Regeneration von Zertifikaten für CUCM

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Neugenerierung von Zertifikaten in Cisco Unified Communications Manager (CUCM) Version 8.x und höher beschrieben.

Voraussetzungen

Anforderungen

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

- *Real Time Monitoring Tool* (RTMT)
- CUCM-Zertifikate

Verwendete Komponenten

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

- CUCM 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 verstehen.

Hintergrundinformationen

In diesem Dokument werden die einzelnen Schritte zur Neuerstellung von Zertifikaten in Cisco Unified Communications Manager (CUCM) Version 8.x und neueren Versionen beschrieben. Dies spiegelt jedoch nicht die Änderungen nach 12.0 an der ITL-Wiederherstellung wider.

RTMT installieren

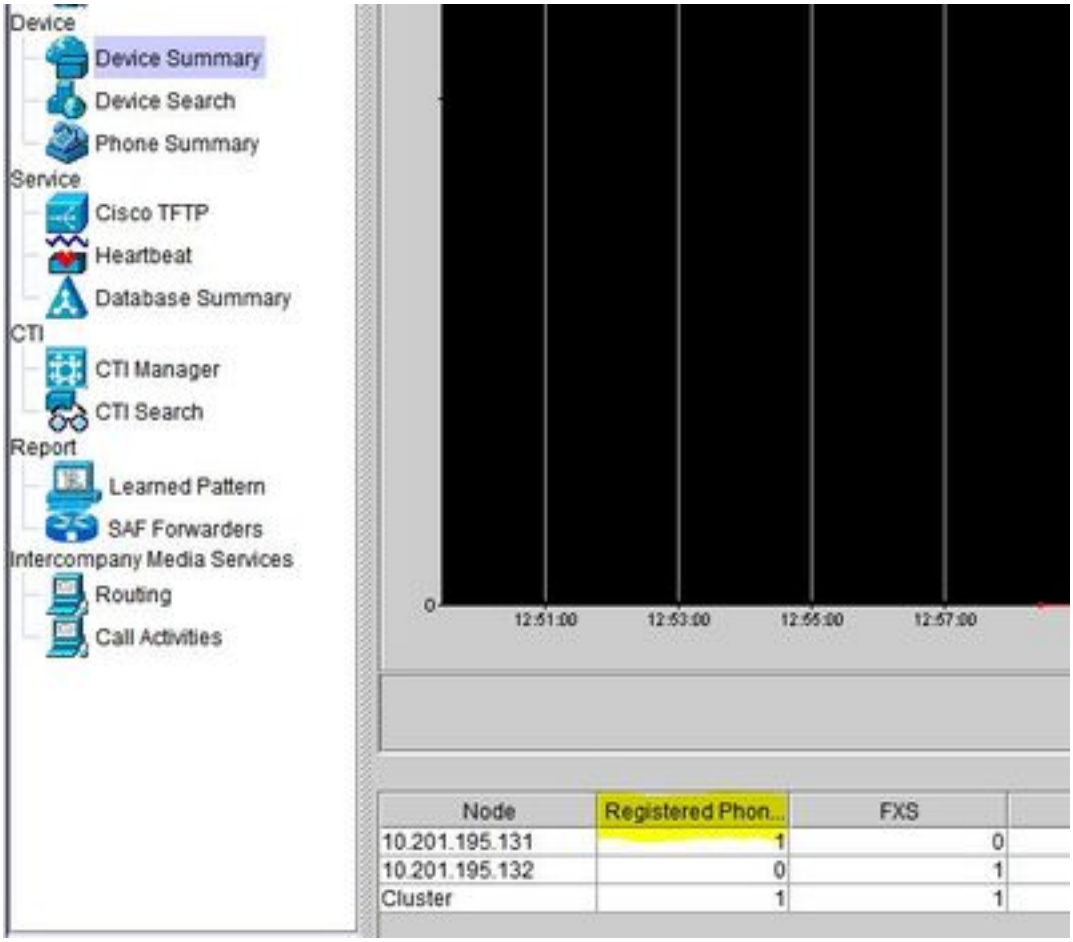
- Laden Sie das RTMT-Tool vom Call Manager herunter, und installieren Sie es. Navigieren Sie zu Call Manager (CM) Administration: **Anwendung > Module > Suchen > Cisco Unified Real-Time Monitoring Tool - Windows > Herunterladen** Installation und Start

