



# **Arbeiten Sie mit der REST-API des Management-Knotens.**

## Element Software

NetApp  
November 12, 2025

# Inhalt

Arbeiten Sie mit der REST-API des Management-Knotens.	1
Übersicht der REST-API-Benutzeroberfläche des Management-Knotens.	1
Genehmigung	1
Anlagenkonfiguration	1
Vermögensverwaltung	1
Autorisierung zur Nutzung von REST-APIs einholen.	1
Aktivieren Sie Active IQ und die NetApp Überwachung.	3
NetApp Hybrid Cloud Control für mehrere vCenter-Center konfigurieren	5
Fügen Sie dem Verwaltungsknoten ein Controller-Asset hinzu.	6
Speichercluster-Assets erstellen und verwalten	8
Abrufen der Installations-ID und der Cluster-ID eines Speichercluster-Assets	9
Fügen Sie ein neues Speichercluster-Asset hinzu.	10
Bearbeiten Sie die gespeicherten Anmeldeinformationen für ein Speichercluster-Asset.	11
Löschen eines Speichercluster-Assets	12
Vorhandene Controller-Assets anzeigen oder bearbeiten	13
Greifen Sie auf die REST-API der Verwaltungsdienste zu.	13
Gespeicherte Informationen über vorhandene Controller anzeigen	14
Den Status eines vorhandenen Controllers anzeigen	14
Bearbeiten Sie die gespeicherten Eigenschaften eines Controllers	14
Konfigurieren Sie einen Proxy-Server	15
Überprüfen Sie die Versionen des Management-Knoten-Betriebssystems und der Dienste.	16
API-Befehle	17
REST-API-UI-Schritte	17
Abrufen von Protokollen von Verwaltungsdiensten	18

# Arbeiten Sie mit der REST-API des Management-Knotens.

## Übersicht der REST-API-Benutzeroberfläche des Management-Knotens

Durch die Verwendung der integrierten REST-API-Benutzeroberfläche(<https://<ManagementNodeIP>/mnode>) Sie können APIs ausführen oder verstehen, die sich auf die Dienste des Verwaltungsknotens beziehen, einschließlich der Konfiguration des Proxy-Servers, Aktualisierungen auf Dienstebene oder der Anlagenverwaltung.

Aufgaben, die Sie mit REST-APIs ausführen können:

### Genehmigung

- "Autorsierung zur Nutzung von REST-APIs einholen."

### Anlagenkonfiguration

- "Aktivieren Sie Active IQ und die NetApp Überwachung."
- "Konfigurieren Sie einen Proxy-Server für den Verwaltungsknoten."
- "NetApp Hybrid Cloud Control für mehrere vCenter-Center konfigurieren"
- "Fügen Sie dem Verwaltungsknoten ein Controller-Asset hinzu."
- "Speichercluster-Assets erstellen und verwalten"

### Vermögensverwaltung

- "Vorhandene Controller-Assets anzeigen oder bearbeiten"
- "Speichercluster-Assets erstellen und verwalten"
- "Verwenden Sie die REST-API, um Element-Systemprotokolle zu erfassen."
- "Überprüfen Sie die Versionen des Management-Knoten-Betriebssystems und der Dienste."
- "Abrufen von Protokollen von Verwaltungsdiensten"

### Weitere Informationen

- "Greifen Sie auf den Verwaltungsknoten zu."
- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element-Softwaredokumentation"

## Autorisierung zur Nutzung von REST-APIs einholen.

Sie müssen sich autorisieren, bevor Sie APIs für Verwaltungsdienste in der REST-API-Benutzeroberfläche verwenden können. Dies geschieht durch den Erhalt eines

## Zugriffstokens.

Um ein Token zu erhalten, benötigen Sie Cluster-Administratoranmeldeinformationen und eine Client-ID. Jeder Token ist ungefähr zehn Minuten gültig. Nach Ablauf eines Tokens können Sie erneut einen neuen Zugriffstoken anfordern.

Die Autorisierungsfunktionalität wird während der Installation und Bereitstellung des Management-Knotens für Sie eingerichtet. Der Token-Dienst basiert auf dem Speichercluster, den Sie während der Einrichtung definiert haben.

### Bevor Sie beginnen

- Ihre Clusterversion sollte die NetApp Element Software 11.3 oder höher verwenden.
- Sie sollten einen Management-Knoten mit Version 11.3 oder höher bereitgestellt haben.

