Arbeiten Sie mit dem Management-Node

Element Software

NetApp
November 19, 2025

Inhalt

Arbeiten Sie mit dem Management-Node

Übersicht über Management-Nodes

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

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

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

- Mit dem Management Node UI (`https://[mNode IP]:442`) können Sie Änderungen an Netzwerk- und Cluster-Einstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.
- Mit der integrierten REST-API-UI (`https://[mNode IP]/mnode`) können Sie APIs in Bezug auf die Management-Node-Services ausführen oder verstehen, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

Installation oder Wiederherstellung eines Management-Node:

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

Zugriff auf den Management-Node:

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

Ändern Sie das Standard-SSL-Zertifikat:

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

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

- "Übersicht über die Management-Node-UI"

Aufgaben mit den MANAGEMENT-Node-REST-APIs:

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

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

- "Zugriff auf Storage-Nodes mithilfe von SSH für die grundlegende Fehlerbehebung"
  - "Aktivieren von Remote-Verbindungen mit NetApp Support"
  - "Verwalten der SSH-Funktionalität auf dem Management-Node"

Weitere Informationen

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

Installation oder Wiederherstellung eines Management-Node

Installieren Sie einen Management-Node

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

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

Was Sie benötigen

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

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

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

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

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

Über diese Aufgabe

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

Bevor Sie dieses Verfahren befolgen, sollten Sie wissen, "Persistente Volumes"ob Sie diese verwenden möchten oder nicht. Persistente Volumes sind optional, jedoch im Falle eines Datenverlusts bei der Management-Node-Konfiguration empfohlen.

Schritte

1. und implementieren Sie die VM

2. Erstellen Sie den Management-Node-Administrator, und konfigurieren Sie das Netzwerk
3. Konfigurieren Sie die Zeitsynchronisierung
4. Richten Sie den Management-Node ein
5. Controller-Assets konfigurieren

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

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

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

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

        Schalten Sie die VM nicht ein, bevor Sie den Schritt angeben, der später in diesem Verfahren ausgeführt werden soll.

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

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

4. Schalten Sie die VM nach Abschluss der Installation für den Management-Node ein.

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

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

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

2. Wenn im Netzwerk ein DHCP-Server (Dynamic Host Configuration Protocol) vorhanden ist, der IPs mit einer MTU (Maximum Transmission Unit) von weniger als 1500 Byte zuweist, müssen Sie die folgenden Schritte durchführen:

   a. Versetzen Sie den Management-Node vorübergehend in ein vSphere-Netzwerk ohne DHCP, z. B. iSCSI,.

   b. Starten Sie die VM neu, oder starten Sie das VM-Netzwerk neu.

   c. Konfigurieren Sie über TUI die korrekte IP-Adresse im Managementnetzwerk mit einer MTU größer oder gleich 1500 Bytes.

   d. Weisen Sie der VM das richtige VM-Netzwerk erneut zu.

   Ein DHCP, der IPs mit einer MTU unter 1500 Byte zuweist, kann Sie verhindern, dass Sie das Management-Node-Netzwerk konfigurieren oder die Management-Node-UI verwenden.

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

   Wenn Sie eine zusätzliche NIC zur Isolierung des Speicherverkehrs benötigen, lesen Sie die Anweisungen zum Konfigurieren einer anderen NIC: "Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)".

Konfigurieren Sie die Zeitsynchronisierung

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

   Ab Element 12.3 werden die Teilschritte a bis (e) automatisch ausgeführt. Fahren Sie für Management-Knoten 12.3 mit fortUnterschritt (f), um die Konfiguration der Zeitsynchronisierung abzuschließen.

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

   ```
   sudo service ntpd stop
   ```

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

   a. Kommentieren Sie die Standard-Server (`server 0.gentoo.pool.ntp.org`), indem Sie vor jedem einen hinzufügen `#`.

   b. Fügen Sie für jeden Standardzeitserver, den Sie hinzufügen möchten, eine neue Zeile hinzu. Die Standardzeitserver müssen die gleichen NTP-Server sein, die auf dem Speicher-Cluster verwendet

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

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. Speichern Sie die Konfigurationsdatei nach Abschluss.

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

```
sudo ntpd -gq
```

5. NTPD neu starten.

```
sudo service ntpd start
```

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

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

a. Periodische Zeitsynchronisierung deaktivieren:

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

b. Den aktuellen Status des Dienstes anzeigen und bestätigen:

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

c. Überprüfen Sie in vSphere, ob das `Synchronize guest time with host` Kontrollkästchen in den VM-Optionen deaktiviert ist.

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

> Bearbeiten Sie NTP nach Abschluss der Zeitsynchronisierung nicht, da es sich auf den NTP auswirkt, wenn Sie auf dem Management-Node ausführen"Setup-Befehl".

Richten Sie den Management-Node ein

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

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

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

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

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

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

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

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

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

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

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

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

d. Proxy-Server konfigurieren:

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

e. (Optional) Verwenden Sie die Parameterhilfe, wenn Sie zusätzliche Informationen über die einzelnen Parameter benötigen:

- **--help (-h)**: Gibt Informationen über jeden Parameter zurück. Parameter werden basierend auf der ursprünglichen Implementierung als erforderlich oder optional definiert. Die Parameteranforderungen für Upgrades und Neuimplementierungen können variieren.

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

Controller-Assets konfigurieren

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

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

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

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

2. Fügen Sie dem Management-Node bekannte Ressourcen eine vCenter Controller-Ressource für NetApp Hybrid Cloud Control hinzu:
   a. Greifen Sie auf die mnode Service API UI auf dem Management Node zu, indem Sie die Management Node IP-Adresse gefolgt von `/mnode`:

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

   b. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus, und füllen Sie Folgendes aus:
      i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
      ii. Geben Sie die Client-ID als `mnode-client`ein.
      iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
      iv. Schließen Sie das Fenster.
   c. Wählen Sie **POST /Assets/{Asset_id}/Controllers** aus, um eine Unterressource des Controllers hinzuzufügen.

