware vSphere Web Client 7.0.

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**. Prüfen Sie, ob das Hardware-Tag in der Tabelle aufgeführt `System` ist.



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 Management-Node-IP-Adresse gefolgt von `/inventory/1/`:

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

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.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **GET /Installations**.
4. Wählen Sie **Probieren Sie es aus**.
5. Wählen Sie **Ausführen**.

   Die API gibt eine Liste aller bekannten Installationen zurück.

6. Speichern Sie aus dem Antworttext 200 den Wert im Feld, den `id` Sie in der Liste der Installationen finden. 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. Greifen Sie auf die REST-API-UI für den Speicherdienst zu, indem Sie die Management-Node-IP-Adresse gefolgt von `/storage/1/`:

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

8. 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.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
9. Wählen Sie **GET /Cluster**.
10. Wählen Sie **Probieren Sie es aus**.
11. Geben Sie die zuvor gespeicherte Installations-ID in den Parameter ein `installationId`.
12. Wählen Sie **Ausführen**.

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

13. Suchen Sie aus dem Antworttext von Code 200 den richtigen Speicher-Cluster, und speichern Sie den Wert im Feld Cluster `storageId`. 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 den für alle Storage-Cluster kopiertStorage Cluster-ID und Installations-ID, die Sie hinzufügen möchten.
- Wenn Sie mehr als einen Storage Node hinzufügen, wissen Sie die Einschränkungen der Unterstützung für und mehrere Storage Cluster bereits zu lesen und zu verstehen"Autorisierende 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. Greifen Sie auf die REST-API-UI für den Speicherdienst zu, indem Sie die Management-Node-IP-Adresse gefolgt von `/storage/1/`:

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

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.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **POST /Cluster**.
4. Wählen Sie **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. Wählen Sie **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.

Stellen Sie sicher, dass Sie die Schritte in befolgt habenRufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab, bevor Sie fortfahren.

Schritte

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

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

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.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **PUT /Clusters/{storageId}** aus.
4. Wählen Sie **Probieren Sie es aus**.

5. Fügen Sie die Storage-Cluster-ID, die Sie zuvor in den Parameter kopiert `storageId` haben, ein.
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. Wählen Sie **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.

Stellen Sie sicher, dass Sie die Schritte in befolgt habenRufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab, bevor Sie fortfahren.

Schritte

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

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

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.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **DELETE /Clusters/{storageId}** aus.
4. Wählen Sie **Probieren Sie es aus**.
5. Geben Sie die Storage-Cluster-ID ein, die Sie zuvor im Parameter kopiert `storageId` haben.
6. Wählen Sie **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.

Was Sie benötigen

- 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 Management-Node-IP-Adresse und dann `/vcenter/1/`:

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

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.
   c. Wählen Sie **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. Wählen Sie **GET /Compute/Controller** aus.
2. Wählen Sie **Probieren Sie es aus**.
3. Wählen Sie **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 wünschen, kopieren Sie die Controller-ID aus dem `id` Feld des Controllers in die Zwischenablage und lesen Sie 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. Wählen Sie **GET /Compute/Controllers/{Controller_id}/Status** aus.
2. Wählen Sie **Probieren Sie es aus**.
3. Geben Sie die Controller-ID ein, die Sie zuvor in den Parameter kopiert `controller_id` haben.
4. Wählen Sie **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. Wählen Sie **PUT /Compute/Controllers/{Controller_id}** aus.
2. Geben Sie die Controller-ID eines vCenter-Controllers in den Parameter ein `controller_id`.
3. Wählen Sie **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. Wählen Sie **Ausführen**.

   Die API gibt aktualisierte Controller-Informationen zurück.

Weitere Informationen

- "Fügen Sie dem Management-Node eine Ressource 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 IP-Adresse des Verwaltungsknotens ein, gefolgt von `/mnode/1/`:

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

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus und geben Sie Cluster-Administrator-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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.
   d. Geben Sie keinen Wert für das Clientgeheimnis ein.
   e. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   f. Schließen Sie das Fenster.
3. Schließen Sie das Dialogfeld * Verfügbare Berechtigungen*.
4. Wählen Sie **GET/Assets** aus.
5. Wählen Sie **Probieren Sie es aus**.
6. Wählen Sie **Ausführen**.
7. Scrollen Sie im Antworttext nach unten zum Abschnitt **Compute** und kopieren Sie die `parent` Werte und `id` für den fehlgeschlagenen Compute-Knoten.
8. Wählen Sie **DELETE/Assets/{Asset_id}/Compute-Nodes/{Compute_id}** aus.
9. Wählen Sie **Probieren Sie es aus**.
10. Geben Sie die Werte und `id` ein `parent`, die Sie in einem vorherigen Schritt kopiert haben.
11. Wählen Sie **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.

Was Sie benötigen

- 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.
- (Verwaltungsknoten 12.0 und 12.2) Sie haben NetApp Hybrid Cloud Control auf Verwaltungsdienste Version 2.16 aktualisiert, bevor Sie einen Proxyserver konfigurieren.

Schritte

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

   ```
   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.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie **PUT /settings**.
4. Wählen Sie **Probieren Sie es aus**.
5. Um einen Proxyserver zu aktivieren, müssen Sie auf true setzen `use_proxy`. 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. Wählen Sie **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}"
```

Sie können den vom API-Befehl verwendeten Träger finden `${TOKEN}`, wenn Sie "Autorisieren". Der Träger `${TOKEN}` ist in der Lockenantwort.

SCHRITTE DER REST API-UI

1. Greifen Sie auf die REST-API-UI für den Service zu, indem Sie die Management-Node-IP-Adresse gefolgt von `/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 Management Services Bundle Version (`"mnode_bundle_version"`), Management Node OS Version) (`"os_version"`und Management Node API Version (`"version"`) sind im Antworttext 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 Logs hinzu.

     Verwenden Sie einen vernünftigen `since` Parameter, wenn Sie Protokolle mit größeren Zeitspannen erfassen.

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

     Verwenden Sie den `GET /services` Befehl, um Services auf dem Management-Node aufzulisten.

   - `stopped`: Auf eingestellt `true`, um Protokolle von angestoppten 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.

Über diese Aufgabe

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. 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

Standardmäßig ist die Fähigkeit für den Remote-Zugriff auf dem Management-Node aktiviert. Informationen zum Deaktivieren der Remote-Zugriffsfunktion finden Sie unter "Verwalten der SSH-Funktionalität auf dem Management-Node". Sie können die Remote-Zugriffsfunktion bei Bedarf wieder aktivieren.

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
```

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. Die SSH-Funktion "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support"ist standardmäßig auf dem Management-Node aktiviert.

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 Benutzeroberfläche von NetApp Hybrid Cloud Control zu verwenden, haben Sie das auf Version 2.20.69 oder höher aktualisiert "Management Services-Bundle".
  - Um die REST-API-UI zu verwenden, haben Sie das auf Version 2.17 aktualisiert "Management Services-Bundle".

Optionen

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

Sie können eine der folgenden Aufgaben nach Ihnen 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. Die SSH-Funktion "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support"ist bei Management-Nodes, auf denen Management-Services 2.18 oder höher ausgeführt werden, 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 mit SSH für einen Storage-Cluster zu aktivieren oder zu deaktivieren, müssen Sie den 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. Die SSH-Funktion "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support"ist standardmäßig auf dem Management-Node aktiviert. 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}"
```

Sie können den vom API-Befehl verwendeten Träger finden `${TOKEN}`, wenn Sie "Autorisieren". Der Träger `${TOKEN}` ist in der Lockenantwort.

SCHRITTE DER REST API-UI

1. Greifen Sie auf die REST-API-UI für den Management-Node-API-Service zu, indem Sie die Management-Node-IP-Adresse gefolgt von `/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 `mnode-client`ein.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie in DER REST API UI **PUT /settings/ssh** aus.
   a. Wählen Sie **Probieren Sie es aus**.
   b. Setzen Sie den Parameter **enabled** auf `false`, um SSH zu deaktivieren oder `true` die SSH-Funktion, die Sie zuvor deaktiviert haben, wieder zu aktivieren.
   c. Wählen Sie **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 dem Management-Node standardmäßig aktiviert.

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}"
```

Sie können den vom API-Befehl verwendeten Träger finden `${TOKEN}`, wenn Sie "Autorisieren". Der Träger `${TOKEN}` ist in der Lockenantwort.

SCHRITTE DER REST API-UI

1. Greifen Sie auf die REST-API-UI für den Management-Node-API-Service zu, indem Sie die Management-Node-IP-Adresse gefolgt von `/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 `mnode-client`ein.
   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. Wählen Sie **Probieren Sie es aus**.
   b. Wählen Sie **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 Storage-Ressourcen für NetApp HCI ausgeschaltet werden, müssen die Storage-Nodes mit der `Shutdown` Element API Methode ordnungsgemäß angehalten werden.

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. Öffnen Sie zum Ausschalten des NetApp HCI Storage-Clusters einen Webbrowser und rufen Sie mithilfe der folgenden URL das Verfahren zum aus- und Ausschalten auf. Dabei `{MVIP}` handelt es sich um die Management-IP-Adresse des NetApp HCI Storage-Systems, und das `nodes=[]` Array enthält die Node-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-Aufruf erfolgreich zurückgegeben wurde, indem Sie überprüfen, ob alle Speicher-Cluster-Nodes im Abschnitt des API-Ergebnisses enthalten sind `successful`.

   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. Vergewissern Sie sich, dass alle kritischen Schweregrade und `volumesOffline` Cluster-Fehler gelöst sind.
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 dann 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"

Überwachen Sie Ihr NetApp HCI System mit NetApp Hybrid Cloud Control

Monitoring von Storage- und Computing-Ressourcen über das Hybrid Cloud Control Dashboard

Die NetApp Hybrid Cloud Control Konsole bietet einen Überblick über alle Storage- und Computing-Ressourcen. Darüber hinaus können Sie die Storage-Kapazität, Storage-Performance und die Computing-Auslastung überwachen.

> Wenn Sie zum ersten Mal eine neue NetApp Hybrid Cloud Control Session starten, kann es möglicherweise zu Verzögerungen beim Laden der NetApp Hybrid Cloud Control Dashboard-Ansicht kommen, wenn der Management-Node viele Cluster verwaltet. Die Ladezeit hängt von der Anzahl der Cluster ab, die aktiv vom Management-Node gemanagt werden. Bei späteren Starts erleben Sie schnellere Ladezeiten.

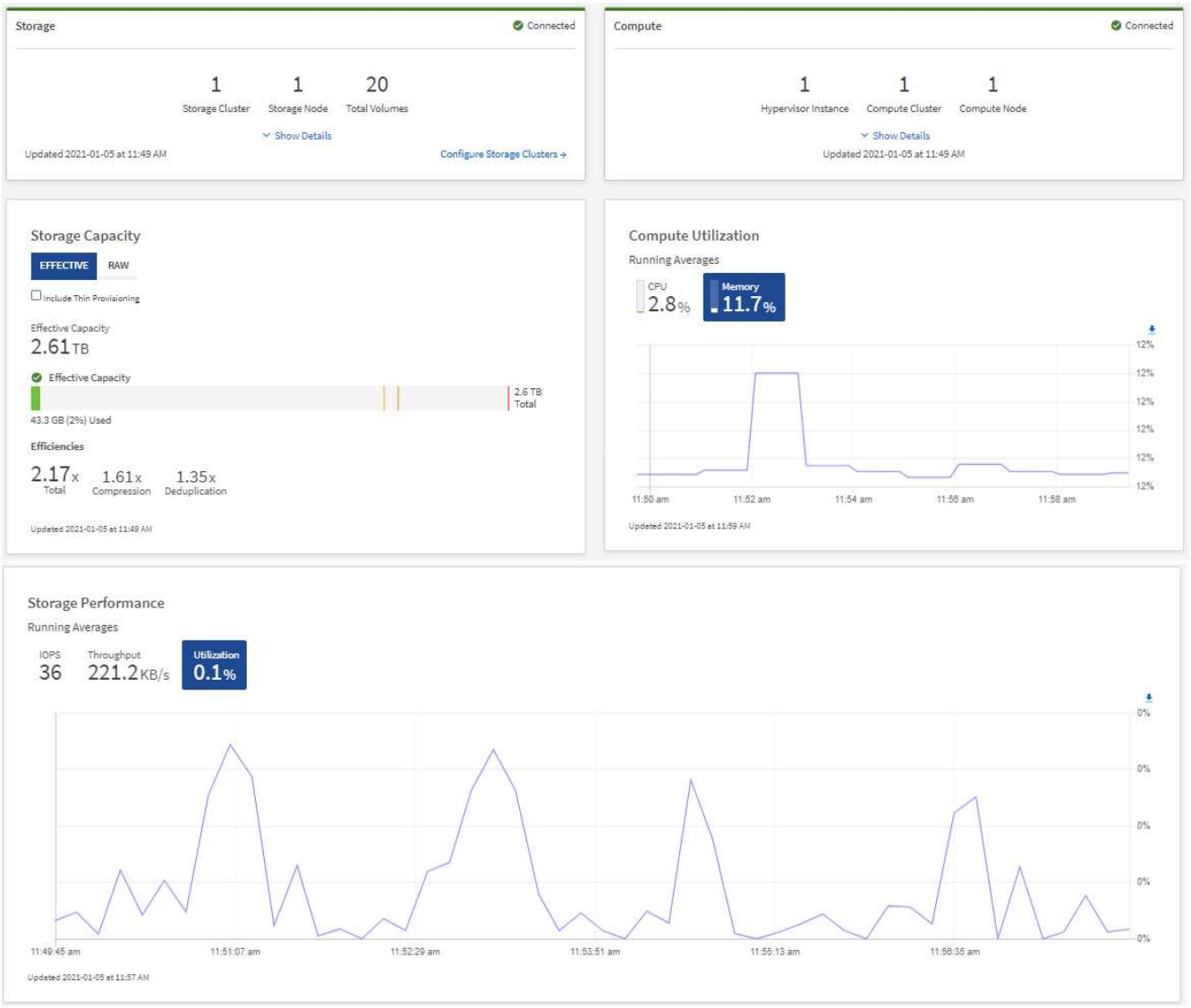
Im Hybrid Cloud Control Dashboard werden nur Compute-Nodes angezeigt, die gemanagt werden und Cluster mit mindestens einem gemanagten Node in H-Series Hardware.

Zugriff auf das NetApp HCC Dashboard

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.
3. Zeigen Sie das Hybrid Cloud Control Dashboard an.

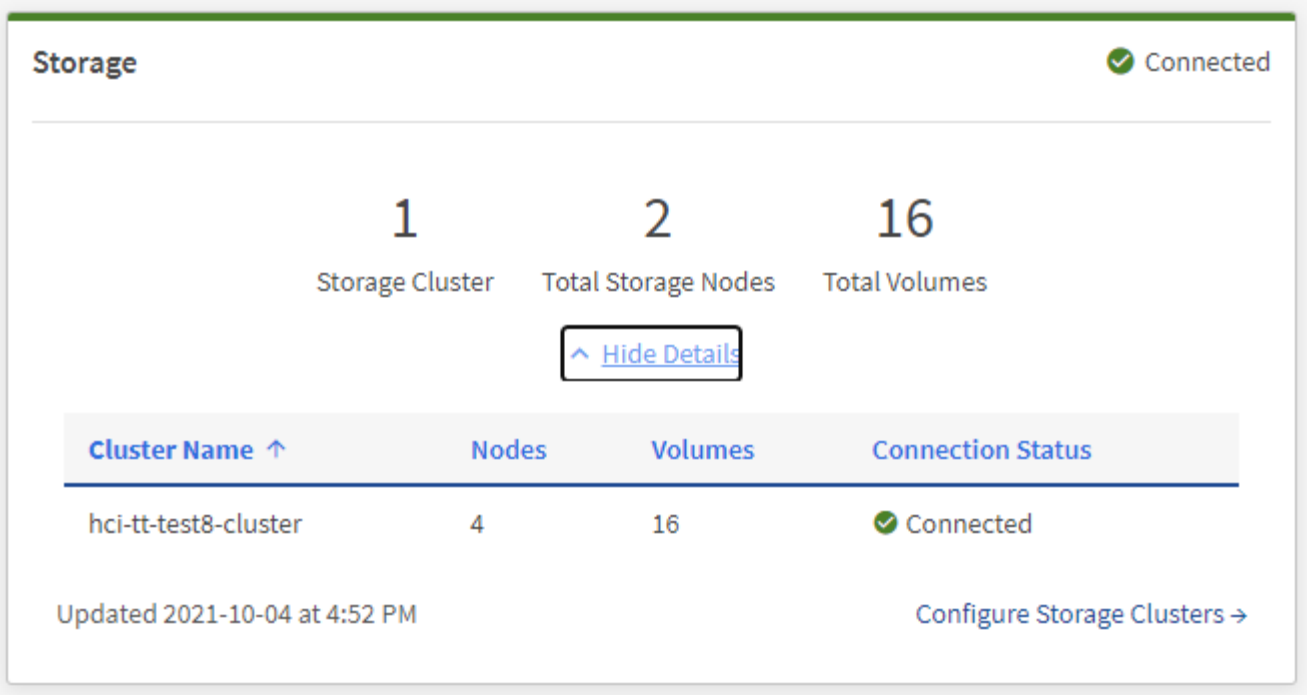


Je nach Ihrer Installation werden möglicherweise einige oder alle diese Teilfenster angezeigt. Beispielsweise werden bei nur für Storage-Installationen im Hybrid Cloud Control Dashboard nur das Teilfenster Storage, das Teilfenster Storage-Kapazität und das Teilfenster Storage-Performance angezeigt.

Monitoring von Storage-Ressourcen

Nutzen Sie den Fensterbereich **Storage**, um Ihre gesamte Speicherumgebung anzuzeigen. Sie können die Anzahl der Storage-Cluster, Storage-Nodes und Volumes insgesamt überwachen.

Um Details anzuzeigen, wählen Sie im Bereich Speicher die Option **Details anzeigen**.



Die Gesamtzahl der Storage-Nodes enthält keine Witness-Nodes aus Storage-Clustern mit zwei Nodes. Die Witness-Nodes sind in die Nummer Nodes im Detailbereich für diesen Cluster enthalten.

Um die letzten Speichercluster-Daten anzuzeigen, verwenden Sie die Seite Speichercluster, auf der Abfragen häufiger durchgeführt werden als auf dem Dashboard.

Monitoring von Computing-Ressourcen

Nutzen Sie die Fensterfläche **Computing**, um Ihre gesamte NetApp H-Series Computing-Umgebung anzuzeigen. Es lässt sich die Anzahl der Computing-Cluster und Computing-Nodes insgesamt überwachen.

Um Details anzuzeigen, wählen Sie in den Rechenfeldern **Details anzeigen** aus.

Ihre vCenter Instanzen werden nur im Computing-Bereich angezeigt, wenn mindestens ein NetApp HCI Computing-Node dieser Instanz zugeordnet ist. Um die vCenter Instanzen aufzulisten, die in NetApp Hybrid Cloud Control verknüpft sind, können Sie die verwenden "APIs".

Zum Managen eines Computing-Node in NetApp Hybrid Cloud Control müssen Sie "Fügen Sie den Computing-Node zu einem vCenter-Host-Cluster hinzu" .

Monitoring der Storage-Kapazität

Das Monitoring der Storage-Kapazität Ihrer Umgebung ist von entscheidender Bedeutung. Mit dem Teilfenster Storage-Kapazität können Sie die Effizienz Ihrer Storage-Kapazität bestimmen, wobei oder ohne aktivierte Komprimierung, Deduplizierung und Thin Provisioning-Funktionen die Effizienz erhöht wird.

Auf der Registerkarte **RAW** sehen Sie den gesamten verfügbaren physischen Speicherplatz in Ihrem Cluster sowie Informationen zum bereitgestellten Speicher auf der Registerkarte **EFFEKTIV**.

Werfen Sie auch einen Blick auf das SolidFire Active IQ Dashboard, um den Cluster-Zustand anzuzeigen. Siehe "Überwachung von Performance, Kapazität und Cluster-Zustand in NetApp SolidFire Active IQ".

Schritte

1. Wählen Sie die Registerkarte * RAW* aus, um den gesamten physischen Speicherplatz anzuzeigen, der in Ihrem Cluster verwendet und verfügbar ist.

   Sehen Sie sich die vertikalen Linien an, um zu bestimmen, ob die genutzte Kapazität unter dem Wert „Warnung“, „Fehler“ oder „kritische Schwellenwerte“ liegt. Bewegen Sie den Mauszeiger über die Linien, um Details anzuzeigen.

   Sie können den Schwellenwert für Warnung festlegen, der standardmäßig 3% unter dem Fehlerschwellenwert liegt. Die Fehler- und kritischen Schwellenwerte sind voreingestellt und können nicht anhand des Designs konfiguriert werden. Der Fehlerschwellenwert gibt an, dass weniger als ein Knoten der Kapazität im Cluster verbleibt. Schritte zum Einstellen des Schwellenwerts finden Sie unter "Cluster-Schwellenwert wird eingestellt".

   Details zu den zugehörigen Cluster-Schwellenwerten Element API finden Sie "„GetClusterFullThreshold“" im *Element API Guide*. Informationen zur Kapazität von Block- und Metadaten finden Sie "Allgemeines zu Cluster-Auslastungsebenen" im *Element User Guide*.

2. Wählen Sie die Registerkarte * EFFECTIVE* aus, um Informationen über den insgesamt bereitgestellten Storage für verbundene Hosts anzuzeigen und Effizienzbewertungen anzuzeigen.
   a. Optional können Sie sich **mit Thin Provisioning** um Thin Provisioning-Effizienzraten im Balkendiagramm für die effektive Kapazität anzuzeigen.
   b. **Balkendiagramm für effektive Kapazität**: Prüfen Sie die vertikalen Linien, um festzustellen, ob Ihre verwendete Kapazität unter der Gesamtsumme oder weniger als Warnung, Fehler oder kritische Schwellenwerte liegt. Ähnlich wie die Registerkarte „Raw“ können Sie den Mauszeiger über die vertikalen Linien bewegen, um Details anzuzeigen.
   c. **Effizienz**: Prüfen Sie diese Bewertungen, um festzustellen, welche Vorteile die Effizienz Ihrer Storage-Kapazität durch aktivierte Komprimierung, Deduplizierung und Thin Provisioning-Funktionen erzielt wird. Wenn die Komprimierung beispielsweise „1,3x“ anzeigt, bedeutet dies, dass die Storage-Effizienz

bei aktivierter Komprimierung 1.3-mal effizienter ist als ohne sie.

> Die Gesamteffizienz entspricht (maxUsedSpace * Efficiency Factor) / 2, wobei Efficiency Factor = (thinProvisioningFactor * deDuplicationFactor * comressionFactor). Wenn Thin Provisioning nicht aktiviert ist, wird dies nicht in der Gesamteffizienz berücksichtigt.

d. Wenn die effektive Storage-Kapazität einen Fehler oder einen kritischen Schwellenwert überschreitet, sollten Sie die Daten auf dem System löschen. Alternativ können Sie auch Ihr System erweitern.

   Siehe "Übersicht über die Erweiterung".

3. Für weitere Analysen und historischen Kontext, siehe "Details zum NetApp SolidFire Active IQ" .

Monitoring der Storage-Performance

Sie können sich ansehen, wie viel IOPS oder Durchsatz Sie aus einem Cluster erhalten können, ohne die nützliche Performance dieser Ressource durch Verwendung des Teilfensters „Storage Performance“ zu überschreiten. Die Storage-Performance ist der Punkt, an dem die maximale Auslastung erreicht wird, bevor die Latenz zum Problem wird.

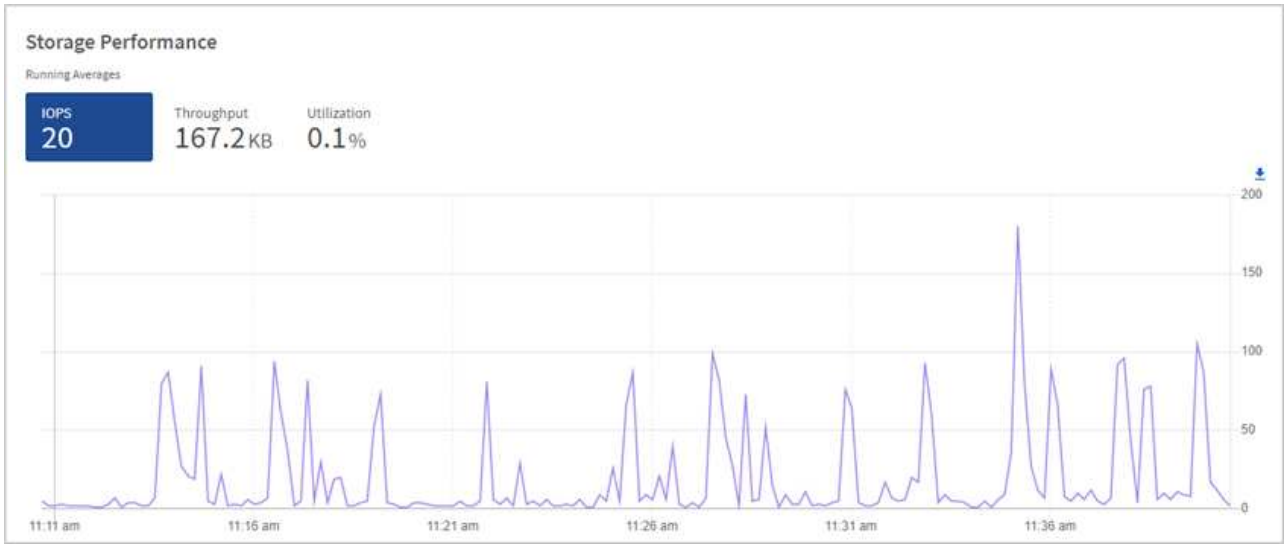
Im Bereich Storage Performance können Sie feststellen, ob die Performance an einem Punkt erreicht wird, an dem die Performance abnimmt, wenn sich die Workloads erhöhen.

Die Informationen in diesem Teilfenster werden alle 10 Sekunden aktualisiert und zeigen einen Durchschnitt aller Punkte im Diagramm an.

Weitere Informationen zur zugehörigen Element API-Methode finden Sie "GetClusterStats" in der Methode im *Element API Reference Guide*.

Schritte

1. Zeigen Sie das Teilfenster Speicher-Performance an. Zeigen Sie für Details den Mauszeiger auf Punkte im Diagramm.
   a. **IOPS** Registerkarte: Siehe die aktuellen Operationen pro Sekunde. Suchen Sie nach Trends in Daten oder Spitzen. Wenn Sie beispielsweise sehen, dass die maximale IOPS 160.000 beträgt und 100.000 freie oder verfügbare IOPS sind, ziehen Sie möglicherweise nach dem Hinzufügen weiterer Workloads zu diesem Cluster in Betracht. Wenn andererseits zu sehen ist, dass nur 140K verfügbar ist, können Sie unter Umständen Workloads auslagern oder Ihr System erweitern.



b. **Throughput** Tab: Monitoring-Muster oder Durchsatzspitzen. Überwachen Sie darüber hinaus kontinuierlich hohe Durchsatzwerte. Dies kann darauf hindeuten, dass sich die maximale Performance der Ressource nähert.

c. **Auslastung** Registerkarte: Überwachen Sie die Auslastung von IOPS in Bezug auf die insgesamt verfügbaren IOPS, die auf der Clusterebene zusammengefasst sind.

2. Werfen Sie weitere Analysen mit dem NetApp Element Plug-in für vCenter Server an die Storage-Performance.

   "Performance, die im NetApp Element Plug-in für vCenter Server dargestellt ist".

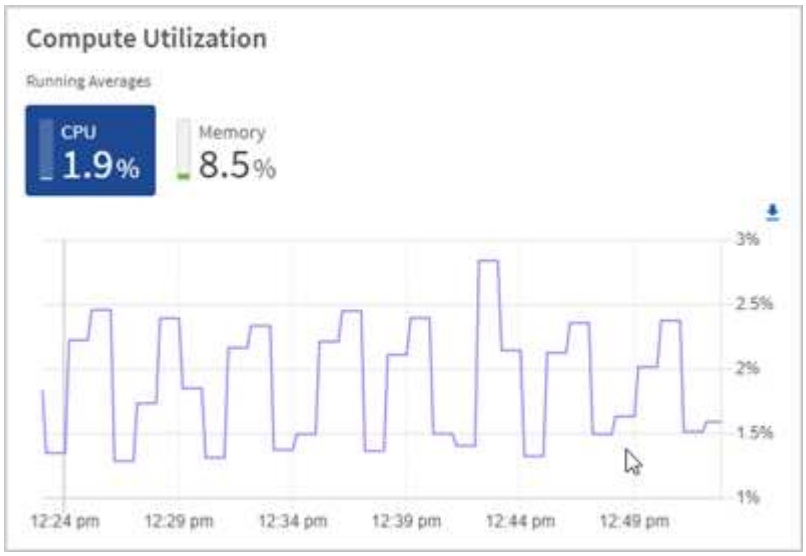
Monitoring der Computing-Auslastung

Neben dem Monitoring der IOPS und des Durchsatzes Ihrer Storage-Ressourcen sollten auch die CPU- und Arbeitsspeicherauslastung der Computing-Ressourcen angezeigt werden. Die gesamten IOPS, die ein Node bereitstellen kann, basieren auf den physischen Merkmalen des Nodes, wie beispielsweise die Anzahl der CPUs, die CPU-Geschwindigkeit und die RAM-Größe.

Schritte

1. Öffnen Sie den Bereich **Computing Utiency**. Wenn Sie sowohl die Registerkarte „CPU“ als auch „Speicher“ verwenden, suchen Sie nach Mustern oder Spitzen in der Auslastung. Achten Sie auch darauf, dass die Auslastung kontinuierlich hoch ist, was darauf hindeutet, dass sich die maximale Auslastung der Computing-Cluster nähert.

   In diesem Teilfenster werden Daten nur für die von dieser Installation gemanagten Computing-Cluster angezeigt.



   a. **CPU** Registerkarte: Siehe den aktuellen Durchschnitt der CPU-Auslastung auf dem Rechner-Cluster.

   b. **Speicher** Registerkarte: Siehe die aktuelle durchschnittliche Speichernutzung auf dem Rechner-Cluster.

2. Für weitere Analysen zu Rechnerinformationen siehe "NetApp SolidFire Active IQ für Archivdaten".

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"
- "NetApp SolidFire Active IQ Dokumentation"

Zeigen Sie Ihren Bestand auf der Seite Knoten an

Sie können Ihre Storage- und Computing-Ressourcen in Ihrem System anzeigen und ihre IP-Adressen, Namen und Softwareversionen festlegen.

Sie können Storage-Informationen für mehrere Node-Systeme und alle NetApp HCI Witness-Nodes anzeigen, die mit zwei oder drei Nodes verbunden sind. Witness Nodes managen das Quorum innerhalb des Clusters. Sie werden nicht für den Storage verwendet. Witness Nodes sind nur für NetApp HCI und nicht für rein Flash-basierte Storage-Umgebungen geeignet.

Weitere Informationen zu Witness Nodes finden Sie unter "Knotendefinitionen".

Bei SolidFire-SDS-Knoten können Sie auf der Registerkarte Speicher den Bestand überwachen.

Schritte

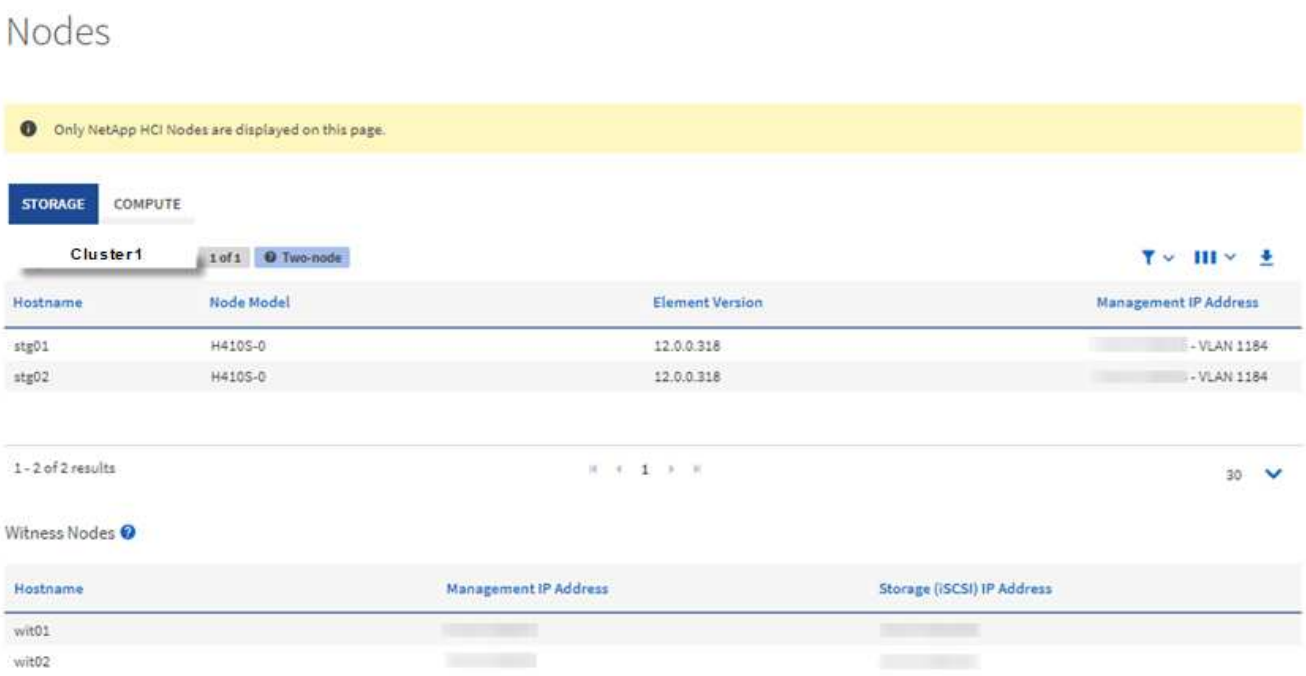
1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser. Beispiel:

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

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

   Das NetApp Hybrid Cloud Control Dashboard wird angezeigt.

3. Wählen Sie in der linken Navigation **Knoten**.



> Wenn Sie zum ersten Mal eine neue NetApp Hybrid Cloud Control Session starten, kann es möglicherweise zu einer Verzögerung beim Laden der Seite NetApp Hybrid Cloud Control Nodes kommen, wenn der Management-Node viele Cluster verwaltet. Die Ladezeit hängt von der Anzahl der Cluster ab, die aktiv vom Management-Node gemanagt werden. Bei späteren Starts erleben Sie schnellere Ladezeiten.

4. Überprüfen Sie auf der Seite Knoten auf der Registerkarte **Storage** die folgenden Informationen:
   a. Zwei-Knoten-Cluster: Auf der Registerkarte Speicher wird eine Bezeichnung „zwei-Knoten“ angezeigt und die zugehörigen Witness Nodes werden aufgelistet.
   b. Drei-Node-Cluster: Die Storage-Nodes und die zugehörigen Witness-Nodes werden aufgeführt. Bei Clustern mit drei Nodes wird ein Witness Node im Standby bereitgestellt, um im Falle eines Node-Ausfalls die Hochverfügbarkeit aufrechtzuerhalten.
   c. Cluster mit mindestens vier Nodes: Es werden Informationen für Cluster mit vier oder mehr Nodes angezeigt. Witness Nodes gelten nicht. Wenn Sie mit zwei oder drei Storage-Nodes begonnen und weitere Nodes hinzugefügt haben, werden die Witness-Nodes weiterhin angezeigt. Andernfalls wird die Tabelle Witness Nodes nicht angezeigt.
   d. Die Firmware-Bundle-Version: Ab Management Services Version 2.14 wird für diese Cluster die Firmware-Bundle-Version angezeigt, wenn auf Clustern mit Element 12.0 oder höher ausgeführt wird.

Wenn die Knoten in einem Cluster unterschiedliche Firmware-Versionen enthalten, sehen Sie in der Spalte **Firmware Bundle Version multiple**.

5. Um Informationen zum Rechnerbestand anzuzeigen, wählen Sie **Compute**.
6. Sie haben verschiedene Möglichkeiten, die Informationen auf diesen Seiten zu bearbeiten:
   a. Um die Liste der Elemente in den Ergebnissen zu filtern, wählen Sie das **Filter**-Symbol und wählen Sie die Filter aus. Sie können auch Text für den Filter eingeben.
   b. Um Spalten ein- oder auszublenden, wählen Sie das Symbol **Spalten anzeigen/ausblenden** aus.
   c. Um die Tabelle herunterzuladen, wählen Sie das Symbol **Download**.
   d. Um die gespeicherten BMC-Anmeldeinformationen für einen Compute-Knoten mit BMC-Verbindungsfehlern hinzuzufügen oder zu bearbeiten, wählen Sie **Verbindungseinstellungen bearbeiten** im Fehlermeldungstext in der Spalte **BMC-Verbindungsstatus** aus. Nur wenn der Verbindungsversuch für einen Compute-Node fehlschlägt, wird in dieser Spalte für diesen Node eine Fehlermeldung angezeigt.

Informationen zur Anzahl der Storage- und Computing-Ressourcen finden Sie im NetApp Hybrid Cloud Control (HCC) Dashboard. Siehe "Überwachen Sie Speicher- und Computing-Ressourcen mit dem HCC Dashboard".

Zum Managen eines Computing-Node in NetApp Hybrid Cloud Control müssen Sie "Fügen Sie den Computing-Node zu einem vCenter-Host-Cluster hinzu" .

Weitere Informationen

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

Verbindungsinformationen für Baseboard Management Controller bearbeiten

Sie können die Zugangsdaten für den Baseboard Management Controller (BMC) Administrator in NetApp Hybrid Cloud Control für jeden Ihrer Computing-Nodes ändern. Vor dem Upgrade der BMC Firmware oder zur Behebung eines oder `Unable to Detect` eines Fehlers, der in NetApp Hybrid Cloud Control angezeigt wird, müssen Sie unter Umständen die Zugangsdaten ändern `Hardware ID not available`.

Was Sie benötigen

Cluster-Administrator-Berechtigungen zum Ändern der BMC-Anmeldedaten.

Wenn Sie BMC-Anmeldedaten während einer Integritätsprüfung festlegen, kann es bis zu 15 Minuten dauern, bis die Änderung auf der Seite **Nodes** angezeigt wird.

Optionen

Wählen Sie eine der folgenden Optionen, um BMC-Anmeldedaten zu ändern:

- um BMC-Informationen zu bearbeiten
- um BMC-Informationen zu bearbeiten

Verwenden Sie NetApp Hybrid Cloud Control, um BMC-Informationen zu bearbeiten

Sie können die gespeicherten BMC-Anmeldedaten über das NetApp Hybrid Cloud Control Dashboard bearbeiten.

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.
3. Wählen Sie im blauen Feld links die NetApp HCI-Installation aus.

   Das NetApp Hybrid Cloud Control Dashboard wird angezeigt.

4. Wählen Sie in der linken Navigation **Knoten**.
5. Um Informationen zum Rechnerbestand anzuzeigen, wählen Sie **Compute**.

   Eine Liste Ihrer Computing-Nodes wird angezeigt. Die Spalte **BMC-Verbindungsstatus** zeigt das Ergebnis der BMC-Verbindungsversuche für jeden Rechner-Knoten an. Wenn der Verbindungsversuch für einen Compute-Node fehlschlägt, wird in dieser Spalte für diesen Node eine Fehlermeldung angezeigt.

6. Um die gespeicherten BMC-Anmeldeinformationen für einen Compute-Knoten mit BMC-Verbindungsfehlern hinzuzufügen oder zu bearbeiten, wählen Sie im Text der Fehlermeldung **Verbindungseinstellungen bearbeiten** aus.
7. Fügen Sie im angezeigten Dialogfeld den korrekten Administrator-Benutzernamen und das Kennwort für den BMC dieses Computing-Knotens hinzu.
8. Wählen Sie **Speichern**.
9. Wiederholen Sie die Schritte 6 bis 8 für alle Rechenknoten, für die keine oder falsche BMC-Anmeldedaten vorhanden sind.

> Durch Aktualisieren der BMC-Informationen wird die Bestandsaufnahme aktualisiert und sichergestellt, dass Management-Node-Services über alle Hardware-Parameter informiert sind, die zum Abschluss des Upgrades erforderlich sind.

VERWENDEN Sie die REST-API, um BMC-Informationen zu bearbeiten

Die gespeicherten BMC-Anmeldedaten können mit der NetApp Hybrid Cloud Control REST-API bearbeitet werden.

Schritte

1. Suchen Sie die Hardware-Tag-Nummer des Computing-Nodes und BMC-Informationen:
   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 `mnode-client`ein.
   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   iv. Schließen Sie das Autorisierungsfenster.
c. Wählen Sie in DER REST API-Benutzeroberfläche **GET /Installations** aus.
d. Wählen Sie **Probieren Sie es aus**.
e. Wählen Sie **Ausführen**.
f. Kopieren Sie aus der Antwort die Installations-Asset(`id`-ID).
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 und speichern Sie aus der Antwort die Knoten Asset id (`id`), BMC IP Adresse (`bmcAddress`) und Node Seriennummer) (`chassisSerialNumber`zur Verwendung in einem späteren Schritt.

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.117.1.111",
      "credentialsAvailable": false,
      "credentialsValidated": false
    },
    "chassisSerialNumber": "221111019323",
    "chassisSlot": "C",
    "hardwareId": null,
    "hardwareTag": "00000000-0000-0000-0000-ac1f6ab4ecf6",
    "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
```

2. Öffnen Sie DIE REST API-UI für den Hardware-Service auf dem Management-Node:

```
https://<ManagementNodeIP>/hardware/2/
```

3. 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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
4. Wählen Sie **PUT /Nodes/{Hardware_id}**.

5. Wählen Sie **Probieren Sie es aus**.
6. Geben Sie die Node-Asset-id ein, die Sie zuvor im Parameter gespeichert `hardware_id` haben.
7. Geben Sie die folgenden Informationen in die Nutzlast ein:

Parameter	Beschreibung
`assetId`	Die Installations-Asset-id(`id`, die Sie in Schritt 1(f) gespeichert haben.
`bmcIp`	Die BMC-IP-Adresse(`bmcAddress`, die Sie in Schritt 1(k) gespeichert haben.
`bmcPassword`	Ein aktualisiertes Passwort zur Anmeldung am BMC.
`bmcUsername`	Ein aktualisierter Benutzername zur Anmeldung am BMC.
`serialNumber`	Die Seriennummer des Chassis der Hardware.

Beispiel für Nutzlast:

```
{
  "assetId": "7bb41e3c-2e9c-2151-b00a-8a9b49c0b0fe",
  "bmcIp": "10.117.1.111",
  "bmcPassword": "mypassword1",
  "bmcUsername": "admin1",
  "serialNumber": "221111019323"
}
```

8. Wählen Sie **Ausführen**, um die BMC-Anmeldeinformationen zu aktualisieren. Ein erfolgreiches Ergebnis liefert eine Antwort ähnlich der folgenden:

```
{
  "credentialid": "33333333-cccc-3333-cccc-333333333333",
  "host_name": "hci-host",
  "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
  "ip": "1.1.1.1",
  "parent": "abcd01y3-ab30-1ccc-11ee-11f123zx7d1b",
  "type": "BMC"
}
```

Weitere Informationen

- "Bekannte Probleme und Behelfslösungen für Computing-Node-Upgrades"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Überwachung von Volumes auf Ihrem Storage-Cluster

Das SolidFire System stellt mithilfe von Volumes Storage bereit. Volumes sind Blockgeräte, auf die über das Netzwerk von iSCSI- oder Fibre Channel-Clients zugegriffen wird. Details zu Zugriffsgruppen, Konten, Initiatoren, genutzter Kapazität, Snapshot Datensicherungsstatus, Anzahl von iSCSI-Sitzungen und der QoS-Richtlinie (Quality of Service) für dieses Volume lassen sich überwachen.

Sie können auch Details zu aktiven und gelöschten Volumes anzeigen.

In dieser Ansicht sollten Sie zunächst die Spalte „verwendete Kapazität“ überwachen.

Sie können nur dann auf diese Informationen zugreifen, wenn Sie über Administratorrechte für NetApp Hybrid Cloud Control verfügen.

Schritte

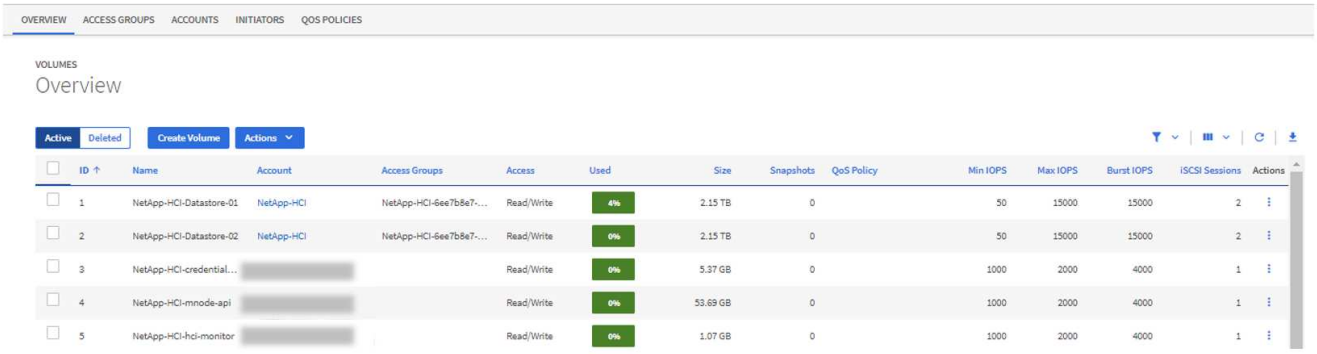
1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser. Beispiel:

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des NetApp HCI-Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie im blauen Feld links die NetApp HCI-Installation aus.

   Das Dashboard für die Hybrid Cloud Control wird angezeigt.

4. Wählen Sie im linken Navigationsbereich den Cluster aus und wählen Sie **Storage** > **Volumes**.



5. Verwenden Sie auf der Seite Volumes die folgenden Optionen:

   a. Filtern Sie die Ergebnisse, indem Sie das Symbol **Filter** wählen.
   b. Durch Auswahl des Symbols **Ausblenden/Anzeigen** können Sie Spalten ausblenden oder anzeigen.
   c. Aktualisieren Sie die Daten, indem Sie das Symbol **Aktualisieren** auswählen.
   d. Laden Sie eine CSV-Datei herunter, indem Sie auf das Symbol **Download** klicken.

6. Überwachen Sie die Spalte „verwendete Kapazität“. Wenn Warnungs-, Fehler- oder kritische Schwellenwerte erreicht werden, steht die Farbe für den Status der verwendeten Kapazität:
   a. Warnung - Gelb
   b. Fehler - Orange
   c. Kritisch – Rot
7. Wählen Sie in der Ansicht Volumes die Registerkarten aus, um weitere Details zu den Volumes anzuzeigen:

   a. **Access Groups**: Sie können die Volume Access Groups sehen, die von Initiatoren einer Sammlung von Volumes für gesicherten Zugriff zugeordnet sind.

      Siehe Informationen über "Volume-Zugriffsgruppen".

   b. **Konten**: Sie können die Benutzerkonten sehen, die es Clients ermöglichen, sich mit Volumes auf einem Knoten zu verbinden. Wenn Sie ein Volume erstellen, wird es einem bestimmten Benutzerkonto zugewiesen.

      Siehe Informationen über "NetApp HCI-Benutzerkonten".

   c. **Initiatoren**: Sie können den iSCSI-Initiator IQN oder Fibre Channel-WWPNs für das Volume sehen. Jeder IQN, der einer Zugriffsgruppe hinzugefügt wird, kann auf jedes Volume in der Gruppe zugreifen, ohne dass eine CHAP-Authentifizierung erforderlich ist. Jeder zu einer Zugriffsgruppe hinzugefügte WWPN ermöglicht den Fibre-Channel-Netzwerkzugriff auf Volumes in der Zugriffsgruppe.

      Weitere Informationen finden "Zugriffsgruppen, Initiatoren und CHAP-Authentifizierungsmethoden" Sie im *NetApp Element-Benutzerhandbuch*.

   d. **QoS-Richtlinien**: Sie sehen die QoS-Richtlinie, die auf das Volume angewendet wird. Eine QoS-Richtlinie wendet standardisierte Einstellungen für IOPS-Minimum, IOPS-Maximum und IOPS-Burst auf mehrere Volumes an.

      Siehe Informationen über "Performance- und QoS-Richtlinien".

   Weitere Informationen finden "Quality of Service-Richtlinien" Sie im *NetApp Element-Benutzerhandbuch*.

Weitere Informationen

- "NetApp SolidFire und Element Documentation Center"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Überwachung von Performance, Kapazität und Cluster-Zustand mit SolidFire Active IQ

Mit SolidFire Active IQ können Sie Ereignisse, Performance und Kapazität der Cluster überwachen. Der Zugriff auf SolidFire Active IQ erfolgt über das NetApp Hybrid Cloud Control Dashboard.

Was Sie brauchen

- Sie benötigen ein NetApp Support-Konto, um diesen Service nutzen zu können.
- Sie müssen für die Verwendung VON REST-APIs für den Management-Node autorisiert sein.
- Sie haben einen Management-Node mit Version 12.0 oder höher implementiert.
- In Ihrer Cluster-Version wird die NetApp Element Software 12.0 oder höher ausgeführt.
- Sie haben Internetzugang. Der Active IQ Collector Service kann nicht von dunklen Seiten verwendet werden.

Über diese Aufgabe erhalten Sie kontinuierlich aktualisierte historische Ansichten von clusterweiten Statistiken. Sie können Benachrichtigungen einrichten, um Sie über angegebene Ereignisse, Schwellenwerte oder Metriken in einem Cluster zu benachrichtigen, damit diese schnell behoben werden können.

Im Rahmen des normalen Support-Vertrags überwacht NetApp Support diese Daten und warnt vor potenziellen Systemproblemen.

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.
3. Wählen Sie im Dashboard oben rechts das Menü aus.
4. Wählen Sie **Active IQ anzeigen**.

   Das "SolidFire Active IQ Dashboard" wird angezeigt.

5. Weitere Informationen zu SolidFire Active IQ finden Sie im "SolidFire Active IQ-Dokumentation".

   Sie können auch über das Dashboard auf die SolidFire Active IQ-Dokumentation zugreifen, indem Sie oben rechts das Menüsymbol auswählen und **Dokumentation** auswählen.

6. Vergewissern Sie sich über die SolidFire Active IQ-Schnittstelle, dass die NetApp HCI Computing- und Storage-Nodes die Telemetrie richtig an Active IQ melden:
   a. Wenn Sie über mehrere NetApp HCI-Installationen verfügen, wählen Sie **Cluster auswählen** aus und wählen Sie den Cluster aus der Liste aus.
   b. Wählen Sie im linken Navigationsbereich **Knoten** aus.
7. Wenn ein Node oder Nodes aus der Liste fehlen, wenden Sie sich an den NetApp Support.

Informationen zur Anzahl der Storage- und Computing-Ressourcen finden Sie im Hybrid Cloud Control (HCC) Dashboard. Siehe "Überwachen Sie Speicher- und Computing-Ressourcen mit dem HCC Dashboard".

Weitere Informationen

- "NetApp SolidFire Active IQ Dokumentation"
- "NetApp Element Plug-in für vCenter Server"

- "Seite „NetApp HCI Ressourcen“"

Sammelt Protokolle für die Fehlerbehebung

Bei Problemen mit der Installation von NetApp HCI oder SolidFire All-Flash-Storage können Sie Protokolle erfassen, die Sie an NetApp Support senden. So erhalten Sie eine Hilfe bei der Diagnose. Kunden können entweder NetApp Hybrid Cloud Control oder DIE REST-API verwenden, um Protokolle auf NetApp HCI oder Element Systemen zu erfassen.

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 die Protokollerfassung

Wählen Sie eine der folgenden Optionen:

- Verwenden Sie NetApp Hybrid Cloud Control zum Erfassen von Protokollen
- VERWENDEN Sie die REST API zum Erfassen von Protokollen

Verwenden Sie NetApp Hybrid Cloud Control zum Erfassen von Protokollen

Der Protokolleinfassungsbereich ist über das NetApp Hybrid Cloud Control Dashboard zugänglich.

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 Storage-Cluster-Administrators für NetApp HCI oder Element bereitstellen.
3. Wählen Sie im Dashboard oben rechts das Menü aus.
4. Wählen Sie **Protokolle Sammeln**.

   Die Seite **Collect Logs** wird angezeigt. Wenn Sie zuvor Protokolle gesammelt haben, können Sie das vorhandene Protokollpaket herunterladen oder eine neue Protokollsammlung starten.

5. Wählen Sie im Dropdown-Menü **Datumsbereich** einen Datumsbereich aus, um festzulegen, welche Daten die Protokolle enthalten sollen.

   Wenn Sie ein benutzerdefiniertes Startdatum angeben, können Sie das Datum auswählen, um den Datumsbereich zu beginnen. Protokolle werden von diesem Datum bis zur aktuellen Zeit gesammelt.

6. Wählen Sie im Abschnitt **Log Collection** die Art der Protokolldateien aus, die das Protokollpaket enthalten soll.

   Bei Storage- und Computing-Protokollen können Sie die Liste der Storage- oder Computing-Nodes erweitern und einzelne Nodes auswählen, um Protokolle von (oder alle Nodes in der Liste) zu erfassen.

7. Wählen Sie **Protokolle sammeln**, um die Protokollsammlung zu starten.

   Die Protokollerfassung wird im Hintergrund ausgeführt, und auf der Seite wird der Fortschritt angezeigt.

   > Abhängig von den gesammelten Protokollen bleibt der Fortschrittsbalken möglicherweise für einige Minuten bei einem bestimmten Prozentsatz oder läuft an einigen Punkten sehr langsam voran.

8. Wählen Sie **Protokolle herunterladen**, um das Protokollpaket herunterzuladen.

   Das Protokollpaket befindet sich in einem komprimierten UNIX .tgz-Dateiformat.

VERWENDEN Sie die REST API zum Erfassen von Protokollen

Sie können REST API verwenden, um NetApp HCI- oder Element-Protokolle zu erfassen.

Schritte

1. Suchen Sie die Storage Cluster ID:
   a. Öffnen Sie die REST-API-UI für den Management-Node:

      ```
      https://<ManagementNodeIP>/logs/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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
2. Protokolle von NetApp HCI oder Element erfassen:
   a. Wählen Sie **POST /Bundle** aus.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Ändern Sie die Werte der folgenden Parameter im Feld **Request Body**, je nachdem, welche Protokolltypen Sie erfassen müssen und für welchen Zeitraum:

Parameter	Typ	Beschreibung
`modifiedSince`	Datumszeichenfolge	Schließen Sie nur Protokolle ein, die nach diesem Datum und dieser Uhrzeit geändert wurden. Der Wert "2020-07-14T20:19:00.000Z" definiert beispielsweise ein Startdatum vom 14. Juli 2020 um 20:19 UTC.
`computeLogs`	Boolesch	Setzen Sie diesen Parameter auf `true`, um Computing-Node-Protokolle einzubeziehen.

Parameter	Typ	Beschreibung
`computeIds`	UUID-Array	Wenn `computeLogs` auf festgelegt ist `true`, füllen Sie diesen Parameter mit den Management-Node-Asset-IDs der Rechenknoten aus, um die Protokollerfassung auf diese spezifischen Rechenknoten zu beschränken. Verwenden Sie den `GET` `https://<ManagementNodeIP>/logs/1/bundle/options` Endpunkt, um alle möglichen Node-IDs anzuzeigen, die Sie verwenden können.
`mnodeLogs`	Boolesch	Setzen Sie diesen Parameter auf `true`, um Management-Node-Protokolle aufzunehmen.
`storageCrashDumps`	Boolesch	Setzen Sie diesen Parameter auf `true`, um Debug-Protokolle beim Absturz des Storage-Node einzubeziehen.
`storageLogs`	Boolesch	Setzen Sie diesen Parameter auf `true`, um Storage-Node-Protokolle einzubeziehen.
`storageNodeIds`	UUID-Array	Wenn `storageLogs` auf festgelegt ist `true`, füllen Sie diesen Parameter mit den Storage-Cluster-Node-IDs aus, um die Protokollsammlung auf diese spezifischen Storage-Nodes zu beschränken. Verwenden Sie den `GET` `https://<ManagementNodeIP>/logs/1/bundle/options` Endpunkt, um alle möglichen Node-IDs anzuzeigen, die Sie verwenden können.

d. Wählen Sie **Ausführen**, um die Protokollerfassung zu starten. Die Antwort sollte eine ähnliche Antwort wie die folgende zurückgeben:

```
{
  "_links": {
    "self": "https://10.1.1.5/logs/1/bundle"
  },
  "taskId": "4157881b-z889-45ce-adb4-92b1843c53ee",
  "taskLink": "https://10.1.1.5/logs/1/bundle"
}
```

3. Überprüfen Sie den Status der Aufgabe zur Protokollerfassung:
   a. Wählen Sie **GET /Bundle** aus.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Wählen Sie **Ausführen** aus, um einen Status der Sammelaufgabe zurückzugeben.
   d. Blättern Sie zum unteren Rand des Antwortkörpers.

      Sie sollten ein Attribut sehen `percentComplete`, das den Fortschritt der Sammlung detailliert beschreibt. Wenn die Sammlung abgeschlossen ist, enthält das `downloadLink` Attribut den vollständigen Download-Link einschließlich des Dateinamens des Protokollpakets.

   e. Kopieren Sie den Dateinamen am Ende des `downloadLink` Attributs.
4. Laden Sie das gesammelte Protokollpaket herunter:
   a. Wählen Sie **GET /Bundle/{filename}**.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Fügen Sie den Dateinamen, den Sie zuvor kopiert haben, in das `filename` Parametertextfeld ein.
   d. Wählen Sie **Ausführen**.

      Nach der Ausführung wird im Bereich Response Body ein Download-Link angezeigt.

   e. Wählen Sie **Datei herunterladen** und speichern Sie die resultierende Datei auf Ihrem Computer.

      Das Protokollpaket befindet sich in einem komprimierten UNIX .tgz-Dateiformat.

Weitere Informationen

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

Aktualisieren Sie Ihr NetApp HCI-System auf Version 1.8

Übersicht der Aktualisierungssequenz

Sie können das NetApp HCI System nach der Implementierung durch das sequenzielle Upgrade aller NetApp HCI Softwarekomponenten weiterhin auf dem neuesten Stand halten.

Zu diesen Komponenten gehören Management-Services, HealthTools, NetApp Hybrid Cloud Control, Element Software, Management-Node, Computing-Firmware, Computing-Treiber, Und das Element Plug-in für vCenter Server.

> Ab dem 2023. November können Sie ein Komponenten-Upgrade nicht mit NetApp Hybrid Cloud Control oder REST API starten, da die (privaten und öffentlichen) Signaturschlüsselzertifikate am 5. November 2023 abgelaufen sind. Sie können dieses Problem beheben, indem Sie die im Knowledge Base-Artikel dokumentierte Problemumgehung befolgen "SolidFire- und HCI-Upgrades können nicht gestartet werden, da Fehler beim Hochladen der Upgradepakete aufgetreten ist".

In den Systemaktualisierungssequenz Inhalten werden die Aufgaben beschrieben, die zum Abschluss eines NetApp HCI System-Upgrades erforderlich sind. Idealerweise führen Sie diese Verfahren als Teil der größeren Upgrade-Sequenz und nicht isoliert durch. Wenn ein komponentenbasiertes Upgrade oder eine Aktualisierung erforderlich ist, lesen Sie die Verfahrensvoraussetzungen, um sicherzustellen, dass zusätzliche Komplexität bewältigt wird.

Im VSphere-Upgrade-SequenzInhalt des Including Element Plug-in for vCenter Server werden zusätzliche Schritte vor und nach dem Upgrade beschrieben, die zur Neuinstallation des Element Plug-ins für vCenter Server erforderlich sind.

Was Sie benötigen

- Sie führen Management-Node 11.3 oder höher aus. Neuere Versionen des Management-Node verfügen über eine modulare Architektur, die individuelle Services zur Verfügung stellt.

  > Um die Version zu überprüfen, melden Sie sich bei Ihrem Management-Node an, und zeigen Sie die Versionsnummer des Elements im Anmeldebanner an. Wenn Sie nicht über 11.3 verfügen, siehe "Upgrade Ihres Management-Node".

- Sie haben ein Upgrade Ihrer Verwaltungsdienste auf mindestens Version 2.1.326 durchgeführt.

  Upgrades mit NetApp Hybrid Cloud Control sind in früheren Service-Bundle-Versionen nicht verfügbar.

- Sie stellen sicher, dass die Systemzeit auf allen Knoten synchronisiert ist und dass NTP für den Speicher-Cluster und die Knoten korrekt konfiguriert ist. Jeder Knoten muss mit einem DNS-Nameserver in der Web-UI pro Knoten konfiguriert werden (`https://[IP address]:442`) ohne ungelöste Clusterfehler im Zusammenhang mit Zeitversatz.

Systemaktualisierungssequenz

Schritte

1. "Aktualisierung der Managementservices von Hybrid Cloud Control".

   Wenn Sie Managementservices auf Version 2.16 oder höher aktualisieren und einen Management-Node 11.3 bis 11.8 ausführen, müssen Sie vor der Aktualisierung der Managementservices den RAM der Management-Node-VM erhöhen.

   Vor einem Upgrade der Element Software müssen Sie das neueste Management-Services-Bundle aktualisieren.

2. "(Optional) Upgrade auf die neuesten HealthTools".

   Ein Upgrade von HealthTools ist nur erforderlich, wenn der Management-Node und die Element-Software, die Sie verwenden, 11.1 oder älter sind. HealthTools sind bei der Durchführung von Element-Upgrades mit NetApp Hybrid Cloud Control nicht erforderlich.

3. "Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen".
4. "Aktualisieren Sie die Element Software und die Storage-Firmware".
5. "(Optional) Aktualisieren Sie nur die Element Storage-Firmware".

   Möglicherweise führen Sie diese Aufgabe aus, wenn außerhalb einer Hauptversion ein neues Speicher-Firmware-Upgrade verfügbar wird.

6. "(Optional) Upgrade Ihres Management-Node".

   Zum Upgrade der Element Software auf dem Storage-Cluster ist kein Upgrade des Betriebssystems des Management-Node mehr erforderlich. Wenn der Management-Node Version 11.3 oder höher ist, können die Managementservices einfach auf die neueste Version aktualisiert werden, um Element-Upgrades mithilfe von NetApp Hybrid Cloud Control durchzuführen. Befolgen Sie für Ihr Szenario die Vorgehensweise zum Upgrade des Management-Node, wenn Sie aus anderen Gründen, wie z. B. Sicherheitsbehebungsmaßnahmen, ein Upgrade des Betriebssystems des Management-Node durchführen möchten.

7. "Aktualisieren Sie Ihr Element Plug-in für vCenter Server".
8. "Vor einem Upgrade der Computing-Firmware müssen Systemzustandsprüfungen für Computing-Nodes durchgeführt werden".
9. "Aktualisieren Sie Ihre Compute-Node-Treiber".
10. "Aktualisieren Sie die Computing-Node-Firmware mit NetApp Hybrid Cloud Control" Oder "Automatisieren Sie Upgrades Ihrer Computing-Firmware mit Ansible".

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"
- "Upgrade eines NetApp SolidFire All-Flash-Storage-Systems"

Verfahren für System-Upgrades

Managementservices aktualisieren

Sie können Ihre Managementservices nach der Installation des Management Node 11.3 oder höher auf die neueste Bundle-Version aktualisieren.

Seit der Version für Element 11.3 Management-Nodes wurde das Design der Management-Nodes auf Grundlage einer neuen modularen Architektur, die individuelle Services bietet, geändert. Diese modularen Services bieten zentrale und erweiterte Management-Funktionalität für NetApp HCI und SolidFire All-Flash-Storage-Systeme. Zu den Managementservices gehören Systemtelemetrie, Protokollierung und Update-Services, der QoSSIOC-Service für das Element Plug-in für vCenter Server, NetApp Hybrid Cloud Control und vieles mehr.

Über diese Aufgabe

- Vor einem Upgrade der Element Software müssen Sie ein Upgrade auf das neueste Management Services Bundle durchführen.

> Aktuelle Versionshinweise zu Management Services, in denen wichtige Services, neue Funktionen, Fehlerbehebungen und Problemumgehungen für die einzelnen Service-Pakete beschrieben werden, finden Sie unter "Die Versionshinweise für Managementservices".

Was Sie benötigen

Ab Management Services 2.20.69 müssen Sie die Endbenutzer-Lizenzvereinbarung (Endbenutzer License Agreement, EULA) akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder -API für Upgrade-Managementservices verwenden:

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 **Upgrade** oben rechts auf der Schnittstelle aus.
4. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Update-Optionen

Die Managementservices können mit der NetApp Hybrid Cloud Control UI oder DER REST-API des Management-Node aktualisiert werden:

- Aktualisieren von Managementservices mit Hybrid Cloud Control (Empfohlene Methode)
- Aktualisieren Sie Managementservices mit der Management-Node-API

Aktualisieren von Managementservices mit Hybrid Cloud Control

Sie können Ihre NetApp Managementservices mit NetApp Hybrid Cloud Control aktualisieren.

Management-Service-Bundles bieten erweiterte Funktionen und Korrekturen an Ihrer Installation außerhalb der

größeren Versionen.

Was Sie benötigen

- Sie führen Management-Node 11.3 oder höher aus.
- Wenn Sie Managementservices auf Version 2.16 oder höher aktualisieren und einen Management-Node 11.3 bis 11.8 ausführen, müssen Sie vor der Aktualisierung der Managementservices den RAM der Management-Node-VM erhöhen:
  a. Schalten Sie die Management-Node-VM aus.
  b. Ändern Sie den RAM der Management-Node-VM von 12 GB in 24 GB RAM.
  c. Schalten Sie die Management-Node-VM ein.
- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben ein Upgrade Ihrer Verwaltungsdienste auf mindestens Version 2.1.326 durchgeführt. Upgrades der NetApp Hybrid Cloud Control sind in früheren Servicepaketen nicht verfügbar.

Eine Liste der verfügbaren Services für jede Service-Bundle-Version finden Sie unter "Versionshinweise Für Management Services".

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 **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite Upgrades die Registerkarte **Management Services** aus.

   Auf der Registerkarte Management Services werden die aktuellen und verfügbaren Versionen der Management Services-Software angezeigt.

   Wenn Ihre Installation nicht auf das Internet zugreifen kann, wird nur die aktuelle Softwareversion angezeigt.

