CUCM용 인증서 재생성

목차

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager) 릴리스 8.X 이상에서 인증서를 재생성하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- *RTMT(실시간 모니터링 도구*)
- CUCM 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM 릴리스 8.X 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 CUCM(Cisco Unified Communications Manager) 릴리스 8.X 이상에서 인증서를 재생성하는 방법에 대한 단계별 절차를 설명합니다. 그러나 이는 ITL 복구에 대한 12.0 이후의 변경 사항을 반영하지 않습니다.

RTMT 설치

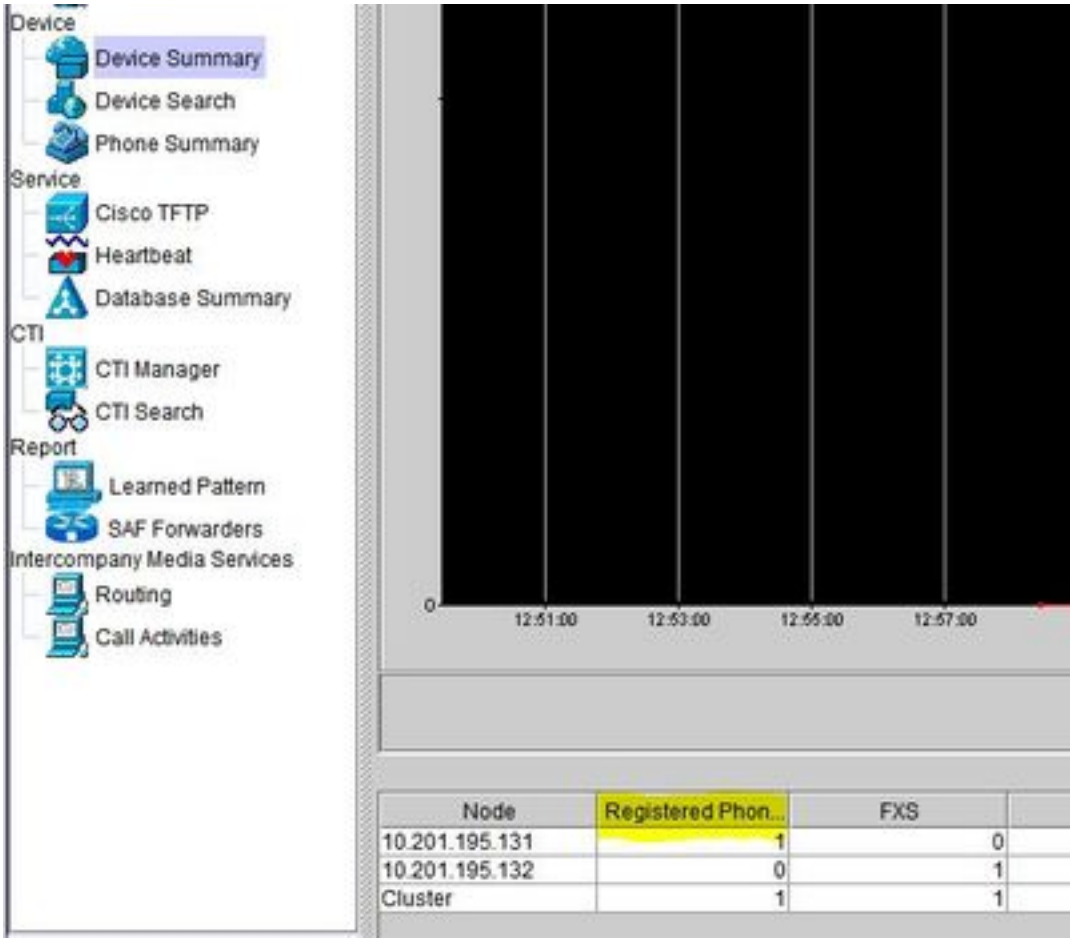
- Call Manager에서 RTMT Tool을 다운로드하여 설치합니다. Call Manager (CM) Administration(CM 관리)으로 이동합니다. **애플리케이션 > 플러그인 > 찾기 > Cisco Unified Real-Time Monitoring Tool - Windows > 다운로드** 설치 및 실행