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

   d. Wählen Sie **Probieren Sie es aus**.
   e. Geben Sie im Feld **Asset_id** die ID der übergeordneten Basis ein, die Sie in die Zwischenablage kopiert haben.
   f. Geben Sie die erforderlichen Nutzlastwerte mit dem Typ und den vCenter-Anmeldedaten ein `vCenter`.
   g. Wählen Sie **Ausführen**.

Weitere Informationen

- "Persistente Volumes"
- "Fügen Sie dem Management-Node eine Controller-Ressource hinzu"
- "Konfigurieren Sie eine Speicher-NIC"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)

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

Bevor Sie beginnen

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

Konfigurationsoptionen

Wählen Sie die für Ihre Umgebung relevante Option:

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

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

Schritte

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

> Die Werte werden `$` für jeden der erforderlichen Parameter für Ihre neue Storage-Netzwerkschnittstelle angezeigt. Das `cluster` Objekt in der folgenden Vorlage ist erforderlich und kann zur Umbenennung des Host-Namens des Management-Node verwendet werden. `--insecure` Oder `-k` Optionen sollten nicht in Produktionsumgebungen verwendet werden.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
     "params": {
                "network": {
                           "$eth1": {
                                    "#default" : false,
                                    "address" : "$storage_IP",
                                    "auto" : true,
                                    "family" : "inet",
                                    "method" : "static",
                                    "mtu" : "9000",
                                    "netmask" : "$subnet_mask",
                                    "status" : "Up"
                                    }
                           },
                "cluster": {
                           "name": "$mnode_host_name"
                           }
             },
    "method": "SetConfig"
}
'
```

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

Schritte

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

> Die Werte werden `$` für jeden der erforderlichen Parameter für Ihre neue Storage-Netzwerkschnittstelle angezeigt. Das `cluster` Objekt in der folgenden Vorlage ist erforderlich und kann zur Umbenennung des Host-Namens des Management-Node verwendet werden. `--insecure` Oder `-k` Optionen sollten nicht in Produktionsumgebungen verwendet werden.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
     "params": {
                "network": {
                           "$eth1": {
                                    "#default" : false,
                                    "address" : "$storage_IP",
                                    "auto" : true,
                                    "family" : "inet",
                                    "method" : "static",
                                    "mtu" : "9000",
                                    "netmask" : "$subnet_mask",
                                    "status" : "Up",
                                    "virtualNetworkTag" : "$vlan_id"
                                    }
                           },
                "cluster": {
                          "name": "$mnode_host_name",
                          "cipi": "$eth1.$vlan_id",
                          "sipi": "$eth1.$vlan_id"
                          }
              },
    "method": "SetConfig"
}
'
```

Weitere Informationen

- "Fügen Sie dem Management-Node eine Controller-Ressource hinzu"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Wiederherstellung eines Management-Node

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

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

Was Sie benötigen

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

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

Schritte

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

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

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

separaten Subnetz vom Management-Node (eth0) befindet und Sie persistente Volumes verwenden möchten, fügen Sie der VM im Storage-Subnetz (eth1) einen zweiten NIC (Network Interface Controller) hinzu oder stellen Sie sicher, dass das Managementnetzwerk zum Speichernetzwerk umgeleitet werden kann.

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

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

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

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

Konfigurieren des Netzwerks

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

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

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

> Wenn Sie eine zusätzliche NIC zur Isolierung des Speicherverkehrs benötigen, lesen Sie die Anweisungen zum Konfigurieren einer anderen NIC: "Konfigurieren eines Speicher-Netzwerkschnittstellentoncontrollers (NIC)".

Konfigurieren Sie die Zeitsynchronisierung

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

> Ab Element 12.3 werden die Teilschritte a bis (e) automatisch ausgeführt. Fahren Sie für Management-Knoten 12.3.1 oder höher mit fortUnterschritt (f), um die Konfiguration der Zeitsynchronisierung abzuschließen.

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

```
sudo service ntpd stop
```

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

a. Kommentieren Sie die Standard-Server (`server 0.gentoo.pool.ntp.org`), indem Sie vor jedem einen hinzufügen `#`.

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

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. Speichern Sie die Konfigurationsdatei nach Abschluss.

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

```
sudo ntpd -gq
```

5. NTPD neu starten.

```
sudo service ntpd start
```

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

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

a. Periodische Zeitsynchronisierung deaktivieren:

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

b. Den aktuellen Status des Dienstes anzeigen und bestätigen:

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

c. Überprüfen Sie in vSphere, ob das `Synchronize guest time with host` Kontrollkästchen in den VM-Optionen deaktiviert ist.

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

Bearbeiten Sie NTP nach Abschluss der Zeitsynchronisierung nicht, da es sich auf den NTP auswirkt, wenn Sie auf dem Management-Node ausführenBefehl „Neuimplementierung“.

Konfigurieren Sie den Management-Node

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

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

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

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

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

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

5. Eine Konfigurationsdatei für Konten und Volumes erstellen:

```
echo '{"trident": true, "mvip": "[mvip IP address]", "account_name":
"[persistent volume account name]"}' | sudo tee /sf/etc/mnode/mnode-
archive/management-services-metadata.json
```

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

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

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

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

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

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

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

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

c. Wenn Sie über den vollständig qualifizierten Domänennamen (FQDN) des Systems auf Element-Webschnittstellen (z. B. den Verwaltungsknoten oder die NetApp-Hybrid-Cloud-Steuerung) zugreifen, "Konfigurieren Sie die Authentifizierung für den Management-Node neu".

> Die SSH-Funktion "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support"ist bei Management-Nodes, auf denen Management-Services 2.18 und höher ausgeführt werden, standardmäßig deaktiviert. Wenn Sie zuvor die SSH-Funktion auf dem Management-Node aktiviert haben, müssen Sie möglicherweise "Deaktivieren Sie SSH erneut"auf dem wiederhergestellten Management-Node ausgeführt werden.

