



Verfahren für System-Upgrades

Element Software

NetApp
January 15, 2024

Inhalt

- Verfahren für System-Upgrades 1
 - Managementservices aktualisieren 1
 - Upgrade auf die neuesten HealthTools 4
 - Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen 5
 - Upgrade der Element Software 15
 - Firmware für Storage-Upgrades 31
 - Upgrade eines Management-Node 40
 - Aktualisieren Sie das Element Plug-in für vCenter Server 55

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 Managementfunktionen für ein SolidFire All-Flash-Storage-System. 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

- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

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 `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

- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

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 über die Benutzeroberfläche von NetApp Hybrid Cloud Control, die NetApp Hybrid Cloud Control API oder die 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

Mit NetApp Hybrid Cloud Control können Sie überprüfen, ob ein Storage-Cluster aktualisiert werden kann.

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
```

- 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-ccb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-896e-4751-ab7b-ccb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccb5f61f9fc",
  "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/{healthCheckId}** 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/{healthCheckId}/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 /{healthCheckId}/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 die `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/kallA00000081tOQAQ/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/kallA00000081tTQAQ/
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/kallA00000081tYQAQ/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 `sfupgradcheck` 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/ka11A00000081tTQAQ/SolidFire-Disk-space-error>

check_pending_nodes:

Test Description: Verify no pending nodes in cluster

More information:

<https://kb.netapp.com/support/s/article/ka11A00000081tOQAQ/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/ka11A00000081tTQAQ/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/ka11A00000081tYQAQ/mNodeconnectivity>

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

- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

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\[\"NetApp KB: Upgrade-Matrix für Storage Cluster mit NetApp Element Software\"\]](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[\)
- **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](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