Endgeräte mit RTMT überwachen

- Starten Sie RTMT, und geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) sowie Benutzername und Kennwort für den Zugriff auf das Tool ein:
- Wählen Sie die **Registerkarte Voice/Video (Sprache/Video)**.Wählen Sie **Geräteübersicht aus**. In diesem Abschnitt werden die Gesamtzahl der registrierten Endpunkte und die Anzahl der Verbindungen zu den einzelnen Knoten angegeben.Überwachung beim Zurücksetzen des Endgeräts, um die Registrierung vor der Erneuerung des nächsten Zertifikats sicherzustellen

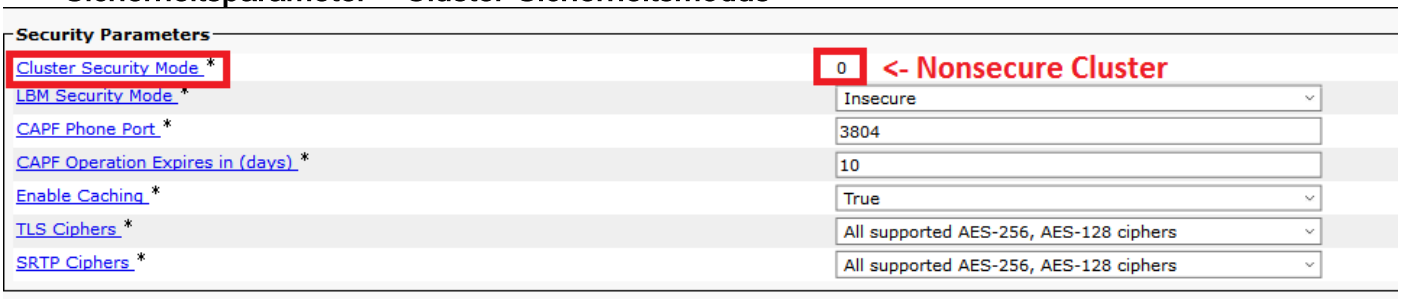
Tipp: Der Regenerationsprozess einiger Zertifikate kann sich auf den Endpunkt auswirken. Berücksichtigen Sie einen Aktionsplan nach den regulären Geschäftszeiten, da die Services neu gestartet und Telefone neu gestartet werden müssen. Überprüfen Sie, ob eine Telefonregistrierung über RTMT dringend empfohlen wird.

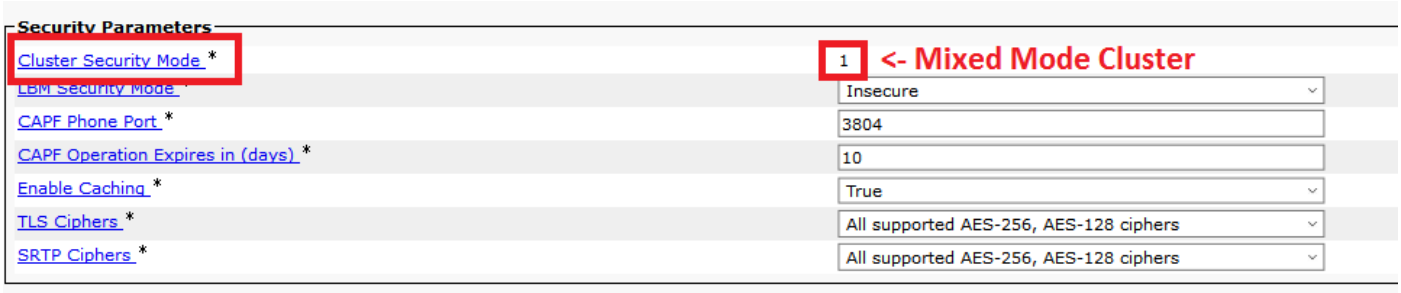
Warnung: Bei Endpunkten mit aktuellen ITL-Diskrepanzen können nach diesem Prozess Registrierungsprobleme auftreten. Das Löschen des ITL auf dem Endpunkt stellt eine typische Best Practice-Lösung dar, nachdem der Regenerationsprozess abgeschlossen und alle anderen Telefone registriert wurden.



Ermitteln Sie, ob sich Ihr Cluster im gemischten Modus oder im ungesicherten Modus befindet.