Weitere Informationen

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

Greifen Sie auf den Management-Node zu

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

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

- Mit Hilfe der Management Node UI (`https:// [mNode IP}:442`) können Sie Änderungen an Netzwerk- und Cluster-Einstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.
- Mit der integrierten REST API UI (`https://[mNode IP}/mnode`) können Sie APIs im Zusammenhang mit den Management-Node-Services ausführen oder verstehen, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

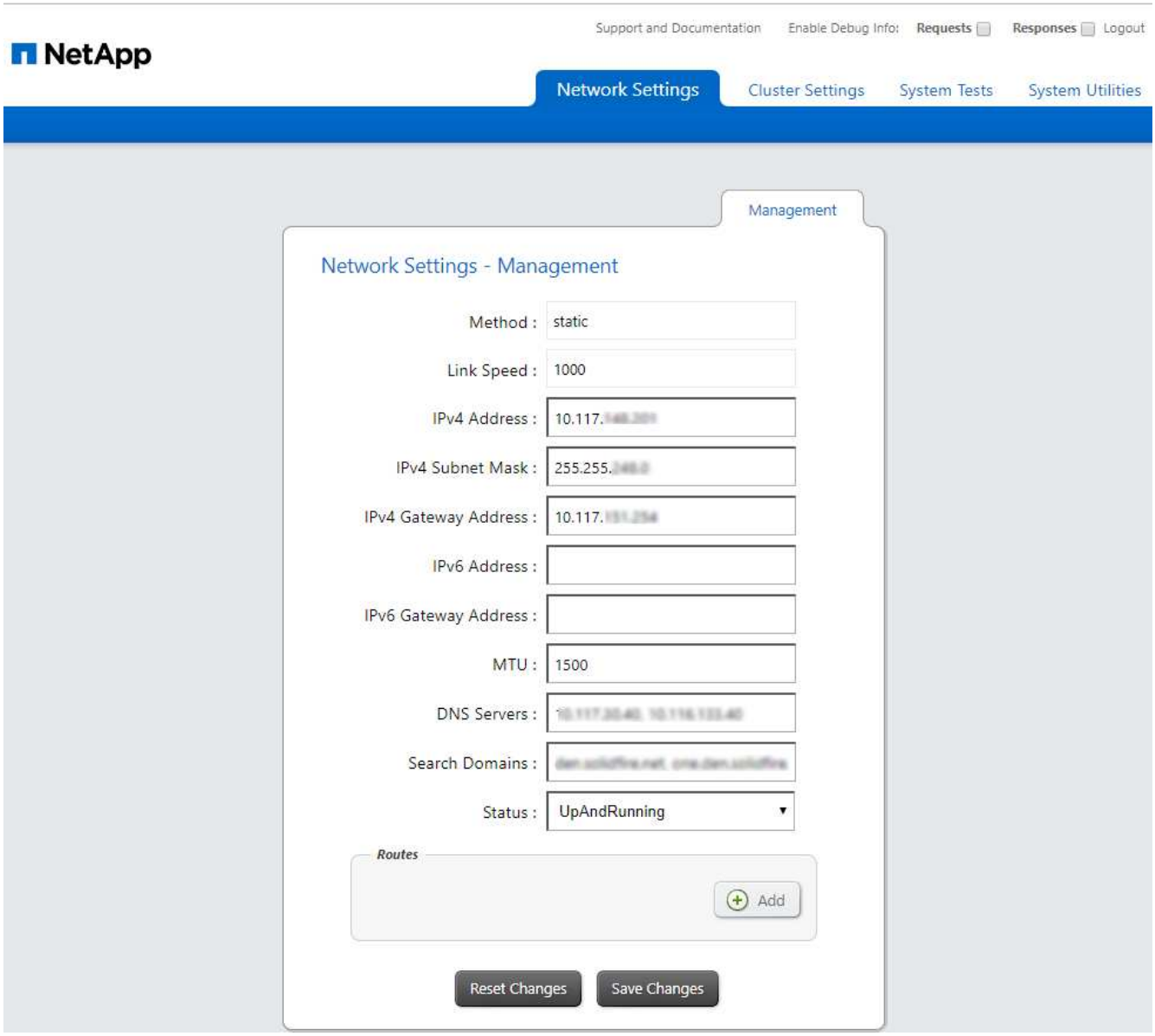
Greifen Sie über die UI auf den Management-Node zu

