Supportverbindungen verwalten

Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/de-de/element-software-128/mnode/task_mnode_enable_node_troubleshooting_sessions.html on November 12, 2025. Always check docs.netapp.com for the latest.

Inhalt

Supportverbindungen verwalten

Zugriff auf Speicherknoten über SSH zur grundlegenden Fehlerbehebung

Ab Element 12.5 können Sie das sfreadonly-Systemkonto auf den Speicherknoten für grundlegende Fehlerbehebungen verwenden. Sie können außerdem den Remote-Support-Tunnelzugriff für den NetApp Support aktivieren und öffnen, um eine erweiterte Fehlerbehebung zu ermöglichen.

Das Systemkonto „sfreadonly“ ermöglicht den Zugriff auf die Ausführung grundlegender Befehle zur Fehlerbehebung im Linux-System und Netzwerk, einschließlich `ping` Die

> Sofern nicht vom NetApp -Support empfohlen, werden jegliche Änderungen an diesem System nicht unterstützt, führen zum Erlöschen Ihres Supportvertrags und können Instabilität oder den Verlust der Datenverfügbarkeit zur Folge haben.

Bevor Sie beginnen

- **Schreibberechtigungen**: Überprüfen Sie, ob Sie Schreibberechtigungen für das aktuelle Arbeitsverzeichnis besitzen.
- **(Optional) Generieren Sie Ihr eigenes Schlüsselpaar**: Ausführen `ssh-keygen` von Windows 10, MacOS oder Linux-Distribution. Dies ist eine einmalige Aktion zur Erstellung eines Benutzerschlüsselpaares und kann für zukünftige Fehlerbehebungssitzungen wiederverwendet werden. Sie könnten Zertifikate verwenden, die mit Mitarbeiterkonten verknüpft sind; das würde in diesem Modell ebenfalls funktionieren.
- **SSH-Funktionalität auf dem Management-Knoten aktivieren**: Informationen zur Aktivierung der Fernzugriffsfunktionalität im Management-Modus finden Sie hier."dieses Thema" Die Bei Managementdiensten ab Version 2.18 ist die Möglichkeit des Fernzugriffs auf dem Managementknoten standardmäßig deaktiviert.
- **SSH-Funktionalität auf dem Speichercluster aktivieren**: Informationen zur Aktivierung der Fernzugriffsfunktionalität auf den Knoten des Speicherclusters finden Sie hier."dieses Thema" Die
- **Firewall-Konfiguration**: Befindet sich Ihr Management-Knoten hinter einem Proxy-Server, sind die folgenden TCP-Ports in der sshd.config-Datei erforderlich:

TCP-Port	Beschreibung	Verbindungsrichtung
443	API-Aufrufe/HTTPS für Reverse-Port-Weiterleitung über einen offenen Support-Tunnel zur Web-UI	Managementknoten zu Speicherknoten
22	SSH-Anmeldezugriff	Managementknoten zu Speicherknoten oder von Speicherknoten zu Managementknoten

Optionen zur Fehlerbehebung

- Fehlerbehebung an einem Clusterknoten
- Fehlerbehebung an einem Clusterknoten mit Hilfe des NetApp Supports

- der nicht Teil des Clusters ist

Fehlerbehebung an einem Clusterknoten

Sie können grundlegende Fehlerbehebungen mithilfe des Systemkontos sfreadonly durchführen:

Schritte

1. Stellen Sie eine SSH-Verbindung zum Management-Knoten her, indem Sie die Anmeldeinformationen Ihres Kontos verwenden, die Sie bei der Installation der Management-Knoten-VM ausgewählt haben.
2. Gehen Sie auf dem Verwaltungsknoten zu `/sf/bin` Die
3. Suchen Sie das passende Skript für Ihr System:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   SignSshKeys.ps1 benötigt PowerShell 7 oder höher, und SignSshKeys.py benötigt Python 3.6.0 oder höher. "Anforderungsmodul" Die

   Der `SignSshKeys` Skript schreibt `user` , `user.pub` , Und `user-cert.pub` Dateien in das aktuelle Arbeitsverzeichnis, die später von der `ssh` Befehl. Wird dem Skript jedoch eine Datei mit einem öffentlichen Schlüssel bereitgestellt, so wird nur ein `<public_key>` Datei (mit `<public_key>` (ersetzt durch das Präfix der an das Skript übergebenen öffentlichen Schlüsseldatei) wird in das Verzeichnis geschrieben.