- Navigieren Sie zu CM Administration. **System > Unternehmensparameter > Sicherheitsparameter > Cluster-Sicherheitsmodus**





Auswirkungen durch den Zertifikatspeicher

Für eine erfolgreiche Systemfunktionalität ist es wichtig, dass alle Zertifikate im gesamten CUCM-Cluster aktualisiert werden. Wenn Zertifikate abgelaufen oder ungültig sind, können sie die

normale Funktionalität des Systems erheblich beeinträchtigen. Die Auswirkungen können je nach Systemeinrichtung unterschiedlich sein. Eine Liste der Dienste für die jeweiligen ungültigen oder abgelaufenen Zertifikate wird angezeigt:

CallManager.pem

- Verschlüsselte/authentifizierte Telefone registrieren sich nicht
- Trivial File Transfer Protocol (TFTP) ist nicht vertrauenswürdig (Telefone akzeptieren keine signierten Konfigurationsdateien und/oder ITL-Dateien)
- Betroffene Telefondienste
- SIP-Trunks (Secure Session Initiation Protocol) oder Medienressourcen (Conference Bridges, Media Termination Point (MTP), Xcoder usw.) können nicht registriert oder verwendet werden.
- Die AXL-Anfrage schlägt fehl.

Tomcat.pem

- Telefone können nicht auf HTTPS-Services zugreifen, die auf dem CUCM-Knoten gehostet werden, z. B. Unternehmensverzeichnis
- Der CUCM kann verschiedene Webprobleme haben, z. B. wenn von anderen Knoten im Cluster nicht auf die Service-Seiten zugegriffen werden kann.
- Probleme mit Extension Mobility (EM) oder Extension Mobility über Cluster hinweg
- Single Sign-On (SSO)
- Wenn UCCX (Unified Contact Center Express) integriert ist, muss aufgrund einer Sicherheitsänderung von CCX 12.5 das CUCM-Tomcat-Zertifikat (selbstsigniert) oder das Tomcat-Root- und Zwischenzertifikat (für CA-signierte Zertifikate) in den UCCX-Tomcat-Trust-Speicher hochgeladen werden, da dies Auswirkungen auf die Desktop-Anmeldungen von Finesse hat.

CAPF.pem

- Telefone führen keine Authentifizierung für Telefon-VPN, 802.1x oder Telefon-Proxy durch
- Für die Telefone können keine LSC-Zertifikate (Locally Significant Certificate) ausgestellt werden.
- Verschlüsselte Konfigurationsdateien funktionieren nicht

IPSec.pem

- Das Disaster Recovery System (DRS)/Disaster Recovery Framework (DRF) funktioniert nicht ordnungsgemäß.
- IPsec-Tunnel zum Gateway (GW) zu anderen CUCM-Clustern funktionieren nicht

TVS (Trust Verification Service)

Der Trust Verification Service (TVS) ist die Hauptkomponente von Security by Default. Mit dem TVS können Cisco Unified IP-Telefone Anwendungsserver wie EM-Services, das Verzeichnis und MIDlet authentifizieren, wenn HTTPS eingerichtet ist.

Der TVS bietet folgende Funktionen:

- Skalierbarkeit - Die Anzahl der Zertifikate, denen Sie vertrauen können, hat keine Auswirkungen auf die Ressourcen des Cisco Unified IP-Telefons.
- Flexibilität - Das Hinzufügen oder Entfernen von Vertrauenszertifikaten wird automatisch im System übernommen.
- Sicherheit als Standard - Nicht medienbezogene und Signalsicherheitsfunktionen sind Teil der Standardinstallation und erfordern keinen Benutzereingriff.

ITL und CTL

- ITL enthält die Zertifikatrolle für Call Manager TFTP, alle TVS-Zertifikate im Cluster und bei Ausführung die CAPF (Certificate Authority Proxy Function).
- Die CTL enthält Einträge für das System Administrator Security Token (SAST), den Cisco CallManager und Cisco TFTP-Services, die auf demselben Server ausgeführt werden, sowie Einträge für CAPF, TFTP-Server und die ASA-Firewall (Adaptive Security Appliance). Auf den TVS wird in der CTL nicht verwiesen.

Zertifikatserneuerung

> **Anmerkung:** Alle Endgeräte müssen eingeschaltet und registriert werden, bevor die Zertifikate regeneriert werden können. Andernfalls muss für die nicht verbundenen Telefone die ITL entfernt werden.

Tomcat-Zertifikat

Identifizieren, ob Zertifikate von Drittanbietern verwendet werden:

