Verfahren für System-Upgrades

HCI

NetApp
December 22, 2023

Inhalt

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-Funktionen für NetApp HCI 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.

> - Management Services 2.22.7 enthält Element Plug-in für vCenter Server 5.0, das das Remote-Plug-in enthält. Wenn Sie das Element-Plug-in verwenden, sollten Sie ein Upgrade auf die Managementservices 2.22.7 oder höher durchführen, um die VMware-Direktive zu erfüllen, die die Unterstützung für lokale Plug-ins überflüssig macht. "Weitere Informationen .".
> - Die neuesten Versionshinweise für Management-Services zu wichtigen Services, neuen Funktionen, Bug Fixes und Behelfslösungen für jedes Service Bundle 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.

Bevor Sie beginnen

- 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 Ihre Managementservices auf mindestens Version 2.1.326 aktualisiert. 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.
5. Befolgen Sie die Anweisungen auf der Seite, um ein Upgrade-Paket für Verwaltungsdienste auf Ihrem Computer herunterzuladen und zu speichern.
6. 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.

Bevor Sie beginnen

- 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 Ihre Managementservices auf mindestens Version 2.1.326 aktualisiert. 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 Managementknoten: `https://<ManagementNodeIP>/mnode`
2. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als ein `mnode-client` Wenn der Wert nicht bereits ausgefüllt ist.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Laden Sie das Service-Bundle mit diesem Befehl auf den Management-Node hoch und extrahieren Sie es. `PUT /services/upload`
4. Implementieren der Managementservices auf dem Management-Node: `PUT /services/deploy`
5. Überwachen Sie den Status der Aktualisierung: `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 ein Element Storage-Upgrade von 11.1 oder früher beginnen, sollten Sie ein Upgrade Ihrer HealthTools Suite durchführen. 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 für nicht erforderlich "Durchführen von Element-Upgrades mit NetApp Hybrid Cloud Control".

> Bei Element Software 12.3.2 handelt es sich um die endgültige Version, die auf NetApp HealthTools aktualisiert werden kann. Falls Sie Element Software 11.3 oder höher verwenden, sollten Sie zum Upgrade der Element Software NetApp Hybrid Cloud Control verwenden. Bei Element Versionen 11.1 oder einer älteren Version können Sie mithilfe von NetApp HealthTools ein Upgrade durchführen.

Was Sie benötigen

- Sie führen Management Node 11.0, 11.1 oder höher aus.
- Sie haben Ihre Managementservices auf mindestens Version 2.1.326 aktualisiert.

  Upgrades von NetApp Hybrid Cloud Control sind in früheren Servicepaket-Versionen nicht verfügbar.

- Sie haben die neueste Version von heruntergeladen "HealthTools" Und kopierte die Installationsdatei auf den Management-Node.

  > Sie können die lokal installierte Version von HealthTools überprüfen, indem Sie die ausführen `sfupdate-healthtools -v` Befehl.

- Um HealthTools mit dunklen Seiten zu verwenden, müssen Sie die folgenden zusätzlichen Schritte ausführen:
  - Laden Sie A herunter "JSON-Datei" Von der NetApp Support Site auf einem Computer, der nicht der Management-Node ist, und benennen Sie ihn in um `metadata.json`.
  - Lassen Sie den Management-Node am dunklen Standort laufen.

Über diese Aufgabe

Für die Befehle in der HealthTools Suite sind eskalierte Berechtigungen erforderlich. Beide Vorwort-Befehle mit `sudo` Oder eskalieren Sie Ihren Benutzer an Root-Rechte.

> Die von Ihnen verwendete HealthTools-Version ist möglicherweise aktueller als die unten angegebene Beispieleingabe und -Antwort.

Schritte

1. Führen Sie die aus `sfupdate-healthtools <path to install file>` Befehl zum Installieren der neuen HealthTools-Software.

   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 die aus `sfupdate-healthtools -v` Befehl, 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 aus  Für den Cluster möchten Sie die Upgrade-Bereitschaft überprüfen.
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. Siehe Upgrade des Storage-Node "Anweisungen" Fortfahren.

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 als ein `mnode-client` Wenn der Wert nicht bereits ausgefüllt ist.

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

      iv. Schließen Sie das Autorisierungsfenster.

   c. Wählen Sie in DER REST API-UI aus `GET /assets`.

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

   e. Wählen Sie **Ausführen**.

   f. Kopieren Sie von der Antwort die `"id"` Von `"storage"` Abschnitt des Clusters, den Sie auf die Upgrade-Bereitschaft überprüfen möchten.

   > Verwenden Sie das nicht `"parent"` Der Wert in diesem Abschnitt, 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 als ein `mnode-client` Wenn der Wert nicht bereits 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 Status als 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` Das ist Teil der Antwort.

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 der `message` „Return“ gibt an, dass im Hinblick auf den Cluster-Systemzustand Probleme aufgetreten sind. Führen Sie folgende 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 überprüfen, ob das Storage-Cluster mit der bereit für ein Upgrade ist `sfupgradecheck` Befehl. Mit diesem Befehl werden Informationen, z. B. ausstehende Nodes, Speicherplatz- und Cluster-Fehler, überprüft.

Wenn sich der Management-Node an einem dunklen Standort ohne externe Konnektivität befindet, muss die Upgrade-Readiness-Prüfung das `metadata.json` Datei, die Sie während heruntergeladen haben "HealthTools-Upgrades" Erfolgreich ausgeführt.

Über diese Aufgabe

In diesem Verfahren wird beschrieben, wie Sie Upgrade-Checks durchführen, die zu einem der folgenden Ergebnisse führen:

- Ausführen des `sfupgradecheck` Der Befehl wird erfolgreich ausgeführt. Das Cluster ist bereit für ein Upgrade.

- Überprüfungen innerhalb des `sfupgradecheck` Werkzeug schlägt 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 die aus `sfupgradecheck` Befehl:

```
sfupgradecheck -u <cluster-user-name> MVIP
```

> Fügen Sie bei Passwörtern, die Sonderzeichen enthalten, einen umgekehrten Schrägstrich hinzu (`\`) Vor jedem besonderen Charakter. Beispiel: `mypass!@1` Muss 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) in der Fehlermeldung aufgeführten Artikel.

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 A herunter "JSON-Datei" Von der NetApp Support Site auf einem Computer, der nicht der Management-Node ist, und benennen Sie ihn in um `metadata.json`.
3. Führen Sie den folgenden Befehl aus:

   ```
   sfupgradecheck -l --metadata=<path-to-metadata-json>
   ```

4. Weitere Informationen finden Sie unter Zusatz "HealthTools-Upgrades" Informationen für dunkle Seiten.
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 das `/var/log` Freier Speicherplatz entspricht einem prozentualen freien Schwellenwert. 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-Pfadinformationen für die Element-Version, auf die Sie aktualisieren, überprüft und bestätigt, dass der Upgrade-Pfad gültig ist.https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Software/What_is_the_upgrade_matrix_for_storage_clusters_running_NetApp_Element_software%3F["NetApp KB: Upgrade-Matrix für Storage Cluster mit NetApp Element Software"^]
- **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 Node muss in der Web-UI pro Node mit einem DNS-Nameserver konfiguriert sein (`https://[IP address]:442`) Ohne ungelöste Cluster Fehler im Zusammenhang mit Zeitverzerrung.
- **System-Ports**: Bei Upgrade-Nutzung von NetApp Hybrid Cloud Control haben Sie sichergestellt, dass die erforderlichen Ports geöffnet sind. Siehe "Netzwerkports" Finden Sie weitere Informationen.
- **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.

> Bevor Sie Ihre Element Software auf Version 12.3.x aktualisieren, müssen Sie ein Upgrade auf das neueste Management Services Bundle durchführen Wenn Sie Ihre Element-Software auf Version 12.3.x aktualisieren, benötigen Sie Managementdienste 2.14.60 oder höher, um fortfahren zu können.

- **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:

- Verwendung der 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 Node der H610S-Serie auf Element 12.3.x aktualisieren und auf dem Node eine Version von Element vor 11.8 ausgeführt wird, müssen Sie zusätzliche Aktualisierungsschritte (Phase 2) Für jeden Storage-Knoten. Wenn Sie Element 11.8 oder höher ausführen, sind die zusätzlichen Aktualisierungsschritte (Phase 2) nicht erforderlich.

Verwendung der 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.

Informationen zu potenziellen Problemen beim Upgrade von Storage-Clustern mit NetApp Hybrid Cloud Control und den zugehörigen Workarounds 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) in der 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 Aktualisierungsstatus 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 Upgrade-Vorgangs abgeschlossen ist, werden Sie in diesem Zustand aufgefordert, Phase 2 des Upgrades auszuführen (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. Gehen Sie zur NetApp HCI Software "download-Seite" Und laden Sie 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 ein `mnode-client`.
      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 die Paket-ID aus der Antwort, und speichern Sie sie (`"id"`) Für den Einsatz 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` Als `SUCCESS` Nach Abschluss.

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 ein `mnode-client`.

