

Unified Communications-Cluster einrichten

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Überprüfung](#)

[CallManager Multi-Server SAN-Zertifikat](#)

[Fehlerbehebung](#)

[Bekanntes Hinweise](#)

Einleitung

In diesem Dokument wird die Einrichtung eines Unified Communications-Clusters mithilfe von CA-signierten Multi-Server-SAN-Zertifikaten (Certificate Authority) beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Unified Communications Manager (CUCM)
- CUCM IM und Presence-Version 10.5

Stellen Sie vor der Konfiguration sicher, dass die folgenden Services verfügbar und funktionsfähig sind:

- Administrations-Webservice für die Cisco Plattform
- Cisco Tomcat Service

Um diese Services über eine Webschnittstelle zu überprüfen, navigieren Sie zu **Cisco Unified Serviceability Page Services > Network Service > Select a server (Cisco Unified Serviceability Page-Services > Netzwerkservice > Server auswählen)**. Um sie in der CLI zu überprüfen, geben Sie den Befehl `utils service list` ein.

Wenn SSO im CUCM-Cluster aktiviert ist, muss es deaktiviert und erneut aktiviert werden.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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 verstehen.

Hintergrundinformationen

In CUCM-Version 10.5 und höher kann diese CSR-Anforderung (Certificate Signing Request) des Vertrauensstellungsspeichers einen alternativen Antragstellernamen (Subject Alternate Name, SAN) und alternative Domänen enthalten.

1. Tomcat - CUCM und IM&P
2. Cisco CallManager - Nur CUCM
3. Cisco Unified Presence - Extensible Messaging and Presence Protocol (CUP-XMPP) - nur IM&P
4. CUP-XMPP Server-to-Server (S2S) - nur IM&P

Es ist einfacher, ein CA-signiertes Zertifikat in dieser Version zu erhalten. Es ist nur ein CSR erforderlich, der von der CA signiert wird, und nicht die Anforderung, von jedem Serverknoten einen CSR zu erhalten und dann für jeden CSR ein CA-signiertes Zertifikat zu erhalten und diese einzeln zu verwalten.

Konfigurieren

Schritt 1:

Melden Sie sich bei der Betriebssystemverwaltung des Herausgebers an, und navigieren Sie zu **Security > Certificate Management > Generate CSR**.

Generate Certificate Signing Request

 Generate  Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat
Distribution*	cs-ccm-pub.v[redacted].com
Common Name*	cs-ccm-pub.v[redacted].com Multi-server(SAN)
Subject Alternate Names (SANs)	
Parent Domain	[redacted].com
Key Length*	
	2048
Hash Algorithm*	
	SHA256

Generate

Close



*- indicates required item.

Schritt 2:

Wählen Sie Multi-Server SAN in Distribution.

Generate Certificate Signing Request

 Generate  Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat
Distribution*	cs-ccm-pub.v[redacted].com
Common Name*	cs-ccm-pub.v[redacted].com Multi-server(SAN)
Subject Alternate Names (SANs)	
Parent Domain	[redacted].com
Key Length*	
	2048
Hash Algorithm*	
	SHA256

Generate

Close



*- indicates required item.

Die SAN-Domänen und die übergeordnete Domäne werden automatisch aufgefüllt.

Vergewissern Sie sich, dass alle Knoten Ihres Clusters für Tomcat aufgelistet sind: Alle CUCM- und IM&P-Knoten für CallManager: Es wurden nur CUCM-Knoten aufgelistet.

Generate Certificate Signing Request

Generate Close

Status

 Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose* tomcat

Distribution* Multi-server(SAN)

Common Name* cs-ccm-pub.com-ms

Subject Alternate Names (SANs)

Auto-populated Domains

- cs-ccm-pub.com
- cs-ccm-sub.com
- cs-imp.k.com

Parent Domain:com

Other Domains

No file selected.
Please import .TXT file only.
For more information please refer to the notes in the Help Section

Key Length* 2048

Hash Algorithm* SHA256

 *- indicates required item.

Schritt 3:

Klicken Sie auf "Generieren", und überprüfen Sie nach dem Generieren, ob alle im CSR aufgeführten Knoten auch in der Liste "Erfolgreicher CSR-Export" angezeigt werden.

Generate Certificate Signing Request

Generate Close

Status

Success: Certificate Signing Request Generated

CSR export operation successful on the nodes [cs-ccm-sub.com, cs-ccm-pub.com, cs-imp.com].

