CUCM IM/P 서비스 셀프 서명 인증서 다시 생성

목차

- 소개
- 사전 요구 사항
  - 요구 사항
  - 사용되는 구성 요소
- 배경 정보
  - 인증서 저장소 사용률
    - Cisco CUP(Unified Presence) 인증서
    - Cisco Unified Presence - CUP-XMPP(Extensible Messaging and Presence Protocol) 인증서
    - Cisco Unified Presence - Extensible Messaging and Presence Protocol - Server to Server(CUP-XMPP-S2S) 인증서
    - IP 보안(IPSec) 인증서
    - Tomcat 인증서
- 인증서 재생성 프로세스
  - CUP 인증서
  - CUP-XMPP 인증서
  - CUP-XMPP-S2S 인증서
  - IPSec 인증서
  - Tomcat 인증서
- 만료된 트러스트 인증서 삭제
- 다음을 확인합니다.
- 문제 해결

소개

이 문서에서는 CUCM IM/P 8.x 이상에서 인증서를 재생성하는 방법에 대한 권장 단계별 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

IM & Presence(IM/P) 서비스 인증서를 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 IM/P 릴리스 8.x 이상을 기반으로 합니다.

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

인증서 저장소 사용률

Cisco CUP(Unified Presence) 인증서

SIP 페더레이션을 위한 보안 SIP 연결, Lync/OCS/LCS를 위한 Microsoft Remote Call Control, CUCM(Cisco Unified Certificate Manager)과 IM/P 간의 보안 연결 등에 사용됩니다.

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

XMPP 세션이 생성될 때 XMPP 클라이언트에 대한 보안 연결을 검증하는 데 사용됩니다.

Cisco Unified Presence - Extensible Messaging and Presence Protocol - Server to Server(CUP-XMPP-S2S) 인증서

외부 페더레이션 XMPP 시스템과의 XMPP 도메인 간 페더레이션에 대한 보안 연결을 확인하는 데 사용됩니다.

IP 보안(IPSec) 인증서

사용 용도:
· DRS(Disaster Recovery System)/DRF(Disaster Recovery Framework)에 대한 보안 연결 확인
· 클러스터의 CUCM(Cisco Unified Communications Manager) 및 IM/P 노드에 대한 IPsec 터널의 보안 연결 확인

Tomcat 인증서

사용 용도:

· 클러스터의 다른 노드에서 서비스 페이지에 액세스하는 것과 같은 다양한 웹 액세스와 Jabber 액세스를 검증합니다.
· SAML SSO(Single Sign-On)에 대한 보안 연결을 확인합니다.

· 클러스터 간 피어에 대한 보안 연결을 검증합니다.

주의: Unified Communication 서버에서 SSO 기능을 사용하고 Cisco Tomcat 인증서가 재생성되는 경우 SSO를 새 인증서로 다시 구성해야 합니다. CUCM 및 AD FS 2.0에서 SSO를 구성하는 링크는 https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html입니다.

참고: CUCM Certificate Regeneration/Renewal Process(CUCM 인증서 재생성/갱신 프로세스) 링크는 https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html입니다.

인증서 재생성 프로세스

CUP 인증서

1단계. 클러스터의 각 서버에 대해 GUI(Graphical User Interface)를 엽니다. IM/P 게시자로 시작한 다음 각 IM/P 가입자 서버에 대한 GUI를 차례로 열고 Cisco Unified OS Administration > Security > Certificate Management.

2단계. 게시자 GUI로 시작하고 모든 인증서를 표시하도록 선택합니다Find. 인증서를 cup.pem 선택합니다. 팝업이 열리면 팝업이 닫히기 전에 성공할 때까지 선택하고Regenerate 기다립니다.

3단계. 후속 가입자로 계속 진행하여 2단계와 동일한 절차를 참조하고 클러스터의 모든 가입자를 완료합니다.

4단계. 모든 노드에서 CUP 인증서가 재생성된 후 서비스를 재시작해야 합니다.