5. Wenn Ihre Installation auf das Internet zugreifen kann und wenn ein Upgrade der Verwaltungsdienste verfügbar ist, wählen Sie **Upgrade beginnen**.
6. Wenn Ihre Installation keinen Zugriff auf das Internet hat, gehen Sie wie folgt vor:

   a. Befolgen Sie die Anweisungen auf der Seite, um ein Upgrade-Paket für Verwaltungsdienste auf Ihrem Computer herunterzuladen und zu speichern.
   b. Wählen Sie **Durchsuchen**, um das gespeicherte Paket zu finden und hochzuladen.

      Nach dem Hochladen des Pakets wird das Upgrade automatisch gestartet.

   Nach Beginn des Upgrades sehen Sie den Aktualisierungsstatus auf dieser Seite. Während des Upgrades besteht unter Umständen keine Verbindung zu NetApp Hybrid Cloud Control und muss sich erneut anmelden, um die Ergebnisse des Upgrades anzuzeigen.

Aktualisieren Sie Managementservices mit der Management-Node-API

Benutzer sollten idealerweise Management-Services-Updates von NetApp Hybrid Cloud Control durchführen. Sie können jedoch ein Service Bundle-Update für Managementservices manuell über die REST-API hochladen, extrahieren und implementieren. Sie können jeden Befehl für den Management-Node von DER REST-API-UI ausführen.

Was Sie benötigen

- Sie haben einen NetApp Element Software-Management-Node 11.3 oder höher implementiert.
- Wenn Sie Managementservices auf Version 2.16 oder höher aktualisieren und einen Management-Node 11.3 bis 11.8 ausführen, müssen Sie vor der Aktualisierung der Managementservices den RAM der Management-Node-VM erhöhen:
  a. Schalten Sie die Management-Node-VM aus.
  b. Ändern Sie den RAM der Management-Node-VM von 12 GB in 24 GB RAM.
  c. Schalten Sie die Management-Node-VM ein.
- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben ein Upgrade Ihrer Verwaltungsdienste auf mindestens Version 2.1.326 durchgeführt. Upgrades der NetApp Hybrid Cloud Control sind in früheren Servicepaketen nicht verfügbar.

> Eine Liste der verfügbaren Services für jede Service-Bundle-Version finden Sie unter "Versionshinweise Für Management Services".

Schritte

1. Öffnen Sie die REST-API-UI auf dem Management-Node: `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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Laden Sie das Service-Bundle auf den Management-Node hoch und extrahieren Sie es mit diesem Befehl: `PUT /services/upload`
4. Bereitstellen der Managementservices auf dem Management-Node: `PUT /services/deploy`
5. Den Status der Aktualisierung überwachen: `GET /services/update/status`

   Ein erfolgreiches Update liefert ein Ergebnis, das dem folgenden Beispiel ähnelt:

```
{
"current_version": "2.10.29",
"details": "Updated to version 2.17.52",
"status": "success"
}
```

Weitere Informationen

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

Upgrade auf die neuesten HealthTools

Bevor Sie mit dem Upgrade des Elements Storage beginnen, sollten Sie Ihre HealthTools Suite aktualisieren. Ein Upgrade von HealthTools ist nur erforderlich, wenn der Management-Node und die Element-Software, die Sie verwenden, 11.1 oder älter sind. HealthTools sind bei der Durchführung von Element-Upgrades mit NetApp Hybrid Cloud Control nicht erforderlich.

Was Sie benötigen

- Sie führen Management Node 11.0, 11.1 oder höher aus.
- Sie haben ein Upgrade Ihrer Verwaltungsdienste auf mindestens Version 2.1.326 durchgeführt.

  Upgrades von NetApp Hybrid Cloud Control sind in früheren Servicepaket-Versionen nicht verfügbar.

- Sie haben die neueste Version von heruntergeladen "HealthTools" und die Installationsdatei auf den Management-Node kopiert.

  Sie können die lokal installierte Version von HealthTools überprüfen, indem Sie den Befehl ausführen `sfupdate-healthtools -v`.

- Um HealthTools mit dunklen Seiten zu verwenden, müssen Sie die folgenden zusätzlichen Schritte ausführen:
  - Laden Sie einen von der NetApp-Support-Website auf einem Computer herunter"JSON-Datei", der nicht der Verwaltungsknoten ist, und benennen Sie ihn in `metadata.json`um.
  - Lassen Sie den Management-Node am dunklen Standort laufen.

Über diese Aufgabe

Für die Befehle in der HealthTools Suite sind eskalierte Berechtigungen erforderlich. Entweder Vorwort-Befehle mit `sudo` oder eskalieren Sie Ihren Benutzer zu root Privileges.

Die von Ihnen verwendete HealthTools-Version ist möglicherweise aktueller als die unten angegebene Beispieleingabe und -Antwort.

Schritte

1. Führen Sie den Befehl aus `sfupdate-healthtools <path to install file>`, um die neue HealthTools-Software zu installieren.

   Beispieleingabe:

   ```
   sfupdate-healthtools /tmp/solidfire-healthtools-2020.03.01.09.tgz
   ```

   Beispielantwort:

```
Checking key signature for file /tmp/solidfirehealthtools-
2020.03.01.09/components.tgz
installing command sfupdate-healthtools
Restarting on version 2020.03.01.09
sfupdate-healthtools /sf/bin/sfupdate-healthtools -r 2020.03.01.09
installing command sfupgradecheck
installing command sfinstall
installing command sfresetupgrade
```

2. Führen Sie den Befehl aus `sfupdate-healthtools -v`, um zu überprüfen, ob die installierte Version aktualisiert wurde.

   Beispielantwort:

```
Currently installed version of HealthTools:
2020.03.01.09
```

Weitere Informationen

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

Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen

Vor dem Upgrade von Element Storage müssen Sie Zustandsprüfungen durchführen, um sicherzustellen, dass alle Storage-Nodes im Cluster für das nächste Element Storage Upgrade bereit sind.

Was Sie benötigen

- **Management Services**: Sie haben das neueste Management Services Bundle (2.10.27 oder höher) aktualisiert.

  Vor einem Upgrade der Element Software müssen Sie ein Upgrade auf das neueste Management Services Bundle durchführen.

- **Management Node**: Sie führen Management Node 11.3 oder höher aus.
- **Element Software**: Ihre Clusterversion wird mit der NetApp Element Software 11.3 oder höher ausgeführt.
- **Endbenutzer-Lizenzvereinbarung (EULA)**: Ab Management Services 2.20.69 müssen Sie die EULA akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder API verwenden, um die Integritätsprüfungen für Element Storage auszuführen:
  a. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

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

c. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.

d. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Optionen zur Zustandsprüfung

Sie können Systemchecks mit der Benutzeroberfläche von NetApp Hybrid Cloud Control (HCC), der HCC API oder der HealthTools Suite durchführen:

- NetApp Hybrid Cloud Control bietet Zustandsüberprüfungen für Element Storage vor Storage-Upgrades (Bevorzugte Methode)
- Nutzen Sie API zur Ausführung von Element Storage-Zustandsprüfungen vor einem Storage-Upgrade
- um vor einem Storage-Upgrade Zustandsprüfungen für Element Storage auszuführen

Weitere Informationen zu den vom Service ausgeführten Storage-Zustandsprüfungen:

- die vom Service durchgeführt werden

NetApp Hybrid Cloud Control bietet Zustandsüberprüfungen für Element Storage vor Storage-Upgrades

Mithilfe von NetApp Hybrid Cloud Control (HCC) können Sie überprüfen, ob ein Storage-Cluster für ein Upgrade bereit ist.

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 **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite **Upgrades** die Registerkarte **Storage** aus.
5. Wählen Sie die Integritätsprüfung für das Cluster aus  , das Sie auf die Upgrade-Bereitschaft prüfen möchten.
6. Wählen Sie auf der Seite **Storage Health Check** die Option **Run Health Check**.
7. Gehen Sie bei Problemen wie folgt vor:

   a. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus.

   b. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus.

   c. Wählen Sie nach der Behebung von Cluster-Problemen die Option **Integritätsprüfung erneut ausführen** aus.

Nachdem die Integritätsprüfung ohne Fehler abgeschlossen wurde, kann das Storage-Cluster aktualisiert

werden. Zum Fortfahren siehe Upgrade des Storage-Nodes"Anweisungen".

Nutzen Sie API zur Ausführung von Element Storage-Zustandsprüfungen vor einem Storage-Upgrade

Mithilfe DER REST-API können Sie überprüfen, ob ein Storage-Cluster aktualisiert werden kann. Bei der Zustandsprüfung werden keine Hindernisse für Upgrades beseitigt, z. B. ausstehende Nodes, Probleme mit Festplattenspeicher und Cluster-Fehler.

Schritte

1. Suchen Sie die Storage Cluster ID:

   a. Öffnen Sie die REST-API-UI für den Management-Node:

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

   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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.

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

      iv. Schließen Sie das Autorisierungsfenster.

   c. Wählen Sie in der REST-API-Benutzeroberfläche `GET /assets` .

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

   e. Wählen Sie **Ausführen**.

   f. Kopieren Sie von der Antwort aus dem `"storage"` Abschnitt des Clusters, den Sie prüfen möchten, ob die `"id"` Upgrade-Bereitschaft vorhanden ist.

   > Verwenden Sie den Wert in diesem Abschnitt nicht `"parent"`, da dies die ID des Management-Node und nicht die ID des Storage-Clusters ist.

   ```
   "config": {},
   "credentialid": "12bbb2b2-f1be-123b-1234-12c3d4bc123e",
   "host_name": "SF_DEMO",
   "id": "12cc3a45-e6e7-8d91-a2bb-0bdb3456b789",
   "ip": "10.123.12.12",
   "parent": "d123ec42-456e-8912-ad3e-4bd56f4a789a",
   "sshcredentialid": null,
   "ssl_certificate": null
   ```

2. Führen Sie Zustandsprüfungen für das Storage Cluster durch:

   a. Öffnen Sie die Storage REST API-UI auf dem Management-Node:

   ```
   https://<ManagementNodeIP>/storage/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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.

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

   iv. Schließen Sie das Autorisierungsfenster.

c. Wählen Sie **POST/Health-Checks**.

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

e. Geben Sie im Feld Parameter die Storage-Cluster-ID ein, die in Schritt 1 erhalten wurde.

```
{
  "config": {},
  "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
}
```

f. Wählen Sie **Ausführen** aus, um eine Integritätsprüfung auf dem angegebenen Speichercluster auszuführen.

   Die Antwort sollte folgendes angeben `initializing`:

```
{
  "_links": {
    "collection": "https://10.117.149.231/storage/1/health-checks",
    "log": "https://10.117.149.231/storage/1/health-checks/358f073f-
896e-4751-ab7b-ccbb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-
896e-4751-ab7b-ccbb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccbb5f61f9fc",
  "state": "initializing",
  "status": null,
  "storageId": "c6d124b2-396a-4417-8a47-df10d647f4ab",
  "taskId": "73f4df64-bda5-42c1-9074-b4e7843dbb77"
}
```

a. Kopieren Sie die `healthCheckID`, die Teil der Antwort ist.

3. Überprüfen Sie die Ergebnisse der Zustandsprüfungen:

   a. Wählen Sie **GET /Health-checks/{healtCheckId}** aus.

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

c. Geben Sie im Feld Parameter die ID für die Integritätsprüfung ein.

d. Wählen Sie **Ausführen**.

e. Blättern Sie zum unteren Rand des Antwortkörpers.

Wenn alle Zustandsprüfungen erfolgreich sind, ähnelt die Rückkehr dem folgenden Beispiel:

```
"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"
```

4. Wenn die `message` Rückgabe darauf hinweist, dass Probleme im Zusammenhang mit dem Clusterstatus aufgetreten sind, führen Sie die folgenden Schritte aus:

a. Wählen Sie **GET /Health-checks/{healtCheckId}/log** aus

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

c. Geben Sie im Feld Parameter die ID für die Integritätsprüfung ein.

d. Wählen Sie **Ausführen**.

e. Überprüfen Sie alle bestimmten Fehler und erhalten Sie die zugehörigen KB-Artikellinks.

f. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus.

g. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus.

h. Nachdem Sie Cluster-Probleme behoben haben, führen Sie wieder **GET /Health-checks /{healtCheckId}/log** aus.

Verwenden Sie HealthTools, um vor einem Storage-Upgrade Zustandsprüfungen für Element Storage auszuführen

Sie können mit dem Befehl überprüfen, ob das Storage-Cluster bereit ist, ein Upgrade `sfupgradecheck` durchzuführen. Mit diesem Befehl werden Informationen, z. B. ausstehende Nodes, Speicherplatz- und Cluster-Fehler, überprüft.

Wenn sich Ihr Management-Node an einem dunklen Standort befindet, muss die Upgrade-Readiness-Prüfung die Datei, die `metadata.json` Sie während heruntergeladen "HealthTools-Upgrades"haben, erfolgreich ausführen.

Über diese Aufgabe

In diesem Verfahren wird beschrieben, wie Sie Upgrade-Checks durchführen, die zu einem der folgenden Ergebnisse führen:

- Der `sfupgradecheck` Befehl wird erfolgreich ausgeführt. Das Cluster ist bereit für ein Upgrade.
- Überprüfungen innerhalb des `sfupgradecheck` Werkzeugs schlagen mit einer Fehlermeldung fehl. Der Cluster ist nicht für ein Upgrade bereit und weitere Schritte sind erforderlich.
- Ihre Upgrade-Prüfung schlägt mit einer Fehlermeldung fehl, dass HealthTools veraltet ist.
- Ihre Upgrade-Prüfung schlägt fehl, da sich Ihr Management-Node an einem dunklen Standort befindet.

Schritte

1. Führen Sie den Befehl aus `sfupgradecheck`:

```
sfupgradecheck -u <cluster-user-name> MVIP
```

> Bei Kennwörtern, die Sonderzeichen enthalten, fügen Sie (`\`vor jedem Sonderzeichen einen umgekehrten Schrägstrich hinzu. Zum Beispiel `mypass!@1` sollte als eingegeben werden `mypass\!\@`.

Beispiel-Eingabebefehl mit Beispielausgabe, bei dem keine Fehler auftreten und Sie bereit für ein Upgrade sind:

```
sfupgradecheck -u admin 10.117.78.244
```

```
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/
SolidFire-Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnecti
vity
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the
management node
Node ID: 1 Upload speed: 90063.90 KBs/sec
Node ID: 3 Upload speed: 106511.44 KBs/sec
Node ID: 2 Upload speed: 85038.75 KBs/sec
```

2. Bei Fehlern sind zusätzliche Maßnahmen erforderlich. Weitere Informationen finden Sie in den folgenden Unterabschnitten.

Das Cluster ist nicht bereit für ein Upgrade

Wenn eine Fehlermeldung zu einer der Zustandsprüfungen angezeigt wird, führen Sie die folgenden Schritte aus:

1. Überprüfen Sie die `sfupgradecheck` Fehlermeldung.

   Beispielantwort:

```
The following tests failed:
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Severity: ERROR
Failed node IDs: 2
Remedy: Remove unneeded files from root drive
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnectivi
ty
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the management node
Node ID: 1 Upload speed: 86518.82 KBs/sec
Node ID: 3 Upload speed: 84112.79 KBs/sec
Node ID: 2 Upload speed: 93498.94 KBs/sec
```

In diesem Beispiel ist der Speicherplatz in Node 1 knapp. Weitere Informationen finden Sie im "Wissensdatenbank" (KB)-Artikel, der in der Fehlermeldung aufgeführt ist.

HealthTools ist veraltet

Wenn eine Fehlermeldung angezeigt wird, dass HealthTools nicht die neueste Version ist, befolgen Sie die folgenden Anweisungen:

1. Überprüfen Sie die Fehlermeldung, und beachten Sie, dass die Upgrade-Prüfung fehlschlägt.

   Beispielantwort:

   ```
   sfupgradecheck failed: HealthTools is out of date:
   installed version: 2018.02.01.200
   latest version: 2020.03.01.09.
   The latest version of the HealthTools can be downloaded from:
   https://mysupport.netapp.com/NOW/cgi-bin/software/
   Or rerun with the -n option
   ```

2. Befolgen Sie die Anweisungen in der Antwort.

Der Management-Node befindet sich an einem dunklen Standort

1. Überprüfen Sie die Meldung, und beachten Sie, dass die Upgrade-Prüfung fehlschlägt:

   Beispielantwort:

   ```
   sfupgradecheck failed: Unable to verify latest available version of
   healthtools.
   ```

2. Laden Sie einen von der NetApp-Support-Website auf einem Computer herunter"JSON-Datei", der nicht der Verwaltungsknoten ist, und benennen Sie ihn in `metadata.json`um.
3. Führen Sie den folgenden Befehl aus:

   ```
   sfupgradecheck -l --metadata=<path-to-metadata-json>
   ```

4. Weitere Informationen finden Sie unter zusätzliche "HealthTools-Upgrades" Informationen zu dunklen Standorten.
5. Überprüfen Sie, ob die HealthTools Suite aktuell ist, indem Sie den folgenden Befehl ausführen:

   ```
   sfupgradecheck -u <cluster-user-name> -p <cluster-password> MVIP
   ```

Storage-Systemprüfungen, die vom Service durchgeführt werden

Bei den Storage-Zustandsprüfungen werden die folgenden Prüfungen pro Cluster durchgeführt.

Prüfen Sie Den Namen	Node/Cluster	Beschreibung
Check_async_Results	Cluster	Überprüft, ob die Anzahl der asynchronen Ergebnisse in der Datenbank unter einer Schwellennummer liegt.
„Check_Cluster_Fehlerbeseitigung“	Cluster	Stellt sicher, dass keine Fehler beim Blockieren von Cluster beim Upgrade auftreten (wie in Element Source definiert)
Check_Upload_Speed	Knoten	Misst die Upload-Geschwindigkeit zwischen dem Storage-Node und dem Management-Node.
Connection_Speed_Check	Knoten	Stellt sicher, dass Nodes mit dem Management-Node verbunden sind, der Upgrade-Pakete bereitstellt, und schätzt die Verbindungsgeschwindigkeit.
Check_Cores	Knoten	Überprüft auf den Kernel Crash Dump und die Core-Dateien auf dem Node. Die Prüfung schlägt bei Abstürzen in einem der letzten Zeit (Schwellenwert 7 Tage) fehl.
Prüfen Sie_root_Disk_space	Knoten	Überprüft, ob das Root-Dateisystem über genügend freien Speicherplatz verfügt, um ein Upgrade durchzuführen.
Überprüfen Sie_var_log_Disk_space	Knoten	Überprüft, ob `/var/log` freier Speicherplatz einen bestimmten prozentualen freien Schwellenwert erreicht. Wenn dies nicht der Fall ist, dreht sich die Prüfung und löscht ältere Protokolle, um unter den Schwellenwert zu fallen. Die Prüfung schlägt fehl, wenn die Erstellung von ausreichend freiem Speicherplatz nicht erfolgreich ist.
Prüfung_ausstehend_Knoten	Cluster	Stellt sicher, dass keine ausstehenden Nodes im Cluster vorhanden sind.

Weitere Informationen

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

Upgrade der Element Software

Für ein Upgrade der NetApp Element Software können Sie die NetApp Hybrid Cloud

Control UI, DIE REST-API oder die HealthTools Suite verwenden. Bestimmte Vorgänge werden bei einem Upgrade der Element Software unterdrückt, z. B. beim Hinzufügen und Entfernen von Nodes, beim Hinzufügen und Entfernen von Laufwerken sowie Befehle, die unter anderem mit Initiatoren, Volume-Zugriffsgruppen und virtuellen Netzwerken verbunden sind.

Was Sie benötigen

- **Administratorrechte**: Sie haben Berechtigungen für den Storage Cluster Administrator, um das Upgrade durchzuführen.
- **Gültiger Upgrade-Pfad**: Sie haben die Upgrade-Pfad-Informationen für die Element-Version, auf die Sie aktualisieren, überprüft und überprüft, ob der Upgrade-Pfad gültig ist. "NetApp KB: Upgrade-Matrix für Storage-Cluster mit NetApp Element Software (Anmeldung erforderlich)"
- **System Time SYNC**: Sie haben sichergestellt, dass die Systemzeit auf allen Knoten synchronisiert ist und NTP für den Speicher-Cluster und die Knoten korrekt konfiguriert ist. Jeder Knoten muss mit einem DNS-Nameserver in der Web-UI pro Knoten konfiguriert werden (`https://[IP address]:442`) ohne ungelöste Clusterfehler im Zusammenhang mit Zeitversatz.
- **System-Ports**: Bei Upgrade-Nutzung von NetApp Hybrid Cloud Control haben Sie sichergestellt, dass die erforderlichen Ports geöffnet sind. Weitere Informationen finden Sie unter "Netzwerkports" .
- **Management-Node**: Für NetApp Hybrid Cloud Control UI und API wird der Management-Node in Ihrer Umgebung mit Version 11.3 ausgeführt.
- **Management Services**: Sie haben Ihr Management Services Bundle auf die neueste Version aktualisiert.

> Sie müssen ein Upgrade auf das neueste Management Services Bundle durchführen, bevor Sie Ihre Element Software auf Version 12 aktualisieren. Wenn Sie Ihre Element Software auf Version 12.2 aktualisieren, benötigen Sie zum Fortfahren Managementservices 2.14.60 oder höher.

- **Cluster Health**: Sie haben überprüft, dass der Cluster bereit ist, aktualisiert zu werden. Siehe "Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen".
- **BMC für H610S-Knoten aktualisiert**: Sie haben die BMC-Version für Ihre H610S-Knoten aktualisiert. Siehe "Versionshinweise und Upgrade-Anweisungen".
- **Endbenutzer-Lizenzvereinbarung (EULA)**: Ab Management Services 2.20.69 müssen Sie die EULA akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder API zum Upgrade von Element Software verwenden:
  a. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

  b. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
  c. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
  d. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Upgrade-Optionen

Wählen Sie eine der folgenden Upgrade-Optionen für Element Software:

- Nutzen Sie die NetApp Hybrid Cloud Control UI für das Upgrade von Element Storage
- Nutzen Sie die NetApp Hybrid Cloud Control API für das Upgrade von Element Storage
- Aktualisieren der Element-Software an angeschlossenen Standorten mithilfe von HealthTools
- Aktualisieren der Element-Software an dunklen Standorten mithilfe von HealthTools

Wenn Sie einen Knoten der H610S-Serie auf Element 12.2 aktualisieren und auf dem Knoten eine Version von Element vor 11.8 ausgeführt wird, müssen Sie für jeden Speicher-Node weitere Upgrade-Schritte () durchführenPhase 2. Wenn Sie Element 11.8 oder höher ausführen, sind die zusätzlichen Aktualisierungsschritte (Phase 2) nicht erforderlich.

Nutzen Sie die NetApp Hybrid Cloud Control UI für das Upgrade von Element Storage

Über die Benutzeroberfläche von NetApp Hybrid Cloud Control können Sie ein Storage-Cluster-Upgrade durchführen.

Potenzielle Probleme beim Upgrade von Storage-Clustern mit NetApp Hybrid Cloud Control und ihren Behelfslösungen finden Sie im "KB-Artikel".

Der Upgrade-Vorgang dauert etwa 30 Minuten pro Node bei nicht-H610S Plattformen.

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 **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite **Upgrades** die Option **Speicherung**.

   Auf der Registerkarte **Storage** werden die Speichercluster aufgelistet, die Teil Ihrer Installation sind. Wenn durch NetApp Hybrid Cloud Control auf ein Cluster zugegriffen werden kann, wird es nicht auf der Seite **Upgrades** angezeigt.

5. Wählen Sie eine der folgenden Optionen aus und führen Sie die für das Cluster zutreffenden Schritte aus:

Option	Schritte
Alle Cluster laufen mit Element 11.8 und höher	a. Wählen Sie **Durchsuchen**, um das heruntergeladene Aktualisierungspaket hochzuladen. b. Warten Sie, bis der Upload abgeschlossen ist. In einer Statusleiste wird der Status des Uploads angezeigt.  Der Datei-Upload geht verloren, wenn Sie vom Browser-Fenster wegnavigieren. Nach dem erfolgreichen Hochladen und Validierungen der Datei wird eine Meldung auf dem Bildschirm angezeigt. Die Validierung kann mehrere Minuten in Anspruch nehmen. Wenn Sie zu diesem Zeitpunkt vom Browser-Fenster weg navigieren, bleibt der Datei-Upload erhalten. c. Wählen Sie **Upgrade Starten**.  Der **Upgrade-Status** ändert sich während des Upgrades, um den Status des Prozesses anzuzeigen. Es ändert sich auch in Reaktion auf Aktionen, die Sie ergreifen, z. B. die Unterbrechung des Upgrades oder wenn das Upgrade einen Fehler zurückgibt. Siehe Statusänderungen des Upgrades.  Während das Upgrade läuft, können Sie die Seite verlassen und zu einem späteren Zeitpunkt zurückkehren, um den Fortschritt zu überwachen. Die Seite aktualisiert den Status und die aktuelle Version nicht dynamisch, wenn die Cluster-Zeile ausgeblendet ist. Die Cluster-Zeile muss erweitert werden, um die Tabelle zu aktualisieren, oder Sie können die Seite aktualisieren. Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist.

Option	Schritte
Sie aktualisieren ein H610S Cluster mit Element Version vor 11.8.	a. Wählen Sie den Dropdown-Pfeil neben dem Cluster aus, das Sie aktualisieren möchten, und wählen Sie aus den verfügbaren Upgrade-Versionen aus. b. Wählen Sie **Upgrade Starten**. Nach Abschluss des Upgrades werden Sie von der Benutzeroberfläche aufgefordert, Phase 2 des Prozesses auszuführen. c. Führen Sie die erforderlichen zusätzlichen Schritte (Phase 2) im aus "KB-Artikel", und bestätigen Sie in der Benutzeroberfläche, dass Sie Phase 2 abgeschlossen haben. Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist. Informationen zu den verschiedenen Änderungen des Upgrade-Status finden Sie unter Statusänderungen des Upgrades.

Statusänderungen des Upgrades

Hier sind die verschiedenen Status, in denen die Spalte **Upgrade Status** in der UI vor, während und nach dem Upgrade-Prozess angezeigt wird:

Upgrade-Status	Beschreibung
Auf dem aktuellen Stand	Der Cluster wurde auf die aktuellste verfügbare Element Version aktualisiert.
Verfügbare Versionen	Neuere Versionen von Element und/oder Storage Firmware stehen für ein Upgrade zur Verfügung.
In Bearbeitung	Das Upgrade läuft. In einer Statusleiste wird der Aktualisierungsstatus angezeigt. Auf dem Bildschirm werden zudem Fehler auf Node-Ebene angezeigt und die Node-ID jedes Node im Cluster wird angezeigt, wenn das Upgrade fortschreitet. Sie können den Status jedes Knotens über die Element-UI oder das NetApp Element Plug-in für vCenter Server UI überwachen.
Anhalten Des Upgrades	Sie können das Upgrade anhalten. Je nach Status des Upgrade-Prozesses kann der Pause-Vorgang erfolgreich oder fehlgeschlagen sein. Es wird eine UI-Eingabeaufforderung angezeigt, in der Sie aufgefordert werden, den Pause-Vorgang zu bestätigen. Um sicherzustellen, dass sich das Cluster vor dem Anhalten eines Upgrades an einem sicheren Ort befindet, kann es bis zu zwei Stunden dauern, bis der Upgrade-Vorgang vollständig angehalten ist. Um das Upgrade fortzusetzen, wählen Sie **Fortsetzen**.

Upgrade-Status	Beschreibung
Angehalten	Sie haben das Upgrade angehalten. Wählen Sie **Fortsetzen**, um den Prozess fortzusetzen.
Fehler	Während des Upgrades ist ein Fehler aufgetreten. Sie können das Fehlerprotokoll herunterladen und an den NetApp Support senden. Nachdem Sie den Fehler behoben haben, können Sie zur Seite zurückkehren und **Fortsetzen** wählen. Wenn Sie das Upgrade fortsetzen, geht die Statusleiste einige Minuten lang zurück, während das System die Zustandsprüfung ausführt und den aktuellen Status des Upgrades überprüft.
Füllen Sie das Follow-up aus	Nur für H610S Nodes, die ein Upgrade von Element Version vor 11.8 durchführen. Nachdem Phase 1 des Aktualisierungsprozesses abgeschlossen ist, werden Sie in diesem Zustand aufgefordert, Phase 2 des Upgrades durchzuführen (siehe "KB-Artikel"). Nachdem Sie Phase 2 abgeschlossen und bestätigt haben, dass Sie den Vorgang abgeschlossen haben, ändert sich der Status auf **bis Datum**.

Nutzen Sie die NetApp Hybrid Cloud Control API für das Upgrade von Element Storage

Mit APIs können Storage-Nodes in einem Cluster auf die neueste Element Softwareversion aktualisiert werden. Sie können ein Automatisierungstool Ihrer Wahl zum Ausführen der APIs verwenden. Der hier dokumentierte API-Workflow nutzt die REST-API-UI, die am Management-Node verfügbar ist.

Schritte

1. Laden Sie das Storage-Upgrade-Paket auf ein Gerät herunter, auf das der Management-Node zugreifen kann. Laden Sie in der NetApp HCI Software "download-Seite" das neueste Storage-Node-Image herunter.
2. Laden Sie das Storage-Upgrade-Paket auf den Management-Node hoch:
   a. Öffnen Sie die REST-API-UI für den Management-Node:

      ```
      https://<ManagementNodeIP>/package-repository/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 `mnode-client`ein.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Autorisierungsfenster.
   c. Wählen Sie in DER REST API-Benutzeroberfläche **POST /Packages** aus.
   d. Wählen Sie **Probieren Sie es aus**.
   e. Wählen Sie **Durchsuchen** und wählen Sie das Aktualisierungspaket aus.
   f. Wählen Sie **Ausführen**, um den Upload zu initiieren.
   g. Kopieren Sie aus der Antwort die Paket-ID (`"id"`) und speichern Sie sie zur Verwendung in einem

späteren Schritt.

3. Überprüfen Sie den Status des Uploads.
   a. Wählen Sie in DER REST-API-Benutzeroberfläche **GET /packages/{id}/Status** aus.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Geben Sie die Paket-ID ein, die Sie im vorherigen Schritt in **id** kopiert haben.
   d. Wählen Sie **Ausführen**, um die Statusanforderung zu initiieren.

      Die Antwort zeigt an `state` `SUCCESS`, dass der Vorgang abgeschlossen ist.

4. Suchen Sie die Storage Cluster ID:
   a. Öffnen Sie die REST-API-UI für den Management-Node:

      ```
      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 `mnode-client`ein.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Autorisierungsfenster.
   c. Wählen Sie in DER REST API-Benutzeroberfläche **GET /Installations** aus.
   d. Wählen Sie **Probieren Sie es aus**.
   e. Wählen Sie **Ausführen**.
   f. Kopieren Sie aus der Antwort die Installations-Asset(`"id"`-ID).
   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 in der Antwort die Speicher-Cluster-ID (`"id"`) des Clusters, den Sie aktualisieren möchten, und speichern Sie sie für einen späteren Schritt.

5. Führen Sie das Storage-Upgrade aus:
   a. Öffnen Sie die Storage REST API-UI auf dem Management-Node:

      ```
      https://<ManagementNodeIP>/storage/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 `mnode-client`ein.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

iv. Schließen Sie das Autorisierungsfenster.

c. Wählen Sie **POST/Upgrades**.

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

e. Geben Sie die Paket-ID des Upgrades in das Feld Parameter ein.

f. Geben Sie im Parameterfeld die Storage-Cluster-ID ein.

Die Nutzlast sollte wie im folgenden Beispiel aussehen:

```
{
  "config": {},
  "packageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4",
  "storageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4"
}
```

g. Wählen Sie **Ausführen**, um das Upgrade zu initiieren.

Die Antwort sollte den Zustand wiefolgt anzeigen `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055`-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
```

```
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",
        "description": "string",
        "remedy": "string",
        "severity": "string",
        "data": {},
        "nodeID": 0
      }
    ]
  },
  "taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
  "dateCompleted": "2020-04-21T22:10:57.057Z",
  "dateCreated": "2020-04-21T22:10:57.057Z"
}
```

a. Kopieren Sie die Upgrade-ID (`"upgradeId"`), die Teil der Antwort ist.

6. Überprüfen Sie den Aktualisierungsfortschritt und die Ergebnisse:

   a. Wählen Sie **GET /Upgrades/{upgradeId}** aus.

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

   c. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein.

   d. Wählen Sie **Ausführen**.

   e. Führen Sie einen der folgenden Schritte aus, wenn während des Upgrades Probleme oder besondere Anforderungen auftreten:

Option	Schritte
Sie müssen Probleme mit dem Clusterzustand aufgrund einer Meldung im Antworttext beheben `failedHealthChecks`.	i. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus. ii. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus. iii. Nachdem Sie Clusterprobleme behoben haben, authentifizieren Sie sich bei Bedarf erneut und wählen Sie **PUT /Upgrades/{UpgradeId}** aus. iv. Wählen Sie **Probieren Sie es aus**. v. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. vi. Geben Sie den Anforderungskörper ein `"action":"resume"`. `{ "action": "resume" }` vii. Wählen Sie **Ausführen**.
Sie müssen das Upgrade unterbrechen, da das Wartungsfenster geschlossen wird oder aus einem anderen Grund.	i. Bei Bedarf erneut authentifizieren und **PUT /Upgrades/{UpgradeId}** auswählen. ii. Wählen Sie **Probieren Sie es aus**. iii. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. iv. Geben Sie den Anforderungskörper ein `"action":"pause"`. `{ "action": "pause" }` v. Wählen Sie **Ausführen**.

Option	Schritte
Wenn Sie ein Upgrade für einen H610S Cluster durchführen, auf dem eine Element-Version vor 11.8 ausgeführt wird, wird der Status im Antworttext angezeigt `finishedNeedsAck`. Für jeden H610S Storage-Node müssen Sie zusätzliche Upgrade-Schritte (Phase 2) durchführen.	i. Siehe [Upgrading H610S storage nodes to Element 12.2 or later (phase 2)] und schließen Sie den Prozess für jeden Node ab. ii. Bei Bedarf erneut authentifizieren und **PUT /Upgrades/{UpgradeId}** auswählen. iii. Wählen Sie **Probieren Sie es aus**. iv. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. v. Geben Sie den Anforderungskörper ein `"action":"acknowledge"`. `{ "action": "acknowledge" }` vi. Wählen Sie **Ausführen**.

f. Führen Sie die **GET /Upgrades/{upgradeId}** API nach Bedarf mehrmals aus, bis der Prozess abgeschlossen ist.

   Während der Aktualisierung zeigt das `status` an `running`, ob keine Fehler aufgetreten sind. Wenn jeder Knoten aktualisiert wird, ändert sich der `step` Wert in `NodeFinished`.

Das Upgrade wurde erfolgreich abgeschlossen, wenn der `percent` Wert lautet `100` und der `state` angezeigt `finished`wird.

Was geschieht bei einem Upgrade mit NetApp Hybrid Cloud Control

Wenn während eines Upgrades ein Laufwerk oder ein Node ausfällt, zeigt die Element-UI Clusterfehler an. Der Upgrade-Prozess setzt nicht auf den nächsten Node fort und wartet auf die Behebung der Cluster-Fehler. Die Fortschrittsleiste in der UI zeigt an, dass das Upgrade auf die Behebung der Cluster-Fehler wartet. In dieser Phase funktioniert die Auswahl von **Pause** in der Benutzeroberfläche nicht, da das Upgrade wartet, bis der Cluster wieder gesund ist. Sie müssen NetApp Support beauftragen, die Fehleruntersuchung zu unterstützen.

NetApp Hybrid Cloud Control verfügt über eine festgelegte Wartezeit von drei Stunden. In diesem Fall kann es zu einem der folgenden Szenarien kommen:

- Die Behebung von Clusterfehlern erfolgt innerhalb des dreistündigen Zeitfensters und das Upgrade wird fortgesetzt. Sie müssen in diesem Szenario keine Maßnahmen ergreifen.
- Das Problem besteht nach drei Stunden weiter, und der Aktualisierungsstatus zeigt **Fehler** mit einem roten Banner an. Sie können das Upgrade fortsetzen, indem Sie nach der Behebung des Problems **Fortsetzen** auswählen.
- Der NetApp Support hat festgestellt, dass das Upgrade vorübergehend abgebrochen werden muss, damit Korrekturmaßnahmen vor dem dreistündigen Fenster durchgeführt werden können. Der Support verwendet die API, um das Upgrade abzubrechen.

Wenn das Cluster-Upgrade abgebrochen wird, während ein Node aktualisiert wird, kann dies dazu führen, dass die Laufwerke nicht ordnungsgemäß vom Node entfernt werden. Wenn die Laufwerke unnormal entfernt werden, muss das Hinzufügen der Laufwerke während eines Upgrades manuell durch den NetApp Support erfolgen. Der Node kann länger dauern, um Firmware-Updates durchzuführen oder Aktivitäten zur Synchronisierung nach dem Update durchzuführen. Wenn der Upgrade-Fortschritt blockiert wird, wenden Sie sich an den NetApp Support.

Aktualisieren der Element-Software an angeschlossenen Standorten mithilfe von HealthTools

Schritte

1. Laden Sie das Storage-Upgrade-Paket herunter. Wechseln Sie zur NetApp HCI Software "download-Seite" und laden Sie das neueste Storage-Node-Image auf ein Gerät herunter, das nicht der Management-Node ist.

   Für ein Upgrade der Element Storage-Software ist die neueste Version von HealthTools erforderlich.

2. Kopieren Sie die ISO-Datei auf den Management-Node an einem zugänglichen Speicherort wie /tmp.

   Wenn Sie die ISO-Datei hochladen, stellen Sie sicher, dass sich der Name der Datei nicht ändert, da andernfalls spätere Schritte fehlschlagen.

3. **Optional**: Laden Sie die ISO vom Management-Knoten auf die Cluster-Knoten vor dem Upgrade herunter.

   Dieser Schritt reduziert die Upgrade-Zeit, indem die ISO vor dem Staging der Storage-Nodes vor dem Ausführen weiterer interner Prüfungen durchgeführt wird, um sicherzustellen, dass das Cluster sich in einem guten Zustand befindet, das aktualisiert werden muss. Durch diesen Vorgang wird das Cluster nicht in den „Upgrade“-Modus versetzt oder es werden keine Cluster-Vorgänge eingeschränkt.

   ```
   sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO> --stage
   ```

   Lassen Sie das Passwort in der Befehlszeile aus, damit Sie zur Eingabe der Informationen aufgefordert werden können `sfinstall`. Bei Kennwörtern, die Sonderzeichen enthalten, fügen Sie (`\`vor jedem Sonderzeichen einen umgekehrten Schrägstrich hinzu. Zum Beispiel `mypass!@1` sollte als eingegeben werden `mypass\!\@`.

   Beispiel Siehe folgenden Beispieleingang:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfisodium-11.0.0.345.iso
   --stage
   ```

   Die Ausgabe für das Beispiel zeigt, dass `sfinstall` versucht zu überprüfen, ob eine neuere Version von `sfinstall` verfügbar ist:

```
sfinstall 10.117.0.244 -u admin
/tmp/solidfire-rtfisodium-11.0.0.345.iso 2018-10-01 16:52:15:
Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https:// mysupport.netapp.com/NOW/cgi-bin/software/
or rerun with --skip-version-check
```

Im folgenden Beispielauszug aus einer erfolgreichen Vorphase:

Nach Abschluss des Staging wird die Meldung nach dem Upgrade-Ereignis angezeigt `Storage Node Upgrade Staging Successful.`

```
flabv0004 ~ # sfinstall -u admin
10.117.0.87 solidfire-rtfi-sodium-patch3-11.3.0.14171.iso --stage
2019-04-03 13:19:58: sfinstall Release Version: 2019.01.01.49 Management
Node Platform:
Ember Revision: 26b042c3e15a Build date: 2019-03-12 18:45
2019-04-03 13:19:58: Checking connectivity to MVIP 10.117.0.87
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.86
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.87
...
2019-04-03 13:19:58: Successfully connected to cluster and all nodes
...
2019-04-03 13:20:00: Do you want to continue? ['Yes', 'No']: Yes
...
2019-04-03 13:20:55: Staging install pack on cluster nodes
2019-04-03 13:20:55: newVersion: 11.3.0.14171
2019-04-03 13:21:01: nodeToStage: nlabp2814, nlabp2815, nlabp2816,
nlabp2813
2019-04-03 13:21:02: Staging Node nlabp2815 mip=[10.117.0.87] nodeID=[2]
(1 of 4 nodes)
2019-04-03 13:21:02: Node Upgrade serving image at
http://10.117.0.204/rtfi/solidfire-rtfisodium-
patch3-11.3.0.14171/filesystem.squashfs
...
2019-04-03 13:25:40: Staging finished. Repeat the upgrade command
without the --stage option to start the upgrade.
```

Die gestaffelte ISOs werden nach Abschluss des Upgrades automatisch gelöscht. Wenn das Upgrade jedoch nicht gestartet wurde und neu erstellt werden muss, können ISOs mithilfe des Befehls manuell destuliert werden:

```
sfinstall <MVIP> -u <cluster_username> --destage
```

Nach dem Start des Upgrades steht die Option Absetzen nicht mehr zur Verfügung.

4. Starten Sie das Upgrade mit dem `sfinstall` Befehl und dem Pfad zur ISO-Datei:

   `sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO>`

   Beispiel

   Der folgende Beispiel-Eingabebefehl kann abgerufen werden:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
   11.0.0.345.iso
   ```

   Die Ausgabe für das Beispiel zeigt, dass `sfinstall` versucht zu überprüfen, ob eine neuere Version von `sfinstall` verfügbar ist:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
   11.0.0.345.iso
   2018-10-01 16:52:15: Newer version of sfinstall available.
   This version: 2018.09.01.130, latest version: 2018.06.05.901.
   The latest version of the HealthTools can be downloaded from:
   https://mysupport.netapp.com/NOW/cgi-bin/software/ or rerun with --skip
   -version-check
   ```

   Im folgenden Beispiel ist ein Auszug aus einem erfolgreichen Upgrade zu sehen. Mit Upgrade-Ereignissen können Sie den Fortschritt des Upgrades überwachen.

   ```
   # sfinstall 10.117.0.161 -u admin solidfire-rtfi-sodium-11.0.0.761.iso
   2018-10-11 18:28
   Checking connectivity to MVIP 10.117.0.161
   Checking connectivity to node 10.117.0.23
   Checking connectivity to node 10.117.0.24
   ...
   Successfully connected to cluster and all nodes
   ################################################################
   You are about to start a new upgrade
   10.117.0.161
   10.3.0.161
   solidfire-rtfi-sodium-11.0.0.761.iso
   Nodes:
   10.117.0.23 nlabp1023 SF3010 10.3.0.161
   10.117.0.24 nlabp1025 SF3010 10.3.0.161
   10.117.0.26 nlabp1027 SF3010 10.3.0.161
   10.117.0.28 nlabp1028 SF3010 10.3.0.161
   ################################################################
   ```

```
Do you want to continue? ['Yes', 'No']: yes
...
Watching for new network faults. Existing fault IDs are set([]).
Checking for legacy network interface names that need renaming
Upgrading from 10.3.0.161 to 11.0.0.761 upgrade method=rtfi
Waiting 300 seconds for cluster faults to clear
Waiting for caches to fall below threshold
...
Installing mip=[10.117.0.23] nodeID=[1] (1 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[7] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
Moving primary slice=[12] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
...
Installing mip=[10.117.114.24] nodeID=[2] (2 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[5] away from mip[10.117.114.24] nodeID[2] ssid[7]
to new ssid[11]
...
Install of solidfire-rtfi-sodium-11.0.0.761 complete.
Removing old software
No staged builds present on nodeID=[1]
No staged builds present on nodeID=[2]
...
Starting light cluster block service check
```

Wenn Sie einen Knoten der H610S-Serie auf Element 12.2 aktualisieren und auf dem Knoten eine Version von Element vor 11.8 ausgeführt wird, müssen Sie für jeden Speicher-Node weitere Upgrade-Schritte () durchführenPhase 2. Wenn Sie Element 11.8 oder höher ausführen, sind die zusätzlichen Aktualisierungsschritte (Phase 2) nicht erforderlich.

Aktualisieren der Element-Software an dunklen Standorten mithilfe von HealthTools

Sie können die HealthTools Suite mit Tools verwenden, um die NetApp Element Software an einer dunklen Stelle zu aktualisieren.

Was Sie benötigen

1. Gehen Sie zur NetApp HCI Software "download-Seite".
2. Wählen Sie das richtige Software-Release aus, und laden Sie das neueste Speicher-Node-Image auf einen Computer herunter, der nicht der Management-Node ist.

Für ein Upgrade der Element Storage-Software ist die neueste Version von HealthTools erforderlich.

3. Laden Sie diese Datei von der NetApp-Support-Website auf einem Computer herunter "JSON-Datei", der nicht der Verwaltungsknoten ist, und benennen Sie sie in um `metadata.json`.
4. Kopieren Sie die ISO-Datei in den Verwaltungsknoten an einem zugänglichen Speicherort wie `/tmp`.

Sie können dies mit, z. B. SCP, tun. Wenn Sie die ISO-Datei hochladen, stellen Sie sicher, dass sich der Name der Datei nicht ändert, da andernfalls spätere Schritte fehlschlagen.

Schritte

1. Führen Sie den Befehl aus `sfupdate-healthtools`:

```
sfupdate-healthtools <path-to-healthtools-package>
```

2. Überprüfen Sie die installierte Version:

```
sfupdate-healthtools -v
```

3. Überprüfen Sie die neueste Version mit der JSON-Metadatendatei:

```
sfupdate-healthtools -l --metadata=<path-to-metadata-json>
```

4. Stellen Sie sicher, dass der Cluster bereit ist:

```
sudo sfupgradecheck -u <cluster_username> -p <cluster_password> MVIP
--metadata=<path-to-metadata-json>
```

5. Führen Sie den `sfinstall` Befehl mit dem Pfad zur ISO-Datei und der JSON-Metadatendatei aus:

```
sfinstall -u <cluster_username> <MVIP> <path-toinstall-file-ISO>
--metadata=<path-to-metadata-json-file>
```

Der folgende Beispiel-Eingabebefehl kann abgerufen werden:

```
sfinstall -u admin 10.117.78.244 /tmp/solidfire-rtfi-11.3.0.345.iso
--metadata=/tmp/metadata.json
```

Optional Sie können dem Befehl das Flag `sfinstall` hinzufügen `--stage`, um das Upgrade im Voraus zu inszenieren.

Wenn Sie einen Knoten der H610S-Serie auf Element 12.2 aktualisieren und auf dem Knoten eine Version von Element vor 11.8 ausgeführt wird, müssen Sie für jeden Speicher-Node weitere Upgrade-Schritte () durchführenPhase 2. Wenn Sie Element 11.8 oder höher ausführen, sind die zusätzlichen Aktualisierungsschritte (Phase 2) nicht erforderlich.

Was passiert, wenn ein Upgrade mit HealthTools fehlschlägt

Falls das Software-Upgrade fehlschlägt, können Sie das Upgrade unterbrechen.

Sie sollten ein Upgrade nur mit Strg-C anhalten. Dies ermöglicht es dem System, sich selbst zu bereinigen.

Wenn `sfinstall` auf die Behebung von Clusterfehlern gewartet wird und wenn ein Fehler dazu führt, dass die Fehler weiterhin auftreten, `sfinstall` wird nicht zum nächsten Node gefahren.

Schritte

1. Sie sollten mit Strg+C anhalten `sfinstall`
2. Wenden Sie sich an den NetApp Support, um bei der Fehleranalyse zu helfen.
3. Setzen Sie das Upgrade mit demselben Befehl fort `sfinstall`.
4. Wenn ein Upgrade mithilfe von Strg+C angehalten wird, wählen Sie eine der folgenden Optionen aus, wenn das Upgrade einen Node aktualisiert.
   - **Wait**: Lassen Sie den aktuell aufrüsterenden Knoten fertig, bevor Sie die Cluster-Konstanten zurücksetzen.
   - **Weiter**: Setzen Sie das Upgrade fort, das die Pause abgebrochen.
   - **Abbrechen**: Setzen Sie die Cluster-Konstanten zurück und brechen Sie das Upgrade sofort ab.

   Wenn das Cluster-Upgrade abgebrochen wird, während ein Node aktualisiert wird, kann dies dazu führen, dass die Laufwerke nicht ordnungsgemäß vom Node entfernt werden. Wenn die Laufwerke unnormal entfernt werden, muss das Hinzufügen der Laufwerke während eines Upgrades manuell durch den NetApp Support erfolgen. Der Node kann länger dauern, um Firmware-Updates durchzuführen oder Aktivitäten zur Synchronisierung nach dem Update durchzuführen. Wenn der Upgrade-Fortschritt blockiert wird, wenden Sie sich an den NetApp Support.

Upgrade von H610S Storage-Nodes auf Element 12.2 (Phase 2)

Wenn Sie einen Node der H610S-Serie auf Element 12.2 aktualisieren und auf dem Node eine Version von Element vor 11.8 ausgeführt wird, umfasst der Upgrade-Prozess zwei Phasen.

Phase 1, die zuerst durchgeführt wird, folgt den gleichen Schritten wie das Standard-Upgrade auf Element 12.2. Es installiert Element Software und alle 5 Firmware-Updates einzeln für das Cluster einzeln und nacheinander. Aufgrund der Firmware-Nutzlast beträgt der Prozess ca. 1.5 bis 2 Stunden pro H610S Node, einschließlich eines einzelnen Kaltstarts am Ende des Upgrades für jeden Node.

Phase 2 umfasst das Ausführen der Schritte zum vollständigen Herunterfahren des Knotens und zum Trennen der Stromversorgung für jeden H610S-Knoten, die in einem erforderlich beschrieben sind "KB". Diese Phase wird voraussichtlich ca. eine Stunde pro H610S Node dauern.

Nach Abschluss von Phase 1 werden vier der fünf Firmware-Updates während des Kaltstarts auf jedem H610S-Knoten aktiviert. Die komplexe CPLD-Firmware (Programmable Logic Device) erfordert jedoch eine komplette Stromabschaltung und eine erneute Verbindung, um vollständig zu installieren. Das CPLD-Firmware-Update schützt vor NVDIMM-Ausfällen und beim Entfernen von Metadaten-Laufwerken während eines späteren Neustarts oder aus- und Einschaltzyklen. Dieses Power-Reset wird etwa eine Stunde pro H610S Node dauern. Sie müssen den Knoten herunterfahren, Netzkabel entfernen oder die Stromversorgung über eine intelligente PDU trennen, ca. 3 Minuten warten und die Stromversorgung wieder anschließen.

Was Sie benötigen

- Sie haben Phase 1 des H610S-Upgrade-Prozesses abgeschlossen und ein Upgrade Ihrer Storage-Nodes unter Verwendung eines der standardmäßigen Element Storage-Upgrade-Verfahren durchgeführt.

Phase 2 erfordert Personal vor Ort.

Schritte

1. (Phase 2) Abschließen des Kaltstarts für jeden H610S-Node im Cluster:

Wenn der Cluster auch keine H610S-Nodes aufweist, sind diese Nodes ohne H610S von Phase 2 ausgenommen und müssen nicht heruntergefahren oder die Stromversorgung getrennt werden.

1. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten und ein Upgrade zu planen.
2. Befolgen Sie hierzu das Verfahren für das Upgrade in Phase 2 "KB", das zum Abschluss eines Upgrades für jeden H610S-Node erforderlich ist.

Weitere Informationen

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

Firmware für Storage-Upgrades

Ab Element 12.0 und den Managementservices Version 2.14 können Sie über die NetApp Hybrid Cloud Control UI und die REST-API reine Firmware-Upgrades auf Ihren H-Series Storage-Nodes durchführen. Dieses Verfahren führt keine Upgrades für Element Software durch und ermöglicht ein Upgrade der Storage-Firmware außerhalb einer größeren Version.

Was Sie benötigen

- **Administratorrechte**: Sie haben Berechtigungen für den Storage Cluster Administrator, um das Upgrade durchzuführen.
- **System Time SYNC**: Sie haben sichergestellt, dass die Systemzeit auf allen Knoten synchronisiert ist und NTP für den Speicher-Cluster und die Knoten korrekt konfiguriert ist. Jeder Knoten muss mit einem DNS-Nameserver in der Web-UI pro Knoten konfiguriert werden (`https://[IP address]:442`) ohne ungelöste Clusterfehler im Zusammenhang mit Zeitversatz.
- **System-Ports**: Bei Upgrade-Nutzung von NetApp Hybrid Cloud Control haben Sie sichergestellt, dass die erforderlichen Ports geöffnet sind. Weitere Informationen finden Sie unter "Netzwerkports" .

- **Management-Node**: Für NetApp Hybrid Cloud Control UI und API wird der Management-Node in Ihrer Umgebung mit Version 11.3 ausgeführt.
- **Management Services**: Sie haben Ihr Management Services Bundle auf die neueste Version aktualisiert.

> Bei H610S Storage-Nodes mit Element Softwareversion 12.0 sollten Sie D-Patch SUST-909 anwenden, bevor Sie ein Upgrade auf das Storage-Firmware-Bundle 2.27 durchführen. Wenden Sie sich an den NetApp Support, um den D-Patch vor dem Upgrade zu erhalten. Siehe "Speicher-Firmware-Paket 2.27 – Versionshinweise".

> Sie müssen ein Upgrade auf das neueste Management Services Bundle durchführen, bevor Sie die Firmware auf Ihren Storage-Nodes aktualisieren. Wenn Sie Ihre Element Software auf Version 12.2 aktualisieren, benötigen Sie zum Fortfahren Managementservices 2.14.60 oder höher.

- **Cluster Health**: Sie haben Health Checks durchgeführt. Siehe "Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen".
- **BMC für H610S-Knoten aktualisiert**: Sie haben die BMC-Version für Ihre H610S-Knoten aktualisiert. Siehe "Versionshinweise und Upgrade-Anweisungen".

> Eine vollständige Matrix der Firmware und Treiber-Firmware für Ihre Hardware finden Sie unter "Unterstützte Firmware-Versionen für NetApp HCI Storage-Nodes".

- **Endbenutzer-Lizenzvereinbarung (EULA)**: Ab Management Services 2.20.69 müssen Sie die EULA akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder API zum Upgrade der Storage-Firmware verwenden:
  a. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

  b. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
  c. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
  d. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Upgrade-Optionen

Wählen Sie eine der folgenden Upgrade-Optionen für die Speicher-Firmware:

- Verwenden Sie die NetApp Hybrid Cloud Control UI für ein Upgrade der Storage-Firmware
- Verwenden Sie die NetApp Hybrid Cloud Control API für ein Upgrade der Storage-Firmware

Verwenden Sie die NetApp Hybrid Cloud Control UI für ein Upgrade der Storage-Firmware

Mit der NetApp Hybrid Cloud Control UI lässt sich die Firmware der Storage-Nodes in Ihrem Cluster aktualisieren.

Was Sie benötigen

- Wenn Ihr Verwaltungsknoten nicht mit dem Internet verbunden ist, haben Sie "Das Storage-Firmware-

Bundle heruntergeladen" .

Potenzielle Probleme beim Upgrade von Storage-Clustern mit NetApp Hybrid Cloud Control und ihren Behelfslösungen finden Sie im "KB-Artikel".

Pro Node dauert das Upgrade etwa 30 Minuten.

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 **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite **Upgrades** die Option **Speicherung**.

Auf der Registerkarte **Storage** werden die Speichercluster aufgelistet, die Teil Ihrer Installation sind. Wenn durch NetApp Hybrid Cloud Control auf ein Cluster zugegriffen werden kann, wird es nicht auf der Seite **Upgrades** angezeigt. Wenn bei Clustern mit Element 12.0 oder höher die aktuelle Firmware-Bundle-Version für diese Cluster aufgeführt ist. Wenn die Knoten in einem einzelnen Cluster unterschiedliche Firmware-Versionen haben oder wenn das Upgrade fortschreitet, wird in der Spalte **Aktuelle Firmware Bundle Version Multiple** angezeigt. Sie können **multiple** auswählen, um zur Seite **Nodes** zu navigieren, um Firmware-Versionen zu vergleichen. Wenn auf allen Clustern Elementversionen vor 12.0 ausgeführt werden, werden Ihnen keine Informationen über die Versionsnummern der Firmware-Bundles angezeigt. Diese Informationen finden Sie auch auf der Seite **Nodes**. Siehe "Zeigen Sie Ihren Bestand an".

Wenn der Cluster aktuell ist und/oder keine Upgrade-Pakete verfügbar sind, werden die Registerkarten **Element** und **Firmware Only** nicht angezeigt. Diese Registerkarten werden auch nicht angezeigt, wenn ein Upgrade ausgeführt wird. Wenn die Registerkarte **Element** angezeigt wird, nicht jedoch die Registerkarte **Firmware only**, stehen keine Firmware-Pakete zur Verfügung.

5. Wählen Sie den Dropdown-Pfeil neben dem Cluster aus, das Sie aktualisieren möchten.
6. Wählen Sie **Durchsuchen**, um das heruntergeladene Aktualisierungspaket hochzuladen.
7. Warten Sie, bis der Upload abgeschlossen ist. In einer Statusleiste wird der Status des Uploads angezeigt.

Der Datei-Upload geht verloren, wenn Sie vom Browser-Fenster wegnavigieren.

Nach dem erfolgreichen Hochladen und Validierungen der Datei wird eine Meldung auf dem Bildschirm angezeigt. Die Validierung kann mehrere Minuten in Anspruch nehmen. Wenn Sie zu diesem Zeitpunkt vom Browser-Fenster weg navigieren, bleibt der Datei-Upload erhalten.

8. Wählen Sie **nur Firmware** aus, und wählen Sie aus den verfügbaren Upgrade-Versionen.
9. Wählen Sie **Upgrade Starten**.

Der **Upgrade-Status** ändert sich während des Upgrades, um den Status des Prozesses anzuzeigen. Es ändert sich auch in Reaktion auf Aktionen, die Sie ergreifen, z. B. die Unterbrechung des Upgrades oder wenn das Upgrade einen Fehler zurückgibt. Siehe Statusänderungen des Upgrades.

Während das Upgrade läuft, können Sie die Seite verlassen und zu einem späteren Zeitpunkt zurückkehren, um den Fortschritt zu überwachen. Die Seite aktualisiert den Status und die aktuelle Version nicht dynamisch, wenn die Cluster-Zeile ausgeblendet ist. Die Cluster-Zeile muss erweitert werden, um die Tabelle zu aktualisieren, oder Sie können die Seite aktualisieren.

Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist.

Statusänderungen des Upgrades

Hier sind die verschiedenen Status, in denen die Spalte **Upgrade Status** in der UI vor, während und nach dem Upgrade-Prozess angezeigt wird:

Upgrade-Status	Beschreibung
Auf dem aktuellen Stand	Das Cluster wurde auf die neueste verfügbare Element-Version aktualisiert oder die Firmware wurde auf die neueste Version aktualisiert.
Erkennung nicht möglich	Dieser Status wird angezeigt, wenn die Speicherdienst-API einen Upgrade-Status zurückgibt, der nicht in der aufgezählten Liste möglicher Upgrade-Status aufgeführt ist.
Verfügbare Versionen	Neuere Versionen von Element und/oder Storage Firmware stehen für ein Upgrade zur Verfügung.
In Bearbeitung	Das Upgrade läuft. In einer Statusleiste wird der Aktualisierungsstatus angezeigt. Auf dem Bildschirm werden zudem Fehler auf Node-Ebene angezeigt und die Node-ID jedes Node im Cluster wird angezeigt, wenn das Upgrade fortschreitet. Sie können den Status jedes Knotens über die Element-UI oder das NetApp Element Plug-in für vCenter Server UI überwachen.
Anhalten Des Upgrades	Sie können das Upgrade anhalten. Je nach Status des Upgrade-Prozesses kann der Pause-Vorgang erfolgreich oder fehlgeschlagen sein. Es wird eine UI-Eingabeaufforderung angezeigt, in der Sie aufgefordert werden, den Pause-Vorgang zu bestätigen. Um sicherzustellen, dass sich das Cluster vor dem Anhalten eines Upgrades an einem sicheren Ort befindet, kann es bis zu zwei Stunden dauern, bis der Upgrade-Vorgang vollständig angehalten ist. Um das Upgrade fortzusetzen, wählen Sie **Fortsetzen**.
Angehalten	Sie haben das Upgrade angehalten. Wählen Sie **Fortsetzen**, um den Prozess fortzusetzen.

Upgrade-Status	Beschreibung
Fehler	Während des Upgrades ist ein Fehler aufgetreten. Sie können das Fehlerprotokoll herunterladen und an den NetApp Support senden. Nachdem Sie den Fehler behoben haben, können Sie zur Seite zurückkehren und **Fortsetzen** wählen. Wenn Sie das Upgrade fortsetzen, geht die Statusleiste einige Minuten lang zurück, während das System die Zustandsprüfung ausführt und den aktuellen Status des Upgrades überprüft.

Was geschieht bei einem Upgrade mit NetApp Hybrid Cloud Control

Wenn während eines Upgrades ein Laufwerk oder ein Node ausfällt, zeigt die Element-UI Clusterfehler an. Der Upgrade-Prozess setzt nicht auf den nächsten Node fort und wartet auf die Behebung der Cluster-Fehler. Die Fortschrittsleiste in der UI zeigt an, dass das Upgrade auf die Behebung der Cluster-Fehler wartet. In dieser Phase funktioniert die Auswahl von **Pause** in der Benutzeroberfläche nicht, da das Upgrade wartet, bis der Cluster wieder gesund ist. Sie müssen NetApp Support beauftragen, die Fehleruntersuchung zu unterstützen.

NetApp Hybrid Cloud Control verfügt über eine festgelegte Wartezeit von drei Stunden. In diesem Fall kann es zu einem der folgenden Szenarien kommen:

- Die Behebung von Clusterfehlern erfolgt innerhalb des dreistündigen Zeitfensters und das Upgrade wird fortgesetzt. Sie müssen in diesem Szenario keine Maßnahmen ergreifen.
- Das Problem besteht nach drei Stunden weiter, und der Aktualisierungsstatus zeigt **Fehler** mit einem roten Banner an. Sie können das Upgrade fortsetzen, indem Sie nach der Behebung des Problems **Fortsetzen** auswählen.
- Der NetApp Support hat festgestellt, dass das Upgrade vorübergehend abgebrochen werden muss, damit Korrekturmaßnahmen vor dem dreistündigen Fenster durchgeführt werden können. Der Support verwendet die API, um das Upgrade abzubrechen.

Wenn das Cluster-Upgrade abgebrochen wird, während ein Node aktualisiert wird, kann dies dazu führen, dass die Laufwerke nicht ordnungsgemäß vom Node entfernt werden. Wenn die Laufwerke unnormal entfernt werden, muss das Hinzufügen der Laufwerke während eines Upgrades manuell durch den NetApp Support erfolgen. Der Node kann länger dauern, um Firmware-Updates durchzuführen oder Aktivitäten zur Synchronisierung nach dem Update durchzuführen. Wenn der Upgrade-Fortschritt blockiert wird, wenden Sie sich an den NetApp Support.

Verwenden Sie die NetApp Hybrid Cloud Control API für ein Upgrade der Storage-Firmware

Mit APIs können Storage-Nodes in einem Cluster auf die neueste Element Softwareversion aktualisiert werden. Sie können ein Automatisierungstool Ihrer Wahl zum Ausführen der APIs verwenden. Der hier dokumentierte API-Workflow nutzt die REST-API-UI, die am Management-Node verfügbar ist.

Schritte

1. Laden Sie das neueste Upgrade-Paket für die Storage-Firmware auf ein Gerät herunter, auf das der Management-Node zugreifen kann. "Bundle-Seite für die Element Software Storage-Firmware" Laden Sie das neueste Image der Storage-Firmware herunter.
2. Laden Sie das Upgrade-Paket für die Speicher-Firmware auf den Management-Node hoch:

a. Öffnen Sie die REST-API-UI für den Management-Node:

```
https://<ManagementNodeIP>/package-repository/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 `mnode-client`ein.

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

iv. Schließen Sie das Autorisierungsfenster.

c. Wählen Sie in DER REST API-Benutzeroberfläche **POST /Packages** aus.

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

e. Wählen Sie **Durchsuchen** und wählen Sie das Aktualisierungspaket aus.

f. Wählen Sie **Ausführen**, um den Upload zu initiieren.

g. Kopieren Sie aus der Antwort die Paket-ID (`"id"`) und speichern Sie sie zur Verwendung in einem späteren Schritt.

3. Überprüfen Sie den Status des Uploads.

a. Wählen Sie in DER REST-API-Benutzeroberfläche **GET /packages/{id}/Status** aus.

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

c. Geben Sie die Firmware-Paket-ID ein, die Sie im vorherigen Schritt in **id** kopiert haben.

d. Wählen Sie **Ausführen**, um die Statusanforderung zu initiieren.

Die Antwort zeigt an `state` `SUCCESS`, dass der Vorgang abgeschlossen ist.

4. Suchen Sie die Installations-Asset-ID:

a. Öffnen Sie die REST-API-UI für den Management-Node:

```
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 `mnode-client`ein.

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

iv. Schließen Sie das Autorisierungsfenster.

c. Wählen Sie in DER REST API-Benutzeroberfläche **GET /Installations** aus.

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

e. Wählen Sie **Ausführen**.

f. Kopieren Sie aus der Antwort die Installations-Asset(`id`-ID).

```
"id": "abcd01e2-xx00-4ccf-11ee-11f111xx9a0b",
"management": {
  "errors": [],
  "inventory": {
    "authoritativeClusterMvip": "10.111.111.111",
    "bundleVersion": "2.14.19",
    "managementIp": "10.111.111.111",
    "version": "1.4.12"
```

g. 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 in der Antwort die Speicher-Cluster-ID (`"id"`) des Clusters, den Sie aktualisieren möchten, und speichern Sie sie für einen späteren Schritt.

```
"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",
```

5. Führen Sie das Speicher-Firmware-Upgrade aus:

a. Öffnen Sie die Storage REST API-UI auf dem Management-Node:

```
https://<ManagementNodeIP>/storage/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 `mnode-client`ein.
   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   iv. Schließen Sie das Fenster.
c. Wählen Sie **POST/Upgrades**.
d. Wählen Sie **Probieren Sie es aus**.
e. Geben Sie die Paket-ID des Upgrades in das Feld Parameter ein.
f. Geben Sie im Parameterfeld die Storage-Cluster-ID ein.
g. Wählen Sie **Ausführen**, um das Upgrade zu initiieren.

