



# **Konsolenagenten verwalten**

## **NetApp Console setup and administration**

NetApp

January 23, 2026

This PDF was generated from <https://docs.netapp.com/de-de/console-setup-admin/task-agent-vm-config.html> on January 23, 2026. Always check docs.netapp.com for the latest.

# Inhalt

Konsolenagenten verwalten .....	1
Verwalten Sie einen VCenter- oder ESXi-Host für den Konsolenagenten .....	1
Zugriff auf die VM-Wartungskonsole .....	1
Installieren Sie ein CA-signiertes Zertifikat für den webbasierten Konsolenzugriff .....	4
Installieren eines HTTPS-Zertifikats .....	4
Erneuern Sie das HTTPS-Zertifikat der Konsole .....	6
Konfigurieren eines Konsolenagenten zur Verwendung eines Proxyservers .....	6
Unterstützte Konfigurationen .....	7
Aktivieren Sie einen expliziten Proxy auf einem Konsolenagenten .....	7
Aktivieren Sie einen transparenten Proxy für einen Konsolenagenten .....	8
Aktualisieren Sie den Proxy des Konsolenagenten, wenn dieser den Zugriff auf das Internet verliert . . .	9
Aktivieren Sie den direkten API-Verkehr .....	9
Fehlerbehebung beim Konsolen-Agent .....	9
Häufige Fehlermeldungen und Lösungen .....	10
Überprüfen Sie den Status des Konsolenagenten .....	11
Anzeigen der Konsolen-Agent-Version .....	11
Überprüfen des Netzwerkzugriffs .....	11
Probleme bei der Installation des Konsolenagenten .....	12
Arbeiten Sie mit dem NetApp Support .....	13
Beheben von Downloadfehlern bei Verwendung eines Google Cloud NAT-Gateways .....	14
Holen Sie sich Hilfe von der NetApp Knowledge Base .....	14
Deinstallieren und Entfernen eines Konsolenagenten .....	14
Deinstallieren Sie den Agenten, wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden .....	15
Entfernen von Konsolenagenten aus der Konsole .....	15

# Konsolenagenten verwalten

## Verwalten Sie einen VCenter- oder ESXi-Host für den Konsolenagenten

Sie können nach der Bereitstellung des Konsolenagenten Änderungen an Ihrem vorhandenen VCenter- oder ESXi-Host vornehmen. Sie können beispielsweise die CPU oder den RAM der VM-Instanz erhöhen, die den Konsolenagenten hostet.

Führen Sie diese Wartungsaufgaben mithilfe der VM-Webkonsole durch:

- Erhöhen Sie die Festplattengröße
- Starten Sie den Agenten neu
- Aktualisieren statischer Routen
- Suchdomänen aktualisieren

### Einschränkungen

Das Upgrade des Agenten über die Konsole wird noch nicht unterstützt. Darüber hinaus können Sie nur Informationen zur IP-Adresse, zum DNS und zu Gateways anzeigen.

## Zugriff auf die VM-Wartungskonsole

Sie können vom VSphere-Client aus auf die Wartungskonsole zugreifen.

### Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.

### Ändern Sie das Kennwort des Wartungsbenedutzers

Sie können das Passwort für die `maint` Benutzer.

### Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `1` , um die `System Configuration` Speisekarte.
6. Eingeben `1` um das Wartungsbenedutzerkennwort zu ändern und den Anweisungen auf dem Bildschirm zu

folgen.

## Erhöhen Sie die CPU oder den RAM der VM-Instanz

Sie können die CPU oder den RAM der VM-Instanz erhöhen, die den Konsolenagenten hostet.

Bearbeiten Sie die VM-Instanzeinstellungen in Ihrem VCenter- oder ESXi-Host und wenden Sie die Änderungen dann mit der Wartungskonsole an.

### Schritte im VSphere-Client

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Klicken Sie mit der rechten Maustaste auf die VM-Instanz und wählen Sie **Einstellungen bearbeiten**.
4. Erhöhen Sie den für die Partition /opt oder /var verwendeten Festplattenspeicher.
  - a. Wählen Sie **Festplatte 2**, um den für /opt verwendeten Festplattenspeicher zu erhöhen.
  - b. Wählen Sie **Festplatte 3**, um den für /var verwendeten Festplattenspeicher zu erhöhen.
5. Speichern Sie Ihre Änderungen.

### Schritte in der Wartungskonsole

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `1 to view the `System Configuration Speisekarte`.
6. Eingeben `2` und folgen Sie den Anweisungen auf dem Bildschirm. Die Konsole sucht nach neuen Einstellungen und vergrößert die Partitionen.

## Netzwerkeinstellungen für die Agent-VM anzeigen

Zeigen Sie die Netzwerkeinstellungen für die Agent-VM im VSphere-Client an, um Netzwerkprobleme zu bestätigen oder zu beheben. Sie können die folgenden Netzwerkeinstellungen nur anzeigen (nicht aktualisieren): IP-Adresse und DNS-Details.

### Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2`, um die `Network Configuration Speisekarte`.
6. Geben Sie eine Zahl zwischen 1 und 6 ein, um die entsprechenden Netzwerkeinstellungen anzuzeigen.

## Aktualisieren Sie die statischen Routen für die Agent-VM

Fügen Sie nach Bedarf statische Routen für die Agent-VM hinzu, aktualisieren oder entfernen Sie sie.

### Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2`, um die `Network Configuration` Speisekarte.
6. Eingeben `7` um statische Routen zu aktualisieren und den Anweisungen auf dem Bildschirm zu folgen.
7. Drücken Sie die Eingabetaste.
8. Nehmen Sie optional weitere Änderungen vor.
9. Eingeben `9` um Ihre Änderungen zu übernehmen.

## Aktualisieren der Domänensucheinstellungen für die Agent-VM

Sie können die Suchdomäneneinstellungen für die Agent-VM aktualisieren.

### Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben `2``, um die `Network Configuration` Speisekarte.
6. Eingeben `8` um die Domänensucheinstellungen zu aktualisieren und den Anweisungen auf dem Bildschirm zu folgen.
7. Drücken Sie die Eingabetaste.
8. Nehmen Sie optional weitere Änderungen vor.
9. Eingeben `9` um Ihre Änderungen zu übernehmen.

## Zugriff auf die Diagnosetools des Agenten

Greifen Sie auf Diagnosetools zu, um Probleme mit dem Konsolenagenten zu beheben. Der NetApp -Support fordert Sie möglicherweise bei der Fehlerbehebung dazu auf.

### Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.

4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben 3 um das Menü „Support und Diagnose“ anzuzeigen.
6. Eingeben 1 um auf die Diagnosetools zuzugreifen und den Anweisungen auf dem Bildschirm zu folgen. + Sie können beispielsweise überprüfen, ob alle Agentendienste ausgeführt werden. "[Überprüfen Sie den Status des Konsolenagenten](#)".

### Fernzugriff auf die Diagnosetools des Agenten

Mit einem Tool wie Putty können Sie remote auf Diagnosetools zugreifen. Aktivieren Sie den SSH-Zugriff auf die Agent-VM, indem Sie ein Einmalkennwort zuweisen.

Der SSH-Zugriff ermöglicht erweiterte Terminalfunktionen wie Kopieren und Einfügen.

#### Schritte

1. Öffnen Sie den VSphere-Client und melden Sie sich bei Ihrem VCenter an.
2. Wählen Sie die VM-Instanz aus, die den Konsolenagenten hostet.
3. Wählen Sie **Webkonsole starten**.
4. Melden Sie sich bei der VM-Instanz mit dem Benutzernamen und dem Kennwort an, die Sie beim Erstellen der VM-Instanz angegeben haben. Der Benutzername ist `maint` und das Kennwort ist das, das Sie beim Erstellen der VM-Instanz angegeben haben.
5. Eingeben 3 , um die `Support and Diagnostics` Speisekarte.
6. Eingeben 2 um auf die Diagnosetools zuzugreifen und den Anweisungen auf dem Bildschirm zu folgen, um ein Einmalkennwort zu konfigurieren, das nach 24 Stunden abläuft.
7. Verwenden Sie ein SSH-Tool wie Putty, um mit dem Benutzernamen eine Verbindung zur Agent-VM herzustellen `diag` und das von Ihnen konfigurierte Einmalkennwort.

## Installieren Sie ein CA-signiertes Zertifikat für den webbasierten Konsolenzugriff

Wenn Sie die NetApp Console im eingeschränkten Modus verwenden, ist die Benutzeroberfläche über die virtuelle Maschine des Konsolenagenten zugänglich, die in Ihrer Cloud-Region oder vor Ort bereitgestellt wird. Standardmäßig verwendet die Konsole ein selbstsigniertes SSL-Zertifikat, um sicheren HTTPS-Zugriff auf die webbasierte Konsole bereitzustellen, die auf dem Konsolenagenten ausgeführt wird.

Falls Ihr Unternehmen dies erfordert, können Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat installieren, das einen besseren Sicherheitsschutz bietet als ein selbstsigniertes Zertifikat. Nachdem Sie das Zertifikat installiert haben, verwendet die Konsole das von der Zertifizierungsstelle signierte Zertifikat, wenn Benutzer auf die webbasierte Konsole zugreifen.

### Installieren eines HTTPS-Zertifikats

Installieren Sie ein von einer Zertifizierungsstelle signiertes Zertifikat für den sicheren Zugriff auf die webbasierte Konsole, die auf dem Konsolenagenten ausgeführt wird.

## Informationen zu diesem Vorgang

Sie können das Zertifikat mit einer der folgenden Optionen installieren:

- Generieren Sie eine Zertifikatsignieranforderung (CSR) von der Konsole aus, übermitteln Sie die Zertifikatsanforderung an eine Zertifizierungsstelle und installieren Sie dann das von der Zertifizierungsstelle signierte Zertifikat auf dem Konsolenagenten.