      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 als 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 aus der Antwort die Storage-Cluster-ID und speichern Sie sie (`"id"`) Des Clusters Sie beabsichtigen, für die Verwendung in einem späteren Schritt zu aktualisieren.

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 ein `mnode-client`.

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 Status als 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"`Das ist Teil der Antwort.

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 Cluster-Systemzustand aufgrund von korrigieren `failedHealthChecks` Nachricht im Antwortkörper.	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/{Upgradeld}** aus. iv. Wählen Sie **Probieren Sie es aus**. v. Geben Sie die Upgrade-ID des vorherigen Schritts in **Upgradeld** ein. vi. Eingabe `"action":"resume"` Im Anforderungsgremium. `{ "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/{Upgradeld}** auswählen. ii. Wählen Sie **Probieren Sie es aus**. iii. Geben Sie die Upgrade-ID des vorherigen Schritts in **Upgradeld** ein. iv. Eingabe `"action":"pause"` Im Anforderungsgremium. `{ "action": "pause" }` v. Wählen Sie **Ausführen**.

Option	Schritte
Wenn Sie ein H610S Cluster mit einer Elementversion vor 11.8 aktualisieren, wird der Status angezeigt `finishedNeedsAck` Im Reaktionskörper. Für jeden H610S Storage-Node müssen Sie zusätzliche Upgrade-Schritte (Phase 2) durchführen.	i. Siehe [Upgrading H610S storage nodes to Element 12.3.x 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. Eingabe `"action":"acknowledge"` Im Anforderungsgremium. `{ "action": "acknowledge" }` vi. Wählen Sie **Ausführen**.

f. Führen Sie die **GET /Upgrades/{upgradeId}** API nach Bedarf mehrmals aus, bis der Prozess abgeschlossen ist.

   Während des Upgrades, die `status` Zeigt an `running` Wenn keine Fehler aufgetreten sind. Wenn jeder Node aktualisiert wird, wird der `step` Wertänderungen an `NodeFinished`.

Das Upgrade wurde erfolgreich abgeschlossen, wenn der abgeschlossen wurde `percent` Wert ist `100` Und das `state` Zeigt an `finished`.

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 und rufen Sie die NetApp HCI Software auf "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 die Eingabe möglich ist `sfinstall` Um die Informationen aufzurufen. Fügen Sie bei Passwörtern, die Sonderzeichen enthalten, einen umgekehrten Schrägstrich hinzu (`\`) Vor jedem besonderen Charakter. Beispiel: `mypass!@1` Muss 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 das `sfinstall` Versucht zu überprüfen, ob eine neuere Version von `sfinstall` Ist verfügbar:

```
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 der Probedurchläufe wird die Meldung angezeigt `Storage Node Upgrade Staging Successful` Nach dem Upgrade-Ereignis.

```
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 `sfinstall` Befehl und der 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 das `sfinstall` Versucht zu überprüfen, ob eine neuere Version von `sfinstall` Ist verfügbar:

```
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 Node der H610S-Serie auf Element 12.3.x aktualisieren und auf dem Node eine Version von Element vor 11.8 ausgeführt wird, müssen Sie zusätzliche Aktualisierungsschritte (Phase 2) Für jeden Storage-Knoten. 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 verwenden, um die NetApp Element-Software an einem dunklen Standort zu aktualisieren, der keine externe Verbindung hat.

Was Sie benötigen

1. Wechseln 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. Hier herunterladen "JSON-Datei" Von der NetApp Support Site auf einem Computer, der nicht der Management-Node ist, und benennen Sie ihn in um `metadata.json`.
4. Kopieren Sie die ISO-Datei auf den Management-Node 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 die aus `sfupdate-healthtools` Befehl:

```
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 die aus `sfinstall` Befehl mit dem Pfad zur ISO-Datei und der JSON-Metadatendatei:

```
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 die hinzufügen `--stage` Fahne an den `sfinstall` Befehl zum Vorstellen des Upgrades im Voraus.

> Wenn Sie einen Node der H610S-Serie auf Element 12.3.x aktualisieren und auf dem Node eine Version von Element vor 11.8 ausgeführt wird, müssen Sie zusätzliche Aktualisierungsschritte (Phase 2) Für jeden Storage-Knoten. 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 unterbrechen Dadurch kann sich das System selbst reinigen.

Wenn `sfinstall` Wartet auf Behebung von Clusterfehlern und falls ein Ausfall dazu führt, dass die Störungen `sfinstall` Fahren Sie nicht mit dem nächsten Node fort.

Schritte

1. Sie sollten aufhören `sfinstall` Mit Strg+C.
2. Wenden Sie sich an den NetApp Support, um bei der Fehleranalyse zu helfen.
3. Setzen Sie das Upgrade mit dem gleichen fort `sfinstall` Befehl.
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.

Aktualisieren der H610S Storage-Nodes auf Element 12.3.x (Phase 2)

Wenn Sie einen Node der H610S Serie auf Element 12.3.x 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 die Standardaktualisierung auf Element 12.3.x Prozess. 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 beinhaltet die Schritte zum vollständigen Herunterfahren des Nodes und zum Trennen der Stromversorgung für jeden H610S-Node, der in einem erforderlich beschrieben ist "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.

Bevor Sie beginnen

- 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 das in dieser Phase 2-Upgrade-Verfahren "KB" Dies ist zum Abschluss eines Upgrades für jeden H610S Node erforderlich.

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 mithilfe der NetApp Hybrid Cloud Control UI und DER REST-API Firmware-reine Upgrades auf Ihren 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 Node muss in der Web-UI pro Node mit einem DNS-Nameserver konfiguriert sein (`https://[IP address]:442`) Ohne ungelöste Cluster Fehler im Zusammenhang mit Zeitverzerrung.
- **System-Ports**: Bei Upgrade-Nutzung von NetApp Hybrid Cloud Control haben Sie sichergestellt, dass die erforderlichen Ports geöffnet sind. Siehe "Netzwerkports" Finden Sie weitere Informationen.

- **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 "Versionshinweise Zum Speicher-Firmware-Bundle 2.27".

> Sie müssen ein Upgrade auf das neueste Management Services Bundle durchführen, bevor Sie die Firmware auf Ihren Storage-Nodes aktualisieren. Wenn Sie die Element Software auf Version 12.2 oder höher aktualisieren, benötigen Sie Managementdienste 2.14.60 oder höher, um fortfahren zu können.

> Wenden Sie sich an den NetApp Support, um die iDRAC/BIOS-Firmware zu aktualisieren. Weitere Informationen finden Sie unter "KB-Artikel".

- **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 der 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 Management-Node nicht mit dem Internet verbunden ist, haben Sie den Zugriff "Laden Sie das Storage-Firmware-Paket für NetApp HCI Storage-Cluster herunter".

> Informationen zu potenziellen Problemen beim Upgrade von Storage-Clustern mit NetApp Hybrid Cloud Control und den zugehörigen Workarounds finden Sie im "KB-Artikel".

> Das Upgrade dauert etwa 30 Minuten pro Storage-Node. Wenn Sie ein Element Storage Cluster auf eine Storage-Firmware vor Version 2.76 aktualisieren, werden einzelne Storage-Nodes während des Upgrades nur neu gebootet, wenn neue Firmware auf den Node geschrieben wurde.

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.

Upgrade-Status	Beschreibung
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.
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 für den Management-Node zugegriffen werden kann. Gehen Sie zu "Bundle-Seite für die Element Software Storage-Firmware" Und laden Sie das neueste Speicher-Firmware-Image 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 ein `mnode-client`.
      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 die Paket-ID aus der Antwort, und speichern Sie sie (`"id"`) Für den Einsatz 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` Als `SUCCESS` Nach Abschluss.
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 ein `mnode-client`.

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 als 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 aus der Antwort die Storage-Cluster-ID und speichern Sie sie (`"id"`) Des Clusters Sie beabsichtigen, für die Verwendung in einem späteren Schritt zu aktualisieren.

```
"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 ein `mnode-client`.

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 Status als 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"`Das ist Teil der Antwort.

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 Cluster-Systemzustand aufgrund von korrigieren `failedHealthChecks` Nachricht im Antwortkörper.	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/{Upgradeld}** aus. iv. Wählen Sie **Probieren Sie es aus**. v. Geben Sie die Upgrade-ID des vorherigen Schritts in **Upgradeld** ein. vi. Eingabe `"action":"resume"` Im Anforderungsgremium. `{ "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/{Upgradeld}** auswählen. ii. Wählen Sie **Probieren Sie es aus**. iii. Geben Sie die Upgrade-ID des vorherigen Schritts in **Upgradeld** ein. iv. Eingabe `"action":"pause"` Im Anforderungsgremium. `{ "action": "pause" }` v. Wählen Sie **Ausführen**.

f. Führen Sie die **GET /Upgrades/{upgradeld}** API nach Bedarf mehrmals aus, bis der Prozess abgeschlossen ist.

   Während des Upgrades, die `status` Zeigt an `running` Wenn keine Fehler aufgetreten sind. Wenn jeder Node aktualisiert wird, wird der `step` Wertänderungen an `NodeFinished`.