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

Schritte

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

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



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

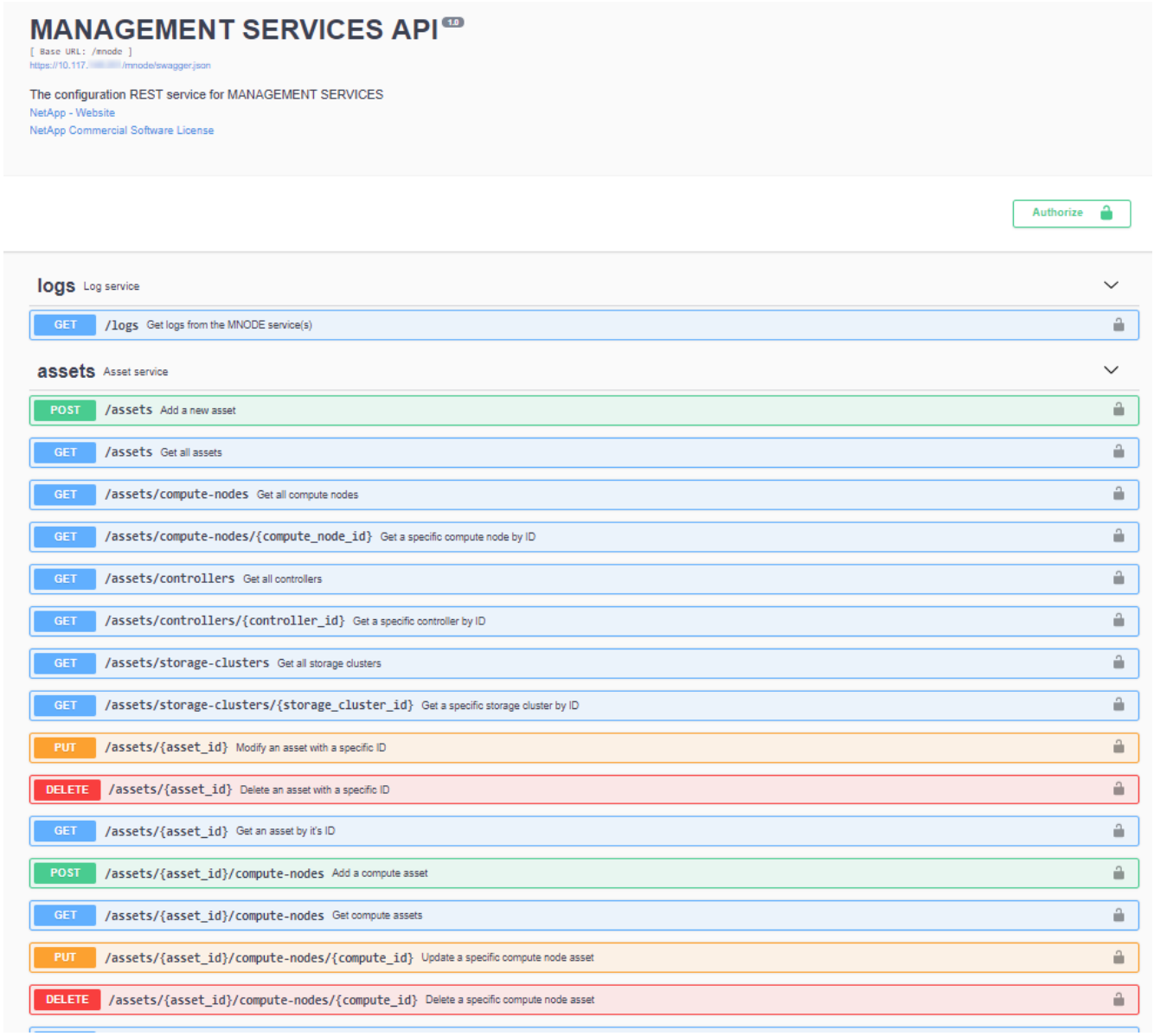
Greifen Sie auf DIE REST-API-UI für den Management-Node zu

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

Schritte

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

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



2. Wählen Sie **autorisieren** oder ein Schloss-Symbol aus und geben Sie Cluster-Administrator-Anmeldeinformationen ein, um APIs zu verwenden.

Weitere Informationen

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

Arbeiten Sie mit der Management-Node-UI

Übersicht über die Management-Node-UI

Mit dem Management Node UI (`https://<ManagementNodeIP>:442`) können Sie Änderungen an Netzwerk- und Cluster-Einstellungen vornehmen, Systemtests ausführen oder Systemdienstprogramme verwenden.

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

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

Weitere Informationen

- "Greifen Sie auf den Management-Node zu"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Konfigurieren der Meldungsüberwachung

Die Tools zur Überwachung von Warnmeldungen sind für das NetApp HCI-Warnungsüberwachung konfiguriert. Diese Tools werden nicht für SolidFire All-Flash-Storage konfiguriert oder verwendet. Das Ausführen der Tools für diese Cluster führt zu dem folgenden Fehler 405, der aufgrund der Konfiguration erwartet wird: `webUIParseError : Invalid response from server. 405`

Weitere Informationen zum Konfigurieren der Alarmüberwachung für NetApp HCI finden Sie unter "Konfigurieren der Meldungsüberwachung"

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

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

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

Aktualisieren der Netzwerkeinstellungen für den Management-Node

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

1. Öffnen Sie die Management-Node-UI pro Node.
2. Wählen Sie die Registerkarte **Netzwerkeinstellungen** aus.
3. Die folgenden Informationen anzeigen oder eingeben:

a. **Methode**: Wählen Sie eine der folgenden Methoden, um die Schnittstelle zu konfigurieren:
   - `loopback`: Zur Definition der IPv4-Loopback-Schnittstelle.
   - `manual`: Verwenden Sie diese Option, um Schnittstellen zu definieren, für die standardmäßig keine Konfiguration erfolgt.
   - `dhop`: Verwendung, um eine IP-Adresse über DHCP zu erhalten.
   - `static`: Zur Definition von Ethernet-Schnittstellen mit statisch zugewiesenen IPv4-Adressen.
b. **Verbindungsgeschwindigkeit**: Die Geschwindigkeit, die von der virtuellen NIC ausgehandelt wird.
c. **IPv4-Adresse**: Die IPv4-Adresse für das eth0-Netzwerk.
d. **IPv4-Subnetzmaske**: Adressenunterteilungen des IPv4-Netzwerks.
e. **IPv4 Gateway-Adresse**: Router-Netzwerkadresse zum Senden von Paketen aus dem lokalen Netzwerk.
f. **IPv6-Adresse**: Die IPv6-Adresse für das eth0-Netzwerk.
g. **IPv6 Gateway-Adresse**: Router-Netzwerkadresse zum Senden von Paketen aus dem lokalen Netzwerk.

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

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

Aktualisiert die Cluster-Einstellungen des Management-Node

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

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

Testen Sie die Einstellungen für den Management-Node

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

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

Weitere Informationen

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

Führen Sie Systemdienstprogramme vom Management-Node aus

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

Schritte

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

      Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

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

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

c. **Alle Support-Pakete löschen**: Löscht alle aktuellen Support-Bundles auf dem Management-Knoten.

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

   > Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

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

   > Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

Weitere Informationen

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

Arbeiten mit DER REST-API des Management-Node

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

Mit der integrierten REST API UI (`https://<ManagementNodeIP>/mnode`) können Sie APIs im Zusammenhang mit den Management-Node-Services ausführen oder

verstehen, einschließlich Proxy-Server-Konfiguration, Service-Level-Updates oder Asset-Management.