### API-Befehl

```
TOKEN=`curl -k -X POST https://$MVIP/auth/connect/token -F client_id=$node-client -F grant_type=password -F username=CLUSTER_ADMIN -F password=CLUSTER_PASSWORD|awk -F':|' '{print $2}'|awk -F',' '{print $1}'|sed s/'"/g`
```

### REST-API-UI-Schritte

1. Sie können auf die REST-API-Benutzeroberfläche des Dienstes zugreifen, indem Sie die IP-Adresse des Verwaltungsknotens gefolgt vom Dienstnamen eingeben, zum Beispiel /\$node/ :

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

2. Wählen Sie **Autorisieren**.



Alternativ können Sie ein Schlosssymbol neben einer beliebigen Service-API auswählen.

3. Bitte füllen Sie Folgendes aus:

- a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
- b. Geben Sie die Client-ID ein als \$node-client Die
- c. Geben Sie keinen Wert für das Clientgeheimnis ein.
- d. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.

4. Schließen Sie das Dialogfeld **Verfügbare Berechtigungen**.



Wenn Sie versuchen, einen Befehl auszuführen, nachdem das Token abgelaufen ist, 401 Error: UNAUTHORIZED Es erscheint eine Meldung. Falls Sie diese Meldung sehen, autorisieren Sie erneut.

## Weitere Informationen

- ["NetApp Element Plug-in für vCenter Server"](#)

- "SolidFire und Element-Softwaredokumentation"

## Aktivieren Sie Active IQ und die NetApp Überwachung.

Sie können die Active IQ Speicherüberwachung aktivieren, falls Sie dies nicht bereits während der Installation oder des Upgrades getan haben. Möglicherweise müssen Sie dieses Verfahren anwenden, wenn Sie SolidFire Active IQ nicht während der Installation eines SolidFire All-Flash-Speichersystems eingerichtet haben.

Der Active IQ Collector-Dienst leitet Konfigurationsdaten und auf der Element-Software basierende Cluster-Leistungsmetriken an SolidFire Active IQ zur Erstellung von historischen Berichten und zur nahezu Echtzeit-Leistungsüberwachung weiter. Der NetApp Überwachungsdienst ermöglicht die Weiterleitung von Fehlern im Speichercluster an vCenter zur Benachrichtigung.

### Bevor Sie beginnen

- Einige Funktionen in Active IQ, beispielsweise Quality of Service (QoS), benötigen Element 11.3 oder höher, um korrekt zu funktionieren. Um sicherzustellen, dass Sie alle Active IQ -Funktionen nutzen können, empfiehlt NetApp Folgendes:
  - Auf Ihrem Speichercluster läuft die NetApp Element Software 11.3 oder höher.
  - Sie haben einen Management-Knoten mit Version 11.3 oder höher bereitgestellt.
- Sie haben Internetzugang. Der Active IQ Collector-Dienst kann nicht von Dark-Sites aus genutzt werden, die keine externe Verbindung haben.

### Schritte

1. Ermitteln Sie die Basis-Asset-ID für die Installation:

- a. Öffnen Sie die REST-API-Benutzeroberfläche des Inventardienstes auf dem Verwaltungsknoten:

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

- b. Wählen Sie **Autorisieren** und führen Sie die folgenden Schritte aus:

- i. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
- ii. Geben Sie die Client-ID ein als `mnode-client` Die
- iii. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
- iv. Schließen Sie das Fenster.