4. Führen Sie das Skript auf dem Management-Knoten aus, um den SSH-Schlüsselbund zu generieren. Das Skript ermöglicht den SSH-Zugriff über das Systemkonto sfreadonly auf allen Knoten im Cluster.

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

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

      Sie können entweder die abgekürzte oder die ausgeschriebene Form des Parameters verwenden.

      - **--ip | -i [IP-Adresse]**: IP-Adresse des Zielknotens, auf dem die API ausgeführt werden soll.
      - **--user | -u [Benutzername]**: Cluster-Benutzer, der zum Ausführen des API-Aufrufs verwendet wird.
      - **(Optional) --duration | -d [Stunden]**: Die Dauer, für die ein signierter Schlüssel gültig bleiben soll, als ganze Zahl in Stunden. Der Standardwert beträgt 24 Stunden.
      - **(Optional) --publickey | -k [Pfad zum öffentlichen Schlüssel]**: Der Pfad zu einem öffentlichen Schlüssel, falls der Benutzer einen solchen angeben möchte.

   b. Vergleichen Sie Ihre Eingabe mit dem folgenden Beispielbefehl. In diesem Beispiel `10.116.139.195` ist die IP-Adresse des Speicherknotens, `admin` ist der Cluster-Benutzername, und die Gültigkeitsdauer des Schlüssels beträgt zwei Stunden:

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

c. Führe den Befehl aus.

5. SSH-Verbindung zu den Knoten-IPs:

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

Sie werden in der Lage sein, grundlegende Befehle zur Fehlerbehebung im Linux-System und Netzwerk auszuführen, wie zum Beispiel: `ping` und andere schreibgeschützte Befehle.

6. (Optional) Deaktivieren"Fernzugriffsfunktionalität" erneut, nachdem die Fehlersuche abgeschlossen ist.

SSH bleibt auf dem Management-Knoten aktiviert, solange Sie es nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Knoten auch nach Updates und Upgrades erhalten, bis sie manuell deaktiviert wird.

Fehlerbehebung an einem Clusterknoten mit Hilfe des NetApp Supports

Der NetApp -Support kann mit einem Systemkonto, das es einem Techniker ermöglicht, detailliertere Element-Diagnosen durchzuführen, eine erweiterte Fehlerbehebung vornehmen.

Schritte

1. Stellen Sie eine SSH-Verbindung zum Management-Knoten her, indem Sie die Anmeldeinformationen Ihres Kontos verwenden, die Sie bei der Installation der Management-Knoten-VM ausgewählt haben.
2. Führen Sie den Befehl „rst“ mit der von NetApp Support übermittelten Portnummer aus, um den Support-Tunnel zu öffnen:

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

   Der NetApp -Support meldet sich über den Support-Tunnel an Ihrem Management-Knoten an.

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

SignSshKeys.ps1 benötigt PowerShell 7 oder höher, und SignSshKeys.py benötigt Python 3.6.0 oder höher. "Anforderungsmodul" Die

Der `SignSshKeys` Skript schreibt `user` , `user.pub` , Und `user-cert.pub` Dateien in das aktuelle Arbeitsverzeichnis, die später von der `ssh` Befehl. Wird dem Skript jedoch eine Datei mit einem öffentlichen Schlüssel bereitgestellt, so wird nur ein `<public_key>` Datei (mit `<public_key>` (ersetzt durch das Präfix der an das Skript übergebenen öffentlichen Schlüsseldatei) wird in das Verzeichnis geschrieben.

5. Führen Sie das Skript aus, um den SSH-Schlüsselbund mit dem `--sfadmin` Flagge. Das Skript aktiviert SSH auf allen Knoten.

