



Managen von Supportverbindungen

HCI

NetApp
October 11, 2024

Inhalt

- Managen von Supportverbindungen 1
 - Starten Sie eine Remote NetApp Support Sitzung 1
 - Verwalten der SSH-Funktionalität auf dem Management-Node 2

Managen von Supportverbindungen

Starten Sie eine Remote NetApp Support Sitzung

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

Über diese Aufgabe

Sie können einen TCP-Port für eine SSH-Reverse-Tunnel-Verbindung mit NetApp Support öffnen. Über diese Verbindung kann sich NetApp Support beim Management Node einloggen. Wenn sich der Managementknoten hinter einem Proxyserver befindet, sind die folgenden TCP-Ports in der Datei `sshd.config` erforderlich:

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



Standardmäßig ist die Fähigkeit für den Remote-Zugriff auf dem Management-Node aktiviert. Informationen zum Deaktivieren der Remote-Zugriffsfunktion finden Sie unter "[Verwalten der SSH-Funktionalität auf dem Management-Node](#)". Sie können die Remote-Zugriffsfunktion bei Bedarf wieder aktivieren.

Schritte

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

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

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

```
rst --killall
```

Weitere Informationen

- "[NetApp Element Plug-in für vCenter Server](#)"
- "[Seite „NetApp HCI Ressourcen“](#)"

Verwalten der SSH-Funktionalität auf dem Management-Node

Sie können den Status der SSH-Funktion auf dem Management-Node (mNode) mithilfe der REST-API deaktivieren, neu aktivieren oder bestimmen. Die SSH-Funktion "[Zugriff auf Session-Session \(Remote Support Tunnel\) durch NetApp Support](#)" ist standardmäßig auf dem Management-Node aktiviert.

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

Was Sie benötigen

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

Optionen

- [Deaktivieren oder aktivieren Sie die SSH-Funktion auf dem Management-Node mithilfe der NetApp Hybrid Cloud Control UI](#)

Sie können eine der folgenden Aufgaben nach Ihnen ausführen "[Authentifizierung](#)":

- [Deaktiviert bzw. aktiviert die SSH-Funktion auf dem Management-Node mithilfe von APIs](#)
- [Ermitteln des Status der SSH-Funktion auf dem Management-Node mithilfe von APIs](#)

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

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



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

Schritte

1. Wählen Sie im Dashboard oben rechts das Optionsmenü aus und wählen Sie **Konfigurieren**.

2. Schalten Sie im Bildschirm **Support Access for Management Node** den Switch ein, um den Management-Node SSH zu aktivieren.
3. Nach Abschluss der Fehlerbehebung schalten Sie im Bildschirm **Support Access for Management Node** den Switch ein, um SSH des Management-Node zu deaktivieren.

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

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

API-Befehl

Für Management Services 2.18 oder höher:

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

Für Managementservices ab Version 2.17:

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



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

SCHRITTE DER REST API-UI

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

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

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

- b. Setzen Sie den Parameter **enabled** auf `false`, um SSH zu deaktivieren oder `true` die SSH-Funktion, die Sie zuvor deaktiviert haben, wieder zu aktivieren.
- c. Wählen Sie **Ausführen**.

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

Sie können ermitteln, ob die SSH-Funktion auf dem Management-Node mithilfe einer Management-Node-Service-API aktiviert ist. SSH ist auf dem Management-Node standardmäßig aktiviert.

API-Befehl

Für Management Services 2.18 oder höher:

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

Für Managementservices ab Version 2.17:

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



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

SCHRITTE DER REST API-UI

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

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

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

Weitere Informationen

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

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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