Konfigurieren Sie das CA-Zertifikat

SnapCenter Software 4.9

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-49/protect-scc/reference_generate_CA_certificate_CSR_file.html on September 26, 2025. Always check docs.netapp.com for the latest.

Inhalt

Konfigurieren Sie das CA-Zertifikat . . . 1
ZertifikatCSR-Datei erstellen . . . 1
Importieren von CA-Zertifikaten . . . 1
Abrufen des Daumenabdrucks für das CA-Zertifikat . . . 2
Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten . . . 3
Konfigurieren Sie das CA-Zertifikat für den benutzerdefinierten SnapCenter-Plug-ins-Dienst auf dem Linux-Host . . . 3
Passwort für benutzerdefinierten Plug-in-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten . . . 4
Konfigurieren Sie Root- oder Zwischenzertifikate in einem benutzerdefinierten Plug-in Trust-Store . . . 4
Konfigurieren Sie das CA-signierte Schlüsselpaar in einem benutzerdefinierten Plug-in-Vertrauensspeicher . . . 5
Konfigurieren der Zertifikatsperrliste (CRL) für benutzerdefinierte SnapCenter-Plug-ins . . . 6
Konfigurieren Sie das CA-Zertifikat für den benutzerdefinierten SnapCenter-Plug-ins-Dienst auf Windows-Host . . . 6
Passwort für benutzerdefinierten Plug-in-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten . . . 6
Konfigurieren Sie Root- oder Zwischenzertifikate in einem benutzerdefinierten Plug-in Trust-Store . . . 7
Konfigurieren Sie das CA-signierte Schlüsselpaar in einem benutzerdefinierten Plug-in-Vertrauensspeicher . . . 7
Konfigurieren der Zertifikatsperrliste (CRL) für benutzerdefinierte SnapCenter-Plug-ins . . . 8
Aktivieren Sie CA-Zertifikate für Plug-ins . . . 9

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

CA Certificate RSA-Schlüssel sollten mindestens 3072 Bit lang sein.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie vor dem Erwerb des Zertifikats das Feld alternativer Antragstellername (SAN) ausfüllen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: *.pfx, *.p12 und *.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „persönlich“.

Abrufen des Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   a. Doppelklicken Sie auf das Zertifikat.
   b. Klicken Sie im Dialogfeld Zertifikat auf die Registerkarte **Details**.
   c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter-Server und allen Plug-in-Hosts durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Beispiel:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Binden Sie das neu installierte Zertifikat an die Windows Host Plug-in-Dienste, indem Sie die folgenden Befehle ausführen:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

   Beispiel:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

Konfigurieren Sie das CA-Zertifikat für den benutzerdefinierten SnapCenter-Plug-ins-Dienst auf dem Linux-Host

Sie sollten das Passwort des benutzerdefinierten Plug-ins-Schlüsselspeichers und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für den benutzerdefinierten Plug-ins-Vertrauensspeicher konfigurieren und das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-ins-Vertrauensspeicher mit dem SnapCenter-Dienst Benutzerdefinierte Plug-ins

konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Benutzerdefinierte Plug-ins verwenden die Datei 'keystore.jks', die sich unter */opt/NetApp/snapcenter/scc/etc* sowohl als Vertrauensspeicher als auch als Schlüsselspeicher befindet.

Passwort für benutzerdefinierten Plug-in-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten

Schritte

1. Sie können benutzerdefinierte Plug-in Schlüsselspeicher Standardpasswort aus benutzerdefinierten Plug-in Agent Eigenschaftsdatei abrufen.

   Es ist der Wert, der dem Schlüssel 'KEYSTORE_PASS' entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:
   ```

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

3. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

> Das Kennwort für den benutzerdefinierten Plug-in-Schlüsselspeicher und für alle zugeordneten Alias-Passwörter des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in einem benutzerdefinierten Plug-in Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel als benutzerdefinierten Plug-in-Vertrauensspeicher konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner mit dem benutzerdefinierten Plug-in-Keystore: /Opt/NetApp/snapcenter/scc/etc
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder
Zwischenzertifikate in einen benutzerdefinierten Plug-in Trust-Store
konfiguriert haben.
```

Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Konfigurieren Sie das CA-signierte Schlüsselpaar in einem benutzerdefinierten Plug-in-Vertrauensspeicher