Aufgaben, die Sie mit REST-APIs durchführen können:

Autorisierung

- "Autorisierung zur Verwendung VON REST-APIs"

Konfiguration der Ressourcen

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

Asset Management

- "Vorhandene Controller-Assets können angezeigt oder bearbeitet werden"
- "Erstellen und Managen von Storage-Cluster-Assets"
- "Verwenden Sie die REST API, um die Protokolle des Element-Systems zu erfassen"
- "Überprüfen Sie die Betriebssystem- und Servicestversionen der Management-Nodes"
- "Abrufen von Protokollen von Managementservices"

Weitere Informationen

- "Greifen Sie auf den Management-Node zu"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Autorisierung zur Verwendung VON REST-APIs

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

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

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

Bevor Sie beginnen

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

API-Befehl

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

SCHRITTE DER REST API-UI

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

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

2. Wählen Sie **Autorisieren** Aus.

   Alternativ können Sie auf einem Sperrsymbol neben einer beliebigen Service-API wählen.

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

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

Weitere Informationen

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

Monitoring von Active IQ und NetApp

Sie können die Active IQ Storage-Überwachung aktivieren, wenn Sie dies bei der Installation oder einem Upgrade nicht bereits getan haben. Möglicherweise müssen Sie dieses Verfahren anwenden, wenn Sie SolidFire Active IQ nicht während der Installation für ein SolidFire All-Flash-Storage-System eingerichtet haben.

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

Bevor Sie beginnen

- Einige Funktionen in Active IQ, beispielsweise Quality of Service (QoS), erfordern Element 11.3 oder höher die ordnungsgemäße Funktion. Um sicherzustellen, dass Sie alle Active IQ-Funktionen nutzen können, empfiehlt NetApp Folgendes:
  - Im Storage Cluster wird die NetApp Element Software 11.3 oder höher ausgeführt.
  - Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.
- Sie haben Internetzugang. Der Active IQ Collector Service kann nicht von dunklen Standorten verwendet werden, die keine externe Verbindung haben.

Schritte

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

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

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

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

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

2. Telemetrie aktivieren:
   a. Greifen Sie auf die mnode Service API UI auf dem Management Node zu, indem Sie die Management

Node IP-Adresse gefolgt von `/mnode`:

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

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

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

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

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

3. Falls noch nicht geschehen, fügen Sie dem Management-Node bekannte Ressourcen eine vCenter Controller Ressource für NetApp Hybrid Cloud Control hinzu:

   Für NetApp Monitoring Services ist ein Controller-Asset erforderlich.

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

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

`ip` Ist die vCenter-IP-Adresse.

e. Wählen Sie **Ausführen**.

Weitere Informationen

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

Konfiguration von NetApp Hybrid Cloud Control für mehrere vCenter

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

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

Was Sie benötigen

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

Schritte

1. "Fügen Sie neue vCenters als Controller Assets hinzu" Zur Konfiguration des Management-Node.
2. Aktualisieren Sie die BestandsdienstAPI auf dem Managementknoten:

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

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

a. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
   i. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   ii. Geben Sie die Client-ID als `mnode-client`ein.
   iii. Wählen Sie **autorisieren**, um eine Sitzung zu starten.

iv. Schließen Sie das Fenster.

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

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

d. Wählen Sie **Ausführen**.

e. Kopieren Sie aus der Antwort die Installations-Asset(`"id"`-ID).

f. Wählen Sie in DER REST-API-UI **GET /installations/{id}** aus.

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

h. Setzen Sie die Aktualisierung auf `True`.

i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.

j. Wählen Sie **Ausführen**.

3. Aktualisieren Sie den Browser NetApp Hybrid Cloud Control, um die Änderungen anzuzeigen.

Weitere Informationen

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

Fügen Sie dem Management-Node eine Controller-Ressource hinzu

Mithilfe der REST API UI können Sie der Management-Node-Konfiguration eine Controller-Ressource hinzufügen.

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

Was Sie benötigen

- In Ihrer Cluster-Version wird die NetApp Element Software 11.3 oder höher ausgeführt.
- Sie haben einen Management-Node mit Version 11.3 oder höher implementiert.
- Sie haben eine neue NetApp HCC-Rolle in vCenter erstellt, um die Management-Node-Services-Ansicht auf reine NetApp Ressourcen zu begrenzen. Siehe "Erstellen einer NetApp HCC-Rolle in vCenter"

Schritte

1. Holen Sie sich die Basis-Asset-ID für die Installation:

a. Öffnen Sie die REST API-UI für den Bestandsdienst auf dem Managementknoten:

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

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

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

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

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

iv. Schließen Sie das Fenster.

c. Wählen Sie in DER REST API UI **GET /Installations** aus.

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

e. Wählen Sie **Ausführen**.

f. Kopieren Sie aus dem Antworttext von Code 200 die `id` für die Installation.

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

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

g. Wählen Sie in DER REST-API-UI **GET /installations/{id}** aus.

h. Wählen Sie **Probieren Sie es aus**.

i. Fügen Sie die Installations-Asset-ID in das Feld **id** ein.

j. Wählen Sie **Ausführen**.

k. Kopieren Sie aus der Antwort die Cluster-Controller-ID (`"controllerId"`) und speichern Sie sie zur Verwendung in einem späteren Schritt.

2. Um einer vorhandenen Basisinressource eine Controller-Unterressource hinzuzufügen, wählen Sie:

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

a. Öffnen Sie die MNODE-Service-REST-API-UI auf dem Management-Node:

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

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

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

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

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

iv. Schließen Sie das Fenster.

c. Wählen Sie **POST /Assets/{Asset_id}/Controllers** aus.

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

e. Geben Sie die übergeordnete Basis-Asset-ID in das Feld **Asset_id** ein.

f. Fügen Sie die erforderlichen Werte der Nutzlast hinzu.

g. Wählen Sie **Ausführen**.

