Installation des Root-Zertifikats auf SDWAN-vEdges

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie ein Root-Zertifikat in SD-WAN-vEdges mit verschiedenen Tools installiert wird.

Voraussetzungen

Anforderungen

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

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)
- Zertifikate
- Grundlegendes Linux

Verwendete Komponenten

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.

- Cisco Catalyst SD-WAN-Validator 20.6.3
- Cisco vEdge 20.6.3

Problem

Ein digitales Zertifikat ist eine elektronische Datei, die die Authentizität eines Geräts, Servers oder Benutzers mithilfe von Kryptografie und PKI (Public Key Infrastructure) zertifiziert. Mithilfe der digitalen Zertifikatsauthentifizierung können Organisationen sicherstellen, dass nur vertrauenswürdige Geräte und Benutzer eine Verbindung zu ihren Netzwerken herstellen können.

Die Identität für vEdge-Hardware-Router wird durch ein von Avnet signiertes Gerätezertifikat bereitgestellt, das während des Herstellungsprozesses generiert und in den TPM-Chip (Trusted Platform Module) eingebrannt wird. Die Symantec/DigiCert- und Cisco Root-Zertifikate sind in der Software vorinstalliert, um die Zertifikate der Steuerungskomponenten als vertrauenswürdig anzuerkennen. Zusätzliche Root-Zertifikate müssen entweder manuell geladen, automatisch vom SD-WAN-Manager verteilt oder während des automatisierten Bereitstellungsprozesses installiert werden.

Eines der häufigsten Probleme in SD-WAN ist der Ausfall der Steuerverbindungen aufgrund eines ungültigen Zertifikats. Dies ist entweder darauf zurückzuführen, dass das Zertifikat nie installiert wurde, oder darauf, dass es beschädigt wurde.

Verwenden Sie den Befehl EXEC show control connections-history, um die Fehlerlegende "Control Connection" (Steuerelementverbindung) zu überprüfen.

<#root>

```
vEdge #

show control connections-history


Legend for Errors
ACSRREJ    - Challenge rejected by peer.              NOVMCFG   - No cfg in vmanage for device.
BDSGVERFL  - Board ID Signature Verify Failure.       NOZTPEN   - No/Bad chassis-number entry in ZTP.
BIDNTPR    - Board ID not Initialized.                OPERDOWN  - Interface went oper down.
BIDNTVRFD  - Peer Board ID Cert not verified.         ORPTMO    - Server's peer timed out.
BIDSIG    - Board ID signing failure.                 RMGSPR    - Remove Global saved peer.
CERTEXPRD  - Certificate Expired                      RXTRDWN   - Received Teardown.
CRTREJSER  - Challenge response rejected by peer.     RDSIGFBD  - Read Signature from Board ID failed.


CRTVERFL   - Fail to verify Peer Certificate.

          SERNTPRES - Serial Number not present.
CTORGNMMIS - Certificate Org name mismatch.           SSLNFAIL  - Failure to create new SSL context.
DCONFAIL   - DTLS connection failure.                 STNMODETD - Teardown extra vBond in STUN server
DEVALC     - Device memory Alloc failures.            SYSIPCHNG - System-IP changed
DHSTMO     - DTLS HandShake Timeout.                  SYSPRCH   - System property changed
DISCVBD    - Disconnect vBond after register reply.   TMRALC    - Timer Object Memory Failure.
DISTLOC    - TLOC Disabled.                           TUNALC    - Tunnel Object Memory Failure.
DUPCLHELO  - Recd a Dup Client Hello, Reset Gl Peer.  TXCHTOBD  - Failed to send challenge to BoardID.
DUPSER     - Duplicate Serial Number.                 UNMSGBDRG - Unknown Message type or Bad Register
DUPSYSIPDEL- Duplicate System IP.                     UNAUTHEL  - Recd Hello from Unauthenticated peer
HAFAIL     - SSL Handshake failure.                   VBDEST    - vDaemon process terminated.
IP_TOS     - Socket Options failure.                  VECRTREV  - vEdge Certification revoked.
LISFD      - Listener Socket FD Error.                VSCRTREV  - vSmart Certificate revoked.
MGRTBLCKD  - Migration blocked. Wait for local TMO.   VB_TMO    - Peer vBond Timed out.
MEMALCFL   - Memory Allocation Failure.               VM_TMO    - Peer vManage Timed out.
NOACTVB    - No Active vBond found to connect.        VP_TMO    - Peer vEdge Timed out.
NOERR      - No Error.                                VS_TMO    - Peer vSmart Timed out.
```

```
NOSLPRCRT  - Unable to get peer's certificate.         XTVMTRDN  - Teardown extra vManage.
NTPRVMINT  - Not preferred interface to vManage.       XTVSTRDN  - Teardown extra vSmart.
STENTRY    - Delete same tloc stale entry.

PEER     PEER     PEER             SITE        DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID     PRIVATE IP       PORT     PUBLIC IP        PORT
-------------------------------------------------------------------------------------------------------
vbond    dtls     -                0           0      10.10.10.1     12346    10.10.10.1     12346   pu
vbond    dtls     -                0           0      10.10.10.2     12346    10.10.10.2     12346   pu
```