In der Zertifikatsverwaltung wird die SAN-Anforderung generiert:

Certificate List (1 - 15 of 15)

Find Certificate List where Certificate begins with tomcat Find Clear Filter + -

Certificate ^	Common Name	Type	Key Type	Distribution	Issued By
tomcat	115pub-ms-.....	CSR Only	RSA	Multi-server(SAN)	--
tomcat	115pub-ms-.....	CA-signed	RSA	Multi-server(SAN)

Schritt 4:

Klicken Sie auf **CSR herunterladen**, wählen Sie den Zertifikatzweck aus, und klicken Sie auf **CSR herunterladen**.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR **Download CSR**

Download Certificate Signing Request

Download CSR Close

Status

Warning: Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Purpose* tomcat

Download CSR Close

*- indicates required item.

Es ist möglich, die lokale Zertifizierungsstelle oder eine externe Zertifizierungsstelle wie VeriSign zu verwenden, um die CSR-Datei (Datei, die im vorherigen Schritt heruntergeladen wurde) zu signieren.

Dieses Beispiel zeigt die Konfigurationsschritte für eine auf Microsoft Windows Server basierende Zertifizierungsstelle. Wenn Sie eine andere Zertifizierungsstelle oder eine externe

Zertifizierungsstelle verwenden, fahren Sie mit Schritt 5 fort.

Melden Sie sich unter <https://<windowsserveripaddress>/certsrv/> an.

Wählen Sie **Zertifikat anfordern > Erweiterte Zertifikatanforderung**.

Kopieren Sie den Inhalt der CSR-Datei in das mit Base64 verschlüsselte Zertifikatanforderungsfeld, und klicken Sie auf **Submit (Senden)**.

The screenshot shows the 'Welcome' page of the Microsoft Active Directory Certificate Services web interface. The page title is 'Microsoft Active Directory Certificate Services -- vasank-DC1-CA'. The main content area contains the following text: 'Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).' Below this text, there is a section titled 'Select a task:' with three links: 'Request a certificate', 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'.

Senden Sie die CSR-Anfrage wie hier dargestellt.

The screenshot shows the 'Submit a Certificate Request or Renewal Request' page of the Microsoft Active Directory Certificate Services web interface. The page title is 'Microsoft Active Directory Certificate Services -- vasank-DC1-CA'. The main content area contains the following text: 'To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.' Below this text, there is a section titled 'Saved Request:' with a text area containing a base-64-encoded certificate request. The text area is labeled 'Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7)'. Below the text area, there is a section titled 'Additional Attributes:' with a text area labeled 'Attributes'. At the bottom of the page, there is a 'Submit' button.

The screenshot shows the 'Certificate Pending' page of the Microsoft Active Directory Certificate Services web interface. The page title is 'Microsoft Active Directory Certificate Services -- vasank-DC1-CA'. The main content area contains the following text: 'Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested. Your Request Id is 32. Please return to this web site in a day or two to retrieve your certificate. Note: You must return with this web browser within 10 days to retrieve your certificate'.

Schritt 5:

Hinweis: Stellen Sie vor dem Hochladen eines Tomcat-Zertifikats sicher, dass SSO deaktiviert ist. Falls sie aktiviert ist, muss SSO deaktiviert und erneut aktiviert werden, sobald der gesamte Tomcat-Zertifikatregenerierungsprozess abgeschlossen ist.

Laden Sie die Zertifizierungsstellenzertifikate mit dem signierten Zertifikat als tomcat-trust hoch. Zuerst das Root-Zertifikat und dann das Zwischenzertifikat, falls vorhanden.



Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR Download CSR

Upload Certificate/Certificate chain

Upload Close

Status



Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File certchain.p7b

Schritt 6:

Laden Sie jetzt das CUCM-signierte Zertifikat als Tomcat hoch, und überprüfen Sie, ob alle Knoten Ihres Clusters unter "Certificate upload operation successfully" aufgeführt sind, wie im Bild gezeigt:

Upload Certificate/Certificate chain

 Upload  Close

Status

-  Certificate upload operation successful for the nodes cs-ccm-pub.com,cs-ccm-sub.com,cs-imp.com.
-  Restart Cisco Tomcat Service for the nodes cs-ccm-pub.com,cs-ccm-sub.com,cs-imp.com using the CLI "utils service restart Cisco Tomcat".

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File No file selected.

 *- indicates required item.