Das Schlüsselpaar, das die Konsole zum Generieren der CSR verwendet, wird intern auf dem Konsolenagenten gespeichert. Die Konsole ruft automatisch dasselbe Schlüsselpaar (privater Schlüssel) ab, wenn Sie das Zertifikat auf dem Konsolenagenten installieren.

- Installieren Sie ein CA-signiertes Zertifikat, das Sie bereits haben.

Bei dieser Option wird die CSR nicht über die Konsole generiert. Sie generieren die CSR separat und speichern den privaten Schlüssel extern. Sie stellen der Konsole den privaten Schlüssel zur Verfügung, wenn Sie das Zertifikat installieren.

## Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **HTTPS-Setup**.

Zum Bearbeiten muss der Konsolenagent verbunden sein.

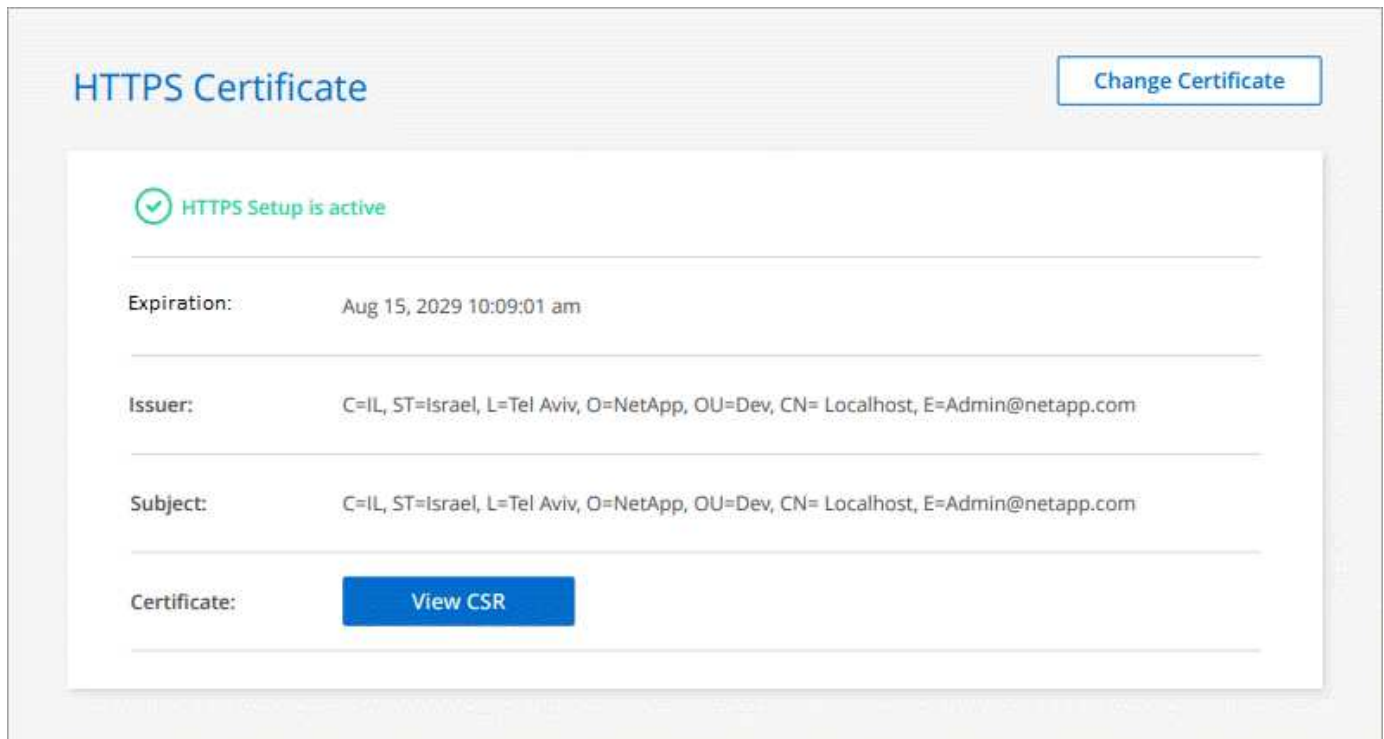
3. Installieren Sie auf der Seite „HTTPS-Setup“ ein Zertifikat, indem Sie eine Zertifikatsignieranforderung (CSR) generieren oder Ihr eigenes CA-signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	<p>a. Geben Sie den Hostnamen oder DNS des Konsolenagent-Hosts (seinen allgemeinen Namen) ein und wählen Sie dann <b>CSR generieren</b>.</p> <p>Die Konsole zeigt eine Zertifikatsignieranforderung an.</p> <p>b. Verwenden Sie die CSR, um eine SSL-Zertifikatsanforderung an eine Zertifizierungsstelle zu senden.</p> <p>Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden.</p> <p>c. Laden Sie die Zertifikatsdatei hoch und wählen Sie dann <b>Installieren</b>.</p>
Installieren Sie Ihr eigenes CA-signiertes Zertifikat	<p>a. Wählen Sie <b>CA-signiertes Zertifikat installieren</b>.</p> <p>b. Laden Sie sowohl die Zertifikatsdatei als auch den privaten Schlüssel und wählen Sie dann <b>Installieren</b>.</p> <p>Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden.</p>