RTMT로 엔드포인트 모니터링

- RTMT를 시작하고 IP 주소 또는 FQDN(Fully Qualified Domain Name)을 입력한 다음 사용자 이름과 비밀번호를 입력하여 툴에 액세스합니다.
- **Voice/Video 탭**을 **선택합니다**.Device **Summary를 선택합니다**. 이 섹션에서는 등록된 엔드포인트의 총수와 각 노드에 대한 개수를 파악합니다엔드포인트가 재설정되는 동안 모니터링하여 다음 인증서 재생성 전에 등록 보장

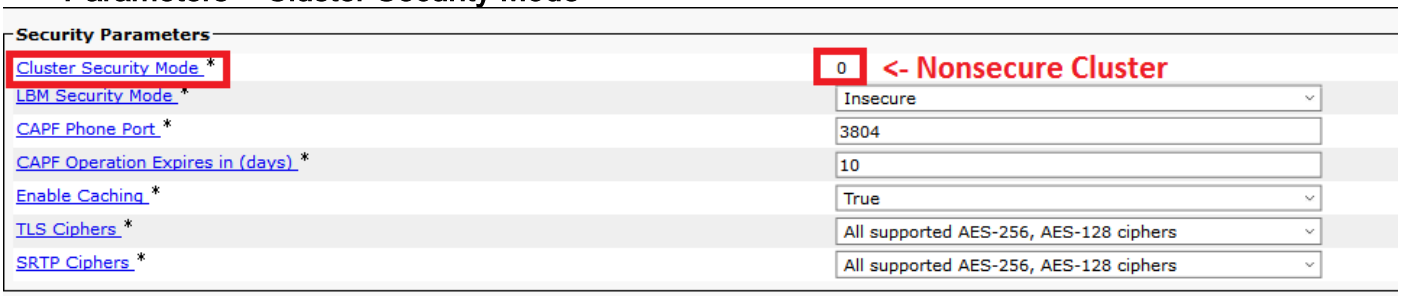
  팁: 일부 인증서의 재생성 프로세스는 엔드포인트에 영향을 줄 수 있습니다. 서비스를 다시 시작하고 전화기를 재부팅해야 하므로 정규 업무 시간 후에 실행 계획을 고려하십시오. RTMT를 통해 전화 등록을 확인하는 것이 좋습니다.

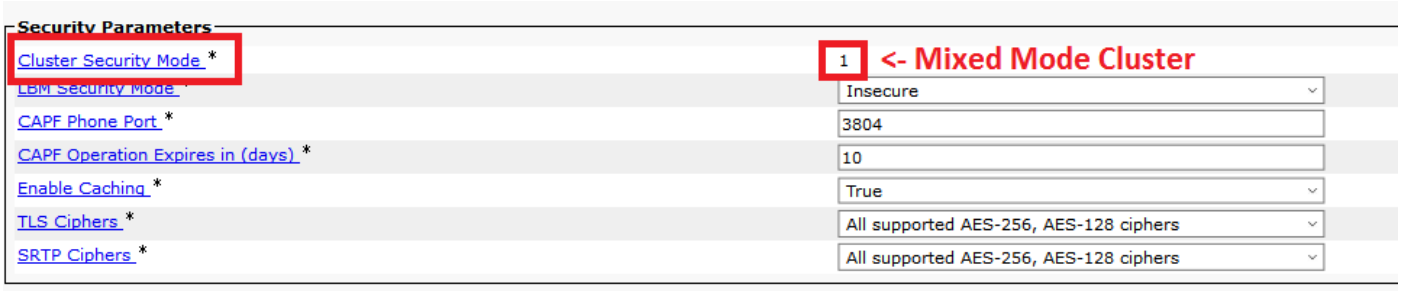
  경고: 현재 ITL 불일치가 있는 엔드포인트는 이 프로세스 이후에 등록 문제가 발생할 수 있습니다. 엔드포인트에서 ITL을 삭제하는 것은 재생성 프로세스가 완료되고 다른 모든 폰이 등록된 후의 일반적인 모범 사례 솔루션입니다.