Sie sollten das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-in Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem benutzerdefinierten Plug-in keystore /opt/NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen Schlüssel hinzu.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Das benutzerdefinierte Standard-Plug-in-Schlüsselspeicher-Passwort ist der Wert der SCHLÜSSELDATEI KEYSTORE_PASS in agent.properties.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Wenn der Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder
Sonderzeichen enthält („*","","), ändern Sie den Alias-Namen in einen
einfachen Namen:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei
agent.properties.
```

Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

8. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar in einen benutzerdefinierten Plug-in Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für benutzerdefinierte SnapCenter-Plug-ins

Über diese Aufgabe

- Benutzerdefinierte SnapCenter-Plug-ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter Custom Plug-ins ist ' opt/NetApp/snapcenter/scc/etc/crl'.

Schritte

1. Sie können das Standardverzeichnis in der Datei agent.properties mit dem Schlüssel CRL_PATH ändern und aktualisieren.

   Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Konfigurieren Sie das CA-Zertifikat für den benutzerdefinierten SnapCenter-Plug-ins-Dienst auf Windows-Host

Sie sollten das Passwort des benutzerdefinierten Plug-ins-Schlüsselspeichers und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für den benutzerdefinierten Plug-ins-Vertrauensspeicher konfigurieren und das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-ins-Vertrauensspeicher mit dem SnapCenter-Dienst Benutzerdefinierte Plug-ins konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Benutzerdefinierte Plug-ins verwenden die Datei *keystore.jks*, die sich unter *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc* befindet, sowohl als Vertrauensspeicher als auch als Schlüsselspeicher.

Passwort für benutzerdefinierten Plug-in-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten

Schritte

1. Sie können benutzerdefinierte Plug-in Schlüsselspeicher Standardpasswort aus benutzerdefinierten Plug-in Agent Eigenschaftsdatei abrufen.

Es ist der Wert, der dem Schlüssel *KEYSTORE_PASS* entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   Keytool -storepasswd -keystore keystore.jks

   Wenn der Befehl "keytool" in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl keytool mit seinem vollständigen Pfad.

   C:\Programme\Java\<jdk_Version>\bin\keytool.exe“ -storepasswd -keystore keystore.jks

3. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

   Keytool -keypasswd -alias „alias_Name_in_cert“ -keystore keystore.jks

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

4. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

   Das Kennwort für den benutzerdefinierten Plug-in-Schlüsselspeicher und für alle zugeordneten Alias-Passwörter des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in einem benutzerdefinierten Plug-in Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel als benutzerdefinierten Plug-in-Vertrauensspeicher konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner mit dem benutzerdefinierten Plug-in-Keystore *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:

   Keytool -Import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder Zwischenzertifikate in einen benutzerdefinierten Plug-in Trust-Store konfiguriert haben.

   Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Konfigurieren Sie das CA-signierte Schlüsselpaar in einem benutzerdefinierten Plug-in-Vertrauensspeicher

Sie sollten das CA-signierte Schlüsselpaar für den benutzerdefinierten Plug-in Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem benutzerdefinierten Plug-in Schlüsselspeicher *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen Schlüssel hinzu.

   Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

   Keytool -list -V -keystore keystore.jks

6. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Das benutzerdefinierte Standard-Plug-in-Schlüsselspeicher-Passwort ist der Wert der SCHLÜSSELDATEI KEYSTORE_PASS in agent.properties.

   Keytool -keypasswd -alias „alias_Name_in_CA_cert“ -keystore keystore.jks

8. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei *agent.properties*.

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

9. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar in einen benutzerdefinierten Plug-in Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für benutzerdefinierte SnapCenter-Plug-ins

Über diese Aufgabe

- Informationen zum Herunterladen der neuesten CRL-Datei für das zugehörige CA-Zertifikat finden Sie unter "Aktualisieren der Listendatei für Zertifikatsperrlisten im SnapCenter CA-Zertifikat".
- Benutzerdefinierte SnapCenter-Plug-ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für benutzerdefinierte SnapCenter Plug-ins ist *'C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in Creator\ etc\crl'*.

Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* mit dem Schlüssel CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter-Server und den entsprechenden Plug-in-Hosts bereitstellen. Sie sollten die CA-Zertifikatsvalidierung für die Plug-ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie ein- oder mehrere Plug-in-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Zeigt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

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.