<p>Alle Cluster laufen mit Element 11.8 und höher</p>	<p>a. Wählen Sie Durchsuchen, um das heruntergeladene Aktualisierungspaket hochzuladen.</p> <p>b. Warten Sie, bis der Upload abgeschlossen ist. In einer Statusleiste wird der Status des Uploads angezeigt.</p> <div data-bbox="922 443 976 499" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="1036 422 1430 520" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p>Der Datei-Upload geht verloren, wenn Sie vom Browser-Fenster wegnavigieren.</p> </div> <p>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.</p> <p>c. Wählen Sie Upgrade Starten.</p> <div data-bbox="922 1077 976 1134" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="1036 919 1430 1287" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p>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.</p> </div> <div data-bbox="922 1539 976 1596" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="1036 1350 1430 1791" style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p>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.</p> </div> <p>Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist.</p>

Option	Schritte
Sie aktualisieren ein H610S Cluster mit Element Version vor 11.8.	<p>a. Wählen Sie den Dropdown-Pfeil neben dem Cluster aus, das Sie aktualisieren möchten, und wählen Sie aus den verfügbaren Upgrade-Versionen aus.</p> <p>b. Wählen Sie Upgrade Starten. Nach Abschluss des Upgrades werden Sie von der Benutzeroberfläche aufgefordert, Phase 2 des Prozesses auszuführen.</p> <p>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.</p> <p>Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist. Informationen zu den verschiedenen Änderungen des Aktualisierungsstatus finden Sie unter Statusänderungen des Upgrades.</p>

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.

Wechseln Sie zur Element 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 ("upgradeld" Das ist Teil der Antwort.
6. Überprüfen Sie den Aktualisierungsfortschritt und die Ergebnisse:
- a. Wählen Sie **GET /Upgrades/{upgradeld}** aus.
 - b. Wählen Sie **Probieren Sie es aus**.
 - c. Geben Sie die Upgrade-ID des vorherigen Schritts in **Upgradeld** ein.
 - d. Wählen Sie **Ausführen**.
 - e. Führen Sie einen der folgenden Schritte aus, wenn während des Upgrades Probleme oder besondere Anforderungen auftreten:

Option	Schritte
<p>Sie müssen Probleme mit dem Cluster-Systemzustand aufgrund von korrigieren <code>failedHealthChecks</code> Nachricht im Antwortkörper.</p>	<ol style="list-style-type: none"> 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 <code>"action": "resume"</code> Im Anforderungsgremium. <div data-bbox="915 785 1487 963" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #f9f9f9; margin: 10px 0;"> <pre>{ "action": "resume" }</pre> </div> vii. Wählen Sie Ausführen.
<p>Sie müssen das Upgrade unterbrechen, da das Wartungsfenster geschlossen wird oder aus einem anderen Grund.</p>	<ol style="list-style-type: none"> 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 <code>"action": "pause"</code> Im Anforderungsgremium. <div data-bbox="915 1402 1487 1581" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #f9f9f9; margin: 10px 0;"> <pre>{ "action": "pause" }</pre> </div> v. Wählen Sie Ausführen.

Option	Schritte
