Selbstsignierte Zertifikate für CUCM IM/P-Dienst neu generieren

Inhalt

Einleitung

In diesem Dokument wird ein schrittweises Verfahren zur Neugenerierung von Zertifikaten in CUCM IM/P 8.x und höher empfohlen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der IM- und Presence-Service-Zertifikate (IM/P) verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf IM/P Version 8.x und höher.

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.

Hintergrundinformationen

Nutzung des Zertifikatspeichers

Cisco Unified Presence (CUP)-Zertifikat

Verwendung für sichere SIP-Verbindungen für SIP-Federation, Microsoft Remote Call Control für Lync/OCS/LCS, sichere Verbindung zwischen Cisco Unified Certificate Manager (CUCM) und IM/P usw.

Cisco Unified Presence - CUP-XMPP-Zertifikat (Extensible Messaging and Presence Protocol)

Wird verwendet, um sichere Verbindungen für XMPP-Clients zu validieren, wenn eine XMPP-Sitzung erstellt wird.

Cisco Unified Presence - Extensible Messaging and Presence Protocol - Server-zu-Server (CUP-XMPP-S2S)-Zertifikat

Wird verwendet, um sichere Verbindungen für XMPP-Domänenverbünde mit einem extern verbundenen XMPP-System zu validieren.

IP Security (IPSec)-Zertifikat

Verwendet für:

- Validierung sicherer Verbindungen für das Disaster Recovery System (DRS)/Disaster Recovery Framework (DRF)
- Validierung sicherer Verbindungen für IPsec-Tunnel zu Cisco Unified Communications Manager (CUCM) und IM/P-Knoten im Cluster

Tomcat-Zertifikat

Verwendet für:

- Validierung verschiedener Web-Zugriffe, z. B. Zugriff auf Service-Seiten von anderen Knoten im Cluster und Jabber Access
- Validierung sicherer Verbindungen für SAML Single Sign-On (SSO)
- Überprüfen der sicheren Verbindung für Intercluster-Peers

Achtung: Wenn Sie die SSO-Funktion auf Ihren Unified Communication-Servern verwenden und die Cisco Tomcat-Zertifikate neu generiert werden, muss die SSO mit den neuen Zertifikaten neu konfiguriert werden. Der Link zum Konfigurieren von SSO auf CUCM und ADFS 2.0 lautet: https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html.

Hinweis: Der Link zum Prozess für die Erneuerung/Erneuerung des CUCM-Zertifikats lautet: https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html.

Zertifikatserneuerung

CUP-Zertifikat

Schritt 1: Öffnen Sie eine grafische Benutzeroberfläche (GUI) für jeden Server in Ihrem Cluster. Beginnen Sie mit dem IM/P-Publisher, öffnen Sie dann nacheinander eine grafische Benutzeroberfläche für jeden IM/P-Subscriber-Server, und navigieren Sie zu Cisco Unified OS Administration > Security > Certificate Management.

Schritt 2: Beginnen Sie mit der Herausgeber-GUI, und wählen Sie, ob alle Zertifikate angezeigt werden sollenFind. Wählen Sie das cup.pem Zertifikat aus. Wählen Sie diese OptionRegenerate aus, und warten Sie, bis das Popup-Fenster geschlossen wird.

Schritt 3: Fahren Sie mit den nachfolgenden Abonnenten fort. Gehen Sie genauso vor wie in Schritt 2., und schließen Sie alle Abonnenten in Ihrem Cluster ab.

Schritt 4: Nachdem das CUP-Zertifikat auf allen Knoten neu generiert wurde, müssen die Dienste neu gestartet werden.

Hinweis: Wenn bei der Konfiguration der Presence Redundancy Group die Option Enable High Availability aktiviert ist, Uncheck muss diese vor dem Neustart der Services aktiviert werden. Auf die Konfiguration der Presence Redundancy Group kann unter zugegriffen werdenCUCM Pub Administration > System > Presence Redundancy Group. Ein Neustart der Services führt zu einem vorübergehenden Ausfall von IM/P und muss außerhalb der Produktionszeiten erfolgen.