참고: Presence Redundancy Group(프레즌스 이중화 그룹) 컨피그레이션에 Enable High Availability(고가용성 활성화)가 선택되어 있으면 서비스를Uncheck 재시작하기 전에 해당 컨피그레이션을 다시 시작합니다. 프레즌스 이중화 그룹 컨피그레이션은 에서 액세스할 수 있습니다CUCM Pub Administration > System > Presence Redundancy Group. 서비스를 다시 시작하면 IM/P가 일시적으로 중단되며 운영 시간 외에 수행해야 합니다.

다음 순서로 서비스를 다시 시작합니다.

· 게시자의 Cisco Unified Serviceability에 로그인합니다.

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco SIP Proxy 서비스

c. 서비스 재시작이 완료되면 가입자 및 Cisco SIP Proxy 서비스를Restart 계속 진행합니다.

d. 게시자부터 시작한 다음 구독자를 계속 진행합니다. Restart Cisco SIP Proxy 서비스(또는에서Cisco Unified Serviceability > Tools > Control Center - Feature Services).

· 게시자의 Cisco Unified Serviceability에 로그인합니다.

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco Presence Engine 서비스

c. 서비스 재시작이 완료되면 가입자에서 Cisco Presence EngineServiceRestart 를 계속 진행합니다.

참고: SIP 페더레이션에 대해 구성된 경우 CiscoRestart XCP SIP Federation Connection Manager 서비스(소재Cisco Unified Serviceability > Tools > Control Center - Feature Services). 게시자로 시작한 다음 가입자로 계속 진행합니다.

CUP-XMPP 인증서

참고: Jabber는 CUCM 및 IM/P Tomcat 및 CUP-XMPP 서버 인증서를 사용하여 Tomcat 및 CUP-XMPP 서비스의 연결을 검증하므로, 이러한 CUCM 및 IM/P 인증서는 대부분의 경우 CA 서명됩니다. Jabber 디바이스에 루트 및 CUP-XMPP 인증서의 일부인 중간 인증서가 인증서 신뢰 저장소에 설치되어 있지 않다고 가정합니다. 이 경우 Jabber 클라이언트는 신뢰할 수 없는 인증서에 대한 보안 경고 팝업을 표시합니다. Jabber 디바이스 트러스트 스토어의 인증서에 아직 설치되지 않은 경우 그룹 정책, MDM, 이메일 등을 통해 루트 및 중간 인증서를 Jabber 디바이스로 푸시해야 합니다. 이는 Jabber 클라이언트에 따라 달라집니다.

참고: CUP-XMPP 인증서가 자체 서명된 경우, CUP-XMPP 인증서가 Jabber 디바이스 인증서의 신뢰 저장소에 설치되지 않은

경우 Jabber 클라이언트는 신뢰할 수 없는 인증서에 대한 보안 경고 팝업을 표시합니다. 아직 설치되지 않은 경우, 자체 서명 CUP-XMPP 인증서는 그룹 정책, MDM, 이메일 등을 통해 Jabber 디바이스에 푸시되어야 하며, 이는 Jabber 클라이언트에 따라 달라집니다.

1단계. 클러스터의 각 서버에 대한 GUI를 엽니다. IM/P 게시자로 시작한 다음 각 IM/P 가입자 서버에 대한 GUI를 차례로 열고 로 **Cisco Unified OS Administration** > **Security** > **Certificate Management**이동합니다.

2단계. 게시자 GUI로 시작하고 모든 인증서를 표시하도록 선택합니다Find. 인증서의 유형 열에서 cup-xmpp.pem 자체 서명 또는 CA 서명 여부를 결정합니다. cup-xmpp.pem 인증서가 서드파티 서명(CA 서명 유형) 배포 다중 SAN인 경우 다중 SAN CUP-XMPP CSR을 생성하고 CA 서명 CUP-XMPP 인증서에 대해 CA에 제출할 때 이 링크를 검토하십시오. CA 서명 다중 서버 주체 대체 이름 컨피그레이션 예제가 포함된 Unified Communication 클러스터 설정입니다.

인증서가 서드파티 서명(CA 서명 유형) 배포 단일 노드인 경우(배포 이름이 인증서의 공용 이름과 같음) 단일 노드 CSR을 생성하고 CA 서명 CUP-XMPP 인증서에 대해 CA에 제출할 때 이 링크를 검토하십시오. Jabber는 cup-xmpp.pem 인증서 검증을 위한 How-To Guide를 CUP-XMPP 완료합니다. 인증서가 cup-xmpp.pem 자체 서명된 경우 3단계로 진행합니다.