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

Um sich per SSH anzumelden `--sfadmin` Für einen Clusterknoten müssen Sie den SSH-Schlüsselbund mithilfe eines `--user` mit `supportAdmin` Zugriff auf den Cluster.

Zum Konfigurieren `supportAdmin` Für den Zugriff auf Cluster-Administratorkonten können Sie die Element-Benutzeroberfläche oder APIs verwenden:

- "Konfigurieren Sie den „supportAdmin“-Zugriff über die Element-Benutzeroberfläche."
- Konfigurieren `supportAdmin` Zugriff durch Verwendung von APIs und Hinzufügen `"supportAdmin"` als die `"access"` Geben Sie Folgendes in die API-Anfrage ein:
  - "Konfigurieren Sie den „supportAdmin“-Zugriff für ein neues Konto."
  - "Konfigurieren Sie den „supportAdmin“-Zugriff für ein bestehendes Konto"

    Um die `clusterAdminID` Sie können die"ListClusterAdmins" API.

Um hinzuzufügen `supportAdmin` Für den Zugriff benötigen Sie Cluster-Administrator- oder Administratorrechte.

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

Sie können entweder die abgekürzte oder die ausgeschriebene Form des Parameters verwenden.

- **--ip | -i [IP-Adresse]**: IP-Adresse des Zielknotens, auf dem die API ausgeführt werden soll.
- **--user | -u [Benutzername]**: Cluster-Benutzer, der zum Ausführen des API-Aufrufs verwendet wird.
- **(Optional) --duration | -d [Stunden]**: Die Dauer, für die ein signierter Schlüssel gültig bleiben soll, als ganze Zahl in Stunden. Der Standardwert beträgt 24 Stunden.

b. Vergleichen Sie Ihre Eingabe mit dem folgenden Beispielbefehl. In diesem Beispiel `192.168.0.1` ist die IP-Adresse des Speicherknotens, `admin` ist der Cluster-Benutzername, die Gültigkeitsdauer des Schlüssels beträgt zwei Stunden, und `--sfadmin` Ermöglicht den Zugriff auf den NetApp -Supportknoten zur Fehlerbehebung:

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

c. Führe den Befehl aus.

6. SSH-Verbindung zu den Knoten-IPs:

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

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

   ```
   rst --killall
   ```

8. (Optional) Deaktivieren"Fernzugriffsfunktionalität" erneut, nachdem die Fehlersuche abgeschlossen ist.

> SSH bleibt auf dem Management-Knoten aktiviert, solange Sie es nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Knoten auch nach Updates und Upgrades erhalten, bis sie manuell deaktiviert wird.

Fehlerbehebung an einem Knoten, der nicht Teil des Clusters ist

Sie können grundlegende Fehlerbehebungsmaßnahmen an einem Knoten durchführen, der noch nicht zu einem Cluster hinzugefügt wurde. Sie können hierfür das Systemkonto „sfreadonly“ mit oder ohne Unterstützung des NetApp -Supports verwenden. Wenn Sie einen Management-Knoten eingerichtet haben, können Sie diesen für SSH verwenden und das für diese Aufgabe bereitgestellte Skript ausführen.

1. Führen Sie von einem Windows-, Linux- oder Mac-Rechner mit installiertem SSH-Client das für Ihr System geeignete Skript aus, das Ihnen vom NetApp Support zur Verfügung gestellt wird.
2. SSH-Verbindung zur Knoten-IP herstellen:

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

3. (Optional) Deaktivieren"Fernzugriffsfunktionalität" erneut, nachdem die Fehlersuche abgeschlossen ist.

> SSH bleibt auf dem Management-Knoten aktiviert, solange Sie es nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Knoten auch nach Updates und Upgrades erhalten, bis sie manuell deaktiviert wird.

Weitere Informationen

- "NetApp Element Plug-in für vCenter Server"
- "NetApp HCI Dokumentation"

Starten Sie eine NetApp Remote-Supportsitzung

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

Sie können einen TCP-Port für eine SSH-Reverse-Tunnel-Verbindung mit dem NetApp -Support öffnen. Diese Verbindung ermöglicht es dem NetApp -Support, sich in Ihren Management-Knoten einzuloggen.