Die Antwort sollte folgendes angeben `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",
        "description": "string",
        "remedy": "string",
        "severity": "string",
        "data": {},
        "nodeID": 0
      }
    ]
  },
```

```
  "taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
  "dateCompleted": "2020-04-21T22:10:57.057Z",
  "dateCreated": "2020-04-21T22:10:57.057Z"
}
```

a. Kopieren Sie die Upgrade-ID (`"upgradeId"`), die Teil der Antwort ist.

6. Überprüfen Sie den Aktualisierungsfortschritt und die Ergebnisse:

   a. Wählen Sie **GET /Upgrades/{upgradeId}** aus.

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

   c. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein.

   d. Wählen Sie **Ausführen**.

   e. Führen Sie einen der folgenden Schritte aus, wenn während des Upgrades Probleme oder besondere Anforderungen auftreten:

Option	Schritte
Sie müssen Probleme mit dem Clusterzustand aufgrund einer Meldung im Antworttext beheben `failedHealthChecks`.	i. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus. ii. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus. iii. Nachdem Sie Clusterprobleme behoben haben, authentifizieren Sie sich bei Bedarf erneut und wählen Sie **PUT /Upgrades/{UpgradeId}** aus. iv. Wählen Sie **Probieren Sie es aus**. v. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. vi. Geben Sie den Anforderungskörper ein `"action":"resume"`. `{ "action": "resume" }` vii. Wählen Sie **Ausführen**.

Option	Schritte
Sie müssen das Upgrade unterbrechen, da das Wartungsfenster geschlossen wird oder aus einem anderen Grund.	i. Bei Bedarf erneut authentifizieren und **PUT /Upgrades/{UpgradeId}** auswählen. ii. Wählen Sie **Probieren Sie es aus**. iii. Geben Sie die Upgrade-ID des vorherigen Schritts in **UpgradeId** ein. iv. Geben Sie den Anforderungskörper ein `"action":"pause"`. `{ "action": "pause" }` v. Wählen Sie **Ausführen**.

f. Führen Sie die **GET /Upgrades/{upgradeId}** API nach Bedarf mehrmals aus, bis der Prozess abgeschlossen ist.

   Während der Aktualisierung zeigt das `status` an `running`, ob keine Fehler aufgetreten sind. Wenn jeder Knoten aktualisiert wird, ändert sich der `step` Wert in `NodeFinished`.

Das Upgrade wurde erfolgreich abgeschlossen, wenn der `percent` Wert lautet `100` und der `state` angezeigt `finished`wird.

Weitere Informationen

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

Upgrade eines Management-Node

Sie können den Management-Node von Version 11.0 oder höher auf den Management-Node Version 12.2 aktualisieren.

> Zum Upgrade der Element Software auf dem Storage-Cluster ist kein Upgrade des Betriebssystems des Management-Node mehr erforderlich. Wenn der Management-Node Version 11.3 oder höher ist, können die Managementservices einfach auf die neueste Version aktualisiert werden, um Element-Upgrades mithilfe von NetApp Hybrid Cloud Control durchzuführen. Befolgen Sie für Ihr Szenario die Vorgehensweise zum Upgrade des Management-Node, wenn Sie aus anderen Gründen, wie z. B. Sicherheitsbehebungsmaßnahmen, ein Upgrade des Betriebssystems des Management-Node durchführen möchten.

Was Sie benötigen

- Das vCenter Plug-in 4.4 oder höher erfordert einen Management-Node 11.3 oder höher, der mit modularer Architektur erstellt wird und individuelle Services bietet.

Upgrade-Optionen

Wählen Sie eine der folgenden Upgrade-Optionen für Management-Nodes:

- Wenn Sie ein Upgrade von Management-Knoten 12.0 durchführen: Aktualisieren Sie einen Management-Node von 12.0 auf Version 12.2
- Wenn Sie ein Upgrade von Management-Knoten 11.3, 11.5, 11.7 oder 11.8 durchführen: Upgrade eines Management-Node auf Version 12.2 von 11.3 bis 11.8
- Wenn Sie ein Upgrade von Management-Knoten 11.0 oder 11.1 durchführen: Aktualisieren Sie einen Management-Node von 11.1 oder 11.0 auf Version 12.2
- Wenn Sie ein Upgrade von einem Management-Node der Version 10.x durchführen: Migration von Management-Node-Version 10.x zu 11.x

Wählen Sie diese Option, wenn Sie **sequenziell** aktualisiert haben (1) die Version der Managementservices und (2) Ihre Element Speicherversion und Ihren vorhandenen Management-Node **beibehalten** möchten:

> Wenn Sie Ihre Managementservices, gefolgt vom Element Storage, nicht nacheinander aktualisieren, können Sie die erneute Authentifizierung mit diesem Verfahren nicht neu konfigurieren. Befolgen Sie stattdessen das entsprechende Upgrade-Verfahren.

- Wenn Sie den vorhandenen Management-Node beibehalten: Konfigurieren Sie die Authentifizierung mithilfe der REST-API des Management-Node neu

Aktualisieren Sie einen Management-Node von 12.0 auf Version 12.2

Sie können ein in-Place-Upgrade des Management-Node von Version 12.0 auf Version 12.2 durchführen, ohne eine neue virtuelle Maschine für den Management-Node bereitstellen zu müssen.

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

Was Sie benötigen

- Der Management-Node, den Sie aktualisieren möchten, ist die Version 12.0 und verwendet IPv4-Netzwerke. Der Management-Node Version 12.2 unterstützt IPv6 nicht.

  > Um die Version Ihres Management-Node zu überprüfen, melden Sie sich bei Ihrem Management-Node an, und zeigen Sie die Versionsnummer des Elements im Anmeldebanner an.

- Sie haben Ihr Management-Services-Bundle mit NetApp Hybrid Cloud Control (HCC) auf die neueste Version aktualisiert. Sie können über die folgende IP auf HCC zugreifen: <code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt;</code>
- Wenn Sie den Verwaltungsknoten auf Version 12.2 aktualisieren, benötigen Sie die Verwaltungsdienste 2.14.60 oder höher, um fortzufahren.
- Sie haben einen zusätzlichen Netzwerkadapter (falls erforderlich) gemäß den Anweisungen für konfiguriert"Konfigurieren einer zusätzlichen Speicher-NIC".

  > Für persistente Volumes ist möglicherweise ein zusätzlicher Netzwerkadapter erforderlich, wenn eth0 nicht an das SVIP weitergeleitet werden kann. Konfigurieren Sie einen neuen Netzwerkadapter im iSCSI-Speichernetzwerk zur Konfiguration von persistenten Volumes.

- Storage-Nodes werden mit Element 11.3 oder höher ausgeführt.

Schritte

1. Konfigurieren Sie den Management-Node-VM-RAM:
   a. Schalten Sie die Management-Node-VM aus.
   b. Ändern Sie den RAM der Management-Node-VM von 12 GB in 24 GB RAM.
   c. Schalten Sie die Management-Node-VM ein.
2. Melden Sie sich bei der Virtual Machine des Management-Node über SSH oder Konsolenzugriff an.
3. Laden Sie den für NetApp HCI von der NetApp-Support-Website auf die virtuelle Maschine des Management-Node herunter "ISO für den Management-Node".

   Der Name der ISO ist ähnlich wie `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Prüfen Sie die Integrität des Downloads, indem Sie md5sum auf der heruntergeladenen Datei ausführen und vergleichen Sie die Ausgabe mit den verfügbaren Ressourcen auf der NetApp Support-Website für NetApp HCI oder Element Software wie im folgenden Beispiel:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

5. Mounten Sie das Management-Node-ISO-Image und kopieren Sie den Inhalt auf das Dateisystem mit den folgenden Befehlen:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
   ```

   ```
   sudo cp -r /mnt/* /upgrade
   ```

6. Wechseln Sie in das Home-Verzeichnis, und heben Sie die Bereitstellung der ISO-Datei auf von `/mnt`:

   ```
   sudo umount /mnt
   ```

7. Löschen Sie die ISO, um Speicherplatz auf dem Management-Node einzusparen:

   ```
   sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

8. (Nur bei Konfigurationen ohne persistente Volumes) Kopieren Sie den Inhalt des Container-Ordners für das Backup:

```
sudo cp -r /var/lib/docker/volumes /sf/etc/mnode
```

9. Führen Sie auf dem Management-Node, den Sie aktualisieren, den folgenden Befehl aus, um die Version des Management-Node-Betriebssystems zu aktualisieren. Das Skript speichert alle erforderlichen Konfigurationsdateien nach dem Upgrade, wie z. B. Active IQ-Collector- und Proxy-Einstellungen.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

   Der Management-Node wird nach Abschluss des Upgrades mit einem neuen OS neu gebootet.

10. (Nur bei Konfigurationen ohne persistente Volumes) Verschieben des Inhalts des Containerordners an den ursprünglichen Speicherort:

```
sudo su
mv /sf/etc/mnode/volumes/* /var/lib/docker/volumes/
```

11. Führen Sie auf dem Verwaltungsknoten das Skript aus `redeploy-mnode`, um die Konfigurationseinstellungen der früheren Verwaltungsdienste beizubehalten:

> Das Skript behält die vorherige Konfiguration der Managementservices bei, einschließlich der Konfiguration über den Active IQ Collector Service, Controller (vCenters) oder Proxy, je nach Ihren Einstellungen.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

> Wenn Sie die SSH-Funktion auf dem Management-Node zuvor deaktiviert haben, müssen Sie "Deaktivieren Sie SSH erneut"auf dem wiederhergestellten Management-Node die entsprechende Option ausführen. Die SSH-Funktion "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support"ist standardmäßig auf dem Management-Node aktiviert.

Upgrade eines Management-Node auf Version 12.2 von 11.3 bis 11.8

Sie können ein in-Place-Upgrade des Management-Node von Version 11.3, 11.5, 11.7 oder 11.8 auf Version 12.2 durchführen, ohne eine neue virtuelle Maschine für den Management-Node bereitstellen zu müssen.

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

Was Sie benötigen

- Der Managementknoten, den Sie aktualisieren möchten, ist die Version 11.3, 11.5, 11.7 oder 11.8 und verwendet IPv4-Netzwerke. Der Management-Node Version 12.2 unterstützt IPv6 nicht.

Um die Version Ihres Management-Node zu überprüfen, melden Sie sich bei Ihrem Management-Node an, und zeigen Sie die Versionsnummer des Elements im Anmeldebanner an.

- Sie haben Ihr Management-Services-Bundle mit NetApp Hybrid Cloud Control (HCC) auf die neueste Version aktualisiert. Sie können über die folgende IP auf HCC zugreifen: <code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt;</code>
- Wenn Sie den Verwaltungsknoten auf Version 12.2 aktualisieren, benötigen Sie die Verwaltungsdienste 2.14.60 oder höher, um fortzufahren.
- Sie haben einen zusätzlichen Netzwerkadapter (falls erforderlich) gemäß den Anweisungen für konfiguriert"Konfigurieren einer zusätzlichen Speicher-NIC".

Für persistente Volumes ist möglicherweise ein zusätzlicher Netzwerkadapter erforderlich, wenn eth0 nicht an das SVIP weitergeleitet werden kann. Konfigurieren Sie einen neuen Netzwerkadapter im iSCSI-Speichernetzwerk zur Konfiguration von persistenten Volumes.

- Storage-Nodes werden mit Element 11.3 oder höher ausgeführt.

Schritte

1. Konfigurieren Sie den Management-Node-VM-RAM:
   a. Schalten Sie die Management-Node-VM aus.
   b. Ändern Sie den RAM der Management-Node-VM von 12 GB in 24 GB RAM.
   c. Schalten Sie die Management-Node-VM ein.
2. Melden Sie sich bei der Virtual Machine des Management-Node über SSH oder Konsolenzugriff an.
3. Laden Sie den für NetApp HCI von der NetApp-Support-Website auf die virtuelle Maschine des Management-Node herunter "ISO für den Management-Node".

Der Name der ISO ist ähnlich wie `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Prüfen Sie die Integrität des Downloads, indem Sie md5sum auf der heruntergeladenen Datei ausführen und vergleichen Sie die Ausgabe mit den verfügbaren Ressourcen auf der NetApp Support-Website für NetApp HCI oder Element Software wie im folgenden Beispiel:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

5. Mounten Sie das Management-Node-ISO-Image und kopieren Sie den Inhalt auf das Dateisystem mit den folgenden Befehlen:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
   ```

```
sudo cp -r /mnt/* /upgrade
```

6. Wechseln Sie in das Home-Verzeichnis, und heben Sie die Bereitstellung der ISO-Datei auf von `/mnt`:

```
sudo umount /mnt
```

7. Löschen Sie die ISO, um Speicherplatz auf dem Management-Node einzusparen:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. Führen Sie auf dem Management-Node 11.3, 11.5, 11.7 oder 11.8 den folgenden Befehl aus, um die Version des Management-Node-Betriebssystems zu aktualisieren. Das Skript speichert alle erforderlichen Konfigurationsdateien nach dem Upgrade, wie z. B. Active IQ-Collector- und Proxy-Einstellungen.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

   Der Management-Node wird nach Abschluss des Upgrades mit einem neuen OS neu gebootet.

9. Führen Sie auf dem Verwaltungsknoten das Skript aus `redeploy-mnode`, um die Konfigurationseinstellungen der früheren Verwaltungsdienste beizubehalten:

   Das Skript behält die vorherige Konfiguration der Managementservices bei, einschließlich der Konfiguration über den Active IQ Collector Service, Controller (vCenters) oder Proxy, je nach Ihren Einstellungen.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

Wenn Sie die SSH-Funktion auf dem Management-Node zuvor deaktiviert haben, müssen Sie "Deaktivieren Sie SSH erneut"auf dem wiederhergestellten Management-Node die entsprechende Option ausführen. Die SSH-Funktion "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support"ist standardmäßig auf dem Management-Node aktiviert.

Aktualisieren Sie einen Management-Node von 11.1 oder 11.0 auf Version 12.2

Sie können ein in-Place-Upgrade des Management-Node von 11.0 oder 11.1 auf Version 12.2 durchführen, ohne eine neue virtuelle Maschine für Management-Nodes bereitstellen zu müssen.

Was Sie benötigen

- Storage-Nodes werden mit Element 11.3 oder höher ausgeführt.

  Verwenden Sie die neuesten HealthTools, um die Element-Software zu aktualisieren.

- Der Management-Node, den Sie aktualisieren möchten, ist die Version 11.0 oder 11.1 und verwendet IPv4-Netzwerke. Der Management-Node Version 12.2 unterstützt IPv6 nicht.

  Um die Version Ihres Management-Node zu überprüfen, melden Sie sich bei Ihrem Management-Node an, und zeigen Sie die Versionsnummer des Elements im Anmeldebanner an. Für Management-Node 11.0 muss der VM-Speicher manuell auf 12 GB erweitert werden.

- Sie haben einen zusätzlichen Netzwerkadapter (falls erforderlich) unter Verwendung der Anweisungen zum Konfigurieren einer Speicher-NIC (eth1) im Management-Node-Benutzerhandbuch Ihres Produkts konfiguriert.

  Für persistente Volumes ist möglicherweise ein zusätzlicher Netzwerkadapter erforderlich, wenn eth0 nicht an das SVIP weitergeleitet werden kann. Konfigurieren Sie einen neuen Netzwerkadapter im iSCSI-Speichernetzwerk zur Konfiguration von persistenten Volumes.

Schritte

1. Konfigurieren Sie den Management-Node-VM-RAM:
   a. Schalten Sie die Management-Node-VM aus.
   b. Ändern Sie den RAM der Management-Node-VM von 12 GB in 24 GB RAM.
   c. Schalten Sie die Management-Node-VM ein.
2. Melden Sie sich bei der Virtual Machine des Management-Node über SSH oder Konsolenzugriff an.
3. Laden Sie den für NetApp HCI von der NetApp-Support-Website auf die virtuelle Maschine des Management-Node herunter "ISO für den Management-Node".

   Der Name der ISO ist ähnlich wie `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Prüfen Sie die Integrität des Downloads, indem Sie md5sum auf der heruntergeladenen Datei ausführen und vergleichen Sie die Ausgabe mit den verfügbaren Ressourcen auf der NetApp Support-Website für NetApp HCI oder Element Software wie im folgenden Beispiel:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

5. Mounten Sie das Management-Node-ISO-Image und kopieren Sie den Inhalt auf das Dateisystem mit den folgenden Befehlen:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso /mnt
   ```

```
sudo cp -r /mnt/* /upgrade
```

6. Wechseln Sie in das Home-Verzeichnis, und heben Sie die Bereitstellung der ISO-Datei von /mnt ab:

```
sudo umount /mnt
```

7. Löschen Sie die ISO, um Speicherplatz auf dem Management-Node einzusparen:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. Führen Sie einen der folgenden Skripte mit Optionen aus, um die Version des Management Node-Betriebssystems zu aktualisieren. Führen Sie nur das für Ihre Version geeignete Skript aus. Jedes Skript speichert alle erforderlichen Konfigurationsdateien nach dem Upgrade, z. B. Active IQ-Collector- und Proxy-Einstellungen.
   a. Führen Sie auf einem 11.1 (11.1.0.73) Management-Node den folgenden Befehl aus:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.3.2288
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
/sf/packages/nma"
```

   b. Führen Sie auf einem 11.1 (11.1.0.72) Management-Node den folgenden Befehl aus:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.1.2281
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
/sf/packages/nma"
```

   c. Führen Sie auf einem 11.0 (11.0.0.781) Management-Node den folgenden Befehl aus:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.0.2253
/sf/packages/solidfire-nma-1.4.8/conf /sf/packages/sioc
/sf/packages/nma"
```

   Der Management-Node wird nach Abschluss des Upgrades mit einem neuen OS neu gebootet.

9. Führen Sie auf dem Management-Knoten 12.2 das Skript aus `upgrade-mnode`, um die vorherigen Konfigurationseinstellungen beizubehalten.

   Wenn Sie von einem 11.0- oder 11.1-Management-Node migrieren, kopiert das Skript den Active IQ Collector in das neue Konfigurationsformat.

   a. Bei einem einzelnen Storage-Cluster, der von einem vorhandenen Management-Node 11.0 oder 11.1 mit persistenten Volumes gemanagt wird:

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
   persistent volume> -pva <persistent volume account name - storage
   volume account>
   ```

   b. Bei einem einzelnen Storage-Cluster, der über einen vorhandenen Management-Node 11.0 oder 11.1 ohne persistente Volumes gemanagt wird:

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user>
   ```

   c. Bei mehreren Storage-Clustern, die durch einen vorhandenen Management-Node 11.0 oder 11.1 mit persistenten Volumes gemanagt werden:

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
   persistent volume> -pva <persistent volume account name - storage
   volume account> -pvm <persistent volumes mvip>
   ```

   d. Für mehrere Storage-Cluster, die von einem vorhandenen Management-Node 11.0 oder 11.1 ohne persistente Volumes gemanagt werden (das `-pvm` Flag dient nur zur Bereitstellung einer der MVIP-Adressen des Clusters):

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for
   persistent volumes>
   ```

10. (Für alle NetApp HCI-Installationen mit NetApp Element Plug-in für vCenter Server) Aktualisieren Sie das vCenter Plug-in auf dem Management-Knoten 12.2, indem Sie die Schritte im Thema ausführen"Aktualisieren Sie das Element Plug-in für vCenter Server".

11. Suchen Sie mit der Management-Node-API die Asset-ID für Ihre Installation:

    a. Melden Sie sich in einem Browser bei DER REST API-UI für den Management-Node an:

       i. Gehen Sie zum Speicher-MVIP und melden Sie sich an. Dadurch wird das Zertifikat für den nächsten Schritt akzeptiert.

    b. Öffnen Sie die REST API-UI für den Bestandsdienst auf dem Managementknoten:

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

c. 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 `mnode-client`ein.

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

   iv. Schließen Sie das Fenster.

d. Wählen Sie in DER REST API UI **GET /Installations** aus.

e. Wählen Sie **Probieren Sie es aus**.

f. Wählen Sie **Ausführen**.

g. Kopieren Sie aus dem Antworttext von Code 200 die `id` für die Installation.

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

12. Suchen Sie in vSphere das Hardware-Tag für Ihren Computing-Node:

    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` die Verwendung in einem späteren Schritt.

13. Hinzufügen eines vCenter-Controller-Assets für HCI-Monitoring und Hybrid Cloud Control zu bekannten Management-Node-Ressourcen:

    a. Wählen Sie **POST /Assets/{Asset_id}/Controllers** aus, um eine Unterressource des Controllers 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 die erforderlichen Nutzlastwerte mit dem Typ und den vCenter-Anmeldedaten ein `vCenter`.

    e. Wählen Sie **Ausführen**.

14. Hinzufügen einer Computing-Node-Ressource zu den bekannten Assets des Management-Node:

    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. Geben Sie als `type` ein und fügen Sie das Hardware-Tag ein `ESXi Host`, das Sie in einem vorherigen Schritt für gespeichert `hardware_tag` haben.

    e. Wählen Sie **Ausführen**.

Migration von Management-Node-Version 10.x zu 11.x

Wenn Sie einen Management-Node bei Version 10.x haben, können Sie kein Upgrade von 10.x auf 11.x durchführen Stattdessen können Sie dieses Migrationsverfahren verwenden, um die Konfiguration von 10.x auf einen neu implementierten 11.1 Management-Node zu kopieren. Wenn Ihr Management-Node derzeit 11.0

oder höher ist, sollten Sie dieses Verfahren überspringen. Sie benötigen Management-Knoten 11.0 oder 11.1 und die neueste HealthTools, um die Element Software von 10.3 + auf 11.x. zu aktualisieren

Schritte

1. Implementieren Sie über die VMware vSphere Schnittstelle den Management-Knoten 11.1 OVA und schalten Sie ihn ein.
2. Öffnen Sie die Management-Node-VM-Konsole, über die die Terminal-Benutzeroberfläche (TUI) aufgerufen wird.
3. Erstellen Sie mit der TUI eine neue Administrator-ID und weisen Sie ein Passwort zu.
4. Melden Sie sich im Management-Knoten TUI mit der neuen ID und dem neuen Passwort am Management-Knoten an und überprüfen Sie, ob es funktioniert.
5. Über vCenter oder den Management-Node TUI erhalten Sie die IP-Adresse des Management-Node 11.1 und suchen Sie nach der IP-Adresse am Port 9443, um die Management-Node-UI zu öffnen.

   ```
   https://<mNode 11.1 IP address>:9443
   ```

6. Wählen Sie in vSphere die Option **NetApp Element-Konfiguration** > **mNode-Einstellungen** aus. (In älteren Versionen lautet das oberste Menü **NetApp SolidFire Konfiguration**.)
7. Wählen Sie **Aktionen** > **Löschen**.
8. Wählen Sie zur Bestätigung * Ja* aus. Das Feld mNode Status sollte nicht konfiguriert melden.

   Wenn Sie zum ersten Mal auf die Registerkarte **mNode-Einstellungen** wechseln, wird das mNode-Statusfeld anstelle des erwarteten **UP** möglicherweise als **nicht konfiguriert** angezeigt; Sie können unter Umständen nicht **Aktionen** > **Löschen** wählen. Aktualisieren Sie den Browser. Das Feld mNode Status wird schließlich **UP** angezeigt.

9. Melden Sie sich von vSphere ab.
10. Öffnen Sie in einem Webbrowser das Management Node Registration Utility und wählen Sie **QoSSIOC Service Management**:

    ```
    https://<mNode 11.1 IP address>:9443
    ```

11. Legen Sie das neue QoSSIOC-Passwort fest.

    Das Standardpasswort lautet `solidfire`. Dieses Passwort ist erforderlich, um das neue Passwort festzulegen.

12. Wählen Sie die Registerkarte **vCenter Plug-in Registration** aus.
13. Wählen Sie **Plug-in aktualisieren**.
14. Geben Sie erforderliche Werte ein. Wenn Sie fertig sind, wählen Sie **UPDATE**.
15. Melden Sie sich bei vSphere an und wählen Sie **NetApp Element-Konfiguration** > **mNode-Einstellungen**.
16. Wählen Sie **Aktionen** > **Konfigurieren**.
17. Geben Sie die IP-Adresse des Verwaltungsknotens, die Benutzer-ID des Verwaltungsknotens (der

Benutzername ist), das Passwort, das Sie auf der Registerkarte **QoSSIOC Service Management** des Registrierungs-Dienstprogramms festgelegt haben, sowie die vCenter-Benutzer-ID und das Passwort an `admin`.

In vSphere sollte auf der Registerkarte **mNode Settings** der mNode-Status als **UP** angezeigt werden, was darauf hinweist, dass der Management-Node 11.1 in vCenter registriert ist.

18. (`https://<mNode 11.1 IP address>:9443`Starten Sie vom Management Node Registration Utility) aus den SIOC-Dienst von **QoSSIOC Service Management** neu.
19. Warten Sie eine Minute und prüfen Sie die Registerkarte **NetApp Element-Konfiguration** > **mNode-Einstellungen**. Dadurch sollte der mNode-Status als **UP** angezeigt werden.

    Wenn der Status **DOWN** ist, überprüfen Sie die Berechtigungen für `/sf/packages/sioc/app.properties`. Die Datei sollte über Lese-, Schreib- und Ausführungsberechtigungen für den Dateibesitzer verfügen. Die richtigen Berechtigungen sollten wie folgt angezeigt werden:

    ```
    -rwx------
    ```

20. Nachdem der SIOC-Prozess gestartet wurde und vCenter den mNode-Status als **UP** anzeigt, überprüfen Sie die Protokolle für den `sf-hci-nma` Service auf dem Management-Knoten. Es sollten keine Fehlermeldungen vorliegen.
21. (Nur für Management-Node 11.1) SSH in den Management-Node Version 11.1 mit Root-Berechtigungen und starten den NMA-Service mit den folgenden Befehlen:

    ```
    # systemctl enable /sf/packages/nma/systemd/sf-hci-nma.service
    ```

    ```
    # systemctl start sf-hci-nma21
    ```

22. Führen Sie Aktionen aus vCenter durch, um ein Laufwerk zu entfernen, ein Laufwerk hinzuzufügen oder Nodes neu zu booten. Dadurch werden Storage-Warnmeldungen ausgelöst, die in vCenter gemeldet werden sollten. Wenn dies funktioniert, funktionieren NMA-Systemwarnungen wie erwartet.
23. Wenn ONTAP Select in vCenter konfiguriert ist, konfigurieren Sie ONTAP Select-Warnmeldungen in NMA, indem Sie die Datei vom vorherigen Management-Knoten in die Datei des Management-Knotens der Version 11.1 `/sf/packages/nma/conf/.ots.properties` kopieren `.ots.properties` und den NMA-Dienst mit dem folgenden Befehl neu starten:

    ```
    systemctl restart sf-hci-nma
    ```

24. Überprüfen Sie, ob ONTAP Select funktioniert, indem Sie die Protokolle mit dem folgenden Befehl anzeigen:

    ```
    journalctl -f | grep -i ots
    ```

25. Konfigurieren Sie Active IQ wie folgt:
    a. Wechseln Sie SSH in den Management-Node Version 11.1 und zum `/sf/packages/collector` Verzeichnis.
    b. Führen Sie den folgenden Befehl aus:

```
sudo ./manage-collector.py --set-username netapp --set-password --set
-mvip <MVIP>
```

    c. Geben Sie bei der entsprechenden Aufforderung das UI-Passwort für den Management-Node ein.
    d. Führen Sie folgende Befehle aus:

```
./manage-collector.py --get-all
```

```
sudo systemctl restart sfcollector
```

    e. Überprüfen Sie die `sfcollector` Protokolle, um sicherzustellen, dass sie funktionieren.
26. In vSphere sollte auf der Registerkarte **NetApp Element-Konfiguration** > **mNode-Einstellungen** der mNode-Status als **UP** angezeigt werden.
27. Überprüfen Sie, ob NMA Systemwarnungen und ONTAP Select-Warnungen meldet.
28. Wenn alles erwartungsgemäß funktioniert, fahren Sie herunter und löschen Sie den Management-Node 10.x VM.

Konfigurieren Sie die Authentifizierung mithilfe der REST-API des Management-Node neu

Bei einem sequenziell aktualisierten Management-Service (1) und (2) Element Storage können bestehende Management-Node weiterhin verwendet werden. Wenn Sie eine andere Upgrade-Reihenfolge eingehalten haben, lesen Sie die Verfahren für Upgrades von vorhandenen Management-Nodes.

Was Sie benötigen

- Sie haben Ihre Managementservices auf 2.10.29 oder höher aktualisiert.
- Im Storage Cluster wird Element 12.0 oder höher ausgeführt.
- Ihr Management-Node ist 11.3 oder höher.
- Sie haben Ihre Managementservices sequenziell aktualisiert und anschließend den Element Storage aktualisiert. Mit diesem Verfahren können Sie die Authentifizierung erst neu konfigurieren, wenn Sie Upgrades in der beschriebenen Reihenfolge durchgeführt haben.

Schritte

1. Öffnen Sie die REST-API-UI für den Management-Node:

```
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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.

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

3. Wählen Sie in DER REST API-Benutzeroberfläche **POST /Services/rekonfigurieren-auth** aus.
4. Wählen Sie **Probieren Sie es aus**.
5. Wählen Sie für den Parameter **load_images** `true` .
6. Wählen Sie **Ausführen**.

   Der Antwortkörper zeigt an, dass die Neukonfiguration erfolgreich war.

Weitere Informationen

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

Aktualisieren Sie das Element Plug-in für vCenter Server

Für bestehende vSphere-Umgebungen mit einem registrierten NetApp Element-Plug-in für vCenter Server können Sie Ihre Plug-in-Registrierung aktualisieren, nachdem Sie das Management-Services-Paket, das den Plug-in-Service enthält, zum ersten Mal aktualisiert haben.

Sie können die Plug-in-Registrierung auf der vCenter Server Virtual Appliance (vCSA) oder Windows mithilfe des Registrierungsprogramms aktualisieren. Sie müssen Ihre Registrierung für das vCenter Plug-in auf jedem vCenter Server ändern, auf dem Sie das Plug-in verwenden müssen.

Dieses Upgrade-Verfahren umfasst die folgenden Upgrade-Szenarien:

- Sie aktualisieren gerade auf Element Plug-in für vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6 4.5, oder 4.4.
- Sie aktualisieren gerade auf einen 7.0, 6.7 oder 6.5 HTML5 vSphere Web Client.

  Das Plug-in ist nicht mit VMware vCenter Server 6.5 für Element Plug-in für VMware vCenter Server 4.6, 4.7 und 4.8 kompatibel.

- Sie aktualisieren gerade auf einen 6.7 Flash vSphere Web Client.

  Das Plug-in ist nicht kompatibel mit Version 6.7 U2 Build 13007421 des HTML5 vSphere Web Client und anderen 6.7 U2 Builds, die vor dem Update 2a (Build 13643870) veröffentlicht wurden. Weitere Informationen zu unterstützten vSphere-Versionen finden Sie in den Versionshinweisen zu "Ihre Version des Plug-ins".

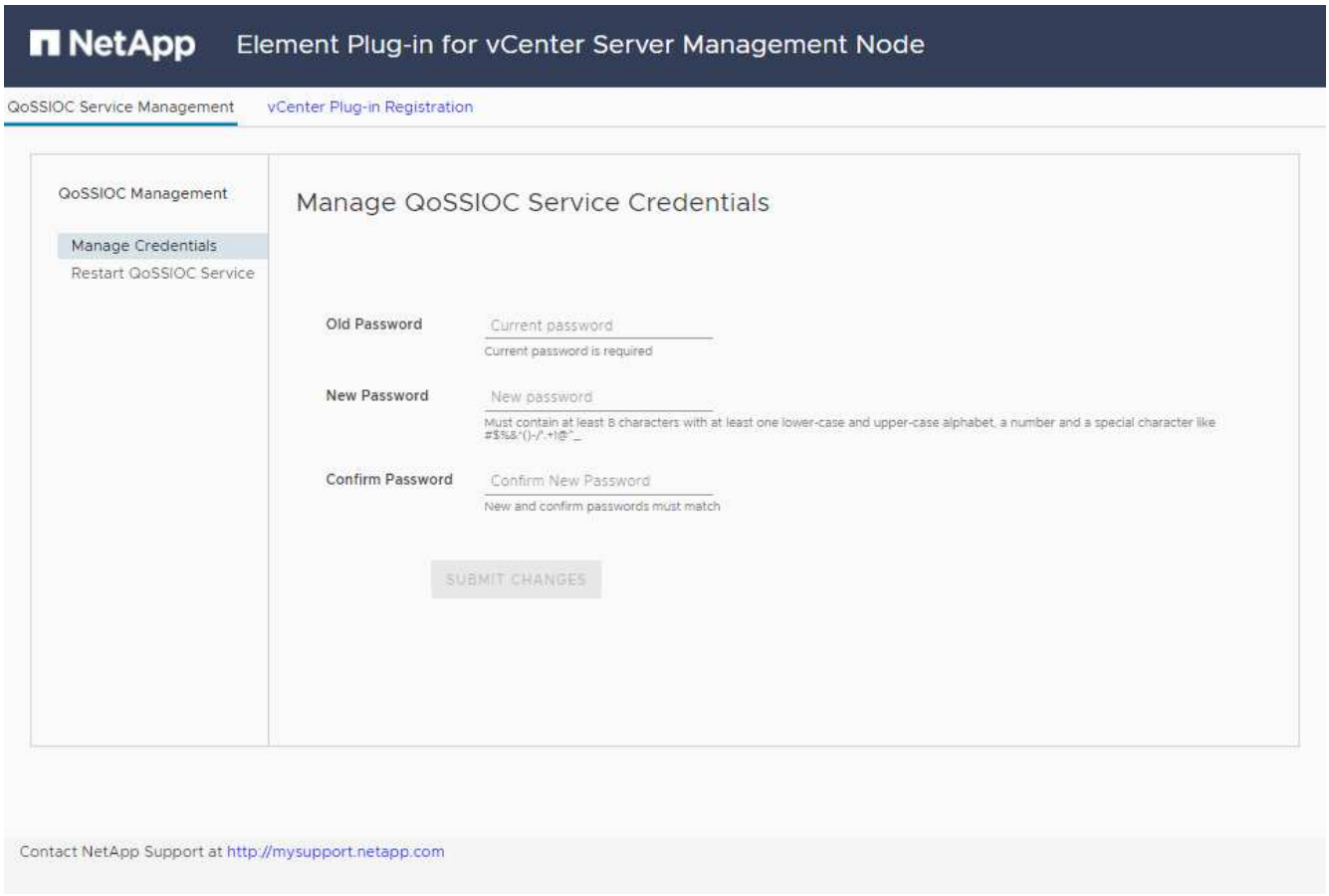
Was Sie benötigen

- **Admin-Berechtigungen**: Sie haben vCenter Administrator-Rollenberechtigungen, um ein Plug-in zu installieren.
- **VSphere Upgrades**: Sie haben alle erforderlichen vCenter Upgrades vor dem Upgrade des NetApp Element Plug-ins für vCenter Server durchgeführt. Bei diesem Verfahren wird vorausgesetzt, dass vCenter Upgrades bereits abgeschlossen wurden.

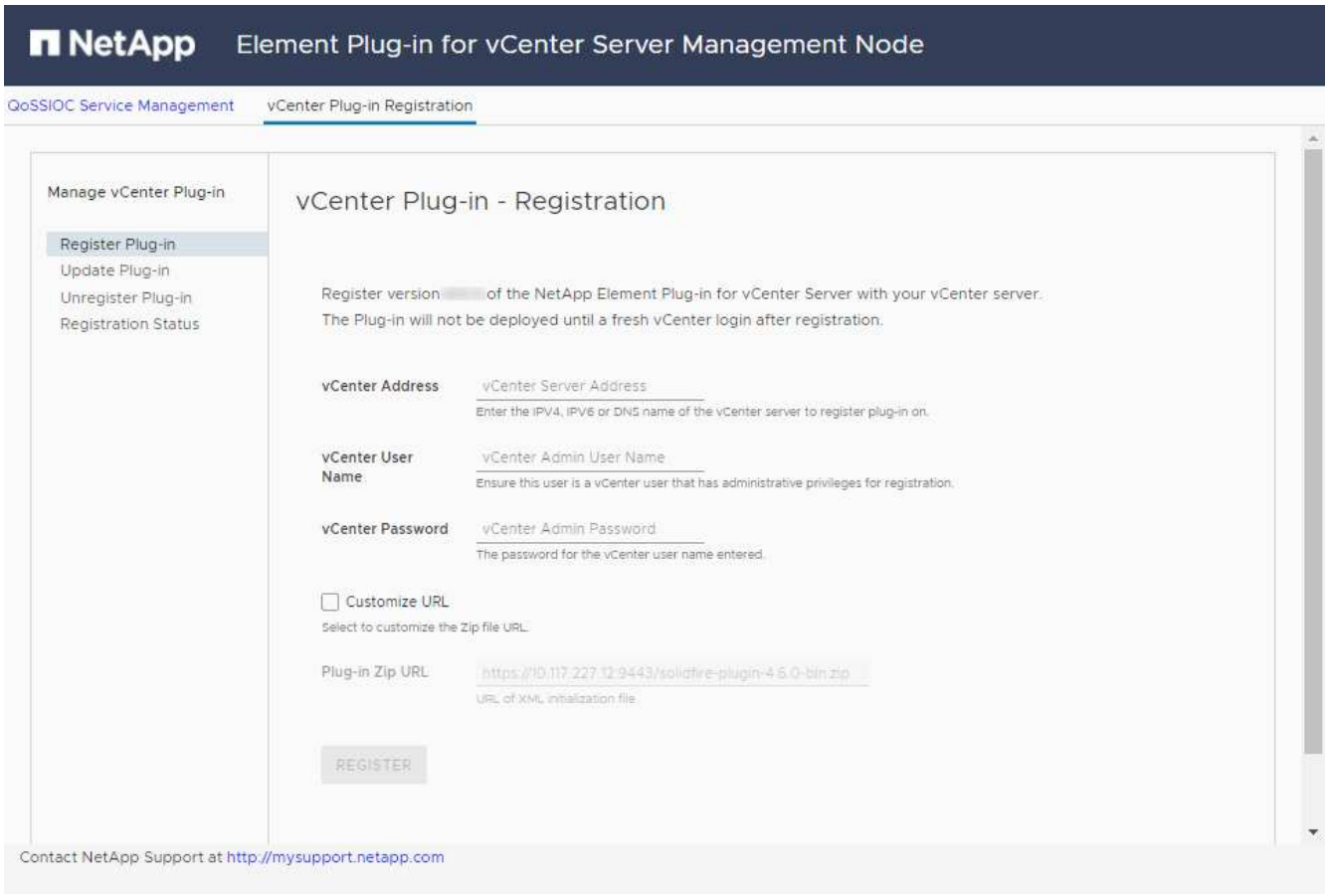
- **VCenter Server**: Ihr vCenter Plug-in Version 4.x ist bei einem vCenter Server registriert. (`https://<ManagementNodeIP>:9443`Wählen Sie im Registrierungs-Dienstprogramm **Registrierungsstatus** aus, füllen Sie die erforderlichen Felder aus, und wählen Sie **Status prüfen** aus, um zu überprüfen, ob das vCenter Plug-in bereits registriert ist und die Versionsnummer der aktuellen Installation.
- **Management Services Updates**: Sie haben Ihr auf die neueste Version aktualisiert "Management Services-Bundle". Updates des vCenter Plug-ins werden mit Updates für Management-Services außerhalb der größeren Produktversionen für NetApp HCI und SolidFire All-Flash-Storage veröffentlicht.
- **Management Node Upgrades**: Sie führen einen Management Node aus, der auf Version 11.3 oder höher war"Upgrade durchgeführt". VCenter Plug-in 4.4 oder höher erfordert einen Management Node ab Version 11.3 mit einer modularen Architektur, die individuelle Services bereitstellt. Der Management-Node muss mit seiner IP-Adresse oder der konfigurierten DHCP-Adresse eingeschaltet werden.
- **Element Storage Upgrades**: Sie haben einen Cluster mit der NetApp Element Software 11.3 oder höher.
- **VSphere Web Client**: Sie haben sich vom vSphere Web Client abgemeldet, bevor Sie ein Plug-in-Upgrade starten. Der Web-Client erkennt Updates, die während dieses Prozesses an Ihrem Plug-in vorgenommen wurden, wenn Sie sich nicht abmelden.

Schritte

1. Geben Sie die IP-Adresse Ihres Management-Knotens in einem Browser ein, einschließlich des TCP-Ports für die Registrierung:
   `https://<ManagementNodeIP>:9443` Die Registrierungsdienstoberfläche öffnet sich zur Seite **Manage QoSSIOC Service Credentials** für das Plug-in.



2. Wählen Sie **vCenter Plug-in Registrierung**.



3. Wählen Sie in **vCenter-Plug-in verwalten** die Option **Update Plug-in** aus.
4. Bestätigen oder aktualisieren Sie die folgenden Informationen:
   a. Die IPv4-Adresse oder der FQDN des vCenter-Dienstes, auf dem Sie Ihr Plug-in registrieren.
   b. Der vCenter Administrator-Benutzername.

      Der von Ihnen eingegebene Benutzername und das Kennwort müssen für einen Benutzer mit den Berechtigungen der vCenter Administrator-Rolle verwendet werden.

   c. Das vCenter Administrator-Passwort.
   d. (Für interne Server/dunkle Sites) Eine benutzerdefinierte URL für das Plug-in ZIP.

      Sie können **Benutzerdefinierte URL** wählen, um die URL anzupassen, wenn Sie einen HTTP- oder HTTPS-Server (dunkle Site) verwenden oder den ZIP-Dateinamen oder die Netzwerkeinstellungen geändert haben. Weitere Konfigurationsschritte, wenn Sie eine URL anpassen möchten, finden Sie in der Dokumentation zum Element Plug-in für vCenter Server zum Ändern von vCenter-Eigenschaften für einen internen HTTP-Server (Dark Site).

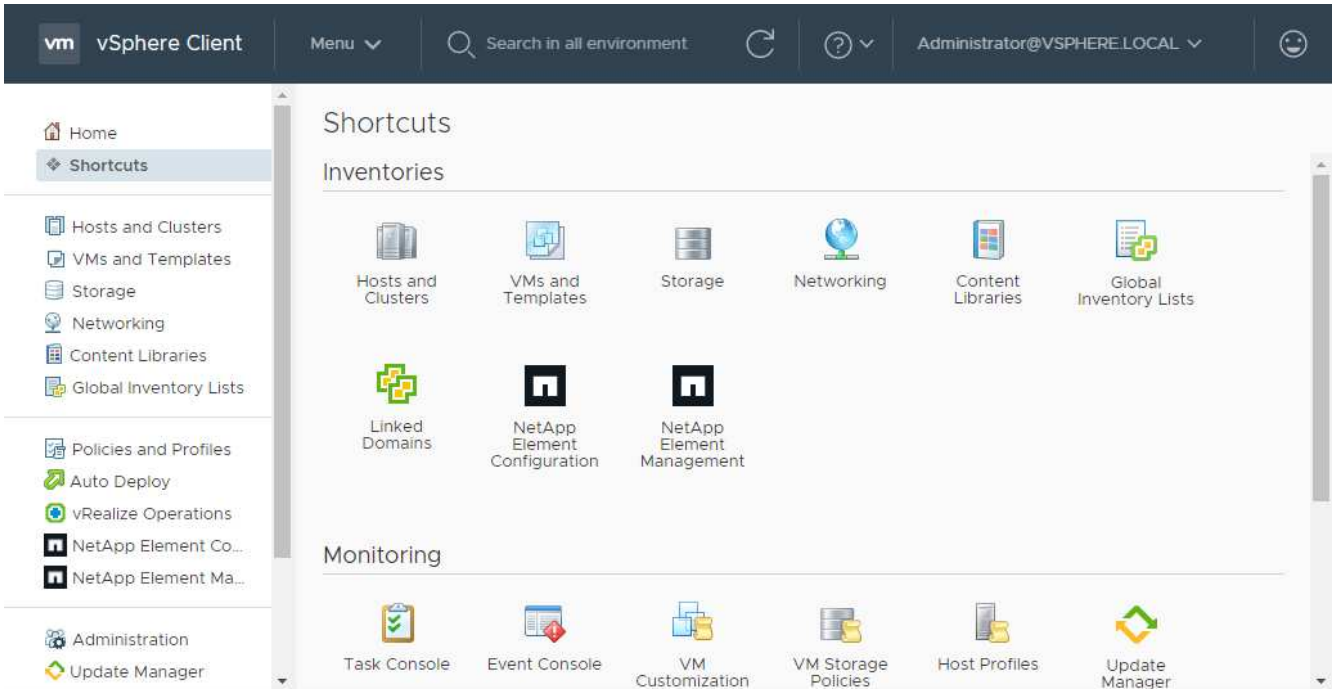
5. Wählen Sie **Aktualisieren**.

   Ein Banner erscheint in der Benutzeroberfläche des Registrierungsprogramms, wenn die Registrierung erfolgreich ist.

6. Melden Sie sich beim vSphere Web Client als vCenter Administrator an. Wenn Sie bereits beim vSphere Web Client angemeldet sind, müssen Sie sich zunächst abmelden und dann erneut anmelden.

Durch diese Aktion wird eine neue Datenbank erstellt und die Installation im vSphere Web Client abgeschlossen.

7. Suchen Sie im vSphere Web Client nach den folgenden abgeschlossenen Aufgaben in der Tasküberwachung, um sicherzustellen, dass die Installation abgeschlossen ist: `Download plug-in` Und `Deploy plug-in`.
8. Stellen Sie sicher, dass die Erweiterungspunkte für NetApp Element-Konfiguration und -Verwaltung auf der Registerkarte **Shortcuts** des vSphere Web Clients und im Seitenbedienfeld angezeigt werden.



Wenn die vCenter Plug-in-Symbole nicht angezeigt werden, lesen Sie die "Element Plug-in für vCenter Server" Dokumentation zur Fehlerbehebung beim Plug-in.

Nach dem Upgrade auf das NetApp Element-Plug-in für vCenter Server 4.8 oder höher mit VMware vCenter Server 6.7U1, wenn die Speicher-Cluster nicht aufgeführt sind oder ein Serverfehler in den Abschnitten **Cluster** und **QoSSIOC-Einstellungen** der NetApp Element-Konfiguration angezeigt wird, lesen Sie die "Element Plug-in für vCenter Server" Dokumentation zur Fehlerbehebung dieser Fehler.

9. Überprüfen Sie die Versionsänderung auf der Registerkarte **über** im Erweiterungspunkt * NetApp Element Konfiguration* des Plug-ins.

   Die folgenden Versionsdetails bzw. Details zu einer neueren Version sollten angezeigt werden:

```
NetApp Element Plug-in Version: 4.10
NetApp Element Plug-in Build Number: 12
```

Das vCenter Plug-in enthält Online-Hilfeinhalte. Um sicherzustellen, dass Ihre Hilfe die neuesten Inhalte enthält, löschen Sie Ihren Browser-Cache, nachdem Sie Ihr Plug-in aktualisiert haben.

Weitere Informationen

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

Vor einem Upgrade der Computing-Firmware müssen Systemzustandsprüfungen für Computing-Nodes durchgeführt werden

Vor dem Upgrade der Computing-Firmware müssen Sie Zustandsprüfungen durchführen, um sicherzustellen, dass alle Computing-Nodes im Cluster aktualisiert werden können. Zustandsprüfungen der Computing-Nodes können nur auf Computing-Clustern von einem oder mehreren gemanagten NetApp HCI Computing-Nodes ausgeführt werden.

Was Sie benötigen

- **Management Services**: Sie haben das neueste Management Services Bundle (2.11 oder höher) aktualisiert.
- **Management Node**: Sie führen Management Node 11.3 oder höher aus.
- **Element Software**: Auf Ihrem Storage Cluster wird die NetApp Element Software 11.3 oder höher ausgeführt.
- **Endbenutzer-Lizenzvereinbarung (EULA)**: Ab Management Services 2.20.69 müssen Sie die EULA akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder API verwenden, um Zustandsprüfungen für Computing-Nodes auszuführen:
  a. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

  b. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
  c. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
  d. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Optionen zur Zustandsprüfung

Sie können Zustandsprüfungen mithilfe der NetApp Hybrid Cloud Control (HCC) UI oder der HCC API ausführen:

- um vor einem Firmware-Upgrade Zustandsprüfungen der Computing-Nodes auszuführen (Bevorzugte Methode)
- Verwenden Sie API zum Ausführen von Zustandsprüfungen des Computing-Nodes vor einem Firmware-Upgrade

Weitere Informationen zu Zustandsprüfungen der Computing-Nodes, die vom Service ausgeführt werden:

- die vom Service durchgeführt werden

Nutzen Sie NetApp Hybrid Cloud Control, um vor einem Firmware-Upgrade Zustandsprüfungen der Computing-Nodes auszuführen

Mit NetApp Hybrid Cloud Control (HCC) können Sie überprüfen, ob ein Compute-Node für ein Firmware-Upgrade bereit ist.

> Wenn Sie mehrere Storage-Cluster-Konfigurationen mit zwei Nodes haben, jedes in ihrem eigenen vCenter, wird der Zustand von Witness Nodes möglicherweise nicht akkurat gemeldet. Wenn Sie also zum Upgrade von ESXi Hosts bereit sind, müssen Sie nur den Witness Node auf dem ESXi Host herunterfahren, der aktualisiert wird. Sie müssen sicherstellen, dass in Ihrer NetApp HCI-Installation immer ein Witness Node ausgeführt wird, indem Sie die Witness Nodes auf andere Weise ausschalten.

Schritte

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

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

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite **Upgrades** die Registerkarte **Compute Firmware** aus.
5. Wählen Sie die Integritätsprüfung für das Cluster aus  , das Sie auf die Upgrade-Bereitschaft prüfen möchten.
6. Wählen Sie auf der Seite **Integritätsprüfung berechnen** die Option **Integritätsprüfung ausführen**.
7. Wenn Probleme auftreten, wird auf der Seite ein Bericht angezeigt. Gehen Sie wie folgt vor:
   a. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus.
   b. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus.
   c. Wählen Sie nach der Behebung von Cluster-Problemen die Option **Integritätsprüfung erneut ausführen** aus.

Nachdem die Integritätsprüfung ohne Fehler abgeschlossen wurde, können die Computing-Nodes im Cluster aktualisiert werden. Weitere Informationen finden Sie unter"Aktualisiert die Computing-Node-Firmware".

Verwenden Sie API zum Ausführen von Zustandsprüfungen des Computing-Nodes vor einem Firmware-Upgrade

Mithilfe DER REST-API können Sie überprüfen, ob die Computing-Nodes in einem Cluster aktualisiert werden können. Bei der Integritätsprüfung werden keine Hindernisse für das Upgrade beseitigt, z. B. Probleme mit ESXi Hosts oder andere Probleme mit vSphere. Daher müssen Sie für jedes Computing-Cluster in Ihrer Umgebung Zustandsprüfungen der Computing-Nodes durchführen.

Schritte

1. Suchen Sie die Controller-ID und die Cluster-ID:
   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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.
   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
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 Antworttext von Code 200 die für die Installation, die `"id"` Sie für die Integritätsprüfungen verwenden möchten.
g. Wählen Sie in DER REST-API-Benutzeroberfläche **GET /installations/{id}** aus.
h. Wählen Sie **Probieren Sie es aus**.
i. Geben Sie die Installations-ID ein.
j. Wählen Sie **Ausführen**.
k. Kopieren Sie aus dem Code 200-Antwortkörper die IDs für die folgenden Elemente:
   i. Die Cluster-ID (`"clusterID"`)
   ii. Eine Controller-ID (`"controllerId"`)

```
{
  "_links": {
    "collection":
"https://10.117.187.199/inventory/1/installations",
    "self":
"https://10.117.187.199/inventory/1/installations/xx94f6f0-12a6-
412f-8b5e-4cf2z58329x0"
  },
  "compute": {
    "errors": [],
    "inventory": {
      "clusters": [
        {
          "clusterId": "domain-1",
          "controllerId": "abc12c3a-aa87-4e33-9f94-xx588c2cdcf6",
          "datacenterName": "NetApp-HCI-Datacenter-01",
          "installationId": "xx94f6f0-12a6-412f-8b5e-
4cf2z58329x0",
          "installationName": "test-nde-mnode",
          "inventoryType": "managed",
          "name": "NetApp-HCI-Cluster-01",
          "summary": {
            "nodeCount": 2,
            "virtualMachineCount": 2
          }
        }
      ],
```

2. Führen Sie Zustandsprüfungen auf den Computing-Nodes im Cluster durch:

   a. Öffnen SIE DIE REST API-UI für den Computing-Service auf dem Management-Node:

      ```
      https://<ManagementNodeIP>/vcenter/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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.

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

   c. Wählen Sie **POST /compute/{CONTROLLER_ID}/Health-Checks** aus.

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

   e. Geben Sie den aus dem vorherigen Schritt kopierten in das Parameterfeld **Controller_ID** ein `"controllerId"`.

f. Geben Sie in der Nutzlast den Wert ein, den `"clusterId"` Sie aus dem vorherigen Schritt kopiert `"cluster"` haben, und entfernen Sie den `"nodes"` Parameter.

```
{
  "cluster": "domain-1"
}
```

g. Wählen Sie **Ausführen**, um eine Integritätsprüfung auf dem Cluster auszuführen.

Die Antwort von Code 200 gibt eine `"resourceLink"` URL mit der Task-ID an, die zur Bestätigung der Ergebnisse der Integritätsprüfung erforderlich ist.