클러스터가 혼합 모드 또는 비보안 모드인지 확인

- CM Administration(CM 관리)으로 이동합니다. **System > Enterprise Parameters > Security Parameters > Cluster Security Mode**





인증서 저장소에 의한 영향

성공적인 시스템 기능을 위해서는 CUCM 클러스터 전체에서 모든 인증서가 업데이트되어야 합니다. 인증서가 만료되거나 유효하지 않은 경우 시스템의 정상적인 기능에 심각한 영향을 미칠 수 있습니다. 영향은 시스템 설정에 따라 다를 수 있습니다. 유효하지 않거나 만료된 특정 인증서에 대한

서비스 목록이 여기에 표시됩니다.

CallManager.pem

- 암호화/인증된 전화기가 등록되지 않음
- TFTP(Trivial File Transfer Protocol)를 신뢰할 수 없습니다(전화기에서 서명된 컨피그레이션 파일 및/또는 ITL 파일을 허용하지 않음).
- 전화 서비스가 영향을 받을 수 있음
- SIP(Secure Session Initiation Protocol) 트렁크 또는 미디어 리소스(컨퍼런스 브리지, MTP(Media Termination Point), Xcoders 등)가 등록되지 않거나 작동하지 않습니다.
- AXL 요청이 실패합니다.

Tomcat.pem

- 전화기는 CUCM 노드에서 호스팅되는 HTTPs 서비스(예: Corporate Directory)에 액세스할 수 없습니다
- CUCM에는 클러스터의 다른 노드에서 서비스 페이지에 액세스할 수 없는 것과 같은 다양한 웹 문제가 있을 수 있습니다
- EM(Extension Mobility) 또는 클러스터 간 익스텐션 모빌리티 문제
- 단일 로그인(SSO)
- UCCX(Unified Contact Center Express)가 통합된 경우 CCX 12.5의 보안 변경 때문에 UCCX tomcat 트러스트 스토어에 CUCM Tomcat 인증서(자체 서명) 또는 Tomcat 루트 및 중간 인증서(CA 서명)를 업로드해야 합니다. Finesse 데스크톱 로그인이 영향을 받기 때문입니다.

CAPF.PEM

- 전화기는 Phone VPN, 802.1x 또는 Phone Proxy에 대해 인증되지 않습니다
- 전화기에 대해 LSC(Locally Significant Certificate) 인증서를 발급할 수 없습니다.
- 암호화된 구성 파일이 작동하지 않음

IPSec.pem

- DRS(Disaster Recovery System)/DRF(Disaster Recovery Framework)가 제대로 작동하지 않음
- 게이트웨이(GW)에 대한 IPsec 터널과 다른 CUCM 클러스터가 작동하지 않음

TVS(Trust Verification Service)

TVS(Trust Verification Service)는 기본적으로 보안의 주요 구성 요소입니다. TVS를 사용하면 HTTPS가 설정된 경우 Cisco Unified IP Phone에서 EM 서비스, 디렉토리 및 MIDlet과 같은 애플리케이션 서버를 인증할 수 있습니다.

TVS는 다음과 같은 기능을 제공합니다.

- 확장성 - Cisco Unified IP Phone 리소스는 신뢰할 수 있는 인증서의 수에 영향을 받지 않습니다.
- 유연성 - 트러스트 인증서 추가 또는 제거가 시스템에 자동으로 반영됩니다.

- 기본적으로 보안 - 비 미디어 및 신호 보안 기능은 기본 설치에 포함되며 사용자의 개입이 필요하지 않습니다.

ITL 및 CTL

- ITL에는 Call Manager TFTP, 클러스터의 모든 TVS 인증서 및 실행 시 CAPF(Certificate Authority Proxy Function)에 대한 인증서 역할이 포함됩니다.
- CTL에는 동일한 서버, CAPF, TFTP 서버 및 ASA(Adaptive Security Appliance) 방화벽에서 실행되는 SAST(System Administrator Security Token), Cisco CallManager 및 Cisco TFTP 서비스에 대한 항목이 포함되어 있습니다. TVS는 CTL에서 참조되지 않습니다.

인증서 재생성 프로세스

> **참고:** 모든 엔드포인트의 전원을 켜고 인증서를 다시 생성하기 전에 등록해야 합니다. 그렇지 않으면 연결되지 않은 전화기에서 ITL을 제거해야 합니다.