Bevor Sie beginnen

- Bei Managementdiensten ab Version 2.18 ist die Möglichkeit des Fernzugriffs auf dem Managementknoten standardmäßig deaktiviert. Informationen zur Aktivierung der Fernzugriffsfunktionalität finden Sie unter "SSH-Funktionalität auf dem Management-Knoten verwalten" Die
- Wenn sich Ihr Management-Knoten hinter einem Proxy-Server befindet, sind die folgenden TCP-Ports in der sshd.config-Datei erforderlich:

TCP-Port	Beschreibung	Verbindungsrichtung
443	API-Aufrufe/HTTPS für Reverse-Port-Weiterleitung über einen offenen Support-Tunnel zur Web-UI	Managementknoten zu Speicherknoten
22	SSH-Anmeldezugriff	Managementknoten zu Speicherknoten oder von Speicherknoten zu Managementknoten

Schritte

- Melden Sie sich an Ihrem Management-Knoten an und öffnen Sie eine Terminal-Sitzung.
- Geben Sie auf Aufforderung 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 "Fernzugriffsfunktionalität" wieder.

> SSH bleibt auf dem Management-Knoten aktiviert, solange Sie es nicht deaktivieren. Die SSH-fähige Konfiguration bleibt auf dem Management-Knoten auch nach Updates und Upgrades erhalten, bis sie manuell deaktiviert wird.

Weitere Informationen

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

SSH-Funktionalität auf dem Management-Knoten verwalten

Sie können die SSH-Funktionalität auf dem Management-Knoten (mNode) mithilfe der REST-API deaktivieren, wieder aktivieren oder deren Status ermitteln. SSH-Funktionalität, die Folgendes bietet"NetApp Support Remote Support Tunnel (RST) Sitzungszugriff" ist standardmäßig deaktiviert auf Management-Knoten, auf denen Management-Dienste 2.18 oder höher ausgeführt werden.

Ab Management Services 2.20.69 können Sie die SSH-Funktionalität auf dem Management-Knoten über die NetApp Hybrid Cloud Control-Benutzeroberfläche aktivieren und deaktivieren.

Was du brauchst

- * NetApp Hybrid Cloud Control-Berechtigungen*: Sie verfügen über Administratorrechte.
- **Cluster-Administratorberechtigungen**: Sie verfügen über Administratorrechte für den Speichercluster.
- **Element-Software**: Auf Ihrem Cluster läuft die NetApp Element -Software 11.3 oder höher.
- **Management-Knoten**: Sie haben einen Management-Knoten mit Version 11.3 oder höher bereitgestellt.
- **Aktualisierungen der Managementdienste**:
  - Um die NetApp Hybrid Cloud Control-Benutzeroberfläche zu verwenden, müssen Sie Ihre "Management-Servicepaket" auf Version 2.20.69 oder höher.
  - Um die REST-API-Benutzeroberfläche zu verwenden, haben Sie Ihre "Management-Servicepaket" auf Version 2.17.

Optionen

- Deaktivieren oder aktivieren Sie die SSH-Funktionalität auf dem Management-Knoten über die NetApp Hybrid Cloud Control-Benutzeroberfläche.

Sie können nach dem"authentifizieren" :

- Deaktivieren oder aktivieren Sie die SSH-Funktionalität auf dem Verwaltungsknoten mithilfe von APIs.
- Ermitteln Sie den Status der SSH-Funktionalität auf dem Management-Knoten mithilfe von APIs.

Deaktivieren oder aktivieren Sie die SSH-Funktionalität auf dem Management-Knoten über die NetApp Hybrid Cloud Control-Benutzeroberfläche.