Einige häufige Ursachen für das Fehlerlabel CRTVERFL sind:

- Das Ablaufdatum des Zertifikats.
- Root-ca ist anders.
  - Legt fest, ob eine Aktualisierung von root-ca in Controllern erfolgt.
  - Eine von Cisco abweichende Zertifizierungsstelle (Certificate Authority, CA) wird verwendet, und Geräte müssen die Root-Zertifizierungsstelle manuell installieren.
- Änderung der Zertifizierungsstelle im Overlay.

Hinweis: Weitere Informationen zu Steuerungsverbindungsfehlern finden Sie unter Problembehandlung bei SD-WAN-Steuerungsverbindungen.

Die Root-CA-Datei muss für alle Komponenten im Overlay identisch sein. Es gibt zwei Möglichkeiten, zu überprüfen, ob die verwendete Root-CA-Datei nicht die richtige ist.

1. Überprüfen Sie die Größe der Datei, dies ist hilfreich in Situationen, in denen die root-ca eine Aktualisierung hatte.

<#root>

```
vBond:/usr/share/viptela$ ls -l
total 5
-rw-r--r-- 1 root root   294 Jul 23 2022 ISR900_pubkey.der
-rw-r--r-- 1 root root  7651 Jul 23 2022 TPMRootChain.pem
-rw-r--r-- 1 root root 16476 Jul 23 2022 ViptelaChain.pem
-rwxr-xr-x 1 root root 32959 Jul 23 2022 ios_core.pem

-rw-r--r-- 1 root root 24445 Dec 28 13:59 root-ca.crt
```

<#root>

```
vEdge:/usr/share/viptela$ ls -l
total 6
drwxr-xr-x 2 root root   4096 Aug 28  2022 backup_certs
-rw-r--r-- 1 root root   1220 Dec 28 13:46 clientkey.crt
-rw------- 1 root root   1704 Dec 28 13:46 clientkey.pem
-rw------- 1 root root   1704 Dec 28 13:46 proxy.key
-rw-r--r-- 1 root root      0 Aug 28  2022 reverse_proxy_mapping
```

```
-rw-r--r-- 1 root root 23228 Aug 28 2022 root-ca.crt
```

2. Zweite und zuverlässigste Möglichkeit, zu überprüfen, dass die Datei genau die gleiche wie die Quelldatei ist mit dem Befehl md5sum root-ca.crt vshell. Sobald md5 bereitgestellt ist, vergleichen Sie das Ergebnis der beiden Komponenten Controller und Edge-Gerät.

<#root>

vBond:/usr/share/viptela$

md5sum root-ca.crt

a4f945b9a1f50f1fa68d539dcf2e54f2 root-ca.crt

<#root>

vEdge:/usr/share/viptela$

md5sum root-ca.crt

b36358d01b36254a54db2f8db2266ced root-ca.crt

Hinweis: Da der Befehl md5sum root-ca.crt vshell verwendet wird, um die Integrität von Dateien zu überprüfen, da praktisch jede Änderung an einer Datei dazu führt, dass der MD5-Hash anders ist.

Lösung

Die Stammzertifikatkette eines Geräts kann mit mehreren Tools installiert werden. Es gibt zwei Möglichkeiten, es mithilfe von Linux-Befehlen zu installieren.