```
{
  "resourceLink": "https://10.117.150.84/vcenter/1/compute/tasks/[This
is the task ID for health check task results]",
  "serviceName": "vcenter-v2-svc",
  "taskId": "ab12c345-06f7-42d7-b87c-7x64x56x321x",
  "taskName": "VCenter service health checks"
}
```

a. Kopieren Sie den Task-ID-Teil der `"resourceLink"` URL, um das Aufgabenergebnis zu überprüfen.

3. Überprüfen Sie die Ergebnisse der Zustandsprüfungen:

a. Zurück zur REST-API-UI für den Computing-Service auf dem Management-Node:

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

b. Wählen Sie **GET /compute/Tasks/{Task_id}** aus.

c. Wählen Sie **Probieren Sie es aus**.

d. Geben Sie den Task-ID-Teil der URL aus der Antwort **POST /compute/{CONTROLLER_ID}/Health-Checks** Code 200 in das `task_id` Parameterfeld ein `"resourceLink"`.

e. Wählen Sie **Ausführen**.

f. Wenn der zurückgegeben zeigt, dass Probleme im Zusammenhang mit dem `status` Zustand des Compute-Node aufgetreten sind, gehen Sie wie folgt vor:

i. Gehen Sie zu den einzelnen KB-Artikel (`KbLink`) für jedes Problem aufgeführt oder führen Sie die angegebene Abhilfe.

ii. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus.

iii. Nachdem Sie Cluster-Probleme behoben haben, führen Sie erneut **POST /compute /{CONTROLLER_ID}/Health-Checks** aus (siehe Schritt 2).

Wenn die Zustandsprüfung ohne Probleme abgeschlossen wurde, weist der Antwortcode 200 auf ein erfolgreiches Ergebnis hin.

Zustandsprüfungen des Computing-Node, die vom Service durchgeführt werden

Ob durch HCC- oder API-Methoden ausgeführte Compute-Zustandsprüfungen machen die folgenden Überprüfungen pro Node. Je nach Umgebung können einige dieser Prüfungen übersprungen werden. Sie sollten die Integritätsprüfungen erneut durchführen, nachdem Sie erkannte Probleme behoben haben.

Prüfen Sie die Beschreibung	Node/Cluster getestet	Aktion erforderlich, um zu lösen	Knowledgebase-Artikel mit Verfahren
Ist DRS aktiviert und vollständig automatisiert?	Cluster	Aktivieren Sie DRS, und stellen Sie sicher, dass es vollständig automatisiert ist.	"Siehe diesen KB". HINWEIS: Wenn Sie über eine Standardlizenz verfügen, versetzen Sie den ESXi Host in den Wartungsmodus und ignorieren Sie diese Fehlerwarnung bei der Integritätsprüfung.
Ist DPM in vSphere deaktiviert?	Cluster	Distributed Power Management deaktivieren.	"Siehe diesen KB".
Ist die HA-Zugangskontrolle in vSphere deaktiviert?	Cluster	Schalten Sie die HA-Zugangskontrolle aus.	"Siehe diesen KB".
IST FT für eine VM auf einem Host im Cluster aktiviert?	Knoten	Unterbrechen Sie die Fehlertoleranz auf allen betroffenen virtuellen Maschinen.	"Siehe diesen KB".
Gibt es in vCenter kritische Alarme für den Cluster?	Cluster	Starten Sie vSphere, und beheben Sie alle Warnmeldungen, bevor Sie fortfahren.	Es ist kein KB zum Beheben des Problems erforderlich.
Gibt es allgemeine/globale Informationsmeldungen in vCenter?	Cluster	Starten Sie vSphere, und beheben Sie alle Warnmeldungen, bevor Sie fortfahren.	Es ist kein KB zum Beheben des Problems erforderlich.
Sind Management-Services auf dem neuesten Stand?	HCI-System	Sie müssen Managementservices aktualisieren, bevor Sie ein Upgrade durchführen oder vor dem Upgrade eine Integritätsprüfung durchführen.	Es ist kein KB zum Beheben des Problems erforderlich. Weitere Informationen finden Sie unter "Diesen Artikel" .
Gibt es Fehler auf dem aktuellen ESXi Knoten in vSphere?	Knoten	Starten Sie vSphere, und beheben Sie alle Warnmeldungen, bevor Sie fortfahren.	Es ist kein KB zum Beheben des Problems erforderlich.

Prüfen Sie die Beschreibung	Node/Cluster getestet	Aktion erforderlich, um zu lösen	Knowledgebase-Artikel mit Verfahren
Sind virtuelle Medien auf eine VM auf einem Host im Cluster eingebunden?	Knoten	Heben Sie die Bereitstellung aller virtuellen Datenträger (CD/DVD/Diskette) von den VMs ab.	Es ist kein KB zum Beheben des Problems erforderlich.
Ist die BMC-Version die erforderliche Mindestversion, die Rotbarsch unterstützt?	Knoten	Aktualisieren Sie Ihre BMC-Firmware manuell.	Es ist kein KB zum Beheben des Problems erforderlich.
Ist ESXi Host eingerichtet und läuft?	Knoten	Starten Sie Ihren ESXi-Host.	Es ist kein KB zum Beheben des Problems erforderlich.
Befinden sich Virtual Machines im lokalen ESXi Storage?	Node/VM	Entfernen oder migrieren Sie lokalen Speicher, der an Virtual Machines angeschlossen ist.	Es ist kein KB zum Beheben des Problems erforderlich.
Ist BMC betriebsbereit?	Knoten	Schalten Sie Ihren BMC ein, und stellen Sie sicher, dass er mit einem Netzwerk verbunden ist, das dieser Managementknoten erreichen kann.	Es ist kein KB zum Beheben des Problems erforderlich.
Gibt es Partner-ESXi-Hosts?	Knoten	Stellen Sie einen oder mehrere ESXi-Hosts im Cluster zur Verfügung (nicht im Wartungsmodus), um virtuelle Maschinen zu migrieren.	Es ist kein KB zum Beheben des Problems erforderlich.
Können Sie eine Verbindung mit BMC über das IPMI-Protokoll herstellen?	Knoten	Aktivieren Sie IPMI-Protokoll auf Baseboard Management Controller (BMC).	Es ist kein KB zum Beheben des Problems erforderlich.
Ist der ESXi Host korrekt dem Hardware-Host (BMC) zugeordnet?	Knoten	Der ESXi-Host ist dem Baseboard Management Controller (BMC) nicht korrekt zugeordnet. Korrigieren Sie die Zuordnung zwischen ESXi Host und Hardware-Host.	Es ist kein KB zum Beheben des Problems erforderlich. Weitere Informationen finden Sie unter "Diesen Artikel" .

Prüfen Sie die Beschreibung	Node/Cluster getestet	Aktion erforderlich, um zu lösen	Knowledgebase-Artikel mit Verfahren
Wie lautet der Status der Witness Nodes im Cluster? Keine der erkannten Zeugen-Nodes ist in Betrieb.	Knoten	Ein Witness-Node wird nicht auf einem anderen ESXi-Host ausgeführt. Schalten Sie den Witness Node auf einem alternativen ESXi-Host ein, und führen Sie die Integritätsprüfung erneut aus. **Ein Witness Node muss jederzeit in der HCI-Installation laufen**.	"Siehe diesen KB"
Wie lautet der Status der Witness Nodes im Cluster? Der Witness Node ist auf diesem ESXi Host betriebsbereit und der alternative Witness Node ist nicht aktiviert.	Knoten	Ein Witness-Node wird nicht auf einem anderen ESXi-Host ausgeführt. Schalten Sie den Witness Node auf einem anderen ESXi Host ein. Wenn Sie bereit sind, ein Upgrade für diesen ESXi-Host durchzuführen, fahren Sie den Witness-Node herunter, der auf diesem ESXi-Host ausgeführt wird, und führen Sie die Integritätsprüfung erneut aus. **Ein Witness Node muss jederzeit in der HCI-Installation laufen**.	"Siehe diesen KB"
Wie lautet der Status der Witness Nodes im Cluster? Der Witness Node ist auf diesem ESXi Host ausgeführt und der alternative Node ist aktiviert, läuft aber auf demselben ESXi Host.	Knoten	Beide Witness Nodes laufen auf diesem ESXi-Host. Verschieben Sie einen Witness Node auf einen alternativen ESXi Host. Wenn Sie bereit sind, ein Upgrade für diesen ESXi-Host durchzuführen, fahren Sie den Witness-Node herunter, der auf diesem ESXi-Host verbleibt, und führen Sie die Integritätsprüfung erneut aus. **Ein Witness Node muss jederzeit in der HCI-Installation laufen**.	"Siehe diesen KB"

Prüfen Sie die Beschreibung	Node/Cluster getestet	Aktion erforderlich, um zu lösen	Knowledgebase-Artikel mit Verfahren
Wie lautet der Status der Witness Nodes im Cluster? Der Witness Node ist auf diesem ESXi Host betriebsbereit, und der alternative Witness Node wird auf einem anderen ESXi Host ausgeführt.	Knoten	Ein Witness-Node wird lokal auf diesem ESXi-Host ausgeführt. Wenn Sie bereit sind, ein Upgrade für diesen ESXi-Host durchzuführen, fahren Sie den Witness-Node nur auf diesem ESXi-Host herunter, und führen Sie die Integritätsprüfung erneut aus. **Ein Witness Node muss jederzeit in der HCI-Installation laufen**.	"Siehe diesen KB"

Weitere Informationen

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

Aktualisieren von Compute-Node-Treibern

Für jeden H-Series Compute-Node können Sie die auf den Knoten verwendeten Treiber mit VMware Update Manager aktualisieren.

Was Sie benötigen

Siehe Firmware und Treiber-Matrix für Ihre Hardware unter "Unterstützte Firmware- und ESXi-Treiberversionen".

Über diese Aufgabe

Führen Sie jeweils nur einen dieser Aktualisierungsvorgänge aus.

Schritte

1. Navigieren Sie zur "NetApp HCI Software-Downloads" Seite, und wählen Sie den Download-Link für die richtige Version von NetApp HCI.
2. Wählen Sie in der Dropdown-Liste * ESXI_drivers* aus.
3. Akzeptieren Sie die Endnutzer-Lizenzvereinbarung.
4. Laden Sie das Treiberpaket für den Node-Typ und die ESXi-Version herunter.
5. Extrahieren Sie das heruntergeladene Treiberpaket auf Ihrem lokalen Computer.

   Das NetApp Treiber-Paket enthält mindestens eine ZIP-Datei des VMware Offline Bundle; extrahieren Sie diese ZIP-Dateien nicht.

6. Nachdem Sie die Firmware auf den Rechenknoten aktualisiert haben, gehen Sie zu **VMware Update Manager** in VMware vCenter.
7. Importieren Sie die Treiber-Offline-Bundle-Datei für die Compute-Knoten in das **Patch-Repository**.

- Für VMware ESXi 7.0 sind alle erforderlichen Treiber für die Compute-Nodes NetApp H610C, H615C, H410C und Hx00E und ihre integrierten Systemkomponenten im Standard-ISO-Image für die Installation von VMware ESXi 7.0 enthalten. Es sind keine zusätzlichen oder aktualisierten Treiber für NetApp HCI-Rechenknoten erforderlich, auf denen VMware ESXi 7.0 (und Updates) ausgeführt wird.
- Führen Sie für VMware ESXi 6.x die folgenden Schritte durch, um die Treiber-Offline-Paketdatei zu importieren:
  i. Wählen Sie die Registerkarte **Updates** aus.
  ii. WÄHLEN SIE **UPLOAD AUS DATEI**.
  iii. Navigieren Sie zu dem Offline-Paket, das zuvor heruntergeladen wurde, und wählen Sie **IMPORT**.

8. Erstellen einer neuen Host-Baseline für den Computing-Node
9. Wählen Sie **Host Extension** für Name und Typ und wählen Sie alle importierten Treiberpakete aus, die in die neue Baseline aufgenommen werden sollen.
10. Wählen Sie im Menü **Host und Cluster** in vCenter den Cluster mit den Compute Nodes aus, die Sie aktualisieren möchten, und navigieren Sie zur Registerkarte **Update Manager**.
11. Wählen Sie **optimieren** und wählen Sie die neu erstellte Host-Baseline aus. Stellen Sie sicher, dass die in der Basislinie enthaltenen Treiber ausgewählt sind.
12. Gehen Sie mit dem Assistenten zu den Optionen für die Fehlerbehebung * des Hosts durch und stellen Sie sicher, dass die Option **VM Power State** nicht ändern ausgewählt ist, um virtuelle Maschinen während der Treiberaktualisierung online zu halten.

> Wenn der VMware Distributed Resource Scheduler (DRS) auf dem Cluster aktiviert ist (dies ist die Standardeinstellung in NetApp HCI-Installationen), werden virtuelle Maschinen automatisch zu anderen Knoten im Cluster migriert.

13. Gehen Sie im Assistenten zur Seite **bereit zum Abschließen** und wählen Sie **Fertig**.

    Die Treiber für alle Computing-Nodes im Cluster werden jeweils um einen Node aktualisiert, während Virtual Machines online bleiben.

Weitere Informationen

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

Aktualisiert die Firmware der Computing-Node

Bei H-Series Computing-Nodes können Sie die Firmware für Hardwarekomponenten wie BMC, BIOS und NIC aktualisieren. Für ein Upgrade der Firmware von Computing-Nodes können Sie die Benutzeroberfläche von NetApp Hybrid Cloud Control, DIE REST-API, ein USB-Laufwerk mit dem neuesten Firmware-Image oder die BMC-Benutzeroberfläche verwenden.

Nach dem Upgrade bootet der Computing-Node in ESXi hoch und funktioniert wie zuvor, wobei die Konfiguration beibehalten wird.

Was Sie benötigen

- **Compute drivers**: Sie haben Ihre Compute Node drivers aktualisiert. Wenn Computing-Node-Treiber nicht

mit der neuen Firmware kompatibel sind, wird das Upgrade nicht gestartet. Informationen zur Treiber- und Firmware-Kompatibilität finden Sie im "Interoperabilitäts-Matrix-Tool (IMT)", und auf dem neuesten Stand finden Sie wichtige Informationen zu Firmware und Treibern, die aktuell "Versionshinweise zu der computing-Node-Firmware"sind.

- **Admin-Berechtigungen**: Sie haben Cluster Administrator und BMC Administrator Berechtigungen, um das Upgrade durchzuführen.
- **System-Ports**: Bei Upgrade-Nutzung von NetApp Hybrid Cloud Control haben Sie sichergestellt, dass die erforderlichen Ports geöffnet sind. Weitere Informationen finden Sie unter "Netzwerkports" .
- **BMC- und BIOS-Mindestversionen**: Der Knoten, den Sie mit NetApp Hybrid Cloud Control aktualisieren möchten, erfüllt die folgenden Mindestanforderungen:

Modell	Minimale BMC-Version	Minimale BIOS-Version
H410C	Alle Versionen werden unterstützt (kein Upgrade erforderlich)	Alle Versionen werden unterstützt (kein Upgrade erforderlich)
H610C	3.96.07	3B01
H615C	4.68.07	3B08.CO

> H615C Computing-Nodes müssen die BMC-Firmware mithilfe des auf Version 4.68 aktualisieren, damit NetApp Hybrid Cloud Control zukünftige Firmware-Upgrades durchführen kann"bundle für computing-Firmware 2.27".

> Eine vollständige Matrix der Firmware und Treiber-Firmware für Ihre Hardware finden Sie unter "Unterstützte Firmware- und ESXi-Treiberversionen".

- **BIOS-Startreihenfolge**: Ändern Sie die Startreihenfolge im BIOS-Setup für jeden Node manuell, um sicherzustellen, dass `USB CD/DVD` sie in der Startliste angezeigt wird. Weitere Informationen finden Sie hier"Artikel".
- **BMC-Zugangsdaten**: Aktualisieren der Zugangsdaten NetApp Hybrid Cloud Control verwendet, um eine Verbindung zum BMC des Computing-Nodes herzustellen. Hierzu können Sie entweder die NetApp Hybrid Cloud Control "UI" oder "API"verwenden. Durch Aktualisieren der BMC-Informationen vor dem Upgrade wird der Bestand aktualisiert und sichergestellt, dass Management-Node-Services über alle Hardwareparameter informiert sind, die zum Abschluss des Upgrades erforderlich sind.
- **Angeschlossene Medien**: Trennen Sie alle physischen USB- oder ISO-Geräte, bevor Sie ein Upgrade der Rechenknoten starten.
- **KVM ESXi Console**: Schließen Sie alle offenen SOL-Sitzungen und aktiven KVM-Sitzungen in der BMC-Benutzeroberfläche, bevor Sie ein Upgrade von Computing-Knoten starten.
- **Witness Node-Anforderungen**: In zwei- und drei-Knoten-Speicher-Clustern muss jeweils einer "Witness Node"in der NetApp HCI-Installation ausgeführt werden.
- **Integritätsprüfung für Compute-Knoten**: Sie haben überprüft, ob der Knoten bereit für ein Upgrade ist. Siehe "Vor einem Upgrade der Computing-Firmware müssen Systemzustandsprüfungen für Computing-Nodes durchgeführt werden".
- **Endbenutzer-Lizenzvertrag (EULA)**: Ab Management Services 2.20.69 müssen Sie die EULA akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder API zum Upgrade der Computing-Node-Firmware verwenden:

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

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

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

c. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.

d. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Über diese Aufgabe

Aktualisieren Sie in Produktionsumgebungen die Firmware auf jeweils einem Computing-Node.

Der ESXi-Host muss vor Durchführung einer Integritätsprüfung und Fortsetzen der Firmware-Aktualisierung aus dem Sperrmodus entfernt werden. Weitere Informationen finden Sie unter "So deaktivieren Sie den Sperrmodus auf ESXi-Host" und "Verhalten des VMware Sperrmodus" .

Bei UI- oder API-Upgrades der NetApp Hybrid Cloud Control wird Ihr ESXi Host automatisch während des Upgrades in den Wartungsmodus versetzt, wenn Sie über die DRS-Funktion und die erforderliche Lizenzierung verfügen. Der Node wird neu gebootet, und nach Abschluss des Upgrades wird der ESXi Host aus dem Wartungsmodus entfernt. Bei USB- und BMC-UI-Optionen müssen Sie den ESXi-Host wie in jedem Verfahren beschrieben manuell in den Wartungsmodus versetzen.

Upgrade-Optionen

Wählen Sie die Option aus, die für Ihr Upgrade-Szenario relevant ist:

- Computing-Node mit der NetApp Hybrid Cloud Control UI aktualisieren (Empfohlen)
- Computing-Node mit der NetApp Hybrid Cloud Control API aktualisieren
- das mit dem neuesten Firmware-Bundle abgebildet ist
- Verwendung der Benutzeroberfläche (UI) des Baseboard Management Controller (BMC)

Computing-Node mit der NetApp Hybrid Cloud Control UI aktualisieren

Ab den Management Services 2.14 können Sie über die Benutzeroberfläche von NetApp Hybrid Cloud Control ein Computing-Node aktualisieren. Sie müssen in der Liste der Nodes den Node auswählen, der aktualisiert werden soll. Auf der Registerkarte **Aktuelle Versionen** werden die aktuellen Firmware-Versionen angezeigt und auf der Registerkarte **vorgeschlagene Versionen** werden ggf. die verfügbaren Upgrade-Versionen angezeigt.

Stellen Sie für ein erfolgreiches Upgrade sicher, dass die Integritätsprüfung auf dem vSphere-Cluster erfolgreich ist.

Das Upgrade von NIC, BIOS und BMC dauert je nach Geschwindigkeit der Netzwerkverbindung zwischen dem Management-Node und dem BMC-Host etwa 60 Minuten pro Node.

Die Verwendung der NetApp Hybrid Cloud Control UI ermöglicht das Upgrade der Computing-Firmware auf H300E/H500E/H700E Computing-Nodes nicht mehr. Für das Upgrade wird empfohlen, dass Sie ein oder das BMC-UIverwendenUSB-Laufwerk, um das Compute-Firmware-Paket zu mounten.

Was Sie benötigen

- Wenn Ihr Management-Node nicht mit dem Internet verbunden ist, haben Sie das Compute-Firmware-Paket von heruntergeladen "NetApp Support-Website".

> Sie sollten die Datei in eine `TAR` Datei extrahieren `TAR.GZ` und dann die Datei in das Compute-Firmware-Paket extrahieren `TAR`.

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 **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite **Upgrades** die Option **Firmware berechnen**.
5. Wählen Sie das Cluster aus, das Sie aktualisieren möchten.

   Die im Cluster aufgeführten Nodes werden zusammen mit den aktuellen Firmware-Versionen und neueren Versionen angezeigt, sofern ein Upgrade verfügbar ist.

6. Wählen Sie **Browse**, um das von der heruntergeladene Compute-Firmware-Paket hochzuladen "NetApp Support-Website".
7. Warten Sie, bis der Upload abgeschlossen ist. In einer Statusleiste wird der Status des Uploads angezeigt.

   > Die Datei wird im Hintergrund hochgeladen, wenn Sie vom Browser-Fenster weg navigieren.

   Nach dem erfolgreichen Hochladen und Validierungen der Datei wird eine Meldung auf dem Bildschirm angezeigt. Die Validierung kann mehrere Minuten in Anspruch nehmen.

8. Wählen Sie das Paket der Compute-Firmware aus.
9. Wählen Sie **Upgrade Starten**.

   Nachdem Sie **Upgrade starten** ausgewählt haben, werden im Fenster ggf. fehlerhafte Integritätsprüfungen angezeigt.

   > Das Upgrade kann nach dem Start nicht angehalten werden. Die Firmware wird nacheinander in der folgenden Reihenfolge aktualisiert: NIC, BIOS und BMC. Melden Sie sich während des Upgrades nicht bei der BMC-Benutzeroberfläche an. Wenn Sie sich am BMC anmelden, wird die SOL-Sitzung (Serial-over-LAN) von Hybrid Cloud Control beendet, die den Upgradeprozess überwacht.

10. Wenn die Integritätsprüfung auf Cluster- oder Node-Ebene mit Warnungen bestanden wurde, aber ohne kritische Ausfälle, wird **bereit für ein Upgrade** angezeigt. Wählen Sie **Upgrade Node**.

Während das Upgrade läuft, können Sie die Seite verlassen und zu einem späteren Zeitpunkt zurückkehren, um den Fortschritt zu überwachen. Während des Upgrades zeigt die Benutzeroberfläche verschiedene Meldungen über den Status des Upgrades an.

Öffnen Sie die SOL-Konsole (Serial-over-LAN) nicht über die BMC-Web-UI, während Sie die Firmware auf H610C-Compute-Nodes aktualisieren. Dies kann zum Fehlschlagen des Upgrades führen.

Die Benutzeroberfläche zeigt eine Meldung an, nachdem das Upgrade abgeschlossen wurde. Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist. Informationen zu den verschiedenen Änderungen des Upgrade-Status finden Sie unter Statusänderungen des Upgrades.

Wenn während des Upgrades ein Fehler auftritt, wird der Node durch NetApp Hybrid Cloud Control neu gebootet, der Wartungsmodus nicht ausgeführt und der Fehlerstatus wird über eine Verbindung zum Fehlerprotokoll angezeigt. Sie können das Fehlerprotokoll mit spezifischen Anweisungen oder Links zu KB-Artikeln herunterladen, um Probleme zu diagnostizieren und zu beheben. Weitere Informationen zu Upgrade-Problemen bei der Computing-Node-Firmware mithilfe von NetApp Hybrid Cloud Control finden Sie in diesem "KB" Artikel.

Statusänderungen des Upgrades

Hier sind die verschiedenen Status, die die UI vor, während und nach dem Upgrade-Prozess anzeigt:

Upgrade-Status	Beschreibung
Mindestens eine Zustandsprüfung des Node ist fehlgeschlagen. Erweitern, um Details anzuzeigen.	Mindestens eine Zustandsprüfung ist fehlgeschlagen.
Fehler	Während des Upgrades ist ein Fehler aufgetreten. Sie können das Fehlerprotokoll herunterladen und an den NetApp Support senden.
Erkennung nicht möglich	Dieser Status wird angezeigt, wenn NetApp Hybrid Cloud Control den Compute-Node nicht abfragen kann, wenn die Compute-Node-Ressource nicht über die Hardware-Tag-Nummer verfügt.
Ein Upgrade ist möglich.	Alle Zustandsprüfungen wurden erfolgreich bestanden und der Node kann aktualisiert werden.
Während des Upgrades ist ein Fehler aufgetreten.	Das Upgrade schlägt mit dieser Benachrichtigung fehl, wenn ein kritischer Fehler auftritt. Laden Sie die Protokolle herunter, indem Sie den Link **Download Logs** auswählen, um den Fehler zu beheben. Sie können versuchen, das Upgrade erneut zu aktualisieren, nachdem Sie den Fehler behoben haben.
Der Node wird aktualisiert.	Das Upgrade läuft. In einer Statusleiste wird der Aktualisierungsstatus angezeigt.

Computing-Node mit der NetApp Hybrid Cloud Control API aktualisieren

Mithilfe von APIs können Sie jeden Computing-Node in einem Cluster auf die neueste Firmware-Version

aktualisieren. Sie können ein Automatisierungstool Ihrer Wahl zum Ausführen der APIs verwenden. Der hier dokumentierte API-Workflow nutzt die REST-API-UI, die am Management-Node verfügbar ist.

Die Verwendung der NetApp Hybrid Cloud Control UI ermöglicht das Upgrade der Computing-Firmware auf H300E/H500E/H700E Computing-Nodes nicht mehr. Für das Upgrade wird empfohlen, dass Sie ein oder das BMC-UIverwendenUSB-Laufwerk, um das Compute-Firmware-Paket zu mounten.

Was Sie benötigen

Computing-Node-Ressourcen, einschließlich vCenter und Hardware-Assets, müssen Management-Node-Ressourcen bekannt sein. Sie können die Inventory Service APIs verwenden, um Assets (`https://<ManagementNodeIP>/inventory/1/`zu überprüfen).

Schritte

1. Rufen Sie die NetApp HCI Software "download-Seite" auf, und laden Sie das neueste Compute-Firmware-Paket auf ein Gerät herunter, auf das der Management-Node zugreifen kann.

   Bei Dark Site-Upgrades können Sie die Upload-Zeit verkürzen, wenn das Upgrade-Paket und der Management-Node lokal sind.

2. Laden Sie das Bundle der Computing-Firmware auf den Management-Node hoch:
   a. Öffnen Sie die REST-API-UI für den Management-Node:

      ```
      https://<ManagementNodeIP>/package-repository/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 `mnode-client`ein.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Autorisierungsfenster.
   c. Wählen Sie in DER REST API-Benutzeroberfläche **POST /Packages** aus.
   d. Wählen Sie **Probieren Sie es aus**.
   e. Wählen Sie **Durchsuchen** und wählen Sie das Rechner-Firmware-Bundle aus.
   f. Wählen Sie **Ausführen**, um den Upload zu initiieren.
   g. Kopieren Sie aus der Antwort die Compute Firmware Bundle ID (`"id"`) und speichern Sie sie zur Verwendung in einem späteren Schritt.
3. Überprüfen Sie den Status des Uploads.
   a. Wählen Sie in DER REST-API-Benutzeroberfläche **GET /packages/{id}/Status** aus.
   b. Wählen Sie **Probieren Sie es aus**.
   c. Geben Sie die ID des Rechenkennebels für die Firmware ein, die Sie im vorherigen Schritt in **id** kopiert haben.
   d. Wählen Sie **Ausführen**, um die Statusanforderung zu initiieren.

      Die Antwort zeigt an `state SUCCESS`, dass der Vorgang abgeschlossen ist.

e. Kopieren und speichern Sie aus der Antwort den Namen des Compute-Firmware-Bündels (`"version"`)(`"name"` und Version) für die Verwendung in einem späteren Schritt.

4. Suchen Sie die Computing-Controller-ID und die Hardware-ID des Nodes für den Node, den Sie aktualisieren möchten:

   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 `mnode-client`ein.

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

      iv. Schließen Sie das Autorisierungsfenster.

   c. Wählen Sie in DER REST API-Benutzeroberfläche **GET /Installations** aus.

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

   e. Wählen Sie **Ausführen**.

   f. Kopieren Sie aus der Antwort die Installations-Asset(`"id"`-ID).

   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. Aus der Antwort, kopieren und speichern Sie die Cluster-Controller(`"controllerId"`-ID)und Node-Hardware-ID (`"hardwareId"`) für die Verwendung in einem späteren Schritt:

   ```
   "compute": {
     "errors": [],
     "inventory": {
       "clusters": [
         {
           "clusterId": "Test-1B",
           "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
   ```

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.111.0.111",
      "credentialsAvailable": true,
      "credentialsValidated": true
    },
    "chassisSerialNumber": "111930011231",
    "chassisSlot": "D",
    "hardwareId": "123a4567-01b1-1243-a12b-11ab11ab0a15",
    "hardwareTag": "00000000-0000-0000-0000-ab1c2de34f5g",
    "id": "e1111d10-1a1a-12d7-1a23-ab1cde23456f",
    "model": "H410C",
```

5. Führen Sie das Upgrade der Computing-Node-Firmware aus:
   a. Öffnen Sie DIE REST API-UI für den Hardware-Service auf dem Management-Node:

      ```
      https://<ManagementNodeIP>/hardware/2/
      ```

   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 `mnode-client`ein.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Autorisierungsfenster.
   c. Wählen Sie **POST /Nodes/{Hardware_id}/Upgrades** aus.
   d. Wählen Sie **Probieren Sie es aus**.
   e. Geben Sie die Hardware-Host-Asset-ID ein, die aus einem vorherigen Schritt gespeichert wurde) im Parameterfeld ein(`"hardwareId"`.
   f. Führen Sie die Nutzlastwerte folgendermaßen aus:
      i. Behalten Sie die Werte `"force": false` bei `"maintenanceMode": true`, damit auf dem Node Zustandsprüfungen durchgeführt werden und der ESXi Host in den Wartungsmodus versetzt wird.
      ii. Geben Sie die aus einem vorherigen Schritt gespeicherte Cluster-Controller-ID ein(`"controllerId"`).
      iii. Geben Sie die Version des Namenspakets für das Compute-Firmware-Paket ein, die Sie aus einem vorherigen Schritt gespeichert haben.

```
{
  "config": {
    "force": false,
    "maintenanceMode": true
  },
  "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
  "packageName": "compute-firmware-12.2.109",
  "packageVersion": "12.2.109"
}
```

g. Wählen Sie **Ausführen**, um das Upgrade zu initiieren.

> Das Upgrade kann nach dem Start nicht angehalten werden. Die Firmware wird nacheinander in der folgenden Reihenfolge aktualisiert: NIC, BIOS und BMC. Melden Sie sich während des Upgrades nicht bei der BMC-Benutzeroberfläche an. Wenn Sie sich am BMC anmelden, wird die SOL-Sitzung (Serial-over-LAN) von Hybrid Cloud Control beendet, die den Upgradeprozess überwacht.

h. Kopieren Sie die Upgrade Task ID, die Teil der Resource Link (`"resourceLink"`) URL in der Antwort ist.

6. Überprüfen Sie den Aktualisierungsfortschritt und die Ergebnisse:

a. Wählen Sie **GET /Task/{Task_id}/logs** aus.

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

c. Geben Sie die Task-ID aus dem vorherigen Schritt in **Task_ID** ein.

d. Wählen Sie **Ausführen**.

e. Führen Sie einen der folgenden Schritte aus, wenn während des Upgrades Probleme oder besondere Anforderungen auftreten:

Option	Schritte
Sie müssen Probleme mit dem Clusterzustand aufgrund einer Meldung im Antworttext beheben `failedHealthChecks`.	i. Gehen Sie zu dem für jedes Problem angegebenen KB-Artikel oder führen Sie das angegebene Heilmittel aus. ii. Wenn ein KB angegeben wird, führen Sie den im entsprechenden KB-Artikel beschriebenen Prozess aus. iii. Nachdem Sie Cluster-Probleme behoben haben, authentifizieren Sie sich bei Bedarf erneut und wählen Sie **POST /Nodes/{Hardware_id}/Upgrades** aus. iv. Wiederholen Sie die Schritte wie zuvor im Aktualisierungsschritt beschrieben.

Option	Schritte
Das Upgrade schlägt fehl und die Schritte zur Risikominderung werden im Upgrade-Protokoll nicht aufgeführt.	i. Siehe hier "KB-Artikel" (Anmeldung erforderlich).

f. Führen Sie die API **GET /Task/{Task_id}/logs** mehrmals nach Bedarf aus, bis der Prozess abgeschlossen ist.

   Während der Aktualisierung zeigt das `status` an `running`, ob keine Fehler aufgetreten sind. Wenn jeder Schritt abgeschlossen ist, ändert sich der `status` Wert in `completed`.

Das Upgrade wurde erfolgreich abgeschlossen, wenn der Status für jeden Schritt lautet `completed` und der `percentageCompleted` Wert lautet `100`.

7. (Optional) Aktualisieren der Firmware-Versionen für jede Komponente bestätigen:
   a. Öffnen Sie DIE REST API-UI für den Hardware-Service auf dem Management-Node:

      ```
      https://<ManagementNodeIP>/hardware/2/
      ```

   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 `mnode-client`ein.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Autorisierungsfenster.
   c. Wählen Sie in DER REST-API-UI **GET /nodes/{Hardware_id}/Upgrades** aus.
   d. (Optional) Geben Sie Datum und Status-Parameter ein, um die Ergebnisse zu filtern.
   e. Geben Sie die Hardware-Host-Asset-ID ein, die aus einem vorherigen Schritt gespeichert wurde) im Parameterfeld ein(`"hardwareId"`.
   f. Wählen Sie **Probieren Sie es aus**.
   g. Wählen Sie **Ausführen**.
   h. Überprüfen Sie in der Antwort, ob die Firmware für alle Komponenten von der vorherigen Version auf die neueste Firmware erfolgreich aktualisiert wurde.

Verwenden Sie ein USB-Laufwerk, das mit dem neuesten Firmware-Bundle abgebildet ist

Sie können ein USB-Laufwerk mit dem neuesten Compute-Firmware-Bundle anschließen, das auf einen USB-Port des Computing-Node heruntergeladen wurde. Alternativ zur Verwendung der in diesem Verfahren beschriebenen USB-Stick-Methode können Sie das Rechner-Firmware-Bundle mit der Option **Virtual CD/DVD** in der virtuellen Konsole in der BMC-Schnittstelle (Baseboard Management Controller) auf dem Rechner-Knoten montieren. Die BMC-Methode dauert erheblich länger als die USB-Stick-Methode. Stellen Sie sicher, dass Ihre Workstation oder Ihr Server über die erforderliche Netzwerkbandbreite verfügt und dass Ihre Browsersitzung mit dem BMC nicht ausläuft.

Was Sie benötigen

- Wenn Ihr Management-Node nicht mit dem Internet verbunden ist, haben Sie das Compute-Firmware-Paket von heruntergeladen "NetApp Support-Website".

Sie sollten die Datei in eine `TAR` Datei extrahieren `TAR.GZ` und dann die Datei in das Compute-Firmware-Paket extrahieren `TAR`.

Schritte

1. Verwenden Sie das Dienstprogramm Etcher, um das Paket der Compute-Firmware auf einem USB-Laufwerk zu blinken.
2. Setzen Sie den Computing-Node mit VMware vCenter in den Wartungsmodus und evakuieren Sie alle Virtual Machines vom Host.

   Wenn der VMware Distributed Resource Scheduler (DRS) auf dem Cluster aktiviert ist (dies ist die Standardeinstellung in NetApp HCI-Installationen), werden virtuelle Maschinen automatisch zu anderen Knoten im Cluster migriert.

3. Stecken Sie das USB-Stick in einen USB-Anschluss am Compute-Node und starten Sie den Compute-Node mithilfe von VMware vCenter neu.
4. Drücken Sie während DES POST-Zyklus des Computing-Knotens **F11**, um den Boot Manager zu öffnen. Möglicherweise müssen Sie **F11** mehrmals in schneller Folge drücken. Sie können diesen Vorgang ausführen, indem Sie eine Video-/Tastatur anschließen oder die Konsole in verwenden `BMC`.
5. Wählen Sie im angezeigten Menü * One Shot* > **USB Flash Drive** aus. Wenn das USB-Stick nicht im Menü angezeigt wird, stellen Sie sicher, dass das USB-Flash-Laufwerk Teil der älteren Startreihenfolge im BIOS des Systems ist.
6. Drücken Sie **Enter**, um das System vom USB-Stick zu starten. Der Firmware-Flash-Prozess beginnt.

   Nachdem die Firmware-Aktualisierung abgeschlossen und der Node neu gebootet wurde, kann es ein paar Minuten dauern, bis ESXi gestartet wird.

7. Verlassen Sie nach Abschluss des Neubootens den Wartungsmodus auf dem aktualisierten Computing-Node mit vCenter.
8. Entfernen Sie das USB-Flash-Laufwerk vom aktualisierten Compute-Node.
9. Wiederholen Sie diesen Vorgang für andere Computing-Nodes im ESXi Cluster, bis alle Computing-Nodes aktualisiert werden.

Verwendung der Benutzeroberfläche (UI) des Baseboard Management Controller (BMC)

Sie müssen die sequenziellen Schritte durchführen, um das Computing-Firmware-Bundle zu laden und den Node auf das Computing-Firmware-Bundle neu zu booten, um sicherzustellen, dass das Upgrade erfolgreich abgeschlossen wurde. Das Paket der Rechner-Firmware sollte sich auf dem System oder der virtuellen Maschine (VM) befinden, die den Webbrowser hostet. Überprüfen Sie, ob Sie das Paket der Computing-Firmware heruntergeladen haben, bevor Sie den Prozess starten.

Es wird empfohlen, das System oder die VM und den Knoten im gleichen Netzwerk zu verwenden.

Über die BMC-UI dauert das Upgrade etwa 25 bis 30 Minuten.

- Firmware-Upgrade auf den Nodes H410C und H300E/H500E/H700E
- Firmware auf H610C/H615C Nodes aktualisieren

Firmware-Upgrade auf den Nodes H410C und H300E/H500E/H700E

Wenn der Node Teil eines Clusters ist, müssen Sie den Node vor dem Upgrade in den Wartungsmodus versetzen und nach dem Upgrade den Wartungsmodus nicht mehr aktivieren.

Ignorieren Sie die folgende Informationsmeldung, die während des Prozesses angezeigt wird: `Untrusty Debug Firmware Key is used, SecureFlash is currently in Debug Mode`

Schritte

1. Wenn der Node Teil eines Clusters ist, versetzen Sie ihn wie folgt in den Wartungsmodus. Falls nicht, fahren sie mit Schritt 2 fort.
   a. Melden Sie sich beim VMware vCenter Web-Client an.
   b. Klicken Sie mit der rechten Maustaste auf den Namen des Hosts (Compute Node) und wählen Sie **Wartungsmodus > Wartungsmodus eingeben**.
   c. Wählen Sie **OK**. VMs auf dem Host werden zu einem anderen verfügbaren Host migriert. Die VM-Migration kann je nach Anzahl der zu migrierenden VMs Zeit in Anspruch nehmen.

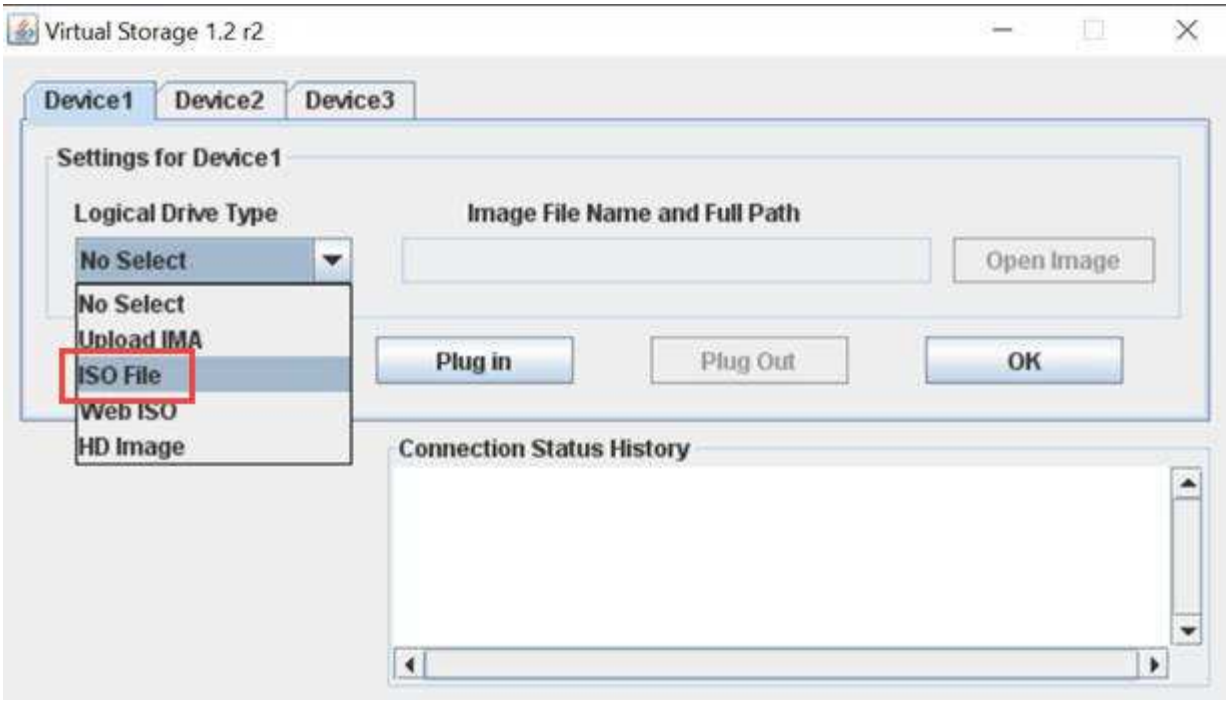
      Stellen Sie sicher, dass alle VMs auf dem Host migriert werden, bevor Sie fortfahren.

2. Navigieren Sie zur BMC-Benutzeroberfläche, `https://BMCIP/#login` wobei BMCIP die IP-Adresse des BMC ist.
3. Melden Sie sich mit Ihren Anmeldedaten an.
4. Wählen Sie **Fernbedienung > Konsolenumleitung**.
5. Wählen Sie **Einführungskonsole**.

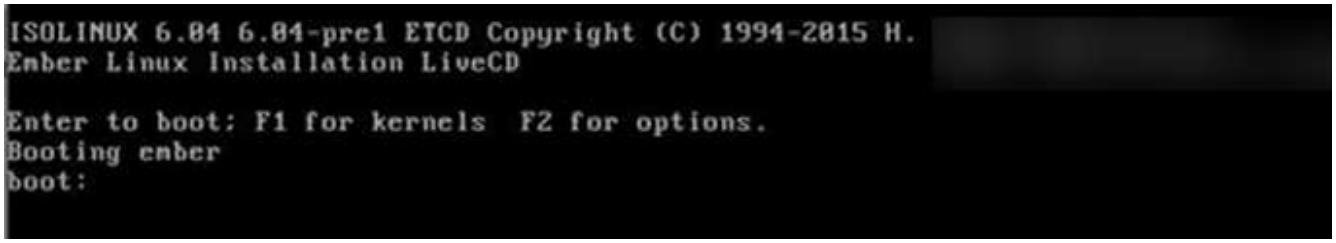
   Sie müssen vielleicht Java installieren oder aktualisieren.

6. Wenn die Konsole geöffnet wird, wählen Sie **Virtueller Datenträger > virtueller Speicher**.
7. Wählen Sie auf dem Bildschirm * Virtueller Speicher* die Option **Logischer Laufwerkstyp** aus und wählen Sie **ISO-Datei**.



8. Wählen Sie **Bild öffnen** aus, um in den Ordner zu navigieren, in dem Sie die Bundle-Datei der Rechner-Firmware heruntergeladen haben, und wählen Sie die Bundle-Datei der Compute-Firmware aus.
9. Wählen Sie **Plug-In**.
10. Wenn der Verbindungsstatus angezeigt wird `Device#: VM Plug-in OK!!`, wählen Sie **OK**.
11. Starten Sie den Knoten neu, indem Sie **F12** drücken und **Neustart** wählen oder **Power Control > Power Reset einstellen** wählen.
12. Drücken Sie während des Neustarts **F11**, um die Startoptionen auszuwählen und das Compute-Firmware-Bundle zu laden. Möglicherweise müssen Sie F11 ein paar Mal drücken, bevor das Startmenü angezeigt wird.

    Das folgende Fenster wird angezeigt:



13. Drücken Sie auf dem obigen Bildschirm **Enter**. Je nach Netzwerk kann es einige Minuten dauern, nachdem Sie **Enter** drücken, um das Upgrade zu starten.

> Einige Firmware-Upgrades können dazu führen, dass die Konsole getrennt wird und/oder Ihre Sitzung auf dem BMC die Verbindung getrennt. Sie können sich wieder beim BMC anmelden, jedoch sind einige Dienste, wie z. B. die Konsole, aufgrund der Firmware-Upgrades möglicherweise nicht verfügbar. Nach Abschluss der Upgrades führt der Node ein Kaltstart durch, das ca. fünf Minuten dauern kann.

14. Melden Sie sich wieder bei der BMC-Benutzeroberfläche an und wählen Sie **System** aus, um die BIOS-Version und die Erstellungszeit nach dem Starten des Betriebssystems zu überprüfen. Wenn das Upgrade

korrekt abgeschlossen wurde, werden die neuen BIOS- und BMC-Versionen angezeigt.

> Die aktualisierte Version wird in der BIOS-Version erst angezeigt, wenn der Node vollständig gebootet wurde.

15. Wenn der Node Teil eines Clusters ist, führen Sie die folgenden Schritte aus. Wenn es sich um einen Standalone-Node handelt, sind keine weiteren Maßnahmen erforderlich.
    a. Melden Sie sich beim VMware vCenter Web-Client an.
    b. Beenden Sie den Wartungsmodus des Hosts. Dies kann eine nicht verbundene rote Markierung anzeigen. Warten Sie, bis alle Status gelöscht sind.
    c. Schalten Sie eine der restlichen VMs ein, die ausgeschaltet waren.

Firmware auf H610C/H615C Nodes aktualisieren

Die Schritte hängen davon ab, ob der Node Standalone oder Teil eines Clusters ist. Der Vorgang dauert etwa 25 Minuten und beinhaltet das Ausschalten des Node, das Hochladen des Bundle der Datenverarbeitungs-Firmware, das Flashen der Geräte und das Einschalten des Node nach dem Upgrade.

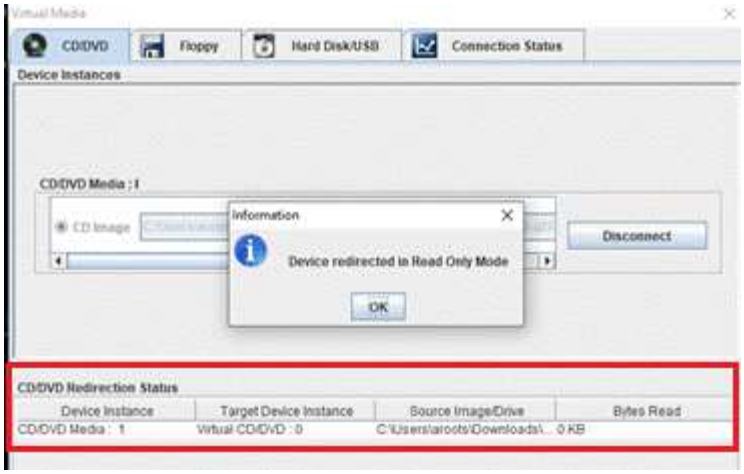
Schritte

1. Wenn der Node Teil eines Clusters ist, versetzen Sie ihn wie folgt in den Wartungsmodus. Falls nicht, fahren sie mit Schritt 2 fort.
    a. Melden Sie sich beim VMware vCenter Web-Client an.
    b. Klicken Sie mit der rechten Maustaste auf den Namen des Hosts (Compute Node) und wählen Sie **Wartungsmodus > Wartungsmodus eingeben**.
    c. Wählen Sie **OK**. VMs auf dem Host werden zu einem anderen verfügbaren Host migriert. Die VM-Migration kann je nach Anzahl der zu migrierenden VMs Zeit in Anspruch nehmen.

    > Stellen Sie sicher, dass alle VMs auf dem Host migriert werden, bevor Sie fortfahren.

2. Navigieren Sie zur BMC-Benutzeroberfläche, `https://BMCIP/#login` wobei BMC IP die IP-Adresse des BMC ist.
3. Melden Sie sich mit Ihren Anmeldedaten an.
4. Wählen Sie **Fernbedienung > KVM (Java) starten**.
5. Wählen Sie im Konsolenfenster **Medien > Assistent für virtuelle Datenträger** aus.

6. Wählen Sie **Browse** und wählen Sie die Compute-Firmware- `.iso`Datei aus.
7. Wählen Sie **Verbinden**. Es wird ein Popup-Fenster angezeigt, in dem der Erfolg angezeigt wird. Der Pfad und das Gerät werden unten angezeigt. Sie können das Fenster * Virtual Media* schließen.



8. Starten Sie den Knoten neu, indem Sie **F12** drücken und **Neustart** wählen oder **Power Control > Power Reset einstellen** wählen.
9. Drücken Sie während des Neustarts **F11**, um die Startoptionen auszuwählen und das Compute-Firmware-Bundle zu laden.
10. Wählen Sie in der angezeigten Liste * AMI Virtual CD-ROM* aus und wählen Sie **Enter**. Wenn Sie die virtuelle AMI-CD-ROM in der Liste nicht sehen, gehen Sie zum BIOS und aktivieren Sie sie in der Startliste. Der Node wird nach dem Speichern neu gebootet. Drücken Sie während des Neustarts **F11**.
11. Wählen Sie auf dem angezeigten Bildschirm **Enter** aus.

> Einige Firmware-Upgrades können dazu führen, dass die Konsole getrennt wird und/oder Ihre Sitzung auf dem BMC die Verbindung getrennt. Sie können sich wieder am BMC anmelden. Einige Services, z. B. die Konsole, sind aufgrund der Firmware-Upgrades möglicherweise nicht verfügbar. Nach Abschluss der Upgrades führt der Node ein Kaltstart durch, das ca. fünf Minuten dauern kann.

12. Wenn Sie die Verbindung zur Konsole getrennt haben, wählen Sie **Fernbedienung** und wählen Sie **KVM starten** oder **KVM starten (Java)** aus, um die Verbindung wiederherzustellen und zu überprüfen, wann der Knoten den Startvorgang abgeschlossen hat. Möglicherweise müssen Sie mehrere erneute Verbindungen einrichten, um zu überprüfen, ob der Node erfolgreich gebootet wurde.

> Während des Einschaltvorgangs etwa fünf Minuten lang zeigt die KVM-Konsole **kein Signal** an.

13. Wählen Sie nach dem Einschalten des Knotens **Dashboard > Geräteinformationen > Weitere Informationen** aus, um die BIOS- und BMC-Versionen zu überprüfen. Die aktualisierten BIOS- und BMC-Versionen werden angezeigt. Die aktualisierte Version des BIOS wird erst angezeigt, wenn der Knoten vollständig gestartet wurde.
14. Wenn Sie den Knoten in den Wartungsmodus versetzt haben, nachdem der Knoten in ESXi gebootet wurde, klicken Sie mit der rechten Maustaste auf den Host-Namen (Compute Node) und wählen Sie **Wartungsmodus > Wartungsmodus beenden** aus, und migrieren Sie die VMs zurück zum Host.
15. Konfigurieren und überprüfen Sie in vCenter mit dem ausgewählten Hostnamen die BIOS-Version.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"

- "Seite „NetApp HCI Ressourcen“"

Aktualisieren Sie Ihre vSphere Komponenten für ein NetApp HCI System mit dem Element Plug-in für vCenter Server

Wenn Sie die VMware vSphere Komponenten Ihrer NetApp HCI Installation aktualisieren, sind für das Element Plug-in für vCenter Server einige zusätzliche Schritte erforderlich.

Schritte

1. Für vCSA-Upgrades, "Löschen" QoSSIOC-Einstellungen im Plug-in (**NetApp Element-Konfiguration > QoSSIOC-Einstellungen**). Das Feld **QoSSIOC Status** wird nach Abschluss des Vorgangs angezeigt `Not Configured`.
2. Für vCSA- und Windows-Upgrades ist "Deregistrieren" das Plug-in vom vCenter Server, mit dem es über das Registrierungs-Dienstprogramm verknüpft ist, erforderlich.
3. "Aktualisieren Sie vSphere einschließlich vCenter Server, ESXi, VMs und anderen VMware Komponenten".

   Wenn Sie ein Upgrade auf VMware vCenter Server 7.0 U3 durchführen, kann das Element Plug-in nicht bereitgestellt werden. Informationen zur Behebung dieses Problems mit Hilfe des Frühjahrsrahmens 4 finden Sie unter "Diesen KB-Artikel".

   Wenn Sie ESXi für Compute-Nodes für einen "Cluster mit zwei Nodes" aktualisieren, aktualisieren Sie jeweils nur einen Compute-Node, sodass nur ein Witness-Node vorübergehend nicht verfügbar ist und das Cluster-Quorum beibehalten werden kann.
4. "Registrieren" Das Element Plug-in für vCenter Server erneut mit vCenter.
5. "Fügen Sie Cluster hinzu" Verwenden des Plug-ins.
6. "Konfigurieren Sie die QoSSIOC-Einstellungen" Verwenden des Plug-ins.
7. "QoSSIOC aktivieren" Für alle vom Plug-in gesteuerten Datenspeicher.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"
- "Technischer Bericht: NetApp HCI Two-Node Storage Cluster"

Erweitern Sie Ihr NetApp HCI System

Übersicht über die Erweiterung

Erweitern Sie Ihr NetApp HCI System mithilfe von NetApp Hybrid Cloud Control. Storage- und Computing-Ressourcen lassen sich separat erweitern oder gleichzeitig erweitern.

Neue und Ersatz-H610S Storage-Nodes weisen möglicherweise zusätzliche Installationsanforderungen auf Grundlage der vorhandenen Element Softwareversion des Storage-Clusters auf. Weitere Informationen erhalten Sie von Ihrem NetApp Support.

Nach der Installation des Node im NetApp HCI-Chassis verwenden Sie NetApp Hybrid Cloud Control, um NetApp HCI für die Verwendung der neuen Ressourcen zu konfigurieren. NetApp HCI erkennt die vorhandene Netzwerkkonfiguration und bietet gegebenenfalls Konfigurationsoptionen innerhalb der vorhandenen Netzwerke und VLANs an.

Wenn Sie die Installation kürzlich erweitert haben und die neuen Assets nicht automatisch zu Ihrer Konfiguration hinzugefügt wurden, müssen Sie die Assets möglicherweise manuell hinzufügen. Siehe "Übersicht über Management-Nodes".

NetApp HCI verwendet die VMware Enhanced vMotion Compatibility (EVC) und stellt die vMotion-Funktionalität sicher, wenn Computing-Nodes mit verschiedenen CPU-Generationen im vSphere-Cluster vorhanden sind. Wenn EVC für die Erweiterung erforderlich ist, aktiviert NetApp HCI dies nach Möglichkeit automatisch.

In den folgenden Situationen müssen Sie möglicherweise EVC-Einstellungen im vSphere-Client manuell ändern, um eine vollständige Erweiterung durchzuführen:

- Die vorhandenen Computing-Nodes weisen eine neuere CPU-Generation auf als die Computing-Nodes, die Sie hinzufügen möchten.
- Die steuernde vCenter Instanz unterstützt nicht die erforderliche EVC-Ebene.
- Die hinzuzufügenden Computing-Nodes haben eine ältere CPU-Generation als die EVC-Einstellung der steuernden vCenter Instanz.

Wenn Sie NetApp HCI Computing- oder Storage-Ressourcen in der NetApp Deployment Engine erweitern, sollten Sie eine Verbindung mit der vCenter Instanz herstellen, die Ihre vorhandenen NetApp HCI Computing-Nodes managt.

Weitere Informationen

- "Erweitern Sie die NetApp HCI Computing-Ressourcen"
- "Erweitern Sie NetApp HCI Storage-Ressourcen"
- "Erweitern Sie gleichzeitig NetApp HCI Storage- und Computing-Ressourcen"
- "Ressourcen-Seite zu NetApp HCI"
- "NetApp Element Plug-in für vCenter Server"

Erweitern Sie NetApp HCI Storage-Ressourcen

Nachdem die NetApp HCI Implementierung abgeschlossen ist, können Sie mithilfe von NetApp Hybrid Cloud Control NetApp HCI Storage-Ressourcen erweitern und konfigurieren.

Was Sie benötigen

- Stellen Sie sicher, dass Sie über freie und nicht genutzte IPv4-Adressen im gleichen Netzwerksegment wie vorhandene Knoten verfügen (jeder neue Node muss im gleichen Netzwerk wie die vorhandenen Knoten seines Typs installiert sein).
- Stellen Sie sicher, dass Sie über einen der folgenden Typen von SolidFire Storage-Cluster-Konten verfügen:
  - Das native Administratorkonto, das während der ersten Implementierung erstellt wurde
  - Ein benutzerdefiniertes Benutzerkonto mit Berechtigungen für Cluster Admin, Laufwerke, Volumes und Nodes
- Stellen Sie sicher, dass Sie mit jedem neuen Knoten die folgenden Aktionen durchgeführt haben:
  - Den neuen Node im NetApp HCI-Chassis mithilfe von installiert"Installationsanweisungen".
  - Verkabelung und Strom zum neuen Node
- Stellen Sie sicher, dass Sie über die Management-IPv4-Adresse eines bereits installierten Storage-Node verfügen. Die IP-Adresse finden Sie auf der Registerkarte **NetApp Element Management** > **Cluster** > **Knoten** des NetApp Element Plug-ins für vCenter Server.
- Stellen Sie sicher, dass jeder neue Node dieselbe Netzwerktopologie und -Verkabelung wie die vorhandenen Storage- oder Computing-Cluster verwendet.

Wenn Sie die Storage-Ressourcen erweitern, sollte die Storage-Kapazität gleichmäßig auf das gesamte Chassis verteilt werden, um die bestmögliche Zuverlässigkeit zu erzielen.

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.
3. Wählen Sie **Expand** oben rechts im Interface.

   Der Browser öffnet die NetApp Deployment Engine.

4. Melden Sie sich bei der NetApp Deployment Engine an, indem Sie die Anmeldedaten des Administrators für das lokale NetApp HCI-Storage-Cluster angeben.

   Sie können sich nicht mit den Anmeldeinformationen für das Lightweight Directory Access Protocol anmelden.

5. Wählen Sie auf der Seite **Willkommen Nein** aus und wählen Sie **Weiter**.

6. Wählen Sie auf der Seite **Available Inventory** die zu hinzuzufügenden Speicherknoten aus und wählen Sie **Continue** aus.
7. Auf der Seite **Netzwerkeinstellungen** wurden einige Netzwerkinformationen von der ersten Bereitstellung erkannt. Jeder neue Storage Node wird nach Seriennummer aufgeführt und Sie müssen ihm die neuen Netzwerkinformationen zuweisen. Führen Sie für jeden neuen Storage-Node die folgenden Schritte aus:
   a. **Hostname**: Wenn NetApp HCI ein Benennungspräfix erkannt hat, kopieren Sie es aus dem Feld Erkennungspräfix und fügen Sie es als Präfix für den neuen eindeutigen Hostnamen ein, den Sie in das Feld Hostname einfügen.
   b. **Managementadresse**: Geben Sie eine Management-IP-Adresse für den neuen Speicherknoten ein, der sich im Subnetz des Managementnetzwerks befindet.
   c. **Speicher (iSCSI) IP-Adresse**: Geben Sie eine iSCSI-IP-Adresse für den neuen Speicherknoten ein, der sich im iSCSI-Netzwerk-Subnetz befindet.
   d. Wählen Sie **Weiter**.

   NetApp HCI nimmt möglicherweise eine Zeit in Anspruch, um die von Ihnen eingegebenen IP-Adressen zu validieren. Die Schaltfläche Weiter ist verfügbar, wenn die IP-Adressvalidierung abgeschlossen ist.
8. Auf der Seite **Review** im Abschnitt Netzwerkeinstellungen werden neue Knoten im Fettdruck angezeigt. Gehen Sie wie folgt vor, um Änderungen in einem beliebigen Abschnitt vorzunehmen:
   a. Wählen Sie **Bearbeiten** für diesen Abschnitt aus.
   b. Wenn Sie fertig sind, wählen Sie auf den folgenden Seiten **Weiter** aus, um zur Seite „Überprüfen“ zurückzukehren.
9. **Optional**: Wenn Sie keine Cluster-Statistiken und Support-Informationen an NetApp Hosted Active IQ Server senden möchten, deaktivieren Sie das endgültige Kontrollkästchen.

   Hierdurch wird der Zustand und die Diagnoseüberwachung in Echtzeit für NetApp HCI deaktiviert. Wenn diese Funktion deaktiviert wird, ist es NetApp nicht mehr möglich, NetApp HCI proaktiv zu unterstützen und zu überwachen, um Probleme zu erkennen und zu beheben, bevor die Produktion beeinträchtigt wird.
10. Wählen Sie **Knoten Hinzufügen**.

    Sie können den Fortschritt überwachen, während NetApp HCI die Ressourcen hinzufügt und konfiguriert.
11. **Optional**: Überprüfen Sie, ob neue Speicherknoten im Element Plug-in für vCenter Server sichtbar sind.

    Wenn Sie ein Storage-Cluster mit zwei Nodes auf vier oder mehr erweitert haben, sind die Witness-Nodes, die zuvor vom Storage-Cluster verwendet wurden, noch als Standby Virtual Machines in vSphere sichtbar. Der neu erweiterte Speicher-Cluster verwendet sie nicht. Wenn Sie VM-Ressourcen zurückfordern möchten, können Sie die virtuellen Witness Node-Maschinen verwenden"Manuell entfernen".

Weitere Informationen

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

Erweitern Sie die NetApp HCI Computing-Ressourcen

Nachdem die NetApp HCI Implementierung abgeschlossen ist, können Sie mithilfe von NetApp Hybrid Cloud Control NetApp HCI Computing-Ressourcen erweitern und konfigurieren.

Was Sie benötigen

- Stellen Sie sicher, dass die vSphere-Instanz von NetApp HCI die Lizenzierung von vSphere Enterprise Plus nutzt, wenn Sie eine Implementierung mit Virtual Distributed Switches erweitern.
- Stellen Sie sicher, dass für keine der in NetApp HCI verwendeten vCenter oder vSphere Instanzen abgelaufene Lizenzen vorhanden sind.
- Stellen Sie sicher, dass Sie über freie und nicht genutzte IPv4-Adressen im gleichen Netzwerksegment wie vorhandene Knoten verfügen (jeder neue Node muss im gleichen Netzwerk wie die vorhandenen Knoten seines Typs installiert sein).
- Stellen Sie sicher, dass Sie über die Anmeldedaten für das vCenter-Administratorkonto verfügen.
- Stellen Sie sicher, dass Sie mit jedem neuen Knoten die folgenden Aktionen durchgeführt haben:
  - Den neuen Node im NetApp HCI-Chassis mithilfe von installiert"Installationsanweisungen".
  - Verkabelung und Strom zum neuen Node
- Stellen Sie sicher, dass jeder neue Node dieselbe Netzwerktopologie und -Verkabelung wie die vorhandenen Storage- oder Computing-Cluster verwendet.

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.
3. Wählen Sie **Expand** oben rechts im Interface.

   Der Browser öffnet die NetApp Deployment Engine.

4. Melden Sie sich bei der NetApp Deployment Engine an, indem Sie die Anmeldedaten des Administrators für das lokale NetApp HCI-Storage-Cluster angeben.

   Sie können sich nicht mit den Anmeldeinformationen für das Lightweight Directory Access Protocol anmelden.

5. Wählen Sie auf der Seite **Willkommen Ja** und dann **Weiter**.
6. Lesen Sie auf der Seite **Endbenutzer-Lizenz** die VMware-Endbenutzer-Lizenzvereinbarung, und wählen Sie **Ich akzeptiere** aus, um die Bedingungen zu akzeptieren, und wählen Sie **Weiter** aus.
7. Führen Sie auf der Seite **vCenter** die folgenden Schritte aus:
   a. Geben Sie einen FQDN oder eine IP-Adresse und Administratoranmeldeinformationen für die vCenter Instanz ein, die mit Ihrer NetApp HCI-Installation verknüpft ist.
   b. Wählen Sie **Weiter**.

c. Wählen Sie ein vSphere-Rechenzentrum aus, in dem Sie die Rechenknoten hinzufügen möchten, oder wählen Sie **Neues Rechenzentrum erstellen**, um die Rechenknoten einem neuen Rechenzentrum hinzuzufügen.

> Wenn Sie **Create New Datacenter** auswählen, wird das Feld Cluster automatisch ausgefüllt.

d. Wenn Sie ein vorhandenes Datacenter ausgewählt haben, wählen Sie ein vSphere Cluster aus, mit dem die neuen Computing-Nodes verknüpft werden sollen.

> Wenn NetApp HCI die Netzwerkeinstellungen des Clusters, die Sie für die Erweiterung ausgewählt haben, nicht erkennen kann, stellen Sie sicher, dass die vmKernel und vmnic Zuordnung für das Management, Storage und vMotion Netzwerke auf die Bereitstellungsstandards eingestellt sind. Weitere Informationen finden Sie unter "Unterstützte Netzwerkänderungen" .

e. Wählen Sie **Weiter**.

8. Geben Sie auf der Seite **ESXi Credentials** ein ESXi-Root-Passwort für den Rechenknoten oder die Knoten ein, die Sie hinzufügen.

   Sie sollten dasselbe Passwort verwenden, das während der ersten NetApp HCI-Implementierung erstellt wurde.

9. Wählen Sie **Weiter**.
10. Wenn Sie einen neuen vSphere Datacenter-Cluster erstellt haben, wählen Sie auf der Seite **Netzwerktopologie** eine Netzwerktopologie aus, die an die neuen Computing-Nodes, die Sie hinzufügen, angepasst ist.

> Wählen Sie die Option mit zwei Kabeln nur aus, wenn Ihre Computing-Nodes die Topologie mit zwei Kabeln verwenden und die vorhandene NetApp HCI-Implementierung mit VLAN-IDs konfiguriert ist.

11. Wählen Sie auf der Seite **Available Inventory** die Knoten aus, die Sie der vorhandenen NetApp HCI-Installation hinzufügen möchten.

> Bei einigen Rechenknoten müssen Sie möglicherweise EV auf der höchsten Ebene aktivieren, die Ihre vCenter-Version unterstützt, bevor Sie sie zu Ihrer Installation hinzufügen können. Zur Aktivierung von EVC für diese Computing-Nodes muss der vSphere Client verwendet werden. Aktualisieren Sie nach dem Aktivieren die Seite „Inventar“, und versuchen Sie erneut, die Computing-Nodes hinzuzufügen.

12. Wählen Sie **Weiter**.
13. **Optional**: Wenn Sie einen neuen vSphere Datacenter-Cluster erstellt haben, importieren Sie auf der Seite **Netzwerkeinstellungen** Netzwerkinformationen aus einer vorhandenen NetApp HCI-Bereitstellung, indem Sie das Kontrollkästchen **Kopiereinstellung aus einem vorhandenen Cluster** aktivieren.

    Dadurch werden das Standard-Gateway und die Subnetzinformationen für jedes Netzwerk gefüllt.

14. Auf der Seite **Netzwerkeinstellungen** wurden einige Netzwerkinformationen von der ersten Bereitstellung erkannt. Jeder neue Computing Node wird nach Seriennummer aufgeführt und Sie müssen ihm neue Netzwerkinformationen zuweisen. Führen Sie für jeden neuen Computing-Node die folgenden Schritte aus:

a. **Hostname**: Wenn NetApp HCI ein Benennungspräfix erkannt hat, kopieren Sie es aus dem Feld **detected Naming Prefix** und fügen Sie es als Präfix für den neuen Hostnamen ein.

b. **Management-IP-Adresse**: Geben Sie eine Management-IP-Adresse für den neuen Compute-Node ein, der sich im Subnetz des Managementnetzwerks befindet.

c. **VMotion IP-Adresse**: Geben Sie eine vMotion-IP-Adresse für den neuen Compute-Knoten ein, der sich im vMotion-Netzwerk-Subnetz befindet.

d. **ISCSI A - IP-Adresse**: Geben Sie eine IP-Adresse für den ersten iSCSI-Port des Compute-Node im iSCSI-Netzwerk-Subnetz ein.

e. **ISCSI B - IP-Adresse**: Geben Sie eine IP-Adresse für den zweiten iSCSI-Port des Compute-Node im iSCSI-Netzwerk-Subnetz ein

f. Wählen Sie **Weiter**.

15. Auf der Seite **Review** im Abschnitt Netzwerkeinstellungen werden neue Knoten im Fettdruck angezeigt. Gehen Sie wie folgt vor, um Änderungen in einem beliebigen Abschnitt vorzunehmen:

a. Wählen Sie **Bearbeiten** für diesen Abschnitt aus.

b. Wenn Sie fertig sind, wählen Sie **Weiter** auf allen nachfolgenden Seiten, um zur Seite **Review** zurückzukehren.

16. **Optional**: Wenn Sie keine Cluster-Statistiken und Support-Informationen an NetApp Hosted SolidFire Active IQ Server senden möchten, deaktivieren Sie das endgültige Kontrollkästchen.

Hierdurch wird der Zustand und die Diagnoseüberwachung in Echtzeit für NetApp HCI deaktiviert. Wenn diese Funktion deaktiviert wird, ist es NetApp nicht mehr möglich, NetApp HCI proaktiv zu unterstützen und zu überwachen, um Probleme zu erkennen und zu beheben, bevor die Produktion beeinträchtigt wird.

17. Wählen Sie **Knoten Hinzufügen**.

Sie können den Fortschritt überwachen, während NetApp HCI die Ressourcen hinzufügt und konfiguriert.

18. **Optional**: Überprüfen Sie, ob neue Rechenknoten im VMware vSphere Web Client sichtbar sind.

Weitere Informationen

- "Seite „NetApp HCI Ressourcen“"
- "Installations- und Setup-Anleitung für NetApp HCI Computing- und Storage-Nodes"
- "VMware Knowledge Base: Unterstützung für vMotion Compatibility (EVC)-Prozessoren"

Erweitern Sie gleichzeitig NetApp HCI Storage- und Computing-Ressourcen

Nachdem die NetApp HCI Implementierung abgeschlossen ist, können Sie mithilfe von NetApp Hybrid Cloud Control gleichzeitig NetApp HCI Storage- und Computing-Ressourcen erweitern und konfigurieren.

Was Sie benötigen

- Stellen Sie sicher, dass die vSphere-Instanz von NetApp HCI die Lizenzierung von vSphere Enterprise Plus nutzt, wenn Sie eine Implementierung mit Virtual Distributed Switches erweitern.
- Stellen Sie sicher, dass für keine der in NetApp HCI verwendeten vCenter oder vSphere Instanzen abgelaufene Lizenzen vorhanden sind.

- Stellen Sie sicher, dass Sie über die Anmeldedaten für das vCenter-Administratorkonto verfügen.
- Stellen Sie sicher, dass Sie über freie und nicht genutzte IPv4-Adressen im gleichen Netzwerksegment wie vorhandene Knoten verfügen (jeder neue Node muss im gleichen Netzwerk wie die vorhandenen Knoten seines Typs installiert sein).
- Stellen Sie sicher, dass Sie über einen der folgenden Typen von SolidFire Storage-Cluster-Konten verfügen:
  - Das native Administratorkonto, das während der ersten Implementierung erstellt wurde
  - Ein benutzerdefiniertes Benutzerkonto mit Berechtigungen für Cluster Admin, Laufwerke, Volumes und Nodes
- Stellen Sie sicher, dass Sie mit jedem neuen Knoten die folgenden Aktionen durchgeführt haben:
  - Den neuen Node im NetApp HCI-Chassis mithilfe von installiert"Installationsanweisungen".
  - Verkabelung und Strom zum neuen Node
- Stellen Sie sicher, dass Sie über die Management-IPv4-Adresse eines bereits installierten Storage-Node verfügen. Die IP-Adresse finden Sie auf der Registerkarte **NetApp Element Management** > **Cluster** > **Knoten** des NetApp Element Plug-ins für vCenter Server.
- Stellen Sie sicher, dass jeder neue Node dieselbe Netzwerktopologie und -Verkabelung wie die vorhandenen Storage- oder Computing-Cluster verwendet.

Über diese Aufgabe

- Sie können den H410C Compute-Node mit vorhandenen NetApp HCI Computing- und Storage-Nodes im selben Chassis und Cluster kombinieren.
- Computing-Nodes und BPU-fähige Computing-Nodes können nicht im selben Cluster miteinander kombiniert werden. Wenn Sie einen GPU-fähigen Computing-Node auswählen, werden die aus CPU-Computing-Nodes nicht wählbar und umgekehrt.
- Wenn Sie Compute-Nodes mit CPU-Generationen hinzufügen, die sich von der CPU-Generation der vorhandenen Computing-Nodes unterscheiden und Enhanced vMotion Compatibility (EVC) auf der steuernden vCenter Instanz deaktiviert ist, müssen Sie EVC aktivieren, bevor Sie fortfahren. Dadurch wird für vMotion Funktionalität nach der Erweiterung gesorgt.

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.
3. Wählen Sie **Expand** oben rechts im Interface.

   Der Browser öffnet die NetApp Deployment Engine.

4. Melden Sie sich bei der NetApp Deployment Engine an, indem Sie die Anmeldedaten des Administrators für das lokale NetApp HCI-Storage-Cluster angeben.

   Sie können sich nicht mit den Anmeldeinformationen für das Lightweight Directory Access Protocol anmelden.

5. Wählen Sie auf der Seite **Willkommen Ja** und dann **Weiter**.
6. Lesen Sie auf der Seite **Endbenutzer-Lizenz** die VMware-Endbenutzer-Lizenzvereinbarung, und wählen Sie **Ich akzeptiere** aus, um die Bedingungen zu akzeptieren, und wählen Sie **Weiter** aus.
7. Führen Sie auf der Seite **vCenter** die folgenden Schritte aus:
   a. Geben Sie einen FQDN oder eine IP-Adresse und Administratoranmeldeinformationen für die vCenter Instanz ein, die mit Ihrer NetApp HCI-Installation verknüpft ist.
   b. Wählen Sie **Weiter**.
   c. Wählen Sie ein vSphere-Rechenzentrum aus, in dem Sie die Rechenknoten hinzufügen möchten, oder wählen Sie **Neues Rechenzentrum erstellen**, um die Rechenknoten einem neuen Rechenzentrum hinzuzufügen.

      Wenn Sie „Neues Datacenter erstellen“ auswählen, wird das Feld „Cluster“ automatisch ausgefüllt.

   d. Wenn Sie ein vorhandenes Datacenter ausgewählt haben, wählen Sie ein vSphere Cluster aus, mit dem die neuen Computing-Nodes verknüpft werden sollen.

      Wenn NetApp HCI die Netzwerkeinstellungen des Clusters, die Sie für die Erweiterung ausgewählt haben, nicht erkennen kann, stellen Sie sicher, dass die vmKernel und vmnic Zuordnung für das Management, Storage und vMotion Netzwerke auf die Bereitstellungsstandards eingestellt sind. Weitere Informationen finden Sie unter "Unterstützte Netzwerkänderungen" .

   e. Wählen Sie **Weiter**.
8. Geben Sie auf der Seite **ESXi Credentials** ein ESXi-Root-Passwort für den Rechenknoten oder die Knoten ein, die Sie hinzufügen.

   Sie sollten dasselbe Passwort verwenden, das während der ersten NetApp HCI-Implementierung erstellt wurde.
9. Wählen Sie **Weiter**.
10. Wenn Sie einen neuen vSphere Datacenter-Cluster erstellt haben, wählen Sie auf der Seite **Netzwerktopologie** eine Netzwerktopologie aus, die an die neuen Computing-Nodes, die Sie hinzufügen, angepasst ist.

    Wählen Sie die Option mit zwei Kabeln nur aus, wenn Ihre Computing-Nodes die Topologie mit zwei Kabeln verwenden und die vorhandene NetApp HCI-Implementierung mit VLAN-IDs konfiguriert ist.
11. Wählen Sie auf der Seite **Available Inventory** die Speicher- und Rechenknoten aus, die Sie hinzufügen möchten, und wählen Sie **Continue** aus.

    Bei einigen Rechenknoten müssen Sie möglicherweise EV auf der höchsten Ebene aktivieren, die Ihre vCenter-Version unterstützt, bevor Sie sie zu Ihrer Installation hinzufügen können. Zur Aktivierung von EVC für diese Computing-Nodes muss der vSphere Client verwendet werden. Aktualisieren Sie nach dem Aktivieren die Seite „Inventar“, und versuchen Sie erneut, die Computing-Nodes hinzuzufügen.
12. Wählen Sie **Weiter**.

13. **Optional**: Wenn Sie einen neuen vSphere Datacenter-Cluster erstellt haben, importieren Sie auf der Seite **Netzwerkeinstellungen** Netzwerkinformationen aus einer vorhandenen NetApp HCI-Bereitstellung, indem Sie das Kontrollkästchen **Kopiereinstellung aus einem vorhandenen Cluster** aktivieren.

    Dadurch werden das Standard-Gateway und die Subnetzinformationen für jedes Netzwerk gefüllt.

14. Auf der Seite **Netzwerkeinstellungen** wurden einige Netzwerkinformationen von der ersten Bereitstellung erkannt. Jeder neue Storage Node wird nach Seriennummer aufgeführt und Sie müssen ihm die neuen Netzwerkinformationen zuweisen. Führen Sie für jeden neuen Storage-Node die folgenden Schritte aus:
    a. **Hostname**: Wenn NetApp HCI ein Benennungspräfix erkannt hat, kopieren Sie es aus dem Feld Erkennungspräfix und fügen Sie es als Präfix für den neuen eindeutigen Hostnamen ein, den Sie in das Feld Hostname einfügen.
    b. **Managementadresse**: Geben Sie eine Management-IP-Adresse für den neuen Speicherknoten ein, der sich im Subnetz des Managementnetzwerks befindet.
    c. **Speicher (iSCSI) IP-Adresse**: Geben Sie eine iSCSI-IP-Adresse für den neuen Speicherknoten ein, der sich im iSCSI-Netzwerk-Subnetz befindet.
    d. Wählen Sie **Weiter**.

    > NetApp HCI nimmt möglicherweise eine Zeit in Anspruch, um die von Ihnen eingegebenen IP-Adressen zu validieren. Die Schaltfläche Weiter ist verfügbar, wenn die IP-Adressvalidierung abgeschlossen ist.

15. Auf der Seite **Review** im Abschnitt Netzwerkeinstellungen werden neue Knoten im Fettdruck angezeigt. Gehen Sie wie folgt vor, um Änderungen in einem beliebigen Abschnitt vorzunehmen:
    a. Wählen Sie **Bearbeiten** für diesen Abschnitt aus.
    b. Wenn Sie fertig sind, wählen Sie auf den folgenden Seiten **Weiter** aus, um zur Seite „Überprüfen“ zurückzukehren.
16. **Optional**: Wenn Sie keine Cluster-Statistiken und Support-Informationen an NetApp Hosted Active IQ Server senden möchten, deaktivieren Sie das endgültige Kontrollkästchen.

    Hierdurch wird der Zustand und die Diagnoseüberwachung in Echtzeit für NetApp HCI deaktiviert. Wenn diese Funktion deaktiviert wird, ist es NetApp nicht mehr möglich, NetApp HCI proaktiv zu unterstützen und zu überwachen, um Probleme zu erkennen und zu beheben, bevor die Produktion beeinträchtigt wird.

17. Wählen Sie **Knoten Hinzufügen**.

    Sie können den Fortschritt überwachen, während NetApp HCI die Ressourcen hinzufügt und konfiguriert.

18. **Optional**: Überprüfen Sie, ob neue Knoten im VMware vSphere Web Client (für Compute Nodes) oder im Element Plug-in für vCenter Server (für Storage-Nodes) sichtbar sind.

    > Wenn Sie ein Storage-Cluster mit zwei Nodes auf vier oder mehr erweitert haben, sind die Witness-Nodes, die zuvor vom Storage-Cluster verwendet wurden, noch als Standby Virtual Machines in vSphere sichtbar. Der neu erweiterte Speicher-Cluster verwendet sie nicht. Wenn Sie VM-Ressourcen zurückfordern möchten, können Sie die virtuellen Witness Node-Maschinen verwenden"Manuell entfernen".