3단계. Find 모든 인증서를 표시하려면 를 선택한 다음 인증서를 cup-xmpp.pem 선택합니다. 팝업이 열리면 팝업이 닫히기 전에 성공할 때까지 선택하고Regenerate 기다립니다.

4단계. 후속 가입자로 계속 진행합니다. 2단계에서 동일한 절차를 참조하고 클러스터의 모든 가입자에 대해 이 절차를 완료합니다.

5단계. 모든 노드에서 CUP-XMPP 인증서가 재생성되면 IM/P 노드에서 Cisco XCP Router 서비스를 재시작해야 합니다.

참고: Presence Redundancy Group Configuration(프레즌스 이중화 그룹 컨피그레이션)에서 Enable High Availability(고가용성 활성화)를 선택한 경우, Uncheck 서비스를 재시작하기 전에 이 옵션을 선택합니다. 프레즌스 이중화 그룹 컨피그레이션은에서 액세스할 수 있습니다CUCM Pub Administration > System > Presence Redundancy Group. 서비스를 다시 시작하면 IM/P가 일시적으로 중단되며 운영 시간 외에 수행해야 합니다.

· 게시자의 Cisco Unified Serviceability에 로그인합니다.

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart Cisco XCP Router 서비스

c. 서비스 재시작이 완료되면 가입자에서 Cisco XCP Router 서비스를Restart 계속 진행합니다.

CUP-XMPP-S2S 인증서

1단계. 클러스터의 각 서버에 대한 GUI를 엽니다. IM/P 게시자로 시작한 다음 각 IM/P 가입자 서버에 대한 GUI를 차례로 열고 로 Cisco Unified OS Administration > Security > Certificate Management 이동합니다.

2단계. 게시자 GUI로 시작하여 모든 인증서를 표시하도록 선택하고 Find 인증서를 cup-xmpp-s2s.pem 선택합니다. 팝업이 열리면 팝업이 닫히기 전에 성공할 때까지 선택하고Regenerate 기다립니다.

3단계. 후속 가입자로 계속 진행하여 2단계에서 동일한 절차를 참조하고 클러스터의 모든 가입자에 대해 완료합니다.

4단계. 모든 노드에서 CUP-XMPP-S2S 인증서가 재생성된 후에는 서비스를 앞서 언급한 순서대로 재시작해야 합니다.

참고: Presence Redundancy Group Configuration(프레즌스 이중화 그룹 컨피그레이션)에서 Enable High Availability(고가용성 활성화)를 선택한 경우,Uncheck 이러한 서비스가 재시작되기 전에 이 옵션을 선택합니다. 프레즌스 이중화 그룹 컨피그레이션 은에서 액세스할 수 CUCM Pub Administration > System > Presence Redundancy Group 있습니다. 서비스를 다시 시작하면 IM/P가 일시적으로 중단되며 운영 시간 외에 수행해야 합니다.

· 게시자의 Cisco Unified Serviceability에 로그인합니다.

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.
b. Restart Cisco XCP Router 서비스
c. 서비스 재시작이 완료되면 가입자에서 Restart Cisco XCP Router 서비스를 계속 진행합니다.

· 게시자의 Cisco Unified Serviceability에 로그인합니다.

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco XCP XMPP Federation Connection Manager 서비스

c. 서비스 재시작이 완료되면 가입자Restart 의 Cisco XCP XMPP Federation Connection Manager 서비스를 계속 진행합니다.

IPSec 인증서

참고: CUCM 게시자의 ipsec.pem 인증서는 유효해야 하며 IPSec 트러스트 저장소의 모든 가입자(CUCM 및 IM/P 노드)에 있어야 합니다. 구독자 ipsec.pem 의 인증서가 표준 배포에서 IPSec 트러스트 저장소로 게시자에 없습니다. 유효성을 확인하려면 CUCM-PUB의 ipsec.pem 인증서 일련 번호와 가입자의 IPSec-trust를 비교합니다. 꼭 일치해야 합니다.