Starten Sie die Dienste in dieser Reihenfolge neu:

- Melden Sie sich bei Cisco Unified Serviceability des Herausgebers an:

antwort: Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco SIP-Proxy-Service

c. Fahren Sie nach Abschluss des Dienstneustarts mit den Abonnenten und dem Cisco SIP-Proxy-Service fortRestart.

d. Beginnen Sie mit dem Herausgeber und dann weiter mit den Abonnenten. Restart Cisco SIP-Proxy-Service (auch von Cisco Unified Serviceability > Tools > Control Center - Feature Services).

- Melden Sie sich bei Cisco Unified Serviceability des Herausgebers an:

antwort: Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco Presence Engine-Service.

c. Fahren Sie nach Abschluss des Dienstneustarts mit dem Restart von Cisco Presence EngineService auf den Abonnenten fort.

Hinweis: Wenn für SIP-Federation konfiguriert, Restart Cisco XCP SIP Federation Connection Manager-Service (unter Cisco Unified Serviceability > Tools > Control Center - Feature Services). Beginnen Sie mit dem Herausgeber und dann weiter mit den Abonnenten.

CUP-XMPP-Zertifikat

Hinweis: Da Jabber die CUCM- und IM/P-Tomcat-Zertifikate sowie die CUP-XMPP-Serverzertifikate verwendet, um die Verbindungen für Tomcat und die CUP-XMPP-Services zu validieren, sind diese CUCM- und IM/P-Zertifikate in den meisten Fällen

---

CA-signiert. Angenommen, das Jabber-Gerät verfügt nicht über das Root-Zertifikat und ein Zwischenzertifikat, das Teil des CUP-XMPP-Zertifikats ist und im Zertifikatvertrauensspeicher installiert ist. In diesem Fall zeigt der Jabber-Client eine Sicherheitswarnung für das nicht vertrauenswürdige Zertifikat an. Wenn das Zertifikat des Jabber Device Trust Stores noch nicht installiert ist, müssen das Root- und alle Zwischenzertifikate über Gruppenrichtlinien, MDM, E-Mail usw. an das Jabber-Gerät gesendet werden. Dies hängt vom Jabber-Client ab.

Hinweis: Wenn das CUP-XMPP-Zertifikat selbstsigniert ist, zeigt der Jabber-Client eine Sicherheitswarnung für das nicht vertrauenswürdige Zertifikat an, wenn das CUP-XMPP-Zertifikat nicht im Trust Store des Jabber-Gerätezertifikats installiert ist. Wenn das selbstsignierte CUP-XMPP-Zertifikat nicht bereits installiert ist, muss es über Gruppenrichtlinien, MDM, E-Mail usw., die vom Jabber-Client abhängen, auf das Jabber-Gerät übertragen werden.

Schritt 1: Öffnen Sie eine grafische Benutzeroberfläche für jeden Server in Ihrem Cluster. Beginnen Sie mit dem IM/P-Publisher, öffnen Sie dann nacheinander eine GUI für jeden IM/P-Subscriber-Server, und navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management**.

Schritt 2: Beginnen Sie mit der Herausgeber-GUI, und wählen Sie, ob alle Zertifikate angezeigt werden sollenFind. Bestimmen Sie in der Typspalte für das cup-xmpp.pem Zertifikat, ob es selbstsigniert oder CA-signiert ist. Wenn es sich bei dem cup-xmpp.pem Zertifikat um eine von einem Drittanbieter signierte (vom Typ CA-signierte) Distribution Multi-SAN handelt, überprüfen Sie diesen Link, wenn Sie einen Multi-SAN CUP-XMPP CSR generieren und an CA für ein CA-signiertes CUP-XMPP-Zertifikat senden. Konfigurationsbeispiel für Unified Communication Cluster mit einem CA-signierten Multi-Server-Betreff.

