Konfigurieren von Umbrella VA zum Empfangen von Benutzer-IP-Zuordnungen

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration der Cisco Umbrella Virtual Appliance (VA) für den Empfang von Benutzer-IP-Zuordnungen über einen sicheren Kanal.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Die Erstellung privater Schlüssel, die Zertifikatserstellung, die Zertifikatssignatur und die Verwaltung liegen außerhalb des Anwendungsbereichs der Umbrella-Komponenten. Dies muss außerhalb dieser Komponenten erfolgen.
- Sie müssen pro virtueller Appliance ein Zertifikat mit einem eindeutigen gemeinsamen Namen erstellen.
- Sie müssen außerdem einen A-Eintrag in Ihrem internen DNS-Server hinzufügen, der diesen Common Name auf die IP-Adresse der virtuellen Appliance verweist.
- Wenn die IP-Adresse einer virtuellen Appliance geändert werden muss, muss auch dieser A-Datensatz entsprechend geändert werden.

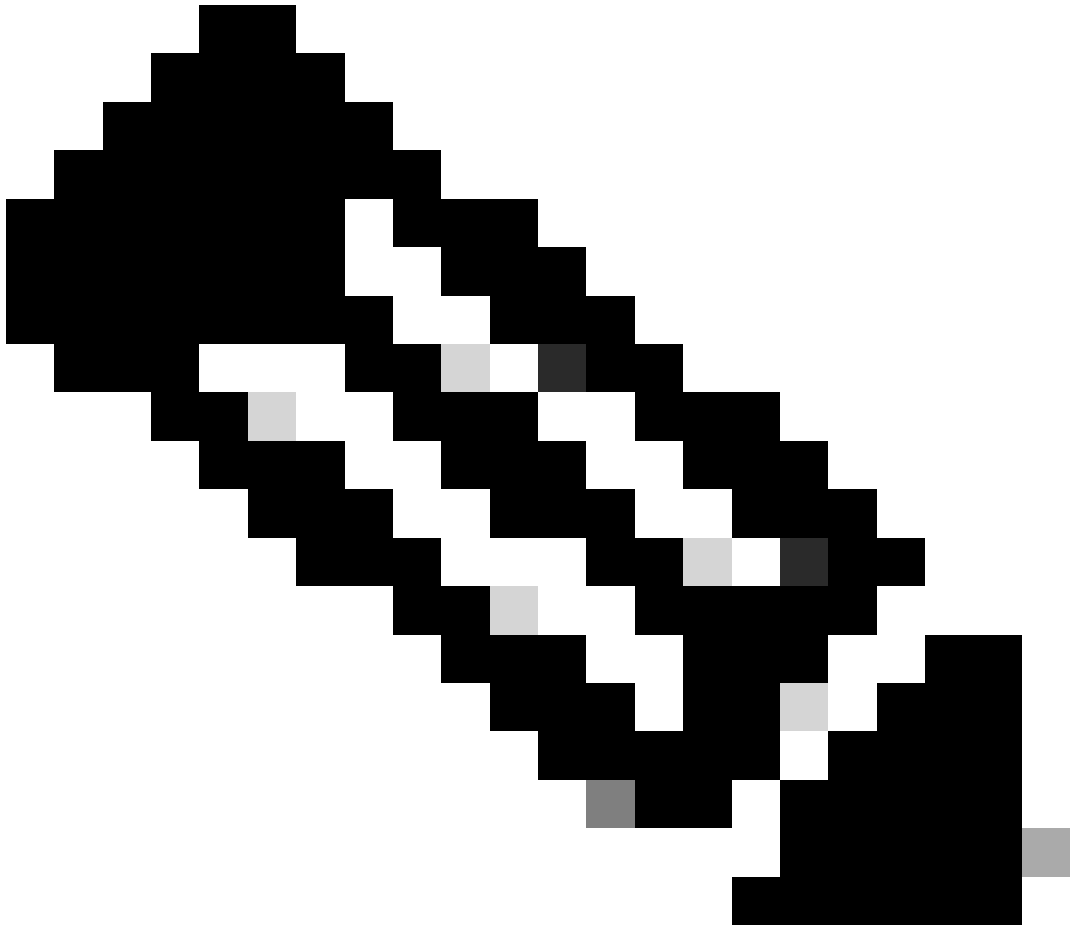
- Der FQDN des Zertifikats muss als lokale Domäne auf dem Umbrella Dashboard konfiguriert werden, damit die VA dies als lokale Domäne erkennt.
- Private Schlüssel und Zertifikate müssen im Format .key bzw. .cer erstellt werden.
- Zu diesem Zweck können Sie entweder selbstsignierte Zertifikate oder CA-signierte Zertifikate verwenden.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Virtuelle Appliance mit Version 2.7 oder höher
- Umbrella AD Connector muss Version 1.5 oder höher ausführen
- Umbrella Chromebook Clients müssen Version 1.3.3 oder höher ausführen