참고: DRS는 CUCM 클러스터 노드(CUCM 및 IM/P 노드) 간의 데이터 인증 및 암호화를 위해 소스 에이전트와 로컬 에이전트 간의 SSL(Secure Socket Layer) 기반 통신을 사용합니다. DRS는 공용/개인 키 암호화에 IPSec 인증서를 사용합니다. Certificate Management(인증서 관리) 페이지에서 IPSEC Trust Store (hostname.pem) 파일을 삭제하면 DRS가 예상대로 작동하지 않습니다. IPSEC 신뢰 파일을 수동으로 삭제하는 경우 IPSEC 인증서를 IPSEC 신뢰 저장소에 업로드해야 합니다. 자세한 내용은 CUCM 보안 가이드의 인증서 관리 도움말 페이지를 참조하십시오.

1단계. 클러스터의 각 서버에 대한 GUI를 엽니다. IM/P 게시자로 시작한 다음 각 IM/P 가입자 서버에 대한 GUI를 차례로 열고 로 Cisco Unified OS Administration > Security > Certificate Management 이동합니다.

2단계. 게시자 GUI로 시작하고 모든 인증서를 표시하도록 선택합니다Find.Choose 인증서를ipsec.pem 표시합니다. 팝업이 열리면 팝업이 닫히기 전에 성공할 때까지 선택하고Regenerate 기다립니다.

3단계. 후속 가입자로 계속 진행하여 2단계에서 동일한 절차를 참조하고 클러스터의 모든 가입자에 대해 완료합니다.

4단계. 모든 노드에서 IPSEC 인증서를 다시 생성한 다음 이러한 서비스를Restart 생성합니다. 게시자의 Cisco Unified Serviceability로 이동합니다Cisco Unified Serviceability > Tools > Control Center - Network Services.
a. Cisco DRF 기본 서비스에서 선택합니다Restart.
Restart b. 서비스 재시작이 완료되면 게시자의 Cisco DRF Local(Cisco DRF 로컬) 서비스를 선택한 다음Restart 각 가입자의 Cisco DRF Local(Cisco DRF 로컬) 서비스를 계속합니다.

Tomcat 인증서

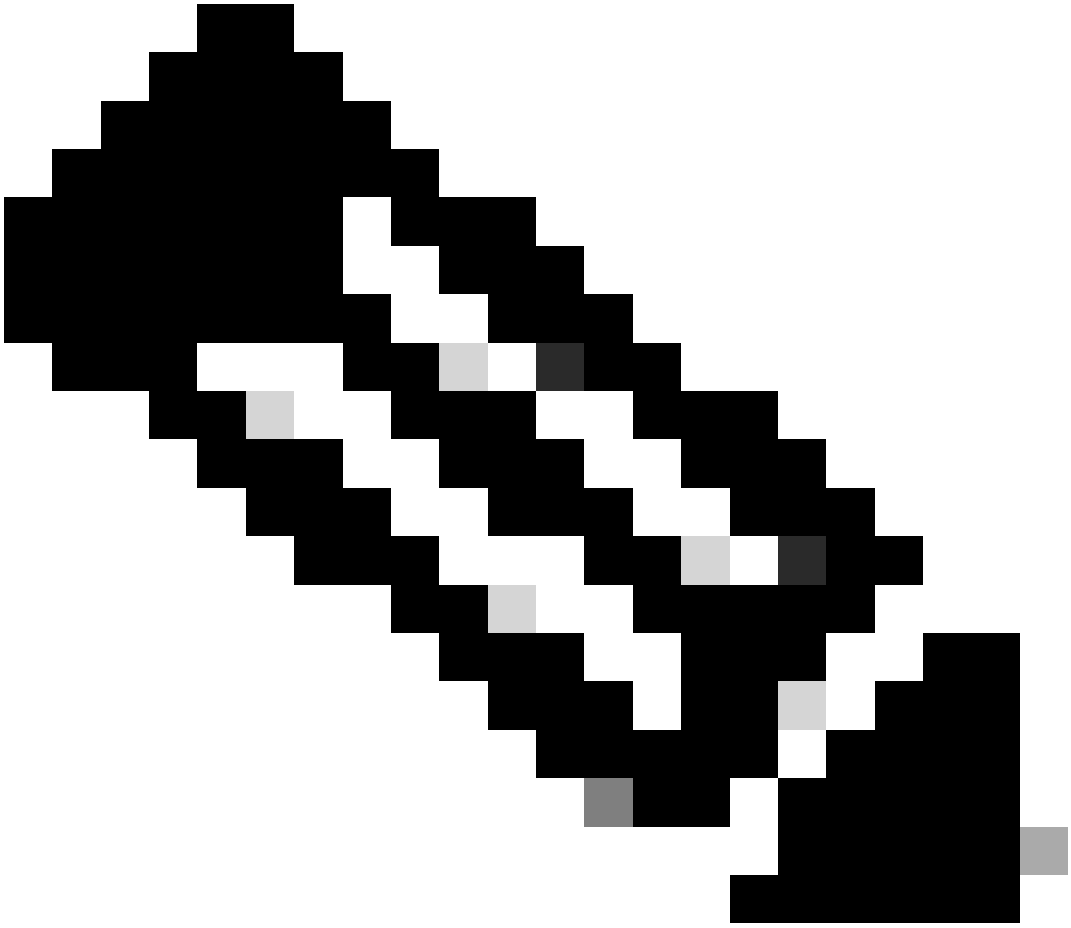
참고: Jabber는 CUCM Tomcat 및 IM/P Tomcat 및 CUP-XMPP 서버 인증서를 사용하여 Tomcat 및 CUP-XMPP 서비스에 대한 연결을 검증하므로, 이러한 CUCM 및 IM/P 인증서는 대부분의 경우 CA 서명됩니다. Jabber 디바이스에 루트와 해당 인증서 신뢰 저장소에 설치된 Tomcat 인증서의 일부인 중간 인증서가 없다고 가정합니다. 이 경우 Jabber 클라이언트는 신뢰할 수 없는 인증서에 대한 보안 경고 팝업을 표시합니다. Jabber 디바이스의 인증서 신뢰 저장소에 아직 설치되지 않은 경우, 그룹 정책, MDM, 이메일 등을 통해 루트 및 중간 인증서를 Jabber 디바이스로 푸시해야 하며, 이는 Jabber 클라이언트에 따라 달라집니다 .