1. Navigieren Sie zu jedem Server in Ihrem Cluster (auf separaten Registerkarten Ihres Webbrowsers), und beginnen Sie mit dem Herausgeber, gefolgt von jedem Abonnenten. Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Beachten Sie in der Spalte Description (Beschreibung), ob Tomcat das vom System generierte selbstsignierte Zertifikat angibt. Wenn Tomcat von einem Drittanbieter signiert wurde, folgen Sie dem angegebenen Link und führen diese Schritte nach der Tomcat-Regeneration durch.Von Drittanbietern signierte Zertifikate finden Sie unter CUCM-Upload CCMAdmin-Web-GUI-Zertifikate.
2. Wählen Sie **Suchen**, um alle Zertifikate anzuzeigen: Wählen Sie das **Tomcat PEM-**Zertifikat aus.Wählen Sie anschließend **Regenerieren** und warten Sie, bis das Popup-Fenster Erfolg angezeigt wird. Schließen Sie das Popup-Fenster, oder gehen Sie zurück, und wählen Sie **Suchen/Liste aus**.
3. Fahren Sie mit jedem nachfolgenden Abonnenten fort. Befolgen Sie die gleichen Schritte in Schritt 2, und schließen Sie alle Abonnenten in Ihrem Cluster ab.
4. Nachdem alle Knoten das Tomcat-Zertifikat neu generiert haben, starten Sie den Tomcat-Dienst auf allen Knoten neu. Beginnen Sie mit dem Verlag dann von den Abonnenten gefolgt. Um Tomcat neu zu starten, müssen Sie für jeden Knoten eine CLI-Sitzung öffnen

und den Befehl utils **service restart Cisco Tomcat** ausführen.

5. Diese Schritte müssen ggf. in der CCX-Umgebung durchgeführt werden:

- Wenn ein selbstsigniertes Zertifikat verwendet wird, laden Sie die Tomcat-Zertifikate von allen Knoten des CUCM-Clusters in den Unified CCX Tomcat Trust Store hoch.
- Wenn ein von einer Zertifizierungsstelle signiertes oder privates Zertifikat verwendet wird, laden Sie das Stammzertifikat der Zertifizierungsstelle von CUCM in den Unified CCX Tomcat-Vertrauensspeicher hoch.
- Starten Sie die Server neu, wie im Dokument zur Zertifikaterneuerung für CCX beschrieben.

Weitere Referenzen:

- UCCX Solution Certificate Management-Leitfaden
- Unified CCX Health Check Utility

IPSEC-Zertifikat

Anmerkung: CUCM/Instant Messaging und Presence (IM&P) vor Version 10.x der DRF Master Der Agent wird auf CUCM Publisher und IM&P Publisher ausgeführt. Der lokale DRF-Dienst wird auf den jeweiligen Abonnenten ausgeführt. Versionen 10.X und höher, DRF Master Der Agent wird nur auf dem CUCM-Publisher und der lokale DRF-Service auf den CUCM-Abonnenten sowie auf dem IM&P-Publisher und den Abonnenten ausgeführt.

Anmerkung: Das Disaster Recovery System verwendet eine SSL-basierte Kommunikation zwischen den Master Agent und der lokale Agent zur Authentifizierung und Verschlüsselung von Daten zwischen den CUCM-Clusterknoten. DRS nutzt die IPSec-Zertifikate für seine Public/Private Key-Verschlüsselung. Beachten Sie, dass DRS nicht wie erwartet funktioniert, wenn Sie die IPSEC-Truststore-Datei (hostname.pem) von der Seite für die Zertifikatsverwaltung löschen. Wenn Sie die IPSEC-trust-Datei manuell löschen, müssen Sie sicherstellen, dass Sie das IPSEC-Zertifikat in den IPSEC-trust-store hochladen. Weitere Informationen finden Sie auf der Hilfeseite zum Zertifikatsmanagement in den Cisco Unified Communications Manager-Sicherheitsleitfäden.

1. Navigieren Sie zu jedem Server in Ihrem Cluster (auf separaten Registerkarten Ihres Webbrowsers), und beginnen Sie mit dem Herausgeber, gefolgt von jedem Abonnenten. Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find**:
   Wählen Sie das **IPSEC-**Zertifikat **für PEM aus**.Wählen Sie anschließend **Regenerieren** und warten Sie, bis das Popup-Fenster Erfolg angezeigt wird. Schließen Sie das Popup-Fenster, oder gehen Sie zurück, und wählen Sie **Suchen/Liste aus**.
2. Mit nachfolgenden Abonnenten fortfahren; Befolgen Sie das gleiche Verfahren in Schritt 1, und schließen Sie alle Teilnehmer in Ihrem Cluster ab.
3. Nachdem alle Knoten das IPSEC-Zertifikat neu generiert haben, starten Sie die Dienste neu.

Navigieren Sie zum Publisher **Cisco Unified Serviceability**. **Cisco Unified Serviceability > Tools > Control Center - Network Services**.Wählen Sie **Neustart** am **Cisco DRF Master**Services.Wenn der Neustart des Diensts abgeschlossen ist, wählen Sie **Restart** im **Cisco DRF Local Service** auf dem Publisher aus, und fahren Sie dann mit den Abonnenten fort. Wählen Sie **Restart** im **Cisco DRF Local Service aus**.

