



Verwalten von Zertifikaten

E-Series Systems

NetApp
March 06, 2023

Inhaltsverzeichnis

- Verwalten von Zertifikaten 1
 - Zertifikatübersicht 1
 - CA-signierte Zertifikate verwenden 2
 - Managementzertifikate zurücksetzen 4
 - Importieren Sie Zertifikate für Arrays 5
 - Anzeigen von Zertifikaten 6
 - Exportieren von Zertifikaten 6
 - Vertrauenswürdige Zertifikate löschen 6
 - Lösen Sie nicht vertrauenswürdige Zertifikate 7

Verwalten von Zertifikaten

Zertifikatübersicht

Die Zertifikatverwaltung im Speicher-Plugin für vCenter ermöglicht die Erstellung von Zertifikatsignierungsanforderungen (CSRs), den Import von Zertifikaten und die Verwaltung vorhandener Zertifikate.

Was sind Zertifikate?

Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und Server für eine sichere Kommunikation im Internet identifizieren. Sie stellen sicher, dass die Webkommunikation in verschlüsselter Form, privat und unverändert, nur zwischen dem angegebenen Server und dem angegebenen Client übertragen wird. Mit dem Storage Plug-in für vCenter können Sie Zertifikate für den Browser auf einem Host-Managementsystem und die Controller in den ermittelten Speicher-Arrays verwalten.

Ein Zertifikat kann von einer vertrauenswürdigen Behörde signiert werden, oder es kann selbst signiert werden. „Unterzeichnen“ bedeutet einfach, dass jemand die Identität des Besitzers bestätigt und festgestellt hat, dass seine Geräte vertrauenswürdig sind.

Die Storage Arrays werden mit einem automatisch generierten, selbstsignierten Zertifikat auf jedem Controller ausgeliefert. Sie können weiterhin die selbst signierten Zertifikate verwenden oder CA-signierte Zertifikate für eine sicherere Verbindung zwischen den Controllern und den Host-Systemen erhalten.



Auch wenn CA-signierte Zertifikate einen besseren Schutz bieten (zum Beispiel die Verhinderung von man-in-the-Middle-Angriffen), verlangen sie auch Gebühren, die teuer sein können, wenn Sie ein großes Netzwerk haben. Im Gegensatz dazu sind selbstsignierte Zertifikate weniger sicher, aber sie sind kostenlos. Daher werden selbst signierte Zertifikate am häufigsten für interne Testumgebungen eingesetzt, nicht in Produktionsumgebungen.

Signierte Zertifikate

Ein signiertes Zertifikat wird von einer Zertifizierungsstelle (CA) validiert, einer vertrauenswürdigen Drittorganisation. Signierte Zertifikate enthalten Angaben über den Eigentümer der Einheit (in der Regel Server oder Website), Datum der Zertifikatausgabe und -Ablauf, gültige Domains für das Unternehmen und eine digitale Signatur bestehend aus Buchstaben und Zahlen.

Wenn Sie einen Browser öffnen und eine Webadresse eingeben, führt Ihr System eine Zertifikatprüfung im Hintergrund durch, um zu bestimmen, ob Sie eine Verbindung zu einer Website herstellen, die ein gültiges, von einer Zertifizierungsstelle signiertes Zertifikat enthält. In der Regel enthält eine mit einem signierten Zertifikat gesicherte Website ein Vorhängeschloss-Symbol und eine https-Bezeichnung in der Adresse. Wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die kein CA-signiertes Zertifikat enthält, zeigt Ihr Browser eine Warnung an, dass die Website nicht sicher ist.

Die CA führt Schritte durch, um Ihre Identität während des Anwendungsprozesses zu überprüfen. Sie senden möglicherweise eine E-Mail an Ihr registriertes Unternehmen, überprüfen Ihre Geschäftsadresse und führen eine HTTP- oder DNS-Verifizierung durch. Wenn der Anwendungsprozess abgeschlossen ist, sendet die Zertifizierungsstelle digitale Dateien zum Laden auf einem Host-Managementsystem. In der Regel umfassen diese Dateien eine Kette des Vertrauens, wie folgt:

- **Root** — an der Spitze der Hierarchie befindet sich das Stammzertifikat, welches einen privaten Schlüssel enthält, der zum Signieren anderer Zertifikate verwendet wird. Das Root identifiziert eine bestimmte CA-

Organisation. Wenn Sie dieselbe Zertifizierungsstelle für alle Netzwerkgeräte verwenden, benötigen Sie nur ein Stammzertifikat.