Wenn es sich bei dem cup-xmpp.pem Zertifikat um einen von einem Drittanbieter signierten (vom Typ CA signierten) Verteilungs-Einzelknoten handelt (der Verteilungsname entspricht dem allgemeinen Namen für das Zertifikat), überprüfen Sie diesen Link, wenn Sie einen CUP-XMPP CSR für einen Einzelknoten generieren und an CA für ein CA-signiertes CUP-XMPP-Zertifikat senden; Jabber Complete How-To Guide for Certificate Validation. Wenn das cup-xmpp.pem Zertifikat selbstsigniert ist, fahren Sie mit Schritt 3 fort.

Schritt 3: Wählen Sie Find, um alle Zertifikate anzuzeigen, und wählen Sie dann das cup-xmpp.pem Zertifikat aus. Wählen Sie diese OptionRegenerate aus, und warten Sie, bis das Popup-Fenster geschlossen wird.

Schritt 4: Fahren Sie mit den nachfolgenden Abonnenten fort. Gehen Sie wie in Schritt 2 vor, und führen Sie diese Schritte für alle Abonnenten in Ihrem Cluster aus.

Schritt 5: Nachdem das CUP-XMPP-Zertifikat auf allen Knoten neu generiert wurde, muss der Cisco XCP-Router-Dienst auf den IM/P-Knoten neu gestartet werden.

Hinweis: Wenn in der Konfiguration der Presence Redundancy Group die Option "High Availability aktivieren" aktiviert ist, Uncheck muss dieser vor dem Neustart des Diensts aktiviert werden. Auf die Konfiguration der Presence Redundancy Group kann unter zugegriffen werdenCUCM Pub Administration > System > Presence Redundancy Group. Ein Neustart des Services führt zu einem vorübergehenden Ausfall von IM/P und muss außerhalb der Produktionszeiten erfolgen.

- Melden Sie sich bei Cisco Unified Serviceability des Herausgebers an:

antwort: Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart den Cisco XCP Router-Service.

c. Fahren Sie nach Abschluss des Service-Neustarts mit dem Restart Cisco XCP-Router-Service auf den Abonnenten fort.

CUP-XMPP-S2S-Zertifikat

Schritt 1: Öffnen Sie eine grafische Benutzeroberfläche für jeden Server in Ihrem Cluster. Beginnen Sie mit dem IM/P-Publisher, öffnen Sie nacheinander eine GUI für jeden IM/P-Subscriber-Server, und navigieren Sie zu Cisco Unified OS Administration > Security > Certificate Management.

Schritt 2: Beginnen Sie mit der Herausgeber-GUI, wählen Sie Find, dass alle Zertifikate angezeigt werden, und wählen Sie das cup-xmpp-s2s.pem Zertifikat aus. Wählen Sie diese OptionRegenerate aus, und warten Sie, bis das Popup-Fenster geschlossen wird.

Schritt 3: Fahren Sie mit den nachfolgenden Abonnenten fort, und verweisen Sie auf das gleiche Verfahren in Schritt 2. Führen Sie den Vorgang für alle Abonnenten in Ihrem Cluster aus.

Schritt 4: Nachdem das CUP-XMPP-S2S-Zertifikat auf allen Knoten neu generiert wurde, müssen die Dienste in der angegebenen Reihenfolge neu gestartet werden.

Hinweis: Wenn bei der Konfiguration der Presence-Redundanzgruppe die Option "Hohe Verfügbarkeit aktivieren" aktiviert ist,Uncheck erfolgt dies vor dem Neustart dieser Services. Auf die Konfiguration der Presence Redundancy Group kann zugegriffen werden CUCM Pub Administration > System > Presence Redundancy Group. Ein Neustart der Services führt zu einem vorübergehenden Ausfall von IM/P und muss außerhalb der Produktionszeiten erfolgen.