Weitere Informationen

- "Seite „NetApp HCI Ressourcen“"

- "NetApp Element Plug-in für vCenter Server"
- "Installations- und Setup-Anleitung für NetApp HCI Computing- und Storage-Nodes"
- "VMware Knowledge Base: Unterstützung für vMotion Compatibility (EVC)-Prozessoren"

Entfernen Sie Witness Nodes nach dem erweitern des Clusters

Nachdem Sie ein Storage-Cluster mit zwei Nodes auf vier oder mehr Nodes erweitert haben, können Sie das Paar Witness Nodes löschen, um Computing-Ressourcen in Ihrer NetApp HCI Installation freizumachen. Die Witness Nodes, die zuvor vom Storage-Cluster verwendet wurden, sind weiterhin als Standby Virtual Machines (VM) im vSphere Web Client sichtbar.

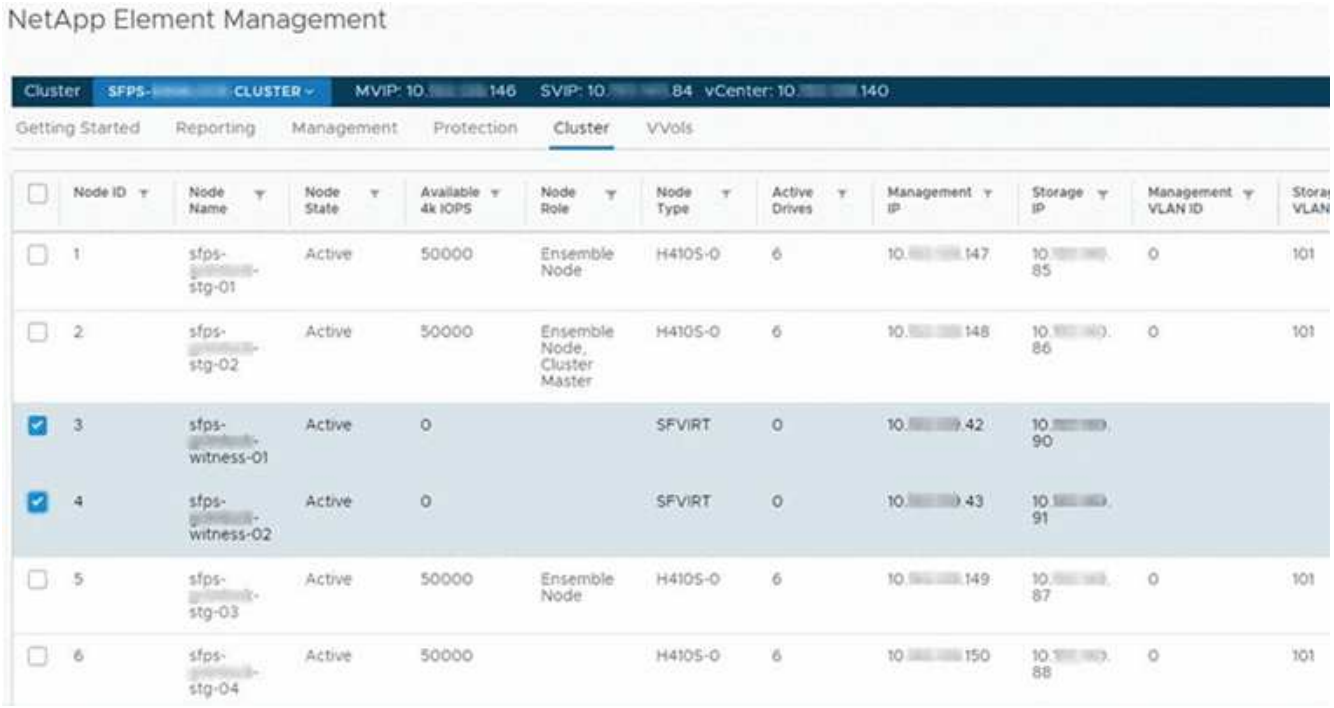
Über diese Aufgabe

Witness-Nodes sind in Clustern mit mehr als vier Storage-Nodes nicht erforderlich. Dies ist eine optionale Vorgehensweise, wenn Sie CPU und Arbeitsspeicher freigeben möchten, nachdem Sie Ihr Cluster mit zwei Nodes auf vier oder mehr Nodes erweitert haben.

Vergewissern Sie sich, dass keine Cluster-Fehler oder -Fehler gemeldet werden. Sie können Informationen zu Systemwarnungen finden, indem Sie im Erweiterungspunkt NetApp Element-Verwaltung in vSphere **Reporting > Alerts** auswählen.

Schritte

1. Greifen Sie über vSphere auf die Registerkarte **Shortcuts** oder auf den Erweiterungspunkt für die NetApp Element-Verwaltung zu.
2. Wählen Sie **NetApp Element-Verwaltung > Cluster > Knoten**.



3. Aktivieren Sie das Kontrollkästchen für den Witness Node, den Sie löschen möchten, und wählen Sie

Actions > Remove aus.

4. Bestätigen Sie die Aktion in der Eingabeaufforderung.
5. Wählen Sie **Hosts und Cluster** aus.
6. Navigieren Sie zu der Witness Node VM, die Sie zuvor entfernt haben.
7. Klicken Sie mit der rechten Maustaste auf die VM, und schalten Sie sie aus.
8. Klicken Sie mit der rechten Maustaste auf die VM, die Sie ausgeschaltet haben, und wählen Sie **von Festplatte löschen** aus.
9. Bestätigen Sie die Aktion in der Eingabeaufforderung.

Weitere Informationen

- "NetApp HCI Storage Cluster mit zwei Nodes – TR-4823"
- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Verwenden Sie Rancher auf NetApp HCI

Übersicht über die NetApp HCI

Rancher ist ein vollständiger Software-Stack, mit dem Teams, die Container einführen, zusammenarbeiten können. Rancher bewältigt die betrieblichen und sicherheitstechnischen Herausforderungen, die beim Management mehrerer Kubernetes-Cluster über verschiedene Infrastrukturen entstehen, und stellt DevOps-Teams integrierte Tools für die Ausführung von Container-Workloads zur Verfügung.

Durch die Implementierung von Rancher auf NetApp HCI wird die Rancher-Kontrollebene implementiert, die auch als *Rancher-Server* bezeichnet wird. Mit ihr können Sie Kubernetes-Cluster vor Ort erstellen. Mit NetApp Hybrid Cloud Control implementieren Sie die Rancher-Kontrollebene.

Nach der Implementierung provisionieren, managen und überwachen Sie über die Rancher-Kontrollebene Kubernetes-Cluster, die von den Dev- und Ops-Teams verwendet werden. Entwicklungs- und Ops-Teams können mit Rancher Aktivitäten auf Benutzer-Clustern durchführen, die sich auf NetApp HCI selbst, einem Public Cloud-Provider oder einer anderen Infrastruktur befinden.

Vorteile von Rancher bei NetApp HCI

- Einfache Installation: Sie müssen nicht lernen, wie man Rancher installiert und konfiguriert. Sie können eine vorlagenbasierte Implementierung implementieren, die von NetApp HCI und Rancher gemeinsam entwickelt wurde.
- Lifecycle-Management: In einer manuellen Rancher-Implementierung werden Updates für die Rancher Server-Applikation oder den Rancher Kubernetes Engine (RKE)-Cluster nicht automatisiert. Rancher auf NetApp HCI bietet die Möglichkeit für Aktualisierungen des Management-Clusters, einschließlich der Rancher-Server und der RKE.

Was Sie mit Rancher auf NetApp HCI tun können

Mit NetApp HCI-Ranglisten können Sie:

- Implementieren von Services zu verschiedenen Cloud-Providern und Ihrer Private Cloud
- Applikationen und Daten lassen sich unabhängig vom Cloud-Standort in einer Hybrid-Cloud-Architektur verschließen, ohne dabei die Service Level Agreements zu beeinträchtigen.
- Erweitern Sie Cloud-native Applikationen selbst.
- Zentralisiertes Management mehrerer Cluster (neu und vorhanden)
- Orchestrierung von Kubernetes-basierten Hybrid Cloud-Applikationen

Option für technischen Support

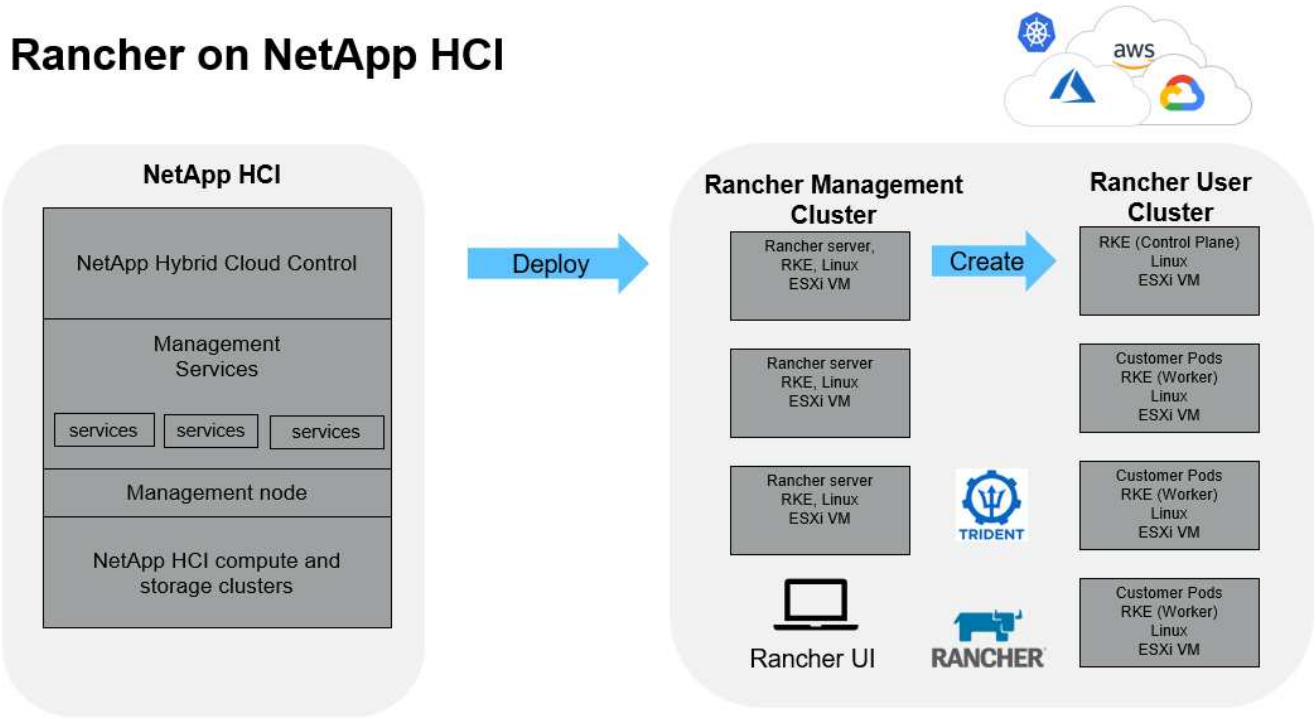
Durch die Verwendung von Rancher auf der Open-Source-Software NetApp HCI und Kubernetes umfasst die kostenlose Implementierung und Nutzung. Lizenzschlüssel sind nicht erforderlich.

Sie können eine NetApp Rancher Support Option wählen, um Core-basierten, Rancher Enterprise Support zu erhalten.

Rancher Support ist nicht in Ihrer NetApp Support Edge Vereinbarung enthalten. Wenden Sie sich an den NetApp Vertrieb oder Ihren Reseller, um Optionen zu erhalten. Wenn Sie Rancher Support von NetApp erwerben, erhalten Sie eine E-Mail mit Anweisungen.

Rancher zu NetApp HCI Architektur und Komponenten

Hier eine Übersicht der verschiedenen Komponenten von Rancher auf NetApp HCI:



- **NetApp Hybrid Cloud Control**: Mit dieser Schnittstelle können Sie Rancher auf NetApp HCI und NetApp Element Software implementieren, die für Rancher auf NetApp HCI erforderlich ist.

  Mit NetApp Hybrid Cloud Control können Sie außerdem Managementservices aktualisieren, das System erweitern, Protokolle erfassen und die Installation überwachen.

- **Management-Services**: Management-Services werden auf dem Management-Node ausgeführt. Mit NetApp Hybrid Cloud Control können Sie Rancher auf NetApp HCI implementieren.
- **Management Cluster**: Rancher auf NetApp HCI implementiert im Rancher Management Cluster drei Virtual Machines, die Sie mit NetApp Hybrid Cloud Control, vCenter Server oder der Rancher Benutzeroberfläche sehen können. Die virtuellen Management-Cluster-Maschinen hosten den Rancher-Server, die Rancher Kubernetes Engine (RKE) und das Linux-Betriebssystem.

  Wenn Sie die beste Performance und höhere Sicherheit erzielen, sollten Sie in Betracht ziehen, einen dedizierten Kubernetes Cluster für den Rancher Management-Server zu verwenden. Sie sollten Ihre Benutzer-Workloads nicht auf dem Management-Cluster ausführen.

- **Benutzer-Cluster**: Die nachgeschalteten Kubernetes-Benutzer-Cluster führen Ihre Anwendungen und Dienste aus. Jeder Cluster, den Sie aus Rancher implementieren oder in Rancher importieren, ist ein Benutzer-Cluster.
- **Trident**: Für die Sortierung auf NetApp HCI steht ein Trident-Katalog zur Verfügung und läuft in den

Benutzer-Clustern. Die Einbindung dieses Katalogs vereinfacht die Trident Implementierung in Benutzer-Cluster.

Weitere Informationen

- "Rancher Dokumentation über Architektur"
- "Ressourcen-Seite zu NetApp HCI"

Rancher zu NetApp HCI Concepts

Erfahren Sie grundlegende Konzepte im Zusammenhang mit Rancher auf NetApp HCI.

- **Rancher Server** oder **Kontrollebene**: Die Rancher-Kontrollebene, manchmal auch als *Rancher Server* bezeichnet, stellt, verwaltet und überwacht Kubernetes-Cluster, die von Entwicklungs- und Operations-Teams verwendet werden.
- **Kataloge**: Kataloge sind GitHub-Repositories oder Helm-Chart-Repositories, die mit Anwendungen gefüllt sind, die für die Bereitstellung bereit sind. Rancher bietet die Möglichkeit, einen Katalog von Helm-Diagrammen zu verwenden, durch den Anwendungen wiederholt implementiert werden können. Rancher umfasst zwei Arten von Katalogen: Integrierte globale Kataloge und benutzerdefinierte Kataloge. Trident wird als Katalog implementiert. Siehe "Rancher Dokumentation über Kataloge".
- **Management Cluster**: Rancher auf NetApp HCI stellt drei virtuelle Maschinen auf dem Rancher Management Cluster bereit, die Sie mit Rancher, Hybrid Cloud Control und dem vCenter Plug-in sehen können. Die virtuellen Maschinen des Management-Clusters hosten den Rancher Server, die Rancher Kubernetes Engine (RKE) und das Linux Betriebssystem.
- **Benutzer-Cluster**: Diese nachgeschalteten Kubernetes-Cluster führen Ihre Apps und Services aus. Bei Kubernetes-Installationen von Rancher sollte das Management-Cluster von den Benutzer-Clustern getrennt sein. Jeder Cluster, den ein Rancher-Benutzer von Rancher aus bereitstellt oder in Rancher importiert, gilt als Benutzercluster.
- **Rancher Node-Vorlage**: Hybrid Cloud Control verwendet eine Rancher-Node-Vorlage, um die Bereitstellung zu vereinfachen.

  Siehe "Rancher-Dokumentation zu Knotenvorlagen".

Trident Software- und Konzepte für persistenten Storage

Trident, selbst eine native Kubernetes-Applikation, wird direkt in einem Kubernetes Cluster ausgeführt. Mit Trident können Kubernetes-Benutzer (z. B. Entwickler, Data Scientists und Kubernetes-Administratoren) persistente Storage-Volumes im gewohnten Kubernetes-Standardformat erstellen, managen und interagieren. Mit Trident können NetApp Lösungen die Anforderungen von Kubernetes-Clustern in Bezug auf persistente Volumes erfüllen.

Mit Rancher können Sie ein persistentes Volume verwenden, das unabhängig von einem bestimmten POD und seiner eigenen Lebenszeit vorhanden ist. Mit Trident für das Management von PVCs (Persistent Volume Claims) sind die Entwickler, die PODs erstellen, von den Details zur Implementierung auf niedrigerer Storage-Ebene isoliert, auf die sie zugreifen.

Wenn eine Container-Applikation eine PVC-Anforderung (Persistent Volume Claim) ausgibt, stellt Trident dynamisch Storage gemäß den Parametern bereit, die für die NetApp Element Software-Storage-Ebene in NetApp HCI angefordert werden.

Ein Trident-Katalog ist für Rancher auf NetApp HCI verfügbar und wird in den Benutzer-Clustern ausgeführt.

Im Rahmen der Rancher on NetApp HCI Implementation ist standardmäßig ein Trident-Installationsprogramm im Rancher-Katalog verfügbar. Die Einbindung dieses Katalogs vereinfacht die Trident Implementierung in Benutzer-Cluster.

Siehe "Installation von Trident mit Rancher auf NetApp HCI".

Weitere Informationen finden Sie auf der "Trident Dokumentation".

Weitere Informationen

- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "Ressourcen-Seite zu NetApp HCI"

Anforderungen für die Rangliste auf NetApp HCI

Stellen Sie vor der Installation von Rancher auf NetApp HCI sicher, dass Ihre Umgebung und Ihr NetApp HCI-System diese Anforderungen erfüllen.

> Wenn Sie versehentlich Rancher auf NetApp HCI mit falschen Informationen bereitstellen (z. B. einen falschen Rancher-Server-FQDN), gibt es keine Möglichkeit, die Bereitstellung zu korrigieren, ohne sie zu entfernen und erneut bereitzustellen. Sie müssen das Rancher auf NetApp HCI-Instanz entfernen und anschließend Rancher auf NetApp HCI von der NetApp Hybrid Cloud Control UI neu implementieren. Weitere Informationen finden Sie unter "Entfernen Sie eine Rancher-Installation auf NetApp HCI" .

Node-Anforderungen erfüllt

- Vergewissern Sie sich, dass Ihr NetApp HCI System mindestens drei Computing-Nodes aufweist. Dies ist für volle Ausfallsicherheit erforderlich. Rancher auf NetApp HCI wird nicht auf reine Storage-Konfigurationen unterstützt.
- Stellen Sie sicher, dass der Datenspeicher, den Sie für die Rancher-Bereitstellung auf NetApp HCI verwenden möchten, mindestens 60 GB freien Speicherplatz hat.
- Stellen Sie sicher, dass auf Ihrem NetApp HCI Cluster Managementservices ab Version 2.17 ausgeführt werden.

Details zu den Nodes

Rancher auf NetApp HCI implementiert ein Management-Cluster mit drei Nodes.

Alle Nodes weisen die folgenden Merkmale auf:

VCPU	RAM (GB)	Festplatte (GB)
2	8	20

Netzwerkanforderungen

- Stellen Sie sicher, dass das Netzwerk, das Sie für die Bereitstellung des Rancher auf dem NetApp HCI-Management-Cluster planen, über eine Route zum Management-Node-Managementnetzwerk verfügt.

- Rancher auf NetApp HCI unterstützt DHCP-Adressen für die Kontrollebene (Rancher Server) und Benutzer-Cluster, wir empfehlen jedoch statische IP-Adressen für Produktionsumgebungen. Stellen Sie sicher, dass Sie die erforderlichen statischen IP-Adressen zugewiesen haben, wenn Sie in einer Produktionsumgebung bereitstellen.
  - Rancher-Server benötigt drei statische IP-Adressen.
  - Jedes Benutzer-Cluster benötigt so viele statische IP-Adressen wie Nodes im Cluster. Beispielsweise erfordert ein Benutzer-Cluster mit vier Nodes vier statische IP-Adressen.
  - Wenn Sie die Verwendung von DHCP-Adressen für die Rancher-Steuerebene oder Benutzer-Cluster planen, stellen Sie sicher, dass die DHCP-Leasingdauer mindestens 24 Stunden beträgt.
- Wenn Sie einen HTTP-Proxy verwenden müssen, um den Internetzugriff für Rancher auf NetApp HCI zu aktivieren, müssen Sie eine Änderung vor der Bereitstellung am Management-Node vornehmen. Melden Sie sich über SSH am Management-Node an, und befolgen Sie die Anweisungen "Anweisungen" in der Docker-Dokumentation, um die Proxy-Einstellungen für Docker manuell zu aktualisieren.
- Wenn Sie während der Bereitstellung einen Proxy-Server aktivieren und konfigurieren, werden die folgenden IP-Adressbereiche und -Domains automatisch zu den Rancher-Server-Noproxy-Einstellungen hinzugefügt:

```
127.0.0.0/8, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, .svc,
.cluster.local
```

- Stellen Sie sicher, dass der Management-Node DNS verwenden kann, um den Hostnamen auf eine IP-Adresse aufzulösen `<any IP address>.nip.io`. Dies ist der während der Bereitstellung verwendete DNS-Provider. Wenn der Management-Node diese URL nicht lösen kann, schlägt die Bereitstellung fehl.
- Stellen Sie sicher, dass Sie DNS-Einträge für jede statische IP-Adresse eingerichtet haben, die Sie benötigen.

Anforderungen für VMware vSphere

- Stellen Sie sicher, dass die VMware vSphere Instanz, die Sie verwenden, Version 6.5, 6.7 oder 7.0 ist.
- Sie können eine Netzwerkkonfiguration für den vSphere Standard Switch (VSS) verwenden. Wenn Sie dies jedoch tun, stellen Sie sicher, dass die für Rancher VMs verwendeten virtuellen Switches und physischen Hosts auf dieselbe Weise auf dieselben Portgruppen zugreifen können, wie es bei normalen VMs sichergestellt wäre.

Implementierungsüberlegungen

Bitte beachten Sie die folgenden Punkte:

- Implementierungsarten
  - Demo-Implementierungen
  - Implementierungen in der Produktion
- Rancher FQDN

Rancher auf NetApp HCI ist nicht resistent gegen Node-Ausfälle, es sei denn, Sie konfigurieren eine Art von Netzwerk-Load-Balancing. Erstellen Sie als einfache Lösung einen Round-Robin-DNS-Eintrag für die drei statischen IP-Adressen, die für Rancher-Server reserviert sind. Diese DNS-Einträge sollten sich auf den Rancher-Server-FQDN auflösen, den Sie für den Zugriff auf den Rancher-Server-Host verwenden, der nach Abschluss der Bereitstellung die Rancher-Web-UI dient.

Implementierungsarten

Sie können NetApp HCI auf folgende Weise implementieren:

- **Demo-Bereitstellungen**: Wenn DHCP in der gezielten Bereitstellungsumgebung verfügbar ist und Sie die Rancher-on-NetApp HCI-Fähigkeit demonstrieren möchten, dann ist eine DHCP-Bereitstellung am sinnvollsten.

  Bei diesem Implementierungsmodell ist die Rancher-UI von jedem der drei Nodes im Management-Cluster aus zugänglich.

  Wenn in Ihrem Unternehmen kein DHCP verwendet wird, können Sie es dennoch mithilfe von vier vor der Bereitstellung zugewiesenen statischen IP-Adressen ausprobieren, ähnlich wie bei einer Produktionsimplementierung.

- **Produktionsimplementierungen**: Für Produktionsbereitstellungen oder wenn DHCP in der zielgerichteten Bereitstellungsumgebung nicht verfügbar ist, sind ein wenig mehr Vorbereitungsarbeiten erforderlich. Der erste Schritt besteht darin, drei aufeinander folgende IP-Adressen zu erhalten. Sie treten während der Implementierung die erste ein.

  Für Produktionsumgebungen empfehlen wir die Verwendung von L4-Load-Balancing oder Round-Robin-DNS-Konfiguration. Dies erfordert eine vierte IP-Adresse und einen separaten Eintrag in Ihrer DNS-Konfiguration.

  - **L4 Load Balancing**: Dies ist eine Technik, bei der eine virtuelle Maschine oder ein Container, der eine Anwendung wie nginx hostet, konfiguriert ist, um Anfragen auf die drei Knoten des Management-Clusters zu verteilen.
  - **Round-Robin DNS**: Dies ist eine Technik, bei der im DNS-System ein einziger Hostname konfiguriert ist, der Anforderungen zwischen den drei Hosts rotiert, die das Management-Cluster bilden.

Rancher FQDN

Für die Installation ist eine Rancher-URL erforderlich, die den vollständig qualifizierten Domänennamen (FQDN) des Hosts enthält, auf dem die Rancher-UI nach Abschluss der Installation bereitgestellt wird.

In allen Fällen ist die Rancher-UI in Ihrem Browser über HTTPS-Protokoll (Port 443) zugänglich.

Für Produktionsimplementierungen ist ein FQDN erforderlich, der für die Load-Balancing-Verteilung über die Management-Cluster-Nodes konfiguriert ist. Ohne den Einsatz von FQDN und Load Balancing ist die Umgebung nicht robust und nur für Demo-Umgebungen geeignet.

Erforderliche Ports

Stellen Sie sicher, dass die Liste der Ports im Abschnitt "Ports for Rancher Server Nodes on RKE" des Abschnitts **Rancher Nodes** des offiziellen "Rancher-Dokumentation" in Ihrer Firewall-Konfiguration zu und von den Knoten, auf denen Rancher Server ausgeführt wird, geöffnet ist.

Erforderliche URLs

Die folgenden URLs sollten über die Hosts zugänglich sein, auf denen sich die Rancher-Steuerebene befindet:

URL	Beschreibung
https://charts.jetstack.io/	Kubernetes-Integration
https://releases.rancher.com/server-charts/stable	Rancher Software-Downloads
https://entropy.ubuntu.com/	Ubuntu entropy Service für zufällige Anzahl Erzeugung
https://raw.githubusercontent.com/vmware/cloud-init-vmware-guestinfo/v1.3.1/install.sh	VMware Gastzugänge
https://download.docker.com/linux/ubuntu/gpg	Docker Ubuntu GPG Public Key
https://download.docker.com/linux/ubuntu	Link zum Docker Download
https://hub.docker.com/	Docker Hub für NetApp Hybrid Cloud Control

NetApp HCI-Ranking einsetzen

Um Rancher in Ihrer NetApp HCI Umgebung einzusetzen, setzen Sie zuerst Rancher auf NetApp HCI ein.

Bevor Sie mit der Bereitstellung beginnen, überprüfen Sie den freien Speicherplatz des Datastore und andere "Anforderungen für die Rangliste auf NetApp HCI".

Rancher Support ist nicht in Ihrer NetApp Support Edge Vereinbarung enthalten. Wenden Sie sich an den NetApp Vertrieb oder Ihren Reseller, um Optionen zu erhalten. Wenn Sie Rancher Support von NetApp erwerben, erhalten Sie eine E-Mail mit Anweisungen.

Was passiert, wenn Sie Rancher auf NetApp HCI implementieren?

Die Implementierung umfasst folgende Schritte, die jeweils weiter beschrieben werden:

- Verwenden Sie NetApp Hybrid Cloud Control, um die Implementierung zu initiieren.
- Die Rancher Implementierung erstellt ein Management Cluster, das drei Virtual Machines enthält.

  Jeder Virtual Machine werden alle Kubernetes-Rollen sowohl für die Kontrollebene als auch für Worker zugewiesen. Das bedeutet, dass die Rancher-UI auf jedem Knoten verfügbar ist.

- Die Rancher Control Plane (oder *Rancher Server*) ist ebenfalls installiert. Zur Vereinfachung der Bereitstellung wird die NetApp HCI Node-Vorlage in Rancher verwendet. Die Rancher Control Plane arbeitet automatisch mit der Konfiguration zusammen, die in der NetApp Deployment Engine zum Aufbau der NetApp HCI Infrastruktur verwendet wurde.
- Nach der Entwicklung erhalten Sie von NetApp eine E-Mail, die Ihnen die Möglichkeit bietet, sich für NetApp Support bei Rancher Implementierungen auf NetApp HCI zu registrieren.
- Nach der Implementierung können die Dev- und Ops-Teams ihre Benutzer-Cluster, ähnlich wie bei Rancher-Implementierungen, bereitstellen.

Schritte zur Bereitstellung eines Ranchers auf NetApp HCI

- Rufen Sie die NetApp Hybrid Cloud Control auf
- NetApp HCI-Ranking einsetzen
- Überprüfen Sie die Bereitstellung mit vCenter Server

Rufen Sie die NetApp Hybrid Cloud Control auf

Um mit der Implementierung zu beginnen, rufen Sie NetApp Hybrid Cloud Control auf.

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

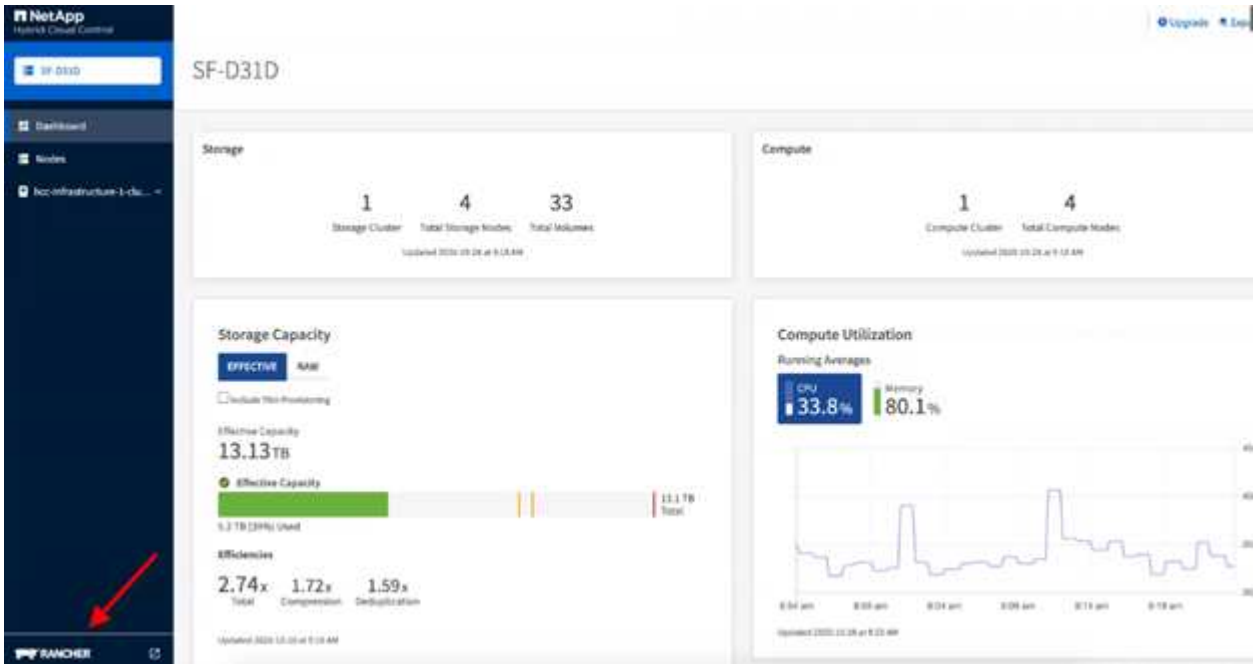
   ```
   https://<ManagementNodeIP>
   ```

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

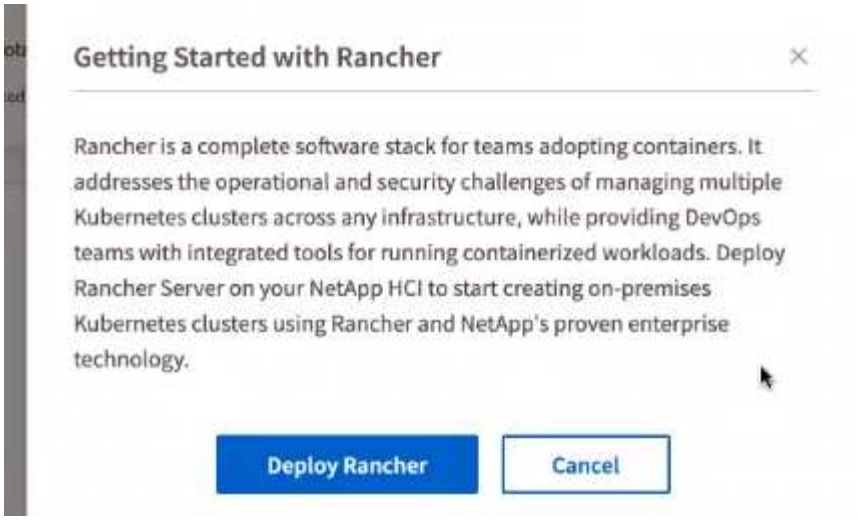
   Die Benutzeroberfläche von NetApp Hybrid Cloud Control wird angezeigt.

NetApp HCI-Ranking einsetzen

1. Wählen Sie im Hybrid Cloud Control das **Rancher**-Symbol unten links in der Navigationsleiste aus.

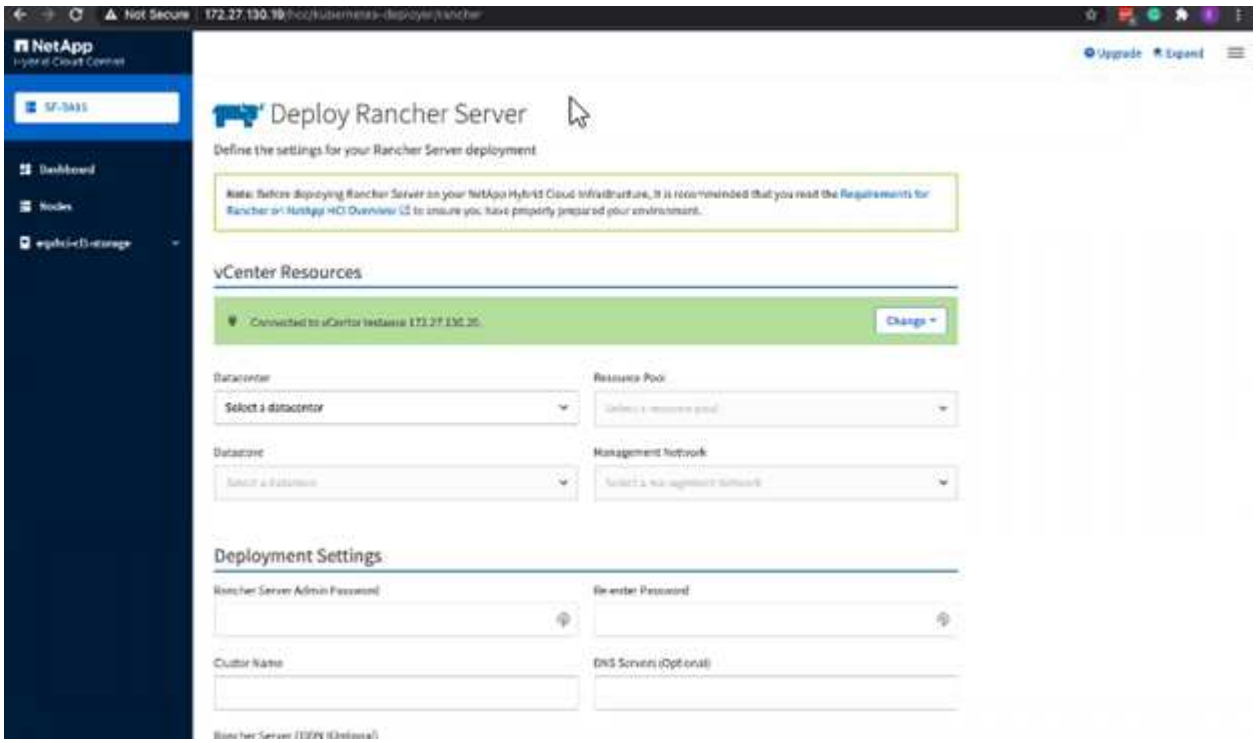


   Ein Popup-Fenster zeigt eine Meldung über die ersten Schritte mit Rancher.



2. Wählen Sie **Rancher Bereitstellen**.

   Die Rancher-UI wird angezeigt.



   Ihre vCenter Zugangsdaten werden basierend auf Ihrer Installation der NetApp Deployment Engine erfasst.

3. Geben Sie **vCenter Ressourcen** Informationen ein. Einige Felder werden als Nächstes beschrieben.
   - **Datacenter**: Wählen Sie ein Rechenzentrum. Nachdem Sie das Datacenter ausgewählt haben, werden alle anderen Felder bereits ausgefüllt, obwohl Sie sie ändern können.
   - **Datastore**: Wählen Sie einen Datenspeicher auf den NetApp HCI Speicherknoten. Dieser Datenspeicher sollte für alle VMware Hosts ausfallsicher sein und auf sie zugreifen können. Wählen Sie keinen lokalen Datenspeicher aus, auf den nur einer der Hosts zugreifen kann.
   - **Managementnetzwerk**: Dieser sollte von den Management Stations und vom Virtual Machine Network aus zugänglich sein, wo die User Cluster gehostet werden.

4. Geben Sie die * Bereitstellungseinstellungen*-Informationen ein:
   - **DNS-Server**: Optional. Wenn Sie Load Balancing verwenden, geben Sie die Informationen zum internen DNS-Server ein.
   - **Rancher Server FQDN**: Um sicherzustellen, dass der Rancher Server bei Knotenausfällen verfügbar bleibt, geben Sie einen vollständig qualifizierten Domänennamen (FQDN) an, den Ihr DNS-Server auf eine der IP-Adressen auflösen kann, die den Knoten des Rancher-Server-Clusters zugewiesen sind. Dieser FQDN mit dem Präfix „https“ wird zur Rancher-URL, mit der Sie auf Ihre Rancher-Implementierung zugreifen können.

     Wenn kein Domänenname angegeben ist, wird stattdessen Wildcard DNS verwendet, und Sie können mit einer der URLs, die nach Abschluss der Bereitstellung angezeigt werden, auf den Rancher Server zugreifen.
5. Geben Sie **Erweiterte Einstellungen** Informationen ein:
   - **Statische IP-Adressen zuweisen**: Wenn Sie statische IP-Adressen aktivieren, geben Sie StartIP-Adressen für drei IPv4-Adressen nacheinander an, eine für jede virtuelle Verwaltungscluster-Maschine. Rancher auf NetApp HCI setzt drei Management Cluster Virtual Machines ein.
   - **Proxy-Server Konfigurieren**:
6. Prüfen Sie das Kontrollkästchen für die Rancher-Endbenutzer-Lizenzvereinbarung, und aktivieren Sie es.
7. Überprüfen Sie das Kontrollkästchen, und aktivieren Sie das Kontrollkästchen, um Informationen zur Rancher-Software zu bestätigen.
8. Wählen Sie **Deploy**.

   Ein Balken zeigt den Fortschritt der Bereitstellung an.

   Die Rancher-Implementierung konnte etwa 15 Minuten dauern.

   Wenn die Bereitstellung abgeschlossen ist, zeigt Rancher eine Meldung über den Abschluss an und liefert eine Rancher-URL.

9. Notieren Sie die Rancher-URL, die am Ende der Bereitstellung angezeigt wird. Sie verwenden diese URL, um auf die Rancher-UI zuzugreifen.

Überprüfen Sie die Bereitstellung mit vCenter Server

Im vSphere-Client sehen Sie das Rancher Management Cluster, das die drei Virtual Machines umfasst.

Nachdem Sie die Bereitstellung abgeschlossen haben, dürfen Sie die Konfiguration des virtuellen VM-Clusters des Rancher-Servers nicht ändern oder die virtuellen Maschinen entfernen. Rancher auf NetApp HCI setzt für den normalen Betrieb auf die bereitgestellte RKE-Management-Cluster-Konfiguration.

Was kommt als Nächstes?

Nach der Bereitstellung können Sie Folgendes tun:

- "Aufgaben nach der Implementierung abschließen"
- "Installation von Trident mit Rancher auf NetApp HCI"
- "Implementieren von Benutzer-Clustern und Applikationen"
- "Managen Sie die Rangliste auf NetApp HCI"
- "Überwachen Sie die Rangliste auf NetApp HCI"

Weitere Informationen

- "Fehlerbehebung bei der Rancher-Implementierung"
- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "Ressourcen-Seite zu NetApp HCI"

Aufgaben nach der Implementierung

Überblick über Aufgaben nach der Implementierung

Nachdem Sie Rancher auf NetApp HCI implementiert haben, sollten Sie die Aktivitäten nach der Implementierung fortsetzen.

- "Stellen Sie sicher, dass Rancher Support-Parität erreicht ist"
- "Verbesserte Resiliency für Rancher Virtual Machines"
- "Monitoring konfigurieren"
- "Installation Von Trident"
- "Aktivieren Sie die Trident Unterstützung für Benutzer-Cluster"

Weitere Informationen

- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"

Stellen Sie sicher, dass Rancher Support-Parität erreicht ist

Nachdem Sie Rancher auf NetApp HCI implementiert haben, müssen Sie sicherstellen, dass die Anzahl der erworbenen Rancher Support-Kerne mit der Anzahl der CPU-Kerne übereinstimmt, die Sie für Rancher Management-VMs und Benutzer-Cluster verwenden.

Wenn Sie Rancher Support nur für einen Teil Ihrer NetApp HCI-Ressourcen erworben haben, müssen Sie in VMware vSphere Maßnahmen ergreifen, um sicherzustellen, dass die Rancher auf NetApp HCI und den verwalteten Benutzer-Clustern nur auf Hosts ausgeführt werden, für die Sie Rancher Support erworben haben.

In der Dokumentation zu VMware vSphere finden Sie Informationen darüber, wie Sie dies durch Beschränkung von Computing-Workloads auf bestimmte Hosts gewährleisten können.

Weitere Informationen

- "VSphere HA und DRS Affinitätsregeln"
- "Anti-Affinitätsregeln für VMs erstellen"
- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"

Verbesserte Resiliency für Rancher Virtual Machines

Nach der Implementierung von Rancher auf NetApp HCI enthält Ihre vSphere Umgebung drei neue Nodes als Virtual Machines, um die Rancher Umgebung zu hosten. Die Rancher Web-UI ist von jedem dieser Knoten verfügbar. Um eine vollständige Ausfallsicherheit zu erzielen, sollten sich die drei Virtual Machines zusammen mit den entsprechenden virtuellen Laufwerken nach Ereignissen wie Stromkreisläufen und Failover auf einem anderen physischen Host befinden.

Um sicherzustellen, dass jede VM und die zugehörigen Ressourcen auf einem anderen physischen Host bleiben, können Sie Antiaffinitätsregeln für VMware vSphere Distributed Resource Scheduler (DRS) erstellen. Dies ist im Rahmen der Rancher-Studie zur NetApp HCI-Implementierung nicht automatisiert.

Anweisungen zur Konfiguration von DRS-Antiaffinitätsregeln finden Sie in den folgenden VMware-Dokumentationsmaterialien:

"Anti-Affinitätsregeln für VMs erstellen"

"VSphere HA und DRS Affinitätsregeln"

Weitere Informationen

- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"

Aktivieren Sie Monitoring

Nach der Implementierung von Rancher auf NetApp HCI können Sie die Funktionen zur Active IQ-Storage-Überwachung (für SolidFire All-Flash-Storage und NetApp HCI) und zur Computing-Überwachung von NetApp HCI (nur für NetApp HCI) aktivieren, falls Sie dies bei der Installation oder bei einem Upgrade noch nicht getan haben.

Anweisungen zum Aktivieren der Überwachung finden Sie unter "Active IQ- und NetApp HCI-Monitoring aktivieren".

Weitere Informationen

- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"

Installation Von Trident

Erfahren Sie, wie Sie Trident installieren, nachdem Sie Rancher auf NetApp HCI installiert haben. Trident ist ein Storage-Orchestrator, der sich in Docker und Kubernetes sowie in Plattformen auf Basis dieser Technologien wie Red hat OpenShift, Rancher und IBM Cloud Private integrieren lässt. Ziel von Trident ist es, die Bereitstellung, Anbindung und Nutzung von Storage für Applikationen transparent und reibungslos zu gestalten. Trident ist ein vollständig von NetApp unterstütztes Open-Source-Projekt. Mit Trident erstellen, managen und interagieren Sie mit persistenten Storage Volumes im gewohnten Kubernetes-Standardformat.

Weitere Informationen zu Trident finden Sie im "Trident Dokumentation".

Was Sie benötigen

- Sie haben Rancher auf NetApp HCI installiert.
- Sie haben Ihre Benutzer-Cluster bereitgestellt.
- Sie haben die Benutzer-Cluster-Netzwerke für Trident konfiguriert. Anweisungen finden Sie unter "Aktivieren Sie die Trident Unterstützung für Benutzer-Cluster" .
- Sie haben die erforderlichen Schritte zur Vorbereitung der Arbeits-Nodes für Trident abgeschlossen. Siehe "Trident Dokumentation".

Über diese Aufgabe

Der Trident Installationskatalog ist im Rahmen der Rancher Installation mit NetApp Hybrid Cloud Control installiert. In dieser Aufgabe installieren und konfigurieren Sie Trident mit dem Installationskatalog. Im Rahmen der Rancher-Installation stellt NetApp eine Node-Vorlage zur Verfügung. Wenn Sie nicht planen, die Node-Vorlage von NetApp zu verwenden und Sie RHEL oder CentOS bereitstellen möchten, kann es zusätzliche Anforderungen geben. Wenn Sie Ihren Arbeitsknoten zu RHEL oder CentOS wechseln, gibt es mehrere Voraussetzungen, die erfüllt werden sollten. Siehe "Trident Dokumentation".

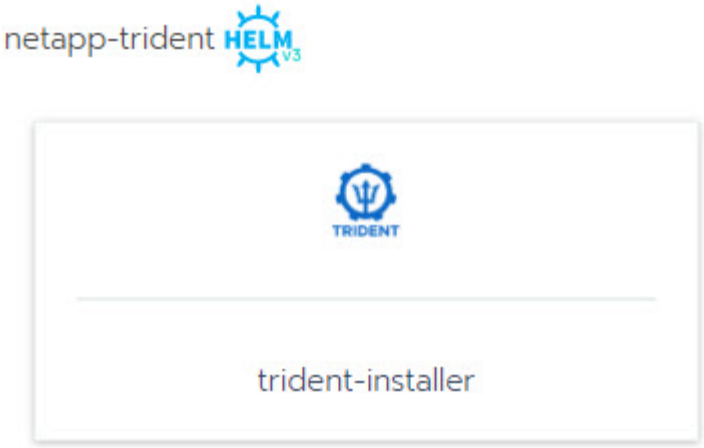
Schritte

1. Wählen Sie in der Rancher UI ein Projekt für Ihren Benutzer-Cluster aus.

   Informationen zu Projekten und Namespaces finden Sie im "Rancher-Dokumentation".

2. Wählen Sie **Apps**, und wählen Sie **Start**.

3. Wählen Sie auf der Seite **Catalog** das Trident-Installationsprogramm aus.



Auf der sich öffnenden Seite können Sie den Pfeil **Detaillierte Beschreibungen** auswählen, um mehr über die Trident App zu erfahren und auch den Link zum "Trident Dokumentation" .

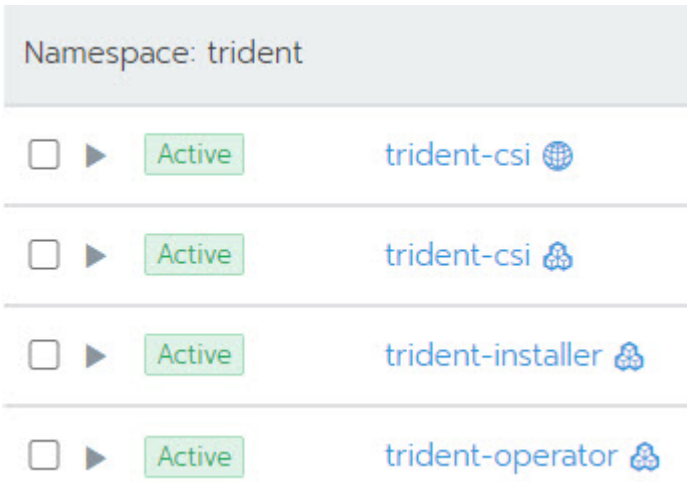
4. Wählen Sie den Pfeil **Konfigurationen Optionen** aus, und geben Sie die Anmeldeinformationen und Informationen zur Speicherkonfiguration ein.

Der standardmäßige Storage-Mandant ist NetApp HCI. Sie können diesen Wert ändern. Sie können auch den Back-End-Namen ändern. Ändern Sie jedoch nicht den Standardwert für den Storage-Treiber, welcher ist **solidfire-san**.

5. Wählen Sie **Start**.

   Dadurch wird der Trident-Workload auf dem * Trident Namespace installiert.

6. Wählen Sie **Ressourcen > Workloads** aus, und überprüfen Sie, ob der Namespace **Trident** die folgenden Komponenten umfasst:



7. (Optional) Wählen Sie **Storage** für das Benutzer-Cluster, um die Speicherklassen anzuzeigen, die Sie für Ihre persistenten Volumes verwenden können.

Die drei Storage-Klassen sind **solidfire-Gold**, **solidfire-Silver** und **solidfire-Bronze**. Sie können eine dieser Speicherklassen als Standard verwenden, indem Sie das Symbol in der Spalte **Standard** auswählen.

Weitere Informationen

- "Aktivieren Sie die Trident Unterstützung für Benutzer-Cluster"
- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"

Aktivieren Sie die Trident Unterstützung für Benutzer-Cluster

Wenn in der NetApp HCI Umgebung keine Route zwischen den Management- und Storage-Netzwerken besteht und Sie Benutzer-Cluster implementieren, die Unterstützung für Trident benötigen, müssen Sie nach der Installation von Trident weitere Netzwerke für Benutzercluster konfigurieren. Für jedes Benutzer-Cluster müssen Sie die Kommunikation zwischen Management- und Storage-Netzwerken ermöglichen. Hierzu können Sie die Netzwerkkonfiguration für jeden Node im Benutzer-Cluster ändern.

Über diese Aufgabe

Führen Sie diese allgemeinen Schritte aus, um die Netzwerkkonfiguration für jeden Node im Benutzer-Cluster zu ändern. Bei diesen Schritten wird davon ausgegangen, dass Sie das Benutzer-Cluster mit der Standard-Node-Vorlage erstellt haben, die mit Rancher auf NetApp HCI installiert ist.

Sie können diese Änderungen im Rahmen einer benutzerdefinierten Node-Vorlage vornehmen, die für zukünftige Benutzer Cluster verwendet werden soll.

Schritte

1. Implementieren Sie ein Benutzer-Cluster mit vorhandener Standardvorlage.
2. Verbinden Sie das Storage-Netzwerk mit dem Benutzer-Cluster.
   a. Öffnen Sie den VMware vSphere Web-Client für die verbundene vCenter-Instanz.
   b. Wählen Sie in der Strukturansicht Hosts und Cluster einen Knoten im neu bereitgestellten Benutzer-Cluster aus.
   c. Bearbeiten Sie die Einstellungen des Node.
   d. Fügen Sie im Dialogfeld Einstellungen einen neuen Netzwerkadapter hinzu.
   e. Suchen Sie in der Dropdown-Liste **New Network** nach einem Netzwerk und wählen Sie **HCI_Internal_Storage_Data_Network** aus.
   f. Erweitern Sie den Abschnitt Netzwerkadapter, und notieren Sie die MAC-Adresse für den neuen Netzwerkadapter.
   g. Wählen Sie **OK**.
3. Laden Sie in Rancher die private SSH-Schlüsseldatei für jeden Knoten im Benutzer-Cluster herunter.
4. Stellen Sie eine Verbindung über SSH mit einem Node im Benutzer-Cluster her und verwenden Sie die

Datei mit dem privaten Schlüssel, die Sie für diesen Node heruntergeladen haben:

```
ssh -i <private key filename> <ip address>
```

5. Bearbeiten und speichern Sie als Superuser die `/etc/netplan/50-cloud-init.yaml` Datei, sodass sie den Abschnitt enthält `ens224`, ähnlich wie im folgenden Beispiel. Ersetzen Sie `<MAC address>` diese durch die zuvor aufgezeichnete MAC-Adresse:

```
network:
    ethernets:
        ens192:
            dhcp4: true
            match:
                macaddress: 00:50:56:91:1d:41
            set-name: ens192
        ens224:
            dhcp4: true
            match:
                macaddress: <MAC address>
            set-name: ens224
    version: 2
```

6. Verwenden Sie den folgenden Befehl, um das Netzwerk neu zu konfigurieren:

```
`netplan try`
```

7. Wiederholen Sie die Schritte 4 bis 6 für jeden verbleibenden Node im Benutzer-Cluster.
8. Wenn Sie das Netzwerk für jeden Node im Benutzer-Cluster neu konfiguriert haben, können Sie Applikationen im Benutzer-Cluster implementieren, die Trident verwenden.

Implementieren von Benutzer-Clustern und Applikationen

Nach der Bereitstellung von Rancher auf NetApp HCI können Sie Benutzer-Cluster einrichten und diesen Clustern Applikationen hinzufügen.

Implementieren Sie Benutzer-Cluster

Nach der Implementierung können die Dev- und Ops-Teams ihre Kubernetes-Benutzer-Cluster, ähnlich wie bei allen Rancher-Implementierungen, implementieren, auf denen sie Applikationen implementieren können.

1. Greifen Sie über die am Ende der Rancher-Implementierung bereitgestellte URL auf die Rancher-UI zu.
2. Erstellen von Benutzer-Clustern. Siehe Rancher Dokumentation über "Implementierung von Workloads".
3. Bereitstellung von Benutzer-Clustern in der Rangliste auf NetApp HCI Siehe Rancher Dokumentation über "Einrichtung von Kubernetes Clustern in Rancher".

Implementieren von Applikationen auf Benutzer-Clustern

Wie bei jeder Rancher-Implementierung fügen Sie auch Applikationen auf Kubernetes-Clustern hinzu.

Siehe Rancher Dokumentation über "Cluster-übergreifende Implementierung von Applikationen".

Weitere Informationen

- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "Ressourcen-Seite zu NetApp HCI"

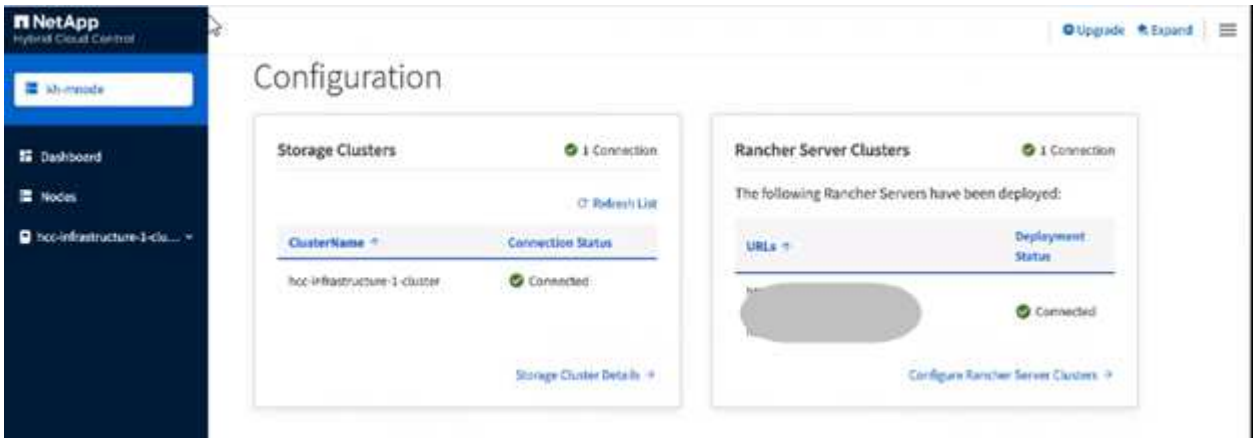
Managen Sie die Rangliste auf NetApp HCI

Nach der Bereitstellung von Rancher auf NetApp HCI können Sie die URLs und den Status der Rancher-Server-Cluster anzeigen. Sie können auch den Rancher-Server löschen.

Identifizieren Sie die URLs und den Status der Rancher-Server-Cluster

Sie können die Cluster-URLs des Rancher-Servers identifizieren und den Serverstatus ermitteln.

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 oben rechts das Options-Symbol aus und wählen Sie **Configure** aus.



Auf der Seite Rancher-Servercluster wird eine Liste der installierten Rancher-Server-Cluster, der zugehörigen URL und des Status angezeigt.

Weitere Informationen

- "Rancher Entfernen"
- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "Ressourcen-Seite zu NetApp HCI"

Überwachung eines Rangers zur NetApp HCI-Implementierung

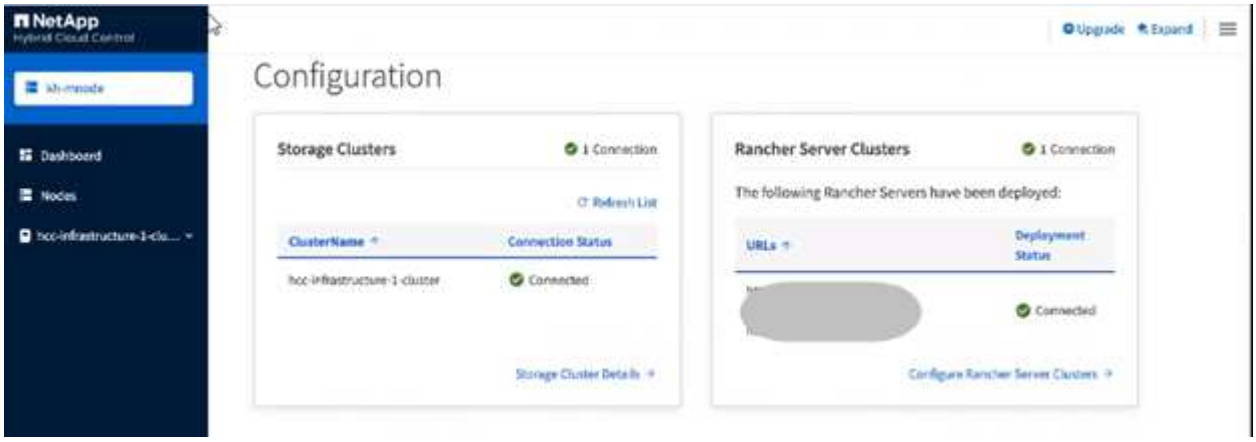
Es gibt verschiedene Möglichkeiten, Rancher-Server, Management-Cluster und andere Details zu überwachen.

- NetApp Hybrid Cloud Control
- Rancher UI
- NetApp Active IQ
- VCenter Server

Überwachen Sie Rancher mit NetApp Hybrid Cloud Control

Mit NetApp Hybrid Cloud Control können Sie den URL-Status des Rancher Servers und den Cluster-Status des Rancher Servers anzeigen. Sie können auch die Knoten überwachen, in denen Rancher ausgeführt wird.

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Element Storage-Cluster-Administrators bereitstellen.
2. Wählen Sie im Dashboard oben rechts das Options-Symbol aus und wählen Sie **Configure** aus.



3. Um die Knoteninformationen anzuzeigen, erweitern Sie im Hybrid Cloud Control Dashboard den Namen Ihres Storage-Clusters und wählen Sie **Nodes** aus.

Überwachen Sie die Rancher-Überwachung mit der Rancher-UI

Mithilfe der Rancher UI können Sie Informationen über die Ranglisten auf NetApp HCI Management-Clustern und Benutzer-Clustern anzeigen.

In der Rancher UI werden Management-Cluster als „lokale Cluster“ bezeichnet.

1. Greifen Sie über die am Ende der Rancher-Implementierung bereitgestellte URL auf die Rancher-UI zu.
2. Siehe "Überwachung in Rancher v2.5".

Überwachen Sie das Rancher-Ranking mit NetApp Active IQ

Mithilfe von NetApp Active IQ können Sie die Rancher-Telemetrie anzeigen, wie z. B.

Installationsinformationen, Nodes, Cluster, Status, Namespace-Informationen, Und vieles mehr.

1. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Element Storage-Cluster-Administrators bereitstellen.
2. Wählen Sie im Menü oben rechts **NetApp Active IQ** aus.

Überwachen Sie Rancher mit vCenter Server

Mit vCenter Server können Sie die Rancher Virtual Machines überwachen.

Weitere Informationen

- "Rancher Dokumentation über Architektur"
- "Kubernetes – Terminologie für Rancher"
- "NetApp Element Plug-in für vCenter Server"
- "Ressourcen-Seite zu NetApp HCI"

Upgrade-Rangliste auf NetApp HCI

Für ein Upgrade der Rancher Software können Sie die UI (HCC) oder DIE REST-API von NetApp Hybrid Cloud Control (HCC) verwenden. HCC bietet einen einfachen Prozess zur Aktualisierung der Komponenten Ihrer Rancher-Bereitstellung, einschließlich Rancher-Server, Rancher Kubernetes Engine (RKE) und des Node-Betriebssystems des Management-Clusters (für Sicherheitsupdates). Alternativ können Sie die API zur Automatisierung von Upgrades verwenden.

Upgrades sind für Komponenten anstelle eines kumulativen Pakets verfügbar. Daher sind einige Komponenten-Upgrades wie das Ubuntu OS in einer schnelleren Kadenz verfügbar. Upgrades wirken sich nur auf Ihre Rancher Server-Instanz und den Management-Cluster aus, auf dem Rancher Server bereitgestellt wird. Upgrades auf das Ubuntu OS des Management-Clusters sind nur für kritische Sicherheitspatches und führen kein Upgrade des Betriebssystems durch. Benutzer-Cluster können nicht von NetApp Hybrid Cloud Control aktualisiert werden.

Was Sie benötigen

- **Administratorrechte**: Sie haben Berechtigungen für den Storage Cluster Administrator, um das Upgrade durchzuführen.
- **Management Services**: Sie haben Ihr Management Services Bundle auf die neueste Version aktualisiert.

> Sie müssen ein Upgrade auf das neueste Management Services Bundle 2.17 oder höher durchführen, um die Rancher Funktionen nutzen zu können.

- **System-Ports**: Bei Upgrade-Nutzung von NetApp Hybrid Cloud Control haben Sie sichergestellt, dass die erforderlichen Ports geöffnet sind. Weitere Informationen finden Sie unter "Netzwerkports" .
- **Endbenutzer-Lizenzvertrag (EULA)**: Ab Management Services 2.20.69 müssen Sie die EULA akzeptieren und speichern, bevor Sie die NetApp Hybrid Cloud Control UI oder API verwenden, um ein Rancher-Upgrade durchzuführen:
  a. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser:

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

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

c. Wählen Sie **Upgrade** oben rechts auf der Schnittstelle aus.

d. Die EULA erscheint. Scrollen Sie nach unten, wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Updates** und wählen Sie **Speichern**.

Upgrade-Optionen

Wählen Sie einen der folgenden Upgrade-Prozesse:

- Mit der NetApp Hybrid Cloud Control UI können Sie eine Rancher-Implementierung aktualisieren
- Mit der NetApp Hybrid Cloud Control API können Sie eine Rancher-Implementierung aktualisieren

Mit der NetApp Hybrid Cloud Control UI können Sie eine Rancher-Implementierung aktualisieren

Über die NetApp Hybrid Cloud Control UI lassen sich alle dieser Komponenten in der Rancher-Implementierung aufrüsten:

- Rancher Server
- Rancher Kubernetes Engine (RKE)
- Sicherheitsupdates für Node OS

Was Sie benötigen

- Eine gute Internetverbindung. Dark Site Upgrades sind nicht verfügbar.

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 **Upgrade** oben rechts auf der Schnittstelle aus.
4. Wählen Sie auf der Seite **Upgrades** die Option **Rancher**.
5. Wählen Sie das Menü **Aktionen** für die Software, die Sie aktualisieren möchten.
   - Rancher Server
   - Rancher Kubernetes Engine (RKE)
   - Sicherheitsupdates für Node OS
6. Wählen Sie **Upgrade** für Rancher Server oder RKE Upgrades oder **Apply Upgrade** für Knoten OS Sicherheitsupdates.

Bei Node OS werden täglich unbeaufsichtigte Upgrades für Sicherheitspatches ausgeführt, der Node wird jedoch nicht automatisch neu gestartet. Durch das Anwenden von Upgrades werden Sie jeden Node neu booten, damit die Sicherheitsupdates wirksam werden.

Ein Banner zeigt an, dass die Aktualisierung der Komponente erfolgreich war. Es kann bis zu 15 Minuten Verzögerung geben, bevor die NetApp Hybrid Cloud Control UI die aktualisierte Versionsnummer anzeigt.

Mit der NetApp Hybrid Cloud Control API können Sie eine Rancher-Implementierung aktualisieren

Mit APIs können Sie jede dieser Komponenten in Ihrer Rancher-Implementierung aktualisieren:

- Rancher Server
- Rancher Kubernetes Engine (RKE)
- Node OS (für Sicherheits-Updates)

Sie können ein Automatisierungstool Ihrer Wahl verwenden, um die APIs oder DIE REST-API-UI auszuführen, die auf dem Management-Node verfügbar ist.

Optionen

- Upgrade Von Rancher Server
- Upgrade RKE
- Wenden Sie Sicherheitsupdates des Node-Betriebssystems an

Bei Node OS werden täglich unbeaufsichtigte Upgrades für Sicherheitspatches ausgeführt, der Node wird jedoch nicht automatisch neu gestartet. Durch das Anwenden von Upgrades werden Sie jeden Node neu booten, damit die Sicherheitsupdates wirksam werden.

Upgrade Von Rancher Server

API-Befehle

1. Initiieren Sie die Anforderung von Upgrade-Versionen der Liste:

```
curl -X POST "https://<ManagementNodeIP>/k8sdeployer/1/upgrade/rancher-versions" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

Sie können den vom API-Befehl verwendeten Träger finden `${TOKEN}`, wenn Sie "Autorisieren". Der Träger `${TOKEN}` ist in der Lockenantwort.

2. Abrufen des Aufgabenstatus mithilfe der Task-ID vom vorherigen Befehl und Kopieren der aktuellen Versionsnummer aus der Antwort:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Initiieren Sie die Upgrade-Anforderung für den Rancher-Server:

```
curl -X PUT "https://<mNodeIP>/k8sdeployer/1/upgrade/rancher/<version
number>" -H "accept: application/json" -H "Authorization: Bearer"
```

4. Abrufen des Aufgabenstatus mithilfe der Task-ID aus der Antwort des Upgrade-Befehls:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

SCHRITTE DER REST API-UI

1. Öffnen Sie die REST-API-UI für den Management-Node:

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

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 `mnode-client`ein.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Autorisierungsfenster.
3. Überprüfen Sie, ob das aktuelle Upgrade-Paket verfügbar ist:
   a. Führen Sie in DER REST API UI **POST /upgrade/rancher-Versionen** aus.
   b. Kopieren Sie aus der Antwort die Task-ID.
   c. Führen Sie **GET /task/{taskID}** mit der Task-ID aus dem vorherigen Schritt aus.
4. Kopieren Sie in der Antwort **/task/{taskID}** die aktuelle Versionsnummer, die Sie für das Upgrade verwenden möchten.
5. Führen Sie das Upgrade des Rancher Servers aus:
   a. Führen Sie in DER REST API-Benutzeroberfläche **PUT /upgrade/rancher/{Version}** mit der aktuellen Versionsnummer aus dem vorherigen Schritt aus.
   b. Kopieren Sie aus der Antwort die Task-ID.
   c. Führen Sie **GET /task/{taskID}** mit der Task-ID aus dem vorherigen Schritt aus.

Das Upgrade wurde erfolgreich abgeschlossen, wenn das die `PercentComplete` `100` aktualisierte Versionsnummer anzeigt und `results` anzeigt.

Upgrade RKE

API-Befehle

1. Initiieren Sie die Anforderung von Upgrade-Versionen der Liste:

```
curl -X POST "https://<mNodeIP>/k8sdeployer/1/upgrade/rke-versions" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

Sie können den vom API-Befehl verwendeten Träger finden `${TOKEN}`, wenn Sie "Autorisieren". Der Träger `${TOKEN}` ist in der Lockenantwort.