Das IPSEC.pem-Zertifikat im Publisher muss gültig sein und in allen Subscribern als IPSEC-Truststores vorhanden sein. Das IPSEC.pem-Abonnementzertifikat ist im Herausgeber nicht als IPSEC-Vertrauensspeicher in einer Standardbereitstellung vorhanden. Um die Gültigkeit zu überprüfen, vergleichen Sie die Seriennummern im IPSEC.pem-Zertifikat aus dem PUB mit dem IPSEC-trust in den SUBs. Sie müssen übereinstimmen.

CAPF-Zertifikat

Warnung: Vergewissern Sie sich, dass der Cluster im gemischten Modus ist, bevor Sie fortfahren. Siehe Abschnitt **Identifizieren, ob sich Ihr Cluster im gemischten oder ungesicherten Modus befindet**.

1. Navigieren Sie zu **Cisco Unified CM Administration > System > Enterprise Parameters**. Überprüfen Sie den Abschnitt Sicherheitsparameter, und stellen Sie sicher, dass der Clustersicherheitsmodus auf 0 oder 1 festgelegt ist. Wenn Sie den Wert 0 angeben, befindet sich der Cluster im ungesicherten Modus. Wenn der Wert 1 ist, befindet sich der Cluster im gemischten Modus, und Sie müssen die CTL-Datei vor dem Neustart der Dienste aktualisieren. Siehe Token- und Tokenless-Links.
2. Navigieren Sie zu jedem Server in Ihrem Cluster (in separaten Registerkarten Ihres Webbrowsers) mit dem Herausgeber beginnen, dann jeden Abonnenten. Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find**. Wählen Sie das **CAPF-PEM-**Zertifikat aus.Wählen Sie nach dem Öffnen **Regenerieren** und warten Sie, bis das Popup-Fenster Erfolg angezeigt wird. Schließen Sie das Popup-Fenster, oder gehen Sie zurück, und wählen Sie **Suchen/Liste aus.**
3. Mit nachfolgenden Abonnenten fortfahren; Befolgen Sie das gleiche Verfahren in Schritt 2, und schließen Sie alle Teilnehmer in Ihrem Cluster ab. Wenn sich der Cluster NUR im gemischten Modus befindet und die CAPF neu generiert wurde - Aktualisieren Sie die CTL, bevor Sie mit dem weiteren Token fortfahren - Tokenlos.Wenn sich der Cluster im gemischten Modus befindet, muss der Call Manager-Dienst vor dem Neustart anderer Dienste ebenfalls neu gestartet werden.
4. Nachdem alle Knoten das CAPF-Zertifikat neu generiert haben, starten Sie die Dienste neu. Rufen Sie den Herausgeber **Cisco Unified Serviceability auf**. **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.Beginnen Sie mit dem Herausgeber, und wählen Sie im **Cisco Certificate Authority Proxy Function Service** only **Restart** (**Neustarten**) aus, sofern aktiv.
5. Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Beginnen Sie mit dem Herausgeber und dann mit den Abonnenten, und wählen Sie **Restart** on **Cisco Trust Verification Service (Auf Cisco Trust überprüfen)**. Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.Beginnen Sie mit dem Herausgeber, und setzen Sie dann den Vorgang mit den Abonnenten fort. Starten Sie den **Cisco TFTP-Dienst** nur dort neu, wo er aktiv ist.
6. Alle Telefone neu starten: **Cisco Unified CM Administration > System > Enterprise-Parameter**Wählen Sie **Reset** (Zurücksetzen), und es erscheint ein Popup mit der Anweisung

Sie sind im Begriff, alle Geräte im System zurückzusetzen. Diese Aktion kann nicht rückgängig gemacht werden. Fortfahren?,wählen Sie **OK** und dann **Zurücksetzen**.

Die Telefone wurden zurückgesetzt. Überwachen Sie deren Aktionen mithilfe des RTMT-Tools, um sicherzustellen, dass das Zurücksetzen erfolgreich war und die Geräte sich wieder beim CUCM registrieren. Warten Sie, bis die Telefonregistrierung abgeschlossen ist, bevor Sie mit dem nächsten Zertifikat fortfahren. Dieser Vorgang der Telefonregistrierung kann einige Zeit in Anspruch nehmen. Beachten Sie, dass Geräte, die vor der Regenerierung fehlerhafte ITLs hatten, sich erst wieder beim Cluster registrieren, wenn dieser entfernt wurde.