<p>Wenn Sie ein H610S Cluster mit einer Elementversion vor 11.8 aktualisieren, wird der Status angezeigt <code>finishedNeedsAck</code> Im Reaktionskörper. Für jeden H610S Storage-Node müssen Sie zusätzliche Upgrade-Schritte (Phase 2) durchführen.</p>	<ol style="list-style-type: none"> i. Siehe Aktualisieren der H610S Storage-Nodes auf Element 12.3.x (Phase 2) Und schließen Sie den Prozess für jeden Node ab. ii. Bei Bedarf erneut authentifizieren und PUT /Upgrades/{Upgradeld} auswählen. iii. Wählen Sie Probieren Sie es aus. iv. Geben Sie die Upgrade-ID des vorherigen Schritts in Upgradeld ein. v. Eingabe <code>"action": "acknowledge"</code> Im Anforderungsgremium. <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>{ "action": "acknowledge" }</pre> </div> vi. 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`.

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 gehen Sie zu Element Software "[download-Seite](#)" Und laden Sie das neueste Storage-Node-Image auf ein Gerät herunter, das nicht auf den Management-Node abgeht.



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 Element 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 `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 `sfinstall` Befehl fort.
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

- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

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](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.

- **Cluster Health:** Sie haben Health Checks durchgeführt. Siehe ["Integritätsprüfungen von Element Storage vor einem Storage Upgrade durchführen"](#).
- **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**.
- **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 Storage-Firmware-Versionen für SolidFire Storage-Nodes"](#)

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 "[Das Storage-Firmware-Bundle heruntergeladen](#)".



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.

Wenn der Cluster aktuell ist und/oder keine Upgrade-Pakete verfügbar sind, werden die Registerkarten **Element** und **Firmware Only** nicht angezeigt. Diese Registerkarten werden auch nicht angezeigt, wenn ein Upgrade ausgeführt wird. Wenn die Registerkarte **Element** angezeigt wird, nicht jedoch die Registerkarte **Firmware only**, stehen keine Firmware-Pakete zur Verfügung.

5. Wählen Sie den Dropdown-Pfeil neben dem Cluster aus, das Sie aktualisieren möchten.
6. Wählen Sie **Durchsuchen**, um das heruntergeladene Aktualisierungspaket hochzuladen.
7. Warten Sie, bis der Upload abgeschlossen ist. In einer Statusleiste wird der Status des Uploads angezeigt.



Der Datei-Upload geht verloren, wenn Sie vom Browser-Fenster wegnavigieren.

Nach dem erfolgreichen Hochladen und Validierungen der Datei wird eine Meldung auf dem Bildschirm angezeigt. Die Validierung kann mehrere Minuten in Anspruch nehmen. Wenn Sie zu diesem Zeitpunkt vom Browser-Fenster weg navigieren, bleibt der Datei-Upload erhalten.

8. Wählen Sie **nur Firmware** aus, und wählen Sie aus den verfügbaren Upgrade-Versionen.

9. Wählen Sie **Upgrade Starten**.



Der **Upgrade-Status** ändert sich während des Upgrades, um den Status des Prozesses anzuzeigen. Es ändert sich auch in Reaktion auf Aktionen, die Sie ergreifen, z. B. die Unterbrechung des Upgrades oder wenn das Upgrade einen Fehler zurückgibt. Siehe [Statusänderungen des Upgrades](#).