2. Abrufen des Aufgabenstatus mithilfe der Task-ID vom vorherigen Befehl und Kopieren der aktuellen Versionsnummer aus der Antwort:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Initiieren Sie die RKE-Upgrade-Anforderung

```
curl -X PUT "https://<mNodeIP>/k8sdeployer/1/upgrade/rke/<version
number>" -H "accept: application/json" -H "Authorization: Bearer"
```

4. Abrufen des Aufgabenstatus mithilfe der Task-ID aus der Antwort des Upgrade-Befehls:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

SCHRITTE DER REST API-UI

1. Öffnen Sie die REST-API-UI für den Management-Node:

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

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 `mnode-client`ein.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Autorisierungsfenster.
3. Überprüfen Sie, ob das aktuelle Upgrade-Paket verfügbar ist:
   a. Führen Sie von DER REST API UI **POST /upgrade/rke-Versionen** aus.
   b. Kopieren Sie aus der Antwort die Task-ID.
   c. Führen Sie **GET /task/{taskID}** mit der Task-ID aus dem vorherigen Schritt aus.
4. Kopieren Sie in der Antwort **/task/{taskID}** die aktuelle Versionsnummer, die Sie für das Upgrade verwenden möchten.

5. Führen Sie das RKE-Upgrade aus:
   a. Führen Sie in DER REST API UI **PUT /Upgrade/rke/{Version}** mit der aktuellen Versionsnummer des vorherigen Schritts aus.
   b. Kopieren Sie die Task-ID aus der Antwort.
   c. Führen Sie **GET /task/{taskID}** mit der Task-ID aus dem vorherigen Schritt aus.

Das Upgrade wurde erfolgreich abgeschlossen, wenn das die `PercentComplete` `100` aktualisierte Versionsnummer anzeigt und `results` anzeigt.

Wenden Sie Sicherheitsupdates des Node-Betriebssystems an

API-Befehle

1. Initiieren Sie die Anforderung für Schecks-Upgrades:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/upgrade/checkNodeUpdates"
-H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

> Sie können den vom API-Befehl verwendeten Träger finden `${TOKEN}`, wenn Sie "Autorisieren". Der Träger `${TOKEN}` ist in der Lockenantwort.

2. Abrufen des Aufgabenstatus mithilfe der Task-ID vom vorherigen Befehl und Überprüfen Sie, ob eine aktuellere Versionsnummer über die Antwort verfügbar ist:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Anwenden der Node-Updates:

```
curl -X POST "https://<mNodeIP>/k8sdeployer/1/upgrade/applyNodeUpdates"
-H "accept: application/json" -H "Authorization: Bearer"
```

> Bei Node OS werden täglich unbeaufsichtigte Upgrades für Sicherheitspatches ausgeführt, der Node wird jedoch nicht automatisch neu gestartet. Durch das Anwenden von Upgrades werden bei jedem Node nacheinander neu gebootet, damit die Sicherheitsupdates wirksam werden.

4. Aufgabenstatus mithilfe der Task-ID aus der Aktualisierungsantwort abrufen `applyNodeUpdates`:

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

SCHRITTE DER REST API-UI

1. Öffnen Sie die REST-API-UI für den Management-Node:

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

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 `mnode-client`ein.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Autorisierungsfenster.
3. Überprüfen Sie, ob ein Upgrade-Paket verfügbar ist:
   a. Führen Sie von DER REST API UI **GET /Upgrade/checkNodeUpdates** aus.
   b. Kopieren Sie aus der Antwort die Task-ID.
   c. Führen Sie **GET /task/{taskID}** mit der Task-ID aus dem vorherigen Schritt aus.
   d. Überprüfen Sie anhand der **/task/{taskID}**-Antwort, ob eine aktuellere Versionsnummer als die Nummer vorhanden ist, die derzeit auf Ihre Knoten angewendet wird.
4. Wenden Sie die Upgrades des Node-Betriebssystems an:

> Bei Node OS werden täglich unbeaufsichtigte Upgrades für Sicherheitspatches ausgeführt, der Node wird jedoch nicht automatisch neu gestartet. Durch das Anwenden von Upgrades werden bei jedem Node nacheinander neu gebootet, damit die Sicherheitsupdates wirksam werden.

   a. Führen Sie in DER REST API-Benutzeroberfläche **POST /upgrade/applyNodeUpdates** aus.
   b. Kopieren Sie aus der Antwort die Task-ID.
   c. Führen Sie **GET /task/{taskID}** mit der Task-ID aus dem vorherigen Schritt aus.
   d. Überprüfen Sie anhand der Antwort **/task/{taskID}**, ob das Upgrade angewendet wurde.

Das Upgrade wurde erfolgreich abgeschlossen, wenn das die `PercentComplete` `100` aktualisierte Versionsnummer anzeigt und `results` anzeigt.

Weitere Informationen

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

Entfernen Sie eine Rancher-Installation auf NetApp HCI

Wenn Sie versehentlich Rancher auf NetApp HCI mit falschen Informationen bereitstellen (z. B. einen falschen Rancher-Server-FQDN), müssen Sie die Installation entfernen und dann neu erstellen. Befolgen Sie diese Schritte, um die Rancher-Installation auf NetApp HCI-Instanz zu entfernen.

Durch diese Aktion werden die Benutzer-Cluster nicht gelöscht.

Sie möchten die Benutzer-Cluster möglicherweise beibehalten. Wenn Sie sie beibehalten, können Sie sie später zu einer anderen Rancher-Implementierung migrieren. Wenn Sie die Benutzer-Cluster löschen möchten, sollten Sie dies zuerst tun, bevor Sie den Rancher-Server löschen; andernfalls ist das Löschen der Benutzer-Cluster nach dem Rancher-Server gelöscht wird schwieriger.

Optionen

- Entfernen Sie Rancher auf NetApp HCI mit NetApp Hybrid Cloud Control (Empfohlen)
- Entfernen Sie Rancher auf NetApp HCI mit DER REST-API

Entfernen Sie Rancher auf NetApp HCI mit NetApp Hybrid Cloud Control

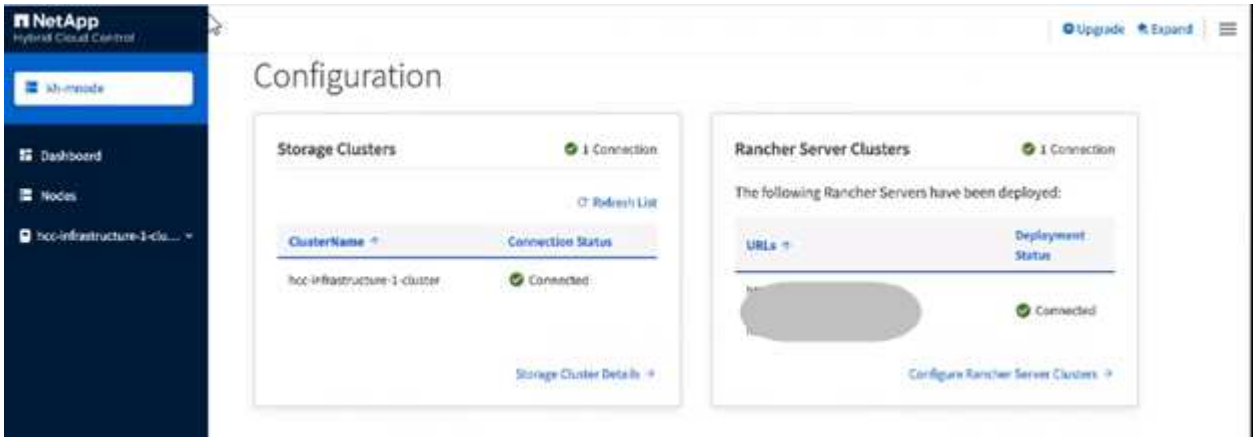
Die Web-UI von NetApp Hybrid Cloud Control entfernt die drei während der Implementierung für das Hosting des Rancher Servers festgelegten Virtual Machines.

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 im Dashboard oben rechts das Menü aus.
4. Wählen Sie **Konfigurieren**.



5. Wählen Sie im Bereich **Rancher Server Clusters Configure Rancher Server Clusters** aus.
6. Wählen Sie das Menü **Aktionen** für die Rancher-Installation, die Sie entfernen müssen.

Durch Auswahl von **Delete** wird der Rancher auf dem NetApp HCI-Verwaltungscluster sofort entfernt.

7. Wählen Sie **Löschen**.

Entfernen Sie Rancher auf NetApp HCI mit DER REST-API

Mithilfe der NetApp Hybrid Cloud Control REST-API sind die drei Virtual Machines entfernt, die während der Implementierung zum Hosten des Rancher Servers eingerichtet wurden.

Schritte

1. Geben Sie die IP-Adresse des Verwaltungsknotens ein, gefolgt von `/k8sdeployer/api/`:

   ```
   https://[IP address]/k8sdeployer/api/
   ```

2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus und geben Sie Cluster-Administrator-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 so ein, als `mnode-client` ob der Wert noch nicht ausgefüllt ist.
   d. Geben Sie keinen Wert für das Clientgeheimnis ein.
   e. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   f. Schließen Sie das Fenster.
3. Schließen Sie das Dialogfeld * Verfügbare Berechtigungen*.
4. Wählen Sie **POST/Destroy**.
5. Wählen Sie **Probieren Sie es aus**.
6. Geben Sie in das Textfeld Text anfordern den FQDN des Rancher-Servers als Wert ein `serverURL`.
7. Wählen Sie **Ausführen**.

   Nach einigen Minuten sollten die virtuellen Maschinen des Rancher-Servers nicht mehr in der Liste „Hosts and Clusters“ im vSphere-Client sichtbar sein. Nach der Entfernung können Sie mit NetApp Hybrid Cloud Control eine erneute Rangliste auf NetApp HCI einrichten.

Weitere Informationen

- "Fehlerbehebung bei der Rancher-Implementierung"
- "NetApp Element Plug-in für vCenter Server"
- "Seite „NetApp HCI Ressourcen“"

Hardware der H-Serie warten

Hardware-Wartung der H-Serie – Übersicht

Sie sollten Hardwarewartungsaufgaben wie den Austausch defekter Nodes, den Austausch defekter Laufwerke in den Storage-Nodes usw. durchführen, um sicherzustellen, dass das System optimal funktioniert.

Hier sind die Links zu den Hardwarewartungsaufgaben:

- "Ersetzen Sie das 2-HE-Gehäuse der H-Serie"
- "Austausch von Gleichstromnetzteilen in H615C und H610S Nodes"
- "DIMMs in Computing-Nodes ersetzen"
- "Austausch von Laufwerken für Storage-Nodes"
- "H410C Nodes ersetzen"
- "H410S Nodes ersetzen"
- "H610C und H615C Nodes ersetzen"
- "H610S Nodes ersetzen"
- "Ersetzen Sie die Netzteile"
- "Ersetzen Sie die Switches SN2010, SN2100 und SN2700"
- "Storage-Node wird in einem 2-Node-Cluster ersetzt"

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "NetApp Element Plug-in für vCenter Server"
- "*TR-4820: Quick Planning Guide für NetApp HCI-Netzwerke*"
- "NetApp Configuration Advisor" Netzwerkvalidierungstool 5.8.1 oder höher

Ersetzen Sie das 2-HE-Gehäuse der H-Serie

Wenn Ihr Gehäuse einen Lüfterausfall hat oder ein Stromausfall auftritt, sollten Sie ihn so schnell wie möglich austauschen. Die Schritte im Chassis-Austauschverfahren hängen von der NetApp HCI-Konfiguration und der Cluster-Kapazität ab. Hierfür sind sorgfältige Überlegungen und eine sorgfältige Planung erforderlich. Wenden Sie sich an den NetApp Support, um Anweisungen zu erhalten und ein Ersatzgehäuse zu bestellen.

Über diese Aufgabe

Vor dem Austauschen des Gehäuses sollten Sie Folgendes berücksichtigen:

- Verfügt Ihr Rack über zusätzlichen Platz für ein neues Chassis?
- Verfügt ein Chassis Ihrer Implementierung über ungenutzte Node-Steckplätze?
- Wenn Ihr Rack zusätzlichen Platz hat, können Sie jeden der Nodes nacheinander vom ausgefallenen

Chassis zum neuen Gehäuse verschieben? Beachten Sie, dass dieser Vorgang möglicherweise Zeit in Anspruch nehmen kann.

- Kann Ihr Storage-Cluster beim Entfernen der Nodes, die Teil des ausgefallenen Chassis sind, online bleiben?
- Können Virtual Machines (VMs) und ESXi Cluster den Workload verarbeiten, wenn Sie die Computing-Nodes entfernen, die Teil des ausgefallenen Chassis sind?

Ersatzoptionen

Wählen Sie eine der folgenden Optionen aus: wenn im Rack zusätzlicher ungenutzter Speicherplatz verfügbar ist wenn im Rack kein zusätzlicher ungenutzter Speicherplatz verfügbar ist

Ersetzen Sie das Chassis, wenn im Rack zusätzlicher ungenutzter Speicherplatz verfügbar ist

Wenn Ihr Rack über zusätzlichen Platz verfügt, können Sie das neue Chassis installieren und Nodes nacheinander zum neuen Chassis verschieben. Wenn eines der installierten Chassis nicht genutzte Node-Steckplätze aufweist, können Sie die Nodes nacheinander vom ausgefallenen Chassis in die nicht verwendeten Steckplätze verschieben und das ausgefallene Chassis entfernen. Stellen Sie vor der Durchführung des Verfahrens sicher, dass die Kabellängen ausreichend sind und Switch-Ports verfügbar sind.

Die Schritte zum Verschieben von Computing-Nodes unterscheiden sich von den Schritten zum Verschieben von Storage-Nodes. Sie sollten sicherstellen, dass die Nodes ordnungsgemäß heruntergefahren werden, bevor Sie sie verschieben. Nachdem Sie alle Nodes aus dem ausgefallenen Chassis verschoben haben, sollten Sie das Chassis aus dem Rack entfernen und es an NetApp zurückgeben.

Installieren Sie das neue Gehäuse

Sie können das neue Chassis in den verfügbaren Rack-Platz installieren und die Nodes in es verschieben.

Was Sie benötigen

- Sie haben ein elektrostatisches Entladungsband (ESD) oder einen anderen antistatischen Schutz.
- Sie haben das Ersatzgehäuse.
- Sie haben einen Aufzug oder zwei oder mehr Personen, um die Schritte durchzuführen.
- Sie haben einen #1 Kreuzschlitzschraubendreher.

Schritte

1. Setzen Sie den antistatischen Schutz auf.
2. Packen Sie das Ersatzgehäuse aus. Bewahren Sie die Verpackung auf, wenn Sie das fehlerhafte Chassis an NetApp zurücksenden.
3. Setzen Sie die Schienen ein, die Sie zusammen mit dem Gehäuse erhalten haben.
4. Schieben Sie das Ersatzgehäuse in das Rack.

   Beim Einbau des Chassis immer genügend Arbeitskraft oder einen Aufzug verwenden.

5. Befestigen Sie das Gehäuse mit den Flügelschrauben der vorderen Montage am Rack und ziehen Sie die Schrauben mit dem Schraubendreher fest.

Verschieben eines Computing-Node

Bevor Sie einen Computing-Node in das neue Gehäuse oder ein vorhandenes Gehäuse mit zusätzlichen nicht verwendeten Steckplätzen verschieben, sollten Sie die Virtual Machines (VMs) migrieren, den Node ordnungsgemäß herunterfahren und die im Node eingesetzten Kabel kennzeichnen.

Stellen Sie sicher, dass beim Verschieben des Knotens ein antistatischer Schutz vorhanden ist.

Schritte

1. Notieren Sie sich die Seriennummer des Node vom Aufkleber auf der Rückseite des Node.
2. Wählen Sie im VMware vSphere Web Client * Hosts und Cluster* aus, wählen Sie einen Knoten (Host) aus und wählen Sie dann **Monitor > Hardwarestatus > Sensoren** aus.
3. Suchen Sie im Abschnitt **Sensoren** die Seriennummer, die Sie auf dem Aufkleber auf der Rückseite des Knotens angegeben haben.
4. Nachdem Sie die passende Seriennummer gefunden haben, migrieren Sie die VMs zu einem anderen verfügbaren Host.

   Die Migrationsschritte finden Sie in der VMware Dokumentation.

5. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie **ein/aus > Herunterfahren** aus. Sie können den Node nun physisch aus dem Chassis entfernen.
6. Beschriften Sie den Knoten und alle Kabel auf der Rückseite des Node.
7. Entfernen Sie den Knoten aus dem Gehäuse, indem Sie den Nockengriff auf der rechten Seite jedes Knotens nach unten ziehen und den Knoten mit beiden Nockengriffen herausziehen.
8. Setzen Sie den Knoten wieder in das neue Gehäuse ein, indem Sie den Knoten in drücken, bis Sie einen Klick hören. Die Beschriftungen, die Sie dem Node angehängt hatten, bevor Sie ihn entfernt haben, helfen Ihnen. Der Node wird automatisch eingeschaltet, wenn Sie ihn ordnungsgemäß installieren.

   Stellen Sie sicher, dass Sie den Knoten von unter unterstützen, wenn Sie ihn installieren. Verwenden Sie keine übermäßige Kraft, während Sie den Node in das Chassis drücken.

   Wenn Sie den Node im neuen Chassis installieren, stellen Sie sicher, dass Sie ihn in seinem ursprünglichen Steckplatz im Chassis installieren.

9. Schließen Sie die Kabel wieder an die gleichen Ports an der Rückseite des Node an. Die Etiketten auf den Kabeln, die Sie beim Abstecken hatten, helfen Ihnen dabei.

   Stellen Sie sicher, dass Sie die Kabel nicht in die Anschlüsse zwingen. Kabel, Ports oder beides können beschädigt werden.

10. Vergewissern Sie sich, dass der Compute-Node (Host) im ESXi-Cluster im VMware vSphere Web Client aufgeführt ist.
11. Führen Sie diese Schritte für alle Computing-Nodes im ausgefallenen Chassis aus.

Verschieben eines Storage-Nodes

Bevor Sie die Storage-Nodes in das neue Chassis verschieben, sollten Sie die Laufwerke entfernen, die Nodes ordnungsgemäß herunterfahren und alle Komponenten kennzeichnen.

Schritte

1. Geben Sie den Node an, den Sie entfernen möchten:
   a. Notieren Sie sich die Seriennummer des Node vom Aufkleber auf der Rückseite des Node.
   b. Wählen Sie im VMware vSphere Web-Client die Option **NetApp Element-Verwaltung** aus, und kopieren Sie die MVIP-IP-Adresse.
   c. Verwenden Sie die MVIP-IP-Adresse in einem Webbrowser, um sich bei der NetApp Element Software-UI mit dem Benutzernamen und Passwort anzumelden, die Sie in der NetApp Deployment Engine konfiguriert haben.
   d. Wählen Sie **Cluster > Knoten**.
   e. Ordnen Sie die Seriennummer, die Sie aufgeführt haben, mit der angegebenen Seriennummer (Service-Tag-Nummer) zusammen.
   f. Notieren Sie sich die Node-ID des Node.
2. Nachdem Sie den Knoten identifiziert haben, verschieben Sie iSCSI-Sitzungen mithilfe des folgenden API-Aufrufs vom Knoten weg:
   `wget --no-check-certificate -q --user=<USER> --password=<PASS> -O - --post -data '{ "method":"MovePrimariesAwayFromNode", "params":{"nodeID":<NODEID>} }' https://<MVIP>/json-rpc/8.0` MVIP ist die MVIP-IP-Adresse, NODEID ist die Node-ID, BENUTZER ist der Benutzername, den Sie beim Einrichten von NetApp HCI in der NetApp-Bereitstellungsmodul konfiguriert haben, und PASS ist das Kennwort, das Sie beim Einrichten von NetApp HCI in der NetApp-Bereitstellungsmodul konfiguriert haben.
3. Wählen Sie **Cluster > Laufwerke** aus, um die dem Knoten zugeordneten Laufwerke zu entfernen.

   Sie sollten auf die Laufwerke warten, die Sie entfernt haben, um sie als verfügbar anzuzeigen, bevor Sie den Node entfernen.

4. Wählen Sie **Cluster > Knoten > Aktionen > Entfernen**, um den Knoten zu entfernen.
5. Verwenden Sie den folgenden API-Aufruf, um den Knoten herunterzufahren:
   `wget --no-check-certificate -q --user=<USER> --password=<PASS> -O - --post -data '{ "method":"Shutdown", "params":{"option":"halt", "nodes":[ <NODEID>]} }' https://<MVIP>/json-rpc/8.0` MVIP ist die MVIP-IP-Adresse, NODEID ist die Knoten-ID, BENUTZER ist der Benutzername, den Sie beim Einrichten von NetApp HCI in der NetApp-Bereitstellungsmodul konfiguriert haben, und PASS ist das Kennwort, das Sie beim Einrichten von NetApp HCI in der NetApp-Bereitstellungsmodul konfiguriert haben. Nachdem der Node heruntergefahren wurde, können Sie ihn physisch aus dem Chassis entfernen.
6. Entfernen Sie die Laufwerke wie folgt vom Node im Chassis:
   a. Entfernen Sie die Blende.
   b. Beschriften Sie die Laufwerke.
   c. Öffnen Sie den Nockengriff, und schieben Sie jedes Laufwerk vorsichtig mit beiden Händen heraus.
   d. Platzieren Sie die Antriebe auf einer antistatischen, Ebenen Fläche.
7. Entfernen Sie den Node wie folgt aus dem Chassis:
   a. Beschriften Sie den Node und die Kabel, die daran angeschlossen sind.
   b. Ziehen Sie den Nockengriff auf der rechten Seite jedes Knotens nach unten und ziehen Sie den Knoten mit beiden Nockengriffen heraus.
8. Setzen Sie den Knoten wieder in das Gehäuse ein, indem Sie den Knoten in drücken, bis Sie einen Klick hören. Die Beschriftungen, die Sie dem Node angehängt hatten, bevor Sie ihn entfernt haben, helfen

Ihnen.

Stellen Sie sicher, dass Sie den Knoten von unter unterstützen, wenn Sie ihn installieren. Verwenden Sie keine übermäßige Kraft, während Sie den Node in das Chassis drücken.

Wenn Sie den Node im neuen Chassis installieren, stellen Sie sicher, dass Sie ihn in seinem ursprünglichen Steckplatz im Chassis installieren.

9. Setzen Sie die Laufwerke in die entsprechenden Schlitze im Knoten ein, indem Sie den Nockengriff auf jedem Laufwerk nach unten drücken, bis er einrastet.
10. Schließen Sie die Kabel wieder an die gleichen Ports an der Rückseite des Node an. Die Etiketten, die Sie beim Trennen an den Kabeln befestigt haben, helfen Ihnen dabei.

Stellen Sie sicher, dass Sie die Kabel nicht in die Anschlüsse zwingen. Kabel, Ports oder beides können beschädigt werden.

11. Nachdem der Node eingeschaltet ist, fügen Sie den Node zum Cluster hinzu.

Es kann bis zu 15 Minuten dauern, bis der Knoten hinzugefügt wurde und unter **Knoten > aktiv** angezeigt wird.

12. Fügen Sie die Laufwerke hinzu.
13. Führen Sie diese Schritte für alle Storage-Nodes im Chassis aus.

Ersetzen Sie das Chassis, wenn im Rack kein zusätzlicher ungenutzter Speicherplatz verfügbar ist

Wenn Ihr Rack keinen zusätzlichen Platz bietet und kein Chassis in der Implementierung über keine ungenutzten Node-Steckplätze verfügt, sollten Sie herausfinden, was ggf. online bleiben kann, bevor Sie das Austauschverfahren durchführen.

Über diese Aufgabe

Vor dem Austausch des Gehäuses sollten Sie die folgenden Punkte berücksichtigen:

- Kann Ihr Storage-Cluster ohne die Storage-Nodes im ausgefallenen Chassis online bleiben? Wenn die Antwort Nein lautet, sollten Sie alle Nodes (sowohl Computing als auch Storage) in Ihrer NetApp HCI Implementierung herunterfahren. Wenn die Antwort Ja ist, können Sie nur die Storage-Nodes im ausgefallenen Chassis herunterfahren.
- Können Ihre VMs und ESXi Cluster ohne die Computing-Nodes im ausgefallenen Chassis online bleiben? Wenn die Antwort Nein lautet, müssen Sie die entsprechenden VMs herunterfahren oder migrieren, um die Computing-Nodes im ausgefallenen Chassis herunterfahren zu können. Wenn die Antwort Ja ist, können Sie nur die Computing-Nodes im ausgefallenen Chassis herunterfahren.

Fahren Sie einen Computing-Node herunter

Bevor Sie den Computing-Node zum neuen Chassis verschieben, sollten Sie die VMs migrieren, ihn korrekt herunterfahren und die Kabel, die im Node eingesetzt wurden, kennzeichnen.

Schritte

1. Notieren Sie sich die Seriennummer des Node vom Aufkleber auf der Rückseite des Node.

2. Wählen Sie im VMware vSphere Web Client * Hosts und Cluster* aus, wählen Sie einen Knoten (Host) aus und wählen Sie dann **Monitor > Hardwarestatus > Sensoren** aus.
3. Suchen Sie im Abschnitt **Sensoren** die Seriennummer, die Sie auf dem Aufkleber auf der Rückseite des Knotens angegeben haben.
4. Nachdem Sie die passende Seriennummer gefunden haben, migrieren Sie die VMs zu einem anderen verfügbaren Host.

   Die Migrationsschritte finden Sie in der VMware Dokumentation.

5. Klicken Sie mit der rechten Maustaste auf den Knoten, und wählen Sie **ein/aus > Herunterfahren** aus. Sie können den Node nun physisch aus dem Chassis entfernen.

Fahren Sie einen Storage-Node herunter

Siehe die Schritte Hier.

Entfernen des Node

Sie sollten sicherstellen, dass Sie den Knoten vorsichtig aus dem Gehäuse entfernen und alle Komponenten kennzeichnen. Die zum physischen Entfernen des Node erforderlichen Schritte sind sowohl für die Storage- als auch für die Computing-Nodes identisch. Entfernen Sie für einen Storage-Node das Laufwerk, bevor Sie den Node entfernen.

Schritte

1. Entfernen Sie bei einem Storage-Node die Laufwerke wie folgt vom Node im Chassis:
   a. Entfernen Sie die Blende.
   b. Beschriften Sie die Laufwerke.
   c. Öffnen Sie den Nockengriff, und schieben Sie jedes Laufwerk vorsichtig mit beiden Händen heraus.
   d. Platzieren Sie die Antriebe auf einer antistatischen, Ebenen Fläche.
2. Entfernen Sie den Node wie folgt aus dem Chassis:
   a. Beschriften Sie den Node und die Kabel, die daran angeschlossen sind.
   b. Ziehen Sie den Nockengriff auf der rechten Seite jedes Knotens nach unten und ziehen Sie den Knoten mit beiden Nockengriffen heraus.
3. Führen Sie diese Schritte für alle Knoten aus, die Sie entfernen möchten. Sie sind jetzt bereit, das ausgefallene Gehäuse zu entfernen.

Ersetzen Sie das Gehäuse

Wenn kein zusätzlicher Speicherplatz im Rack vorhanden ist, sollten Sie das ausgefallene Chassis deinstallieren und durch das neue Gehäuse ersetzen.

Schritte

1. Setzen Sie den antistatischen Schutz auf.
2. Packen Sie das Ersatzgehäuse aus, und halten Sie es auf einer Ebenen Fläche. Die Verpackung bleibt erhalten, wenn Sie die fehlerhafte Einheit an NetApp zurücksenden.
3. Entfernen Sie das fehlerhafte Chassis aus dem Rack und legen Sie es auf eine Ebene Fläche.

Verwenden Sie beim Bewegen eines Chassis ausreichend Personal oder einen Aufzug.

4. Entfernen Sie die Schienen.
5. Installieren Sie die neuen Schienen, die Ihnen zusammen mit dem Ersatzgehäuse geliefert wurden.
6. Schieben Sie das Ersatzgehäuse in das Rack.
7. Befestigen Sie das Gehäuse mit den Flügelschrauben der vorderen Montage am Rack und ziehen Sie die Schrauben mit dem Schraubendreher fest.
8. Installieren Sie die Nodes wie folgt in das neue Chassis:
   a. Setzen Sie den Knoten wieder in seinen ursprünglichen Steckplatz im Chassis ein, indem Sie den Knoten in drücken, bis Sie einen Klick hören. Die Beschriftungen, die Sie dem Node angehängt haben, bevor Sie ihn entfernt haben, helfen Ihnen.

      Stellen Sie sicher, dass Sie den Knoten von unter unterstützen, wenn Sie ihn installieren. Verwenden Sie keine übermäßige Kraft, während Sie den Node in das Chassis drücken.

   b. Bei Speicherknoten installieren Sie die Laufwerke in den entsprechenden Steckplätzen im Knoten, indem Sie den Nockengriff auf jedem Laufwerk nach unten drücken, bis er hörbar einrastet.
   c. Schließen Sie die Kabel wieder an die gleichen Ports an der Rückseite des Node an. Die Etiketten, die Sie beim Trennen an den Kabeln befestigt haben, führen Sie zu diesem Zeitpunkt.

      Stellen Sie sicher, dass Sie die Kabel nicht in die Anschlüsse zwingen. Kabel, Ports oder beides können beschädigt werden.

9. Stellen Sie sicher, dass die Nodes wie folgt online sind:

Option	Schritte
Wenn Sie alle Nodes (Storage und Computing) in Ihrer NetApp HCI-Implementierung neu installieren	a. Vergewissern Sie sich im VMware vSphere Web Client, dass die Computing-Nodes (Hosts) im ESXi-Cluster aufgeführt sind. b. Vergewissern Sie sich im Element Plug-in für vCenter Server, dass die Storage Nodes als aktiv aufgeführt sind.

Option	Schritte
Wenn Sie nur die Nodes im ausgefallenen Chassis neu installiert haben	a. Vergewissern Sie sich im VMware vSphere Web Client, dass die Computing-Nodes (Hosts) im ESXi-Cluster aufgeführt sind. b. Wählen Sie im Element Plug-in für vCenter Server die Option **Cluster > Knoten > Ausstehend** aus. c. Wählen Sie den Knoten aus, und wählen Sie **Hinzufügen**. Es kann bis zu 15 Minuten dauern, bis der Knoten hinzugefügt wurde und unter **Knoten > aktiv** angezeigt wird. d. Wählen Sie **Laufwerke**. e. Fügen Sie in der Liste verfügbar die Laufwerke hinzu. f. Führen Sie diese Schritte für alle Storage-Nodes durch, die Sie neu installiert haben.

10. Vergewissern Sie sich, dass die Volumes und Datastores verfügbar sind.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Austausch von Gleichstromnetzteilen in H615C und H610S Nodes

H615C und H610S Nodes unterstützen zwei–48 V bis –60 V DC-Netzteile. Diese Einheiten sind bei der Bestellung von H615C oder H610S Nodes als optionale Add-ons erhältlich. Sie können diese Anleitung verwenden, um die Netzteileinheiten im Gehäuse zu entfernen und durch Gleichstromnetzteile zu ersetzen oder ein defektes Gleichstromnetzteil durch ein neues Gleichstromnetzteil zu ersetzen.

Was Sie benötigen

- Wenn Sie ein defektes DC-Netzteil ersetzen, haben Sie ein Ersatznetzteil in Anspruch genommen.
- Wenn Sie die Wechselstromnetzteile in Ihrem Gehäuse gegen Gleichstromeinheiten austauschen, haben Sie die Ausfallzeiten für das Verfahren berücksichtigt.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder andere antistatische Vorsichtsmaßnahmen getroffen.
- Sie haben sichergestellt, dass die Anforderungen an die Stromversorgung erfüllt sind:
  - Versorgungsspannung: – (48-60) V DC

- Stromaufnahme: 37A (Maximum)
- Leistungsschalter Anforderungen: 40A Trennschalter

- Sie haben dafür gesorgt, dass die Materialien in Ihrer Umgebung den RoHS-Spezifikationen entsprechen.
- Sie haben sichergestellt, dass die Kabelanforderungen erfüllt sind:
  - Ein UL 10 AWG, maximal 2 m (gestrandet) schwarzes Kabel [– (48-60) V DC]
  - Ein UL 10 AWG, maximal 2 m (gestrandet) rotes Kabel [V DC-Rückleitung]
  - Ein UL 10 AWG, maximal 2 m grünes/gelbes Kabel, grün mit gelbem Streifen, Litzen (Sicherheitsmasse)

Über diese Aufgabe

Das Verfahren gilt für die folgenden Node-Modelle:

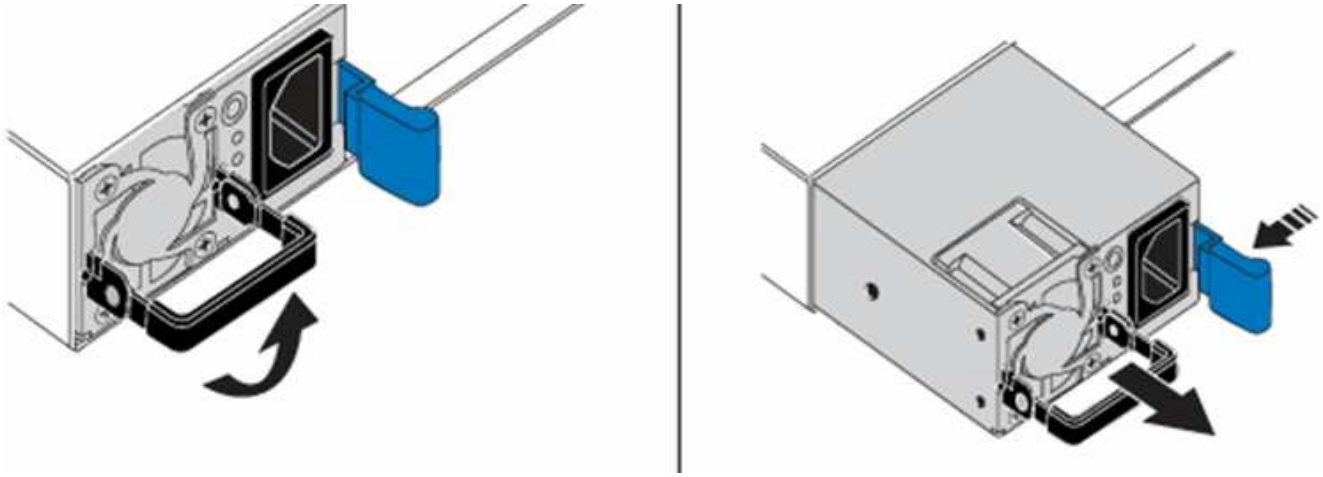
- 1-HE-H615C Computing-Chassis
- 1-HE-H610S Storage-Chassis

Bei H615C und H610S werden die Begriffe „Node“ und „Chassis“ austauschbar verwendet, da Node und Chassis keine separaten Komponenten sind, anders als bei einem 2-HE-Chassis mit vier Nodes.

Sie können in Ihrer Installation keine Wechselstromnetzteile und Gleichstromnetzteile mischen.

Schritte

1. Schalten Sie die Netzteile aus und ziehen Sie die Netzkabel ab. Wenn Sie ein defektes DC-Netzteil ersetzen, schalten Sie die Stromquelle aus und entfernen Sie alle Kabel, die in den blauen Stecker gesteckt sind.
2. Heben Sie den Nockengriff an, und drücken Sie die blaue Verriegelung, um das Netzteil herauszuschieben.



Die Abbildung ist ein Beispiel. Die Position des Netzteils im Gehäuse und die Farbe der Entriegelungstaste variieren je nach Gehäusetyp.

Stellen Sie sicher, dass Sie beide Hände verwenden, um das Gewicht des Netzteils zu unterstützen.

3. Richten Sie die Kanten des Netzteils mit beiden Händen an der Öffnung im Gehäuse aus. Schieben Sie das Gerät vorsichtig mit dem Nockengriff in das Gehäuse, bis es einrastet, und bringen Sie den Nockengriff in die aufrechte Position zurück.

4. Verkabeln Sie die Gleichstromnetzteile. Stellen Sie sicher, dass die Stromquelle ausgeschaltet ist, während Sie das Gleichstromnetzteil und die Stromquelle verkabeln.
   a. Stecken Sie die schwarzen, roten und grünen/gelben Kabel in die blauen Anschlüsse.
   b. Stecken Sie den blauen Stecker in die Gleichstromnetzteile und die Stromquelle.

5. Schalten Sie die Gleichstromnetzteile ein.

Die Netzteil-LEDs leuchten, wenn das Gleichstromnetzteil online geschaltet wird. Grüne LED-Anzeigen zeigen an, dass die Netzteile ordnungsgemäß funktionieren.

6. Senden Sie das fehlerhafte Gerät an NetApp zurück. Befolgen Sie die Anweisungen im Lieferumfang, die Sie erhalten haben.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

DIMMs in Computing-Nodes ersetzen

Sie können ein fehlerhaftes Dual Inline Memory Module (DIMM) in NetApp HCI-Computing-Nodes ersetzen, anstatt den gesamten Node zu ersetzen.

Was Sie benötigen

- Bevor Sie mit diesem Verfahren beginnen, sollten Sie den NetApp Support kontaktieren und ein Ersatzteil erhalten haben. Bei der Installation des Ersatzes ist der Support beteiligt. Wenn Sie dies noch nicht getan haben, wenden Sie sich an "Support".
- Geplante Systemausfallzeiten sind geplant, da der Node heruntergefahren oder aus- und wieder eingeschaltet und der Node im NetApp Safe Mode gebootet werden muss, um auf die Terminal User

Interface (TUI) zuzugreifen.

Über diese Aufgabe

Dieses Verfahren gilt für die folgenden Computing-Node-Modelle:

- H410C Nodes Ein H410C Node wird in ein 2-HE-NetApp HCI-Chassis eingesetzt.
- H610C Node: Ein H610C Node ist in das Chassis integriert.
- H615C Node: Ein H615C Node ist in das Chassis integriert.

> H410C und H615C Nodes enthalten DIMMs verschiedener Anbieter. Stellen Sie sicher, dass Sie DIMMs verschiedener Anbieter in einem Gehäuse nicht mischen.

> Die Begriffe „Chassis“ und „Node“ werden im Fall von H610C und H615C gemeinsam verwendet, da der Node und das Chassis keine separaten Komponenten sind.

Nachfolgend sind die Schritte aufgeführt, die beim Austausch von DIMMs bei Computing-Nodes erforderlich sind:

- Bereiten Sie den Austausch des DIMM vor
- Ersetzen Sie das DIMM aus dem Gehäuse

Bereiten Sie den Austausch des DIMM vor

Wenn Probleme mit dem DIMM auftreten, zeigt VMware ESXi Warnungen an, wie `Memory Configuration Error`, , `Memory Uncorrectable ECC` `Memory Transition to Critical` und `Memory Critical Overtemperature`. Selbst wenn die Meldungen nach einer Weile verschwinden, könnte das Hardware-Problem weiterhin bestehen. Sie sollten das fehlerhafte DIMM diagnostizieren und beheben. Informationen zum fehlerhaften DIMM erhalten Sie vom vCenter Server. Wenn Sie mehr Informationen benötigen, als über den vCenter Server verfügbar ist, müssen Sie den Hardwarecheck im TUI ausführen.

Schritte

1. Greifen Sie auf den Knoten zu, indem Sie sich bei vCenter Server anmelden.
2. Klicken Sie mit der rechten Maustaste auf den Node, der den Fehler meldet, und wählen Sie die Option aus, um den Node in den Wartungsmodus zu versetzen.
3. Migrieren Sie die Virtual Machines (VMs) zu einem anderen verfügbaren Host.

   > Die Migrationsschritte finden Sie in der VMware Dokumentation.

4. Schalten Sie den Computing-Node aus.

   > Wenn Sie über die Informationen verfügen, welche DIMM-Module ausgetauscht werden müssen und nicht auf die TUI zugreifen müssen, können Sie die folgenden Schritte in diesem Abschnitt überspringen.

5. Schließen Sie eine Tastatur, ein Video und eine Maus (KVM) an die Rückseite des Knotens an, der den Fehler gemeldet hat.
6. Drücken Sie den Netzschalter an der Vorderseite des Knotens. Das Booten des Node dauert etwa sechs Minuten. Auf dem Bildschirm wird ein Startmenü angezeigt.

7. Identifizieren Sie den Steckplatz, der den Fehler protokolliert hat wie folgt:
   a. Für H615C gehen Sie wie folgt vor:
      i. Melden Sie sich bei der Benutzeroberfläche von BMC an.
      ii. Wählen Sie **Protokolle & Berichte** > **IPMI-Ereignisprotokoll** aus.
      iii. Suchen Sie im Ereignisprotokoll den Speicherfehler und identifizieren Sie den Steckplatz, in dem der Fehler protokolliert wird.

8. Führen Sie bei H410C- und H615C-Knoten die Schritte aus, um die Teilenummer des DIMM-Herstellers zu ermitteln.

> H410C und H615C Nodes sind DIMMs verschiedener Hersteller enthalten. Es sollten keine verschiedenen DIMM-Typen im selben Gehäuse kombiniert werden. Sie sollten den Hersteller des fehlerhaften DIMM identifizieren und einen Austausch desselben Typs bestellen.

   a. Melden Sie sich beim BMC an, um die Konsole auf dem Node zu starten.
   b. Drücken Sie auf der Tastatur * F2*, um zum Menü **System/Protokolle anpassen** zu gelangen.
   c. Geben Sie bei der entsprechenden Aufforderung das Passwort ein.

> Das Passwort sollte mit den Parametern übereinstimmen, die Sie bei der Einrichtung von NetApp HCI in der NetApp Deployment Engine konfiguriert haben.

   a. Drücken Sie im Menü Systemanpassung den Abwärtspfeil, um zu Fehlerbehebungsoptionen zu navigieren, und drücken Sie **Enter**.

b. Verwenden Sie im Menü Optionen für den Fehlerbehebungsmodus den Pfeil nach oben oder unten, um ESXi Shell und SSH zu aktivieren, die standardmäßig deaktiviert sind.

c. Drücken Sie zweimal die Taste <Esc>, um die Fehlerbehebungsoptionen zu beenden.

d. Führen Sie den Befehl mit einer der folgenden Optionen aus `smbiosDump`:

Option	Schritte

Option A	i. Stellen Sie eine Verbindung zum ESXi-Host (Compute-Node) her, indem Sie die IP-Adresse des Hosts und die von Ihnen definierten Root-Anmeldedaten verwenden.
	ii. Führen Sie den `smbiosDump` Befehl aus. Die folgende Beispielausgabe finden Sie unter:
	`Memory Device:#30`
	`Location: "P1-DIMMA1"`
	`Bank: "P0_Node0_Channel0_Dimm0"`
	`Manufacturer:"Samsung"`
	`Serial: "38EB8380"`
	`Asset Tag: "P1-DIMMA1_AssetTag (date:18/15)"`
	`Part Number: "M393A4K40CB2-CTD"`
	`Memory Array: #29`
	`Form Factor: 0x09(DIMM)`
	`Type: 0x1a (DDR4)`
	`Type Detail: 0x0080 (Synchronous)`
	`Data Width: 64 bits (+8 ECC bits)`
	`Size: 32 GB`

Option B	i. Drücken Sie **Alt + F1**, um Shell einzugeben, und melden Sie sich beim Knoten an, um den Befehl auszuführen.

9. Wenden Sie sich an den NetApp Support, um Unterstützung bei den nächsten Schritten zu erhalten. Der NetApp Support benötigt folgende Informationen, um einen Teileaustausch zu bearbeiten:
   - Seriennummer der Nodes
   - Cluster-Name
   - Systemereignisprotokoll von der BMC-Benutzeroberfläche (**Protokolle und Berichte** > **IPMI-Ereignisprotokoll**> **Ereignisprotokolle herunterladen**)
   - Die Ausgabe erfolgt über den `smbiosDump` Befehl

Ersetzen Sie das DIMM aus dem Gehäuse

Bevor Sie das fehlerhafte DIMM-Modul im Gehäuse entfernen und austauschen, stellen Sie sicher, dass Sie alle ausgeführt haben"Vorbereitungsschritte".

DIMMs sollten in den gleichen Steckplätzen, aus denen sie entfernt wurden, ersetzt werden.

Schritte

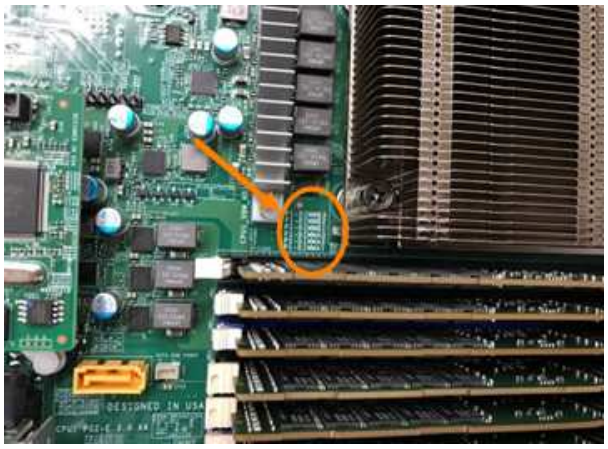
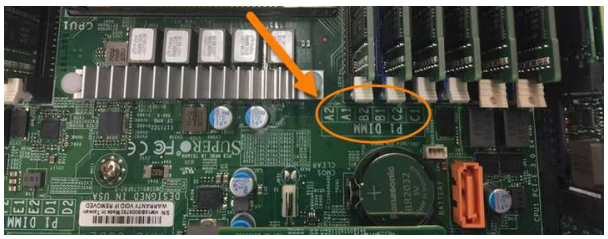
1. Fahren Sie das Chassis oder den Node herunter.

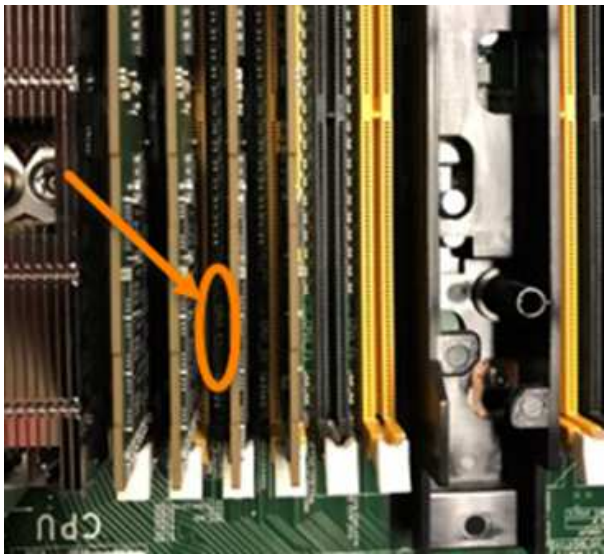
   Für ein H610C oder H615C Chassis schalten Sie das Chassis herunter. Für H410C Nodes in einem 2-HE-Chassis mit vier Nodes schalten Sie nur den Node mit dem fehlerhaften DIMM aus.

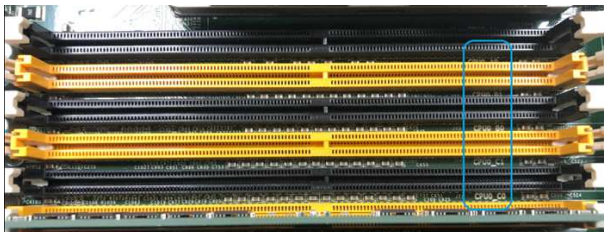
2. Entfernen Sie die Stromkabel und Netzwerkkabel, schieben Sie den Node bzw. das Chassis vorsichtig aus dem Rack und legen Sie ihn auf eine flache, antistatische Oberfläche.

   Ziehen Sie die Verwendung von Twistbinen für Kabel in Betracht.

3. Setzen Sie den antistatischen Schutz auf, bevor Sie die Gehäuseabdeckung öffnen, um das DIMM auszutauschen.
4. Führen Sie die für Ihr Node-Modell relevanten Schritte aus:

Node-Modell	Schritte
H410C	a. Suchen Sie das ausgefallene DIMM, indem Sie die zuvor angegebene Steckplatznummer/ID mit der Nummerierung auf der Hauptplatine vergleichen. Hier sind Beispielbilder, die die DIMM-Steckplatznummern auf der Hauptplatine anzeigen:   b. Drücken Sie die beiden Halteclips nach außen, und ziehen Sie das DIMM vorsichtig nach oben. Hier sehen Sie ein Beispielbild mit den Halteklammern:  c. Installieren Sie das ErsatzDIMM richtig. Wenn Sie das DIMM richtig in den Steckplatz einsetzen, verriegeln die beiden Clips. Stellen Sie sicher, dass Sie nur die hinteren Enden des DIMM berühren. Wenn Sie auf andere Teile des DIMM drücken, kann dies zu einer Beschädigung der Hardware führen.

Node-Modell	Schritte
H610C	a. Heben Sie die Abdeckung wie in der folgenden Abbildung dargestellt an: b. Lösen Sie die vier blauen Sicherungsschrauben an der Rückseite des Knotens. Hier sehen Sie ein Beispielbild, das die Position von zwei Sicherungsschrauben zeigt. Die anderen beiden Schrauben befinden sich auf der anderen Seite des Knotens:  c. Entfernen Sie beide PCI-Kartensteckplatzhalter. d. Entfernen Sie die GPU und die Luftstromabdeckung. e. Suchen Sie das ausgefallene DIMM, indem Sie die zuvor angegebene Steckplatznummer/ID mit der Nummerierung auf der Hauptplatine vergleichen. Hier ist ein Beispielbild, das die Position der DIMM-Steckplatznummern auf der Hauptplatine anzeigt:  f. Drücken Sie die beiden Halteclips nach außen, und ziehen Sie das DIMM vorsichtig nach oben. g. Installieren Sie das ErsatzDIMM richtig. Wenn Sie das DIMM richtig in den Steckplatz einsetzen, verriegeln die beiden Clips.

Node-Modell	Schritte
H615C	a. Heben Sie die Abdeckung wie in der folgenden Abbildung dargestellt an: b. Entfernen Sie die GPU (wenn auf Ihrem H615C Node GPU installiert ist) und die Luftstromabdeckung. c. Suchen Sie das ausgefallene DIMM, indem Sie die zuvor angegebene Steckplatznummer/ID mit der Nummerierung auf der Hauptplatine vergleichen. Hier ist ein Beispielbild, das die Position der DIMM-Steckplatznummern auf der Hauptplatine anzeigt:  d. Drücken Sie die beiden Halteclips nach außen, und ziehen Sie das DIMM vorsichtig nach oben. e. Installieren Sie das ErsatzDIMM richtig. Wenn Sie das DIMM richtig in den Steckplatz einsetzen, verriegeln die beiden Clips. Stellen Sie sicher, dass Sie nur die hinteren Enden des DIMM berühren. Wenn Sie auf andere Teile des DIMM drücken, kann dies zu einer Beschädigung der Hardware führen. f. Setzen Sie die Luftstromabdeckung wieder ein. g. Setzen Sie die Abdeckung wieder auf den Knoten. h. Installieren Sie das H610C Chassis im Rack und stellen Sie sicher, dass das Chassis beim Einschieben einrastet.

5. Schließen Sie die Stromkabel und Netzwerkkabel an. Stellen Sie sicher, dass alle Port-LEDs eingeschaltet sind.
6. Drücken Sie den Netzschalter an der Vorderseite des Knotens, wenn er nicht automatisch eingeschaltet wird, wenn Sie ihn installieren.
7. Nachdem der Node in vSphere angezeigt wird, klicken Sie mit der rechten Maustaste auf den Namen und nehmen Sie den Node aus dem Wartungsmodus.

8. Überprüfen Sie die Hardwareinformationen wie folgt:
   a. Melden Sie sich bei der Baseboard Management Controller (BMC) UI an.
   b. Wählen Sie **System > Hardware-Informationen**, und überprüfen Sie die aufgeführten DIMMs.

Wie es weiter geht

Nachdem der Knoten wieder in den normalen Betrieb zurückkehrt, überprüfen Sie in vCenter die Registerkarte Zusammenfassung, um sicherzustellen, dass die Speicherkapazität wie erwartet ist.

Wenn das DIMM nicht ordnungsgemäß installiert ist, funktioniert der Node ordnungsgemäß, ist aber mit einer geringeren als erwarteten Speicherkapazität ausgestattet.

Nach dem DIMM-Ersatzverfahren können Sie die Warnungen und Fehler auf der Registerkarte Hardwarestatus in vCenter löschen. Sie können dies tun, wenn Sie den Fehlerverlauf der Hardware, die Sie ausgetauscht haben, löschen möchten. "Weitere Informationen .".

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Austausch von Laufwerken für Storage-Nodes

Wenn ein Laufwerk defekt ist oder der Verschleiß des Laufwerks unter einen Schwellenwert fällt, sollten Sie dieses austauschen. Alarme in der Element Software UI und VMware vSphere Web Client benachrichtigen Sie, wenn ein Laufwerk ausgefallen ist oder ausfällt. Sie können ein ausgefallenes Laufwerk im laufenden Betrieb austauschen.

Über diese Aufgabe

Dieses Verfahren dient zum Austausch von Laufwerken in H410S und H610S Storage-Nodes. Durch das Entfernen eines Laufwerks kann das Laufwerk offline geschaltet werden. Alle Daten auf dem Laufwerk werden entfernt und auf andere Laufwerke im Cluster migriert. Die Datenmigration auf andere aktive Laufwerke im System kann abhängig von Kapazitätsauslastung und aktiver I/O im Cluster einige Minuten bis eine Stunde dauern.

Best Practices zur Handhabung von Laufwerken

Für den Umgang mit Laufwerken sollten Sie folgende Best Practices beachten:

- Halten Sie das Laufwerk in der ESD-Tasche, bis Sie bereit sind, es zu installieren.
- Öffnen Sie die ESD-Tasche von Hand oder schneiden Sie die Oberseite mit einer Schere ab.
- Tragen Sie stets ein ESD-Handgelenkband, das an einer unbemalten Oberfläche auf Ihrem Chassis geerdet ist.
- Beim Entfernen, Installieren oder Tragen eines Laufwerks immer beide Hände verwenden.
- Niemals ein Laufwerk in das Chassis zwingen.
- Verwenden Sie beim Transport von Laufwerken stets die genehmigte Verpackung.
- Legen Sie keine Laufwerke aufeinander ab.

Best Practices zum Hinzufügen und Entfernen von Laufwerken

Beachten Sie folgende Best Practices, um Laufwerke zum Cluster hinzuzufügen und Laufwerke aus dem Cluster zu entfernen:

- Fügen Sie alle Blocklaufwerke hinzu, und stellen Sie sicher, dass die Blocksynchronisierung abgeschlossen ist, bevor Sie die Slice-Laufwerke hinzufügen.
- Fügen Sie für Element Software ab 10.x alle Blocklaufwerke gleichzeitig ein. Stellen Sie sicher, dass Sie dies nicht für mehr als drei Knoten gleichzeitig tun.
- Fügen Sie bei der Element Software 9.x und früher drei Laufwerke gleichzeitig hinzu, um sie vollständig zu synchronisieren, bevor Sie die nächste Gruppe von drei hinzufügen.
- Entfernen Sie das Slice-Laufwerk, und stellen Sie sicher, dass die Schichtsynchronisierung abgeschlossen ist, bevor Sie die Blocklaufwerke entfernen.
- Entfernen Sie alle Blocklaufwerke gleichzeitig aus einem einzelnen Node. Vergewissern Sie sich, dass die Blocksynchronisierung abgeschlossen ist, bevor Sie zum nächsten Node fahren.

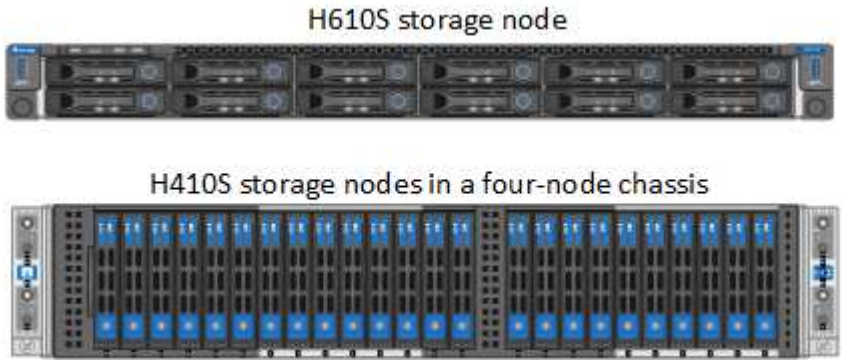
Schritte

1. Entfernen Sie das Laufwerk aus dem Cluster, indem Sie entweder die NetApp Element Software UI oder den NetApp Element Management Extension Point in Element Plug-in für vCenter Server verwenden.

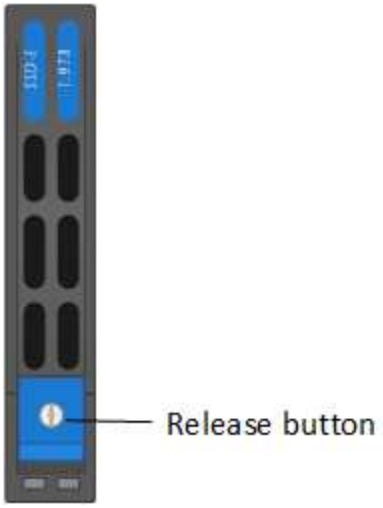
Option	Schritte
Verwenden der Element-UI	a. Wählen Sie in der Element UI die Option **Cluster > Laufwerke** aus. b. Wählen Sie **fehlgeschlagen** aus, um die Liste der ausgefallenen Laufwerke anzuzeigen. c. Notieren Sie sich die Steckplatznummer des ausgefallenen Laufwerks. Sie benötigen diese Informationen, um das ausgefallene Laufwerk im Chassis zu finden. d. Wählen Sie **Aktionen** für das Laufwerk, das Sie entfernen möchten. e. Wählen Sie **Entfernen**. Sie können das Laufwerk nun physisch aus dem Gehäuse entfernen.

Option	Schritte
Verwenden des Element Plug-ins für die vCenter Server-UI	a. Wählen Sie im Erweiterungspunkt NetApp Element Management des vSphere Web Clients die Option **NetApp Element-Verwaltung > Cluster** aus. b. Wenn zwei oder mehr Cluster hinzugefügt werden, stellen Sie sicher, dass der Cluster, den Sie für die Aufgabe verwenden möchten, in der Navigationsleiste ausgewählt ist. c. Wählen Sie in der Dropdown-Liste * All* aus, um die komplette Liste der Laufwerke anzuzeigen. d. Aktivieren Sie das Kontrollkästchen für jedes Laufwerk, das Sie entfernen möchten. e. Wählen Sie **Laufwerke Entfernen**. f. Bestätigen Sie die Aktion. Falls nicht genügend Kapazität zum Entfernen aktiver Laufwerke vor dem Entfernen eines Node vorhanden ist, wird beim Bestätigen des Entfernens des Laufwerks eine Fehlermeldung angezeigt. Nachdem Sie den Fehler behoben haben, können Sie das Laufwerk nun physisch aus dem Gehäuse entfernen.

2. Setzen Sie das Laufwerk aus dem Gehäuse wieder ein:
   a. Packen Sie das Ersatzlaufwerk aus und legen Sie es auf eine flache, statische Oberfläche in der Nähe des Racks. Speichern Sie das Verpackungsmaterial für, wenn Sie das ausgefallene Laufwerk an NetApp zurücksenden. Hier ist die Vorderansicht der H610S und H410S Storage-Nodes mit den Laufwerken:



   b. Führen Sie die Schritte auf Grundlage des Node-Modells durch:

Node-Modell	Schritte
H410S	i. Identifizieren Sie den Knoten, indem Sie die Seriennummer (Service-Tag) mit der Nummer, die Sie in der Element-UI angegeben haben, übereinstimmen. Die Seriennummer befindet sich auf einem Aufkleber auf der Rückseite jedes Node. Nachdem Sie den Node identifiziert haben, können Sie mithilfe der Steckplatzinformationen den Steckplatz identifizieren, in dem sich das ausgefallene Laufwerk befindet. Die Laufwerke sind alphabetisch von A bis D und von 0 bis 5 angeordnet. ii. Entfernen Sie die Blende. iii. Drücken Sie die Entriegelungstaste am ausgefallenen Laufwerk:  Wenn Sie die Entriegelungstaste drücken, öffnen sich der Nockengriff an den Antriebsfedern teilweise und der Antrieb löst sich von der Mittelplatine aus. iv. Öffnen Sie den Nockengriff, und schieben Sie das Laufwerk vorsichtig mit beiden Händen heraus. v. Platzieren Sie das Laufwerk auf einer antistatischen, Ebenen Fläche. vi. Setzen Sie das Ersatzlaufwerk mit beiden Händen vollständig in den Steckplatz ein. vii. Drücken Sie den Nockengriff nach unten, bis er einrastet. viii. Bringen Sie die Blende wieder an. ix. Benachrichtigen Sie den NetApp Support über den Austausch von Laufwerken. Der NetApp Support enthält Anweisungen zum Zurücksenden des ausgefallenen Laufwerks.

Node-Modell	Schritte
H610S	i. Ordnen Sie die Steckplatznummer des ausgefallenen Laufwerks von der Element-UI mit der Nummer auf dem Chassis an. Die LED am ausgefallenen Laufwerk leuchtet gelb. ii. Entfernen Sie die Blende. iii. Drücken Sie die Entriegelungstaste, und entfernen Sie das ausgefallene Laufwerk wie in der folgenden Abbildung gezeigt: Stellen Sie sicher, dass der Griff des Fachs vollständig geöffnet ist, bevor Sie versuchen, das Laufwerk aus dem Gehäuse zu schieben. iv. Schieben Sie das Laufwerk heraus, und legen Sie es auf eine statisch freie, Ebene Fläche. v. Drücken Sie die Entriegelungstaste am Ersatzlaufwerk, bevor Sie es in den Laufwerkschacht einsetzen. Die Feder des Griffs der Laufwerksfachleiste ist geöffnet. vi. Setzen Sie das Ersatzlaufwerk ohne übermäßige Kraft ein. Wenn das Laufwerk vollständig eingesetzt ist, hören Sie einen Klick. vii. Schließen Sie den Griff des Laufwerksfachs vorsichtig. viii. Bringen Sie die Blende wieder an. ix. Benachrichtigen Sie den NetApp Support über den Austausch von Laufwerken. Der NetApp Support enthält Anweisungen zum Zurücksenden des ausgefallenen Laufwerks.

3. Sie können das Laufwerk entweder über die Element UI oder über den NetApp Element Management Extension Point im Element Plug-in für vCenter Server wieder zum Cluster hinzufügen.

Wenn Sie ein neues Laufwerk in einem bestehenden Knoten installieren, registriert sich das Laufwerk automatisch als **verfügbar** in der Element UI. Sie sollten das Laufwerk zum Cluster hinzufügen, bevor es am Cluster teilnehmen kann.

Option	Schritte
Verwenden der Element-UI	a. Wählen Sie in der Element UI die Option **Cluster > Laufwerke**. b. Wählen Sie **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen. c. Wählen Sie das Aktionen-Symbol für das Laufwerk aus, das Sie hinzufügen möchten, und wählen Sie **Hinzufügen**.
Verwenden des Element Plug-ins für die vCenter Server-UI	a. Wählen Sie im Erweiterungspunkt NetApp Element Management des vSphere Web Clients die Option **NetApp Element-Verwaltung > Cluster > Laufwerke** aus. b. Wählen Sie aus der Dropdown-Liste verfügbar das Laufwerk aus, und wählen Sie **Hinzufügen**. c. Bestätigen Sie die Aktion.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

H410C Nodes ersetzen

Sie sollten einen Computing-Node ersetzen, wenn CPU-Fehler, andere Probleme mit der Hauptplatine auftreten oder der Computer nicht eingeschaltet wird. Die Anweisungen gelten für die Nodes H410C. Wenn Sie einen H410C Compute-Node besitzen, auf dem NetApp HCI Bootstrap OS Version 1.6P1 oder höher ausgeführt wird, müssen Sie den Node nicht ersetzen, wenn das Speicher-DIMM ausfällt. Sie müssen nur das ausgefallene DIMM ersetzen. Wenn die DIMMs im Knoten nicht ausgefallen sind, können Sie sie im Ersatzknoten verwenden.

Der Ersatzknoten sollte die gleiche Version von NetApp HCI Bootstrap OS haben wie die anderen Compute-Knoten in der NetApp HCI Installation.

Was Sie benötigen

- Sie haben festgestellt, dass der Compute-Node ersetzt werden muss.
- Sie verfügen über einen Ersatz-Computing-Node. Wenn Sie einen Ersatzknoten bestellen möchten, wenden Sie sich an den NetApp Support. Der Compute-Node wird mit installiertem Bootstrap-Betriebssystem an Sie geliefert. Knoten werden ab Werk mit der neuesten Version von Bootstrap OS ausgeliefert. Möglicherweise müssen Sie auf dem Knoten in den folgenden Szenarien den Prozess zur Rückkehr zum Werkabbild (RTFI) durchführen:
  - Auf Ihrer aktuellen NetApp HCI-Installation wird eine Version von Bootstrap OS vor der neuesten Version ausgeführt. In diesem Fall Downgrade der neue Knoten auf die Betriebssystemversion, auf die Ihre NetApp HCI-Installation ausgeführt wird.

- Auf dem ausgelieferten Ersatz-Node wird vor der neuesten Version ein Bootstrap OS ausgeführt. Bei der NetApp HCI Installation, wo der Node ersetzt wird, wird bereits die aktuelle Version ausgeführt. In diesem Fall wird der RTFI-Prozess die Betriebssystemversion auf dem neuen Knoten auf die neueste Version aktualisieren. Siehe "Verwendung eines USB-Schlüssels für RTFI (Anmeldung erforderlich)" und "Wie RTFI durch die Verwendung des BMC (Anmeldung erforderlich)".