Das Multi-Server-SAN wird in der Zertifikatsverwaltung aufgeführt, wie im Bild gezeigt:

ipsecc-trust	cs-ccm-pub.com	Self-signed	cs-ccm-pub.com	cs-ccm-pub.com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY.com	Self-signed	ITLRECOVERY.com	ITLRECOVERY.com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-ccm-pub.com.ms	CA-signed	Multi-server(SAN)DC1-CA	12/19/2015	Certificate Signed byDC1-CA
tomcat-trust	cs-ccm-pub.com.ms	CA-signed	Multi-server(SAN)DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	cs-ccm-pub.com	Self-signed	cs-ccm-pub.com	cs-ccm-pub.com	04/21/2019	Trust Certificate
tomcat-trust	VerSign_Class_3_Secure_Server_CA_-_G3	CA-signed	VerSign_Class_3_Secure_Server_CA_-_G3	VerSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	Trust Certificate
tomcat-trust	dc1-ccm-pub.com	Self-signed	dc1-ccm-pub.com	dc1-ccm-pub.com	04/17/2019	Trust Certificate
tomcat-trust	dc1-ccm-pub.com	Self-signed	dc1-ccm-pub.com	dc1-ccm-pub.com	04/18/2019	Trust Certificate
tomcat-trustDC1-CA	Self-signedDC1-CADC1-CA	04/29/2004	Root CA
TVS	cs-ccm-pub.com	Self-signed	cs-ccm-pub.com	cs-ccm-pub.com	04/18/2019	Self-signed certificate generated by system

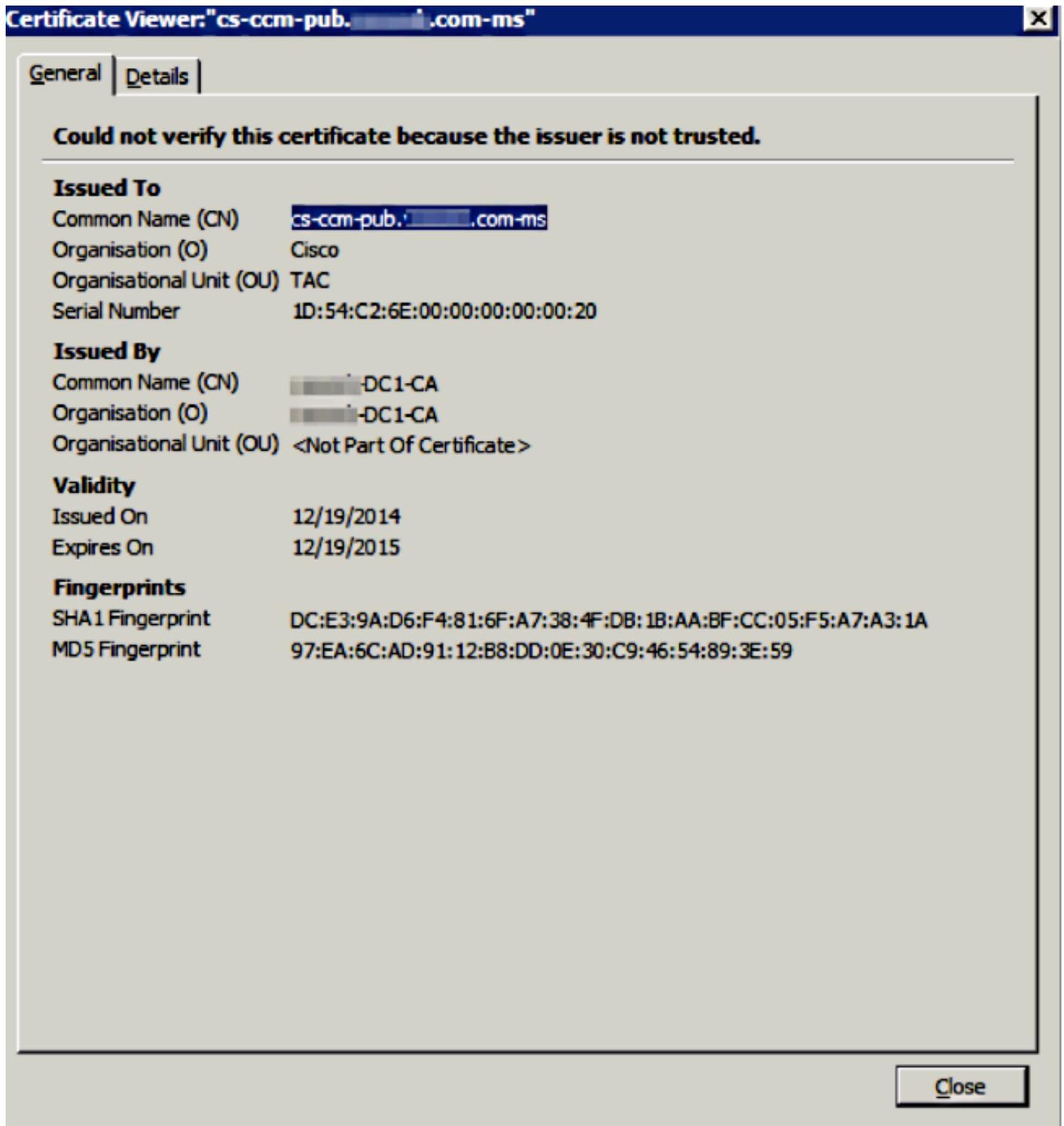
Schritt 7.