참고: Tomcat 인증서가 자체 서명된 경우, Tomcat 인증서가 Jabber 디바이스의 인증서 신뢰 저장소에 설치되지 않은 경우, Jabber 클라이언트는 신뢰할 수 없는 인증서에 대한 보안 경고 팝업을 표시합니다. Jabber 디바이스의 인증서 신뢰 저장소에 아직 설치되지 않은 경우, 그룹 정책, MDM, 이메일 등을 통해 자체 서명된 CUP-XMPP 인증서를 Jabber 디바이스로 푸시해야 합니다. 이는 Jabber 클라이언트에 따라 다릅니다.

1단계. 클러스터의 각 서버에 대한 GUI를 엽니다. IM/P 게시자로 시작한 다음 각 IM/P 가입자 서버에 대한 GUI를 차례로 열고 로 Cisco Unified OS Administration > Security > Certificate Management 이동합니다.

2단계. 게시자 GUI로 시작하고 모든 인증서Find 를 표시하도록 선택합니다.
· 인증서의 Type(유형) 열에서tomcat.pem 자체 서명 또는 CA 서명 여부를 결정합니다.

· 인증서가tomcat.pem 서명한(CA 서명 유형) 배포 멀티 SAN인 경우, 멀티 SAN Tomcat CSR을 생성하는 방법에 대한 이 링크를 검토하고 CA 서명 Tomcat 인증서인 CA 서명 멀티 서버 주체 대체 이름 컨피그레이션을 사용하여 CA에 제출합니다.



참고: 다중 SAN Tomcat CSR은 CUCM 게시자에서 생성되고 클러스터의 모든 CUCM 및 IM/P 노드에 배포됩니다.

tomcat.pem

· 인증서가 서드파티 서명(CA 서명 유형) 배포 단일 노드인 경우(배포 이름이 인증서의 공용 이름과 같음) 이 링크를 검토하여 단일 노드 CUP-XMPP CSR을 생성한 후 CA 서명 CUP-XMPP 인증서용 CA에 제출합니다. Jabber 인증서 검증을 위한 How-To Guide를 완료합니다

· 인증서 tomcat.pem 가 자체 서명된 경우 3단계로 진행합니다.