Das Upgrade wurde erfolgreich abgeschlossen, wenn der abgeschlossen wurde `percent` Wert ist `100`

Und das `state` Zeigt an `finished`.

Weitere Informationen

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

Upgrade eines Management-Node

Sie können Ihren Management-Node von Version 11.0 oder höher auf den Management-Node Version 12.3.x 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.

> 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:

> - Der Management-Node 12.3.2 enthält eine Verringerung der Sicherheit für Storage-Cluster bei aktivierter Virtual Volumes (VVols)-Funktion. Wenn sich Ihr Storage-Cluster bereits in Element 12.3 befindet und die VVols Funktion aktiviert ist, sollten Sie ein Upgrade auf 12.3 durchführen.
> - Im Management-Node 12.3 gibt es keine weiteren Funktionsänderungen oder Bug Fixes. Wenn Sie bereits Management-Node 12.3 ausführen, müssen Sie kein Upgrade auf 12.3 durchführen.

- Wenn Sie ein Upgrade von Management-Node 12.3 durchführen, gibt es keine weiteren Funktionsänderungen oder Bug Fixes im Management Node 12.3.1. Wenn Sie bereits Management-Node 12.3 ausführen, müssen Sie kein Upgrade auf 12.3 durchführen.

> Wenn Sie bei einem mit nde implementierten Management-Node 12.3 ein Upgrade ausführen, wird das Upgrade auf 12.3.x abgeschlossen. Beim Neustart kann es jedoch zu einem Fehler beim Upgrade kommen. Wenn dies geschieht, booten Sie den Management-Node neu, sodass 12.3.x korrekt angezeigt wird

- Wenn Sie ein Upgrade von Management-Node 12.2 durchführen:Aktualisieren eines Management-Node auf Version 12.3.x von 12.2
- Wenn Sie ein Upgrade von Management-Node 12.0 durchführen:Aktualisieren eines Management-Node auf Version 12.3.x von 12.0
- Wenn Sie ein Upgrade von Management-Node 11.3, 11.5, 11.7 oder 11.8 durchführen:Aktualisieren eines Management-Node auf Version 12.3.x von 11.3 bis 11.8

- Wenn Sie ein Upgrade von Management-Node 11.0 oder 11.1 durchführen:Aktualisieren eines Management-Node auf Version 12.3.x von 11.1 oder 11.0
- Wenn Sie ein Upgrade von einem Management-Node Version 10.x durchführen:Migration von Management-Node-Version 10.x zu 11.x

Wählen Sie die folgende Option, wenn Sie **sequenziell** aktualisiert haben (1) die Version der Managementservices und (2) Ihre Element Speicherversion haben 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 eines Management-Node auf Version 12.3.x von 12.2

Sie können ein Upgrade des Management-Node von Version 12.2 auf Version 12.3.x durchführen, ohne eine neue Management Node Virtual Machine bereitstellen zu müssen.

> Der Element 12.3.x-Management-Node ist ein optionales Upgrade. Bei bestehenden Implementierungen wird dieser Bedarf nicht benötigt.

Was Sie benötigen

- Der RAM der Management-Node-VM ist 24 GB.
- Der Management-Node, den Sie aktualisieren möchten, ist die Version 12.0 und verwendet IPv4-Netzwerke. Der Management-Node der Version 12.3.x 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 Ihren Managementknoten auf Version 12.3.x aktualisieren, benötigen Sie Managementdienste 2.14.60 oder höher, um fortzufahren.
- Sie haben (falls erforderlich) einen zusätzlichen Netzwerkadapter mit 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. Melden Sie sich bei der Virtual Machine des Management-Node über SSH oder Konsolenzugriff an.

2. Laden Sie die herunter "ISO für den Management-Node" Für NetApp HCI von der NetApp Support Site bis zur Management-Node Virtual Machine.

   > Der Name der ISO ist ähnlich wie `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. 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
   ```

4. 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
   ```

5. Wechseln Sie in das Home-Verzeichnis, und heben Sie die Bereitstellung der ISO-Datei von ab `/mnt`:

   ```
   sudo umount /mnt
   ```

6. 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
   ```

7. 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.

> Nachdem Sie den in diesem Schritt beschriebenen Sudo-Befehl ausgeführt haben, wird die SSH-Sitzung abgebrochen. Für kontinuierliches Monitoring ist ein Konsolenzugriff erforderlich. Wenn während des Upgrades kein Konsolenzugriff verfügbar ist, versuchen Sie die SSH-Anmeldung erneut, und überprüfen Sie die Verbindung nach 15 bis 30 Minuten. Nach der Anmeldung können Sie die neue Betriebssystemversion im SSH-Banner bestätigen, die angibt, dass das Upgrade erfolgreich war.

8. Führen Sie auf dem Management-Node den aus `redeploy-mnode` Skript zur Beibehaltung der Konfigurationseinstellungen für frühere Managementservices:

> 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 zuvor auf dem Management-Node deaktiviert hatten, müssen Sie dies ausführen "Deaktivieren Sie SSH erneut" Auf dem wiederhergestellten Management-Node. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist standardmäßig auf dem Management-Node aktiviert.

Aktualisieren eines Management-Node auf Version 12.3.x von 12.0

Sie können ein Upgrade des Management-Node von Version 12.0 auf Version 12.3.x durchführen, ohne eine neue Management Node Virtual Machine bereitstellen zu müssen.

> Der Element 12.3.x-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 der Version 12.3.x 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 Ihren Managementknoten auf Version 12.3.x aktualisieren, benötigen Sie Managementdienste 2.14.60 oder höher, um fortzufahren.
- Sie haben (falls erforderlich) einen zusätzlichen Netzwerkadapter mit 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 die herunter "ISO für den Management-Node" Für NetApp HCI von der NetApp Support Site bis zur Management-Node Virtual Machine.

   > 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 ab `/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, 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.

> Nachdem Sie den in diesem Schritt beschriebenen Sudo-Befehl ausgeführt haben, wird die SSH-Sitzung abgebrochen. Für kontinuierliches Monitoring ist ein Konsolenzugriff erforderlich. Wenn während des Upgrades kein Konsolenzugriff verfügbar ist, versuchen Sie die SSH-Anmeldung erneut, und überprüfen Sie die Verbindung nach 15 bis 30 Minuten. Nach der Anmeldung können Sie die neue Betriebssystemversion im SSH-Banner bestätigen, die angibt, dass das Upgrade erfolgreich war.

9. Führen Sie auf dem Management-Node den aus `redeploy-mnode` Skript zur Beibehaltung der Konfigurationseinstellungen für frühere Managementservices:

> 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>
```

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

Aktualisieren eines Management-Node auf Version 12.3.x von 11.3 bis 11.8

Sie können ein Upgrade des Management-Node von Version 11.3, 11.5, 11.7 oder 11.8 auf Version 12.3.x durchführen, ohne eine neue Management-Node-Virtual Machine bereitstellen zu müssen.

> Der Element 12.3.x-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 der Version 12.3.x 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 Ihren Managementknoten auf Version 12.3.x aktualisieren, benötigen Sie Managementdienste 2.14.60 oder höher, um fortzufahren.
- Sie haben (falls erforderlich) einen zusätzlichen Netzwerkadapter mit 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 die herunter "ISO für den Management-Node" Für NetApp HCI von der NetApp Support Site bis zur Management-Node Virtual Machine.

   > 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 ab `/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.

> Nachdem Sie den in diesem Schritt beschriebenen Sudo-Befehl ausgeführt haben, wird die SSH-Sitzung abgebrochen. Für kontinuierliches Monitoring ist ein Konsolenzugriff erforderlich. Wenn während des Upgrades kein Konsolenzugriff verfügbar ist, versuchen Sie die SSH-Anmeldung erneut, und überprüfen Sie die Verbindung nach 15 bis 30 Minuten. Nach der Anmeldung können Sie die neue Betriebssystemversion im SSH-Banner bestätigen, die angibt, dass das Upgrade erfolgreich war.