## Ergebnis

Der Konsolenagent verwendet jetzt das von der Zertifizierungsstelle signierte Zertifikat, um sicheren HTTPS-

Zugriff bereitzustellen. Das folgende Bild zeigt einen Agenten, der für sicheren Zugriff konfiguriert ist:



## Erneuern Sie das HTTPS-Zertifikat der Konsole

Sie sollten das HTTPS-Zertifikat des Agenten vor Ablauf erneuern, um einen sicheren Zugriff zu gewährleisten. Wenn Sie das Zertifikat nicht vor Ablauf erneuern, wird eine Warnung angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

### Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **HTTPS-Setup**.

Es werden Details zum Zertifikat angezeigt, einschließlich des Ablaufdatums.

3. Wählen Sie **Zertifikat ändern** und folgen Sie den Schritten zum Generieren einer CSR oder zum Installieren Ihres eigenen CA-signierten Zertifikats.

## Konfigurieren eines Konsolenagenten zur Verwendung eines Proxyserver

Wenn Ihre Unternehmensrichtlinien die Verwendung eines Proxyserver für die gesamte Kommunikation mit dem Internet erfordern, müssen Sie Ihre Agenten für die Verwendung dieses Proxyserver konfigurieren. Wenn Sie während der Installation keinen Konsolenagenten für die Verwendung eines Proxyserver konfiguriert haben, können Sie den Konsolenagenten jederzeit für die Verwendung dieses Proxyserver konfigurieren.

Der Proxyserver des Agenten ermöglicht ausgehenden Internetzugriff ohne öffentliche IP oder NAT-Gateway. Der Proxyserver bietet ausgehende Konnektivität nur für den Konsolenagenten, nicht für Cloud Volumes



ONTAP Systeme.

Wenn Cloud Volumes ONTAP -Systeme keinen ausgehenden Internetzugang haben, konfiguriert die Konsole sie so, dass sie den Proxyserver des Konsolenagenten verwenden. Sie müssen sicherstellen, dass die Sicherheitsgruppe des Konsolenagenten eingehende Verbindungen über Port 3128 zulässt. Öffnen Sie diesen Port, nachdem Sie den Konsolenagenten bereitgestellt haben.

Wenn der Konsolenagent selbst keine ausgehende Internetverbindung hat, können Cloud Volumes ONTAP -Systeme den konfigurierten Proxyserver nicht verwenden.

## Unterstützte Konfigurationen

- Transparente Proxyserver werden für Agenten unterstützt, die Cloud Volumes ONTAP -Systeme bedienen. Wenn Sie NetApp -Datendienste mit Cloud Volumes ONTAP verwenden, erstellen Sie einen dedizierten Agenten für Cloud Volumes ONTAP, bei dem Sie einen transparenten Proxyserver verwenden können.
- Explizite Proxyserver werden von allen Agenten unterstützt, einschließlich derjenigen, die Cloud Volumes ONTAP -Systeme verwalten, und derjenigen, die NetApp -Datendienste verwalten.
- HTTP und HTTPS.
- Der Proxyserver kann sich in der Cloud oder in Ihrem Netzwerk befinden.



Nachdem Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Konsolen-Agenten und fügen einen neuen Agenten mit dem neuen Proxy-Typ hinzu.

## Aktivieren Sie einen expliziten Proxy auf einem Konsolenagenten

Wenn Sie einen Konsolenagenten für die Verwendung eines Proxyservers konfigurieren, verwenden dieser Agent und die von ihm verwalteten Cloud Volumes ONTAP -Systeme (einschließlich aller HA-Mediatoren) alle den Proxyserver.

Dieser Vorgang startet den Konsolenagenten neu. Stellen Sie sicher, dass der Konsolenagent im Leerlauf ist, bevor Sie fortfahren.

### Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Wählen Sie **HTTP-Proxy-Konfiguration**.
4. Wählen Sie im Feld „Konfigurationstyp“ **Expliziter Proxy** aus.
5. Wählen Sie **Proxy aktivieren**.
6. Geben Sie den Server mit der Syntax an `<a href="http://<em>address:port</em>" class="bare">http://<em>address:port</em></a>` oder `<a href="https://<em>address:port</em>" class="bare">https://<em>address:port</em></a>`
7. Geben Sie einen Benutzernamen und ein Kennwort an, wenn für den Server eine Basisauthentifizierung erforderlich ist.

Beachten Sie Folgendes:

- Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
- Für einen Domänenbenutzer müssen Sie den ASCII-Code für das \ wie folgt eingeben:  
Domänenname%92Benutzername

Beispiel: netapp%92proxy

- Die Konsole unterstützt keine Passwörter, die das @-Zeichen enthalten.