- Melden Sie sich bei Cisco Unified Serviceability des Herausgebers an:

antwort: Cisco Unified Serviceability > Tools > Control Center - Network Services.
b. Restart den Cisco XCP Router-Service.
c. Fahren Sie nach Abschluss des Service-Neustarts mit Restart des Cisco XCP-Router-Service auf den Abonnenten fort.

- Melden Sie sich bei Cisco Unified Serviceability des Herausgebers an:

antwort: Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart den Cisco XCP XMPP Federation Connection Manager-Dienst.

c. Fahren Sie nach Abschluss des Dienstneustarts mit dem Dienst Restart des Cisco XCP XMPP Federation Connection Manager auf den Abonnenten fort.

IPSec-Zertifikat

Hinweis: Das ipsec.pem Zertifikat im CUCM-Publisher muss gültig sein und in allen Subscribern (CUCM- und IM/P-Knoten) im IPSec-Trust Store vorhanden sein. Das ipsec.pem Zertifikat des Abonnenten ist im Publisher nicht als IPSec-Vertrauensspeicher in einer Standardbereitstellung vorhanden. Um die Gültigkeit zu überprüfen, vergleichen Sie die Seriennummern im ipsec.pem Zertifikat vom CUCM-PUB mit dem IPSec-Trust in den Teilnehmern. Sie müssen übereinstimmen.

Hinweis: Der DRS verwendet eine SSL-basierte Kommunikation (Secure Socket Layer) zwischen dem Quell-Agent und dem lokalen

---

Agent zur Authentifizierung und Verschlüsselung von Daten zwischen den CUCM-Clusterknoten (CUCM- und IM/P-Knoten). DRS nutzt die IPSec-Zertifikate für seine Public/Private Key-Verschlüsselung. Beachten Sie, dass DRS nicht wie erwartet funktioniert, wenn Sie die IPSEC-hostname.pem Vertrauensspeicherdatei (IPSEC Trust Store) von der Seite für die Zertifikatsverwaltung löschen. Wenn Sie die IPSEC-Vertrauensdatei manuell löschen, müssen Sie sicherstellen, dass Sie das IPSEC-Zertifikat in den IPSEC-Vertrauensspeicher hochladen. Weitere Informationen finden Sie auf der Hilfeseite zum Zertifikatsmanagement in den CUCM-Sicherheitsleitfäden.

Schritt 1: Öffnen Sie eine grafische Benutzeroberfläche für jeden Server in Ihrem Cluster. Beginnen Sie mit dem IM/P-Publisher, öffnen Sie nacheinander eine GUI für jeden IM/P-Subscriber-Server, und navigieren Sie zu Cisco Unified OS Administration > Security > Certificate Management.

Schritt 2: Beginnen Sie mit der Herausgeber-GUI, und wählen Sie, Find um alle Zertifikate anzuzeigen.Choose das Zertifikatipsec.pem. Wählen Sie diese OptionRegenerate aus, und warten Sie, bis das Popup-Fenster geschlossen wird.

Schritt 3: Fahren Sie mit den nachfolgenden Abonnenten fort, und verweisen Sie auf das gleiche Verfahren in Schritt 2. Führen Sie den Vorgang für alle Abonnenten in Ihrem Cluster aus.

Schritt 4: Nachdem alle Knoten das IPSEC-Zertifikat neu generiert haben, werden dannRestart diese Dienste bereitgestellt. Navigieren Sie zu Cisco Unified Serviceability des Herausgebers; Cisco Unified Serviceability > Tools > Control Center - Network Services.
Restart a. Wählen Sie im primären Cisco DRF-Service die Option aus.
b. Wählen Sie nach Abschluss des Dienstneustarts Restart den lokalen Cisco DRF-Dienst auf dem Publisher aus, und fahren Sie dann mit Restart dem lokalen Cisco DRF-Dienst auf jedem Subscriber fort.