Während das Upgrade läuft, können Sie die Seite verlassen und zu einem späteren Zeitpunkt zurückkehren, um den Fortschritt zu überwachen. Die Seite aktualisiert den Status und die aktuelle Version nicht dynamisch, wenn die Cluster-Zeile ausgeblendet ist. Die Cluster-Zeile muss erweitert werden, um die Tabelle zu aktualisieren, oder Sie können die Seite aktualisieren.

Sie können Protokolle herunterladen, nachdem die Aktualisierung abgeschlossen ist.

Statusänderungen des Upgrades

Hier sind die verschiedenen Status, in denen die Spalte **Upgrade Status** in der UI vor, während und nach dem Upgrade-Prozess angezeigt wird:

Upgrade-Status	Beschreibung
Auf dem aktuellen Stand	Das Cluster wurde auf die neueste verfügbare Element-Version aktualisiert oder die Firmware wurde auf die neueste Version aktualisiert.
Erkennung nicht möglich	Dieser Status wird angezeigt, wenn die Speicherdienst-API einen Upgrade-Status zurückgibt, der nicht in der aufgezählten Liste möglicher Upgrade-Status aufgeführt ist.
Verfügbare Versionen	Neuere Versionen von Element und/oder Storage Firmware stehen für ein Upgrade zur Verfügung.
In Bearbeitung	Das Upgrade läuft. In einer Statusleiste wird der Aktualisierungsstatus angezeigt. Auf dem Bildschirm werden zudem Fehler auf Node-Ebene angezeigt und die Node-ID jedes Node im Cluster wird angezeigt, wenn das Upgrade fortschreitet. Sie können den Status jedes Knotens über die Element-UI oder das NetApp Element Plug-in für vCenter Server UI überwachen.
Anhalten Des Upgrades	Sie können das Upgrade anhalten. Je nach Status des Upgrade-Prozesses kann der Pause-Vorgang erfolgreich oder fehlgeschlagen sein. Es wird eine UI-Eingabeaufforderung angezeigt, in der Sie aufgefordert werden, den Pause-Vorgang zu bestätigen. Um sicherzustellen, dass sich das Cluster vor dem Anhalten eines Upgrades an einem sicheren Ort befindet, kann es bis zu zwei Stunden dauern, bis der Upgrade-Vorgang vollständig angehalten ist. Um das Upgrade fortzusetzen, wählen Sie Fortsetzen .

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.

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 abubrechen.



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 Storage-Firmware-Upgrade-Paket auf ein Gerät herunter, auf das der Management-Node zugreifen kann. Gehen Sie zu Element Software "[download-Seite](#)" 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 ("upgradeld" Das ist Teil der Antwort.
6. Überprüfen Sie den Aktualisierungsfortschritt und die Ergebnisse:
- a. Wählen Sie **GET /Upgrades/{upgradeld}** aus.
 - b. Wählen Sie **Probieren Sie es aus.**
 - c. Geben Sie die Upgrade-ID des vorherigen Schritts in **Upgradeld** ein.
 - d. Wählen Sie **Ausführen.**
 - e. Führen Sie einen der folgenden Schritte aus, wenn während des Upgrades Probleme oder besondere Anforderungen auftreten:

Option	Schritte