- **Intermediate** — Abzweigung von der Wurzel sind die Zwischenzertifikate. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.
- **Server** — unten in der Kette befindet sich das Server-Zertifikat, welches Ihre spezifische Entität, wie z.B. eine Website oder ein anderes Gerät, identifiziert. Jeder Controller in einem Storage Array benötigt ein separates Serverzertifikat.

Selbstsignierte Zertifikate

Jeder Controller im Speicher-Array verfügt über ein vorinstalliertes, selbstsigniertes Zertifikat. Ein selbst signiertes Zertifikat ähnelt einem CA-signierten Zertifikat, außer dass es vom Eigentümer des Unternehmens anstelle eines Dritten validiert wird. Wie ein Zertifikat mit einer Zertifizierungsstelle enthält auch ein selbstsigniertes Zertifikat einen eigenen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt und über eine HTTPS-Verbindung zwischen einem Server und einem Client gesendet werden.

Selbstsignierte Zertifikate werden von Browsern nicht „vertrauenswürdig“. Jedes Mal, wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die nur ein selbstsigniertes Zertifikat enthält, wird im Browser eine Warnmeldung angezeigt. Sie müssen in der Warnmeldung auf einen Link klicken, der Ihnen die Nutzung der Website ermöglicht. Dadurch akzeptieren Sie im Wesentlichen das selbstsignierte Zertifikat.

Managementzertifikat

Wenn Sie das Plugin öffnen, versucht der Browser zu überprüfen, ob der Management-Host eine vertrauenswürdige Quelle ist, indem er nach einem digitalen Zertifikat prüft. Wenn der Browser ein von einer Zertifizierungsstelle signiertes Zertifikat nicht findet, wird eine Warnmeldung angezeigt. Von dort aus können Sie auf der Website fortfahren, um das selbstsignierte Zertifikat für diese Sitzung zu akzeptieren. Sie können auch signierte digitale Zertifikate von einer Zertifizierungsstelle beziehen, damit die Warnmeldung nicht mehr angezeigt wird.

Vertrauenswürdige Zertifikate

Während einer Plugin-Sitzung werden möglicherweise zusätzliche Sicherheitsmeldungen angezeigt, wenn Sie versuchen, auf einen Controller zuzugreifen, der kein von einer Zertifizierungsstelle signiertes Zertifikat hat. In diesem Fall können Sie dem selbst signierten Zertifikat dauerhaft vertrauen oder die CA-signierten Zertifikate für die Controller importieren, damit das Plugin eingehende Clientanforderungen von diesen Controllern authentifizieren kann.

CA-signierte Zertifikate verwenden

Sie können CA-signierte Zertifikate für den sicheren Zugriff auf das Managementsystem abrufen und importieren, das das Storage Plugin für vCenter hostet.

Die Verwendung von CA-signierten Zertifikaten ist ein dreistufiges Verfahren:

- [Schritt 1: Eine CSR-Datei ausfüllen.](#)
- [Schritt 2: CSR-Datei senden.](#)
- [Schritt 3: Import Management Zertifikate.](#)

Schritt 1: Eine CSR-Datei ausfüllen

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) generieren, die Ihre Organisation und das Host-System identifiziert, auf dem das Plugin ausgeführt wird. Alternativ können Sie eine CSR-Datei mit einem Tool wie OpenSSL generieren und zu überspringen [Schritt 2: CSR-Datei senden](#).