Tomcat 인증서

서드파티 인증서가 사용 중인지 확인:

1. 클러스터의 각 서버(웹 브라우저의 별도 탭)로 이동하여 게시자를 시작으로 각 가입자를 찾습니다. **Cisco** Unified **OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Find(찾기)로 이동합니다**.
   Tomcat이 시스템에서 생성한 자체 서명 인증서임을 나타내는 경우 Description 열에서 확인합니다. Tomcat이 서드파티 서명한 경우 제공된 링크를 따라 Tomcat 재생성 후 해당 단계를 수행합니다.서드파티 서명 인증서는 CUCM Uploading CCMAdmin Web GUI Certificates를 참조하십시오.
2. 모든 **인증서**를 표시하려면 Find를 선택합니다. Tomcat pem **Certificate를** 선택합니다.연 다음 Regenerate(**재생성**)를 선택하고 Success(성공) 팝업이 표시될 때까지 기다린 다음 팝업을 닫거나 뒤로 이동하여 **Find/List(찾기/목록)를 선택합니다**.
3. 각 후속 가입자로 계속 진행하여 2단계에서 동일한 절차를 수행하고 클러스터의 모든 가입자에 대해 완료합니다.
4. 모든 노드에서 Tomcat 인증서를 다시 생성한 후 모든 노드에서 tomcat 서비스를 재시작합니다. 게시자로 시작한 다음 구독자를 추가합니다. Tomcat을 재시작하려면 각 노드에 대한 CLI 세션을 열고 utils service restart **Cisco** Tomcat 명령을 **실행해야 합니다**.

```
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:
```

5. CCX 환경에서 다음 단계가 필요합니다(해당하는 경우).

- 자체 서명 인증서를 사용하는 경우 CUCM 클러스터의 모든 노드에서 Tomcat 인증서를 Unified CCX Tomcat 트러스트 저장소에 업로드합니다.
- CA 서명 또는 개인 CA 서명 인증서를 사용하는 경우 CUCM의 루트 CA 인증서를 Unified CCX

Tomcat 트러스트 저장소에 업로드합니다.
- CCX용 인증서 재생성 문서에 설명된 대로 서버를 재시작합니다.

추가 참조:

- UCCX 솔루션 인증서 관리 가이드
- Unified CCX 상태 확인 유틸리티

IPSEC 인증서

참고: CUCM/IM&P(Instant Messaging and Presence) 이전 버전10.X DRF Master 에이전트는 CUCM 게시자 및 IM&P 게시자에서 모두 실행됩니다. DRF 로컬 서비스는 가입자에서 각각 실행됩니다. 버전 10.X 이상, DRF Master 에이전트는 CUCM 게시자에서만 실행되고 DRF 로컬 서비스는 CUCM 구독자 및 IM&P 게시자와 구독자에서 실행됩니다.

참고: 재해 복구 시스템은 SSL(Secure Socket Layer) 기반 통신을 사용하여 Master CUCM 클러스터 노드 간의 데이터 인증 및 암호화를 위한 에이전트 및 로컬 에이전트 DRS는 공용/개인 키 암호화에 IPSec 인증서를 사용합니다. Certificate Management 페이지에서 IPSEC truststore (hostname.pem) 파일을 삭제하면 DRS가 예상대로 작동하지 않습니다. IPSEC-trust 파일을 수동으로 삭제하는 경우 IPSEC 인증서를 IPSEC 신뢰 저장소에 업로드해야 합니다. 자세한 내용은 Cisco Unified Communications Manager 보안 가이드의 인증서 관리 도움말 페이지를 참조하십시오.

1. 클러스터의 각 서버(웹 브라우저의 별도 탭)로 이동하여 게시자를 시작으로 각 가입자를 찾습니다. **Cisco** Unified **OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Find**:
   IPSEC pem **Certificate를** 선택합니다.연 다음 Regenerate(**재생성**)를 선택하고 Success(성공) 팝업이 표시될 때까지 기다린 다음 팝업을 닫거나 뒤로 이동하여 **Find/List(찾기/목록)를 선택합니다**.
2. 후속 가입자로 계속 진행; 1단계에서 동일한 절차를 수행하고 클러스터의 모든 가입자에 대해 완료합니다.
3. 모든 노드가 IPSEC 인증서를 다시 생성한 후 서비스를 다시 시작합니다.
   게시자 **Cisco** Unified Serviceability로 **이동합니다**. **Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스)**.재시작 **위치** 선택 **Cisco DRF Master**서비스.서비스 재시작이 완료되면 게시자의 **Cisco DRF Local Service**에서 **Restart(재시작)**를 선택한 다음 가입자로 계속 진행하고 **Cisco DRF Local Service**에서 **Restart(재시작)를** 선택합니다.