<p>Sie müssen Probleme mit dem Cluster-Systemzustand aufgrund von korrigieren <code>failedHealthChecks</code> Nachricht im Antwortkörper.</p>	<ol style="list-style-type: none"> 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 <code>"action": "resume"</code> Im Anforderungsgremium. <div data-bbox="915 1423 1487 1602" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre> { "action": "resume" } </pre> </div> vii. Wählen Sie Ausführen.

Option	Schritte
Sie müssen das Upgrade unterbrechen, da das Wartungsfenster geschlossen wird oder aus einem anderen Grund.	<ol style="list-style-type: none"> 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. <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>{ "action": "pause" }</pre> </div> 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

- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

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 12.2 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 das Management-Services-Bundle mit NetApp Hybrid Cloud Control auf die neueste Version aktualisiert. NetApp Hybrid Cloud Control kann über folgende IP-Adresse darauf zugreifen:

https://<ManagementNodeIP>

- 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 Element Software 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 der NetApp Support Site für 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 das Management-Services-Bundle mit NetApp Hybrid Cloud Control auf die neueste Version aktualisiert. NetApp Hybrid Cloud Control kann über folgende IP-Adresse darauf zugreifen:
`https://<ManagementNodeIP>`
- 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 Element Software 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 der NetApp Support Site für 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 das Management-Services-Bundle mit NetApp Hybrid Cloud Control auf die neueste Version aktualisiert. NetApp Hybrid Cloud Control kann über folgende IP-Adresse darauf zugreifen:
`https://<ManagementNodeIP>`
- 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 Element Software 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 Site für 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 Element Software 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 Site für 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 SolidFire All-Flash-Storage-Installationen mit dem NetApp Element Plug-in für vCenter Server) Aktualisieren Sie das vCenter Plug-in auf dem 12.3.x-Management-Node, indem Sie die Schritte im 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.

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

- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

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 vCenter Plug-in 5.0 oder 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 vCenter Plug-in 4.10 oder früher

Dieses Upgrade-Verfahren umfasst die folgenden Upgrade-Szenarien:

- Sie aktualisieren gerade auf Element Plug-in für vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6 4.5, oder 4.4.
- Sie aktualisieren gerade auf einen 7.0, 6.7 oder 6.5 HTML5 vSphere Web Client.