- c. Wählen Sie in der REST-API-Benutzeroberfläche **GET /installations** aus.
- d. Wählen Sie **Ausprobieren**.
- e. Wählen Sie **Ausführen**.
- f. Kopieren Sie aus dem Antworttext des Codes 200 den `id` für die Installation.

```
{
  "installations": [
    {
      "_links": {
        "collection": "https://10.111.211.111/inventory/1/installations",
        "self": "https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



Ihre Installation verfügt über eine Basis-Asset-Konfiguration, die während der Installation oder des Upgrades erstellt wurde.

## 2. Telemetrie aktivieren:

- Greifen Sie auf die API-Benutzeroberfläche des mnode-Dienstes auf dem Management-Knoten zu, indem Sie die IP-Adresse des Management-Knotens gefolgt von eingeben. /mnode :

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

- Wählen Sie **Autorisieren** oder ein beliebiges Schlosssymbol und führen Sie die folgenden Schritte aus:

- Geben Sie den Cluster-Benutzernamen und das Passwort ein.
- Geben Sie die Client-ID ein als mnode-client Die
- Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
- Schließen Sie das Fenster.

- Basis-Asset konfigurieren:

- Wählen Sie **PUT /assets/{asset\_id}**.
- Wählen Sie **Ausprobieren**.
- Geben Sie Folgendes in die JSON-Nutzlast ein:

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

- Geben Sie die Basis-ID aus dem vorherigen Schritt in **asset\_ID** ein.
- Wählen Sie **Ausführen**.

Der Active IQ Dienst wird automatisch neu gestartet, sobald Assets geändert werden. Das Ändern

von Assets führt zu einer kurzen Verzögerung, bevor die Einstellungen angewendet werden.

3. Falls noch nicht geschehen, fügen Sie ein vCenter-Controller-Asset für NetApp Hybrid Cloud Control zu den bekannten Assets des Management-Knotens hinzu:



Für die Überwachungsdienste von NetApp wird ein Controller benötigt.

- a. Wählen Sie **POST /assets/{asset\_id}/controllers**, um ein Controller-Sub-Asset hinzuzufügen.
- b. Wählen Sie **Ausprobieren**.
- c. Geben Sie die übergeordnete Basis-Asset-ID, die Sie in Ihre Zwischenablage kopiert haben, in das Feld **asset\_id** ein.
- d. Geben Sie die erforderlichen Nutzlastwerte ein mit **type** als **vCenter** und vCenter-Anmeldeinformationen.

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



`ip` ist die vCenter IP-Adresse.

- e. Wählen Sie **Ausführen**.

## Weitere Informationen

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

## NetApp Hybrid Cloud Control für mehrere vCenter-Center konfigurieren

Sie können NetApp Hybrid Cloud Control so konfigurieren, dass Assets von zwei oder mehr vCenter-Servern verwaltet werden, die nicht im Linked Mode arbeiten.

Dieses Verfahren sollten Sie nach Ihrer Erstinstallation anwenden, wenn Sie Assets für eine kürzlich skalierte Installation hinzufügen müssen oder wenn neue Assets nicht automatisch zu Ihrer Konfiguration hinzugefügt wurden. Verwenden Sie diese APIs, um Assets hinzuzufügen, die kürzlich zu Ihrer Installation hinzugefügt wurden.

### Was du brauchst

- Auf Ihrem Cluster läuft die NetApp Element Software 11.3 oder höher.
- Sie haben einen Management-Knoten mit Version 11.3 oder höher bereitgestellt.

## Schritte

1. "["Neue vCenter-Center als Controller-Assets hinzufügen"](#) zur Konfiguration des Management-Knotens.
2. Aktualisieren Sie die Inventardienst-API auf dem Verwaltungsknoten:

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



Alternativ können Sie 2 Minuten warten, bis der Bestand in der NetApp Hybrid Cloud Control-Benutzeroberfläche aktualisiert ist.

- a. Wählen Sie **Autorisieren** und führen Sie die folgenden Schritte aus:
    - i. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
    - ii. Geben Sie die Client-ID ein als `mnode-client`. Die
    - iii. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
    - iv. Schließen Sie das Fenster.
  - b. Wählen Sie in der REST-API-Benutzeroberfläche **GET /installations** aus.
  - c. Wählen Sie **Ausprobieren**.
  - d. Wählen Sie **Ausführen**.
  - e. Kopieren Sie aus der Antwort die Installations-Asset-ID.`("id")`.
  - f. Wählen Sie in der REST-API-Benutzeroberfläche **GET /installations/{id}** aus.
  - g. Wählen Sie **Ausprobieren**.
  - h. Aktualisierung einstellen auf `True`. Die
  - i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.
  - j. Wählen Sie **Ausführen**.
3. Aktualisieren Sie den NetApp Hybrid Cloud Control-Browser, um die Änderungen zu sehen.

## Weitere Informationen

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

## Fügen Sie dem Verwaltungsknoten ein Controller-Asset hinzu.

Sie können der Management-Knotenkonfiguration über die REST-API-Benutzeroberfläche ein Controller-Asset hinzufügen.

Möglicherweise müssen Sie ein Asset hinzufügen, wenn Sie Ihre Installation kürzlich skaliert haben und neue Assets nicht automatisch zu Ihrer Konfiguration hinzugefügt wurden. Verwenden Sie diese APIs, um Assets hinzuzufügen, die kürzlich zu Ihrer Installation hinzugefügt wurden.

### Was du brauchst

- Auf Ihrem Cluster läuft die NetApp Element Software 11.3 oder höher.

- Sie haben einen Management-Knoten mit Version 11.3 oder höher bereitgestellt.
- Sie haben in vCenter eine neue NetApp HCC-Rolle erstellt, um die Ansicht der Management-Knotendienste auf NetApp-Assets zu beschränken. Sehen "[Erstellen Sie eine NetApp HCC-Rolle in vCenter](#)"

## Schritte

1. Ermitteln Sie die Basis-Asset-ID für die Installation:
  - a. Öffnen Sie die REST-API-Benutzeroberfläche des Inventardienstes auf dem Verwaltungsknoten:

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

- b. Wählen Sie **Autorisieren** und führen Sie die folgenden Schritte aus:
  - i. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
  - ii. Geben Sie die Client-ID ein als mnode-client Die
  - iii. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
  - iv. Schließen Sie das Fenster.
- c. Wählen Sie in der REST-API-Benutzeroberfläche **GET /installations** aus.
- d. Wählen Sie **Ausprobieren**.
- e. Wählen Sie **Ausführen**.
- f. Kopieren Sie aus dem Antworttext des Codes 200 den **id** für die Installation.