- Sie haben ein elektrostatisches Entladungsband (ESD) oder andere antistatische Vorsichtsmaßnahmen getroffen.
- Sie haben jedes Kabel gekennzeichnet, das mit dem Computing-Node verbunden ist.

Über diese Aufgabe

Alarme im VMware vSphere Web Client warnen Sie bei einem Ausfall eines Knotens. Sie sollten die Seriennummer des ausgefallenen Knotens vom VMware vSphere Web Client mit der Seriennummer auf dem Aufkleber auf der Rückseite des Node übereinstimmen.

Beim Austausch eines H410C Computing-Node sind folgende Punkte zu beachten:

- Sie können den H410C Compute-Node mit vorhandenen NetApp HCI Computing- und Storage-Nodes im selben Chassis und Cluster kombinieren.
- Der Compute-Node H410C arbeitet nur mit Netzspannung (200-240 V AC). Sie sollten sicherstellen, dass die Stromanforderungen erfüllt sind, wenn Sie einem vorhandenen NetApp HCI-System H410C Nodes hinzufügen.

Schritte im Überblick

Hier finden Sie einen allgemeinen Überblick über die Schritte dieses Verfahrens:

- Bereiten Sie den Austausch des Computing-Nodes vor
- Ersetzen Sie den Computing-Node im Chassis
- Entfernen Sie die Computing-Node-Ressource in NetApp HCI 1.7 und höher
- Fügen Sie den Computing-Node dem Cluster hinzu
- Implementieren Sie Witness-Nodes für Storage-Cluster mit zwei und drei Nodes neu

Hier sind einige zusätzliche Aufgaben, die Sie möglicherweise durchführen müssen, wenn Ihr System die spezifischen Bedingungen hat, für die sie gelten:

- "Entfernen Sie Witness Nodes, um Computing-Ressourcen freizumachen"
- wenn Sie einen Ersatzknoten mit einem nicht standardmäßigen BMC-Passwort erhalten haben
- Aktualisieren Sie die BMC-Firmware auf Ihrem Node

Bereiten Sie den Austausch des Computing-Nodes vor

Sie sollten die auf dem Node gehosteten Virtual Machines (VMs) zu einem verfügbaren Host migrieren und den ausgefallenen Node aus dem Cluster entfernen. Sie sollten Details zum ausgefallenen Node, z. B. Seriennummer und Netzwerkinformationen, abrufen.

Schritte

1. Führen Sie im VMware vSphere Web Client die Schritte durch, um die VMs auf einen anderen verfügbaren Host zu migrieren.

   Die Migrationsschritte finden Sie in der VMware Dokumentation.

2. Führen Sie die Schritte aus, um den Knoten aus dem Inventar zu entfernen. Die Schritte hängen von der Version von NetApp HCI in Ihrer aktuellen Installation ab:

NetApp HCI-Versionsnummer	Schritte
NetApp HCI 1.3 und höher	a. Wählen Sie den fehlgeschlagenen Knoten aus, und wählen Sie **Monitor > Hardwarestatus > Sensoren**. b. Notieren Sie die Seriennummer des ausgefallenen Nodes. Dadurch können Sie den Node im Chassis identifizieren, indem Sie die Seriennummer auf dem Aufkleber auf der Rückseite des Node mit der angegebenen Seriennummer angeben. c. Klicken Sie mit der rechten Maustaste auf den fehlgeschlagenen Knoten und wählen Sie **Verbindung > Verbindung trennen**. d. Wählen Sie **Ja**, um die Aktion zu bestätigen. e. Klicken Sie mit der rechten Maustaste auf den fehlgeschlagenen Knoten und wählen Sie **aus Bestand entfernen**. f. Wählen Sie **Ja**, um die Aktion zu bestätigen.
NetApp HCI Versionen vor 1.3	a. Klicken Sie mit der rechten Maustaste auf den Knoten und wählen Sie **aus Bestand entfernen**. b. Wählen Sie den fehlgeschlagenen Knoten aus, und wählen Sie **Monitor > Hardwarestatus > Sensoren**. c. Notieren Sie die Seriennummer des Node 0. Diese ist die Seriennummer des ausgefallenen Node. Dadurch können Sie den Node im Chassis identifizieren, indem Sie die Seriennummer auf dem Aufkleber auf der Rückseite des Node mit der angegebenen Seriennummer angeben. d. Wenn der fehlgeschlagene Knoten ausgewählt wurde, wählen Sie **Verwalten > Netzwerk > VMkernel-Adapter** aus, und kopieren Sie die vier aufgeführten IP-Adressen. Sie können diese Informationen wiederverwenden, wenn Sie die ersten Schritte zur Netzwerkkonfiguration in VMware ESXi ausführen.

Ersetzen Sie den Computing-Node im Chassis

Nachdem Sie den ausgefallenen Node aus dem Cluster entfernt haben, können Sie den Node aus dem Chassis entfernen und den Ersatz-Node installieren.

Stellen Sie sicher, dass Sie einen antistatischen Schutz haben, bevor Sie die hier beschriebenen Schritte ausführen.

Schritte

1. Setzen Sie den antistatischen Schutz auf.
2. Packen Sie den neuen Node aus, und stellen Sie ihn auf eine Ebene Fläche in der Nähe des Chassis ein. Bewahren Sie das Verpackungsmaterial der Verpackung auf, wenn Sie den ausgefallenen Node an NetApp zurücksenden.
3. Beschriften Sie jedes Kabel, das an der Rückseite des Node eingesetzt ist, den Sie entfernen möchten. Nach der Installation des neuen Node sollten die Kabel wieder in die ursprünglichen Ports eingesetzt werden.
4. Trennen Sie alle Kabel vom Node.
5. Wenn Sie die DIMMs wiederverwenden möchten, entfernen Sie sie.
6. Ziehen Sie den Nockengriff auf der rechten Seite des Knotens nach unten, und ziehen Sie den Knoten mit beiden Nockengriffen heraus. Der Nockengriff, den Sie nach unten ziehen sollten, hat einen Pfeil darauf, um die Richtung anzuzeigen, in der er sich bewegt. Der andere Nockengriff bewegt sich nicht und ist dort, um den Knoten herausziehen zu helfen.

   Unterstützen Sie den Node mit beiden Händen, wenn Sie ihn aus dem Chassis ziehen.

7. Legen Sie den Knoten auf eine Ebene Fläche. Sie sollten den Node verpacken und ihn an NetApp zurücksenden.
8. Installieren Sie den Ersatzknoten.
9. Drücken Sie den Node in, bis Sie einen Klick hören.

   Stellen Sie sicher, dass Sie beim Einschieben des Node in das Chassis keine übermäßige Kraft verwenden.

   Stellen Sie sicher, dass der Node eingeschaltet ist. Wenn er nicht automatisch eingeschaltet wird, drücken Sie den Netzschalter an der Vorderseite des Knotens.

10. Wenn Sie die DIMMs aus dem ausgefallenen Knoten entfernt haben, setzen Sie sie in den Ersatzknoten ein.

    Sie sollten DIMMs in denselben Steckplätzen ersetzen, die sie im ausgefallenen Node aus entfernt wurden.

11. Schließen Sie die Kabel wieder an die Anschlüsse an, von denen Sie sie ursprünglich getrennt haben. Die Etiketten, die Sie beim Trennen an den Kabeln angebracht hatten, helfen Ihnen dabei.

    Wenn die Luftströmungsöffnungen an der Rückseite des Gehäuses durch Kabel oder Etiketten blockiert sind, kann dies zu vorzeitigen Komponentenausfällen aufgrund einer Überhitzung führen. Zwingen Sie die Kabel nicht zu den Ports. Kabel, Ports oder beides können beschädigt werden.

    Stellen Sie sicher, dass der Ersatz-Node auf die gleiche Weise wie die anderen Nodes im Chassis verkabelt ist.

Entfernen Sie die Computing-Node-Ressource in NetApp HCI 1.7 und höher

In NetApp HCI 1.7 und höher sollte nach dem physischen Austausch des Nodes die Computing-Node-Ressource über die Management-Node-APIs entfernt werden. Zur Verwendung VON REST-APIs muss auf Ihrem Storage-Cluster NetApp Element Software 11.5 oder höher ausgeführt werden. Sie sollten einen Management-Node mit Version 11.5 oder höher implementiert haben.

Schritte

1. Geben Sie die IP-Adresse des Verwaltungsknotens gefolgt von /mnode ein:
   `https://[IP address]/mnode`
2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus und geben Sie Cluster-Administrator-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 mNode-Client ein, wenn der Wert nicht bereits gefüllt ist. Geben Sie keinen Wert für das Clientgeheimnis ein.
   d. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

   > Wenn nach dem Autorisieren die `Auth Error TypeError: Failed to fetch` Fehlermeldung angezeigt wird, müssen Sie möglicherweise das SSL-Zertifikat für die MVIP Ihres Clusters akzeptieren. Kopieren Sie die IP in die Token-URL, fügen Sie die IP in eine andere Browser-Registerkarte ein und autorisieren Sie sie erneut. Wenn Sie versuchen, einen Befehl auszuführen, nachdem das Token abgelaufen ist, erhalten Sie einen `Error: UNAUTHORIZED` Fehler. Wenn Sie diese Antwort erhalten, autorisieren Sie erneut.

3. Schließen Sie das Dialogfeld Verfügbare Berechtigungen.
4. Wählen Sie **GET/Assets** aus.
5. Wählen Sie **Probieren Sie es aus**.
6. Wählen Sie **Ausführen**. Scrollen Sie im Antwortkörper nach unten zum Abschnitt „Computing“ und kopieren Sie die übergeordneten Werte und die id für den fehlgeschlagenen Rechenknoten.
7. Wählen Sie **DELETE/Assets/{Asset_id}/Compute-Nodes/{Compute_id}** aus.
8. Wählen Sie **Probieren Sie es aus**. Geben Sie die übergeordneten und id-Werte in Schritt 7 ein.
9. Wählen Sie **Ausführen**.

Fügen Sie den Computing-Node dem Cluster hinzu

Der Computing-Node sollte wieder dem Cluster hinzugefügt werden. Die Schritte hängen von der Version von NetApp HCI ab, die Sie ausführen.

NetApp HCI 1.6P1 und höher

Sie können NetApp Hybrid Cloud Control nur verwenden, wenn Ihre NetApp HCI Installation unter Version 1.6P1 oder höher ausgeführt wird.

Was Sie benötigen

- Stellen Sie sicher, dass der vSphere Instance NetApp HCI die Lizenzierung von vSphere Enterprise Plus

nutzt, wenn Sie eine Implementierung mit Virtual Distributed Switches erweitern.

- Stellen Sie sicher, dass für keine der in NetApp HCI verwendeten vCenter oder vSphere Instanzen abgelaufene Lizenzen vorhanden sind.
- Stellen Sie sicher, dass Sie über freie und nicht genutzte IPv4-Adressen im gleichen Netzwerksegment wie vorhandene Knoten verfügen (jeder neue Node muss im gleichen Netzwerk wie die vorhandenen Knoten seines Typs installiert sein).
- Stellen Sie sicher, dass Sie über die Anmeldedaten für das vCenter-Administratorkonto verfügen.
- Stellen Sie sicher, dass jeder neue Node dieselbe Netzwerktopologie und -Verkabelung wie die vorhandenen Storage- oder Computing-Cluster verwendet.
- "Verwalten Sie die Initiatoren und Volume-Zugriffsgruppen" Für den neuen Computing-Node.

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.
3. Wählen Sie im Fenster Installation erweitern die Option **erweitern**.
4. Melden Sie sich bei der NetApp Deployment Engine an, indem Sie die Anmeldedaten des Administrators für das lokale NetApp HCI-Storage-Cluster angeben.

   Sie können sich nicht mit den Anmeldeinformationen für das Lightweight Directory Access Protocol anmelden.

5. Wählen Sie auf der Willkommensseite **Ja** aus.
6. Führen Sie auf der Seite Endbenutzer-Lizenz die folgenden Aktionen durch:
   a. Lesen Sie die VMware-Endbenutzer-Lizenzvereinbarung.
   b. Wenn Sie die Bedingungen akzeptieren, wählen Sie **Ich akzeptiere** am Ende des Vertragstextes.
7. Wählen Sie **Weiter**.
8. Führen Sie auf der vCenter Seite die folgenden Schritte aus:
   a. Geben Sie einen FQDN oder eine IP-Adresse und Administratoranmeldeinformationen für die vCenter Instanz ein, die mit Ihrer NetApp HCI-Installation verknüpft ist.
   b. Wählen Sie **Weiter**.
   c. Wählen Sie ein vorhandenes vSphere Datacenter aus, zu dem der neue Computing-Node hinzugefügt werden soll, oder wählen Sie **Neues Datacenter erstellen** aus, um die neuen Computing-Nodes einem neuen Datacenter hinzuzufügen.

      Wenn Sie „Neues Datacenter erstellen“ auswählen, wird das Feld „Cluster“ automatisch ausgefüllt.

   d. Wenn Sie ein vorhandenes Datacenter ausgewählt haben, wählen Sie ein vSphere Cluster aus, mit dem die neuen Computing-Nodes verknüpft werden sollen.

Wenn NetApp HCI die Netzwerkeinstellungen des ausgewählten Clusters nicht erkennen kann, stellen Sie sicher, dass die vmKernel- und vmnic-Zuordnung für die Management-, Storage- und vMotion-Netzwerke auf die Bereitstellungsstandards eingestellt sind.

e. Wählen Sie **Weiter**.

9. Geben Sie auf der Seite ESXi-Anmeldeinformationen ein ESXi-Root-Passwort für den hinzuzufügenden Computing-Node oder die Nodes ein. Sie sollten dasselbe Passwort verwenden, das während der ersten NetApp HCI-Implementierung erstellt wurde.
10. Wählen Sie **Weiter**.
11. Wenn Sie ein neues vSphere Datacenter-Cluster erstellt haben, wählen Sie auf der Seite Netzwerktopologie eine Netzwerktopologie aus, die mit den neuen Computing-Nodes, die Sie hinzufügen, übereinstimmt.

Sie können die Option mit zwei Kabeln nur auswählen, wenn Ihre Computing-Nodes die Topologie mit zwei Kabeln verwenden und die vorhandene NetApp HCI-Implementierung mit VLAN-IDs konfiguriert ist.

12. Wählen Sie auf der Seite „Available Inventory“ den Node aus, den Sie der vorhandenen NetApp HCI-Installation hinzufügen möchten.

Bei einigen Computing-Nodes müssen Sie EVC möglicherweise auf der höchsten Ebene aktivieren, die Ihre vCenter-Version unterstützt, bevor Sie sie zu Ihrer Installation hinzufügen können. Sie sollten den vSphere-Client verwenden, um EVC für diese Computing-Nodes zu aktivieren. Aktualisieren Sie nach der Aktivierung die Seite **Inventar**, und versuchen Sie erneut, die Computing-Nodes hinzuzufügen.

13. Wählen Sie **Weiter**.
14. Optional: Wenn Sie einen neuen vSphere Datacenter-Cluster erstellt haben, importieren Sie auf der Seite Netzwerkeinstellungen Netzwerkinformationen aus einer vorhandenen NetApp HCI-Bereitstellung, indem Sie das Kontrollkästchen **Kopiereinstellung aus einem vorhandenen Cluster** aktivieren. Dadurch werden das Standard-Gateway und die Subnetzinformationen für jedes Netzwerk gefüllt.
15. Auf der Seite Netzwerkeinstellungen wurden einige Netzwerkinformationen von der ersten Bereitstellung erkannt. Der neue Compute-Node wird nach Seriennummer aufgeführt, und Sie sollten ihm neue Netzwerkinformationen zuweisen. Führen Sie für den neuen Computing-Node die folgenden Schritte aus:
    a. Wenn NetApp HCI ein Benennungspräfix erkannt hat, kopieren Sie es aus dem Feld Namenspräfix, und fügen Sie es als Präfix für den neuen eindeutigen Hostnamen ein, den Sie im Feld **Hostname** hinzufügen.
    b. Geben Sie im Feld **Management-IP-Adresse** eine Management-IP-Adresse für den Compute-Node im Subnetz des Managementnetzwerks ein.
    c. Geben Sie im Feld vMotion IP-Adresse eine vMotion IP-Adresse für den Computing-Node im Subnetz des vMotion-Netzwerks ein.
    d. Geben Sie im Feld iSCSI A - IP-Adresse eine IP-Adresse für den ersten iSCSI-Port des Compute-Node im iSCSI-Netzwerk-Subnetz ein.
    e. Geben Sie im Feld iSCSI B - IP-Adresse eine IP-Adresse für den zweiten iSCSI-Port des Compute-Node im iSCSI-Netzwerk-Subnetz ein.
16. Wählen Sie **Weiter**.

17. Auf der Seite „Überprüfung“ im Abschnitt „Netzwerkeinstellungen“ wird der neue Knoten fett gedruckt. Wenn Sie die Informationen in einem beliebigen Abschnitt ändern müssen, führen Sie die folgenden Schritte aus:
    a. Wählen Sie **Bearbeiten** für diesen Abschnitt aus.
    b. Wenn Sie die Änderungen abgeschlossen haben, wählen Sie auf allen nachfolgenden Seiten die Option Fortfahren, um zur Seite „Überprüfen“ zurückzukehren.
18. Optional: Wenn Sie keine Cluster-Statistiken und Support-Informationen an von NetApp gehostete SolidFire Active IQ Server senden möchten, deaktivieren Sie das endgültige Kontrollkästchen. Hierdurch wird der Zustand und die Diagnoseüberwachung in Echtzeit für NetApp HCI deaktiviert. Wenn diese Funktion deaktiviert wird, ist es für NetApp nicht mehr möglich, NetApp HCI proaktiv zu unterstützen und zu überwachen, um Probleme zu erkennen und zu beheben, bevor die Produktion beeinträchtigt wird.
19. Wählen Sie **Knoten Hinzufügen**. Sie können den Fortschritt überwachen, während NetApp HCI die Ressourcen hinzufügt und konfiguriert.
20. Optional: Vergewissern Sie sich, dass der neue Computing-Node in vCenter sichtbar ist.

NetApp HCI 1.4 P2, 1.4 und 1.3

Wenn Ihre NetApp HCI-Installation Version 1.4P2, 1.4 oder 1.3 ausführt, können Sie den Node mit der NetApp Deployment Engine dem Cluster hinzufügen.

Was Sie benötigen

- Stellen Sie sicher, dass der vSphere Instance NetApp HCI die Lizenzierung von vSphere Enterprise Plus nutzt, wenn Sie eine Implementierung mit Virtual Distributed Switches erweitern.
- Stellen Sie sicher, dass für keine der in NetApp HCI verwendeten vCenter oder vSphere Instanzen abgelaufene Lizenzen vorhanden sind.
- Stellen Sie sicher, dass Sie über freie und nicht genutzte IPv4-Adressen im gleichen Netzwerksegment wie vorhandene Knoten verfügen (jeder neue Node muss im gleichen Netzwerk wie die vorhandenen Knoten seines Typs installiert sein).
- Stellen Sie sicher, dass Sie über die Anmeldedaten für das vCenter-Administratorkonto verfügen.
- Stellen Sie sicher, dass jeder neue Node dieselbe Netzwerktopologie und -Verkabelung wie die vorhandenen Storage- oder Computing-Cluster verwendet.

Schritte

1. Navigieren Sie zur Management-IP-Adresse eines der vorhandenen Speicher-Nodes: `http://<storage_node_management_IP_address>/`
2. Melden Sie sich bei der NetApp Deployment Engine an, indem Sie die Anmeldedaten des Administrators für das lokale NetApp HCI-Storage-Cluster angeben.

    Sie können sich nicht mit den Anmeldeinformationen für das Lightweight Directory Access Protocol anmelden.

3. Wählen Sie **Erweitern Sie Ihre Installation**.
4. Wählen Sie auf der Willkommensseite **Ja** aus.
5. Führen Sie auf der Seite Endbenutzer-Lizenz die folgenden Aktionen durch:
    a. Lesen Sie die VMware-Endbenutzer-Lizenzvereinbarung.
    b. Wenn Sie die Bedingungen akzeptieren, wählen Sie **Ich akzeptiere** am Ende des Vertragstextes.

6. Wählen Sie **Weiter**.
7. Führen Sie auf der vCenter Seite die folgenden Schritte aus:
   a. Geben Sie einen FQDN oder eine IP-Adresse und Administratoranmeldeinformationen für die vCenter Instanz ein, die mit Ihrer NetApp HCI-Installation verknüpft ist.
   b. Wählen Sie **Weiter**.
   c. Wählen Sie ein vorhandenes vSphere Datacenter aus, dem der neue Computing-Node hinzugefügt werden soll.
   d. Wählen Sie ein vSphere-Cluster aus, dem der neue Computing-Node zugeordnet werden soll.

      Wenn Sie einen Compute-Node mit einer CPU-Generation hinzufügen, der sich von der CPU-Generation der vorhandenen Computing-Nodes unterscheidet und bei der steuernden vCenter Instanz Enhanced vMotion Compatibility (EVC) deaktiviert ist, sollten Sie EVC aktivieren, bevor Sie fortfahren. Dadurch wird für vMotion Funktionalität nach der Erweiterung gesorgt.

   e. Wählen Sie **Weiter**.
8. Erstellen Sie auf der Seite ESXi Credentials ESXi Administrator Credentials für den hinzuzufügenden Computing-Node. Sie sollten dieselben Master-Anmeldeinformationen verwenden, die während der ersten NetApp HCI-Bereitstellung erstellt wurden.
9. Wählen Sie **Weiter**.
10. Wählen Sie auf der Seite „Available Inventory“ den Node aus, den Sie der vorhandenen NetApp HCI-Installation hinzufügen möchten.

    Bei einigen Computing-Nodes müssen Sie EVC möglicherweise auf der höchsten Ebene aktivieren, die Ihre vCenter-Version unterstützt, bevor Sie sie zu Ihrer Installation hinzufügen können. Sie sollten den vSphere-Client verwenden, um EVC für diese Computing-Nodes zu aktivieren. Aktualisieren Sie nach dem Aktivieren die Seite „Inventar“, und versuchen Sie erneut, die Computing-Nodes hinzuzufügen.

11. Wählen Sie **Weiter**.
12. Führen Sie auf der Seite Netzwerkeinstellungen die folgenden Schritte aus:
    a. Überprüfen Sie die bei der ersten Bereitstellung erkannten Informationen.
    b. Jeder neue Computing-Node wird nach Seriennummer aufgeführt. Sollten Sie ihm neue Netzwerkinformationen zuweisen. Führen Sie für jeden neuen Storage-Node die folgenden Schritte aus:
       i. Wenn NetApp HCI ein Benennungspräfix erkannt hat, kopieren Sie es aus dem Feld Erkennungspräfix, und fügen Sie es als Präfix für den neuen eindeutigen Hostnamen ein, den Sie im Feld Hostname hinzufügen.
       ii. Geben Sie im Feld Management-IP-Adresse eine Management-IP-Adresse für den Computing-Node im Subnetz des Managementnetzwerks ein.
       iii. Geben Sie im Feld vMotion IP-Adresse eine vMotion IP-Adresse für den Computing-Node im Subnetz des vMotion-Netzwerks ein.
       iv. Geben Sie im Feld iSCSI A - IP-Adresse eine IP-Adresse für den ersten iSCSI-Port des Compute-Node im iSCSI-Netzwerk-Subnetz ein.
       v. Geben Sie im Feld iSCSI B - IP-Adresse eine IP-Adresse für den zweiten iSCSI-Port des Compute-Node im iSCSI-Netzwerk-Subnetz ein.

c. Wählen Sie **Weiter**.

13. Auf der Seite „Überprüfung“ im Abschnitt „Netzwerkeinstellungen“ wird der neue Knoten fett gedruckt. Wenn Sie Änderungen an den Informationen in einem beliebigen Abschnitt vornehmen möchten, führen Sie die folgenden Schritte aus:
    a. Wählen Sie **Bearbeiten** für diesen Abschnitt aus.
    b. Wenn Sie die Änderungen abgeschlossen haben, wählen Sie auf den nachfolgenden Seiten **Weiter** aus, um zur Seite Überprüfung zurückzukehren.
14. Optional: Wenn Sie keine Cluster-Statistiken und Support-Informationen an von NetApp gehostete Active IQ Server senden möchten, deaktivieren Sie das endgültige Kontrollkästchen. Hierdurch wird der Zustand und die Diagnoseüberwachung in Echtzeit für NetApp HCI deaktiviert. Wenn diese Funktion deaktiviert wird, ist es für NetApp nicht mehr möglich, NetApp HCI proaktiv zu unterstützen und zu überwachen, um Probleme zu erkennen und zu beheben, bevor die Produktion beeinträchtigt wird.
15. Wählen Sie **Knoten Hinzufügen**. Sie können den Fortschritt überwachen, während NetApp HCI die Ressourcen hinzufügt und konfiguriert.
16. Optional: Vergewissern Sie sich, dass der neue Computing-Node in vCenter sichtbar ist.

NetApp HCI 1.2, 1.1 und 1.0

Nachdem der Node physisch ersetzt wurde, sollten Sie ihn zurück zum VMware ESXi Cluster hinzufügen und verschiedene Netzwerkkonfigurationen durchführen, damit Sie alle verfügbaren Funktionen nutzen können.

Sie sollten über eine Konsole oder Tastatur, Video, Maus (KVM) verfügen, um diese Schritte auszuführen.

Schritte

1. VMware ESXi Version 6.0.0 installieren und konfigurieren Sie wie folgt:
    a. Wählen Sie auf der Fernbedienung oder dem KVM-Bildschirm die Option **Power Control > Set Power Reset** aus. Hierdurch wird der Node neu gestartet.
    b. Wählen Sie im sich öffnenden Startmenü durch Drücken der nach-unten-Taste die Option **ESXi Install** aus.

        Dieses Fenster bleibt nur fünf Sekunden lang geöffnet. Wenn Sie die Auswahl nicht in fünf Sekunden treffen, sollten Sie den Knoten erneut starten.

    c. Drücken Sie **Enter**, um den Installationsvorgang zu starten.
    d. Führen Sie die Schritte im Installationsassistenten durch.

        Wenn Sie aufgefordert werden, den Datenträger auszuwählen, auf dem ESXi installiert werden soll, sollten Sie das zweite Laufwerk in der Liste durch Auswahl der nach-unten-Taste auswählen. Wenn Sie zur Eingabe eines Root-Passworts aufgefordert werden, sollten Sie das gleiche Passwort eingeben, das Sie in der NetApp Deployment Engine beim Einrichten von NetApp HCI konfiguriert haben.

    e. Drücken Sie nach Abschluss der Installation **Enter**, um den Knoten neu zu starten.

        Standardmäßig wird der Knoten mit dem NetApp HCI Bootstrap-Betriebssystem neu gestartet. Sie sollten eine einmalige Konfiguration auf dem Knoten durchführen, damit er VMware ESXi verwendet.

2. Konfigurieren Sie VMware ESXi auf dem Knoten wie folgt:
   a. Geben Sie im Anmeldefenster des NetApp HCI Bootstrap OS Terminal User Interface (TUI) die folgenden Informationen ein:
      i. Benutzername: Element
      ii. Passwort: CatchTheFire!
   b. Drücken Sie die nach-unten-Taste, um **OK** auszuwählen.
   c. Drücken Sie zum Anmelden die Eingabetaste*.
   d. Wählen Sie im Hauptmenü mit der nach-unten-Taste **Support Tunnel > Open Support Tunnel** aus.
   e. Geben Sie im angezeigten Fenster Portinformationen ein.

      Hierzu sollten Sie sich an den NetApp Support wenden. NetApp Support meldet sich beim Node an, um die Boot-Konfigurationsdatei festzulegen und die Konfigurationsaufgabe abzuschließen.

   f. Starten Sie den Node neu.
3. Konfigurieren Sie das Managementnetzwerk wie folgt:
   a. Melden Sie sich bei VMware ESXi an, indem Sie die folgenden Anmeldedaten eingeben:
      i. Benutzername: Root
      ii. Passwort: Das Passwort, das Sie beim Installieren von VMware ESXi festgelegt haben.

      Das Passwort sollte mit den Parametern übereinstimmen, die Sie bei der Einrichtung von NetApp HCI in der NetApp Deployment Engine konfiguriert haben.

   b. Wählen Sie * Managementnetzwerk konfigurieren*, und drücken Sie **Enter**.
   c. Wählen Sie **Netzwerkadapter** aus, und drücken Sie **Enter**.
   d. Wählen Sie **vmnic2** und **vmnic3** aus, und drücken Sie **Enter**.
   e. Wählen Sie **IPv4-Konfiguration** aus, und drücken Sie die Leertaste auf der Tastatur, um die Option statische Konfiguration auszuwählen.
   f. Geben Sie die IP-Adresse, die Subnetzmaske und die Standard-Gateway-Informationen ein, und drücken Sie **Enter**. Sie können die kopierten Informationen wiederverwenden, bevor Sie den Node entfernt haben. Die IP-Adresse, die Sie hier eingeben, ist die Management-Netzwerk-IP-Adresse, die Sie zuvor kopiert haben.
   g. Drücken Sie * Esc*, um den Abschnitt Managementnetzwerk konfigurieren zu beenden.
   h. Wählen Sie **Ja**, um die Änderungen anzuwenden.
4. Fügen Sie den Node (Host) zum Cluster hinzu und konfigurieren Sie das Netzwerk, so dass der Node mit den anderen Nodes im Cluster synchronisiert wird:
   a. Wählen Sie im VMware vSphere Web Client **Hosts und Cluster** aus.
   b. Klicken Sie mit der rechten Maustaste auf den Cluster, dem Sie den Knoten hinzufügen möchten, und wählen Sie **Host hinzufügen**. Der Assistent führt Sie durch das Hinzufügen des Hosts.

Wenn Sie zur Eingabe des Benutzernamens und des Passworts aufgefordert werden, verwenden Sie die folgenden Anmeldedaten: Benutzername: Root Passwort: Das Passwort, das Sie bei der Einrichtung von NetApp HCI in der NetApp Deployment Engine konfiguriert haben

Es kann ein paar Minuten dauern, bis der Node dem Cluster hinzugefügt wurde. Nach Abschluss des Prozesses wird der neu hinzugefügte Node unter dem Cluster aufgeführt.

c. Wählen Sie den Knoten aus, und wählen Sie dann **Verwalten > Networking > Virtuelle Switches** aus, und führen Sie die folgenden Schritte aus:
   i. Wählen Sie **vSwitch0**. Es sollte nur vSwitch0 in der angezeigten Tabelle angezeigt werden.
   ii. Wählen Sie in der angezeigten Grafik **VM Network** aus, und wählen Sie **X** aus, um die VM-Netzwerk-Portgruppe zu entfernen.
   iii. Bestätigen Sie die Aktion.
   iv. Wählen Sie **vSwitch0** und dann das Bleistiftsymbol, um die Einstellungen zu bearbeiten.
   v. Wählen Sie im Fenster vSwitch0 - Einstellungen bearbeiten die Option **Teaming und Failover** aus.
   vi. Stellen Sie sicher, dass vmnic3 unter Standby-Adapter aufgeführt ist, und wählen Sie **OK** aus.
   vii. Wählen Sie in der angezeigten Grafik **Management Network** aus, und wählen Sie das Bleistiftsymbol, um die Einstellungen zu bearbeiten.
   viii. Wählen Sie im Fenster Verwaltungsnetzwerk - Einstellungen bearbeiten die Option **Teaming und Failover** aus.
   ix. Bewegen Sie vmnic3 mit dem Pfeilsymbol in den Standby-Adapter, und wählen Sie **OK** aus.
d. Wählen Sie im Dropdown-Menü Aktionen die Option **Netzwerke hinzufügen** aus, und geben Sie die folgenden Details in das angezeigte Fenster ein:
   i. Wählen Sie für den Verbindungstyp **Virtuelle Maschine Portgruppe für einen Standard-Switch** aus, und wählen Sie **Weiter**.
   ii. Wählen Sie für das Zielgerät die Option zum Hinzufügen eines neuen Standardschalters aus, und wählen Sie **Weiter**.
   iii. Wählen Sie **+** Aus.
   iv. Wählen Sie im Fenster Physikalische Adapter zu Switch hinzufügen die Option vmnic0 und vmnic4 aus, und wählen Sie **OK**. Vmnic0 und vmnic4 sind jetzt unter Aktive Adapter aufgelistet.
   v. Wählen Sie **Weiter**.
   vi. Überprüfen Sie unter Verbindungseinstellungen, ob VM Network die Netzwerkbezeichnung ist, und wählen Sie **Weiter**.
   vii. Wenn Sie bereit sind, fortzufahren, wählen Sie **Finish**. VSwitch1 wird in der Liste der virtuellen Switches angezeigt.
e. Wählen Sie **vSwitch1** und wählen Sie das Bleistiftsymbol, um die Einstellungen wie folgt zu bearbeiten:
   i. Stellen Sie unter Eigenschaften die MTU auf 9000 ein, und wählen Sie **OK**. Wählen Sie in der angezeigten Grafik **VM Network** aus, und wählen Sie das Bleistiftsymbol, um die Einstellungen wie folgt zu bearbeiten:
f. Wählen Sie **Sicherheit** aus, und wählen Sie die folgenden Optionen aus:

i. Wählen Sie **Teaming und Failover**, und aktivieren Sie das Kontrollkästchen **Override**.

ii. Bewegen Sie vmnic0 mithilfe des Pfeilsymbols in Standby-Adapter.

iii. Wählen Sie **OK**.

g. Wenn vSwitch1 ausgewählt ist, wählen Sie aus dem Dropdown-Menü Aktionen die Option **Netzwerk hinzufügen** aus, und geben Sie die folgenden Details in das angezeigte Fenster ein:

i. Wählen Sie für den Verbindungstyp **VMkernel Netzwerkadapter** aus, und wählen Sie **Weiter**.

ii. Wählen Sie für das Zielgerät die Option, um einen vorhandenen Standard-Switch zu verwenden, navigieren Sie zu vSwitch1, und wählen Sie **Weiter** aus.

iii. Ändern Sie unter Port-Eigenschaften das Netzwerketikett in vMotion, aktivieren Sie unter Enable Services das Kontrollkästchen für vMotion Traffic und wählen Sie **Next** aus.

iv. Geben Sie unter IPv4-Einstellungen die IPv4-Informationen ein, und wählen Sie **Weiter**. Die IP-Adresse, die Sie hier eingeben, ist die vMotion IP-Adresse, die Sie zuvor kopiert haben.

v. Wenn Sie bereit sind, fortzufahren, wählen Sie **Fertig stellen**.

h. Wählen Sie in der angezeigten Grafik vMotion aus, und wählen Sie das Bleistiftsymbol aus, um die Einstellungen wie folgt zu bearbeiten:

i. Wählen Sie **Sicherheit** aus, und wählen Sie die folgenden Optionen aus:

ii. Wählen Sie **Teaming und Failover**, und aktivieren Sie das Kontrollkästchen **Override**.

iii. Bewegen Sie vmnic4 mithilfe des Pfeilsymbols in Standby-Adapter.

iv. Wählen Sie **OK**.

i. Wenn vSwitch1 ausgewählt ist, wählen Sie aus dem Dropdown-Menü Aktionen die Option **Netzwerk hinzufügen** aus, und geben Sie die folgenden Details in das angezeigte Fenster ein:

i. Wählen Sie für den Verbindungstyp **VMkernel Netzwerkadapter** aus, und wählen Sie **Weiter**.

ii. Wählen Sie für das Zielgerät die Option zum Hinzufügen eines neuen Standardschalters aus, und wählen Sie **Weiter**.

iii. Wählen Sie **+** Aus.

iv. Wählen Sie im Fenster Physikalische Adapter zu Switch hinzufügen die Option vmnic1 und vmnic5 aus, und wählen Sie **OK**. Vmnic1 und vmnic5 sind jetzt unter Aktive Adapter aufgeführt.

v. Wählen Sie **Weiter**.

vi. Ändern Sie unter Port-Eigenschaften das Netzwerketikett in iSCSI-B, und wählen Sie **Weiter**.

vii. Geben Sie unter IPv4-Einstellungen die IPv4-Informationen ein, und wählen Sie **Weiter**. Die hier angegebene IP-Adresse ist die iSCSI-B-IP-Adresse, die Sie zuvor kopiert haben.

viii. Wenn Sie bereit sind, fortzufahren, wählen Sie **Finish**. VSwitch2 wird in der Liste der virtuellen Switches angezeigt.

j. Wählen Sie **vSwitch2** und wählen Sie das Bleistiftsymbol, um die Einstellungen wie folgt zu bearbeiten:

i. Stellen Sie unter Eigenschaften die MTU auf 9000 ein, und wählen Sie **OK**.

k. Wählen Sie in der angezeigten Grafik **iSCSI-B** aus, und wählen Sie das Bleistiftsymbol, um die Einstellungen wie folgt zu bearbeiten:

i. Wählen Sie **Sicherheit** aus, und wählen Sie die folgenden Optionen aus:

ii. Wählen Sie **Teaming und Failover**, und aktivieren Sie das Kontrollkästchen **Override**.

iii. Bewegen Sie vmnic1 mit dem Pfeilsymbol in nicht verwendete Adapter.

iv. Wählen Sie **OK**.

l. Wählen Sie im Dropdown-Menü Aktionen die Option **Netzwerke hinzufügen** aus, und geben Sie die folgenden Details in das angezeigte Fenster ein:

i. Wählen Sie für den Verbindungstyp **VMkernel Netzwerkadapter** aus, und wählen Sie **Weiter**.

ii. Wählen Sie für das Zielgerät die Option, um einen vorhandenen Standard-Switch zu verwenden, navigieren Sie zu vSwitch2, und wählen Sie **Weiter** aus.

iii. Ändern Sie unter Port-Eigenschaften die Netzwerkbezeichnung auf iSCSI-A und wählen Sie **Next** aus.

iv. Geben Sie unter IPv4-Einstellungen die IPv4-Informationen ein, und wählen Sie **Weiter**. Die IP-Adresse, die Sie hier eingeben, ist die iSCSI-A-IP-Adresse, die Sie zuvor kopiert haben.

v. Wenn Sie bereit sind, fortzufahren, wählen Sie **Fertig stellen**.

m. Wählen Sie in der angezeigten Grafik **iSCSI-A** aus, und wählen Sie das Bleistiftsymbol, um die Einstellungen wie folgt zu bearbeiten:

i. Wählen Sie **Sicherheit** aus, und wählen Sie die folgenden Optionen aus:

ii. Wählen Sie **Teaming und Failover**, und aktivieren Sie das Kontrollkästchen **Override**.

iii. Bewegen Sie vmnic5 mit dem Pfeilsymbol in nicht verwendete Adapter.

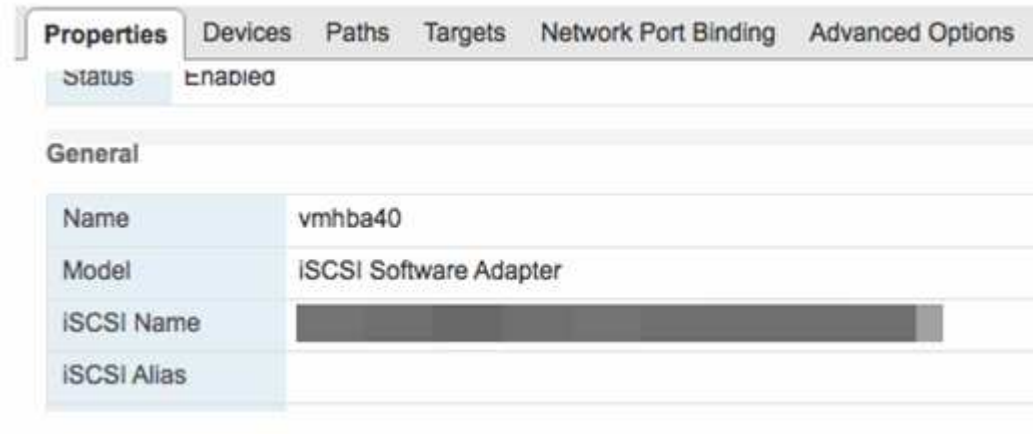
iv. Wählen Sie **OK**.

n. Wenn der neu hinzugefügte Knoten ausgewählt und die Registerkarte Verwalten geöffnet ist, wählen Sie **Storage > Speicheradapter** aus, und führen Sie die folgenden Schritte aus:

i. Wählen Sie **+** und wählen Sie **Software iSCSI Adapter**.

ii. Um den iSCSI-Adapter hinzuzufügen, wählen Sie im Dialogfeld **OK** aus.

iii. Wählen Sie unter Speicheradapter den iSCSI-Adapter aus, und kopieren Sie auf der Registerkarte Eigenschaften den iSCSI-Namen.



Sie benötigen den iSCSI-Namen beim Erstellen des Initiators.

a. Führen Sie im NetApp SolidFire vCenter Plug-in folgende Schritte aus:

i. Wählen Sie **Verwaltung > Initiatoren > Erstellen**.

ii. Wählen Sie **Einen einzelnen Initiator erstellen** aus.

iii. Geben Sie die zuvor kopierte IQN-Adresse im Feld IQN/WWPN ein.

iv. Wählen Sie **OK**.

v. Wählen Sie **Massenaktionen** aus, und wählen Sie **zu Volume Access Group** hinzufügen.

vi. Wählen Sie **NetApp HCI**, und wählen Sie **Hinzufügen**.

b. Wählen Sie im VMware vSphere Web Client unter Storage Adapter den iSCSI-Adapter aus, und führen Sie die folgenden Schritte aus:

i. Wählen Sie unter Adapterdetails die Option **Ziele > dynamische Erkennung > Hinzufügen** aus.

ii. Geben Sie die SVIP-IP-Adresse in das Feld iSCSI-Server ein.

Um die SVIP-IP-Adresse zu erhalten, wählen Sie **NetApp Element-Verwaltung** und kopieren Sie die SVIP-IP-Adresse. Behalten Sie die Standard-Portnummer wie lautet bei. Es sollte 3260 sein.

iii. Wählen Sie **OK**. Es wird eine Meldung angezeigt, die eine erneute Überprüfung des Speicheradapters empfiehlt.

iv. Wählen Sie das Symbol für den erneuten Scan aus.

v. Wählen Sie unter Adapterdetails die Option **Network Port Binding** aus, und wählen Sie **+** aus.

vi. Aktivieren Sie die Kontrollkästchen für iSCSI-B und iSCSI-A, und wählen Sie OK. Es wird eine Meldung angezeigt, die eine erneute Überprüfung des Speicheradapters empfiehlt.

vii. Wählen Sie das Symbol für den erneuten Scan aus. Nachdem die erneute Überprüfung abgeschlossen ist, überprüfen Sie, ob die Volumes im Cluster auf dem neuen Computing-Node (Host) sichtbar sind.

Implementieren Sie Witness-Nodes für Storage-Cluster mit zwei und drei Nodes neu

Nachdem Sie den ausgefallenen Computing-Node physisch ersetzt haben, sollten Sie die NetApp HCI Witness Node VM neu bereitstellen, wenn der ausgefallene Computing-Node den Witness Node hostet. Diese Anweisungen gelten nur für Computing-Nodes, die Teil einer NetApp HCI Installation mit zwei oder drei Storage-Clustern sind.

Was Sie benötigen

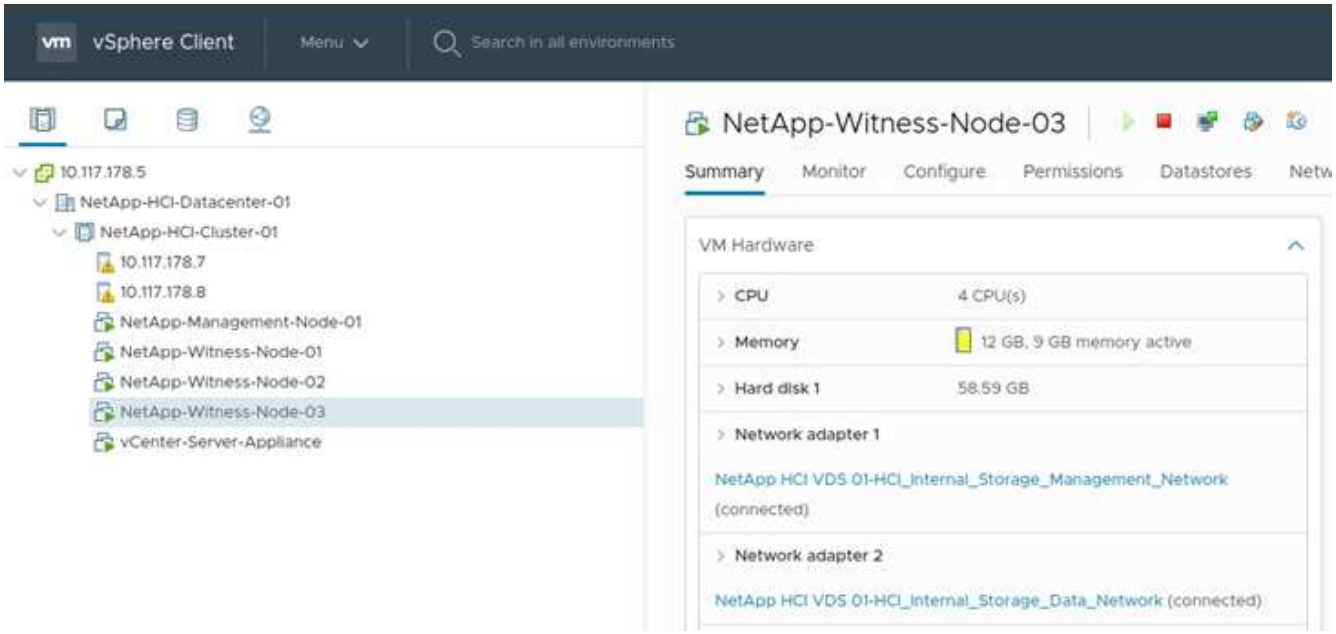
- Stellen Sie die folgenden Informationen zusammen:
  - Cluster-Name aus dem Storage-Cluster
  - Subnetzmaske, Gateway-IP-Adresse, DNS-Server und Domain-Informationen für das Management-Netzwerk
  - Subnetzmaske für das Storage-Netzwerk
- Stellen Sie sicher, dass Sie Zugriff auf das Storage Cluster haben, damit Sie dem Cluster die Witness Nodes hinzufügen können.
- Berücksichtigen Sie die folgenden Bedingungen, um zu entscheiden, ob Sie den vorhandenen Witness Node aus dem VMware vSphere Web Client oder dem Storage-Cluster entfernen möchten:
  - Wenn Sie denselben VM-Namen für den neuen Witness Node verwenden möchten, sollten Sie alle Verweise auf den alten Witness Node aus vSphere löschen.
  - Wenn Sie denselben Hostnamen auf dem neuen Witness Node verwenden möchten, sollten Sie zuerst den alten Witness Node aus dem Storage-Cluster entfernen.

Sie können den alten Witness Node nicht entfernen, wenn das Cluster nur zwei physische Storage-Nodes (und keine Witness Nodes) aufweist. In diesem Szenario sollten Sie zuerst den neuen Witness Node zum Cluster hinzufügen, bevor Sie den alten entfernen. Sie können den Witness Node mithilfe des NetApp Element Management-Erweiterungspunkts aus dem Cluster entfernen.

Wann sollten Sie Witness Nodes neu bereitstellen?

Sie sollten Witness Nodes in den folgenden Szenarien erneut bereitstellen:

- Sie haben einen fehlgeschlagenen Computing-Node ersetzt, der Teil einer NetApp HCI Installation ist. Er verfügt über ein Storage-Cluster mit zwei oder drei Nodes und der ausgefallene Computing-Node hostet eine Witness-Node-VM.
- Sie haben auf dem Rechenknoten die Prozedur Return to Factory Image (RTFI) durchgeführt.
- Die Witness Node VM ist beschädigt.
- Die Witness Node VM wurde versehentlich aus ESXi entfernt. Die VM wird mithilfe der Vorlage konfiguriert, die im Rahmen der ursprünglichen Implementierung mithilfe der NetApp Deployment Engine erstellt wurde. Hier ist ein Beispiel für eine Witness Node VM:



Schritte

1. Wählen Sie im VMware vSphere Web Client **Hosts und Cluster** aus.
2. Klicken Sie mit der rechten Maustaste auf den Compute-Node, der die Witness Node VM hostet, und wählen Sie **New Virtual Machine** aus.
3. Wählen Sie * aus Vorlage* bereitstellen aus, und wählen Sie **Weiter**.
4. Führen Sie die Schritte im Assistenten aus:
   a. Wählen Sie **Data Center**, suchen Sie die VM-Vorlage und wählen Sie **Next**.
   b. Geben Sie einen Namen für die VM im folgenden Format ein: NetApp-Witness-Node-##

   ## sollte durch eine Nummer ersetzt werden.

c. Lassen Sie die Standardauswahl für den VM-Standort unverändert, und wählen Sie **Weiter**.

d. Behalten Sie die Standardauswahl für die Ziel-Computing-Ressource unverändert bei, und wählen Sie **Weiter**.

e. Wählen Sie den lokalen Datenspeicher aus, und wählen Sie **Weiter** aus. Der freie Speicherplatz auf dem lokalen Datastore ist je nach Computing-Plattform unterschiedlich.

f. Wählen Sie **Power on Virtual Machine after creation** aus der Liste der Deploy-Optionen aus, und wählen Sie **Next**.

g. Überprüfen Sie die Auswahl, und wählen Sie **Fertig stellen**.

5. Konfigurieren Sie die Management-, Storage-Netzwerk- und Cluster-Einstellungen für den Witness Node wie folgt:

a. Wählen Sie im VMware vSphere Web Client **Hosts und Cluster** aus.

b. Klicken Sie mit der rechten Maustaste auf den Zeugen-Knoten, und schalten Sie ihn ein, wenn er nicht bereits eingeschaltet ist.

c. Wählen Sie in der Ansicht Zusammenfassung des Witness Node die Option **Web Console starten** aus.

d. Warten Sie, bis der Witness Node mit dem blauen Hintergrund zum Menü hochstartet.

e. Wählen Sie eine beliebige Stelle in der Konsole aus, um auf das Menü zuzugreifen.

f. Konfigurieren Sie das Managementnetzwerk wie folgt:

i. Drücken Sie die nach-unten-Taste, um zum Netzwerk zu navigieren, und drücken Sie dann **Enter** für OK.

ii. Navigieren Sie zu **Network config**, und drücken Sie dann **Enter** für OK.

iii. Navigieren Sie zu **net0**, und drücken Sie dann **Enter** für OK.

iv. Drücken Sie **Tab**, bis Sie zum IPv4-Feld gelangen. Löschen Sie gegebenenfalls die vorhandene IP im Feld und geben Sie die Management-IP-Informationen für den Witness-Knoten ein. Überprüfen Sie auch die Subnetzmaske und das Gateway.

Auf der VM-Host-Ebene wird kein VLAN-Tagging angewendet, Tagging wird in vSwitch behandelt.

v. Drücken Sie **Tab**, um zu OK zu navigieren, und drücken Sie **Enter**, um die Änderungen zu speichern. Nach der Konfiguration des Managementnetzwerks kehrt der Bildschirm zum Netzwerk zurück.

g. Konfigurieren Sie das Storage-Netzwerk wie folgt:

i. Drücken Sie die nach-unten-Taste, um zum Netzwerk zu navigieren, und drücken Sie dann **Enter** für OK.

ii. Navigieren Sie zu **Network config**, und drücken Sie dann **Enter** für OK.

iii. Navigieren Sie zu **net1**, und drücken Sie dann **Enter** für OK.

iv. Drücken Sie **Tab**, bis Sie zum IPv4-Feld gelangen. Löschen Sie gegebenenfalls die vorhandene IP im Feld und geben Sie die Speicher-IP-Informationen für den Witness-Knoten ein.

v. Drücken Sie **Tab**, um zu OK zu navigieren, und drücken Sie **Enter**, um die Änderungen zu speichern.

vi. Setzen Sie die MTU auf 9000.

Wenn die MTU nicht festgelegt ist, bevor Sie den Witness Node zum Cluster hinzufügen, werden für inkonsistente MTU-Einstellungen Cluster-Warnungen angezeigt. Dadurch wird verhindert, dass die Speicherbereinigung ausgeführt wird und Performance-Probleme auftreten.

vii. Drücken Sie **Tab**, um zu OK zu navigieren, und drücken Sie **Enter**, um die Änderungen zu speichern. Nach der Konfiguration des Speichernetzwerks kehrt der Bildschirm zum Netzwerk zurück.

h. Konfigurieren Sie die Cluster-Einstellungen wie folgt:

i. Drücken Sie **Tab**, um zu Abbrechen zu navigieren, und drücken Sie **Enter**.

ii. Navigieren Sie zu **Cluster-Einstellungen**, und drücken Sie dann **Enter** für OK.

iii. Drücken Sie **Tab**, um zu Einstellungen ändern zu navigieren, und drücken Sie **Enter**, um Einstellungen zu ändern.

iv. Drücken Sie **Tab**, um zum Feld Hostname zu navigieren, und geben Sie den Hostnamen ein.

v. Drücken Sie die nach-unten-Taste, um das Feld Cluster zuzugreifen, und geben Sie vom Storage-Cluster den Cluster-Namen ein.

vi. Drücken Sie die **Tab**-Taste, um zur OK-Taste zu navigieren, und drücken Sie **Enter**.

6. Fügen Sie den Witness Node dem Storage-Cluster wie folgt hinzu:

a. Greifen Sie über den vSphere Web Client auf den Erweiterungspunkt für die NetApp Element-Verwaltung über die Registerkarte **Shortcuts** oder das Seitenfeld zu.

b. Wählen Sie **NetApp Element-Verwaltung > Cluster**.

c. Wählen Sie die Unterregisterkarte **Nodes** aus.

d. Wählen Sie in der Dropdown-Liste * Ausstehend* aus, um die Liste der Knoten anzuzeigen. Der Witness Node sollte in der Liste der ausstehenden Nodes angezeigt werden.

e. Aktivieren Sie das Kontrollkästchen für den Knoten, den Sie hinzufügen möchten, und wählen Sie **Knoten hinzufügen**. Nach Abschluss der Aktion wird der Node in der Liste der aktiven Nodes für das Cluster angezeigt.

Ändern Sie das Passwort, wenn Sie einen Ersatzknoten mit einem nicht standardmäßigen BMC-Passwort erhalten haben

Einige Austauschknoten können mit nicht standardmäßigen Passwörtern für die Baseboard Management Controller (BMC) Benutzeroberfläche geliefert werden. Wenn Sie einen Ersatzknoten mit einem nicht standardmäßigen BMC-Passwort erhalten, sollten Sie das Passwort auf den Standard „ADMIN“ ändern.

Schritte

1. Ermitteln Sie, ob Sie einen Ersatzknoten mit einem nicht standardmäßigen BMC-Kennwort erhalten haben:

a. Suchen Sie nach einem Aufkleber unter dem IPMI-Port an der Rückseite des erhaltenen Ersatzknoten. Wenn Sie einen Aufkleber unter dem IPMI-Port finden, bedeutet dies, dass Sie einen Knoten mit einem nicht standardmäßigen BMC-Passwort erhalten haben. Das folgende Beispielbild finden Sie unter:

b. Notieren Sie sich das Passwort.

2. Melden Sie sich bei der BMC-Benutzeroberfläche mit dem eindeutigen Kennwort an, das auf dem Aufkleber gefunden wurde.
3. Wählen Sie **Werkseinstellung** aus, und wählen Sie die Optionsschaltfläche **Aktuelle Einstellungen entfernen und die Benutzereinstellungen auf ADMIN/ADMIN** setzen:
4. Wählen Sie **Wiederherstellen**.
5. Melden Sie sich ab und melden Sie sich dann wieder an, um zu bestätigen, dass die Anmeldeinformationen jetzt geändert wurden.

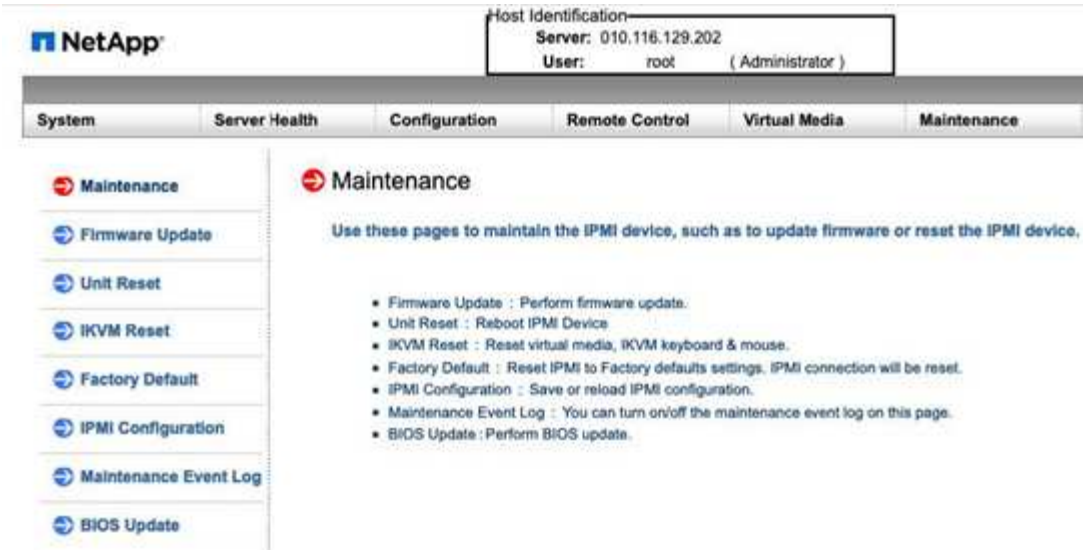
Aktualisieren Sie die BMC-Firmware auf Ihrem Node

Nach dem Austausch des Computing-Node müssen Sie eventuell die Firmware-Version aktualisieren. Sie können die neueste Firmware-Datei aus dem Dropdown-Menü auf der herunterladen"NetApp Support Site (Anmeldung erforderlich)".

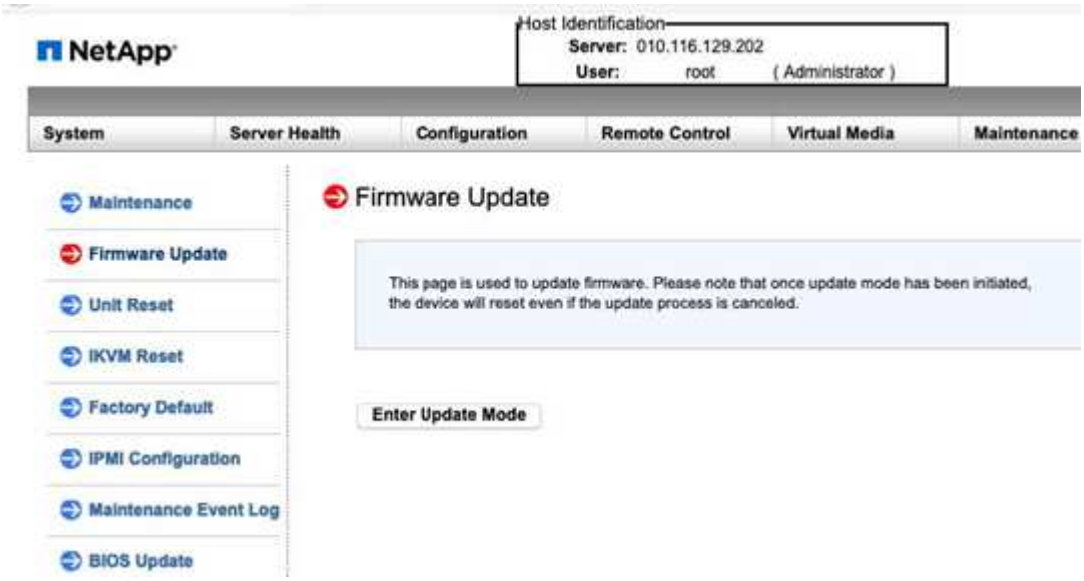
Schritte

1. Melden Sie sich bei der Baseboard Management Controller (BMC) UI an.
2. Wählen Sie **Wartung > Firmware-Aktualisierung**.

3. Wählen Sie in der BMC-Konsole die Option **Wartung** aus.



4. Wählen Sie auf der Registerkarte Wartung in der Navigation links in der Benutzeroberfläche die Option **Firmware-Aktualisierung** aus, und wählen Sie **Aktualisierungsmodus eingeben**.



5. Wählen Sie im Bestätigungsdialogfeld * Ja* aus.
6. Wählen Sie **Durchsuchen**, um das hochzuladende Firmware-Image auszuwählen, und wählen Sie **Firmware hochladen**. Das Laden der Firmware von einem Standort außerhalb der direkten Umgebung des Node kann zu längeren Ladezeiten und möglichen Timeouts führen.
7. Lassen Sie die Konfigurationsprüfungen beibehalten zu, und wählen Sie **Upgrade starten**. Das Upgrade dauert etwa 5 Minuten. Wenn Ihre Upload-Zeit 60 Minuten überschreitet, brechen Sie den Upload ab und übertragen Sie die Datei auf einen lokalen Rechner in der Nähe des Knotens. Wenn Ihre Sitzung nicht mehr verfügbar ist, wird möglicherweise eine Reihe von Warnungen angezeigt, während Sie versuchen, sich wieder im Firmware-Update-Bereich der BMC-Benutzeroberfläche anzumelden. Wenn Sie das Upgrade abbrechen, werden Sie zur Anmeldeseite umgeleitet.
8. Wählen Sie nach Abschluss der Aktualisierung die Option **OK** aus, und warten Sie, bis der Knoten neu gestartet wurde. Melden Sie sich nach dem Upgrade an, und wählen Sie **System** aus, um zu überprüfen, ob die **Firmware-Version** mit der von Ihnen hochgeladenen Version übereinstimmt.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

H410S Nodes ersetzen

Sie sollten einen Storage-Node ersetzen, wenn ein dualer Inline-Speichermodul (DIMM) ausfällt, CPU-Fehler, Probleme mit der Radian-Karte oder andere Probleme mit dem Motherboard auftreten oder sich dieser nicht einschalten lässt. Warnmeldungen im VMware vSphere Web Client warnen Sie, wenn ein Speicherknoten fehlerhaft ist. Sie sollten die NetApp Element Software-UI verwenden, um die Seriennummer (Service-Tag) des ausgefallenen Nodes zu erhalten. Sie benötigen diese Informationen, um den fehlgeschlagenen Node im Chassis zu finden.

Was Sie benötigen

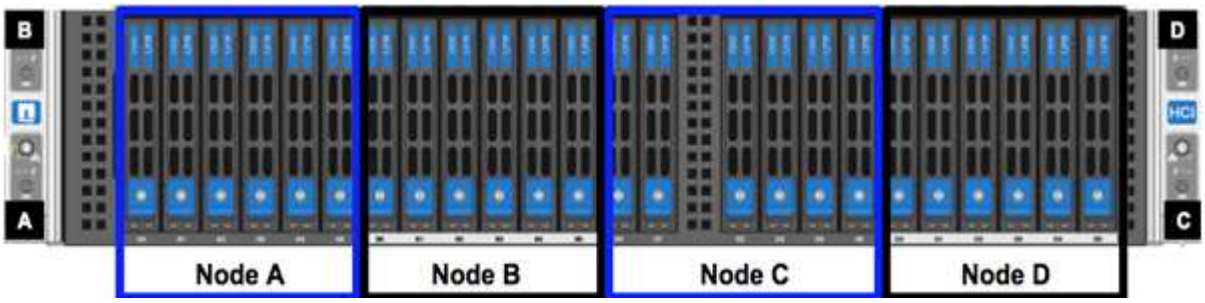
- Sie haben festgestellt, dass der Storage-Node ersetzt werden muss.
- Sie verfügen über einen Ersatz-Storage-Node.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder andere antistatische Vorsichtsmaßnahmen getroffen.
- Sie haben jedes Kabel gekennzeichnet, das mit dem Speicher-Node verbunden ist.

Über diese Aufgabe

Das Ersatzverfahren gilt für H410S Storage-Nodes in einem 2-HE-NetApp HCI-Chassis mit vier Nodes.

Folgende Rückansicht eines Chassis mit vier Nodes mit H410S Nodes:

Hier ist die Vorderansicht eines Chassis mit vier Nodes mit H410S Nodes, in dem die entsprechenden Schächte für jeden Node angezeigt werden:



Schritte im Überblick

Hier finden Sie einen allgemeinen Überblick über die Schritte dieses Verfahrens:

- Bereiten Sie den Austausch des Storage-Nodes vor
- Ersetzen Sie den Storage-Node im Chassis
- Fügen Sie den Storage-Node dem Cluster hinzu

Bereiten Sie den Austausch des Storage-Nodes vor

Sie sollten den fehlerhaften Storage-Node ordnungsgemäß aus dem Cluster entfernen, bevor Sie den Ersatz-Node installieren. Dies ist möglich, ohne dass es zu einer Serviceunterbrechung kommt. Sie sollten die Seriennummer des ausgefallenen Storage Node von der Element UI beziehen und diesen mit der Seriennummer auf dem Aufkleber auf der Rückseite des Node übereinstimmen.

Beim Ausfall von Komponenten, wenn der Node beispielsweise weiterhin online ist und funktioniert, sollten Sie die Laufwerke aus dem Cluster entfernen, bevor Sie den ausgefallenen Node entfernen.

Schritte

1. Wenn ein DIMM-Fehler auftritt, entfernen Sie die dem Node zugeordneten Laufwerke, die Sie anschließend vom Cluster ersetzen. Sie können entweder die NetApp Element Software-UI oder den NetApp Element Management-Erweiterungspunkt in Element Plug-in für vCenter Server verwenden, bevor Sie den Knoten entfernen.
2. Entfernen Sie die Knoten, indem Sie entweder die NetApp Element Software UI oder den NetApp Element Management Extension Point im Element Plug-in für vCenter Server verwenden:

Option	Schritte
Verwenden der Element-UI	a. Wählen Sie in der Element UI die Option **Cluster > Knoten**. b. Notieren Sie sich die Seriennummer (Service-Tag) des fehlerhaften Knotens. Diese Informationen müssen der Seriennummer auf dem Aufkleber auf der Rückseite des Node entsprechen. c. Nachdem Sie die Seriennummer notieren, entfernen Sie den Node wie folgt aus dem Cluster: d. Wählen Sie **Actions** für den Knoten, den Sie entfernen möchten. e. Wählen Sie **Entfernen**. Sie können den Knoten nun physisch aus dem Gehäuse entfernen.