게시자의 IPSEC.pem 인증서가 유효해야 하며 모든 가입자에 IPSEC 신뢰 저장소로 존재해야 합니다. 구독자 IPSEC.pem 인증서가 표준 배포에서 IPSEC 신뢰 저장소로 게시자에 존재하지 않습니다. 유효성을 확인하기 위해 PUB의 IPSEC.pem 인증서에 있는 일련 번호와 SUB의 IPSEC-trust를 비교합니다. 꼭 일치해야 합니다.

CAPF 인증서

경고: 계속하기 전에 클러스터가 혼합 모드인지 확인하십시오. 클러스터가 **혼합 모드 또는 비보안 모드에 있는지 확인 섹션을 참조하십시오**.

1. **Cisco** Unified **CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise**

Parameters(엔터프라이즈 매개변수)로 이동합니다.
[보안 매개변수] 섹션을 확인하고 클러스터 보안 모드가 0 또는 1로 설정되었는지 확인합니다. 값이 0이면 클러스터는 비보안 모드에 있습니다. 1이면 클러스터가 혼합 모드이며 서비스를 다시 시작하기 전에 CTL 파일을 업데이트해야 합니다. 토큰 및 토큰리스 링크를 참조하십시오
.

2. 웹 브라우저의 개별 탭에서 클러스터의 각 서버로 이동한 다음 게시자로 시작하고 각 가입자로 이동합니다. **Cisco** Unified **OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Find(찾기)로 이동합니다**.
CAPF pem **Certificate(CAPF PEM 인증서)를** 선택합니다.연 다음 Regenerate(**재생성**)를 선택하고 Success(성공) 팝업이 표시될 때까지 기다린 다음 팝업을 닫거나 뒤로 이동하여 **Find/List(찾기/목록)를 선택합니다**
3. 후속 구독자를 계속 진행합니다. 2단계에서 동일한 절차를 수행하고 클러스터의 모든 가입자에 대해 완료합니다. 클러스터가 혼합 모드에만 있고 CAPF가 재생성된 경우 - 추가 토큰 - 토큰리스를 진행하기 전에 CTL을 업데이트합니다.클러스터가 혼합 모드인 경우 다른 서비스를 다시 시작하기 전에 Call Manager 서비스를 다시 시작해야 합니다.
4. 모든 노드에서 CAPF 인증서를 다시 생성한 후 서비스를 다시 시작합니다.
게시자 **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성)로 이동합니다**. **Cisco Unified Serviceability(Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)**.게시자로 시작하고 활성화된 **Cisco Certificate Authority Proxy Function Service**에서만 **Restart(재시작)**를 선택합니다.
5. **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스)로 이동합니다**. 게시자로 시작한 다음 구독자로 계속 진행합니다. Restart on **Cisco Trust Verification Service(Cisco Trust Verification 서비스**에서 **다시 시작)를** 선택합니다. **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동합니다**.게시자로 시작한 다음 가입자를 계속 사용하여 **Cisco** TFTP **서비스를** 활성 상태에서만 재시작합니다
.
6. 모든 전화 재부팅: **Cisco Unified CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수)**Reset(**재설정**)을 선택하면 **You are about to reset all devices in the system(시스템의 모든 디바이스를 재설정하려고 합니다) 문구가** 포함된 팝업이 표시됩니다**. 이 작업은 실행 취소할 수 없습니다. 계속하시겠습니까? OK(확인)**를 선택한 다음 Reset(재설정)**을 선택합니다**.

이제 전화기가 재설정됩니다. RTMT 툴을 통해 이들의 작업을 모니터링하여 재설정이 성공했는지 그리고 디바이스가 CUCM에 다시 등록되었는지 확인합니다. 다음 인증서로 진행하기 전에 전화 등록이 완료될 때까지 기다립니다. 이러한 전화 등록 프로세스는 시간이 걸릴 수 있습니다. 재생성 프로세스 전에 ITL이 잘못된 디바이스는 제거할 때까지 클러스터에 다시 등록되지 않습니다.