```
{
  "installations": [
    {
      "_links": {
        "collection":
          "https://10.111.211.111/inventory/1/installations",
        "self":
          "https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



Ihre Installation verfügt über eine Basis-Asset-Konfiguration, die während der Installation oder des Upgrades erstellt wurde.

- g. Wählen Sie in der REST-API-Benutzeroberfläche **GET /installations/{id}** aus.
- h. Wählen Sie **Ausprobieren**.
- i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.
- j. Wählen Sie **Ausführen**.
- k. Kopieren und speichern Sie die Cluster-Controller-ID aus der Antwort. ("controllerId" ) zur

- Verwendung in einem späteren Schritt.
2. Um einem bestehenden Basis-Asset ein Controller-Sub-Asset hinzuzufügen, wählen Sie Folgendes aus:

```
POST /assets/{asset_id}/controllers
```

- a. Öffnen Sie die Benutzeroberfläche der mNode-Dienst-REST-API auf dem Management-Knoten:

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

- b. Wählen Sie **Autorisieren** und führen Sie die folgenden Schritte aus:
- Geben Sie den Cluster-Benutzernamen und das Passwort ein.
  - Geben Sie die Client-ID ein als `mnode-client`. Die
  - Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
  - Schließen Sie das Fenster.
- c. Wählen Sie **POST /assets/{asset\_id}/controllers**.
- d. Wählen Sie **Ausprobieren**.
- e. Geben Sie die übergeordnete Basis-Asset-ID im Feld **asset\_id** ein.
- f. Fügen Sie die erforderlichen Werte zur Nutzlast hinzu.
- g. Wählen Sie **Ausführen**.

## Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "SolidFire und Element-Softwaredokumentation"

## Speichercluster-Assets erstellen und verwalten

Sie können neue Speichercluster-Assets zum Verwaltungsknoten hinzufügen, die gespeicherten Anmeldeinformationen für bekannte Speichercluster-Assets bearbeiten und Speichercluster-Assets vom Verwaltungsknoten mithilfe der REST-API löschen.

### Was du brauchst

- Stellen Sie sicher, dass auf Ihrem Speichercluster die NetApp Element Software Version 11.3 oder höher läuft.
- Stellen Sie sicher, dass Sie einen Management-Knoten mit Version 11.3 oder höher bereitgestellt haben.

### Optionen für die Verwaltung von Speichercluster-Assets

Wählen Sie eine der folgenden Optionen:

- Abrufen der Installations-ID und der Cluster-ID eines Speichercluster-Assets
- Fügen Sie ein neues Speichercluster-Asset hinzu.
- Bearbeiten Sie die gespeicherten Anmeldeinformationen für ein Speichercluster-Asset.

- Löschen eines Speichercluster-Assets

## Abrufen der Installations-ID und der Cluster-ID eines Speichercluster-Assets

Sie können die Installations-ID und die ID des Speicherclusters über die REST-API abrufen. Sie benötigen die Installations-ID, um ein neues Speichercluster-Asset hinzuzufügen, und die Cluster-ID, um ein bestimmtes Speichercluster-Asset zu ändern oder zu löschen.

### Schritte

1. Greifen Sie auf die REST-API-Benutzeroberfläche für den Inventarisierungsdienst zu, indem Sie die IP-Adresse des Verwaltungsknotens gefolgt von eingeben. /inventory/1/ :

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

2. Wählen Sie **Autorisieren** oder ein beliebiges Schlosssymbol und führen Sie die folgenden Schritte aus:
  - a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
  - b. Geben Sie die Client-ID ein als mnode-client Die
  - c. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
  - d. Schließen Sie das Fenster.
3. Wählen Sie **GET /installations**.
4. Wählen Sie **Ausprobieren**.
5. Wählen Sie **Ausführen**.

Die API gibt eine Liste aller bekannten Installationen zurück.