9. Führen Sie auf dem Management-Node den aus `redeploy-mnode` Skript zur Beibehaltung der Konfigurationseinstellungen für frühere Managementservices:

> 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>
```

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

Aktualisieren eines Management-Node auf Version 12.3.x von 11.1 oder 11.0

Sie können ein Upgrade des Management-Node von 11.0 oder 11.1 auf Version 12.3.x durchführen, ohne eine neue Management Node Virtual Machine 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 der Version 12.3.x 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 die herunter "ISO für den Management-Node" Für NetApp HCI von der NetApp Support Site bis zur Management-Node Virtual Machine.

   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.

> Nachdem Sie den in diesem Schritt beschriebenen Sudo-Befehl ausgeführt haben, wird die SSH-Sitzung abgebrochen. Für kontinuierliches Monitoring ist ein Konsolenzugriff erforderlich. Wenn während des Upgrades kein Konsolenzugriff verfügbar ist, versuchen Sie die SSH-Anmeldung erneut, und überprüfen Sie die Verbindung nach 15 bis 30 Minuten. Nach der Anmeldung können Sie die neue Betriebssystemversion im SSH-Banner bestätigen, die angibt, dass das Upgrade erfolgreich war.

9. Führen Sie auf dem 12.3.x-Management-Node den aus `upgrade-mnode` Skript zur Beibehaltung der früheren Konfigurationseinstellungen.

> 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. Bei mehreren Storage-Clustern, die von einem vorhandenen Management-Node 11.0 oder 11.1 ohne persistente Volumes gemanagt werden (der `-pvm` Das Flag soll eine der MVIP-Adressen des Clusters angeben):

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for
persistent volumes>
```

10. (Bei allen NetApp HCI-Installationen mit NetApp Element-Plug-in für vCenter Server) Aktualisieren Sie das vCenter-Plug-in auf dem 12.3.x-Management-Node, indem Sie die in aufgeführten Schritte ausführen "Aktualisieren Sie das Element Plug-in für vCenter Server" Thema:
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. Wechseln Sie zum Speicher-MVIP und melden Sie sich an. Durch diese Aktion 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 ein `mnode-client`.
        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 Text Code 200 Antwort den `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` Zur 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 ein `vCenter` Und vCenter Zugangsdaten.

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. Eingabe `ESXi Host` Als `type` Und fügen Sie das Hardware-Tag ein, das Sie während eines vorherigen Schritts für gespeichert haben `hardware_tag`.
    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-Node 11.0 oder 11.1 und den "Aktuelles HealthTools" Aktualisierung der Element Software von 10.3 + bis 11.x

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 Management-Node-IP-Adresse, Management-Node-Benutzer-ID an (der Benutzername ist `admin`), Passwort, das Sie auf der Registerkarte **QoSSIOC Service Management** des Registrierungsprogramms und vCenter Benutzer-ID und Passwort festgelegt haben.