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte **Management** die Option **CSR abschließen** aus.
3. Geben Sie die folgenden Informationen ein, und klicken Sie dann auf **Weiter**:
 - **Organisation** — der vollständige, rechtliche Name Ihres Unternehmens oder Ihrer Organisation. Fügen Sie Suffixe wie Inc. Oder Corp. Mit ein
 - **Organisationseinheit (optional)** — die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet.
 - **Stadt/Ort** — die Stadt, in der sich Ihr Hostsystem oder Ihr Geschäft befindet.
 - **Bundesland/Region (optional)** — der Staat oder die Region, in der sich Ihr Hostsystem oder Ihr Geschäft befindet.
 - **Land ISO Code** — der zweistellige ISO-Code Ihres Landes (International Organization for Standardization), wie z. B. die USA.
4. Geben Sie die folgenden Informationen über das Hostsystem ein, auf dem das Plugin ausgeführt wird:
 - **Allgemeiner Name** — die IP-Adresse oder der DNS-Name des Hostsystems, auf dem das Plugin läuft. Stellen Sie sicher, dass diese Adresse korrekt ist; sie muss genau mit dem übereinstimmen, was Sie eingeben, um auf das Plugin im Browser zuzugreifen. Verwenden Sie kein http:// oder https://. Der DNS-Name kann nicht mit einem Platzhalter beginnen.
 - **Alternative IP-Adressen** — Wenn der allgemeine Name eine IP-Adresse ist, können Sie optional weitere IP-Adressen oder Aliase für das Host-System eingeben. Verwenden Sie für mehrere Einträge ein kommagetrenntes Format.
 - **Alternative DNS-Namen** — Wenn der gemeinsame Name ein DNS-Name ist, geben Sie weitere DNS-Namen für das Host-System ein. Verwenden Sie für mehrere Einträge ein kommagetrenntes Format. Falls es keine alternativen DNS-Namen gibt, aber Sie im ersten Feld einen DNS-Namen eingegeben haben, kopieren Sie diesen Namen hier. Der DNS-Name kann nicht mit einem Platzhalter beginnen.
5. Stellen Sie sicher, dass die Host-Informationen richtig sind. Wenn dies nicht der Fall ist, schlagen die von der Zertifizierungsstelle zurückgegebenen Zertifikate fehl, wenn Sie versuchen, sie zu importieren.
6. Klicken Sie Auf **Fertig Stellen**.

Schritt 2: CSR-Datei senden

Nachdem Sie eine CSR-Datei (Certificate Signing Request) erstellt haben, senden Sie die generierte CSR-Datei an eine CA, um signierte Management-Zertifikate für das System zu erhalten, das das Plugin hostet.

Systeme der E-Series erfordern ein PEM-Format (Base64 ASCII-Kodierung) für signierte Zertifikate, das die folgenden Dateitypen umfasst: .Pem, .crt, .cer oder .key.

Schritte

1. Suchen Sie die heruntergeladene CSR-Datei.

Der Speicherort des Downloads hängt von Ihrem Browser ab.

2. Senden Sie die CSR-Datei an eine CA (z. B. Verisign oder DigiCert), und fordern Sie signierte Zertifikate

im PEM-Format an.



Nachdem Sie eine CSR-Datei an die CA gesendet haben, erstellen SIE keine weitere CSR-Datei erneut.

Immer wenn Sie eine CSR erstellen, erstellt das System ein privates und öffentliches Schlüsselpaar. Der öffentliche Schlüssel ist Teil der CSR, während der private Schlüssel im Schlüsselspeicher des Systems aufbewahrt wird. Wenn Sie die signierten Zertifikate erhalten und importieren, stellt das System sicher, dass sowohl der private als auch der öffentliche Schlüssel das ursprüngliche Paar sind. Wenn die Schlüssel nicht übereinstimmen, funktionieren die signierten Zertifikate nicht und Sie müssen neue Zertifikate von der CA anfordern.

Schritt 3: Import Management Zertifikate

Nachdem Sie von der Zertifizierungsstelle (CA) signierte Zertifikate erhalten haben, importieren Sie die Zertifikate in das Hostsystem, auf dem das Plugin installiert ist.

Bevor Sie beginnen

- Sie müssen über die signierten Zertifikate der Zertifizierungsstelle verfügen. Diese Dateien umfassen das Stammzertifikat, ein oder mehrere Zwischenzertifikate und das Serverzertifikat.
- Wenn die CA eine verkettete Zertifikatdatei (z. B. eine .p7b-Datei) lieferte, müssen Sie die verkettete Datei in einzelne Dateien entpacken: Das Stammzertifikat, ein oder mehrere Zwischenzertifikate und das Serverzertifikat. Sie können das Windows-certmgr-Dienstprogramm zum Entpacken der Dateien verwenden (Rechtsklick und Menü wählen: Alle Aufgaben[Export]). Base-64-Kodierung wird empfohlen. Wenn die Exporte abgeschlossen sind, wird für jede Zertifikatdatei in der Kette eine CER-Datei angezeigt.
- Sie müssen die Zertifikatdateien auf das Hostsystem kopieren, auf dem das Plugin ausgeführt wird.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte * Management* die Option **Import**.