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

```
"installations": [  
    {  
        "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",  
        "name": "my-sf-installation",  
        "_links": {  
            "collection": "https://localhost/inventory/1/installations",  
            "self": "https://localhost/inventory/1/installations/1234a678-  
12ab-35dc-7b4a-1234a5b6a7ba"  
        }  
    }  
]
```

7. Greifen Sie auf die REST-API-Benutzeroberfläche für den Speicherdiensst zu, indem Sie die IP-Adresse des Verwaltungsknotens gefolgt von eingeben. /storage/1/ :

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

8. Wählen Sie **Autorisieren** oder ein beliebiges Schlosssymbol und führen Sie die folgenden Schritte aus:
    - a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
    - b. Geben Sie die Client-ID ein als `mnode-client` Die
    - c. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
    - d. Schließen Sie das Fenster.
  9. Wählen Sie **GET /clusters**.
  10. Wählen Sie **Ausprobieren**.
  11. Geben Sie die zuvor gespeicherte Installations-ID in das folgende Feld ein: `installationId` Parameter.
  12. Wählen Sie **Ausführen**.
- Die API gibt eine Liste aller bekannten Speichercluster in dieser Installation zurück.
13. Ermitteln Sie anhand des Antworttextes des Codes 200 den korrekten Speichercluster und speichern Sie den Wert im Cluster. `storageId` Feld. Dies ist die Speichercluster-ID.

## Fügen Sie ein neues Speichercluster-Asset hinzu.

Mit der REST-API können Sie ein oder mehrere neue Speichercluster-Assets zum Management-Knoteninventar hinzufügen. Wenn Sie ein neues Speichercluster-Asset hinzufügen, wird dieses automatisch beim Verwaltungsknoten registriert.

### Was du brauchst

- Sie haben kopiert [Speichercluster-ID und Installations-ID](#) für beliebige Speichercluster, die Sie hinzufügen möchten.
- Wenn Sie mehr als einen Speichercluster hinzufügen, haben Sie die Einschränkungen des "[Autoritativer Cluster](#)" und Unterstützung für mehrere Speichercluster.



Alle im autoritativen Cluster definierten Benutzer sind auch in allen anderen mit der NetApp Hybrid Cloud Control-Instanz verbundenen Clustern als Benutzer definiert.

### Schritte

1. Greifen Sie auf die REST-API-Benutzeroberfläche für den Speicherdiensst zu, indem Sie die IP-Adresse des Verwaltungsknotens gefolgt von eingeben. `/storage/1/` :

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

2. Wählen Sie **Autorisieren** oder ein beliebiges Schlosssymbol und führen Sie die folgenden Schritte aus:
  - a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
  - b. Geben Sie die Client-ID ein als `mnode-client` Die
  - c. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.

- d. Schließen Sie das Fenster.
3. Wählen Sie **POST /clusters**.
  4. Wählen Sie **Ausprobieren**.
  5. Geben Sie die Informationen des neuen Speicherclusters in den folgenden Parametern im Feld **Anfragetext** ein:

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

Parameter	Typ	Beschreibung
installationId	Schnur	Die Installation, in die der neue Speichercluster integriert werden soll. Geben Sie die zuvor gespeicherte Installations-ID in dieses Feld ein.
mvip	Schnur	Die IPv4-Management-Virtual-IP-Adresse (MVIP) des Speicherclusters.
password	Schnur	Das Passwort, das zur Kommunikation mit dem Speichercluster verwendet wird.
userId	Schnur	Die Benutzer-ID, die zur Kommunikation mit dem Speichercluster verwendet wird (der Benutzer muss über Administratorrechte verfügen).

6. Wählen Sie **Ausführen**.

Die API gibt ein Objekt zurück, das Informationen über das neu hinzugefügte Speichercluster-Asset enthält, wie z. B. Name, Version und IP-Adressinformationen.

## **Bearbeiten Sie die gespeicherten Anmeldeinformationen für ein Speichercluster-Asset.**

Sie können die gespeicherten Anmeldeinformationen bearbeiten, die der Verwaltungsknoten für die Anmeldung an einem Speichercluster verwendet. Der von Ihnen ausgewählte Benutzer muss über Cluster-Administratorrechte verfügen.



Stellen Sie sicher, dass Sie die folgenden Schritte befolgt haben:[Abrufen der Installations-ID und der Cluster-ID eines Speichercluster-Assets](#) bevor wir fortfahren.

## Schritte

- Greifen Sie auf die REST-API-Benutzeroberfläche für den Speicherdienst zu, indem Sie die IP-Adresse des Verwaltungsknotens gefolgt von eingeben. /storage/1/ :

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

- Wählen Sie **Autorisieren** oder ein beliebiges Schlosssymbol und führen Sie die folgenden Schritte aus:
  - Geben Sie den Cluster-Benutzernamen und das Passwort ein.
  - Geben Sie die Client-ID ein als mnode-client Die
  - Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
  - Schließen Sie das Fenster.
- Wählen Sie **PUT /clusters/{storageId}**.
- Wählen Sie **Ausprobieren**.
- Fügen Sie die zuvor kopierte Speichercluster-ID in das folgende Feld ein: storageId Parameter.
- Ändern Sie einen oder beide der folgenden Parameter im Feld **Anfragetext**:

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

Parameter	Typ	Beschreibung
password	Schnur	Das Passwort, das zur Kommunikation mit dem Speichercluster verwendet wird.
userId	Schnur	Die Benutzer-ID, die zur Kommunikation mit dem Speichercluster verwendet wird (der Benutzer muss über Administratorrechte verfügen).