8. Wählen Sie **Speichern**.

## Aktivieren Sie einen transparenten Proxy für einen Konsolenagenten

Nur Cloud Volumes ONTAP unterstützt die Verwendung eines transparenten Proxys auf dem Konsolenagenten. Wenn Sie zusätzlich zu Cloud Volumes ONTAP NetApp -Datendienste verwenden, sollten Sie einen separaten Agenten für die Verwendung für Datendienste oder für Cloud Volumes ONTAP erstellen.

Stellen Sie vor der Aktivierung eines transparenten Proxys sicher, dass die folgenden Anforderungen erfüllt sind:

- Der Agent wird im selben Netzwerk wie der transparente Proxyserver installiert.
- Die TLS-Prüfung ist auf dem Proxyserver aktiviert.
- Sie verfügen über ein Zertifikat im PEM-Format, das mit dem auf dem transparenten Proxyserver verwendeten Zertifikat übereinstimmt.
- Sie verwenden den Konsolenagenten für keine anderen NetApp -Datendienste als Cloud Volumes ONTAP.

Um einen vorhandenen Agenten für die Verwendung eines transparenten Proxyservers zu konfigurieren, verwenden Sie das Wartungstool des Konsolenagenten, das über die Befehlszeile auf dem Konsolenagentenhost verfügbar ist.

Wenn Sie einen Proxyserver konfigurieren, wird der Konsolenagent neu gestartet. Stellen Sie sicher, dass der Konsolenagent im Leerlauf ist, bevor Sie fortfahren.

### Schritte

Stellen Sie sicher, dass Sie über eine Zertifikatsdatei im PEM-Format für den Proxyserver verfügen. Wenn Sie kein Zertifikat haben, wenden Sie sich an Ihren Netzwerkadministrator, um eines zu erhalten.

1. Öffnen Sie eine Befehlszeilenschnittstelle auf dem Konsolenagent-Host.
2. Navigieren Sie zum Verzeichnis des Wartungstools des Konsolenagenten:  
`/opt/application/netapp/service-manager-2/agent-maint-console`
3. Führen Sie den folgenden Befehl aus, um den transparenten Proxy zu aktivieren.  
`/home/ubuntu/<certificate-file>.pem` ist das Verzeichnis und der Name der Zertifikatsdatei, die Sie für den Proxyserver haben:

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Stellen Sie sicher, dass die Zertifikatsdatei im PEM-Format vorliegt und sich im selben Verzeichnis wie der Befehl befindet, oder geben Sie den vollständigen Pfad zur Zertifikatsdatei an.

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

## Ändern Sie den transparenten Proxy für den Konsolenagenten

Sie können den vorhandenen transparenten Proxy-Server eines Console-Agenten aktualisieren, indem Sie die folgende Funktion verwenden: `proxy update` Befehl oder entfernen Sie den transparenten Proxy-Server mithilfe des Befehls `proxy remove` Befehl. Weitere Informationen finden Sie in der Dokumentation zu ["Agenten-Wartungskonsole"](#) Die



Nachdem Sie einen Proxy konfiguriert haben, können Sie den Proxy-Typ nicht mehr ändern. Wenn Sie den Proxy-Typ ändern müssen, entfernen Sie den Konsolen-Agenten und fügen einen neuen Agenten mit dem neuen Proxy-Typ hinzu.

## Aktualisieren Sie den Proxy des Konsolenagenten, wenn dieser den Zugriff auf das Internet verliert

Wenn sich die Proxy-Konfiguration für Ihr Netzwerk ändert, verliert Ihr Agent möglicherweise den Zugriff auf das Internet. Zum Beispiel, wenn jemand das Passwort für den Proxyserver ändert oder das Zertifikat aktualisiert. In diesem Fall müssen Sie direkt vom Konsolenagent-Host auf die Benutzeroberfläche zugreifen und die Einstellungen aktualisieren. Stellen Sie sicher, dass Sie Netzwerkzugriff auf den Konsolen-Agent-Host haben und sich bei der Konsole anmelden können.

## Aktivieren Sie den direkten API-Verkehr

Wenn Sie einen Console-Agenten für die Verwendung eines Proxy-Servers konfiguriert haben, können Sie den direkten API-Datenverkehr auf dem Console-Agenten aktivieren, um API-Aufrufe direkt an Cloud-Anbieterdienste zu senden, ohne den Proxy zu durchlaufen. Agenten, die in AWS, Azure oder Google Cloud ausgeführt werden, unterstützen diese Option.

Wenn Sie Azure Private Links mit Cloud Volumes ONTAP deaktivieren und Service-Endpunkte verwenden, aktivieren Sie den direkten API-Verkehr. Andernfalls wird der Datenverkehr nicht richtig weitergeleitet.

["Erfahren Sie mehr über die Verwendung eines Azure Private Link oder von Service-Endpunkten mit Cloud Volumes ONTAP"](#)

### Schritte

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie auf der Seite **Übersicht** das Aktionsmenü für einen Konsolenagenten und wählen Sie **Agent bearbeiten**.

Zum Bearbeiten muss der Konsolenagent aktiv sein.

3. Wählen Sie **Direkten API-Verkehr unterstützen**.
4. Aktivieren Sie das Kontrollkästchen, um die Option zu aktivieren, und wählen Sie dann **Speichern**.