Tomcat-Zertifikat

Hinweis: Da Jabber die CUCM-Tomcat-, IM/P-Tomcat- und CUP-XMPP-Serverzertifikate verwendet, um die Verbindungen für Tomcat- und CUP-XMPP-Services zu validieren, sind diese CUCM- und IM/P-Zertifikate in den meisten Fällen CA-signiert. Angenommen, auf dem Jabber-Gerät sind weder der Root noch ein Zwischenzertifikat, das Teil des Tomcat-Zertifikats ist, in dessen Zertifikatvertrauensspeicher installiert. In diesem Fall zeigt der Jabber-Client eine Sicherheitswarnung für das nicht vertrauenswürdige Zertifikat an. Wenn das Zertifikat nicht bereits im Zertifikatvertrauensspeicher des Jabber-Geräts installiert ist, müssen der Root und alle Zwischenzertifikate per Gruppenrichtlinie, MDM, E-Mail usw. an das Jabber-Gerät gesendet werden. Dies hängt vom Jabber-Client ab.

Hinweis: Wenn das Tomcat-Zertifikat selbstsigniert ist, zeigt der Jabber-Client eine Sicherheitswarnung für das nicht vertrauenswürdige Zertifikat an, wenn das Tomcat-Zertifikat nicht im Zertifikatvertrauensspeicher des Jabber-Geräts installiert ist. Wenn das selbstsignierte CUP-XMPP-Zertifikat nicht bereits im Zertifikatvertrauensspeicher des Jabber-Geräts installiert ist, muss es per Gruppenrichtlinie, MDM, E-Mail usw. an das Jabber-Gerät gesendet werden. Dies hängt vom Jabber-Client ab.

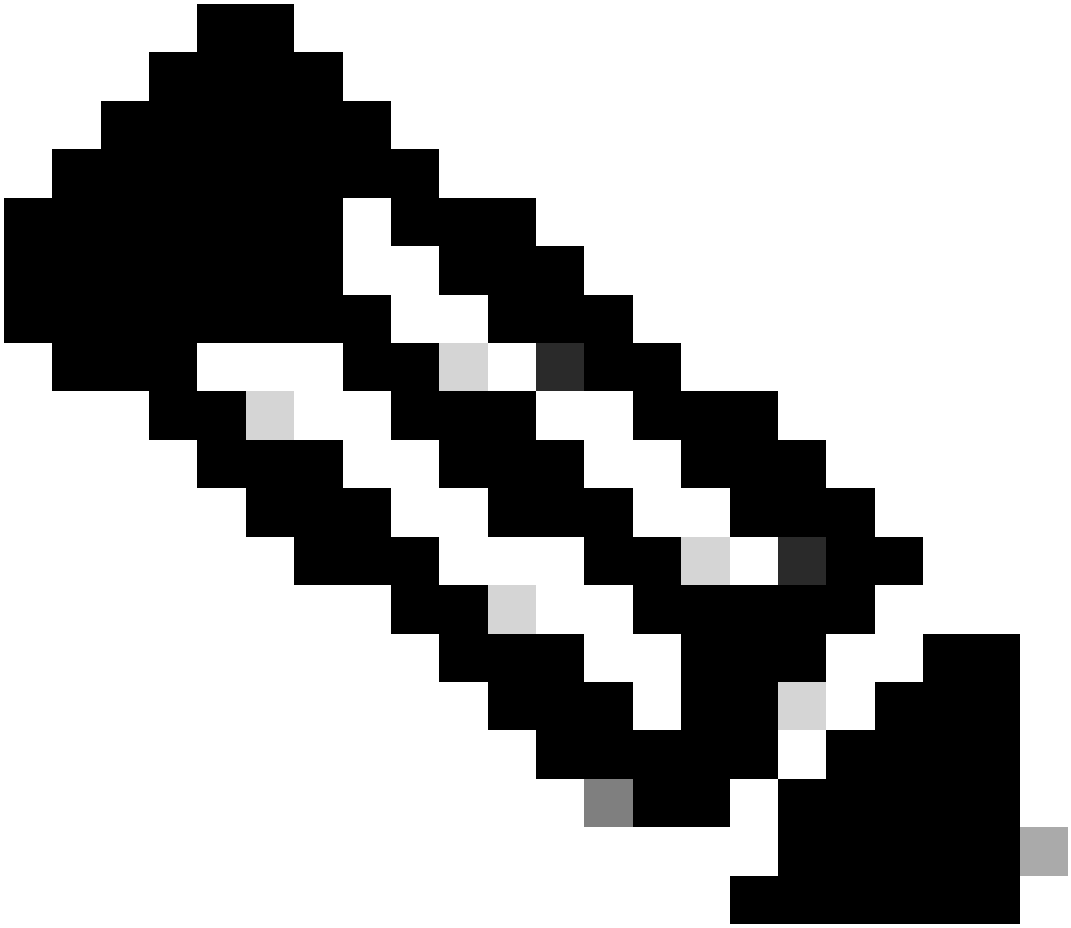
Schritt 1: Öffnen Sie eine grafische Benutzeroberfläche für jeden Server in Ihrem Cluster. Beginnen Sie mit dem IM/P-Publisher, öffnen Sie nacheinander eine GUI für jeden IM/P-Subscriber-Server, und navigieren Sie zu Cisco Unified OS Administration > Security > Certificate Management.