Es wird ein Dialogfeld zum Importieren der Zertifikatdateien geöffnet.

3. Klicken Sie auf **Durchsuchen**, um zuerst die Stamm- und Zwischenzertifikatdateien auszuwählen und dann das Serverzertifikat auszuwählen. Wenn Sie die CSR aus einem externen Tool generiert haben, müssen Sie auch die private Schlüsseldatei importieren, die zusammen mit der CSR erstellt wurde.

Die Dateinamen werden im Dialogfeld angezeigt.

4. Klicken Sie Auf **Import**.

Ergebnis

Die Dateien werden hochgeladen und validiert. Die Zertifikatinformationen werden auf der Seite Zertifikatverwaltung angezeigt.

Managementzertifikate zurücksetzen

Für das Managementsystem, das das Storage Plugin für vCenter hostet, können Sie das Managementzertifikat in den ursprünglichen, werkseitig selbstsignierten Zustand zurücksetzen.

Über diese Aufgabe

Mit dieser Aufgabe wird das aktuelle Management-Zertifikat aus dem Hostsystem gelöscht, auf dem das Storage Plugin für vCenter ausgeführt wird. Nach dem Zurücksetzen des Zertifikats wird das Host-System auf das selbstsignierte Zertifikat zurückgesetzt.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte **Verwaltung** die Option **Zurücksetzen**.

Das Dialogfeld „Zertifikat zurücksetzen bestätigen“ wird geöffnet.

3. Geben Sie Reset in das Feld ein, und klicken Sie dann auf **Zurücksetzen**.

Nach der Aktualisierung Ihres Browsers kann der Browser den Zugriff auf die Zielseite blockieren und melden, dass die Website HTTP Strict Transport Security verwendet. Diese Bedingung tritt auf, wenn Sie wieder auf selbstsignierte Zertifikate wechseln. Um die Bedingung zu löschen, die den Zugriff auf das Ziel blockiert, müssen Sie die Browserdaten aus dem Browser löschen.

Ergebnis

Das System setzt auf die Verwendung des selbstsignierten Zertifikats des Servers zurück. Das System fordert Benutzer daher auf, das selbstsignierte Zertifikat für ihre Sitzungen manuell anzunehmen.

Importieren Sie Zertifikate für Arrays

Bei Bedarf können Zertifikate für die Speicher-Arrays importiert werden, sodass sie sich mit dem System authentifizieren können, das das Storage Plug-in für vCenter hostet. Zertifikate können von einer Zertifizierungsstelle (CA) signiert oder selbst signiert werden.

Bevor Sie beginnen

Wenn Sie vertrauenswürdige Zertifikate importieren, müssen die Zertifikate für die Speicher-Array-Controller mit System Manager importiert werden.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte * Trusted* aus.

Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

3. Wählen Sie entweder Menü:Import[Certificates], um ein CA-Zertifikat oder Menü zu importieren:Importieren[Self-signierte Speicher-Array-Zertifikate], um ein selbstsigniertes Zertifikat zu importieren.
4. Um die Ansicht einzuschränken, können Sie das Filterfeld **Zertifikate anzeigen verwenden, das...** ist, oder Sie können die Zertifikatzeilen sortieren, indem Sie auf eine der Spaltenüberschrift klicken.
5. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf **Import**.

Das Zertifikat wird hochgeladen und validiert.

Anzeigen von Zertifikaten

Sie können zusammenfassende Informationen für ein Zertifikat anzeigen, das die Organisation, die das Zertifikat verwendet, die Behörde, die das Zertifikat ausgestellt hat, den Gültigkeitszeitraum und die Fingerabdrücke (eindeutige Kennungen) umfasst.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie eine der folgenden Registerkarten aus:
 - **Management** — zeigt das Zertifikat für das System, das das Plugin hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Es ermöglicht sicheren Zugriff auf das Plugin.
 - **Trusted** — zeigt Zertifikate, auf die das Plugin für Speicher-Arrays und andere Remote-Server zugreifen kann, z. B. einen LDAP-Server. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.
3. Um weitere Informationen zu einem Zertifikat anzuzeigen, wählen Sie seine Zeile aus, wählen Sie die Ellipsen am Zeilenende aus und klicken Sie dann auf **Ansicht** oder **Export**.