---



Anmerkung: Wenn Ihr VA oder AD Connector frühere Versionen ausführen, können Sie

---

ein Support-Ticket bei Umbrella öffnen, um ein Upgrade auf die entsprechenden unterstützten Versionen zu erhalten.

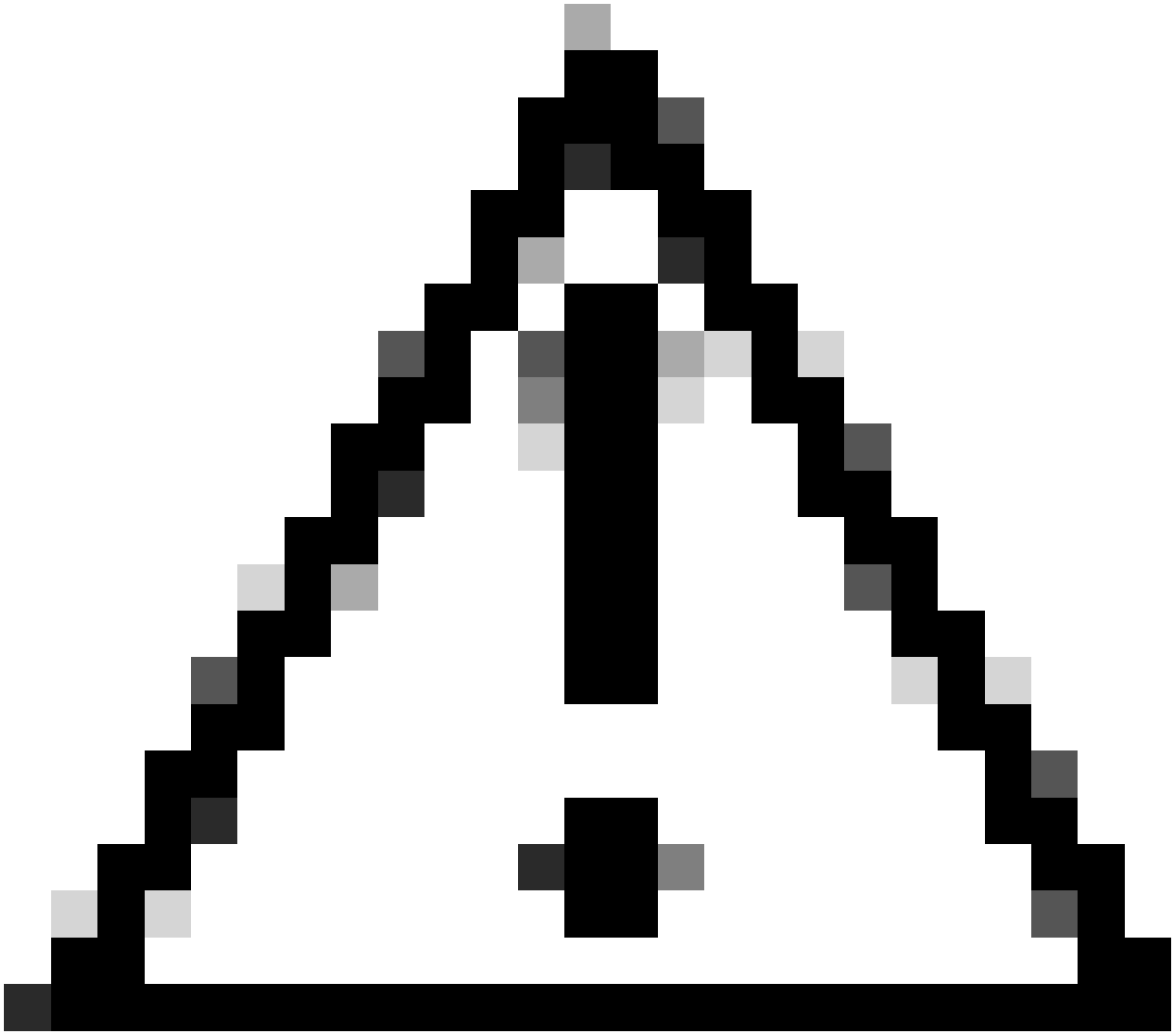
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Virtuelle Umbrella Appliances mit Version 2.6 oder früheren Versionen unterstützen das Empfangen von Benutzer-IP-Zuordnungen vom Umbrella Active Directory (AD) Connector und den Umbrella Chromebook Clients nur in unverschlüsselter Form auf Port 443. Daher war es eine zwingende Voraussetzung für die Bereitstellung, dass der AD Connector und VA- oder Chromebook Clients und VA nur über ein vertrauenswürdiges Netzwerk kommunizieren.