- Wählen Sie **Ausführen**.

## Löschen eines Speichercluster-Assets

Sie können ein Storage-Cluster-Asset löschen, wenn der Storage-Cluster nicht mehr in Betrieb ist. Wenn Sie ein Speichercluster-Asset entfernen, wird es automatisch vom Management-Knoten abgemeldet.



Stellen Sie sicher, dass Sie die folgenden Schritte befolgt haben:[Abrufen der Installations-ID und der Cluster-ID eines Speichercluster-Assets](#) bevor wir fortfahren.

## Schritte

- Greifen Sie auf die REST-API-Benutzeroberfläche für den Speicherdienst zu, indem Sie die IP-Adresse

des Verwaltungsknotens gefolgt von eingeben. /storage/1/ :

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

2. Wählen Sie **Autorisieren** oder ein beliebiges Schlosssymbol und führen Sie die folgenden Schritte aus:
  - a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
  - b. Geben Sie die Client-ID ein als mnode-client Die
  - c. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
  - d. Schließen Sie das Fenster.
3. Wählen Sie **DELETE /clusters/{storageld}**.
4. Wählen Sie **Ausprobieren**.
5. Geben Sie die zuvor kopierte Speichercluster-ID in das Feld ein. storageId Parameter.
6. Wählen Sie **Ausführen**.

Im Erfolgsfall liefert die API eine leere Antwort.

## Weitere Informationen

- "[Autoritativer Cluster](#)"
- "[NetApp Element Plug-in für vCenter Server](#)"
- "[SolidFire und Element-Softwaredokumentation](#)"

## Vorhandene Controller-Assets anzeigen oder bearbeiten

Sie können Informationen über vorhandene VMware vCenter-Controller in der Management-Knotenkonfiguration mithilfe der REST-API anzeigen und bearbeiten. Bei den Controllern handelt es sich um VMware vCenter-Instanzen, die beim Management-Knoten Ihrer NetApp SolidFire -Installation registriert sind.

### Bevor Sie beginnen

- Stellen Sie sicher, dass auf Ihrem Cluster die NetApp Element Software Version 11.3 oder höher ausgeführt wird.
- Stellen Sie sicher, dass Sie einen Management-Knoten mit Version 11.3 oder höher bereitgestellt haben.

### Greifen Sie auf die REST-API der Verwaltungsdienste zu.

#### Schritte

1. Greifen Sie auf die REST-API-Benutzeroberfläche für Verwaltungsdienste zu, indem Sie die IP-Adresse des Verwaltungsknotens gefolgt von eingeben. /vcenter/1/ :

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

2. Wählen Sie **Autorisieren** oder ein beliebiges Schlosssymbol und führen Sie die folgenden Schritte aus:

- a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
- b. Geben Sie die Client-ID ein als `mnode-client` Die
- c. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
- d. Schließen Sie das Fenster.

## Gespeicherte Informationen über vorhandene Controller anzeigen

Sie können die vorhandenen vCenter-Controller, die beim Management-Knoten registriert sind, auflisten und die darüber gespeicherten Informationen mithilfe der REST-API anzeigen.

### Schritte

1. Wählen Sie **GET /compute/controllers**.
2. Wählen Sie **Ausprobieren**.
3. Wählen Sie **Ausführen**.

Die API gibt eine Liste aller bekannten vCenter-Controller zurück, zusammen mit der IP-Adresse, der Controller-ID, dem Hostnamen und der Benutzer-ID, die zur Kommunikation mit jedem Controller verwendet werden.

4. Wenn Sie den Verbindungsstatus eines bestimmten Controllers abrufen möchten, kopieren Sie die Controller-ID aus der `id` Kopieren Sie das Feld dieses Controllers in Ihre Zwischenablage und sehen Sie nach [Den Status eines vorhandenen Controllers anzeigen](#) Die

## Den Status eines vorhandenen Controllers anzeigen

Sie können den Status aller vorhandenen, beim Management-Knoten registrierten vCenter-Controller anzeigen. Die API gibt einen Status zurück, der angibt, ob NetApp Hybrid Cloud Control eine Verbindung zum vCenter-Controller herstellen kann, sowie den Grund für diesen Status.