CallManager 인증서

경고: 계속하기 전에 클러스터가 혼합 모드인지 확인하십시오. 클러스터가 **혼합 모드 또는 비보안 모드에 있는지 확인 섹션을 참조하십시오**.

경고: CallManager.PEM 및 TVS.PEM 인증서를 동시에 다시 생성하지 마십시오. 이로 인해 클러스터의 모든 엔드포인트에서 ITL을 제거해야 하는 엔드포인트에 설치된 ITL과 복구할 수 없는 불일치가 발생합니다. CallManager.PEM에 대한 전체 프로세스를 마치고 전화기가 다시 등록되면 TVS.PEM에 대한 프로세스를 시작합니다.

1. **Cisco** Unified **CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수)로 이동합니다**. [보안 매개변수] 섹션을 확인하고 클러스터 보안 모드가 0 또는 1로 설정되었는지 확인합니다. 값이 0이면 클러스터는 비보안 모드에 있습니다. 1이면 클러스터가 혼합 모드이며 서비스를 다시 시작하기 전에 CTL 파일을 업데이트해야 합니다. 토큰 및 토큰리스 링크를 참조하십시오.
2. 웹 브라우저의 개별 탭에서 클러스터의 각 서버로 이동한 다음 게시자로 시작하고 각 가입자로 이동합니다. **Cisco** Unified **OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Find(찾기)로 이동합니다**.
CallManager pem 인증서를 선택합니다.연 다음 Regenerate(**재생성**)를 선택하고 Success(성공) 팝업이 표시될 때까지 기다린 다음 팝업을 닫거나 뒤로 이동하여 **Find/List(찾기/목록)를 선택합니다**.
3. 후속 구독자를 계속 진행합니다. 2단계에서 동일한 절차를 수행하고 클러스터의 모든 가입자에 대해 완료합니다. 클러스터가 혼합 모드에만 있고 CallManager 인증서가 재생성된 경우 - 추가 토큰 - 토큰리스 진행하기 전에 CTL을 업데이트합니다.
4. Publisher Cisco Unified Serviceability에 로그인합니다. **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동합니다**.게시자로 시작한 다음 가입자를 계속 사용하여 **Cisco** CallManager 서비스를 **활성 상태**로 다시 시작합니다.
5. **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동합니다.**
Publisher로 시작한 다음 가입자를 계속 진행합니다. **활성** 상태의 **경우에만 Cisco CTIManager** 서비스를 재시작합니다.
6. **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스)로 이동합니다**.
게시자로 시작한 다음 가입자를 계속 진행하고 **Cisco Trust Verification Service를 다시 시작합니다**.
7. **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동합니다**.
Publisher로 시작한 다음 가입자를 계속 사용하여 **Cisco** TFTP **Service를** 활성 상태에서만 재시작합니다.
8. 모든 전화 재부팅: **Cisco Unified CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수)**Reset(**재설정**)을 선택하면 **You are about to reset all devices in the system(시스템의 모든 디바이스를 재설정하려고 합니다) 문구가** 포함된 팝업이 표시됩니다**. 이 작업은 실행 취소할 수 없습니다. 계속하시겠습니까? OK(확인)**를 선택한 다음 Reset(재설정)을 **선택합니다**

이제 전화기가 재설정됩니다. RTMT 툴을 통해 이들의 작업을 모니터링하여 재설정이 성공했는지 그리고 디바이스가 CUCM에 다시 등록되었는지 확인합니다. 다음 인증서로 진행하기 전에 전화 등록이 완료될 때까지 기다립니다. 이러한 전화 등록 프로세스는 시간이 걸릴 수 있습니다. 재생성 프로세스 전에 잘못된 ITL이 있었던 디바이스는 ITL을 제거할 때까지 클러스터에 다시 등록되지 않습니다.

TVS 인증서

경고: CallManager.PEM 및 TVS.PEM 인증서를 동시에 다시 생성하지 마십시오. 이로 인해 클러스터의 모든 엔드포인트에서 ITL을 제거해야 하는 엔드포인트에 설치된 ITL과 복구할 수 없는 불일치가 발생합니다.

참고: TVS는 Call Manager를 대신하여 인증서를 인증합니다. 이 인증서를 마지막으로 다시 생성합니다.