CallManager-Zertifikat

Warnung: Vergewissern Sie sich, dass der Cluster im gemischten Modus ist, bevor Sie fortfahren. Siehe Abschnitt **Identifizieren, ob sich Ihr Cluster im gemischten oder ungesicherten Modus befindet**.

Warnung: Generieren Sie nicht gleichzeitig CallManager.PEM- und TVS.PEM-Zertifikate. Dies führt zu einer nicht wiederherstellbaren Diskrepanz mit der installierten ITL auf Endpunkten, die das Entfernen der ITL von ALLEN Endpunkten im Cluster erfordern. Beenden Sie den gesamten Prozess für CallManager.PEM, und starten Sie den Prozess für TVS.PEM, sobald die Telefone wieder registriert sind.

1. Navigieren Sie zu **Cisco Unified CM Administration > System > Enterprise Parameters**: Überprüfen Sie den Abschnitt Sicherheitsparameter, und stellen Sie sicher, dass der Clustersicherheitsmodus auf 0 oder 1 festgelegt ist. Wenn Sie den Wert 0 angeben, befindet sich der Cluster im ungesicherten Modus. Wenn der Wert 1 ist, befindet sich der Cluster im gemischten Modus, und Sie müssen die CTL-Datei vor dem Neustart der Dienste aktualisieren. Siehe Token- und Tokenless-Links.
2. Navigieren Sie zu jedem Server in Ihrem Cluster (in separaten Registerkarten Ihres Webbrowsers) mit dem Herausgeber beginnen, dann jeden Abonnenten. Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find**. Wählen Sie das CallManager-PEM-Zertifikat aus.Wählen Sie anschließend **Regenerieren** und warten Sie, bis das Popup-Fenster Erfolg angezeigt wird. Schließen Sie das Popup-Fenster, oder gehen Sie zurück, und wählen Sie **Suchen/Liste aus**.
3. Mit nachfolgenden Abonnenten fortfahren; Befolgen Sie das gleiche Verfahren in Schritt 2, und schließen Sie alle Teilnehmer in Ihrem Cluster ab. Wenn sich der Cluster NUR im gemischten Modus befindet und das CallManager-Zertifikat neu generiert wurde, aktualisieren Sie die CTL, bevor Sie mit dem weiteren Token fortfahren - Tokenlos
4. Anmeldung bei Publisher Cisco Unified Serviceability: Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.Beginnen Sie mit dem Herausgeber, und setzen Sie dann die Abonnenten fort, und starten Sie den **Cisco CallManager-Service** neu, sofern aktiv.
5. Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Feature Services** Beginnen Sie mit dem Publisher, und fahren Sie dann mit den Abonnenten fort. Starten Sie den **Cisco CTIManager-Dienst** nur dann neu, wenn er aktiv ist.
6. Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Beginnen Sie mit dem Publisher, und setzen Sie dann die Abonnenten fort, und starten Sie den **Cisco Trust Verification Service neu**.
7. Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.

Beginnen Sie mit dem Publisher, und fahren Sie dann mit den Abonnenten fort. Starten Sie den **Cisco TFTP-Service** nur dort neu, wo er aktiv ist.

8. Alle Telefone neu starten: **Cisco Unified CM Administration > System > Enterprise-Parameter**Wählen Sie **Reset** (Zurücksetzen), und es erscheint ein Popup mit der Anweisung **Sie sind im Begriff, alle Geräte im System zurückzusetzen. Diese Aktion kann nicht rückgängig gemacht werden. Fortfahren?,**wählen Sie **OK** und dann **Zurücksetzen**

Die Telefone wurden zurückgesetzt. Überwachen Sie deren Aktionen mithilfe des RTMT-Tools, um sicherzustellen, dass das Zurücksetzen erfolgreich war und die Geräte sich wieder beim CUCM registrieren. Warten Sie, bis die Telefonregistrierung abgeschlossen ist, bevor Sie mit dem nächsten Zertifikat fortfahren. Dieser Vorgang der Telefonregistrierung kann einige Zeit in Anspruch nehmen. Beachten Sie, dass Geräte, die vor der Regenerierung fehlerhafte ITLs hatten, sich erst wieder beim Cluster registrieren, wenn die ITL entfernt wurde.

TVS-Zertifikat

Warnung: Generieren Sie nicht gleichzeitig CallManager.PEM- und TVS.PEM-Zertifikate. Dies führt zu einer nicht wiederherstellbaren Diskrepanz mit der installierten ITL auf Endpunkten, die das Entfernen der ITL von ALLEN Endpunkten im Cluster erfordern.

Anmerkung: Der TVS authentifiziert Zertifikate für den Call Manager. Dieses Zertifikat zuletzt erneut generieren.