Option	Schritte
Verwenden des Element Plug-ins für die vCenter Server-UI	a. Wählen Sie im Erweiterungspunkt NetApp Element Management des vSphere Web Clients die Option **NetApp Element-Verwaltung > Cluster** aus. b. Wählen Sie die Unterregisterkarte **Nodes** aus. c. Aktivieren Sie in der aktiven Ansicht das Kontrollkästchen für jeden Knoten, den Sie entfernen möchten, und wählen Sie **Aktionen > Entfernen**. d. Bestätigen Sie die Aktion. Alle aus einem Cluster entfernten Nodes werden in der Liste der ausstehenden Nodes angezeigt.

Ersetzen Sie den Storage-Node im Chassis

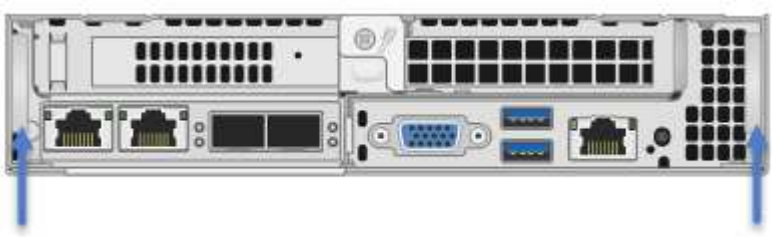
Sie sollten den Ersatz-Node im selben Steckplatz im Chassis installieren, aus dem Sie den fehlerhaften Node entfernen. Sie sollten die Seriennummer, die Sie über die UI notiert haben, verwenden und sie der Seriennummer auf der Rückseite des Node entsprechen.

Stellen Sie sicher, dass Sie einen antistatischen Schutz haben, bevor Sie die hier beschriebenen Schritte ausführen.

Schritte

1. Packen Sie den neuen Storage-Node aus, und stellen Sie ihn auf eine Ebene Fläche in der Nähe des Chassis ein. Bewahren Sie das Verpackungsmaterial der Verpackung auf, wenn Sie den ausgefallenen Node an NetApp zurücksenden.
2. Beschriften Sie jedes Kabel, das an der Rückseite des Storage Node eingesetzt wird, den Sie entfernen möchten. Nach der Installation des neuen Speicherknoten müssen die Kabel in die ursprünglichen Anschlüsse eingesetzt werden.
3. Trennen Sie alle Kabel vom Storage-Node.
4. Ziehen Sie den Nockengriff auf der rechten Seite des Knotens nach unten, und ziehen Sie den Knoten mit beiden Nockengriffen heraus. Der Nockengriff, den Sie nach unten ziehen sollten, hat einen Pfeil darauf, um die Richtung anzuzeigen, in der er sich bewegt. Der andere Nockengriff bewegt sich nicht und ist dort, um den Knoten herausziehen zu helfen.

   Unterstützen Sie den Node mit beiden Händen, wenn Sie ihn aus dem Chassis ziehen.



5. Legen Sie den Knoten auf eine Ebene Fläche.

6. Installieren Sie den Ersatzknoten.
7. Drücken Sie den Node in, bis Sie einen Klick hören.

   Stellen Sie sicher, dass Sie beim Einschieben des Node in das Chassis keine übermäßige Kraft verwenden.

8. Schließen Sie die Kabel wieder an die Anschlüsse an, von denen Sie sie ursprünglich getrennt haben. Die Etiketten, die Sie beim Trennen an den Kabeln angebracht hatten, helfen Ihnen dabei.

   Wenn die Luftströmungsöffnungen an der Rückseite des Gehäuses durch Kabel oder Etiketten blockiert sind, kann dies zu vorzeitigen Komponentenausfällen aufgrund einer Überhitzung führen. Zwingen Sie die Kabel nicht zu den Ports. Kabel, Ports oder beides können beschädigt werden.

   Stellen Sie sicher, dass der Ersatz-Node auf die gleiche Weise wie die anderen Nodes im Chassis verkabelt ist.

9. Drücken Sie die Taste an der Vorderseite des Knotens, um ihn wieder einschalten zu können.

Fügen Sie den Storage-Node dem Cluster hinzu

Sie sollten den Storage-Node wieder dem Cluster hinzufügen. Die Schritte hängen von der Version von NetApp HCI ab, die Sie ausführen.

Was Sie benötigen

- Sie verfügen über freie und nicht genutzte IPv4-Adressen im gleichen Netzwerksegment wie vorhandene Nodes (jeder neue Node muss im gleichen Netzwerk installiert sein wie vorhandene Knoten seines Typs).
- Sie verfügen über einen der folgenden Typen von SolidFire Storage Cluster Accounts:
  - Das native Administratorkonto, das während der ersten Implementierung erstellt wurde
  - Ein benutzerdefiniertes Benutzerkonto mit Berechtigungen für Cluster Admin, Laufwerke, Volumes und Nodes
- Sie haben den neuen Node verkabelt und mit Strom versorgt.
- Sie verfügen über die Management-IPv4-Adresse eines bereits installierten Storage-Node. Die IP-Adresse finden Sie auf der Registerkarte **NetApp Element-Verwaltung > Cluster > Knoten** des NetApp Element-Plug-ins für vCenter Server.
- Dabei ist sichergestellt, dass der neue Node dieselbe Netzwerktopologie und -Verkabelung wie die vorhandenen Storage-Cluster verwendet.

  Sorgen Sie dafür, dass die Storage-Kapazität gleichmäßig auf das gesamte Chassis verteilt wird, um eine optimale Zuverlässigkeit zu erzielen.

NetApp HCI 1.6P1 und höher

Sie können NetApp Hybrid Cloud Control nur verwenden, wenn Ihre NetApp HCI Installation unter Version 1.6P1 oder höher ausgeführt wird.

Schritte

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

```
https://<ManagementNodeIP>/manager/login
```

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des NetApp HCI-Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie im Fenster Installation erweitern die Option **erweitern**.
4. Melden Sie sich bei der NetApp Deployment Engine an, indem Sie die Anmeldedaten des Administrators für das lokale NetApp HCI-Storage-Cluster angeben.

   Sie können sich nicht mit den Anmeldeinformationen für das Lightweight Directory Access Protocol anmelden.

5. Wählen Sie auf der Willkommensseite **Nein**.
6. Wählen Sie **Weiter**.
7. Wählen Sie auf der Seite „Available Inventory“ den Storage-Node aus, den Sie der vorhandenen NetApp HCI-Installation hinzufügen möchten.
8. Wählen Sie **Weiter**.
9. Auf der Seite Netzwerkeinstellungen wurden einige Netzwerkinformationen von der ersten Bereitstellung erkannt. Jeder neue Storage Node wird nach Seriennummer aufgeführt. Sollten Sie ihm neue Netzwerkinformationen zuweisen. Führen Sie folgende Schritte aus:
   a. Wenn NetApp HCI ein Benennungspräfix erkannt hat, kopieren Sie es aus dem Feld Erkennungspräfix, und fügen Sie es als Präfix für den neuen eindeutigen Hostnamen ein, den Sie im Feld Hostname hinzufügen.
   b. Geben Sie im Feld Management-IP-Adresse eine Management-IP-Adresse für den neuen Storage Node im Subnetz des Managementnetzwerks ein.
   c. Geben Sie im Feld Speicher (iSCSI) IP-Adresse eine iSCSI-IP-Adresse für den neuen Speicherknoten ein, der sich im iSCSI-Netzwerk-Subnetz befindet.
   d. Wählen Sie **Weiter**.

   NetApp HCI nimmt möglicherweise eine Zeit in Anspruch, um die von Ihnen eingegebenen IP-Adressen zu validieren. Die Schaltfläche Weiter ist verfügbar, wenn die IP-Adressvalidierung abgeschlossen ist.

10. Auf der Seite „Überprüfung“ im Abschnitt „Netzwerkeinstellungen“ werden neue Knoten fett gedruckt. Wenn Sie die Informationen in einem beliebigen Abschnitt ändern müssen, führen Sie die folgenden Schritte aus:
    a. Wählen Sie **Bearbeiten** für diesen Abschnitt aus.
    b. Wenn Sie die Änderungen abgeschlossen haben, wählen Sie auf den nachfolgenden Seiten **Weiter** aus, um zur Seite Überprüfung zurückzukehren.
11. Optional: Wenn Sie keine Cluster-Statistiken und Support-Informationen an von NetApp gehostete Active IQ Server senden möchten, deaktivieren Sie das endgültige Kontrollkästchen. Hierdurch wird der Zustand und die Diagnoseüberwachung in Echtzeit für NetApp HCI deaktiviert. Wenn diese Funktion deaktiviert wird, ist es für NetApp nicht mehr möglich, NetApp HCI proaktiv zu unterstützen und zu überwachen, um Probleme zu erkennen und zu beheben, bevor die Produktion beeinträchtigt wird.
12. Wählen Sie **Knoten Hinzufügen**. Sie können den Fortschritt überwachen, während NetApp HCI die Ressourcen hinzufügt und konfiguriert.

13. Optional: Überprüfen Sie, ob neue Storage-Nodes im VMware vSphere Web Client sichtbar sind.

NetApp HCI 1.4 P2, 1.4 und 1.3

Wenn Ihre NetApp HCI-Installation Version 1.4P2, 1.4 oder 1.3 ausführt, können Sie den Node mit der NetApp Deployment Engine dem Cluster hinzufügen.

Schritte

1. Navigieren Sie zur Management-IP-Adresse eines der vorhandenen Speicher-Nodes: `http://<storage_node_management_IP_address>/`
2. Melden Sie sich bei der NetApp Deployment Engine an, indem Sie die Anmeldedaten des Administrators für das lokale NetApp HCI-Storage-Cluster angeben.

   Sie können sich nicht mit den Anmeldeinformationen für das Lightweight Directory Access Protocol anmelden.

3. Wählen Sie **Erweitern Sie Ihre Installation**.
4. Wählen Sie auf der Willkommensseite **Nein**.
5. Wählen Sie **Weiter**.
6. Wählen Sie auf der Seite „Available Inventory“ den Speicher-Node aus, der der NetApp HCI-Installation hinzugefügt werden soll.
7. Wählen Sie **Weiter**.
8. Führen Sie auf der Seite Netzwerkeinstellungen die folgenden Schritte aus:
   a. Überprüfen Sie die bei der ersten Bereitstellung erkannten Informationen. Jeder neue Storage Node wird nach Seriennummer aufgeführt. Sollten Sie ihm neue Netzwerkinformationen zuweisen. Führen Sie für jeden neuen Storage-Node die folgenden Schritte aus:
      i. Wenn NetApp HCI ein Benennungspräfix erkannt hat, kopieren Sie es aus dem Feld Erkennungspräfix, und fügen Sie es als Präfix für den neuen eindeutigen Hostnamen ein, den Sie im Feld Hostname hinzufügen.
      ii. Geben Sie im Feld Management-IP-Adresse eine Management-IP-Adresse für den neuen Storage Node im Subnetz des Managementnetzwerks ein.
      iii. Geben Sie im Feld Speicher (iSCSI) IP-Adresse eine iSCSI-IP-Adresse für den neuen Speicherknoten ein, der sich im iSCSI-Netzwerk-Subnetz befindet.
   b. Wählen Sie **Weiter**.
   c. Auf der Seite „Überprüfung“ im Abschnitt „Netzwerkeinstellungen“ wird der neue Knoten fett gedruckt. Wenn Sie Änderungen an den Informationen in einem beliebigen Abschnitt vornehmen möchten, führen Sie die folgenden Schritte aus:
      i. Wählen Sie **Bearbeiten** für diesen Abschnitt aus.
      ii. Wenn Sie die Änderungen abgeschlossen haben, wählen Sie auf den nachfolgenden Seiten **Weiter** aus, um zur Seite Überprüfung zurückzukehren.
9. Optional: Wenn Sie keine Cluster-Statistiken und Support-Informationen an von NetApp gehostete Active IQ Server senden möchten, deaktivieren Sie das endgültige Kontrollkästchen. Hierdurch wird der Zustand und die Diagnoseüberwachung in Echtzeit für NetApp HCI deaktiviert. Wenn diese Funktion deaktiviert wird, ist es für NetApp nicht mehr möglich, NetApp HCI proaktiv zu unterstützen und zu überwachen, um Probleme zu erkennen und zu beheben, bevor die Produktion beeinträchtigt wird.
10. Wählen Sie **Knoten Hinzufügen**. Sie können den Fortschritt überwachen, während NetApp HCI die

Ressourcen hinzufügt und konfiguriert.

11. Optional: Überprüfen Sie, ob neue Storage-Nodes im VMware vSphere Web Client sichtbar sind.

NetApp HCI 1.2, 1.1 und 1.0

Bei der Installation des Knotens zeigt die Terminal-Benutzeroberfläche (TUI) die für die Konfiguration des Knotens erforderlichen Felder an. Sie müssen die erforderlichen Konfigurationsinformationen für den Node eingeben, bevor Sie mit dem Hinzufügen des Node zum Cluster fortfahren.

Sie müssen die TUI verwenden, um statische Netzwerkinformationen sowie Cluster-Informationen zu konfigurieren. Wenn Sie Out-of-Band-Management verwendet haben, müssen Sie es auf dem neuen Node konfigurieren.

Sie sollten über eine Konsole oder Tastatur, ein Video, eine Maus (KVM) verfügen, um diese Schritte auszuführen und über die erforderlichen Netzwerk- und Clusterinformationen zum Konfigurieren des Knotens verfügen.

Schritte

1. Schließen Sie eine Tastatur und einen Monitor an den Knoten an. Die TUI wird auf dem tty1 Terminal mit der Registerkarte Netzwerkeinstellungen angezeigt.
2. Verwenden Sie die Bildschirmnavigation, um die Bond1G- und Bond10G-Netzwerkeinstellungen für den Node zu konfigurieren. Sie sollten die folgenden Informationen für Bond1G eingeben:
   - IP-Adresse. Sie können die Management-IP-Adresse vom ausgefallenen Node wiederverwenden.
   - Subnetzmaske. Wenn Sie nicht wissen, kann Ihr Netzwerkadministrator diese Informationen bereitstellen.
   - Gateway-Adresse. Wenn Sie nicht wissen, kann Ihr Netzwerkadministrator diese Informationen bereitstellen. Sie sollten die folgenden Informationen für Bond10G eingeben:
   - IP-Adresse. Sie können die Speicher-IP-Adresse vom ausgefallenen Knoten wiederverwenden.
   - Subnetzmaske. Wenn Sie nicht wissen, kann Ihr Netzwerkadministrator diese Informationen bereitstellen.
3. Geben Sie ein `s`, um die Einstellungen zu speichern, und geben Sie dann ein `y`, um die Änderungen zu übernehmen.
4. Geben Sie ein `c`, um zur Registerkarte Cluster zu navigieren.
5. Verwenden Sie die Bildschirmnavigation, um den Hostnamen und das Cluster für den Knoten einzustellen.

   Wenn Sie den Standardhostnamen in den Namen des Node ändern möchten, den Sie entfernt haben, sollten Sie dies jetzt tun.

   Am besten sollte derselbe Name für den neuen Node verwendet werden, den Sie ersetzt haben, um in Zukunft zu Verwirrungen zu vermeiden.

6. Geben Sie ein, `s` um die Einstellungen zu speichern. Die Cluster-Mitgliedschaft ändert sich von „verfügbar“ in „Ausstehend“.
7. Wählen Sie im NetApp Element Plug-in für vCenter Server die Option **NetApp Element-Verwaltung > Cluster > Knoten** aus.
8. Wählen Sie in der Dropdown-Liste * Ausstehend* aus, um die Liste der verfügbaren Knoten anzuzeigen.

9. Wählen Sie den Knoten aus, den Sie hinzufügen möchten, und wählen Sie **Hinzufügen**.

   Es kann bis zu 15 Minuten dauern, bis der Node dem Cluster hinzugefügt und unter Nodes > aktiv angezeigt wird.

   Das Hinzufügen der Laufwerke gleichzeitig kann zu Unterbrechungen führen. Best Practices zum Hinzufügen und Entfernen von Laufwerken finden Sie unter "Diesen KB-Artikel" (Anmeldung erforderlich).

10. Wählen Sie **Laufwerke**.
11. Wählen Sie in der Dropdown-Liste die Option **verfügbar** aus, um die verfügbaren Laufwerke anzuzeigen.
12. Wählen Sie die Laufwerke aus, die Sie hinzufügen möchten, und wählen Sie **Hinzufügen**.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

H610C und H615C Nodes ersetzen

Sie sollten ein Chassis ersetzen, um Computing-Node-Ausfälle im Zusammenhang mit der CPU, der Hauptplatine zu reparieren oder wenn es nicht eingeschaltet wird. Wenn ein defektes DIMM auf dem H610C-Rechenknoten vorhanden ist, auf dem NetApp HCI Bootstrap OS Version 1.6 oder höher ausgeführt wird, können Sie das DIMM austauschen und müssen das Gehäuse nicht ersetzen. Für H615C Nodes müssen Sie das Chassis nicht ersetzen, wenn ein DIMM ausfällt. Sie können nur das ausgefallene DIMM ersetzen.

Für H610C und H615C werden die Begriffe „Node“ und „Chassis“ austauschbar verwendet, da sich der Node und das Chassis nicht durch separate Komponenten unterscheiden.

Was Sie benötigen

- Sie haben überprüft, ob der Node ausgefallen ist.
- Sie verfügen über ein Ersatzgehäuse. Wenn Sie ein Ersatzteil bestellen möchten, wenden Sie sich bitte an den NetApp Support.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder einen anderen antistatischen Schutz.
- Sie haben jedes Kabel gekennzeichnet, das mit dem Chassis verbunden ist.

Über diese Aufgabe

Alarme im VMware vSphere Web Client warnen Sie bei einem Host-Ausfall. Sie müssen die Seriennummer des ausgefallenen Hosts vom VMware vSphere Web Client mit der Seriennummer auf dem Aufkleber auf der Rückseite des Node übereinstimmen.

Schritte im Überblick

Hier finden Sie einen allgemeinen Überblick über die Schritte in diesem Verfahren: Bereiten Sie den Austausch des Node vor Ersetzen Sie den Node Fügen Sie den Node dem Cluster hinzu Installieren Sie die GPU-Treiber

Bereiten Sie den Austausch des Node vor

Bevor Sie den Node ersetzen, sollten Sie die auf dem Node gehosteten Virtual Machines (VMs) auf einen verfügbaren Host migrieren und den Node aus dem Cluster entfernen. Sie sollten Details zum Node, z. B. Seriennummer und Netzwerkinformationen, erhalten.

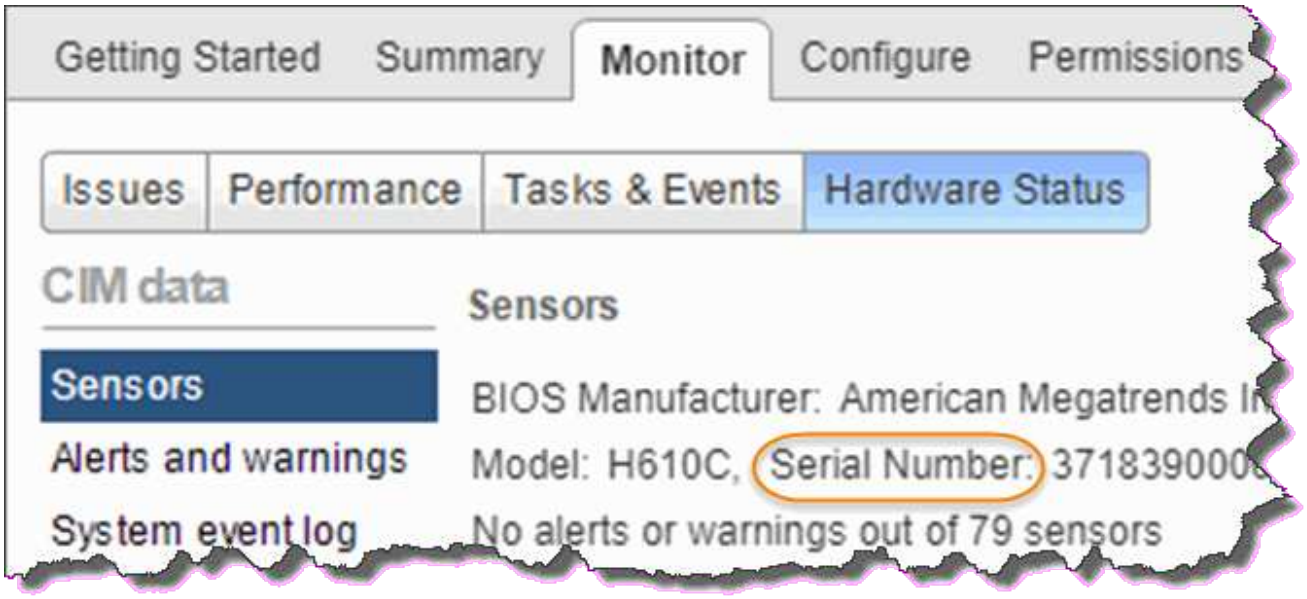
Beim Ausfall von Komponenten, wenn der Node beispielsweise weiterhin online ist und funktioniert, sollten Sie die Laufwerke aus dem Cluster entfernen, bevor Sie den ausgefallenen Node entfernen.

Schritte

1. Führen Sie im VMware vSphere Web Client die Schritte durch, um die VMs auf einen anderen verfügbaren Host zu migrieren.

   Die Migrationsschritte finden Sie in der VMware Dokumentation.

2. Wählen Sie den fehlgeschlagenen Knoten aus, und wählen Sie **Monitor > Hardwarestatus > Sensoren**.
3. Notieren Sie sich die Seriennummer des ausgefallenen Nodes. Der folgende Screenshot ist nur ein Beispiel:



   Sie benötigen die Seriennummer zum Identifizieren des Chassis, indem Sie der Nummer, die Sie mit der Seriennummer auf dem Aufkleber auf der Rückseite des Node angegeben haben, entsprechen.

4. Klicken Sie mit der rechten Maustaste auf den fehlgeschlagenen Knoten und wählen Sie **Verbindung > Verbindung trennen**.
5. Wählen Sie **Ja**, um die Aktion zu bestätigen.
6. Klicken Sie mit der rechten Maustaste auf den fehlgeschlagenen Knoten und wählen Sie **aus Bestand entfernen**.
7. Wählen Sie **Ja**, um die Aktion zu bestätigen.

Ersetzen Sie den Node

Nachdem Sie den ausgefallenen Node aus dem Cluster entfernt haben, können Sie das ausgefallene Chassis entfernen und das Ersatzgehäuse installieren.

Stellen Sie sicher, dass Sie einen antistatischen Schutz haben, bevor Sie die hier beschriebenen Schritte ausführen.

Schritte

1. Packen Sie das neue Gehäuse aus und legen Sie es auf eine Ebene Fläche. Bewahren Sie das Verpackungsmaterial der Verpackung auf, wenn Sie das fehlerhafte Chassis an NetApp zurücksenden.
2. Beschriften Sie jedes Kabel, das an der Rückseite des Gehäuses eingesetzt wird, das Sie entfernen möchten. Nach der Installation des neuen Gehäuses müssen Sie die Kabel wieder in die ursprünglichen Anschlüsse stecken.
3. Trennen Sie alle Kabel von der Rückseite des Gehäuses.
4. Entfernen Sie das Gehäuse, indem Sie die Rändelschrauben an den BefestigungsOhren lösen. Sie müssen das fehlerhafte Chassis an NetApp verpacken und an NetApp zurücksenden.
5. Schieben Sie das Ersatzgehäuse auf die Schienen.

   Achten Sie darauf, dass Sie beim Einschieben des Gehäuses auf die Schienen keine übermäßige Kraft verwenden.

6. Nur für H615C. Entfernen Sie die DIMMs aus dem fehlerhaften Gehäuse und setzen Sie diese DIMMs in das Ersatzgehäuse ein.

   Sie sollten die DIMMs in den gleichen Steckplätzen ersetzen, aus denen sie im ausgefallenen Node entfernt wurden.

7. Entfernen Sie die beiden Netzteile auf beiden Seiten des ausgefallenen Gehäuses und setzen Sie sie in das Ersatzgehäuse ein.
8. Schließen Sie die Kabel wieder an die Anschlüsse an, von denen Sie sie ursprünglich getrennt haben. Die Etiketten, die Sie beim Abstecken der Kabel hinzugefügt haben, helfen Ihnen dabei.

   Wenn die Luftströmungsöffnungen an der Rückseite des Gehäuses durch Kabel oder Etiketten blockiert sind, kann dies zu vorzeitigen Komponentenausfällen aufgrund einer Überhitzung führen. Zwingen Sie die Kabel nicht zu den Ports. Kabel, Ports oder beides können beschädigt werden.

9. Schalten Sie das Chassis ein.

Fügen Sie den Node dem Cluster hinzu

Sie sollten NetApp HCI so konfigurieren, dass der neue Compute-Node verwendet wird.

Was Sie benötigen

- Der vSphere Instance NetApp HCI verwendet vSphere Enterprise Plus-Lizenzen, wenn Sie den Knoten einer Implementierung mit Virtual Distributed Switches hinzufügen.
- Keine der vCenter oder vSphere Instanzen, die mit NetApp HCI verwendet werden, verfügen über abgelaufene Lizenzen.

- Sie verfügen über freie und nicht genutzte IPv4-Adressen im gleichen Netzwerksegment wie vorhandene Nodes (der neue Node muss im gleichen Netzwerk wie die vorhandenen Knoten seines Typs installiert sein).
- Sie haben die Anmeldedaten für das vCenter-Administratorkonto bereit.

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.
3. Wählen Sie im Fenster Installation erweitern die Option **erweitern**. Der Browser öffnet die NetApp Deployment Engine.
4. Melden Sie sich bei der NetApp Deployment Engine an, indem Sie die Anmeldedaten des Administrators für das lokale NetApp HCI-Storage-Cluster angeben.

   Sie können sich nicht mit den Anmeldeinformationen für das Lightweight Directory Access Protocol anmelden.

5. Wählen Sie auf der Willkommensseite **Ja** aus.
6. Führen Sie auf der Seite Endbenutzer-Lizenz die folgenden Aktionen durch:
   a. Lesen Sie die VMware-Endbenutzer-Lizenzvereinbarung.
   b. Wenn Sie die Bedingungen akzeptieren, wählen Sie **Ich akzeptiere** am Ende des Vertragstextes.
7. Wählen Sie Fortfahren.
8. Führen Sie auf der vCenter Seite die folgenden Schritte aus:
   a. Geben Sie einen FQDN oder eine IP-Adresse und Administratoranmeldeinformationen für die vCenter Instanz ein, die mit Ihrer NetApp HCI-Installation verknüpft ist.
   b. Wählen Sie **Weiter**.
   c. Wählen Sie ein vorhandenes vSphere Datacenter aus, zu dem die neuen Computing-Nodes hinzugefügt werden sollen, oder klicken Sie auf „Create New Datacenter“, um das neue Computing-Node zu einem neuen Datacenter hinzuzufügen.

      Wenn Sie „Neues Datacenter erstellen“ auswählen, wird das Feld „Cluster“ automatisch ausgefüllt.

   d. Wenn Sie ein vorhandenes Datacenter ausgewählt haben, wählen Sie ein vSphere Cluster aus, mit dem die neuen Computing-Nodes verknüpft werden sollen.

      Wenn die NetApp HCI die Netzwerkeinstellungen des Clusters, die Sie für die Erweiterung ausgewählt haben, nicht erkennen kann, stellen Sie sicher, dass die vmKernel und vmnic Zuordnung für das Management, die Storage- und vMotion-Netzwerke auf die Bereitstellungsstandards eingestellt sind.

   e. Wählen Sie **Weiter**.

9. Geben Sie auf der Seite ESXi-Anmeldeinformationen ein ESXi-Root-Passwort für den hinzuzufügenden Computing-Node oder die Nodes ein. Sie sollten dasselbe Passwort verwenden, das während der ersten NetApp HCI-Implementierung erstellt wurde.
10. Wählen Sie **Weiter**.
11. Wenn Sie ein neues vSphere Datacenter-Cluster erstellt haben, wählen Sie auf der Seite Netzwerktopologie eine Netzwerktopologie aus, die mit den neuen Computing-Nodes, die Sie hinzufügen, übereinstimmt.

    Sie können die Option mit zwei Kabeln nur auswählen, wenn Ihre Computing-Nodes die Topologie mit zwei Kabeln verwenden und die vorhandene NetApp HCI-Implementierung mit VLAN-IDs konfiguriert ist.

12. Wählen Sie auf der Seite „Available Inventory“ den Node aus, der der vorhandenen NetApp HCI-Installation hinzugefügt werden soll.

    Bei einigen Computing-Nodes müssen Sie EVC möglicherweise auf der höchsten Ebene aktivieren, die Ihre vCenter-Version unterstützt, bevor Sie sie zu Ihrer Installation hinzufügen können. Sie sollten den vSphere-Client verwenden, um EVC für diese Computing-Nodes zu aktivieren. Aktualisieren Sie nach dem Aktivieren die Seite „Inventar“, und versuchen Sie erneut, die Computing-Nodes hinzuzufügen.

13. Wählen Sie **Weiter**.
14. Optional: Wenn Sie einen neuen vSphere Datacenter-Cluster erstellt haben, importieren Sie auf der Seite Netzwerkeinstellungen Netzwerkinformationen aus einer vorhandenen NetApp HCI-Bereitstellung, indem Sie das Kontrollkästchen **Kopiereinstellung aus einem vorhandenen Cluster** aktivieren. Dadurch werden das Standard-Gateway und die Subnetzinformationen für jedes Netzwerk gefüllt.
15. Auf der Seite Netzwerkeinstellungen wurden einige Netzwerkinformationen von der ersten Bereitstellung erkannt. Jeder neue Computing-Node wird nach Seriennummer aufgeführt. Sollten Sie ihm neue Netzwerkinformationen zuweisen. Führen Sie für jeden neuen Computing-Node die folgenden Schritte aus:
    a. Wenn NetApp HCI ein Benennungspräfix erkannt hat, kopieren Sie es aus dem Feld Erkennungspräfix, und fügen Sie es als Präfix für den neuen eindeutigen Hostnamen ein, den Sie im Feld Hostname hinzufügen.
    b. Geben Sie im Feld Management-IP-Adresse eine Management-IP-Adresse für den Computing-Node im Subnetz des Managementnetzwerks ein.
    c. Geben Sie im Feld vMotion IP-Adresse eine vMotion IP-Adresse für den Computing-Node im Subnetz des vMotion-Netzwerks ein.
    d. Geben Sie im Feld iSCSI A - IP-Adresse eine IP-Adresse für den ersten iSCSI-Port des Compute-Node im iSCSI-Netzwerk-Subnetz ein.
    e. Geben Sie im Feld iSCSI B - IP-Adresse eine IP-Adresse für den zweiten iSCSI-Port des Compute-Node im iSCSI-Netzwerk-Subnetz ein.
16. Wählen Sie **Weiter**.
17. Auf der Seite „Überprüfung“ im Abschnitt „Netzwerkeinstellungen“ wird der neue Knoten fett gedruckt. Wenn Sie die Informationen in einem beliebigen Abschnitt ändern müssen, führen Sie die folgenden Schritte aus:
    a. Wählen Sie **Bearbeiten** für diesen Abschnitt aus.
    b. Wenn Sie die Änderungen abgeschlossen haben, wählen Sie auf den nachfolgenden Seiten **Weiter** aus, um zur Seite Überprüfung zurückzukehren.

18. Optional: Wenn Sie keine Cluster-Statistiken und Support-Informationen an von NetApp gehostete SolidFire Active IQ Server senden möchten, deaktivieren Sie das endgültige Kontrollkästchen. Hierdurch wird der Zustand und die Diagnoseüberwachung in Echtzeit für NetApp HCI deaktiviert. Wenn diese Funktion deaktiviert wird, ist es für NetApp nicht mehr möglich, NetApp HCI proaktiv zu unterstützen und zu überwachen, um Probleme zu erkennen und zu beheben, bevor die Produktion beeinträchtigt wird.
19. Wählen Sie **Knoten Hinzufügen**. Sie können den Fortschritt überwachen, während NetApp HCI die Ressourcen hinzufügt und konfiguriert.
20. Optional: Vergewissern Sie sich, dass neue Computing-Nodes in vCenter sichtbar sind.

Installieren Sie die GPU-Treiber

Compute-Nodes mit NVIDIA-GPUs (Graphics Processing Units) wie der H610C Node müssen die in VMware ESXi installierten NVIDIA-Softwaretreiber installiert sein, damit sie von der höheren Rechenleistung profitieren können. Um die GPU-Treiber zu installieren, muss der Compute-Node über eine GPU-Karte verfügen.

Schritte

1. Öffnen Sie einen Browser, und rufen Sie das NVIDIA Lizenzierungsportal unter der folgenden URL auf: `https://nvid.nvidia.com/dashboard/`
2. Laden Sie je nach Umgebung eines der folgenden Treiberpakete auf Ihren Computer herunter:

VSphere Version	Treiberpaket
VSphere 6.0	NVIDIA-GRID-vSphere-6.0-390.94-390.96-392.05.zip
VSphere 6.5	NVIDIA-GRID-vSphere-6.5-410.92-410.91-412.16.zip
VSphere 6.7	NVIDIA-GRID-vSphere-6.7-410.92-410.91-412.16.zip

3. Extrahieren Sie das Treiberpaket auf Ihrem Computer. Die resultierende .VIB-Datei ist die unkomprimierte Treiberdatei.
4. Kopieren Sie die .VIB-Treiberdatei von Ihrem Computer auf ESXi, die auf dem Computing-Knoten ausgeführt wird. Die folgenden Beispielbefehle für jede Version gehen davon aus, dass sich der Treiber im Verzeichnis US-Dollar HOME/NVIDIA/ESX6.x/ auf dem Management-Host befindet. Das SCP Utility ist in den meisten Linux Distributionen jederzeit verfügbar oder als Download-Dienstprogramm für alle Windows Versionen erhältlich:

Option	Beschreibung
ESXi 6.0	scp: STARTSEITE/NVIDIA/ESX6.0/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.
ESXi 6.5	scp: STARTSEITE/NVIDIA/ESX6.5/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.

Option	Beschreibung
ESXi 6.7	scp: STARTSEITE/NVIDIA/ESX6.7/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.

5. Verwenden Sie die folgenden Schritte, um sich als Root-Protokoll auf dem ESXi Host einzuloggen und den NVIDIA vGPU-Manager in ESXi zu installieren.
   a. Führen Sie den folgenden Befehl aus, um sich beim ESXi-Host als Root-Benutzer anzumelden:
   `ssh root@<ESXi_IP_ADDRESS>`
   b. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob derzeit keine NVIDIA-GPU-Treiber installiert sind:
   `nvidia-smi` Dieser Befehl sollte die Meldung zurückgeben `nvidia-smi: not found`.
   c. Führen Sie die folgenden Befehle aus, um den Wartungsmodus auf dem Host zu aktivieren und den NVIDIA vGPU-Manager aus der VIB-Datei zu installieren:
   `esxcli system maintenanceMode set --enable true`
   `esxcli software vib install -v /NVIDIA**.vib` Sie sollten die Meldung sehen `Operation finished successfully`.
   d. Führen Sie den folgenden Befehl aus, und überprüfen Sie, ob alle acht GPU-Treiber in der Befehlsausgabe aufgeführt sind:
   `nvidia-smi`
   e. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das NVIDIA vGPU-Paket ordnungsgemäß installiert und geladen wurde:
   `vmkload_mod -l | grep nvidia` Der Befehl sollte die Ausgabe ähnlich der folgenden zurückgeben: `nvidia 816 13808`
   f. Führen Sie die folgenden Befehle aus, um den Wartungsmodus zu beenden und den Host neu zu booten:
   `esxcli system maintenanceMode set –enable false`
   `reboot -f`
6. Wiederholen Sie die Schritte 4-6 für alle anderen neu implementierten Computing-Nodes mit NVIDIA-GPUs.
7. Führen Sie die folgenden Aufgaben anhand der Anweisungen auf der NVIDIA-Dokumentationswebsite durch:
   a. Installieren Sie den NVIDIA Lizenzserver.
   b. Konfigurieren Sie die Virtual Machine-Gastsysteme für die NVIDIA vGPU-Software.
   c. Wenn Sie vGPU-fähige Desktops im Kontext einer Virtual Desktop Infrastructure (VDI) verwenden, konfigurieren Sie die VMware Horizon View für NVIDIA vGPU-Software.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

H610S Nodes ersetzen

Möglicherweise müssen Sie das Gehäuse austauschen, wenn der Lüfter, die CPU (Central Processing Unit) oder ein Duales Inline-Speichermodul (DIMM) ausfällt oder

Überhitzungsprobleme oder Probleme mit dem Bootvorgang beheben. Die blinkende gelbe LED an der Vorderseite des Chassis zeigt an, dass ein Chassis möglicherweise ausgetauscht werden muss. Wenden Sie sich zunächst an den NetApp Support, bevor Sie fortfahren.

Informationen zu den Installationsanforderungen für H610S-Nodes finden Sie im"KB-Artikel". Neue und Ersatz-H610S Storage-Nodes weisen möglicherweise zusätzliche Installationsanforderungen auf Grundlage der vorhandenen Element Softwareversion des Storage-Clusters auf. Weitere Informationen erhalten Sie von Ihrem NetApp Support.

Die Begriffe „Node“ und „Chassis“ werden bei H610S gemeinsam verwendet, bei dem es sich um ein 1-HE-Chassis handelt.

Best Practices zum Hinzufügen und Entfernen von Laufwerken

Beim Hinzufügen von Laufwerken zum Cluster sollten Sie folgende Best Practices beachten:

- Fügen Sie alle Blocklaufwerke hinzu, und stellen Sie sicher, dass die Blocksynchronisierung abgeschlossen ist, bevor Sie die Slice-Laufwerke hinzufügen.
- Fügen Sie für Element Software ab 10.x alle Blocklaufwerke gleichzeitig ein. Stellen Sie sicher, dass Sie dies nicht für mehr als drei Knoten gleichzeitig tun.
- Fügen Sie bei der Element Software 9.x und früher drei Laufwerke gleichzeitig hinzu, um sie vollständig zu synchronisieren, bevor Sie die nächste Gruppe von drei hinzufügen.
- Entfernen Sie das Slice-Laufwerk, und stellen Sie sicher, dass die Schichtsynchronisierung abgeschlossen ist, bevor Sie die Blocklaufwerke entfernen.
- Entfernen Sie alle Blocklaufwerke gleichzeitig aus einem einzelnen Node. Vergewissern Sie sich, dass die Blocksynchronisierung abgeschlossen ist, bevor Sie zum nächsten Node fahren.

Was Sie benötigen

- Sie haben den NetApp Support kontaktiert. Wenn Sie einen Ersatz bestellen, sollten Sie beim NetApp Support einen Case eröffnen.
- Sie haben den Ersatzknoten erhalten.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder einen anderen antistatischen Schutz.
- Wenn Sie den RTFI-Prozess (Return to Factory Image) durchführen müssen, haben Sie den USB-Schlüssel erhalten. NetApp Support hilft Ihnen bei der Entscheidung, ob der RTFI-Prozess ausgeführt werden muss.
- Sie verfügen über eine Tastatur und einen Monitor.
- Sie haben den ausgefallenen Node ordnungsgemäß aus dem Cluster entfernt.
- Wenn ein DIMM ausgefallen ist, haben Sie die Laufwerke entfernt, bevor Sie den Node aus dem Cluster entfernen.

Über diese Aufgabe

Alarme im VMware vSphere Web Client warnen Sie bei einem Host-Ausfall. Sie müssen die Seriennummer des ausgefallenen Hosts vom VMware vSphere Web Client mit der Seriennummer auf dem Aufkleber auf der Rückseite des Node übereinstimmen.

Schritte

1. Suchen Sie die Service-Tag-Nummer an der Vorderseite des ausgefallenen Gehäuses.

2. Vergewissern Sie sich, dass die Seriennummer auf der Service-Tag-Nummer der NetApp Support-Fallnummer bei der Bestellung des Ersatzgehäuses entspricht.
3. Schließen Sie die Tastatur und den Monitor an die Rückseite des defekten Gehäuses an.
4. Überprüfen Sie die Seriennummer des ausgefallenen Nodes mit NetApp Support.
5. Schalten Sie das Chassis aus.
6. Beschriften Sie die Laufwerke vorn und die Kabel auf der Rückseite mit ihren Positionen, damit Sie sie nach dem Austausch an denselben Stellen wiederaufnehmen können.

   Die Anordnung der Laufwerke im Gehäuse ist in der folgenden Abbildung dargestellt:

7. Entfernen Sie die Kabel.
8. Entfernen Sie das Gehäuse, indem Sie die Rändelschrauben an den BefestigungsOhren lösen. Sie sollten das fehlerhafte Chassis verpacken und an NetApp zurücksenden.
9. Setzen Sie das Ersatzgehäuse ein.
10. Entfernen Sie die Laufwerke sorgfältig aus dem ausgefallenen Chassis und setzen Sie sie in das Ersatzgehäuse ein.

    Sie sollten die Laufwerke in die gleichen Steckplätze einsetzen, bevor Sie sie entfernt haben.

11. Entfernen Sie die Netzteile aus dem ausgefallenen Gehäuse und setzen Sie sie in das Ersatzgehäuse ein.
12. Stecken Sie die Netzteilkabel und die Netzwerkkabel in die ursprünglichen Anschlüsse.

13. SFP-Transceiver (Small Form-Factor Pluggable) können möglicherweise in die 10-GbE-Ports des Ersatz-Nodes eingesetzt werden. Sie sollten sie entfernen, bevor Sie die 10-GbE-Ports verkabeln.

> Wenn der Switch die Kabel nicht erkennt, lesen Sie die Dokumentation des Switch-Anbieters.

14. Schalten Sie das Gehäuse ein, indem Sie den Netzschalter an der Vorderseite drücken. Es dauert etwa fünf Minuten und 30 Sekunden, bis der Node gebootet wird.
15. Führen Sie die Konfigurationsschritte durch.
    - Wenn der H610S-Node Teil einer NetApp HCI Installation ist, konfigurieren Sie die Storage-Ressource mit NetApp Hybrid Cloud Control. Siehe "Erweitern Sie NetApp HCI Storage-Ressourcen".
    - Wenn der H610S-Node Teil einer SolidFire All-Flash-Storage-Installation ist, konfigurieren Sie den Node mithilfe der NetApp Element Software-Benutzeroberfläche (UI). Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Ersetzen Sie die Netzteile

Jedes Chassis besitzt zwei Netzteile für Redundanz bei der Stromversorgung. Wenn ein Netzteil defekt ist, sollten Sie es so schnell wie möglich austauschen, um sicherzustellen, dass das Gehäuse über eine redundante Stromquelle verfügt.

Was Sie benötigen

- Sie haben festgestellt, dass das Netzteil defekt ist.
- Sie haben ein Ersatznetzteil.
- Sie haben überprüft, dass das zweite Netzteil in Betrieb ist.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder andere antistatische Vorsichtsmaßnahmen getroffen.

Über diese Aufgabe

Das Ersatzverfahren gilt für die folgenden Node-Modelle:

- Zwei Höheneinheiten (2 HE) mit vier Nodes NetApp HCI-Chassis
- 2 HE H610C Computing-Chassis
- 1-HE-H615C Computing-Chassis
- 1-HE-H610S Storage-Chassis

> Bei H610C, H615C und H610S werden die Begriffe „Node“ und „Chassis“ austauschbar verwendet, da Node und Chassis keine separaten Komponenten sind, im Gegensatz zum 2-HE-Chassis mit vier Nodes.

Alarme im VMware vSphere Web Client geben Informationen über das fehlerhafte Netzteil, die sich auf PS1

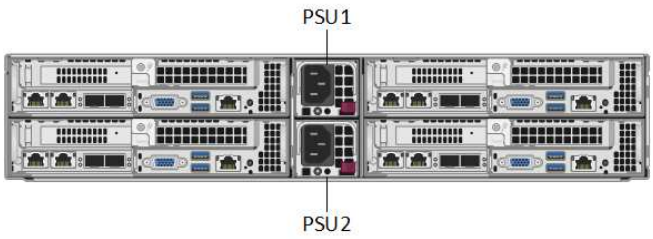
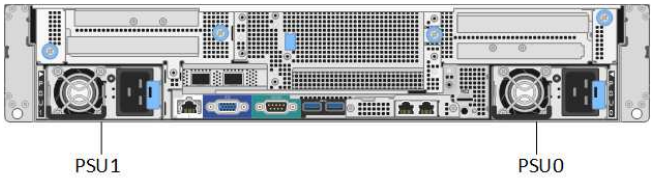
oder PS2 beziehen. In einem NetApp HCI 2-HE-Chassis mit vier Nodes bezeichnet PS1 die Einheit in der oberen Zeile des Gehäuses und PS2 die Einheit in der unteren Zeile des Gehäuses. Sie können das fehlerhafte Netzteil austauschen, während das Gehäuse eingeschaltet und funktionsfähig ist, solange das redundante Netzteil funktioniert.

Schritte

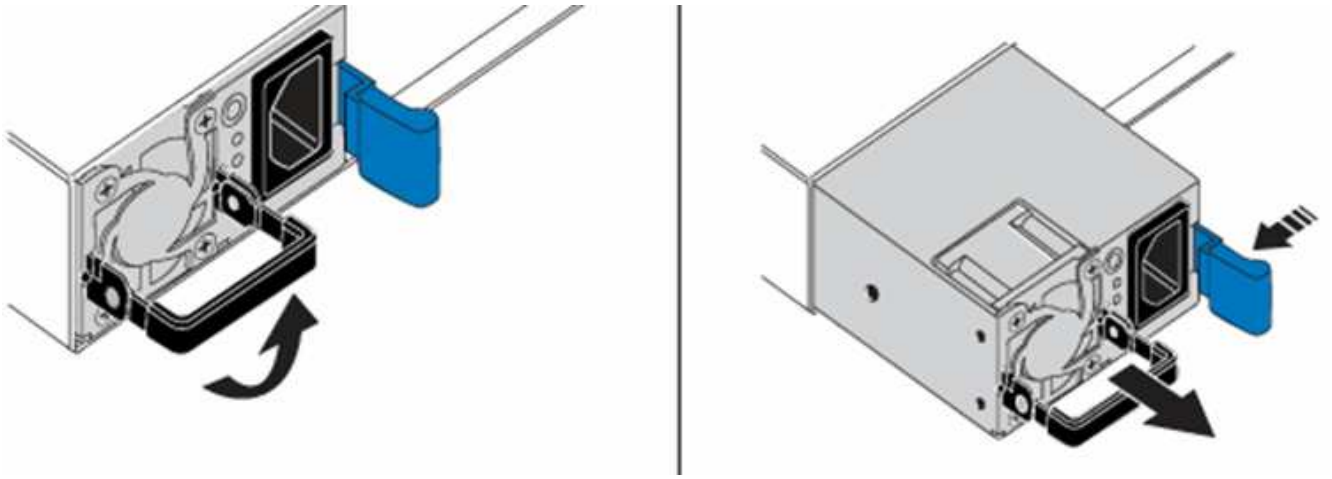
1. Suchen Sie das defekte Netzteil im Gehäuse. Die LED auf dem defekten Gerät zeigt gelb an.

   Die Netzteile befinden sich je nach Gehäusetyp unterschiedlich.

   Die Positionen der Netzteile finden Sie in den folgenden Bildern:

Modell	Position der Netzteile
2-HE-NetApp HCI-Storage-Chassis mit vier Nodes	 Die Nodes in Ihrem Chassis können je nach Node-Typ (Storage oder Computing) unterschiedlich aussehen.
H610C Chassis	
H615C Chassis	
H610S Chassis	

2. Ziehen Sie das Netzkabel vom Netzteil ab.
3. Heben Sie den Nockengriff an, und drücken Sie die blaue Verriegelung, um das Netzteil herauszuschieben.



Die Abbildung ist ein Beispiel. Die Position des Netzteils im Gehäuse und die Farbe der Entriegelungstaste variieren je nach Gehäusetyp.

Stellen Sie sicher, dass Sie beide Hände verwenden, um das Gewicht des Netzteils zu unterstützen.

4. Richten Sie die Kanten des Netzteils mit beiden Händen an der Öffnung im Gehäuse aus. Schieben Sie das Gerät vorsichtig mit dem Nockengriff in das Gehäuse, bis es einrastet, und bringen Sie den Nockengriff in die aufrechte Position zurück.
5. Schließen Sie das Netzkabel an.
6. Senden Sie das fehlerhafte Gerät an NetApp zurück. Befolgen Sie die Anweisungen im Lieferumfang, die Sie erhalten haben.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Ersetzen Sie die Switches SN2010, SN2100 und SN2700

Führen Sie die Best Practices und Schritte von NetApp durch, um einen fehlerhaften SN2000-Switch unterbrechungsfrei zu ersetzen.

Was Sie benötigen

- Stellen Sie sicher, dass Putty auf dem Laptop installiert ist und dass Sie die Ausgabe erfassen. In diesem Video erfahren Sie, wie Sie Putty konfigurieren, um die Ausgabesitzung zu erfassen.

[] | *https://img.youtube.com/vi/2LZfWH8HffA/maxresdefault.jpg*

- Stellen Sie sicher, dass Sie NetApp Config Advisor vor und nach dem Austausch ausführen. Dies kann dabei helfen, andere Probleme zu erkennen, bevor die Wartung gestartet wird. Laden Sie Config Advisor herunter und installieren Sie es, und greifen Sie auf die Kurzanleitung von "Hier (Anmeldung erforderlich)"zu.
- Beziehen Sie ein Netzkabel, die grundlegenden Handwerkzeuge und Etiketten.

- Stellen Sie sicher, dass Sie ein Wartungsfenster von zwei bis vier Stunden geplant haben.
- Machen Sie sich mit den folgenden Switch-Ports vertraut:

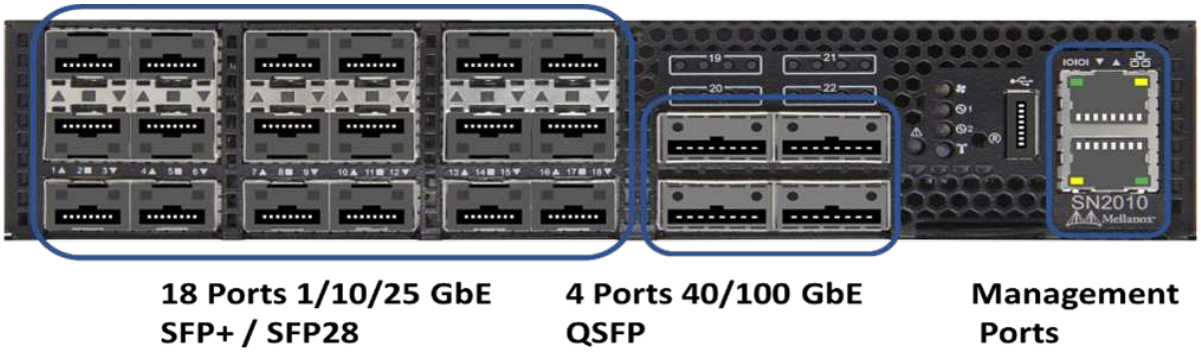


Abbildung 1. SN2010-Schaltfaceplate und -Anschlüsse

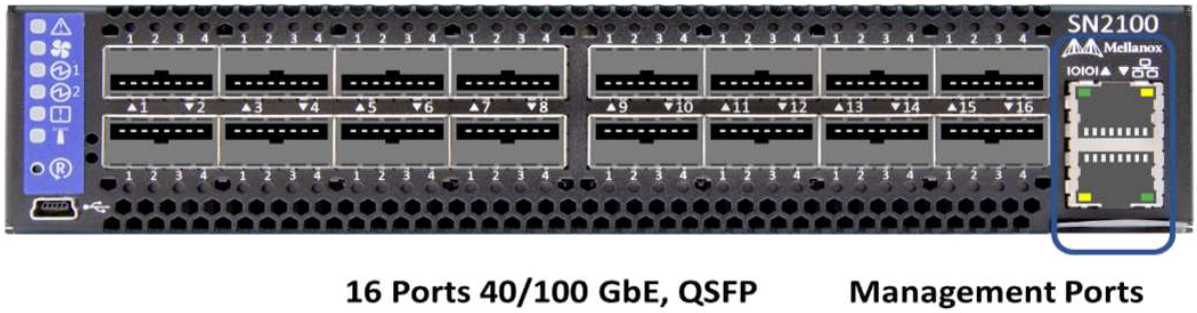


Abbildung 2. SN2100-Switch-Frontplatte und -Anschlüsse

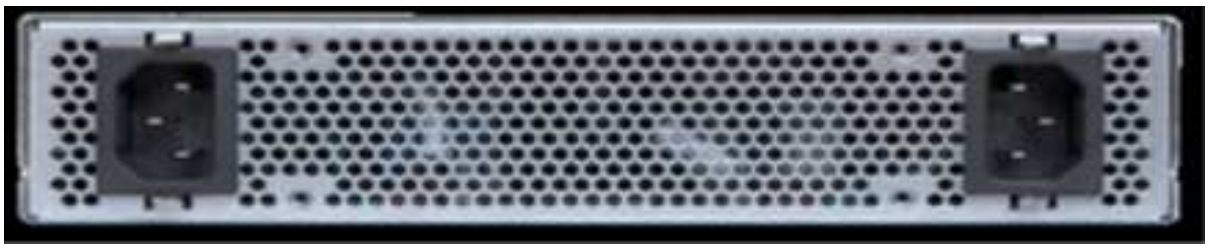


Abbildung 3. Schalter SN2010 und SN2100 hinten

Abbildung 4. SN2700-Schalter vorn und hinten

Über diese Aufgabe

Führen Sie die Schritte in diesem Verfahren in der folgenden Reihenfolge aus. So wird sichergestellt, dass die Downtime minimal ist und der Ersatz-Switch vor dem Austausch des Switches vorkonfiguriert ist.

Wenden Sie sich an den NetApp Support, wenn Sie Hilfe benötigen.

Hier eine Übersicht der Schritte im Verfahren:

- Bereiten Sie den Austausch des fehlerhaften Schalters vor
- Erstellen Sie die Konfigurationsdatei
- und setzen Sie den Austausch ein
- Überprüfen Sie die Betriebssystemversion auf dem Switch
- Konfigurieren Sie den Ersatzschalter
- Führen Sie den Austausch durch

Bereiten Sie den Austausch des fehlerhaften Schalters vor

Führen Sie die folgenden Schritte aus, bevor Sie den defekten Schalter austauschen.

Schritte

1. Stellen Sie sicher, dass der Austauschschalter das gleiche Modell wie der fehlerhafte Schalter hat.
2. Kennzeichnen Sie alle Kabel, die mit dem defekten Schalter verbunden sind.
3. Identifizieren Sie den externen Dateiserver, auf dem die Switch-Konfigurationsdateien gespeichert werden.
4. Stellen Sie sicher, dass Sie die folgenden Informationen erhalten haben:
   a. Die für die Erstkonfiguration verwendete Schnittstelle: RJ-45-Port oder Serial Terminal Interface.
   b. Die für den Switch-Zugriff benötigten Anmeldeinformationen: IP-Adresse des Management-Ports des nicht fehlerhaften Switch und des fehlerhaften Switch.
   c. Die Passwörter für den Administratorzugriff.

Erstellen Sie die Konfigurationsdatei

Sie können einen Switch mit den von Ihnen erstellten Konfigurationsdateien konfigurieren. Wählen Sie eine der folgenden Optionen, um die Konfigurationsdatei für den Switch zu erstellen.

Option	Schritte

Erstellen Sie die Sicherungskonfigurationsdatei über den fehlerhaften Switch	1. Stellen Sie eine Remote-Verbindung mit Ihrem Switch über SSH her, wie im folgenden Beispiel gezeigt:
	`ssh admin@<switch_IP_address`
	2. Geben Sie den Konfigurationsmodus ein, wie im folgenden Beispiel gezeigt:
	`switch > enable`
	`switch # configure terminal`
	3. Suchen Sie die verfügbaren Konfigurationsdateien wie im folgenden Beispiel gezeigt:
	`switch (config) #`
	`switch (config) # show configuration files`
	4. Speichern Sie die aktive BIN-Konfigurationsdatei auf einem externen Server:
	`switch (config) # configuration upload my-filename scp://myusername@my-server/path/to/my/<file>`

Option	Schritte

Erstellen Sie die Sicherungskonfigurationsdatei, indem Sie die Datei von einem anderen Switch aus ändern	1. Stellen Sie eine Remote-Verbindung mit Ihrem Switch über SSH her, wie im folgenden Beispiel gezeigt:
	`ssh admin@<switch_IP_address`
	2. Geben Sie den Konfigurationsmodus ein, wie im folgenden Beispiel gezeigt:
	`switch > enable`
	`switch # configure terminal`
	3. Laden Sie eine textbasierte Konfigurationsdatei vom Switch auf einen externen Server hoch, wie im folgenden Beispiel dargestellt:
	`switch (config) #`
	`switch (config) # configuration text file my-filename upload scp://root@my-server/root/tmp/my-filename`
	4. Ändern Sie die folgenden Felder in der Textdatei auf den fehlerhaften Switch:
	`## Network interface configuration`
	`##`
	`no interface mgmt0 dhcp`
	`interface mgmt0 ip address XX.XXX.XX.XXX /22`
	`##`
	`## Other IP configuration`
	`##`
	`hostname oldhostname`

Entfernen Sie den defekten Schalter, und setzen Sie den Austausch ein

Führen Sie die Schritte aus, um den fehlerhaften Schalter zu entfernen und den Austausch zu installieren.

Schritte

1. Suchen Sie die Stromkabel am defekten Schalter.
2. Nachdem der Switch neu gestartet wurde, kennzeichnen und trennen Sie die Netzkabel.
3. Kennzeichnen und ziehen Sie alle Kabel vom defekten Schalter ab, und sichern Sie sie, um Schäden beim Austausch des Switches zu vermeiden.
4. Entfernen Sie den Schalter aus dem Rack.
5. Setzen Sie den Ersatzschalter in das Rack ein.
6. Schließen Sie die Stromkabel und Management-Port-Kabel an.

> Der Schalter schaltet sich automatisch ein, wenn die Wechselstromversorgung aktiviert wird. Es gibt keinen Netzschalter. Es kann bis zu fünf Minuten dauern, bis die Systemstatus-LED grün leuchtet.

7. Schließen Sie den Switch über den RJ-45-Managementport oder die serielle Terminal-Schnittstelle an.

Überprüfen Sie die Betriebssystemversion auf dem Switch

Überprüfen Sie die Version der Betriebssystemsoftware auf dem Switch. Die Version auf dem fehlerhaften Schalter und der gesunde Schalter sollten übereinstimmen.

Schritte

1. Stellen Sie über SSH eine Remote-Verbindung zum Switch her.
2. Wechseln Sie in den Konfigurationsmodus.
3. Führen Sie den `show version` Befehl aus. Das folgende Beispiel zeigt:

```
SFPS-HCI-SW02-A (config) #show version
Product name:      Onyx
Product release:   3.7.1134
Build ID:          #1-dev
Build date:        2019-01-24 13:38:57
Target arch:       x86_64
Target hw:         x86_64
Built by:          jenkins@e4f385ab3f49
Version summary:   X86_64 3.7.1134 2019-01-24 13:38:57 x86_64

Product model:     x86onie
Host ID:           506B4B3238F8
System serial num: MT1812X24570
System UUID:       27fe4e7a-3277-11e8-8000-506b4b891c00

Uptime:            307d 3h 6m 33.344s
CPU load averages: 2.40 / 2.27 / 2.21
Number of CPUs:    4
System memory:     3525 MB used / 3840 MB free / 7365 MB total
Swap:              0 MB used / 0 MB free / 0 MB total
```

4. Wenn die Versionen nicht übereinstimmen, sollten Sie das Betriebssystem aktualisieren. Weitere Informationen finden Sie im"Mellanox Software-Upgrade-Leitfaden".

Konfigurieren Sie den Ersatzschalter

Führen Sie die Schritte zur Konfiguration des Ersatzschalters durch. Weitere Informationen finden Sie unter "Mellanox-Konfigurationsmanagement" .

Schritte

1. Wählen Sie eine der Optionen aus, die für Sie gilt:

Option	Schritte

Aus DER BIN-Konfigurationsdatei	1. Holen Sie sich die BIN-Konfigurationsdatei, wie im folgenden Beispiel gezeigt:
	`switch (config) # configuration fetch scp://myusername@my-server/path/to/my/<file>`
	2. Laden Sie die BIN-Konfigurationsdatei, die Sie im vorherigen Schritt abgerufen haben, wie im folgenden Beispiel gezeigt:
	`switch (config) # configuration switch-to my-filename`
	3. Geben Sie ein, `yes` um den Neustart zu bestätigen.

Option	Schritte

Aus der Textdatei	1. Zurücksetzen des Schalters auf die Werkseinstellungen:
	`switch (config) # reset factory keep-basic`
	2. Anwenden der textbasierten Konfigurationsdatei:
	`switch (config) # configuration text file my-filename apply`
	3. Laden Sie eine textbasierte Konfigurationsdatei vom Switch auf einen externen Server hoch, wie im folgenden Beispiel dargestellt:
	`switch (config) #`
	`switch (config) # configuration text file my-filename upload scp://root@my-server/root/tmp/my-filename`
	Ein Neustart ist nicht erforderlich, wenn Sie die Textdatei anwenden.

Führen Sie den Austausch durch

Führen Sie die Schritte durch, um den Ersatzvorgang abzuschließen.

Schritte

1. Führen Sie die Kabel mithilfe der Etiketten in die Kabelführung ein.
2. Mit NetApp Config Advisor. Rufen Sie die Kurzanleitung von auf"Hier (Anmeldung erforderlich)".
3. Überprüfen Sie Ihre Storage-Umgebung.
4. Stellen Sie den fehlerhaften Switch an NetApp zurück.

Weitere Informationen

- "Ressourcen-Seite zu NetApp HCI"
- "SolidFire und Element Software Documentation Center"

Storage-Node wird in einem 2-Node-Cluster ersetzt

Bevor Sie einen Storage-Node ersetzen, der Teil eines Clusters mit zwei Nodes ist, sollten Sie zunächst einen dritten Storage-Node (der einen neuen Satz an IP-Adressen erfordert) hinzufügen, eine Synchronisierung durchführen und dann den fehlerhaften Node entfernen. Das Cluster bleibt im Status „beeinträchtigt“, bis ein Ersatz-Node dem Cluster hinzugefügt wird.

Was Sie benötigen

- Sie verfügen über neue Management-IP- und Storage-IP-Adressen.
- Sie haben überprüft, ob im Cluster die Meldung angezeigt `ClusterCannotSync` wird, nachdem der Node offline geschaltet wurde. So wird sichergestellt, dass sich das Cluster vollständig neu synchronisiert, wenn der neue Node wieder zum Cluster hinzugefügt wird. Diese Meldung wird ungefähr sechs Minuten nach dem Offline-Modus des Storage-Node angezeigt.
- Sie haben den NetApp Support kontaktiert. Wenn Sie einen Ersatz bestellen, sollten Sie beim NetApp Support einen Case eröffnen.
- Sie haben den Ersatzknoten erhalten.
- Sie haben ein elektrostatisches Entladungsband (ESD) oder einen anderen antistatischen Schutz.

Über diese Aufgabe

Alarme im VMware vSphere Web Client warnen Sie bei einem Host-Ausfall. Sie müssen die Seriennummer des ausgefallenen Hosts vom VMware vSphere Web Client mit der Seriennummer auf dem Aufkleber auf der Rückseite des Node übereinstimmen.

Schritte

1. Entfernen Sie den fehlerhaften Node physisch aus dem Rack. Die Schritte hängen vom Typ des verwendeten Storage-Node ab. Siehe "H410S Nodes ersetzen" und "H610S Nodes ersetzen".

   Entfernen Sie jetzt nicht den Node aus dem Cluster.

2. Installieren Sie den Ersatzknoten in demselben Steckplatz.
3. Verkabeln Sie den Node.
4. Schalten Sie den Node ein.
5. Schließen Sie eine Tastatur und einen Monitor an den Knoten an.
6. Durchführen der Konfigurationsschritte:
   a. Konfigurieren Sie die IPMI/BMC-IP-Adresse.
   b. Konfigurieren Sie den neuen Node mit der neuen Management-IP- und Storage-IP-Adresse sowie dem Cluster-Namen.
7. Nachdem der Node zum Cluster hinzugefügt wurde, fügen Sie die Laufwerke hinzu.
8. Entfernen Sie nach Abschluss der Synchronisierung die ausgefallenen Laufwerke und den ausgefallenen Node aus dem Cluster.
9. Verwenden Sie NetApp Hybrid Cloud Control, um den neuen, hinzugefügten Storage-Node zu konfigurieren. Siehe "Erweitern Sie NetApp HCI Storage-Ressourcen".

Weitere Informationen

- "NetApp HCI Documentation Center"
- "SolidFire und Element Software Documentation Center"

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- "Hinweis zum Compute-Firmware-Bundle 2.146"
- "Hinweis zum Speicher-Firmware-Paket 2.146"
- "Hinweis zum Speicher-Firmware-Paket 2.99.2"
- "Hinweis zum Compute-Firmware-Bundle 2.76"
- "Hinweis zum Speicher-Firmware-Paket 2.76"
- "Hinweis zum Compute Firmware Bundle 2.27"
- "Hinweis zum Speicher-Firmware-Paket 2.27"
- "Hinweis zur ISO für die Rechner-Firmware"
- "Hinweis für H610S BMC"
- "Hinweis zu Managementservices 2.23.64 (NetApp Element-Plug-in für VMware vCenter Server 5.1.12)"
- "Hinweis zu Management Services 2.22.7 (NetApp Element-Plug-in für VMware vCenter Server 5.0.37)"
- "Hinweis zu Managementservices 2.21.61 (NetApp Element-Plug-in für vCenter Server 4.10.12)"
- "Hinweis zu Managementservices 2.20.69 (NetApp Element-Plug-in für vCenter Server 4.9.14)"

- "Hinweis zu Managementservices 2.19.48 (NetApp Element-Plug-in für vCenter Server 4.8.34)"
- "Hinweis zu Managementservices 2.18.91 (NetApp Element-Plug-in für vCenter Server 4.7.10)"
- "Hinweis zu Managementservices 2.17.56 (NetApp Element-Plug-in für vCenter Server 4.6.32)"
- "Hinweis für Managementservices 2.17 (NetApp Element-Plug-in für vCenter Server 4.6.29)"
- "Hinweis zu Managementservices 2.16 (NetApp Element-Plug-in für vCenter Server 4.6.29)"
- "Hinweis zu Managementservices 2.14 (NetApp Element-Plug-in für vCenter Server 4.5.42)"
- "Hinweis zu Managementservices 2.13 (NetApp Element-Plug-in für vCenter Server 4.5.42)"
- "Hinweis zu Managementservices 2.11 (NetApp Element-Plug-in für vCenter Server 4.4.72)"
- "Hinweis für NetApp HCI 1.8"