### Schritte

1. Wählen Sie **GET /compute/controllers/{controller\_id}/status**.
2. Wählen Sie **Ausprobieren**.
3. Geben Sie die zuvor kopierte Controller-ID in das Feld ein. `controller_id` Parameter.
4. Wählen Sie **Ausführen**.

Die API gibt den Status dieses bestimmten vCenter-Controllers sowie den Grund für diesen Status zurück.

## Bearbeiten Sie die gespeicherten Eigenschaften eines Controllers

Sie können den gespeicherten Benutzernamen oder das Passwort für jeden der vorhandenen vCenter-Controller bearbeiten, die beim Verwaltungsknoten registriert sind. Die gespeicherte IP-Adresse eines vorhandenen vCenter-Controllers kann nicht bearbeitet werden.

### Schritte

1. Wählen Sie **PUT /compute/controllers/{controller\_id}**.
2. Geben Sie die Controller-ID eines vCenter-Controllers in der `controller_id` Parameter.

3. Wählen Sie **Ausprobieren**.

4. Ändern Sie einen der folgenden Parameter im Feld **Anfragetext**:

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

5. Wählen Sie **Ausführen**.

Die API liefert aktualisierte Controller-Informationen.

## Weitere Informationen

- "[Fügen Sie dem Verwaltungsknoten ein Controller-Asset hinzu.](#)"
- "[NetApp Element Plug-in für vCenter Server](#)"
- "[SolidFire und Element-Softwaredokumentation](#)"

## Konfigurieren Sie einen Proxy-Server

Wenn sich Ihr Cluster hinter einem Proxy-Server befindet, müssen Sie die Proxy-Einstellungen so konfigurieren, dass Sie ein öffentliches Netzwerk erreichen können.

Für Telemetrie-Sammler und Reverse-Tunnel-Verbindungen wird ein Proxy-Server verwendet. Sie können einen Proxy-Server über die REST-API-Benutzeroberfläche aktivieren und konfigurieren, falls Sie während der Installation oder des Upgrades noch keinen Proxy-Server konfiguriert haben. Sie können auch die Einstellungen des bestehenden Proxy-Servers ändern oder einen Proxy-Server deaktivieren.

Der Befehl zum Konfigurieren eines Proxy-Servers aktualisiert die aktuellen Proxy-Einstellungen für den Verwaltungsknoten und gibt diese anschließend zurück. Die Proxy-Einstellungen werden von Active IQ, dem NetApp Überwachungsdienst, und anderen Element-Software-Dienstprogrammen verwendet, die auf dem Management-Knoten installiert sind, einschließlich des Reverse-Support-Tunnels für den NetApp Support.

### Bevor Sie beginnen

- Sie sollten die Host- und Anmeldeinformationen für den Proxy-Server kennen, den Sie konfigurieren.
- Stellen Sie sicher, dass auf Ihrem Cluster die NetApp Element Software Version 11.3 oder höher ausgeführt wird.
- Stellen Sie sicher, dass Sie einen Management-Knoten mit Version 11.3 oder höher bereitgestellt haben.
- (Management-Knoten 12.0 und höher) Sie haben NetApp Hybrid Cloud Control auf die Management-Services-Version 2.16 aktualisiert, bevor Sie einen Proxy-Server konfiguriert haben.

### Schritte

1. Greifen Sie auf die REST-API-Benutzeroberfläche des Management-Knotens zu, indem Sie die IP-Adresse

des Management-Knotens gefolgt von eingeben. /mnode :

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

2. Wählen Sie **Autorisieren** oder ein beliebiges Schlosssymbol und führen Sie die folgenden Schritte aus:
  - a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
  - b. Geben Sie die Client-ID ein als mnode-client Die
  - c. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
  - d. Schließen Sie das Fenster.
3. Wählen Sie **PUT /settings**.
4. Wählen Sie **Ausprobieren**.
5. Um einen Proxy-Server zu aktivieren, müssen Sie Folgendes einstellen: `use_proxy` zu wahr. Geben Sie die IP-Adresse oder den Hostnamen und die Proxy-Portziele ein.

Der Proxy-Benutzername, das Proxy-Passwort und der SSH-Port sind optional und sollten weggelassen werden, wenn sie nicht verwendet werden.

```
{
  "proxy_ip_or_hostname": "[IP or name]",
  "use_proxy": [true/false],
  "proxy_username": "[username]",
  "proxy_password": "[password]",
  "proxy_port": [port value],
  "proxy_ssh_port": [port value: default is 443]
}
```

6. Wählen Sie **Ausführen**.



Je nach Ihrer Umgebung müssen Sie möglicherweise Ihren Management-Knoten neu starten.

