

# 보안 인증서 관리 향상

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

## 소개

이 문서에서는 사용자 환경을 개선하고 클러스터 전체에서 인증서 삭제를 허용하는 기능에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 Cisco CUCM(Unified Communication Manager) 버전 11.0 이상에 대한 지식을 보유하고 있는 것을 권장합니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

## 배경 정보

CUCM 및 IM&P에 관리자가 모르는 상태에서 투명하게 복제되는 특정 인증서가 있습니다. 즉, 한 서버에서 Admin이 인증서를 업로드하면 클러스터 내의 다른 서버로 푸시됩니다.이는 EMCC(Extension Mobility Cross Cluster) 기능을 지원하기 위해 수행됩니다.

이전에는 대규모 클러스터에서 불필요한 인증서를 삭제해야 하는 경우 관리자가 각 서버에 로그인하고 인증서를 수동으로 삭제해야 했습니다.또한 지정된 창 내에서 이 작업을 수행하지 않으면 삭제된 인증서가 30분마다 실행되는 CertSync 서비스 때문에 다시 나타날 수 있으며, 이는 파일 시스템 및 인증서 테이블이 동기화되도록 합니다.이러한 문제를 방지하기 위해, 오늘날 고객은 모든 노드에서 CertSync 서비스를 비활성화하고 모든 노드에서 인증서를 삭제합니다.이로 인해 사용자 환경이 매우 나빠집니다.

새로운 기능 개선을 통해 이러한 인스턴스가 발생하지 않습니다.

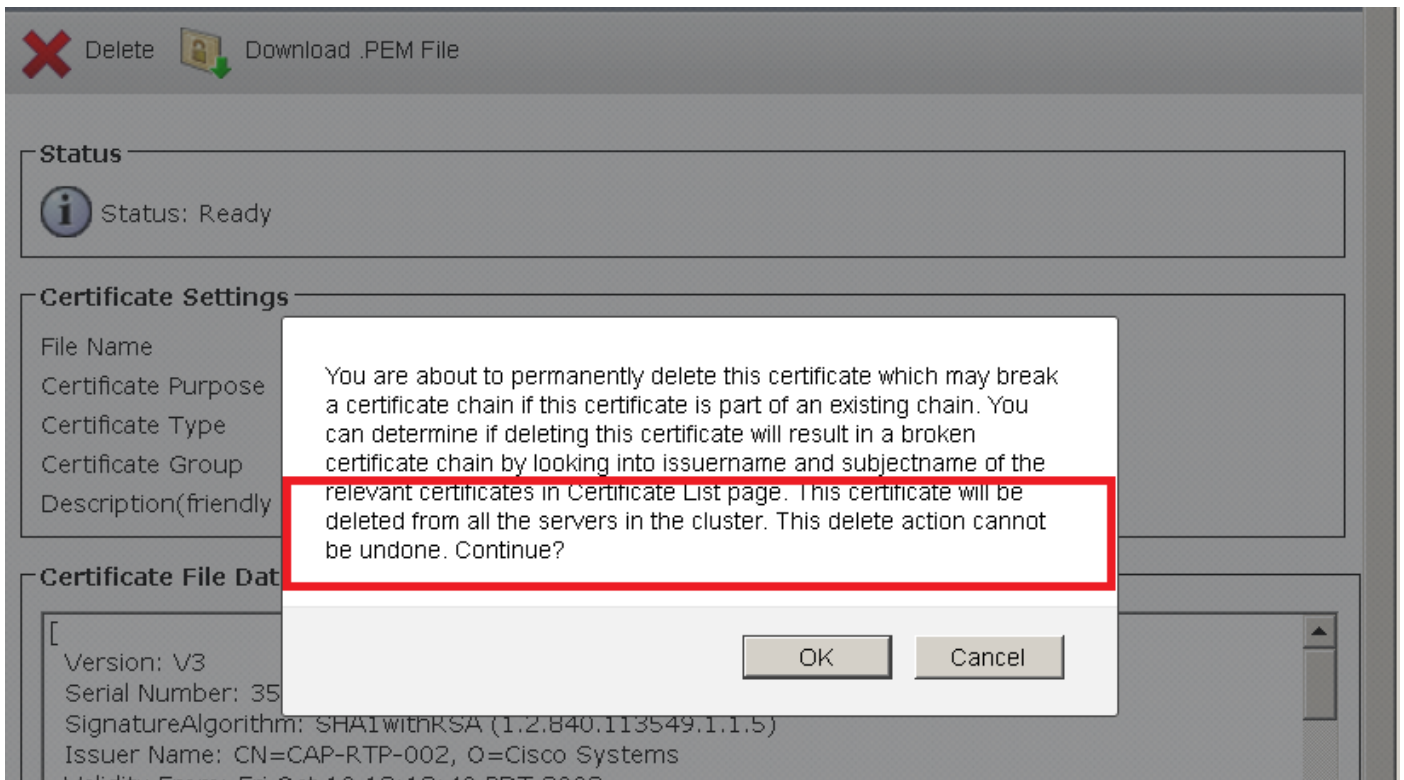
이 기능을 인증서 관리로 변경하면 클러스터의 모든 노드에서 인증서를 자동으로 삭제할 수 있습니다.

클러스터의 한 노드에서 인증서가 삭제되면 클러스터의 다른 모든 노드에서 인증서가 삭제됩니다.

## 구성

Cisco Call Manager에서 Cisco Unified OS Administration(Cisco Unified OS 관리) > Under Security(보안) > Certificate Management(인증서 관리)로 이동합니다.

삭제해야 하는 인증서를 선택합니다.다음 항목이 표시됩니다.



확인을 클릭하면 다음 단계가 수행됩니다.