Sie können die SSH-Funktionalität auf dem Management-Knoten deaktivieren oder wieder aktivieren. SSH-Funktionalität, die Folgendes bietet"NetApp Support Remote Support Tunnel (RST) Sitzungszugriff" ist standardmäßig deaktiviert auf Management-Knoten, auf denen Management-Dienste 2.18 oder höher ausgeführt werden. Das Deaktivieren von SSH beendet oder trennt keine bestehenden SSH-Client-Sitzungen zum Management-Knoten. Wenn Sie SSH deaktivieren und es zu einem späteren Zeitpunkt wieder aktivieren möchten, können Sie dies über die NetApp Hybrid Cloud Control-Benutzeroberfläche tun.

Um den Supportzugriff per SSH für einen Speichercluster zu aktivieren oder zu deaktivieren, müssen Sie Folgendes verwenden:"Element UI Cluster-Einstellungsseite" Die

Schritte

1. Wählen Sie im Dashboard oben rechts das Optionsmenü und anschließend **Konfigurieren**.
2. Im Bildschirm **Supportzugriff für Management-Knoten** den Schalter umlegen, um SSH für den Management-Knoten zu aktivieren.
3. Nachdem Sie die Fehlerbehebung abgeschlossen haben, schalten Sie im Bildschirm **Supportzugriff für Management-Knoten** den Schalter um, um den SSH-Zugriff auf den Management-Knoten zu deaktivieren.

Deaktivieren oder aktivieren Sie die SSH-Funktionalität auf dem Verwaltungsknoten mithilfe von APIs.

Sie können die SSH-Funktionalität auf dem Management-Knoten deaktivieren oder wieder aktivieren. SSH-Funktionalität, die Folgendes bietet"NetApp Support Remote Support Tunnel (RST) Sitzungszugriff" ist standardmäßig deaktiviert auf Management-Knoten, auf denen Management-Dienste 2.18 oder höher ausgeführt werden. Das Deaktivieren von SSH beendet oder trennt keine bestehenden SSH-Client-Sitzungen zum Management-Knoten. Wenn Sie SSH deaktivieren und es zu einem späteren Zeitpunkt wieder aktivieren möchten, können Sie dies mit derselben 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 Management-Dienste 2.17 oder früher:

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

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

REST-API-UI-Schritte

1. Greifen Sie auf die REST-API-Benutzeroberfläche für den Management-Node-API-Dienst zu, indem Sie die IP-Adresse des Management-Nodes gefolgt von eingeben. `/mnode/` :

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

2. Wählen Sie **Autorisieren** und führen Sie die folgenden Schritte aus:
   a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
   b. Geben Sie die Client-ID ein als `mnode-client` Die
   c. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie in der REST-API-Benutzeroberfläche **PUT /settings/ssh** aus.
   a. Wählen Sie **Ausprobieren**.
   b. Setzen Sie den Parameter **aktiviert** auf `false` SSH deaktivieren oder `true` um die zuvor deaktivierte SSH-Funktionalität wieder zu aktivieren.
   c. Wählen Sie **Ausführen**.

Ermitteln Sie den Status der SSH-Funktionalität auf dem Management-Knoten mithilfe von APIs.

Ob die SSH-Funktionalität auf dem Management-Knoten aktiviert ist, können Sie über eine Management-Knoten-Service-API feststellen. SSH ist auf Management-Knoten, auf denen Management-Dienste der Version 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 Management-Dienste 2.17 oder früher:

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

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

REST-API-UI-Schritte

1. Greifen Sie auf die REST-API-Benutzeroberfläche für den Management-Node-API-Dienst zu, indem Sie die IP-Adresse des Management-Nodes gefolgt von eingeben. `/mnode/` :

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

2. Wählen Sie **Autorisieren** und führen Sie die folgenden Schritte aus:
   a. Geben Sie den Cluster-Benutzernamen und das Passwort ein.
   b. Geben Sie die Client-ID ein als `mnode-client` Die
   c. Wählen Sie **Autorisieren**, um eine Sitzung zu starten.
   d. Schließen Sie das Fenster.
3. Wählen Sie in der REST-API-Benutzeroberfläche **GET /settings/ssh** aus.
   a. Wählen Sie **Ausprobieren**.
   b. Wählen Sie **Ausführen**.

Weitere Informationen

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

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT 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, BEISPIELHAFTE 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 IRGENDEINER 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.