웹 브라우저의 개별 탭에서 클러스터의 각 서버로 이동한 다음 게시자로 시작하고 각 가입자로 이동합니다. **Cisco** Unified **OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Find(찾기)**:

- TVS pem **Certificate(TVS pem** 인증서)를 선택합니다.
- 연 다음 Regenerate(**재생성**)를 선택하고 Success(성공) 팝업이 표시될 때까지 기다린 다음 팝업을 닫거나 뒤로 이동하여 **Find/List(찾기/목록)를 선택합니다**.

1. 후속 구독자를 계속 진행합니다. 1단계에서 동일한 절차를 수행하고 클러스터의 모든 가입자에 대해 완료합니다. 모든 노드에서 TVS 인증서를 다시 생성한 후 서비스를 다시 시작합니다. Publisher **Cisco** Unified Serviceability에 **로그인합니다**. **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스)로 이동합니다**.게시자에서 **Cisco Trust Verification Service**에서 **재시작을 선택합니다** .서비스 재시작이 완료되면 가입자를 계속 진행하고 **Cisco Trust Verification Service를 재시작합니다**.
2. Publisher로 시작한 다음 가입자를 계속 사용하여 **Cisco TFTP Service를** 활성 상태에서만 재시작합니다.
3. 모든 전화 재부팅: **Cisco Unified CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수)**.Reset(**재설정**)을 선택하면 **You are about to reset all devices in the system(시스템의 모든 디바이스를 재설정하려고 합니다) 문구가** 포함된 팝업이 표시됩니다**. 이 작업은 실행 취소할 수 없습니다. 계속하시겠습니까? OK(확인)**를 선택한 다음 Reset(재설정)**을 선택합니다**.

이제 전화기가 재설정됩니다. RTMT 툴을 통해 이들의 작업을 모니터링하여 재설정이 성공했는지 그리고 디바이스가 CUCM에 다시 등록되었는지 확인합니다. 다음 인증서로 진행하기 전에 전화 등록이 완료될 때까지 기다립니다. 이러한 전화 등록 프로세스는 시간이 걸릴 수 있습니다. 재생성 프로세스 전에 잘못된 ITL이 있었던 디바이스는 ITL을 제거할 때까지 클러스터에 다시 등록되지 않습니다.

ITLRecovery 인증서

참고: ITLRecovery 인증서는 디바이스가 신뢰할 수 있는 상태를 잃을 때 사용됩니다. 인증서는 ITL과 CTL 모두에 나타납니다(CTL 제공자가 활성화된 경우).
디바이스의 트러스트 상태가 손실되면 비보안 클러스터의 경우 명령 **utils itl reset localkey**를 사용하고 혼합 모드 클러스터의 경우 명령 **utils ctl reset localkey**를 사용할 수 있습니다.
ITLRecovery 인증서가 사용되는 방법 및 신뢰할 수 있는 상태를 복구하는 데 필요한 프로세스에 대해 자세히 알아보려면 Call Manager 버전의 보안 가이드를 읽어 보십시오.
클러스터가 키 길이 2048을 지원하는 버전으로 업그레이드되고 클러스터 서버 인증서가 2048로 재생성되었으며 ITLRecovery가 재생성되지 않고 현재 키 길이가 1024인 경우 ITL recovery 명령이 실패하고 ITLRecovery 방법이 사용되지 않습니다.

1. 웹 브라우저의 개별 탭에서 클러스터의 각 서버로 이동한 다음 게시자로 시작하고 각 가입자로 이동합니다. **Cisco** Unified **OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Find**:
   ITLRecovery pem **Certificate를** 선택합니다.연 다음 Regenerate(**재생성**)를 선택하고 Success(성공) 팝업이 표시될 때까지 기다린 다음 팝업을 닫거나 뒤로 이동하여 **Find/List(찾기/목록)를 선택합니다**.