Schritt 2: Beginnen Sie mit der Herausgeber-GUI, und wählen Sie, Find um alle Zertifikate anzuzeigen.

- Bestimmen Sie in der Spalte Type (Typ) für das tomcat.pem Zertifikat, ob es selbstsigniert oder CA-signiert ist.

- Wenn es sich bei dem tomcat.pem Zertifikat um ein von einem Drittanbieter signiertes (vom Typ CA-signiertes) Distributions-Multi-SAN handelt, lesen Sie diesen Link, um einen Multi-SAN Tomcat CSR zu generieren und an CA für ein CA-signiertes Tomcat-Zertifikat zu senden. Unified Communication Cluster Setup mit CA-signiertem Multi-Server Subject Alternate Name Configuration Example

---



Hinweis: Der Multi-SAN-Tomcat-CSR wird auf dem CUCM-Publisher generiert und an alle CUCM- und IM/P-Knoten im Cluster verteilt.

- Wenn es sich bei dem tomcat.pem Zertifikat um einen signierten Verteilungsknoten eines Drittanbieters (Typ CA-signiert) handelt (der Verteilungsname entspricht dem Common Name für das Zertifikat), überprüfen Sie diesen Link, um einen CUP-XMPP CSR für einen einzelnen Knoten zu generieren, und senden Sie ihn an CA für ein CUP-XMPP-Zertifikat mit CA-Signierung, Jabber Complete How-To Guide for Certificate Validation

· Wenn das tomcat.pem Zertifikat selbstsigniert ist, fahren Sie mit Schritt 3 fort.

Schritt 3: Wählen SieFind diese Option, um alle Zertifikate anzuzeigen:

· Wählen Sie das tomcat.pem Zertifikat aus.

Regenerate · Sobald Sie geöffnet haben, wählen Sie und warten Sie, bis Sie das Erfolgs-Pop-up sehen, bevor das Pop-up geschlossen wird.

Schritt 4: Fahren Sie mit jedem nachfolgenden Abonnenten fort, lesen Sie das Verfahren in Schritt 2, und schließen Sie alle Abonnenten in Ihrem Cluster ab.

Schritt 5: Nachdem alle Knoten das Tomcat-Zertifikat neu generiert habenRestart, wird der Tomcat-Dienst auf allen Knoten neu erstellt. Beginnen Sie mit dem Verlag, gefolgt von den Abonnenten.