Navigieren Sie zu jedem Server in Ihrem Cluster (in separaten Registerkarten Ihres Webbrowsers) mit dem Herausgeber beginnen, dann jeden Abonnenten. Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find**:

- Wählen Sie das **TVS-PEM-**Zertifikat aus.
- Wählen Sie anschließend **Regenerieren** und warten Sie, bis das Popup-Fenster Erfolg angezeigt wird. Schließen Sie das Popup-Fenster, oder gehen Sie zurück, und wählen Sie **Suchen/Liste aus**.

1. Mit nachfolgenden Abonnenten fortfahren; Befolgen Sie das gleiche Verfahren in Schritt 1, und schließen Sie alle Teilnehmer in Ihrem Cluster ab. Nachdem alle Knoten das TVS-Zertifikat neu generiert haben, starten Sie die Dienste neu: Melden Sie sich bei Publisher **Cisco Unified Serviceability an**. Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Network Services**.Wählen Sie im Publisher die Option **Restart** on **Cisco Trust Verification Service (Bei Cisco Trust Verification-Service neu starten)**.Fahren Sie nach Abschluss des Servicestarts mit den Abonnenten fort, und starten Sie den **Cisco Trust Verification Service neu**.
2. Beginnen Sie mit dem Publisher, und fahren Sie dann mit den Abonnenten fort. Starten Sie den **Cisco TFTP-Service** nur dort neu, wo er aktiv ist.
3. Alle Telefone neu starten: **Cisco Unified CM Administration > System > Enterprise-Parameter**.Wählen Sie **Reset** (Zurücksetzen), und es erscheint ein Popup mit der Anweisung **Sie sind im Begriff, alle Geräte im System zurückzusetzen. Diese Aktion kann nicht rückgängig gemacht werden. Fortfahren?,**wählen Sie **OK** und dann **Zurücksetzen**.

Die Telefone wurden zurückgesetzt. Überwachen Sie deren Aktionen mithilfe des RTMT-Tools, um sicherzustellen, dass das Zurücksetzen erfolgreich war und die Geräte sich wieder beim CUCM registrieren. Warten Sie, bis die Telefonregistrierung abgeschlossen ist, bevor Sie mit dem

nächsten Zertifikat fortfahren. Dieser Vorgang der Telefonregistrierung kann einige Zeit in Anspruch nehmen. Beachten Sie, dass Geräte, die vor der Regenerierung fehlerhafte ITLs hatten, sich erst wieder beim Cluster registrieren, wenn die ITL entfernt wurde.

ITLRecovery-Zertifikat

Anmerkung: Das ITLRecovery-Zertifikat wird verwendet, wenn Geräte ihren vertrauenswürdigen Status verlieren. Das Zertifikat wird sowohl im ITL als auch im CTL angezeigt (wenn der CTL-Anbieter aktiv ist).
Wenn Geräte ihren Vertrauensstatus verlieren, können Sie den Befehl utils **itl reset localkey** für nicht sichere Cluster und den Befehl utils **ctl reset localkey** für Mix-Mode-Cluster verwenden. Lesen Sie den Sicherheitsleitfaden für Ihre Call Manager-Version, um sich mit der Verwendung des ITLRecovery-Zertifikats und dem Prozess vertraut zu machen, der zur Wiederherstellung des vertrauenswürdigen Status erforderlich ist.
Wenn der Cluster auf eine Version aktualisiert wurde, die eine Schlüssellänge von 2048 unterstützt, und die Cluster-Serverzertifikate auf 2048 regeneriert wurden und die ITLRecovery nicht regeneriert wurde und aktuell 1024 Schlüssellänge aufweist, schlägt der ITL-Wiederherstellungsbefehl fehl, und die ITLRecovery-Methode wird nicht verwendet.