2. 후속 가입자로 계속 진행; 2단계에서 동일한 절차를 수행하고 클러스터의 모든 가입자에 대해 완료합니다.
3. 모든 노드가 ITLRecovery 인증서를 다시 생성한 후에는 다음과 같은 순서로 서비스를 다시 시작해야 합니다. 혼합 모드에 있는 경우 - Token(토큰) - Tokenless(토큰 없음)로 진행하기 전에 CTL을 업데이트합니다.Publisher **Cisco** Unified Serviceability에 **로그인합니다**. **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스)로 이동합니다**.게시자에서 **Cisco Trust Verification Service**에서 **재시작을 선택합니다**. 서비스 재시작이 완료되면 가입자를 계속 진행하고 **Cisco Trust Verification Service를 재시작합니다**.
4. Publisher로 시작한 다음 가입자를 계속 사용하여 **Cisco TFTP Service를** 활성 상태에서만 재시작합니다.
5. 모든 전화 재부팅: **Cisco Unified CM Administration(Cisco Unified CM 관리) > System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수)**Reset(**재설정**)을 선택하면 **You are about to reset all devices in the system(시스템의 모든 디바이스를 재설정하려고 합니다) 문구가** 포함된 팝업이 표시됩니다**. 이 작업은 실행 취소할 수 없습니다. 계속하시겠습니까? OK(확인)**를 선택한 다음 Reset(재설정)**을 선택합니다**.
6. 전화기는 이제 재설정되는 동안 새 ITL/CTL을 업로드합니다.

만료된 트러스트 인증서 삭제

참고: 삭제해야 하거나 더 이상 필요하지 않거나 만료된 트러스트 인증서를 식별합니다. CallManager.pem, tomcat.pem, ipsec.pem, CAPF.pem 및 TVS.pem을 포함하는 5개의 기본 인증서를 삭제하지 마십시오. 적절한 경우 트러스트 인증서를 삭제할 수 있습니다. 다시 시작하는 다음 서비스는 해당 서비스 내에서 레거시 인증서의 정보를 지우도록 설계되었습니다.

1. **Cisco** Unified Serviceability(**Cisco Unified 서비스 가용성) > Tools(툴) > Control Center - Network Services(제어 센터 - 네트워크 서비스)로 이동합니다**. 드롭다운에서 CUCM Publisher를 선택합니다.Stop **Certificate Change Notification(인증서 변경 알림 중지)을 선택합니다**.클러스터의 모든 Call Manager 노드에 대해 반복합니다.IMP 서버가 있는 경우: 드롭다운 메뉴에서 IMP 서버를 한 번에 하나씩 선택하고 **플랫폼 관리 웹 서비스 및 Cisco Intercluster Sync Agent 중지를 선택합니다**.
2. **Cisco** Unified **OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Find(찾기)로 이동합니다**.
   만료된 신뢰 인증서를 찾습니다. 버전 10.X 이상에서는 만료로 필터링할 수 있습니다. 10.0 이하 버전의 경우 특정 인증서를 수동으로 식별하거나 수신한 경우 RTMT 알림을 통해 식별해야 합니다.)동일한 신뢰 인증서가 여러 노드에 나타날 수 있습니다. 각 노드에서 개별적으로 삭제해야 합니다.삭제할 트러스트 인증서를 선택합니다(팝업을 받거나 같은 페이지의 인증서로 이동한 버전에 따라 다름) 삭제를 **선택합니다**. (이 인증서를 영구적으로 삭제하려고 합니다"로 시작하는 팝업이 표시됩니다.)확인을 **선택합니다**.
3. 삭제할 모든 신뢰 인증서에 대해 이 과정을 반복합니다.
4. 완료되면 삭제된 인증서와 직접 관련된 서비스를 다시 시작해야 합니다. 이 섹션에서는 전화기를 재부팅할 필요가 없습니다. Call Manager 및 CAPF는 엔드포인트에 영향을 미칩니다. Tomcat-trust: 명령줄을 통해 Tomcat 서비스 재시작(Tomcat 섹션 참조)CAPF-Trust: cisco Certificate Authority Proxy 기능 다시 시작(CAPF 섹션 참조) 엔드포인트를 재부팅하지 마십시오.통화 관리자 신뢰: CallManager Service/CTIManager(CallManager 섹션 참조) 엔드포인트를 재부팅하지 마십시오. 엔드포인트에 영향을 미치고 다시 시작됩니다.IPSEC 트러스트: DRF Master/DRF Local(IPSEC 섹션 참조)TVS(자체 서명)에는 신뢰 인증서가 없습니다.

5. 1단계에서 이전에 중지한 서비스를 다시 시작합니다.

확인

이 구성에서는 확인 절차를 사용할 수 없습니다.

문제 해결

이 구성에서는 문제 해결 절차를 사용할 수 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.