Ab Version 2.7 können virtuelle Umbrella Appliances AD-Benutzer-IP-Zuordnungen vom AD Connector über HTTPS und ähnlich GSuite-Benutzer-IP-Zuordnungen von jedem Umbrella Chromebook Client über HTTPS empfangen.

In diesem Artikel werden die Konfigurationsschritte für die einzelnen Komponenten beschrieben, um die HTTPS-Kommunikation zu aktivieren. Standardmäßig ist die HTTPS-Kommunikation deaktiviert, und der AD-Connector und die Chromebook-Clients kommunizieren nur über HTTP mit der VA.



Vorsicht: Durch das Aktivieren dieser Funktion können die CPU- und Speicherauslastung in der VA und dem Umbrella AD Connector erhöht und der DNS-Durchsatz für die VA reduziert werden. Daher wird empfohlen, diese Funktion nur zu aktivieren, wenn dies aufgrund von Compliance-Anforderungen für Ihr Unternehmen erforderlich ist.

Virtuelle Appliance

Hinzufügen eines privaten Schlüssels und Zertifikats zur VA

So fügen Sie der VA den privaten Schlüssel und das Zertifikat hinzu:
1. Öffnen Sie die Datei mit dem privaten Schlüssel mit einem Texteditor.

2. Wählen Sie alle aus, kopieren Sie sie, und fügen Sie dann die doppelten Anführungszeichen für diesen Befehl ein:

```
config va ssl key "paste the contents of the .key file here"
```

Zertifikat zur VA hinzufügen

So fügen Sie das Zertifikat der VA hinzu:
1. Öffnen Sie die Zertifikatsdatei mit einem Texteditor.

2. Wählen Sie alle aus, kopieren Sie sie, und fügen Sie dann die doppelten Anführungszeichen für den folgenden Befehl ein:

```
config va ssl cert "paste the contents of the .crt file here"
```

Aktivieren von HTTPS in der VA

Aktivieren Sie HTTPS in der VA mit dem folgenden Befehl:

```
config va ssl enable
```

Überprüfung der HTTPS-Aktivierung

Überprüfen Sie mithilfe des folgenden Befehls, ob HTTPS aktiviert ist:

```
config va show
```

Die Ausgabe dieses Befehls kann den HTTPS-Status sowie Details zum SSL-Zertifikat enthalten.