## Fehlerbehebung beim Konsolen-Agent

Um Probleme mit einem Konsolenagenten zu beheben, können Sie die Probleme selbst überprüfen oder mit dem NetApp -Support zusammenarbeiten, der Sie möglicherweise

nach Ihrer System-ID, Agentenversion oder den neuesten AutoSupport -Nachrichten fragt.

Wenn Sie über ein NetApp Support Site-Konto verfügen, können Sie auch die ["NetApp Wissensdatenbank."](#)

## Häufige Fehlermeldungen und Lösungen

Diese Tabelle listet häufige Fehlermeldungen auf und zeigt, wie man sie beheben kann:

Fehlermeldung	Erläuterung	Was zu tun
Die Benutzeroberfläche des Konsolenagenten konnte nicht geladen werden	Die Agenteninstallation ist fehlgeschlagen	<ul style="list-style-type: none"><li>• Stellen Sie sicher, dass der Service Manager-Dienst aktiv ist.</li><li>• Stellen Sie sicher, dass alle Container ausgeführt werden.</li><li>• Stellen Sie sicher, dass Ihre Firewall den Zugriff auf den Dienst über Port 8888 zulässt.</li><li>• Sollten weiterhin Probleme auftreten, wenden Sie sich bitte an den Support.</li></ul>
Auf die NetApp Agent-Benutzeroberfläche kann nicht zugegriffen werden	Diese Meldung wird angezeigt, wenn versucht wird, auf die IP-Adresse eines Agenten zuzugreifen. Die Initialisierung des Agenten kann fehlschlagen, wenn er nicht über den richtigen Netzwerkzugriff verfügt oder instabil ist.	<ul style="list-style-type: none"><li>• Stellen Sie eine Verbindung zum Konsolenagenten her.</li><li>• Überprüfen Sie, ob der Service Manager-Dienst</li><li>• Stellen Sie sicher, dass der Agent über den erforderlichen Netzwerkzugriff verfügt. <a href="#">"Erfahren Sie mehr über erforderliche Endpunkte für den Netzwerkzugriff."</a></li></ul>
Agenteneinstellungen konnten nicht geladen werden	Die Konsole zeigt diese Meldung an, wenn Sie versuchen, auf die Seite mit den Agenteneinstellungen zuzugreifen.	<ul style="list-style-type: none"><li>• Überprüfen Sie, ob der OCCM-Container ausgeführt wird und funktioniert.</li><li>• Wenn das Problem weiterhin besteht, wenden Sie sich an den Support.</li></ul>
Supportinformationen für den Agenten konnten nicht geladen werden.	Diese Meldung wird angezeigt, wenn der Agent nicht auf Ihr Supportkonto zugreifen kann.	<ul style="list-style-type: none"><li>• Prüfen Sie, ob der Agent ausgehenden Zugriff auf die erforderlichen Endpunkte hat. <a href="#">"Erfahren Sie mehr über erforderliche Endpunkte für den Netzwerkzugriff."</a></li></ul>

## Überprüfen Sie den Status des Konsolenagenten

Verwenden Sie einen der folgenden Befehle, um Ihren Konsolenagenten zu überprüfen. Alle Dienste sollten den Status „Wird ausgeführt“ haben. Wenn dies nicht der Fall ist, wenden Sie sich an den NetApp Support.



Ausführlichere Informationen zum Zugriff auf die Konsolen-Agent-Diagnose finden Sie in den folgenden Themen:

- ["Überprüfen Sie den Status des Konsolenagenten \(für Linux-Hostbereitstellungen\)."](#)
- ["Überprüfen Sie den Status des Konsolenagenten \(für VCenter-Bereitstellungen\)."](#)

### Docker (für Ubuntu- und VCenter-Bereitstellungen)

```
docker ps -a
```

### Podman (für RedHat Enterprise Linux-Bereitstellungen)

```
podman ps -a
```

## Anzeigen der Konsolen-Agent-Version

Zeigen Sie die Version des Konsolenagenten an, um das Upgrade zu bestätigen, oder teilen Sie sie Ihrem NetApp -Vertreter mit.

### Schritte

1. Wählen Sie **Administration > Support > Agenten**.

Die Konsole zeigt die Version oben auf der Seite an.

## Überprüfen des Netzwerkzugriffs

Stellen Sie sicher, dass der Konsolenagent über den erforderlichen Netzwerkzugriff verfügt. ["Erfahren Sie mehr über die erforderlichen Netzwerkzugriffspunkte."](#)

### Führen Sie Konfigurationsprüfungen auf dem Konsolenagenten durch.

Führen Sie Konfigurationsprüfungen an den Konsolenagenten über die Konsole oder die Agentenwartungskonsole durch, um sicherzustellen, dass sie verbunden sind.

Sie können Konfigurationsprüfungen auch über die Agentenwartungskonsole durchführen. ["Erfahren Sie mehr über die Verwendung des Befehls config-checker validate."](#)



Sie können nur Agenten validieren, die den Status **Verbunden** haben.