Starten Sie den Tomcat-Dienst auf allen Knoten in der SAN-Liste (zuerst Publisher und dann Subscriber) über CLI mit dem Befehl: `utils service restart Cisco Tomcat neu`.

```
admin:
admin:utils service restart Cisco Tomcat
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

Überprüfung

Melden Sie sich unter <http://<fqdnofccm>:8443/ccmadmin> an, um sicherzustellen, dass das neue Zertifikat verwendet wird.



CallManager Multi-Server SAN-Zertifikat

Ein ähnliches Verfahren kann für das CallManager-Zertifikat verwendet werden. In diesem Fall sind die automatisch ausgefüllten Domänen nur CallManager-Knoten. Wenn der Cisco CallManager-Dienst nicht ausgeführt wird, können Sie ihn in der SAN-Liste belassen oder entfernen.

Warnung: Dieser Prozess wirkt sich auf die Telefonregistrierung und die Anrufverarbeitung aus. Planen Sie ein Wartungsfenster für Arbeiten mit CUCM-/TVS-/ITL-/CAPF-Zertifikaten

ein.

Stellen Sie vor dem CA-signierten SAN-Zertifikat für CUCM Folgendes sicher:

- Das IP-Telefon kann dem Trust Verification Service (TVS) vertrauen. Dies kann durch den Zugriff auf einen beliebigen HTTPS-Service über das Telefon verifiziert werden. Wenn beispielsweise der Zugriff auf das Firmenverzeichnis funktioniert, bedeutet dies, dass das Telefon dem TVS-Dienst vertraut.
- Überprüfen Sie, ob sich der Cluster im ungesicherten oder gemischten Modus befindet.

Um festzustellen, ob es sich um einen Cluster im gemischten Modus handelt, wählen Sie **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Nicht sicher; 1 == Gemischter Modus)**.

Warnung: Wenn Sie sich vor dem Neustart der Dienste in einem Cluster im gemischten Modus befinden, muss die CTL aktualisiert werden: [Token](#) oder [Tokenlos](#).

Nachdem Sie das von der Zertifizierungsstelle ausgestellte Zertifikat installiert haben, muss die nächste Dienstliste in den aktivierten Knoten neu gestartet werden:

- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager
- Cisco Unified Serviceability > Tools > Control Center - Netzwerkservices > Cisco Trust Verification Service

Fehlerbehebung

Diese Protokolle unterstützen das Cisco Technical Assistance Center bei der Identifizierung von Problemen im Zusammenhang mit der Generierung von SAN-CSRs mit mehreren Servern und dem Hochladen eines von einer Zertifizierungsstelle signierten Zertifikats.

- API der Cisco Unified OS-Plattform
- Cisco Tomcat
- IPT-Plattform CertMgr-Protokolle
- [Zertifikatverlängerungsprozess](#)

Bekannte Hinweise

- Cisco Bug-ID [CSCur97909](#) - Beim Hochladen eines Multiserver-Zertifikats werden selbstsignierte Zertifikate in der DB nicht gelöscht.
- Cisco Bug-ID [CSCus47235](#) - CUCM 10.5.2 CN nicht dupliziert in SAN für CSR
- Cisco Bug-ID [CSCup28852](#) - Telefon-Reset alle 7 Minuten aufgrund von Zertifikat-Update, wenn Sie Multi-Server-Zertifikat verwenden

Wenn ein vorhandenes Multiserver-Zertifikat vorhanden ist, wird die Regenerierung in folgenden Szenarien empfohlen:

- Änderung des Hostnamens oder der Domäne Wenn ein Hostname oder eine

Domänenänderung vorgenommen wird, werden die Zertifikate automatisch als selbstsigniert neu generiert. Um sie in eine CA-Signiert zu ändern, müssen die vorherigen Schritte ausgeführt werden.

- Wenn dem Cluster ein neuer Knoten hinzugefügt wurde, muss ein neuer CSR generiert werden, um den neuen Knoten aufzunehmen.
- Wenn ein Abonnent wiederhergestellt wird und keine Sicherung verwendet wurde, kann der Knoten über neue selbstsignierte Zertifikate verfügen. Um den Subscriber aufzunehmen, kann ein neuer CSR für den gesamten Cluster erforderlich sein. (Es liegt eine Erweiterungsanfrage vor. Cisco Bug-ID: [CSCuv75957](#) um diese Funktion hinzuzufügen.)

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.