1. Navigieren Sie zu jedem Server in Ihrem Cluster (in separaten Registerkarten Ihres Webbrowsers) mit dem Herausgeber beginnen, dann jeden Abonnenten. Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find**:
Wählen Sie das **ITLRecovery-**Zertifikat aus.Wählen Sie anschließend **Regenerieren** und warten Sie, bis das Popup-Fenster Erfolg angezeigt wird. Schließen Sie das Popup-Fenster, oder gehen Sie zurück, und wählen Sie **Suchen/Liste aus**.
2. Mit nachfolgenden Abonnenten fortfahren; Befolgen Sie das gleiche Verfahren in Schritt 2, und schließen Sie alle Teilnehmer in Ihrem Cluster ab.
3. Nachdem alle Knoten das ITLRecovery-Zertifikat neu generiert haben, müssen die Dienste in der folgenden Reihenfolge neu gestartet werden: Wenn Sie sich im gemischten Modus befinden, aktualisieren Sie die CTL, bevor Sie mit dem Token fortfahren - Tokenlos.Melden Sie sich bei Publisher **Cisco Unified Serviceability an**. Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Network Services**.Wählen Sie im Publisher die Option **Restart** on **Cisco Trust Verification Service (Bei Cisco Trust Verification-Service neu starten)**. Fahren Sie nach Abschluss des Servicestarts mit den Abonnenten fort, und starten Sie den **Cisco Trust Verification Service neu**.
4. Beginnen Sie mit dem Publisher, und fahren Sie dann mit den Abonnenten fort. Starten Sie den **Cisco TFTP-Service** nur dort neu, wo er aktiv ist.
5. Alle Telefone neu starten: **Cisco Unified CM Administration > System > Enterprise-Parameter**Wählen Sie **Reset** (Zurücksetzen), und es erscheint ein Popup mit der Anweisung **Sie sind im Begriff, alle Geräte im System zurückzusetzen. Diese Aktion kann nicht rückgängig gemacht werden. Fortfahren?,**wählen Sie **OK** und dann **Zurücksetzen**.
6. Telefone laden jetzt die neue ITL/CTL hoch, während sie zurückgesetzt werden.

Abgelaufene Vertrauenszertifikate löschen

Anmerkung: Geben Sie die Vertrauenszertifikate an, die gelöscht werden müssen, nicht mehr benötigt werden oder abgelaufen sind. Löschen Sie nicht die fünf Basiszertifikate, die CallManager.pem, tomcat.pem, ipsec.pem, CAPF.pem und TVS.pem enthalten.

Vertrauenswürdige Zertifikate können bei Bedarf gelöscht werden. Der nächste Dienst, der neu startet, dient zum Löschen von Informationen über Legacy-Zertifikate innerhalb dieser Dienste.

1. Navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Wählen Sie aus dem Dropdown-Menü den CUCM Publisher aus.Wählen Sie **Stopp Certificate Change Notification aus**.Wiederholen Sie den Vorgang für jeden Call Manager-Knoten in Ihrem Cluster.Wenn Sie über einen IMP-Server verfügen: Wählen Sie im Dropdown-Menü nacheinander Ihre IMP-Server aus, und wählen Sie **Stopp Platform Administration Web Services und Cisco Intercluster Sync Agent aus**.
2. Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Suche nach abgelaufenen Vertrauenszertifikaten (Bei Versionen 10.X und höher können Sie nach Ablauf filtern. Bei Versionen unter 10.0 müssen Sie die jeweiligen Zertifikate manuell oder über die RTMT-Warnmeldungen identifizieren, wenn diese eingehen.)Das gleiche Vertrauenszertifikat kann in mehreren Knoten vorhanden sein. Sie muss einzeln von jedem Knoten gelöscht werden.Wählen Sie das zu löschende Vertrauenszertifikat aus (je nach Version wird entweder ein Popup-Fenster angezeigt, oder Sie navigieren zum Zertifikat auf derselben Seite). Wählen Sie **Löschen aus**. (Sie erhalten ein Popup, das mit "Sie sind im Begriff, dieses Zertifikat endgültig zu löschen" beginnt.*)*Wählen Sie **OK**.
3. Wiederholen Sie den Vorgang für jedes zu löschende Vertrauenszertifikat.
4. Nach Fertigstellung müssen Dienste neu gestartet werden, die sich direkt auf die gelöschten Zertifikate beziehen. In diesem Abschnitt müssen Sie Telefone nicht neu starten. Call Manager und CAPF wirken sich auf Endgeräte aus. Tomcat-Trust: Tomcat Service über die Befehlszeile neu starten (siehe Tomcat-Abschnitt)CAPF-Trust: Neustarten der Cisco Certificate Authority Proxy-Funktion (siehe Abschnitt "CAPF") Starten Sie die Endgeräte nicht neu.CallManager-Vertrauenswürdigkeit: CallManager Service/CTIManager (Siehe CallManager-Abschnitt) Starten Sie Endpunkte nicht neu. Auswirkungen auf Endpunkte und NeustartsIPSEC-Trust: DRF Master/DRF Lokal (siehe Abschnitt IPSEC).Der TVS (selbstsigniert) verfügt nicht über Vertrauenszertifikate.
5. Dienste neu starten, die zuvor in Schritt 1 angehalten wurden.

Verifizierung

Für diese Konfiguration sind keine Prüfverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind keine Verfahren 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.