    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. Über das Registrierungsprogramm für den Management-Node (`https://<mNode 11.1 IP address>:9443`), starten Sie den SIOC-Service 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** lautet, prüfen 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-Node. 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 kopieren `.ots.properties` Datei vom vorherigen Management-Node auf den Management-Node Version 11.1 `/sf/packages/nma/conf/.ots.properties` Datei und starten Sie den NMA-Dienst mit dem folgenden Befehl neu:

```
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. SSH in zum Management-Node der Version 11.1 und gehen Sie zu `/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. Verifizieren `sfcollector` Protokolle, um zu bestätigen, dass es funktioniert.
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.

Bevor Sie beginnen

- 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 als ein `mnode-client` Wenn der Wert nicht bereits 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

Bei bestehenden vSphere Umgebungen mit einem registrierten NetApp Element Plug-in für VMware vCenter Server können Sie Ihre Plug-in-Registrierung aktualisieren, nachdem Sie das Management-Services-Paket, das den Plug-in-Service enthält, 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.

> Management Services 2.22.7 enthält Element Plug-in für vCenter Server 5.0, das das Remote-Plug-in enthält. Wenn Sie das Element-Plug-in verwenden, sollten Sie ein Upgrade auf die Managementservices 2.22.7 oder höher durchführen, um die VMware-Direktive zu erfüllen, die die Unterstützung für lokale Plug-ins überflüssig macht. "Weitere Informationen .".

Element Plug-in für vCenter 5.0 und höher

Dieses Upgrade-Verfahren umfasst die folgenden Upgrade-Szenarien:

- Sie führen ein Upgrade auf Element Plug-in für vCenter Server 5.2, 5.1 oder 5.0 durch.
- Sie aktualisieren gerade auf einen 8.0 oder 7.0 HTML5 vSphere Web Client.

Das Element Plug-in für vCenter 5.0 oder höher ist nicht mit vCenter Server 6.7 und 6.5 kompatibel.

Wenn Sie von Element Plug-in für vCenter Server 4.x auf 5.x aktualisieren, gehen die bereits mit dem Plug-in konfigurierten Cluster verloren, da die Daten nicht von einer vCenter-Instanz in ein Remote-Plug-in kopiert werden können. Sie müssen die Cluster dem Remote-Plug-in erneut hinzufügen. Dies ist eine einmalige Aktivität beim Upgrade von einem lokalen Plug-in auf ein Remote-Plug-in.

Element Plug-in für vCenter 4.10 und früher

Dieses Upgrade-Verfahren umfasst die folgenden Upgrade-Szenarien:

- Sie aktualisieren gerade auf Element Plug-in für VMware 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 kompatibel mit VMware vCenter Server 8.0 für Element Plug-in für VMware vCenter Server 4.x
- 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

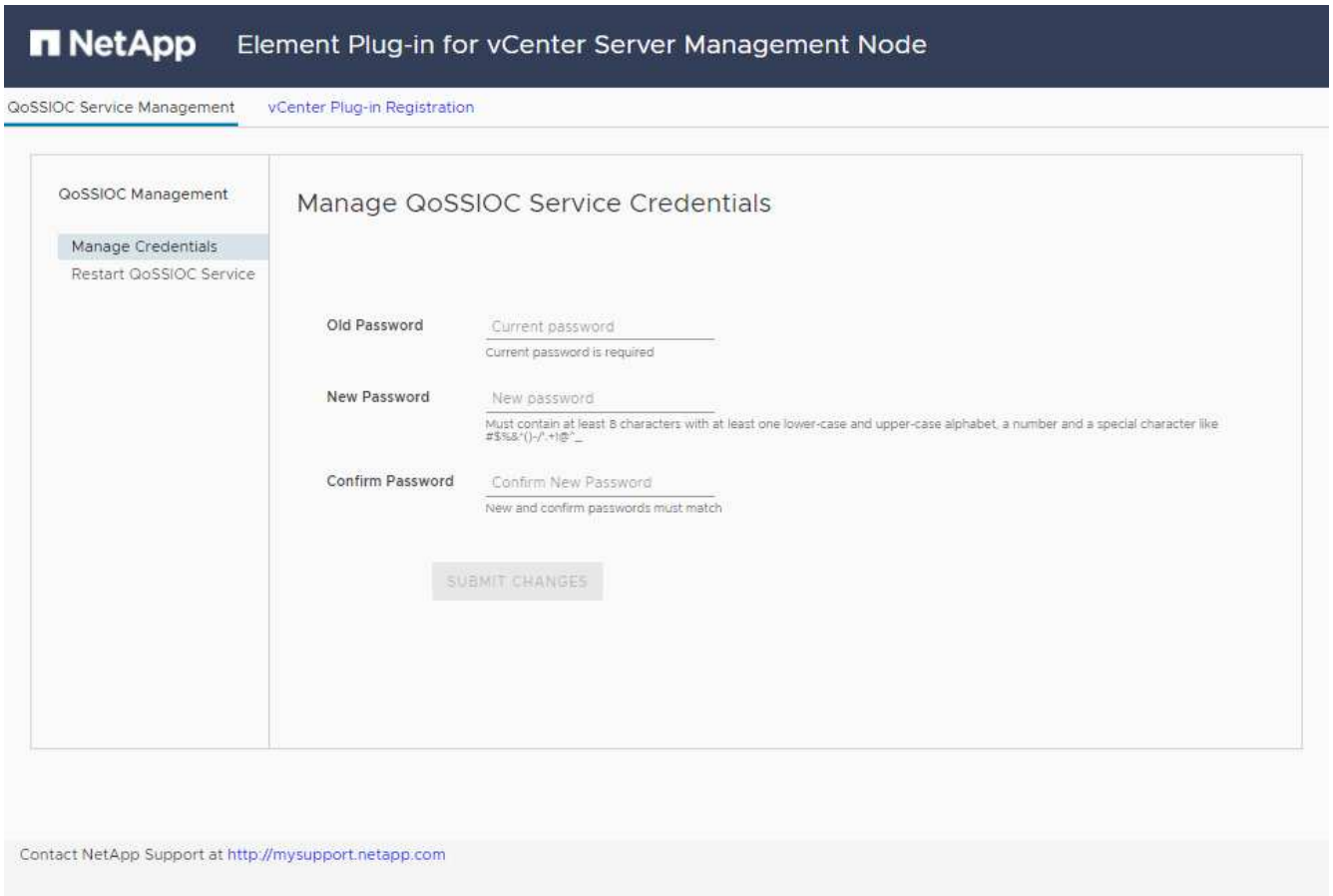