· Um den Restart Tomcat-Dienst zu aktivieren, müssen Sie eine CLI-Sitzung für jeden Knoten öffnen und den Befehl ausführen, bis der Dienst Cisco Tomcat neu startet, wie im Bild gezeigt:

Abgelaufene Vertrauenszertifikate löschen

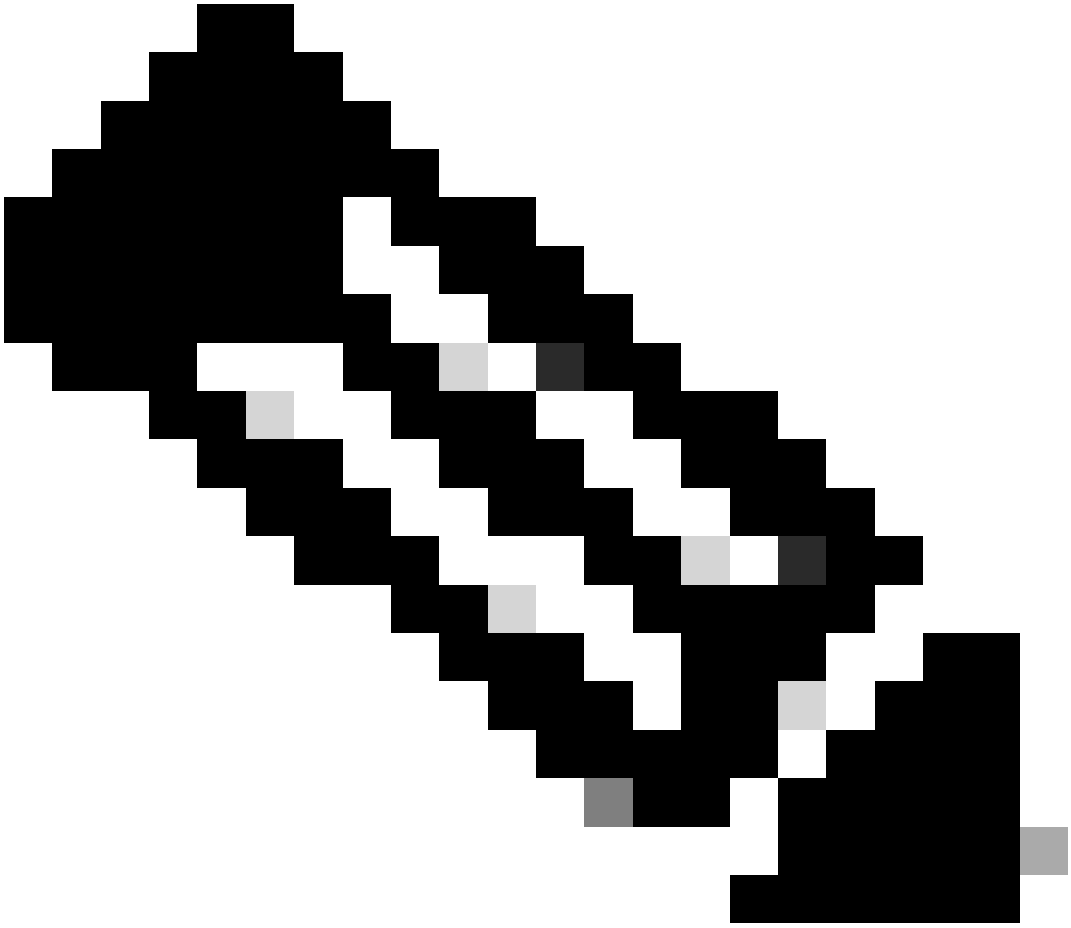
Hinweis: Vertrauenswürdige Zertifikate (die auf "-trust" enden) können bei Bedarf gelöscht werden. Vertrauenswürdige Zertifikate, die gelöscht werden können, sind Zertifikate, die nicht mehr benötigt werden, abgelaufen sind oder veraltet sind. Löschen Sie nicht die fünf Identitätszertifikate: die cup.pem , cup-xmpp.pem , cup-xmpp-s2s.pem , ipsec.pem und tomcat.pem Zertifikate. Der Dienst startet neu, wie dargestellt, um alle Informationen aus dem Arbeitsspeicher dieser Legacy-Zertifikate innerhalb dieser Dienste zu löschen.