Weitere Informationen

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

Erstellen und Managen von Storage-Cluster-Assets

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

Was Sie benötigen

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

Optionen für das Storage Cluster Asset Management

Wählen Sie eine der folgenden Optionen:

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

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

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

Schritte

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

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

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

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

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

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

d. Schließen Sie das Fenster.

3. Wählen Sie **GET /Installations**.
4. Wählen Sie **Probieren Sie es aus**.
5. Wählen Sie **Ausführen**.

   Die API gibt eine Liste aller bekannten Installationen zurück.

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

```
"installations": [
    {
      "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",
      "name": "my-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-UI für den Speicherdienst zu, indem Sie die Management-Node-IP-Adresse gefolgt von `/storage/1/`:

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

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

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

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

Fügen Sie eine neue Storage-Cluster-Ressource hinzu

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

Was Sie benötigen

- Sie haben den für alle Storage-Cluster kopiertStorage Cluster-ID und Installations-ID, die Sie hinzufügen möchten.
- Wenn Sie mehr als einen Storage Node hinzufügen, wissen Sie die Einschränkungen der Unterstützung für und mehrere Storage Cluster bereits zu lesen und zu verstehen"Autorisierende Cluster".

> Alle Benutzer, die auf dem autorisierenden Cluster definiert werden, werden als Benutzer auf allen anderen Clustern definiert, die an die NetApp Hybrid Cloud Control Instanz gebunden sind.

Schritte

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

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

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

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

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

6. Wählen Sie **Ausführen**.

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

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

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

Stellen Sie sicher, dass Sie die Schritte in befolgt habenRufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab, bevor Sie fortfahren.

Schritte

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

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

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

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

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

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

7. Wählen Sie **Ausführen**.

Löschen einer Speichercluster-Ressource

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

Stellen Sie sicher, dass Sie die Schritte in befolgt habenRufen Sie die Installations-ID und die Cluster-ID einer Storage-Cluster-Ressource ab, bevor Sie fortfahren.

Schritte

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

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

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

Bei Erfolg gibt die API eine leere Antwort zurück.

Weitere Informationen

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

Vorhandene Controller-Assets können angezeigt oder bearbeitet werden

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

Bevor Sie beginnen

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

Zugriff auf DIE REST-API für Managementservices

Schritte

1. Rufen Sie die REST-API-UI für Managementservices auf, indem Sie die Management-Node-IP-Adresse und dann `/vcenter/1/`:

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

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

Anzeigen gespeicherter Informationen zu vorhandenen Controllern

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

Schritte

1. Wählen Sie **GET /Compute/Controller** aus.
2. Wählen Sie **Probieren Sie es aus**.
3. Wählen Sie **Ausführen**.

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

4. Wenn Sie den Verbindungsstatus eines bestimmten Controllers wünschen, kopieren Sie die Controller-ID aus dem `id` Feld des Controllers in die Zwischenablage und lesen Sie Den Status eines vorhandenen Controllers anzeigen.

Den Status eines vorhandenen Controllers anzeigen

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

Schritte

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

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

Bearbeiten Sie die gespeicherten Eigenschaften eines Controllers

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

Schritte

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

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

5. Wählen Sie **Ausführen**.

   Die API gibt aktualisierte Controller-Informationen zurück.

Weitere Informationen

- "Fügen Sie dem Management-Node eine Controller-Ressource hinzu"
- "NetApp Element Plug-in für vCenter Server"
- "Dokumentation von SolidFire und Element Software"

Konfigurieren Sie einen Proxyserver

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

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

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

Bevor Sie beginnen

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

Schritte

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

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

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

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

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

6. Wählen Sie **Ausführen**.

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

Weitere Informationen

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

Überprüfen Sie die Betriebssystem- und Servicestversionen der Management-Nodes

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

Was Sie benötigen

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

Optionen

- API-Befehle
- SCHRITTE DER REST API-UI

API-Befehle

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

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

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

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

Sie können den vom API-Befehl verwendeten Träger finden `${TOKEN}`, wenn Sie "Autorisieren". Der Träger `${TOKEN}` ist in der Lockenantwort.

SCHRITTE DER REST API-UI

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

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

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

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

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

Weitere Informationen

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

Abrufen von Protokollen von Managementservices

Sie können mithilfe der REST API Protokolle von den Services abrufen, die auf dem Management-Node ausgeführt werden. Sie können Protokolle aus allen öffentlichen

Diensten abrufen oder bestimmte Dienste angeben und Abfrageparameter verwenden, um die Rückgabeergebnisse besser zu definieren.

Was Sie benötigen

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

Schritte

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

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

   - Für Managementservices ab Version 2.20.69:

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

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

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

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

     Verwenden Sie einen vernünftigen `since` Parameter, wenn Sie Protokolle mit größeren Zeitspannen erfassen.

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

     Verwenden Sie den `GET /services` Befehl, um Services auf dem Management-Node aufzulisten.

   - `stopped`: Auf eingestellt `true`, um Protokolle von angestoppten Diensten abzurufen.
6. Wählen Sie **Ausführen**.

7. Wählen Sie im Antwortkörper **Download** aus, um die Protokollausgabe zu speichern.

Weitere Informationen

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

Managen von Supportverbindungen

Zugriff auf Storage-Nodes mithilfe von SSH für die grundlegende Fehlerbehebung

Ab Element 12.5 können Sie das sfReadonly System-Konto auf den Storage-Nodes für eine grundlegende Fehlerbehebung nutzen. Sie können außerdem den Zugriff auf den Remote-Support-Tunnel für eine erweiterte Fehlerbehebung aktivieren und öffnen.

Das sfreadonly-Systemkonto ermöglicht den Zugriff auf grundlegende Linux-System- und Netzwerk-Fehlerbehebungsbefehle einschließlich ausführen `ping`.

> Sofern nicht vom NetApp Support beraten, werden Änderungen an diesem System nicht unterstützt, sodass Sie Ihren Support-Vertrag aufgeben und möglicherweise die Daten instabil oder unzugänglich machen können.

Bevor Sie beginnen

- **Schreibberechtigungen**: Stellen Sie sicher, dass Sie Schreibberechtigungen in das aktuelle Arbeitsverzeichnis haben.
- **(Optional) Generieren Sie Ihr eigenes Schlüsselpaar**: Laufen Sie `ssh-keygen` von Windows 10, MacOS, oder Linux Distribution. Dies ist eine einmalige Aktion, um ein Benutzerschlüsselpaar zu erstellen und kann für zukünftige Fehlerbehebungssitzungen verwendet werden. Möglicherweise möchten Sie Zertifikate verwenden, die mit Mitarbeiterkonten verknüpft sind, was auch in diesem Modell funktionieren würde.
- **SSH-Fähigkeit auf dem Management-Knoten aktivieren**: Um Remote-Zugriffsfunktionen im Management-Modus zu aktivieren, siehe "Diesem Thema". Für Managementservices ab Version 2.18 ist die Möglichkeit für den Remote-Zugriff auf dem Management-Node standardmäßig deaktiviert.
- **SSH-Fähigkeit auf dem Storage-Cluster aktivieren**: Um Remote-Zugriffsfunktionen auf den Storage-Cluster-Knoten zu aktivieren, siehe "Diesem Thema".
- **Firewall-Konfiguration**: Wenn sich Ihr Management-Knoten hinter einem Proxy-Server befindet, sind die folgenden TCP-Ports in der Datei sshd.config erforderlich:

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

Fehlerbehebungsoptionen

- Fehlerbehebung für einen Cluster-Node
- Fehlerbehebung für einen Cluster Node mit NetApp Support
- der nicht zum Cluster gehört

Fehlerbehebung für einen Cluster-Node

Sie können grundlegende Fehlerbehebungsmaßnahmen mit dem sfReadonly Systemkonto durchführen:

Schritte

1. SSH zum Management-Node mit Ihren Account-Anmeldedaten, die Sie beim Installieren der Management-Node-VM ausgewählt haben.
2. Wechseln Sie auf dem Management-Knoten zu `/sf/bin`.
3. Suchen Sie das passende Skript für Ihr System:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   SignSshKeys.ps1 ist abhängig von PowerShell 7 oder höher und SignSshKeys.py ist abhängig von Python 3.6.0 oder höher und dem "Anträgen-Modul".

   Das `SignSshKeys` Skript schreibt `user`, , `user.pub` und `user-cert.pub` Dateien in das aktuelle Arbeitsverzeichnis, die später vom Befehl verwendet werden `ssh`. Wenn dem Skript jedoch eine Public Key-Datei zur Verfügung gestellt wird, wird nur eine `<public_key>` Datei (mit dem Präfix der Public Key-Datei, die `<public_key>` an das Skript übergeben wird) in das Verzeichnis geschrieben.

4. Führen Sie das Skript auf dem Management-Node aus, um die SSH-Schlüsselkette zu generieren. Das Skript ermöglicht den SSH-Zugriff über das sfReadonly Systemkonto über alle Nodes im Cluster hinweg.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--publickey [public key path]
```