3단계. 모든 인증서를 표시하려면 선택 Find합니다.
· 인증서를 tomcat.pem 선택합니다.
· 열리면 팝업이 닫히기 전에 성공 팝업이 표시될 때까지 선택하고Regenerate 기다립니다.

4단계. 각 후속 가입자로 계속 진행하여 2단계의 절차를 참조하고 클러스터의 모든 가입자를 완료합니다.

5단계. Restart 모든 노드에서 Tomcat 인증서를 다시 생성한 후 모든 노드에서 Tomcat 서비스가 생성됩니다. 게시자로 시작하고 그 뒤에 가입자가 옵니다.
· Tomcat 서비스를 Restart 제공하려면 이미지에 표시된 대로 각 노드에 대한 CLI 세션을 열고 서비스가 Cisco Tomcat을 다시 시작할 때까지 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:
```

만료된 트러스트 인증서 삭제

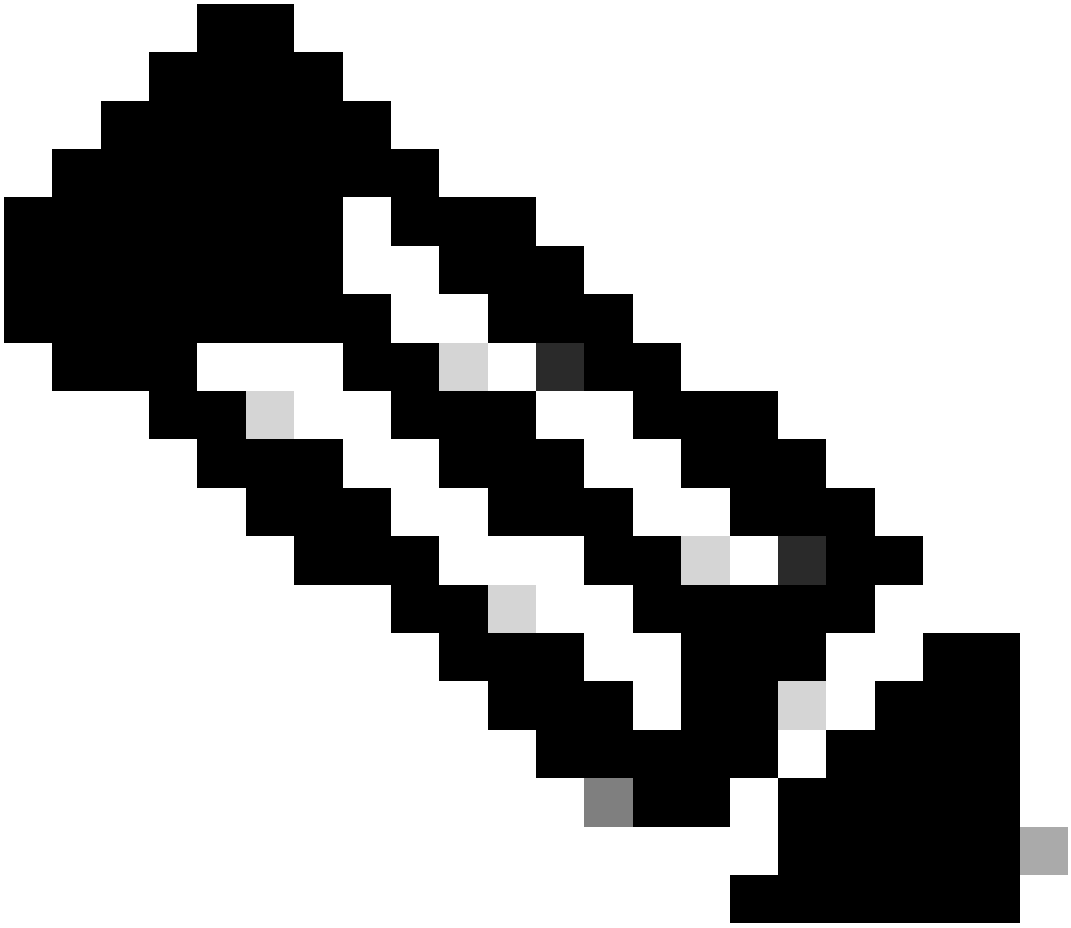
참고: 신뢰 인증서(-trust로 끝나는 인증서)는 적절한 경우 삭제할 수 있습니다. 삭제할 수 있는 신뢰 인증서는 더 이상 필요하지 않거나, 만료되었거나, 더 이상 사용되지 않는 인증서입니다. 5개의 ID 인증서(cup.pem , cup-xmpp.pem , cup-xmpp-s2s.pem , ipsec.pem 및 tomcat.pem 인증서)를 삭제하지 마십시오. 표시된 대로 서비스는 해당 서비스 내에서 이러한 레거시 인증서의 모든 메모리 내 정보를 지우도록 설계되었습니다.

참고: Presence Redundancy Group Configuration(프레즌스 이중화 그룹 컨피그레이션)에서 Enable High Availability(고가용성 활성화)를 선택한 경우, Uncheck 서비스가 Stopped/Started 또는 활성화되기 전에 이Restarted를 선택합니다. 프레즌스 이중화 그룹 컨피그레이션은에서 액세스할 수 있습니다CUCM Pub Administration > System > Presence Redundancy Group. 그림과 같이 일부 서비스를 다시 시작하면 IM/P가 일시적으로 중단되므로 운영 시간 외에 수행해야 합니다.

1단계. 다음으로 이동합니다.Cisco Unified Serviceability > Tools > Control Center - Network Services

Stop · 드롭다운 메뉴에서 IM/P 게시자를 선택하고 Cisco Certificate Expiry Monitor(Cisco 인증서 만료 모니터)에서 선택한 다음Stop Cisco Intercluster Sync Agent에서 선택합니다.

· 클러스터의 각 IM/P 노드에 대해 이러한 서비스를 반복합니다Stop.