### Schritte von der Konsole

1. Wählen Sie **Administration > Agenten**.
2. Wählen Sie im Aktionsmenü des Konsolenagenten, den Sie überprüfen möchten, die Option **Validieren** aus.

Name	Location	Status	Region
BXP9161ga		Connected	N/A
BXP9181		Connected	N/A
nikhil	aws	Failed	US
nikhil	aws	Failed	US

Die Validierung kann bis zu 15 Minuten dauern. Die Ergebnisse werden nach Abschluss des Vorgangs angezeigt.

## Probleme bei der Installation des Konsolenagenten

Wenn die Installation fehlschlägt, sehen Sie sich den Bericht und die Protokolle an, um die Probleme zu beheben.

Sie können auch direkt vom Konsolen-Agent-Host in den folgenden Verzeichnissen auf den Validierungsbericht im JSON-Format und die Konfigurationsprotokolle zugreifen:

```
/tmp/netapp-console-agents/logs
/tmp/netapp-console-agents/results.json
```



- Bei der Bereitstellung neuer Agenten prüft NetApp die folgenden Endpunkte: "[hier aufgeführt](#)". Diese Konfigurationsprüfung schlägt mit einem Fehler fehl, wenn Sie die vorherigen Endpunkte verwenden, die für Upgrades verwendet wurden. "[hier aufgeführt](#)". NetApp empfiehlt, Ihre Firewall-Regeln so schnell wie möglich zu aktualisieren, um den Zugriff auf die aktuellen Endpunkte zu ermöglichen und den Zugriff auf die vorherigen Endpunkte zu blockieren. "[Erfahren Sie, wie Sie Ihr Netzwerk aktualisieren](#)".
- Wenn Sie die Endpunkte in Ihrer Firewall aktualisieren, funktionieren Ihre vorhandenen Agenten weiterhin.

## Deaktivieren Sie Konfigurationsprüfungen für manuelle Installationen

Es kann vorkommen, dass Sie die Konfigurationsprüfungen deaktivieren müssen, die während der Installation die ausgehende Konnektivität überprüfen. Wenn Sie beispielsweise einen Agenten in Ihrer Government Cloud-Umgebung manuell installieren, müssen Sie die Konfigurationsprüfungen deaktivieren, da die Installation sonst fehlschlägt.

### Schritte

Sie deaktivieren die Konfigurationsprüfung, indem Sie das Flag *skipConfigCheck* in der Datei *com/opt/application/netapp/service-manager-2/config.json* setzen. Standardmäßig ist dieses Flag auf „false“ gesetzt und die Konfigurationsprüfung überprüft den ausgehenden Zugriff für den Agenten. Setzen Sie dieses Flag auf „true“, um die Prüfung zu deaktivieren. Machen Sie sich mit der JSON-Syntax vertraut, bevor Sie diesen Schritt ausführen.

Um die Konfigurationsprüfung wieder zu aktivieren, führen Sie diese Schritte aus und setzen Sie das Flag

`skipConfigCheck` auf „false“.

### Schritte

1. Greifen Sie als Root oder mit Sudo-Berechtigungen auf den Konsolen-Agent-Host zu.
2. Erstellen Sie eine Sicherungskopie der Datei `/opt/application/netapp/service-manager-2/config.json`, um sicherzustellen, dass Sie Ihre Änderungen rückgängig machen können.
3. Stoppen Sie den Dienst Service Manager 2, indem Sie den folgenden Befehl ausführen:

```
systemctl stop netapp-service-manager.service
```

1. Bearbeiten Sie die Datei `/opt/application/netapp/service-manager-2/config.json` und ändern Sie den Wert des Flags `skipConfigCheck` auf „true“.

```
"skipConfigCheck": true
```

2. Speichern Sie Ihre Datei.
3. Starten Sie den Dienst Service Manager 2 neu, indem Sie den folgenden Befehl ausführen:

```
systemctl restart netapp-service-manager.service
```

## Arbeiten Sie mit dem NetApp Support

Wenn Sie die Probleme mit Ihrem Konsolenagenten nicht lösen konnten, sollten Sie sich an den NetApp -Support wenden. Der NetApp Support fragt möglicherweise nach der Konsolen-Agent-ID oder fordert Sie auf, ihm die Konsolen-Agent-Protokolle zu senden, falls diese noch nicht vorliegen.

### Suchen Sie die Konsolen-Agent-ID

Um Ihnen den Einstieg zu erleichtern, benötigen Sie möglicherweise die System-ID Ihres Konsolenagenten. Die ID wird normalerweise für Lizenzierungs- und Fehlerbehebungs Zwecke verwendet.

### Schritte

1. Wählen Sie **Administration > Support > Agenten**.

Die System-ID finden Sie oben auf der Seite.