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

      Sie können entweder den abgekürzten oder den vollständigen Parameter verwenden.

      - **--ip: -i [ip-Adresse]**: IP-Adresse des Ziel-Knotens für die API, gegen die ausgeführt werden soll.
      - *--user: Cluster-Benutzer verwendet, um den API-Aufruf auszuführen.
      - **(Optional) --duration -d [hours]**: Die Dauer eines signierten Schlüssels sollte als Ganzzahl in Stunden gültig sein. Die Standardeinstellung ist 24 Stunden.
      - **(Optional) --publickey (öffentlicher Schlüsselpfad)**: Der Weg zu einem öffentlichen Schlüssel, wenn der Benutzer sich entscheidet, einen zu liefern.

   b. Vergleichen Sie Ihre Angaben mit dem folgenden Beispielbefehl. In diesem Beispiel `10.116.139.195` ist die IP des Speicher-Node, `admin` der Cluster-Benutzername und die Dauer der Schlüsselgültigkeit

beträgt zwei Stunden:

```
sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
2
```

c. Führen Sie den Befehl aus.

5. SSH an die Node-IPs:

```
ssh -i user sfreadonly@[node_ip]
```

Sie können grundlegende Linux-System- und Netzwerk-Fehlerbehebungsbefehle ausführen, wie `ping`, und andere schreibgeschützte Befehle.

6. (Optional) nach Abschluss der Fehlerbehebung erneut deaktivieren"Remote-Zugriffsfunktion".

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

Fehlerbehebung für einen Cluster Node mit NetApp Support

NetApp Support kann bei einer Systemkonto eine erweiterte Fehlerbehebung durchführen, sodass Techniker eine umfassendere Elementdiagnose durchführen können.

Schritte

1. SSH zum Management-Node mit Ihren Account-Anmeldedaten, die Sie beim Installieren der Management-Node-VM ausgewählt haben.
2. Führen Sie den rst-Befehl mit der Port-Nummer aus, die von NetApp Support gesendet wurde, um den Support-Tunnel zu öffnen:

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

   Der NetApp Support meldet sich mithilfe des Support-Tunnels am Management-Node an.

3. Wechseln Sie auf dem Management-Knoten zu `/sf/bin`.
4. Suchen Sie das passende Skript für Ihr System:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

SignSshKeys.ps1 ist abhängig von PowerShell 7 oder höher und SignSshKeys.py ist abhängig von Python 3.6.0 oder höher und dem "Anträgen-Modul".

Das `SignSshKeys` Skript schreibt `user`, , `user.pub` und `user-cert.pub` Dateien in das aktuelle Arbeitsverzeichnis, die später vom Befehl verwendet werden `ssh`. Wenn dem Skript jedoch eine Public Key-Datei zur Verfügung gestellt wird, wird nur eine `<public_key>` Datei (mit dem Präfix der Public Key-Datei, die `<public_key>` an das Skript übergeben wird) in das Verzeichnis geschrieben.