참고: Tomcat-trust 인증서를 삭제해야 하는 경우 CUCM 게시자의Cisco Unified Serviceability > Tools > Control Center - Network Services 로 이동합니다.

· 드롭다운에서 CUCM 게시자를 선택합니다.

· Cisco Certificate Expiry Monitor(Cisco 인증서 만료 모니터)에서 선택한 Stop다음 Cisco Certificate Change Notification(Cisco 인증서 변경 알림)에서Stop 선택합니다.

· 클러스터의 모든 CUCM 노드에 대해 반복합니다.

2단계. 로 Cisco Unified OS Administration > Security > Certificate Management > Find 이동합니다.

· 만료된 트러스트 인증서를 찾습니다(버전 10.x 이상에서는 Expiration으로 필터링할 수 있음). 10.0 이전 버전에서는 수동으로 또는

RTMT 알림(수신된 경우)을 통해 특정 인증서를 식별해야 합니다.
· 동일한 신뢰 인증서가 여러 노드에 나타날 수 있으며 각 노드에서 개별적으로 삭제해야 합니다.
· 삭제할 신뢰 인증서를 선택합니다(버전에 따라 팝업을 받거나 같은 페이지의 인증서로 이동함).

· 선택Delete("이 인증서를 영구적으로 삭제하려고 합니다..."로 시작하는 팝업이 표시됩니다.)
· 클릭 OK.

3단계. 삭제할 모든 신뢰 인증서에 대해 이 과정을 반복합니다.

4단계. 완료되면 삭제된 인증서와 직접 관련된 서비스를 다시 시작해야 합니다.

· CUP-trust: Cisco SIP Proxy, Cisco Presence Engine, 그리고 SIP Federation에 대해 구성된 경우 Cisco XCP SIP Federation Connection Manager(CUP 인증서 섹션 참조)
· CUP-XMPP-trust: Cisco XCP Router(CUP-XMPP 인증서 섹션 참조)
· CUP-XMPP-S2S-trust: Cisco XCP Router 및 Cisco XCP XMPP Federation Connection Manager
· IPSec-trust: DRF Source/DRF Local(IPSec 인증서 섹션 참조)
· Tomcat-trust: 명령줄을 통해 Tomcat 서비스를 다시 시작합니다(Tomcat 인증서 섹션 참조).

5단계. 1단계에서 중지된 서비스를 다시 시작합니다.

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 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.