Exportieren von Zertifikaten

Sie können ein Zertifikat exportieren, um die vollständigen Details anzuzeigen.

Bevor Sie beginnen

Um die exportierte Datei zu öffnen, müssen Sie über eine Zertifikatanzeige-Anwendung verfügen.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie eine der folgenden Registerkarten aus:
 - **Management** — zeigt das Zertifikat für das System, das das Plugin hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Es ermöglicht sicheren Zugriff auf das Plugin.
 - **Trusted** — zeigt Zertifikate, auf die das Plugin für Speicher-Arrays und andere Remote-Server zugreifen kann, z. B. einen LDAP-Server. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.
3. Wählen Sie auf der Seite ein Zertifikat aus, und klicken Sie dann am Ende der Zeile auf die Ellipsen.
4. Klicken Sie auf **Exportieren** und speichern Sie dann die Zertifikatdatei.
5. Öffnen Sie die Datei in Ihrer Zertifikatanzeige-Anwendung.

Vertrauenswürdige Zertifikate löschen

Sie können ein oder mehrere nicht mehr benötigte Zertifikate löschen, z. B. ein abgelaufenes Zertifikat.

Bevor Sie beginnen

Importieren Sie das neue Zertifikat, bevor Sie das alte löschen.



Beachten Sie, dass das Löschen eines Root- oder Zwischenzertifikats mehrere Speicher-Arrays beeinflussen kann, da diese Arrays dieselben Zertifikatdateien gemeinsam nutzen können.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte * Trusted* aus.
3. Wählen Sie ein oder mehrere Zertifikate in der Tabelle aus, und klicken Sie dann auf **Löschen**.



Die Löschfunktion ist für vorinstallierte Zertifikate nicht verfügbar.

Das Dialogfeld Vertrauenswürdiges Zertifikat bestätigen wird geöffnet.

4. Bestätigen Sie den Löschvorgang, und klicken Sie dann auf **Löschen**.

Das Zertifikat wird aus der Tabelle entfernt.

Lösen Sie nicht vertrauenswürdige Zertifikate

Auf der Zertifikatsseite können Sie nicht vertrauenswürdige Zertifikate auflösen, indem Sie ein selbstsigniertes Zertifikat aus dem Speicher-Array importieren oder ein Zertifikat der Zertifizierungsstelle importieren, das von einem vertrauenswürdigen Dritten ausgestellt wurde.

Bevor Sie beginnen

Wenn Sie ein Zertifikat importieren möchten, muss Folgendes sichergestellt sein:

- Sie haben für jeden Controller im Speicher-Array eine Zertifikatsignierungsanforderung (.CSR-Datei) generiert und an die CA gesendet.
- Die CA hat vertrauenswürdige Zertifikatdateien zurückgegeben.
- Die Zertifikatdateien sind auf Ihrem lokalen System verfügbar.

Über diese Aufgabe

Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array versucht, eine sichere Verbindung zum Plugin herzustellen, aber die Verbindung wird nicht als sicher bestätigt. Möglicherweise müssen Sie zusätzliche vertrauenswürdige CA-Zertifikate installieren, wenn eine der folgenden Optionen zutrifft:

- Sie haben kürzlich ein Speicher-Array hinzugefügt.
- Ein oder beide Zertifikate sind abgelaufen oder widerrufen.
- Ein oder beide Zertifikate fehlen ein Stammzertifikat oder ein Zwischenzertifikat.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte * Trusted* aus.

Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

3. Wählen Sie entweder Menü:Import[Certificates], um ein CA-Zertifikat oder Menü zu importieren:Importieren[Self-signierte Speicher-Array-Zertifikate], um ein selbstsigniertes Zertifikat zu

importieren.

4. Um die Ansicht einzuschränken, können Sie das Filterfeld **Zertifikate anzeigen verwenden, das...** ist, oder Sie können die Zertifikatzeilen sortieren, indem Sie auf eine der Spaltenüberschrift klicken.
5. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf **Import**.

Das Zertifikat wird hochgeladen und validiert.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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