- **Admin-Berechtigungen**: Sie haben vCenter Administrator-Rollenberechtigungen, um ein Plug-in zu installieren.
- **VSphere Upgrades**: Sie haben alle erforderlichen vCenter Upgrades vor dem Upgrade des NetApp Element Plug-ins für vCenter Server durchgeführt. Bei diesem Verfahren wird vorausgesetzt, dass vCenter Upgrades bereits abgeschlossen wurden.
- **VCenter Server**: Ihr vCenter Plug-in Version 5.x oder 4.x ist mit einem vCenter Server registriert. Über das Registrierungsdienstprogramm (`https://[management node IP]:9443`Wählen Sie **Registrierungsstatus**, füllen Sie die erforderlichen Felder aus und wählen Sie **Prüfstatus** aus, um zu überprüfen, ob das vCenter Plug-in bereits registriert ist und die Versionsnummer der aktuellen Installation.
- **Management Services-Updates**: Sie haben Ihre aktualisiert "Management Services-Bundle" Zur aktuellen

Version wechseln. Updates für das vCenter Plug-in werden mithilfe von Updates für die Managementservices bereitgestellt, die außerhalb der größeren Produktversionen für NetApp HCI veröffentlicht werden.

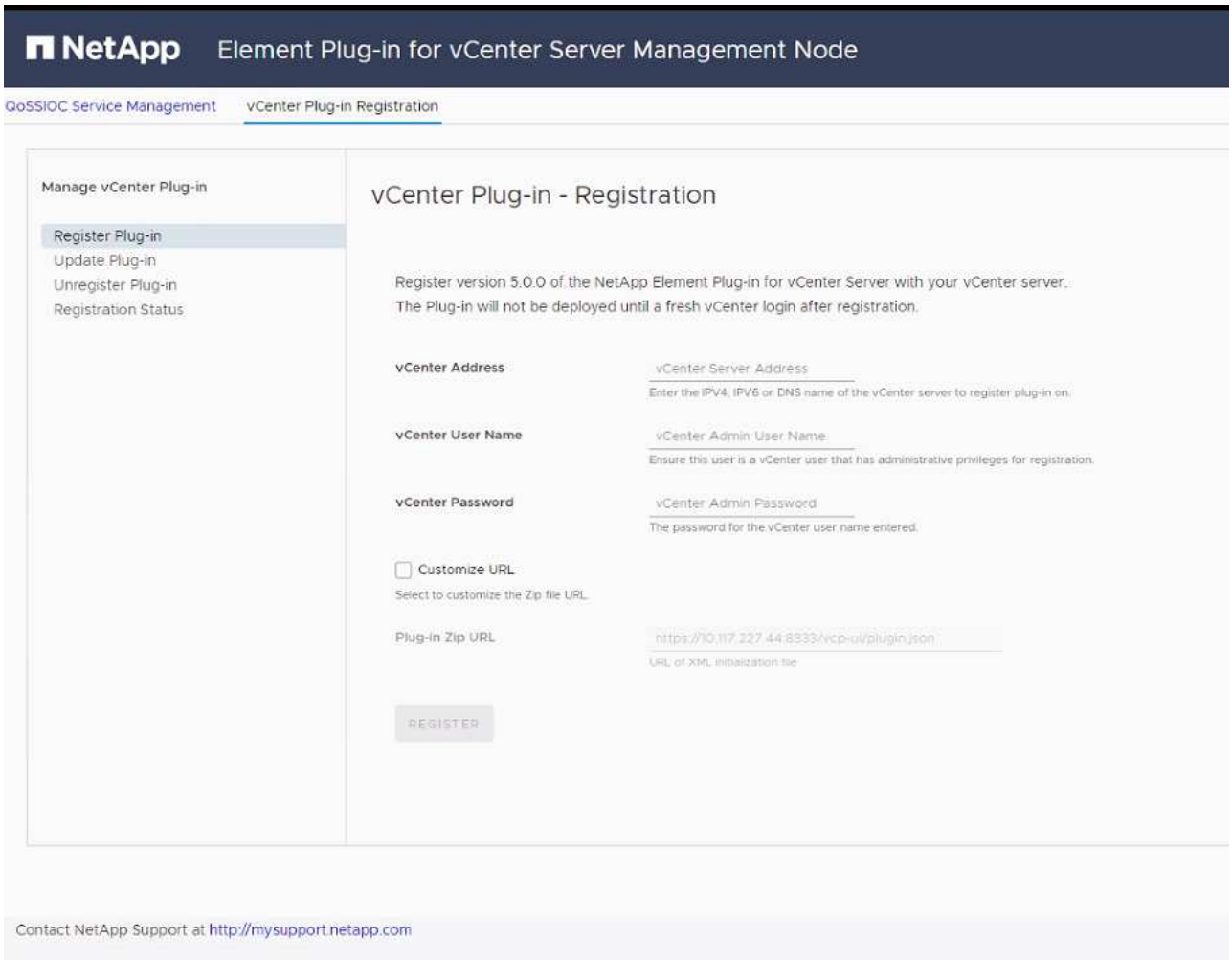
- **Management-Knoten-Upgrades**:
  - Ab dem Element vCenter Plug-in 5.0 führen Sie einen Management-Node aus, der schon einmal verwendet wurde "Upgrade durchgeführt" Auf Version 12.3.x oder höher.
  - Für Element vCenter Plug-in 4.4 bis 4.10 führen Sie einen Management-Node aus, der schon einmal verwendet wurde "Upgrade durchgeführt" Auf Version 11.3 oder höher. VCenter Plug-in 4.4 oder höher erfordert einen Management-Node mit mindestens 11.3 Versionen und einer modularen Architektur, die individuelle Services bietet. Der Management-Node muss mit seiner IP-Adresse oder der konfigurierten DHCP-Adresse eingeschaltet werden.
- * Element Storage-Upgrades*:
  - Ab dem Element vCenter Plug-in 5.0 verfügen Sie über einen Cluster, auf dem die NetApp Element Software 12.3.x oder höher ausgeführt wird.
  - Für Element vCenter Plug-in 4.10 oder eine frühere Version verfügen Sie über 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

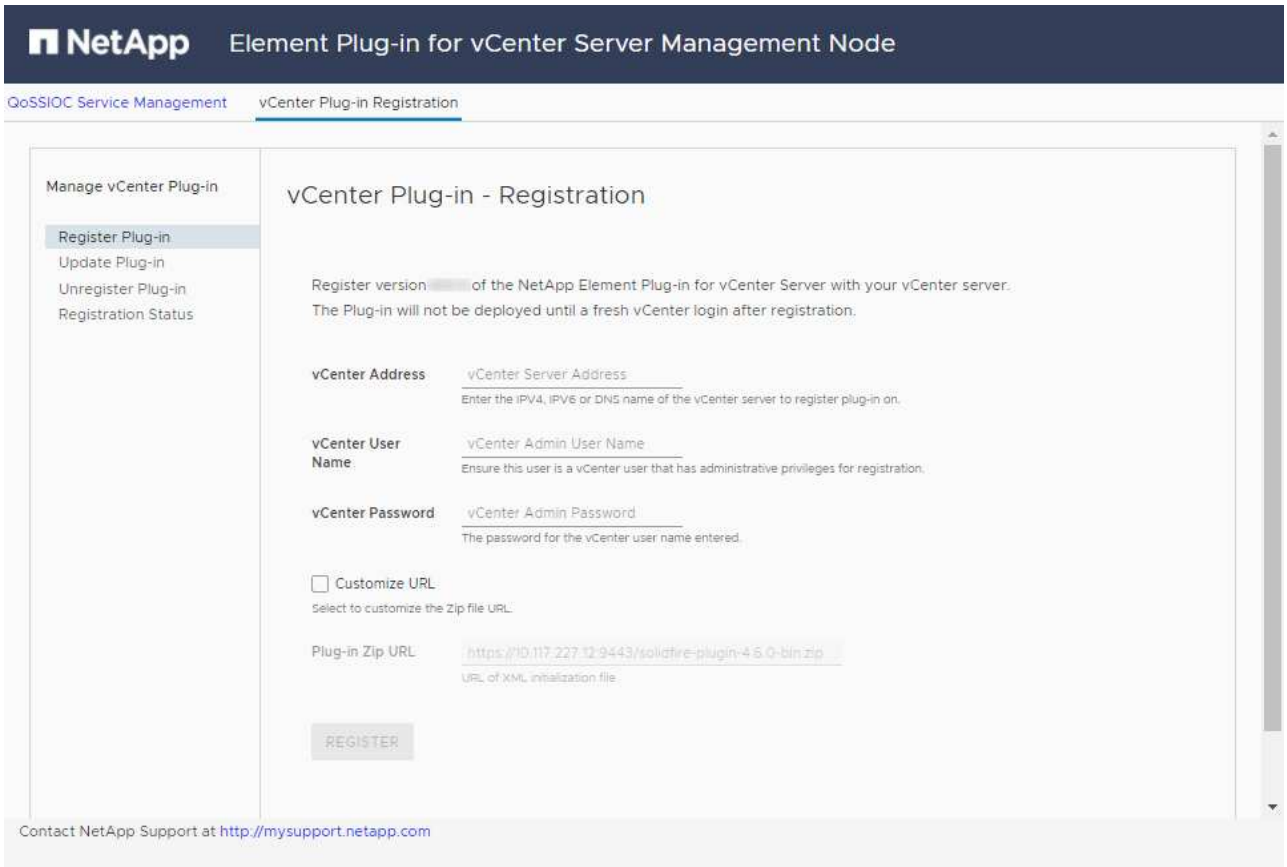
1. Geben Sie die IP-Adresse für den Management-Node in einem Browser ein, einschließlich des TCP-Ports für die Registrierung: `https://[management node IP]:9443`Die Registrierungs-Utility-Benutzeroberfläche wird auf der Seite * QoSSIOC Service Credentials* verwalten für das Plug-in geöffnet.



2. Wählen Sie **vCenter Plug-in Registrierung**.
   - Die vCenter Plug-in-Registrierungsseite für Element Plug-in für vCenter Server 5.x:



- Die Seite vCenter Plug-in-Registrierung für Element Plug-in für vCenter Server 4.10 oder früher:



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) je nach Element Plug-in für vCenter Version, eine benutzerdefinierte URL für die Plug-in-JSON-Datei oder Plug-in ZIP:
      i. Beginnend mit dem Element Plug-in für vCenter Server 5.0, einer benutzerdefinierten URL für die JSON-Plug-in-Datei.