## Weitere Informationen

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

## Überprüfen Sie die Versionen des Management-Knoten-Betriebssystems und der Dienste.

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

### Was du brauchst

- Auf Ihrem Cluster läuft die NetApp Element Software 11.3 oder höher.
- Sie haben einen Management-Knoten mit Version 11.3 oder höher bereitgestellt.

## Optionen

- [API-Befehle](#)
- [REST-API-UI-Schritte](#)

## API-Befehle

- Ermitteln Sie Versionsinformationen zum Betriebssystem des Management-Knotens, zum Management-Services-Bundle und zum Management-Knoten-API-Dienst (mnode-api), die auf dem Management-Knoten ausgeführt werden:

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

- Versionsinformationen zu einzelnen Diensten, die auf dem Verwaltungsknoten ausgeführt werden, abrufen:

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



Sie können den Träger finden \${TOKEN} wird vom API-Befehl verwendet, wenn Sie "autorisieren" Die Der Überbringer \${TOKEN} befindet sich in der Curl-Antwort.

## REST-API-UI-Schritte

1. Greifen Sie auf die REST-API-Benutzeroberfläche des Dienstes zu, indem Sie die IP-Adresse des Management-Knotens gefolgt von eingeben. /mnode/ :

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

2. Führen Sie einen der folgenden Schritte aus:

- Ermitteln Sie Versionsinformationen zum Betriebssystem des Management-Knotens, zum Management-Services-Bundle und zum Management-Knoten-API-Dienst (mnode-api), die auf dem Management-Knoten ausgeführt werden:
  - i. Wählen Sie **GET /about**.
  - ii. Wählen Sie **Ausprobieren**.
  - iii. Wählen Sie **Ausführen**.

Die Version des Management-Services-Bundles("mnode\_bundle\_version" ), Management-Knoten-Betriebssystemversion("os\_version" ), und der Management-Node-API-Version("version" ) werden im Antworttext angegeben.

- Versionsinformationen zu einzelnen Diensten, die auf dem Verwaltungsknoten ausgeführt werden,

abrufen:

- i. Wählen Sie **GET /services**.
- ii. Wählen Sie **Ausprobieren**.
- iii. Wählen Sie als Status **Läuft** aus.
- iv. Wählen Sie **Ausführen**.

Die auf dem Management-Knoten laufenden Dienste werden im Antworttext angegeben.

## Weitere Informationen

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

## Abrufen von Protokollen von Verwaltungsdiensten

Sie können Protokolle der auf dem Management-Knoten laufenden Dienste mithilfe der REST-API abrufen. Sie können Protokolle von allen öffentlichen Diensten abrufen oder bestimmte Dienste angeben und Abfrageparameter verwenden, um die Rückgabergebnisse genauer zu definieren.

### Was du brauchst

- Auf Ihrem Cluster läuft die NetApp Element Software 11.3 oder höher.
- Sie haben einen Management-Knoten mit Version 11.3 oder höher bereitgestellt.

### Schritte

1. Öffnen Sie die REST-API-Benutzeroberfläche auf dem Management-Knoten.

- Beginnend mit Managementdienstleistungen 2.21.61:

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

- Für Management-Dienste 2.20.69 oder früher:

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

2. Wählen Sie **Autorisieren** oder ein beliebiges Schlosssymbol und führen Sie die folgenden Schritte aus:

- a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
- b. Geben Sie die Client-ID als mnode-client ein, falls der Wert noch nicht ausgefüllt ist.
- c. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
- d. Schließen Sie das Fenster.

3. Wählen Sie **GET /logs**.

4. Wählen Sie **Ausprobieren**.

5. Geben Sie die folgenden Parameter an:

- `Lines` Geben Sie die Anzahl der Zeilen ein, die das Protokoll zurückgeben soll. Dieser Parameter ist eine ganze Zahl mit dem Standardwert 1000.



Vermeiden Sie das Anfordern des gesamten Verlaufs der Protokollinhalte, indem Sie die Anzahl der Zeilen auf 0 setzen.

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



Verwenden Sie eine angemessene `since` Parameter beim Erfassen von Protokollen über längere Zeiträume.

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



Verwenden Sie die `GET /services` Befehl zum Auflisten der Dienste auf dem Verwaltungsknoten.

- `stopped`: Aufstellen `true` um Protokolle von gestoppten Diensten abzurufen.

6. Wählen Sie **Ausführen**.

7. Wählen Sie im Antworttext die Option **Herunterladen**, um die Protokollausgabe zu speichern.

## Weitere Informationen finden Sie hier.

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

## **Copyright-Informationen**

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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 BESCHRÄNKKT 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, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 IRGENDERWEINER 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.