- Das Plug-in ist nicht 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 kompatibel mit vSphere Web Client Version 6.7 U2 für Flash, 6.7 U3 (Flash und HTML5) und 7.0 U1. Das Plug-in ist nicht kompatibel mit Version 6.7 U2 Build 13007421 des HTML5 vSphere Web Client und anderen 6.7 U2 Builds, die vor dem Update 2a (Build 13643870) veröffentlicht wurden. Weitere Informationen zu unterstützten vSphere-Versionen finden Sie in den Versionshinweisen zu "[Ihre Version des Plug-ins](#)".

Was Sie benötigen

- **Admin-Berechtigungen:** Sie haben vCenter Administrator-Rollenberechtigungen, um ein Plug-in zu installieren.
- **vSphere Upgrades:** Sie haben alle erforderlichen vCenter Upgrades vor dem Upgrade des NetApp Element Plug-ins für vCenter Server durchgeführt. Bei diesem Verfahren wird vorausgesetzt, dass vCenter Upgrades bereits abgeschlossen wurden.
- **vCenter Server:** Ihr vCenter Plug-in Version 4.x oder 5.x ist mit einem vCenter Server registriert. Über das Registrierungsdienstprogramm (`https://<ManagementNodeIP>: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 Management-Services-Updates veröffentlicht, die außerhalb der wichtigsten Produktversionen für NetApp SolidFire All-Flash-Storage 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://<ManagementNodeIP>:9443` Die Registrierungs-Utility-Benutzeroberfläche wird auf der Seite *** QoSSIOC Service Credentials*** verwaltet für das Plug-in geöffnet.

QoSSIOC Management

- Manage Credentials
- Restart QoSSIOC Service

Manage QoSSIOC Service Credentials

Old Password
Current password is required

New Password
Must contain at least 8 characters with at least one lower-case and upper-case alphabet, a number and a special character like #!@:()~!@#%^&*~

Confirm Password
New and confirm passwords must match

Contact NetApp Support at <http://mysupport.netapp.com>

2. Wählen Sie **vCenter Plug-in Registrierung**.

- Die vCenter Plug-in-Registrierungsseite für Element Plug-in für vCenter Server 5.x:

Manage vCenter Plug-in

- Register Plug-in
- Update Plug-in
- Unregister Plug-in
- Registration Status

vCenter Plug-in - Registration

Register version 5.0.0 of the NetApp Element Plug-in for vCenter Server with your vCenter server. The Plug-in will not be deployed until a fresh vCenter login after registration.

vCenter Address
Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on.

vCenter User Name
Ensure this user is a vCenter user that has administrative privileges for registration.

vCenter Password
The password for the vCenter user name entered.

Customize URL
Select to customize the Zip file URL.

Plug-in Zip URL
URL of XML initialization file

Contact NetApp Support at <http://mysupport.netapp.com>

- 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.

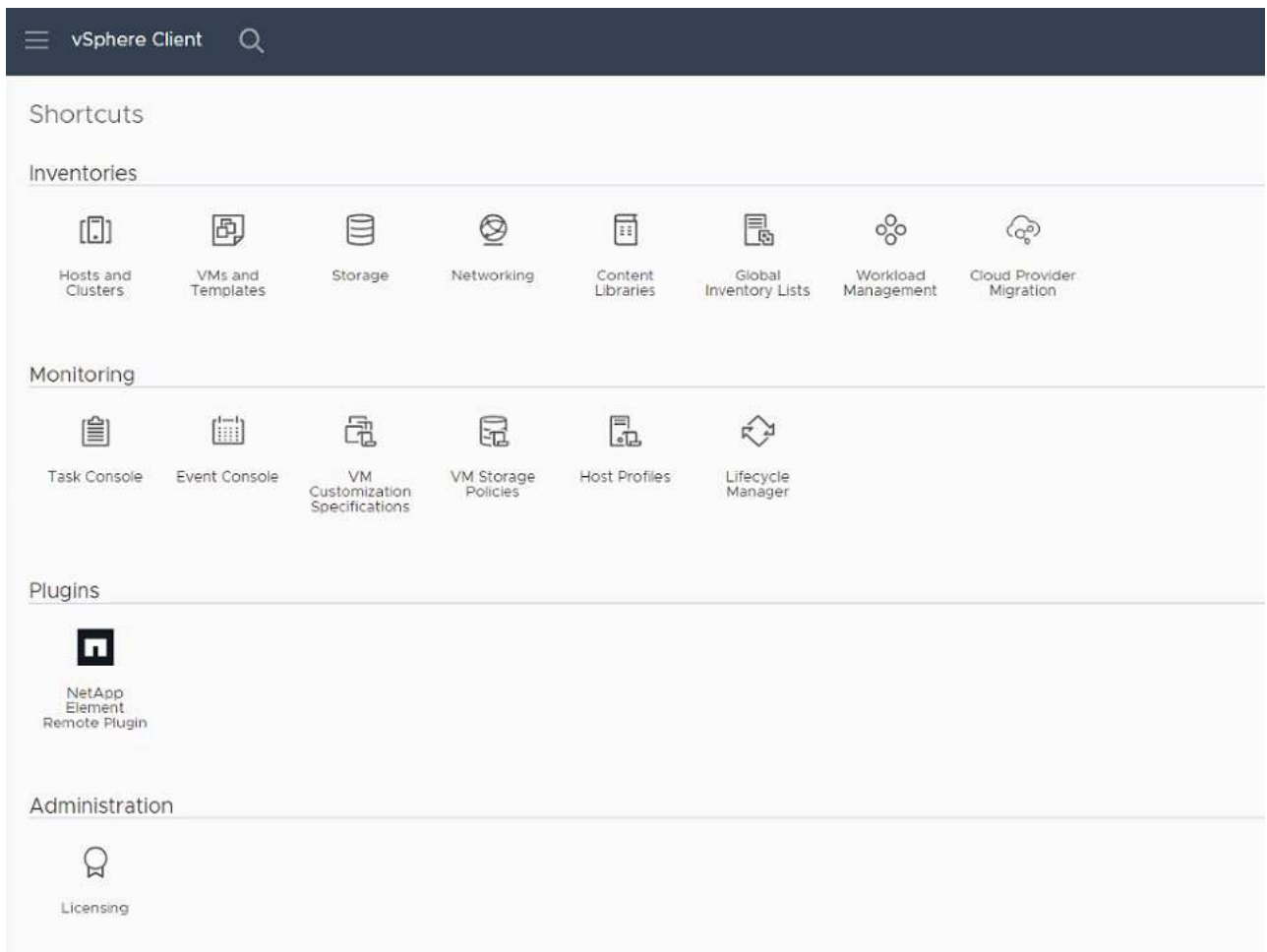


Durch diese Aktion wird eine neue Datenbank erstellt und die Installation im vSphere Web Client abgeschlossen.

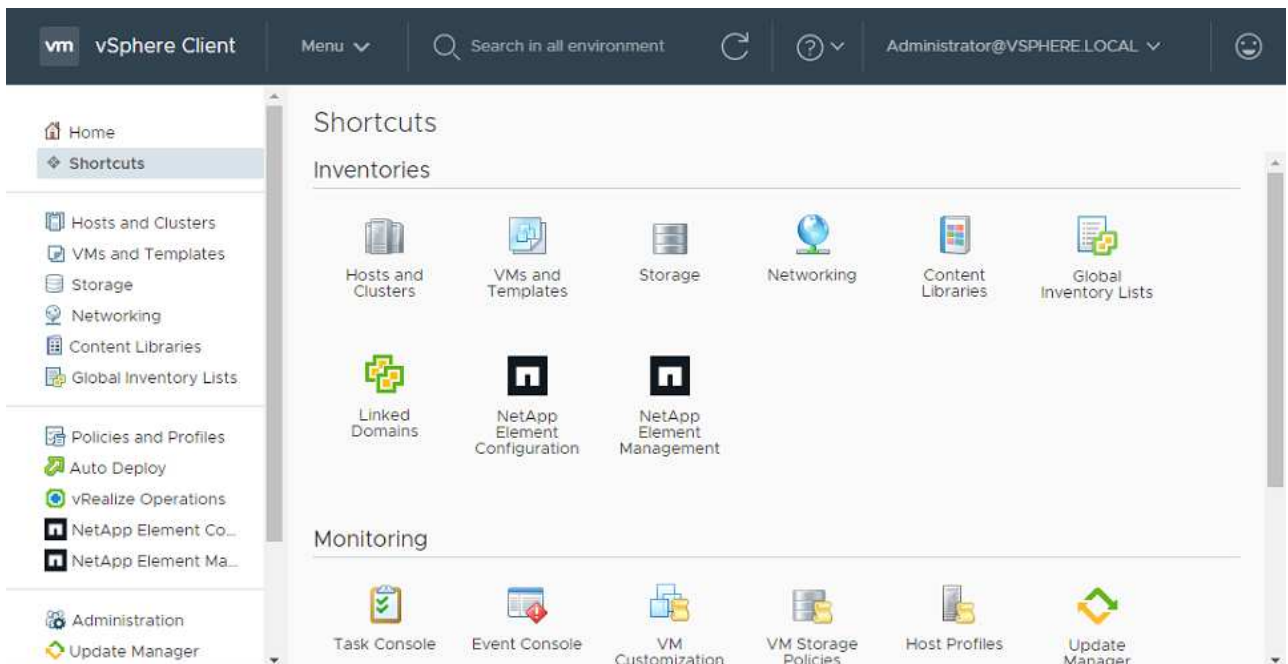
7. Suchen Sie im vSphere Web Client nach den folgenden abgeschlossenen Aufgaben im Task Monitor, um sicherzustellen, dass die Installation abgeschlossen wurde: `Download plug-in` Und `Deploy plug-in`.

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

- ["Dokumentation von SolidFire und Element Software"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.