5. Führen Sie das Skript aus, um den SSH-Schlüsselbund mit dem Flag zu generieren `--sfadmin`. Das Skript ermöglicht SSH über alle Nodes hinweg.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--sfadmin
```

Um SSH als `--sfadmin` zu einem Cluster-Node zu erstellen, müssen Sie den SSH-Schlüsselbund mit einem mit `supportAdmin` Zugriff auf das Cluster generieren `--user`.

Um den Zugriff für Cluster-Administratorkonten zu konfigurieren `supportAdmin`, können Sie die Element UI oder die APIs verwenden:

- "Konfigurieren Sie den Zugriff auf „SupportAdmin“ über die Element UI"
- Konfigurieren Sie `supportAdmin` den Zugriff mithilfe von APIs und fügen Sie als `"access"` Typ in der API-Anforderung hinzu `"supportAdmin"`:
  - "Konfigurieren Sie den Zugriff auf „SupportAdmin“ für ein neues Konto"
  - "Konfigurieren Sie den Zugriff auf „SupportAdmin“ für ein vorhandenes Konto"

    Um denzu erhalten `clusterAdminID`, können Sie die API verwenden"ListenClusteradministratoren".

Um den Zugriff hinzuzufügen `supportAdmin`, müssen Sie über einen Clusteradministrator oder einen Administrator-Privileges verfügen.

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

   Sie können entweder den abgekürzten oder den vollständigen Parameter verwenden.

   - **--ip: -i [ip-Adresse]**: IP-Adresse des Ziel-Knotens für die API, gegen die ausgeführt werden soll.
   - *--user: Cluster-Benutzer verwendet, um den API-Aufruf auszuführen.
   - **(Optional) --duration -d [hours]**: Die Dauer eines signierten Schlüssels sollte als Ganzzahl in Stunden gültig sein. Die Standardeinstellung ist 24 Stunden.

b. Vergleichen Sie Ihre Angaben mit dem folgenden Beispielbefehl. In diesem Beispiel `192.168.0.1` ist die IP des Speicher-Node, `admin` der Cluster-Benutzername, die Dauer der Gültigkeit des Schlüssels beträgt zwei Stunden und `--sfadmin` ermöglicht den Zugriff auf den NetApp-Support-Node zur Fehlerbehebung:

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2
--sfadmin
```

c. Führen Sie den Befehl aus.

6. SSH an die Node-IPs:

```
ssh -i user sfadmin@[node_ip]
```

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

```
rst --killall
```

8. (Optional) nach Abschluss der Fehlerbehebung erneut deaktivieren"Remote-Zugriffsfunktion".

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

Fehlerbehebung für einen Node, der nicht zum Cluster gehört

Sie können grundlegende Fehlerbehebung für einen Node ausführen, der noch nicht zu einem Cluster hinzugefügt wurde. Sie können das sfReadonly System-Konto zu diesem Zweck mit oder ohne Hilfe von NetApp Unterstützung verwenden. Wenn ein Management-Node eingerichtet wurde, können Sie ihn für SSH verwenden und das angegebene Skript für diese Aufgabe ausführen.

1. Führen Sie auf einem Windows-, Linux- oder Mac-Computer mit installiertem SSH-Client das entsprechende Skript für Ihr von NetApp Support bereitgestellte System aus.
2. SSH an die Node-IP:

```
ssh -i user sfreadonly@[node_ip]
```

3. (Optional) nach Abschluss der Fehlerbehebung erneut deaktivieren"Remote-Zugriffsfunktion".

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

Weitere Informationen

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

Starten Sie eine Remote NetApp Support Sitzung

Falls Sie technischen Support für Ihr SolidFire All-Flash-Storage-System benötigen, kann

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

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

Bevor Sie beginnen

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

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

Schritte

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

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

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

```
rst --killall
```

- (Optional) Deaktivieren Sie "Remote-Zugriffsfunktion" erneut.

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

Weitere Informationen

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

Verwalten der SSH-Funktionalität auf dem Management-Node

Sie können den Status der SSH-Funktion auf dem Management-Node (mNode) mithilfe der REST-API deaktivieren, neu aktivieren oder bestimmen. Die SSH-Funktion "Zugriff

auf Session-Session (Remote Support Tunnel) durch NetApp Support"ist bei Management-Nodes, auf denen Management-Services 2.18 oder höher ausgeführt werden, standardmäßig deaktiviert.

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

Was Sie benötigen

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

Optionen

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

Sie können eine der folgenden Aufgaben nach Ihnen ausführen"Authentifizierung":

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

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

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

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

Schritte

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

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

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

API-Befehl

Für Management Services 2.18 oder höher:

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

Für Managementservices ab Version 2.17:

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

Sie können den vom API-Befehl verwendeten Träger finden `${TOKEN}`, wenn Sie "Autorisieren". Der Träger `${TOKEN}` ist in der Lockenantwort.

SCHRITTE DER REST API-UI

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

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

2. Wählen Sie **autorisieren** aus, und füllen Sie Folgendes aus:
   a. Geben Sie den Benutzernamen und das Passwort für den Cluster ein.
   b. Geben Sie die Client-ID als `mnode-client`ein.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie in DER REST API UI **PUT /settings/ssh** aus.
   a. Wählen Sie **Probieren Sie es aus**.
   b. Setzen Sie den Parameter **enabled** auf `false`, um SSH zu deaktivieren oder `true` die zuvor deaktivierte SSH-Funktion wieder zu aktivieren.
   c. Wählen Sie **Ausführen**.

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

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

API-Befehl

Für Management Services 2.18 oder höher:

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

Für Managementservices ab Version 2.17:

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

Sie können den vom API-Befehl verwendeten Träger finden `${TOKEN}`, wenn Sie "Autorisieren". Der Träger `${TOKEN}` ist in der Lockenantwort.

SCHRITTE DER REST API-UI

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

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

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

Weitere Informationen

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

Copyright-Informationen

Markeninformationen