Beispiel:

```
HTTPS status : enabled
SSL Certificate Start Time : 2024-04-16 16:11:08
SSL Certificate Expiry Time : 2025-04-16 16:11:08
Issuer : C = US, ST = MASSACHUSETTS, L = BOSTON, O = CISCOSUPPORT, CN = server.domain.com
Common Names : vmhost.domain.com
```

Es kann bis zu 20 Minuten dauern, bis die VA Ereignisse über HTTPS empfängt. Nach etwa 20 Minuten können Sie mit dem Befehl `config va status` überprüfen. Der AD Connector-Status befindet sich in der Zwischenzeit im gelben Zustand (gestoppt) und wechselt in den grünen Zustand, sobald die VA beginnt, Ereignisse über HTTPS zu empfangen.

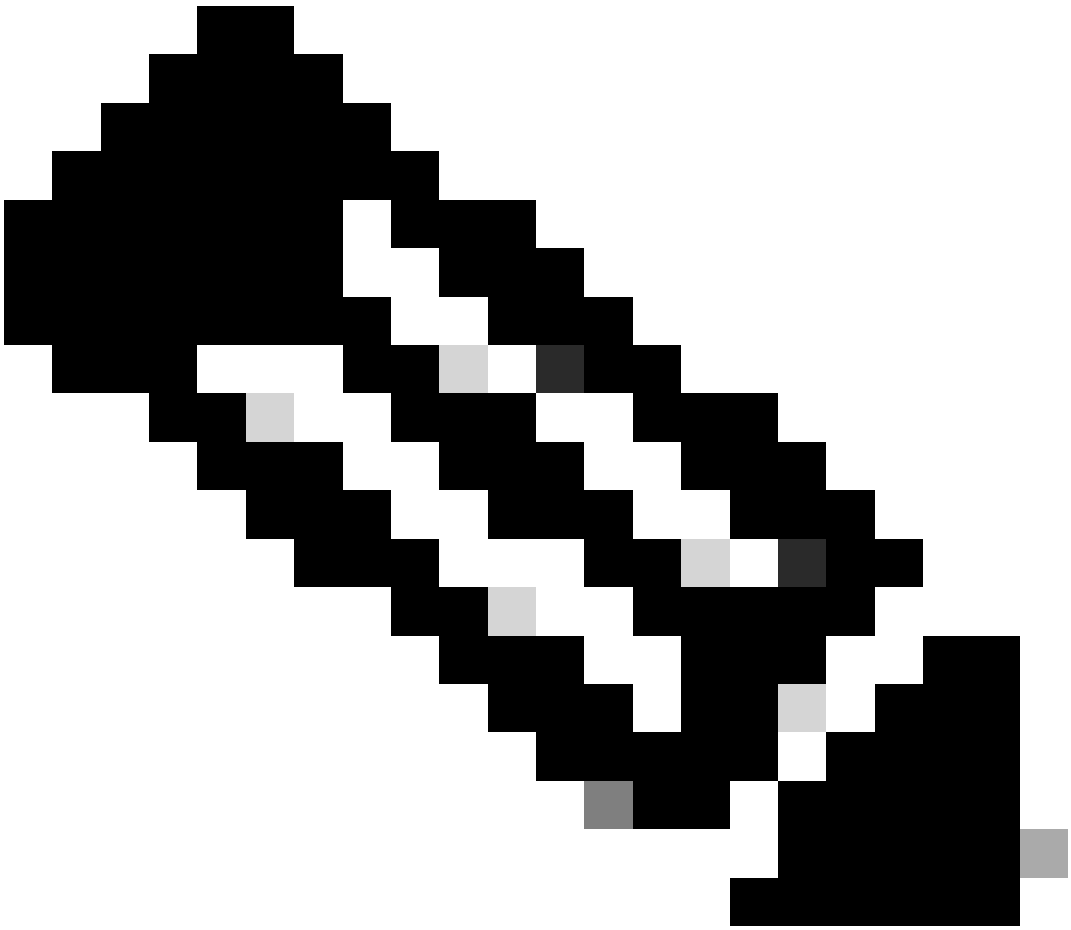
Wenn Sie HTTPS deaktivieren und zu HTTP zurückkehren möchten, verwenden Sie den Befehl `config va ssl disable`.