Erstellen Sie root-ca mit dem Linux CAT-Befehl in vShell

Hinweis: Dieses Verfahren gilt für Root-CA-Dateien, die keine leeren Zeilen innerhalb des Inhalts haben, für Situationen mit leeren Zeilen, die Linux vi Editor-Prozedur verwendet.

Schritt 1: Holen Sie die Datei "root-ca.crt" vom Validator ab, und kopieren Sie sie.

Die Root-CA ist auf allen Controllern gleich und kann von jedem Controller im Pfad/usr/share/viptela/ kopiert werden.

<#root>

vBond#

vshell

vBondvBond:~$

cat /usr/share/viptela/root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Schritt 2: Erstellen Sie die Datei root-ca.crt im vedge.

Navigieren Sie von vshell zu /home/admin oder /home/<benutzername> und erstellen Sie die Datei root-ca.crt.

<#root>

vEdge#

vshell

vEdge:~$

cat <<"" >> root-ca.crt

```
> -----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
```

```
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
>
vEdge:~$
```

Schritt 3: Validierung abgeschlossen ist.

<#root>

```
vEdge:~$
```

cat root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
vEdge:~$
```

Hinweis: Es ist wichtig, zu überprüfen, ob die Datei vollständig ist. Wenn Sie sie nicht vollständig sind, löschen Sie die Datei mit dem Befehl rm root-ca.crt vshell und erstellen Sie sie erneut in Schritt 2.

Beenden Sie vshell und fahren Sie mit dem Abschnitt fort.

<#root>

```
vEdge:~$
```

exit

Erstellen von root-ca mit VI Text Editor in vShell

Schritt 1: Holen Sie die Datei "root-ca.crt" vom Validator ab, und kopieren Sie sie.

Die Root-CA ist auf allen Controllern gleich und kann von jedem Controller im Pfad/usr/share/viptela/ kopiert werden.

<#root>

vBond#

vshell

vBond:~$

cat /usr/share/viptela/root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Schritt 2: Erstellen Sie die Datei root-ca.crt im vedge.

Navigieren Sie von vshell zu /home/admin oder /home/<benutzername> und erstellen Sie die Datei root-ca.crt.

<#root>

vEdge#

vshell

vEdge:~$

cd /usr/share/viptela/

vEdge:~$

pwd

```
/home/admin
vEdge:~$ vi root-ca.crt
```

Sobald Sie auf die Eingabetaste klicken, wird die Eingabeaufforderung des Editors angezeigt.

Schritt 3: In Einfügemodus wechseln

- Geben Sie i ein, und fügen Sie den Inhalt des Zertifikats aus Schritt 1 ein. Blättern Sie nach unten, und überprüfen Sie, ob das Zertifikat vollständig ist.

Schritt 4: Escape-Einfügemodus und Zertifikat speichern.

- Drücken Sie die ESC-Taste.
- Geben Sie :wq! gefolgt von der Eingabetaste ein, um die Änderungen zu speichern und den Editor zu beenden.

<#root>

vEdge:/usr/share/viptela$

cat root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Schritt 5: Validierung abgeschlossen ist.

<#root>

vEdge:~$

cat root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
```

```
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ8OM5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
vEdge:~$
```

Hinweis: Es ist wichtig, zu überprüfen, ob die Datei vollständig ist. Wenn Sie sie nicht vollständig sind, löschen Sie die Datei mit dem Befehl rm root-ca.crt vshell und erstellen Sie sie erneut in Schritt 2.

Beenden Sie vshell und fahren Sie mit dem Abschnitt fort.

<#root>

```
vEdge:~$
```

exit

Zertifikat installieren

Schritt 1: Installieren Sie das root-ca-Zertifikat mit dem Befehl request root-cert-chain install <path>.

<#root>

```
vEdge#
```

request root-cert-chain install /home/admin/root-ca.crt

```
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/PKI.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

Schritt 2: Überprüfen Sie, ob es mit dem Befehl show control local properties installiert wurde.

<#root>

```
vEdge#
```

show control local-properties

```
personality vedge
organization-name organization-name
root-ca-chain-status Installed
```

```
certificate-status Installed
certificate-validity Valid
certificate-not-valid-before Apr 11 17:57:17 2023 GMT
certificate-not-valid-after Apr 10 17:57:17 2024 GMT
```

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.