         Sie können **Benutzerdefinierte URL** wählen, um die URL anzupassen, wenn Sie einen HTTP- oder HTTPS-Server (dunkle Site) verwenden oder den JSON-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).

      ii. Für Element Plug-in für vCenter Server 4.10 oder früher, 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).

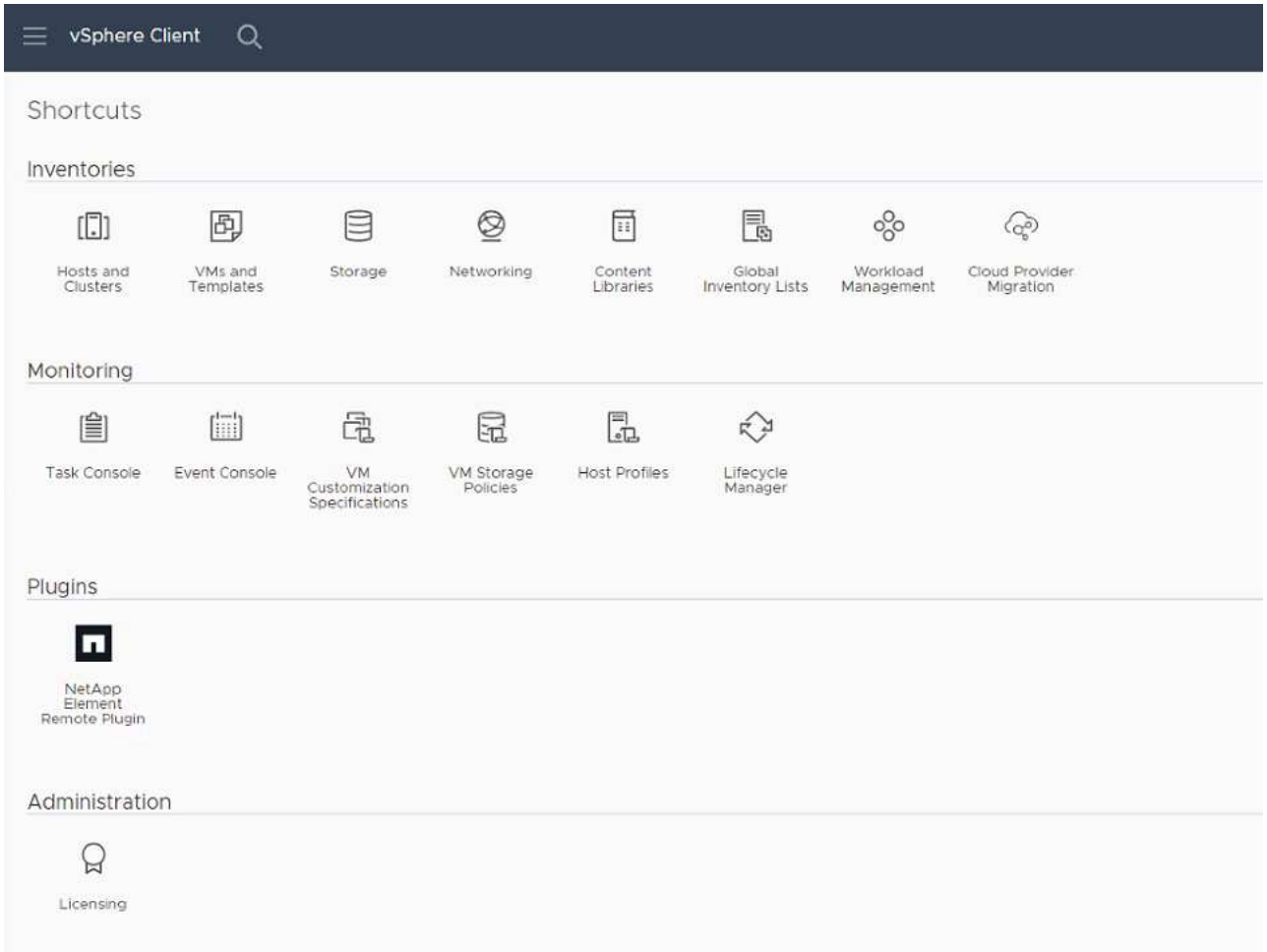
5. Wählen Sie **Aktualisieren**.

   Ein Banner erscheint in der Benutzeroberfläche des Registrierungsprogramms, wenn die Registrierung erfolgreich ist.

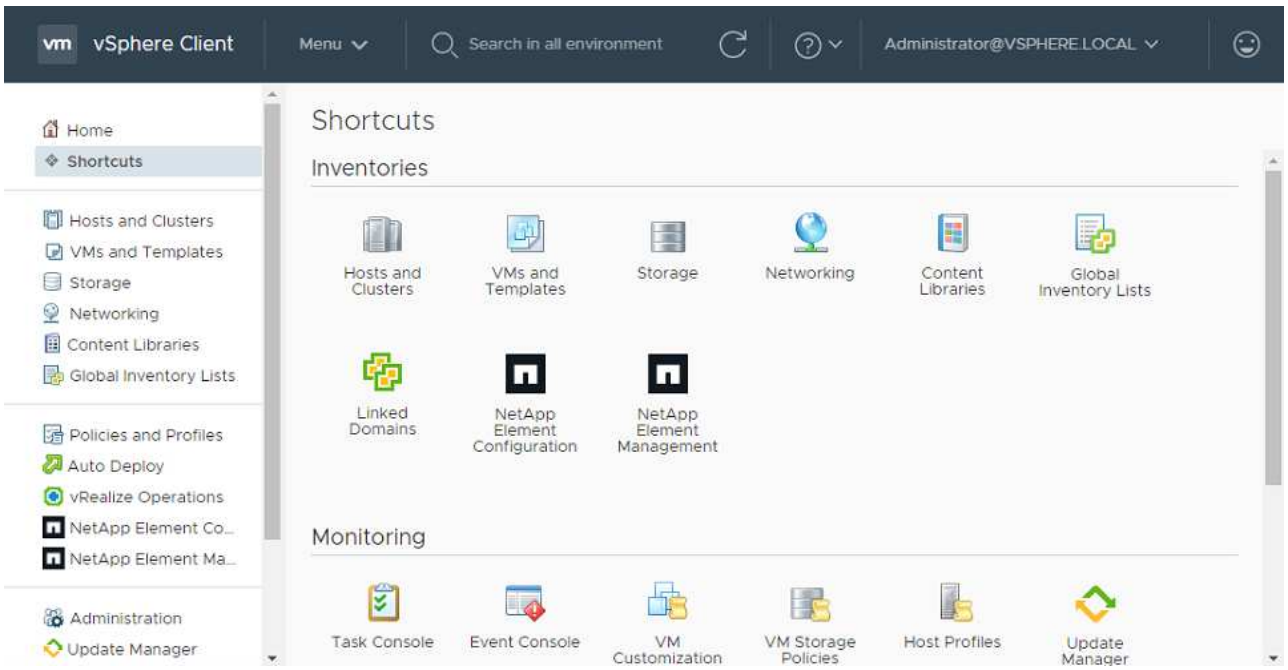
6. Melden Sie sich beim vSphere Web Client als vCenter Administrator an. Wenn Sie bereits beim vSphere Web Client angemeldet sind, müssen Sie sich zuerst abmelden, zwei bis drei Minuten warten und sich erneut anmelden.

   > 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 im Task Monitor, um sicherzustellen, dass die Installation abgeschlossen wurde: `Download plug-in` Und `Deploy plug-in`.
8. Überprüfen Sie, ob die Plug-in-Erweiterungspunkte auf der Registerkarte **Shortcuts** des vSphere Web Clients und im Seitenfenster angezeigt werden.
   - Ab dem Element Plug-in für vCenter Server 5.0 erscheint der NetApp Element Remote Plugin Extension Point:



- Bei Element Plug-in für vCenter Server 4.10 oder früher werden die Erweiterungspunkte für NetApp Element-Konfiguration und -Verwaltung angezeigt:



Wenn die vCenter-Plug-in-Symbole nicht angezeigt werden, lesen Sie "Element Plug-in für vCenter Server" Dokumentation zur Fehlerbehebung beim Plug-in.

Nach dem Upgrade auf 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, siehe "Element Plug-in für vCenter Server" Dokumentation über die Fehlerbehebung bei diesen Fehlern.

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: 5.2
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

Mit der Benutzeroberfläche von NetApp Hybrid Cloud Control oder der NetApp Hybrid Cloud Control API lassen sich Systemchecks durchführen:

- 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

Mithilfe von NetApp Hybrid Cloud Control kann sichergestellt werden, dass ein Computing-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 aus  Für den Cluster möchten Sie die Upgrade-Bereitschaft überprüfen.

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. Siehe "Aktualisiert die Computing-Node-Firmware" Fortfahren.

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 als ein `mnode-client` Wenn der Wert nicht bereits 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 Text Code 200 Antwort den `"id"` Für die Installation, die Sie für Zustandsprüfungen 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 als ein `mnode-client` Wenn der Wert nicht bereits 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 das ein `"controllerId"` Sie haben aus dem vorherigen Schritt im Parameterfeld **Controller_ID** kopiert.

f. Geben Sie in der Nutzlast das ein `"clusterId"` Die Sie aus dem vorherigen Schritt als kopiert haben `"cluster"` Wert und entfernen Sie den `"nodes"` Parameter.