Wenn Sie HTTPS erneut aktivieren möchten, müssen Sie den privaten Schlüssel und das Zertifikat erneut hinzufügen und dann den Befehl `config va enable` verwenden.

Active Directory

Wenn Sie ein CA-signiertes Zertifikat für jede VA verwenden, stellen Sie sicher, dass das Root-Zertifikat und das ausstellende CA-Zertifikat für jedes VA-Zertifikat auf jedem System installiert sind, auf dem der AD Connector am gleichen Standort wie die VA ausgeführt wird.

Wenn Sie selbstsignierte Zertifikate für jede VA verwenden, stellen Sie sicher, dass jedes VA-Zertifikat auf jedem System installiert ist, auf dem der AD Connector im gleichen Umbrella-Standort wie die VA ausgeführt wird.



Anmerkung: Auf dem AD-Connector müssen nur Zertifikate für VAs installiert werden, die

---

sich am selben Umbrella-Standort wie der AD-Connector befinden.

Es kann bis zu 20 Minuten dauern, bis die VA den HTTPS-Status mit Umbrella synchronisiert, das dann mit dem AD-Connector synchronisiert wird. Daher kann es bis zu 20 Minuten dauern, bis der Connector beginnt, Daten über HTTPS an die VA zu senden. Alle in diesem Zeitraum gesendeten Benutzer-IP-Zuordnungen werden von der VA verworfen. Es wird daher empfohlen, die Konfigurationsänderung in der VA nur während der Ausfallzeiten vorzunehmen, wenn keine Benutzeranmeldungen erwartet werden.

Umbrella Android-Client

Wenn Sie CA-signierte Zertifikate für VAs verwenden, stellen Sie sicher, dass das Stammzertifikat und die ausstellenden CA-Zertifikate für jedes VA-Zertifikat an jedes Android-Gerät übertragen und dort installiert werden.

Wenn Sie selbstsignierte Zertifikate für VAs verwenden, stellen Sie sicher, dass jedes VA-Zertifikat auf jedes Android-Gerät übertragen und dort installiert wird.

Sobald das Zertifikat verfügbar ist, kann der Umbrella Android Client mit diesem Zertifikat beginnen, einen HTTPS-Kanal mit der VA einzurichten.

Umbrella Chromebook Client

Wenn Sie CA-signierte Zertifikate für VAs verwenden, stellen Sie sicher, dass das Stammzertifikat und die ausstellenden CA-Zertifikate für jedes VA-Zertifikat an jedes Chromebook übertragen und dort installiert werden.

Wenn Sie selbstsignierte Zertifikate für VAs verwenden, stellen Sie sicher, dass jedes VA-Zertifikat an jedes Chromebook übertragen und dort installiert wird.

Sobald das Zertifikat verfügbar ist, kann der Umbrella Chromebook Client mit diesem Zertifikat beginnen, um einen HTTPS-Kanal mit der VA einzurichten.

Weitere Informationen finden Sie im Artikel Umbrella Chromebook Client: Senden von Benutzer-IP-Zuordnungen über einen sicheren Kanal an die Umbrella Virtual Appliance.

