Managen von Supportverbindungen

Element Software

NetApp
March 01, 2023

Inhaltsverzeichnis

Managen von Supportverbindungen 1
Zugriff auf Storage-Nodes mithilfe von SSH für die grundlegende Fehlerbehebung 1
Starten Sie eine Remote NetApp Support Sitzung 6
Verwalten der SSH-Funktionalität auf dem Management-Node 7

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 die Ausführung grundlegender Befehle zur Fehlerbehebung im Linux-System und Netzwerk, einschließlich `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 `ssh-keygen` Aus 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-Funktion auf dem Management-Node aktivieren**: Um die Remote-Zugriffsfunktion im Verwaltungsmodus 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-Funktion auf dem Storage-Cluster aktivieren**: Um die Remote-Zugriffsfunktion 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 am Management-Node 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".
   >
   > Der `SignSshKeys` Skript-Schreibvorgänge `user`, `user.pub`, und `user-cert.pub` Dateien in das aktuelle Arbeitsverzeichnis, die später vom verwendet werden `ssh` Befehl. Wenn dem Skript jedoch eine öffentliche Schlüsseldatei zur Verfügung gestellt wird, ist nur a verfügbar `<public_key>` Datei (mit `<public_key>` Ersetzt durch das Präfix der in das Skript übergebenen öffentlichen Schlüsseldatei) 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` Die IP des Storage-Nodes `admin` Ist der Cluster-Benutzername und die Dauer der Schlüsselgültigkeit 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 wie ausführen `ping`, Und anderen schreibgeschützten Befehlen.

6. (Optional) Deaktivieren "Remote-Zugriffsfunktion" Nach Abschluss der Fehlerbehebung 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.

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 am Management-Node 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".

Der `SignSshKeys` Skript-Schreibvorgänge `user`, `user.pub`, und `user-cert.pub` Dateien in das aktuelle Arbeitsverzeichnis, die später vom verwendet werden `ssh` Befehl. Wenn dem Skript jedoch eine öffentliche Schlüsseldatei zur Verfügung gestellt wird, ist nur a verfügbar `<public_key>` Datei (mit `<public_key>` Ersetzt durch das Präfix der in das Skript übergebenen öffentlichen Schlüsseldatei) wird in das Verzeichnis geschrieben.

5. Führen Sie das Skript aus, um die SSH-Schlüsselkette mit dem zu generieren `--sfadmin` Flagge. Das Skript ermöglicht SSH über alle Nodes hinweg.

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

Für SSH als `--sfadmin` Um einen Cluster-Knoten zu erhalten, müssen Sie die SSH-Schlüsselanhänger mit einem generieren `--user` Mit `supportAdmin` Zugriff auf das Cluster.

Zu konfigurieren `supportAdmin` Zugriff für Cluster-Administratorkonten können Sie die Element UI oder die APIs verwenden:

- "Konfigurieren Sie den Zugriff auf „SupportAdmin“ über die Element UI"
- Konfigurieren `supportAdmin` Zugriff über APIs und Hinzufügen `"supportAdmin"` Als der `"access"` Geben Sie die API-Anforderung ein:
  - "Konfigurieren Sie den Zugriff auf „SupportAdmin“ für ein neues Konto"
  - "Konfigurieren Sie den Zugriff auf „SupportAdmin“ für ein vorhandenes Konto"

    Um die zu bekommen `clusterAdminID`, Sie können die verwenden "ListenClusteradministratoren" API:

Hinzufügen `supportAdmin` Zugriff: Sie müssen über Cluster-Administrator- oder Administratorrechte 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` Die IP des Storage-Nodes `admin` Ist der Cluster-Benutzername, die Schlüsseldauer beträgt zwei Stunden, und `--sfadmin` Ermöglicht NetApp Support Node-Zugriff 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) Deaktivieren "Remote-Zugriffsfunktion" Nach Abschluss der Fehlerbehebung 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.

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) Deaktivieren "Remote-Zugriffsfunktion" Nach Abschluss der Fehlerbehebung 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"
- "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 Fernzugriffsfunktionen 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 "Remote-Zugriffsfunktion" Ein weiteres Jahr in der

> 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 „SolidFire und Element 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. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Knoten, die Management-Services 2.18 oder höher ausführen, 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 NetApp Hybrid Cloud Control UI zu verwenden, haben Sie Ihr aktualisiert "Management Services-Bundle" Auf Version 2.20.69 oder höher.
  - Um die REST API-UI zu verwenden, haben Sie das aktualisiert "Management Services-Bundle" Auf Version 2.17.

Optionen

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

Nach der Durchführung können Sie eine der folgenden Aufgaben 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. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Knoten, die Management-Services 2.18 oder höher ausführen, 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 über SSH für ein Storage-Cluster zu aktivieren oder zu deaktivieren, müssen Sie die 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. SSH-Funktion, die bietet "Zugriff auf Session-Session (Remote Support Tunnel) durch NetApp Support" Ist auf Management-Knoten, die Management-Services 2.18 oder höher ausführen, 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}"
```

Ihr könnt den Träger finden `${TOKEN}` Wird von dem API-Befehl verwendet, wenn Sie "Autorisieren". Der Träger `${TOKEN}` Ist in der Curl-Antwort.

SCHRITTE DER REST API-UI

1. Rufen Sie die REST-API-UI für den API-Service des Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/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 ein `mnode-client`.
   c. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie in DER REST API-Benutzeroberfläche **PUT /settings/ssh** aus.

a. Wählen Sie **Probieren Sie es aus**.

b. Legen Sie den Parameter **Enabled** auf fest `false` Um SSH oder zu deaktivieren `true` Um 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}"
```

Ihr könnt den Träger finden `${TOKEN}` Wird von dem API-Befehl verwendet, wenn Sie "Autorisieren". Der Träger `${TOKEN}` Ist in der Curl-Antwort.

SCHRITTE DER REST API-UI

1. Rufen Sie die REST-API-UI für den API-Service des Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/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 ein `mnode-client`.

   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 „SolidFire und Element Ressourcen“"