### Beispiel

The screenshot shows a grid of information about the console agent. The 'System ID' field, which contains the value 'a39d460d-a64e-47e2-b066-ac...', is highlighted with a red rectangular box. Other visible fields include 'Agent name' (staging-onprem-connector), 'Version/Build' (3.9.56 / 875), 'Company' (netapp), 'Client ID' (4mcQIG1xzzDEhGq0CgorxV1Da...), and 'Server Name' (2da1c40131a6).

staging-onprem-connector Agent name	3.9.56 / 875 Version/Build	netapp Company
4mcQIG1xzzDEhGq0CgorxV1Da... Client ID	a39d460d-a64e-47e2-b066-ac... System ID	2da1c40131a6 Server Name

2. Bewegen Sie den Mauszeiger über die ID und klicken Sie darauf, um sie zu kopieren.

## Laden Sie eine AutoSupport -Nachricht herunter oder senden Sie sie

Wenn bei Ihnen Probleme auftreten, werden Sie von NetApp möglicherweise aufgefordert, zur Fehlerbehebung eine AutoSupport -Nachricht an den NetApp -Support zu senden.



Aufgrund des Lastenausgleichs benötigt die NetApp Console bis zu fünf Stunden, um AutoSupport -Nachrichten zu senden. Laden Sie für dringende Mitteilungen die Datei herunter und senden Sie sie manuell.

### Schritte

1. Wählen Sie **Administration > Support > Agenten**.
2. Wählen Sie je nachdem, wie Sie die Informationen an den NetApp Support senden müssen, eine der folgenden Optionen:
  - a. Wählen Sie die Option zum Herunterladen der AutoSupport -Nachricht auf Ihren lokalen Computer. Sie können es dann mit einer bevorzugten Methode an den NetApp -Support senden.
  - b. Wählen Sie \* AutoSupport senden\*, um die Nachricht direkt an den NetApp -Support zu senden.

## Beheben von Downloadfehlern bei Verwendung eines Google Cloud NAT-Gateways

Der Konsolenagent lädt automatisch Softwareupdates für Cloud Volumes ONTAP herunter. Ihre Konfiguration kann dazu führen, dass der Download fehlschlägt, wenn ein Google Cloud NAT-Gateway verwendet wird. Sie können dieses Problem beheben, indem Sie die Anzahl der Teile begrenzen, in die das Software-Image unterteilt ist. Dieser Schritt muss mithilfe der API abgeschlossen werden.

### Schritt

1. Senden Sie eine PUT-Anfrage an `/occm/config` mit dem folgenden JSON als Text:

```
{
  "maxDownloadSessions": 32
}
```

Der Wert für `maxDownloadSessions` kann 1 oder eine beliebige Ganzzahl größer als 1 sein. Wenn der Wert 1 ist, wird das heruntergeladene Bild nicht geteilt.

Beachten Sie, dass 32 ein Beispielwert ist. Der Wert hängt von Ihrer NAT-Konfiguration und der Anzahl gleichzeitiger Sitzungen ab.

["Erfahren Sie mehr über den API-Aufruf /occm/config"](#)

## Holen Sie sich Hilfe von der NetApp Knowledge Base

["Informationen zur Fehlerbehebung anzeigen, die vom NetApp Support-Team erstellt wurden"](#) .

## Deinstallieren und Entfernen eines Konsolenagenten

Deinstallieren Sie einen Konsolenagenten, um Probleme zu beheben oder ihn dauerhaft



vom Host zu entfernen. Die erforderlichen Schritte hängen vom verwendeten Bereitstellungsmodus ab. Nachdem Sie einen Konsolenagenten aus Ihrer Umgebung entfernt haben, können Sie ihn aus der Konsole entfernen.

["Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console"](#) .

## Deinstallieren Sie den Agenten, wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden

Wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden (mit anderen Worten, der Agent-Host verfügt über eine ausgehende Konnektivität), sollten Sie die folgenden Schritte ausführen, um den Agenten zu deinstallieren.

### Schritte

1. Stellen Sie eine Verbindung zur Linux-VM für den Agenten her.
2. Führen Sie vom Linux-Host aus das Deinstallationsskript aus:

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

*silent* führt das Skript aus, ohne Sie zur Bestätigung aufzufordern.

## Entfernen von Konsolenagenten aus der Konsole

Wenn Sie eine Agenten-VM gelöscht oder den Agenten deinstalliert haben, sollten Sie ihn aus der Liste der Agenten in der Konsole entfernen. Nach dem Löschen einer Agenten-VM oder der Deinstallation der Agentensoftware wird der Agent in der Konsole als **Getrennt** angezeigt.

Beachten Sie beim Entfernen eines Konsolenagenten Folgendes:

- Durch diese Aktion wird die virtuelle Maschine nicht gelöscht.
- Diese Aktion kann nicht rückgängig gemacht werden. Wenn Sie einen Konsolenagenten einmal entfernt haben, können Sie ihn nicht wieder hinzufügen.

### Schritte

1. Wählen Sie **Administration > Agenten**.
2. Auf der Seite **Übersicht** wählen Sie das Aktionsmenü für einen getrennten Agenten und anschließend **Agent entfernen**.
3. Geben Sie zur Bestätigung den Namen des Agenten ein und wählen Sie dann **Entfernen**.

## Copyright-Informationen

Copyright © 2026 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 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.