Konfigurationssequenz

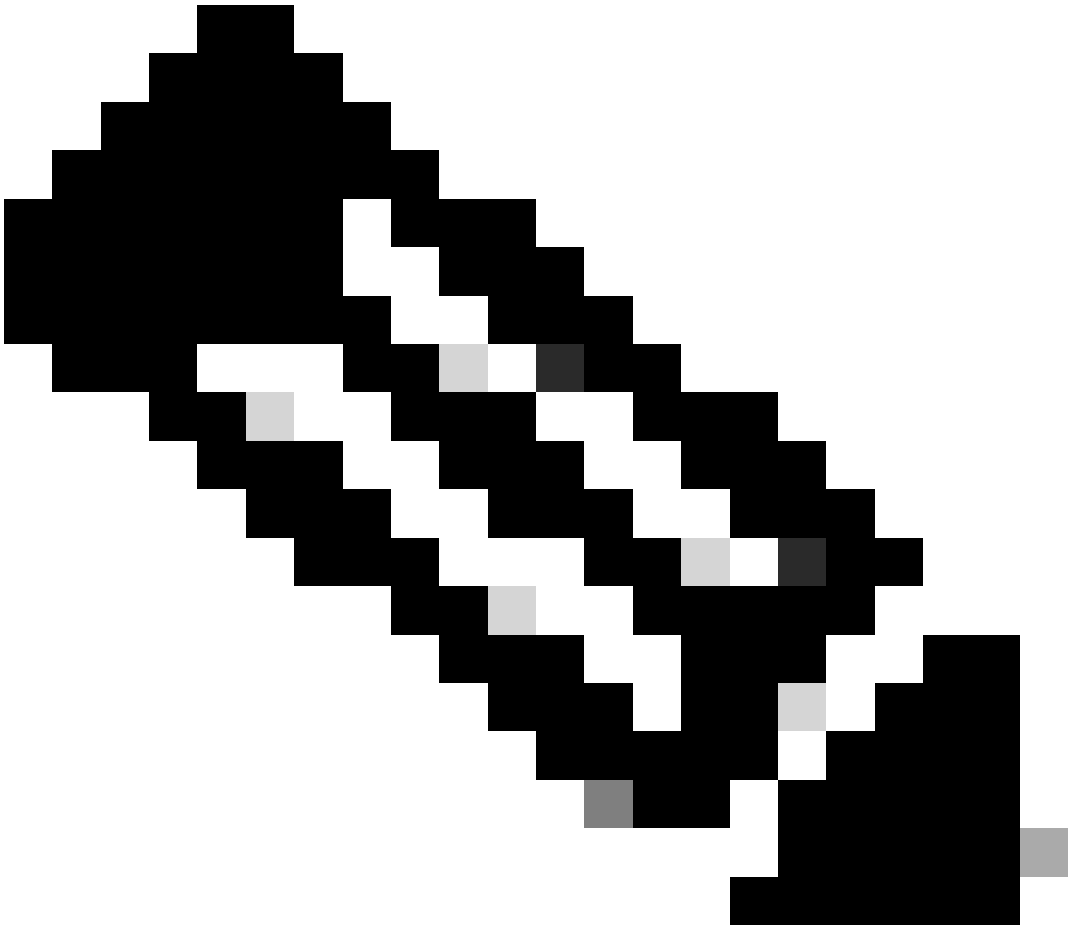
Wenn HTTPS in der VA aktiviert ist, akzeptiert die VA keine Benutzer-IP-Zuordnungen, die unverschlüsselt über HTTP gesendet werden. Daher werden alle über HTTP gesendeten Benutzeranmeldungen verworfen, und die Benutzerzuordnung für DNS-Anfragen dieser Benutzer ist nicht verfügbar. Es wird daher empfohlen, die folgenden Komponenten in dieser Reihenfolge zu konfigurieren:

1. Erstellen Sie das Zertifikat und den privaten Schlüssel für jede VA auf der Grundlage eines CA-signierten oder selbstsignierten Zertifikats.

2. Fügen Sie das Zertifikat und den privaten Schlüssel zu jeder VA hinzu.

3. Stellen Sie sicher, dass das Root-Zertifikat und die übergeordneten Zwischenzertifikate für jedes VA-Zertifikat (oder VA-selbstsigniertes Zertifikat) auf jedem System installiert sind, auf dem der AD-Connector am gleichen Standort wie das VA ausgeführt wird, und auf jedem Chromebook.

4. Aktivieren Sie während der Ausfallzeiten HTTPS in der VA.



Anmerkung: Das Zertifikat in der VA muss vor Ablauf ausgetauscht werden, und das dazwischen liegende übergeordnete Zertifikat und das Root-Zertifikat müssen auf den AD Connector- und Umbrella Chromebook-Clients installiert werden. Ist dies nicht der Fall, können die AD Connector- und Umbrella-Chromebook-Clients nicht mit der VA kommunizieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.