```
{
  "cluster": "domain-1"
}
```

g. Wählen Sie **Ausführen**, um eine Integritätsprüfung auf dem Cluster auszuführen.

   Die Antwort auf Code 200 gibt ein `"resourceLink"` URL mit angehängter Task-ID, 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 Teil der Task-ID des `"resourceLink"` URL zur Überprüfung des Aufgabenergebnisses.

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 Teil der Task-ID des ein `"resourceLink"` URL aus der Antwort **POST /compute /{CONTROLLER_ID}/Health-Checks** Code 200 im `task_id` Parameterfeld.

   e. Wählen Sie **Ausführen**.

   f. Wenn der `status` Dieser Wert gibt an, dass im Hinblick auf den Zustand von Computing-Node Probleme aufgetreten sind. Führen Sie folgende Schritte aus:

      i. Gehen Sie zum jeweiligen KB-Artikel (`KbLink`) Für jedes Problem aufgelistet 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

Überprüfungen des Rechenstzustands, ob sie durch NetApp Hybrid Cloud Control oder API-Methoden durchgeführt werden, führen folgende Prüfungen pro Node durch. 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. Siehe "Diesen Artikel" Finden Sie weitere Informationen.
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. Siehe "Diesen Artikel" Finden Sie weitere Informationen.

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-Computing-Node können Sie die auf den Nodes verwendeten Treiber mithilfe des VMware Update Manager aktualisieren.

Was Sie benötigen

Informationen zur Hardware finden Sie in der Firmware- und Treibermatrix unter "Unterstützte Firmware- und ESXi-Treiberversionen".

Über diese Aufgabe

Führen Sie jeweils nur einen dieser Aktualisierungsvorgänge aus.

Sie sollten die aktuelle Version des ESXi-Treibers überprüfen, bevor Sie die Firmware-Aktualisierungen berechnen. Wenn der Treiber veraltet ist, aktualisieren Sie zuerst den Treiber. Dann aktualisieren Sie die Computing-Firmware für Ihre Computing-Nodes.

Schritte

1. Wechseln Sie zum "NetApp HCI Software-Downloads" Und wählen Sie den Download-Link für die korrekte 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. 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. Siehe "Interoperabilitäts-Matrix-Tool (IMT)" Informationen zur Kompatibilität von Treibern und Firmware erhalten Sie auf dem neuesten Stand "Versionshinweise zu der computing-Node-Firmware" Für wichtige, spätbreakende Firmware- und Treiberdetails.
- **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. Siehe "Netzwerkports" Finden Sie weitere Informationen.
- **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 BMC-Firmware mit der Version 4.68 aktualisieren "bundle für computing-Firmware 2.27" Und NetApp Hybrid Cloud Control zur Durchführung zukünftiger Firmware-Upgrades zu aktivieren.

> Eine vollständige Matrix der Firmware und der Treiber-Firmware für Ihre Hardware finden Sie unter "Unterstützte Firmware- und ESXi-Treiberversionen".

- **BIOS-Startreihenfolge**: Ändern Sie die Startreihenfolge im BIOS-Setup für jeden Knoten manuell `USB CD/DVD` Wird in der Boot-Liste angezeigt. Siehe das "Artikel" Finden Sie weitere Informationen.
- **BMC-Zugangsdaten**: Aktualisieren der Zugangsdaten NetApp Hybrid Cloud Control verwendet, um eine Verbindung zum BMC des Computing-Nodes herzustellen. Dazu wird entweder die NetApp Hybrid Cloud Control verwendet "UI" Oder "API". 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 Storage-Clustern mit zwei und drei Nodes, eines "Witness Node" Muss jederzeit 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. Siehe "So deaktivieren Sie den Sperrmodus auf ESXi-Host" Und "Verhalten des VMware Sperrmodus" Finden Sie weitere Informationen.

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.

> Überprüfen Sie vor dem Upgrade die aktuelle ESXi Treiberversion. Wenn der Treiber veraltet ist, aktualisieren Sie zuerst den Treiber. Dann aktualisieren Sie die Computing-Firmware für Ihre Computing-Nodes.

Upgrade-Optionen

Wählen Sie die Option aus, die für Ihr Upgrade-Szenario relevant ist:

- Verwenden Sie die UI von NetApp Hybrid Cloud Control zum Upgrade eines Computing-Node (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)

Verwenden Sie die UI von NetApp Hybrid Cloud Control zum Upgrade eines Computing-Node

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 ein Upgrade sollten Sie ein verwenden USB-Laufwerk Oder im BMC-UI So mounten Sie das Computing-Firmware-Bundle.

Was Sie benötigen

- Wenn der Management-Node nicht mit dem Internet verbunden ist, haben Sie das Paket der Computing-Firmware von heruntergeladen "NetApp Support Website".

  Sie sollten die extrahieren `TAR.GZ` Datei zu A `TAR` Datei, und extrahieren Sie dann die `TAR` Datei zum Paket der Compute-Firmware.

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 **Durchsuchen** aus, um das von Ihnen heruntergeladene Paket der Rechner-Firmware 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 Konsole „Serial-over-LAN“ (SOL) nicht über die BMC Web-UI, während Sie die Firmware auf den H610C und H615C Computing-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 Aktualisierungsstatus 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 über Probleme bei Upgrades der Computing-Node-Firmware mithilfe von NetApp Hybrid Cloud Control finden Sie hier "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.

Upgrade-Status	Beschreibung
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 ein Upgrade sollten Sie ein verwenden USB-Laufwerk Oder im BMC-UI So mounten Sie das Computing-Firmware-Bundle.

Was Sie benötigen

Computing-Node-Ressourcen, einschließlich vCenter und Hardware-Assets, müssen Management-Node-Ressourcen bekannt sein. Sie können die Inventurservice-APIs verwenden, um die Ressourcen zu überprüfen (`https://<ManagementNodeIP>/inventory/1/`).

Schritte

1. Wechseln Sie zur NetApp HCI-Software "Download-Seite" Laden Sie anschließend das neueste Computing-Firmware-Bundle auf ein Gerät herunter, auf das der Management-Node zugreifen kann.
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 ein `mnode-client`.
      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 Bundle-ID der Computing-Firmware und speichern Sie sie (`"id"`) Für den Einsatz 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` Als `SUCCESS` Nach Abschluss.

   e. Kopieren Sie in der Antwort den Namen des Computing-Firmware-Pakets und speichern Sie sie (`"name"`) Und Version (`"version"`) Für den Einsatz 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 ein `mnode-client`.
      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 als 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 aus der Antwort die Cluster-Controller-ID und speichern Sie sie (`"controllerId"`` Und Knoten Hardware-ID (`"hardwareId"`) Zur 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 ein `mnode-client`.
      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 (`"hardwareId"` Aus einem vorherigen Schritt) im Parameterfeld gespeichert.
   f. Führen Sie die Nutzlastwerte folgendermaßen aus:
      i. Die Werte beibehalten `"force": false` Und `"maintenanceMode": true"` So werden Zustandsprüfungen auf dem Node durchgeführt, und der ESXi Host ist auf den Wartungsmodus festgelegt.

ii. Geben Sie die Cluster-Controller-ID ein (`"controllerId"` Aus einem vorherigen Schritt gespeichert).

iii. Geben Sie den Namen und die Version des Computing-Firmware-Pakets ein, die Sie in 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 Ressourcenverknüpfung ist (`"resourceLink"`) URL in der Antwort.

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 Cluster-Systemzustand aufgrund von korrigieren `failedHealthChecks` Nachricht im Antwortkörper.	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.
Das Upgrade schlägt fehl und die Schritte zur Risikominderung werden im Upgrade-Protokoll nicht aufgeführt.	i. Siehe das "KB-Artikel" (anmeldung erforderlich).

f. Führen Sie die API **GET /Task/{Task_id}/logs** mehrmals nach Bedarf aus, bis der Prozess abgeschlossen ist.

   Während des Upgrades, die `status` Zeigt an `running` Wenn keine Fehler aufgetreten sind. Wenn jeder Schritt beendet ist, das `status` Wertänderungen an `completed`.

Das Upgrade wurde erfolgreich abgeschlossen, wenn der Status für jeden Schritt lautet `completed` Und das `percentageCompleted` Wert ist `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 ein `mnode-client`.
      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 (`"hardwareId"` Aus einem vorherigen Schritt) im Parameterfeld gespeichert.
   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 der Management-Node nicht mit dem Internet verbunden ist, haben Sie das Paket der Computing-Firmware von heruntergeladen "NetApp Support Website".

> Sie sollten die extrahieren `TAR.GZ` Datei zu A `TAR` Datei, und extrahieren Sie dann die `TAR` Datei zum Paket der Compute-Firmware.

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 durchführen, indem Sie ein Video/eine 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

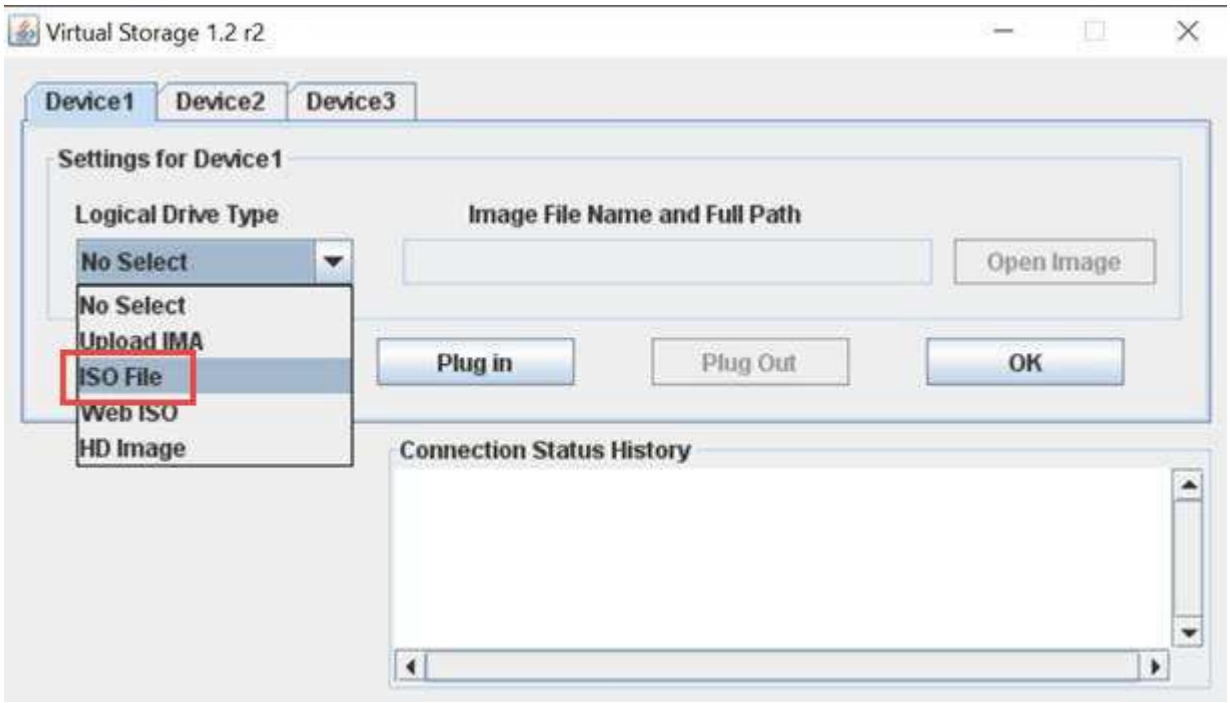
1. Wenn der Node Teil eines Clusters ist, versetzen Sie ihn wie folgt in den Wartungsmodus. Falls nicht, fahren Sie mit Schritt 2 fort.
   a. Melden Sie sich beim VMware vCenter Web-Client an.
   b. Klicken Sie mit der rechten Maustaste auf den Namen des Hosts (Compute Node) und wählen Sie **Wartungsmodus > 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**.

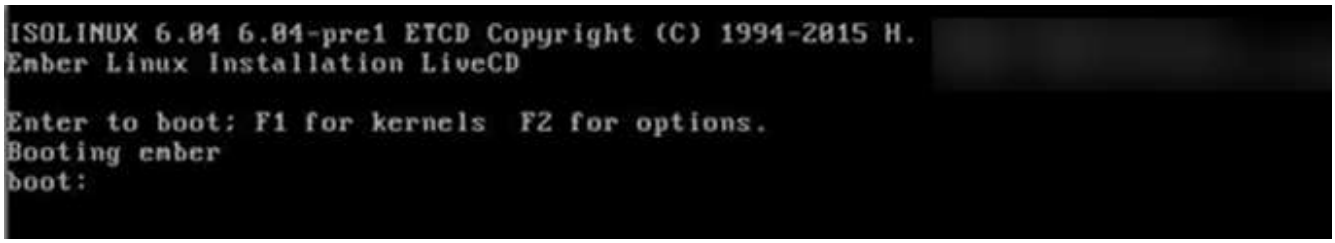
   Sie müssen vielleicht Java installieren oder aktualisieren.

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.

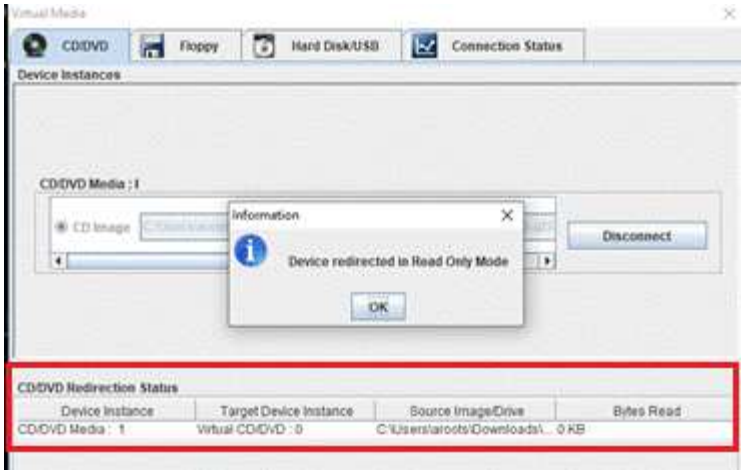
Schritte

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 **Durchsuchen** und wählen Sie die Rechner-Firmware aus `.iso` Datei:
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“"

Automatisieren Sie Upgrades der Computing-Node-Firmware mit Ansible

Sie können die System-Firmware auf NetApp HCI Compute-Nodes aktualisieren, einschließlich Firmware für Komponenten wie BMC, BIOS und NIC mithilfe von Workflows in NetApp Hybrid Cloud Control. Bei Installationen mit großen Computing-Clustern können die Workflows mithilfe von Ansible automatisiert werden, um ein Rolling Upgrade des gesamten Clusters durchzuführen.

NetApp bietet die Ansible-Rolle zur Automatisierung von Computing-Node-Firmware-Upgrades. Die Automatisierung ist eine zusätzliche Komponente, die zusätzliche Einrichtung und Softwarekomponenten erforderlich macht. Änderungen der Ansible Automatisierung werden nur in Verbindung mit Mühe unterstützt.

Die Ansible-Rolle für Upgrades kann nur auf Computing-Nodes der NetApp HCI H-Serie ausgeführt werden. Sie können diese Rolle nicht für ein Upgrade von Computing-Nodes von Drittanbietern verwenden.

Was Sie benötigen

- **Vorbereitung und Voraussetzungen für Firmware-Upgrades**: Ihre NetApp HCI-Installation muss für das Firmware-Upgrade bereit sein, wie in der Anleitung für beschrieben "Firmware-Upgrades werden durchgeführt".
- **Bereitschaft zur Durchführung der Automatisierung auf Ansible-Steuerungsknoten**: Ein physischer oder virtueller Server zur Ausführung der Firmware-Update-Automatisierung in Ansible.

Über diese Aufgabe

In einer Produktionsumgebung sollten Computing-Nodes in einem Cluster einzeln oder nacheinander in einer NetApp HCI Installation aktualisiert werden. APIs in NetApp Hybrid Cloud Control koordinieren den allgemeinen Upgrade der Computing-Node-Firmware für einen einzelnen Computing-Node. Dazu gehören auch Zustandsprüfungen, Wartungsaufgaben von ESXi auf den Computing-Nodes und Neustart des Computing-Node zur Anwendung der Firmware-Upgrades. Die Ansible-Rolle bietet die Möglichkeit, das Firmware-Upgrade für eine Gruppe von Computing-Nodes oder ganzen Clustern zu orchestrieren.

Starten Sie mit der Firmware-Upgrade-Automatisierung

Navigieren Sie zum, um zu beginnen "NetApp Ansible Repository auf GitHub" Und laden Sie die herunter `nar_compute_nodes_firmware_upgrades` Rolle und Dokumentation:

Weitere Informationen

- "Seite „NetApp HCI Ressourcen“"