Hinweis: Wenn in der Konfiguration der Presence Redundancy Group die Option Enable High Availability (Hochverfügbarkeit aktivieren) aktiviert ist, Uncheck muss dies geschehen, bevor ein Service aktiviert wird Stopped/Started oder Restarted. Auf die Konfiguration der Presence Redundancy Group kann unter zugegriffen werdenCUCM Pub Administration > System > Presence Redundancy Group. Ein Neustart einiger Dienste führt, wie dargestellt, zu einem vorübergehenden Ausfall von IM/P und muss außerhalb der Produktionszeiten erfolgen.

Schritt 1: Navigieren Sie zu:Cisco Unified Serviceability > Tools > Control Center - Network Services

· Wählen Sie aus dem Dropdown-Menü Ihren IM/P-Publisher aus, wählen Sie Stop Cisco Certificate Expiry Monitor und dann Cisco Intercluster Sync Agent ausStop.

· Wiederholen Sie Stop diese Services für jeden IM/P-Knoten in Ihrem Cluster.



Hinweis: Wenn das Tomcat-trust-Zertifikat gelöscht werden muss, navigieren Sie zum Cisco Unified Serviceability > Tools > Control Center - Network Services des CUCM-Herausgebers.

- Wählen Sie aus dem Dropdown-Menü den CUCM-Publisher aus.
- Wählen Sie Stop im Cisco Certificate Expiry Monitor und anschließend in Cisco Certificate Change Notification ausStop.
- Wiederholen Sie den Vorgang für jeden CUCM-Knoten in Ihrem Cluster.

Schritt 2: Navigieren Sie zu Cisco Unified OS Administration > Security > Certificate Management > Find.

- Suchen Sie nach abgelaufenen Vertrauenszertifikaten (für Version 10.x und höher können Sie nach Ablauf filtern. Bei älteren Versionen als 10.0 müssen Sie die jeweiligen Zertifikate manuell oder über die RTMT-Warnmeldungen identifizieren, falls diese

eingehen).

- Das gleiche Vertrauenszertifikat kann in mehreren Knoten auftreten, es muss einzeln von jedem Knoten gelöscht werden.
- Wählen Sie das zu löschende Vertrauenszertifikat aus (je nach Version erhalten Sie entweder ein Popup-Fenster oder Sie werden auf derselben Seite zum Zertifikat navigiert).

- Wählen Sie Delete (Sie erhalten ein Popup, das mit "Sie sind im Begriff, dieses Zertifikat endgültig zu löschen..." beginnt).
•Klicken Sie auf OK.

Schritt 3: Wiederholen Sie den Vorgang für jedes Vertrauenszertifikat, das gelöscht werden soll.

Schritt 4: Nach Fertigstellung müssen Dienste neu gestartet werden, die sich direkt auf die gelöschten Zertifikate beziehen.

- CUP-Trust: Cisco SIP Proxy, Cisco Presence Engine und, falls für SIP Federation konfiguriert, Cisco XCP SIP Federation Connection Manager (siehe Abschnitt "CUP-Zertifikat")
- CUP-XMPP-trust: Cisco XCP Router (siehe Abschnitt CUP-XMPP-Zertifikat)
- CUP-XMPP-S2S-Trust: Cisco XCP-Router und Cisco XCP XMPP Federation Connection Manager
- IPSec-trust: DRF Source/DRF Local (siehe IPSec-Zertifikatabschnitt)
- Tomcat-trust: Starten Sie den Tomcat-Dienst über die Befehlszeile neu (siehe Tomcat-Zertifikatabschnitt).

Schritt 5: In Schritt 1 beendete Neustartdienste.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

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.