1. 인증서가 서버에서 로컬로 삭제됩니다.
2. 인증서가 성공적으로 삭제되면 플랫폼 이벤트가 트리거됩니다.이 플랫폼 이벤트는 클러스터의 모든 서버(CUCM 및 IM&P)로 전송됩니다. 플랫폼 이벤트에 있는 정보는 인증서의 이름과 함께 장치 유형(CallManager, Tomcat 또는 Phone-SAST)입니다(예: RootCA.pem). 플랫폼 이벤트를 사용하면 이벤트 클러스터 전체에서 삭제 이벤트를 트리거할 수 있습니다.

인증서 삭제 작업은 다음 인증서에만 적용됩니다.

### CUCM

1. Tomcat 트러스트
2. CallManager-trust

### 3. 전화-SAST-트러스트

CUCM IM& Presence

#### 1. 톰cat 트러스트

## 다음을 확인합니다.

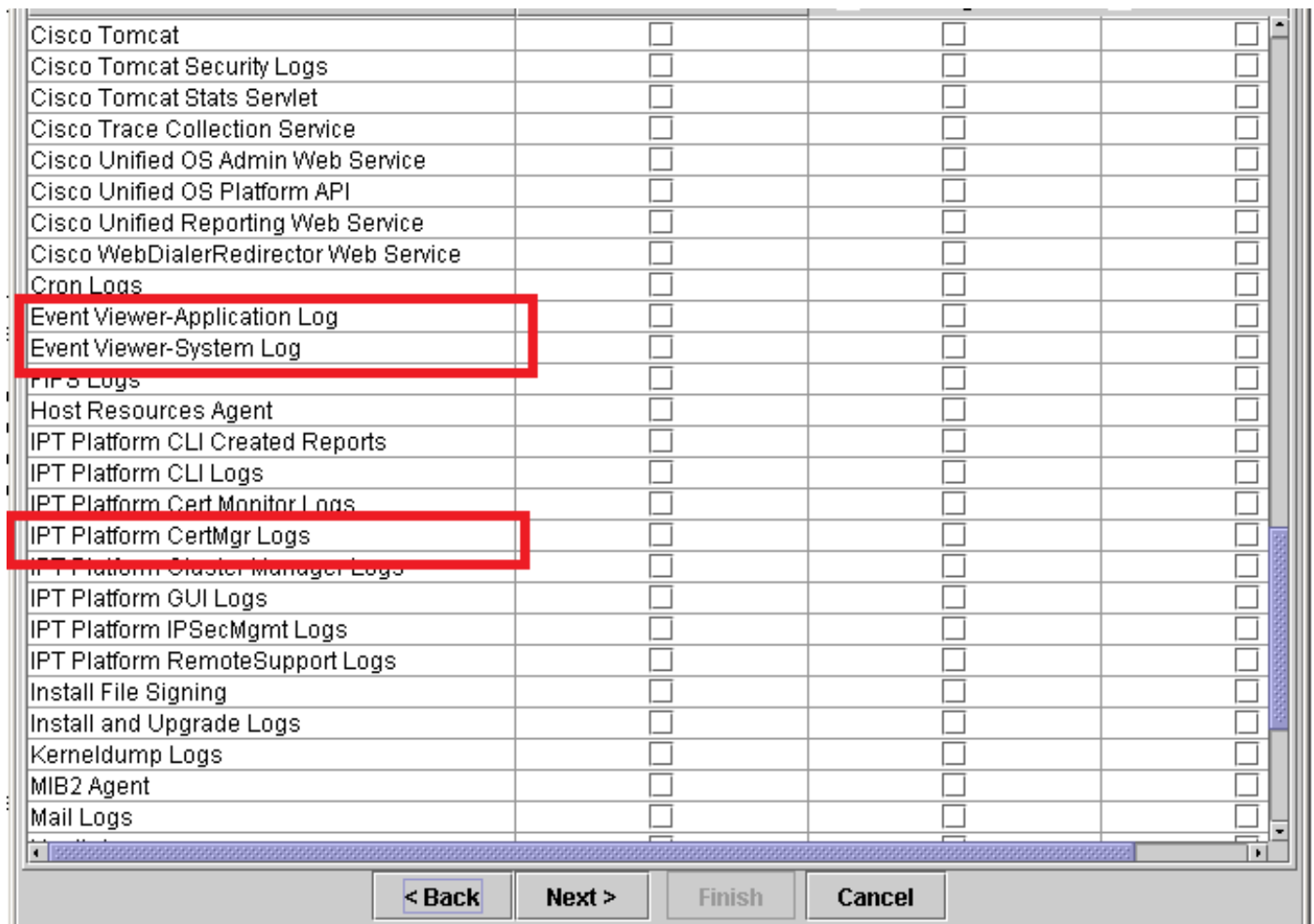
현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

## 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

클러스터의 다른 노드에 있는 인증서가 삭제되지 않은 경우 RTMT에서 이러한 로그를 수집하여 이 문제를 해결하십시오.

1. 이벤트 뷰어-애플리케이션 로그
2. 이벤트 뷰어-시스템 로그
3. IPT 플랫폼 CertMgr 로그



샘플 메시지:

7월 6일 03:12:05 CM11 사용자 6 log\_impl:platform-event(—no-wait platform-event-clusterwide-certificate-delete HOSTNAME=CM11하위 UNIT=tomcat-trust Type=certs-trust NAME=testcert.pem)에 대한 요청을 받았습니다.

이 로그는 인증서가 한 노드에서 삭제될 때 클러스터의 다른 노드에서 인증서 테스트 인증서를 삭제하기 위해 이벤트를 수신했음을 나타냅니다.

삭제 작업에 대한 certMgmt 로그에서:

이 로그는 인증서 관리가 tomcat\_trust에서 certificate.pem의 삭제 요청을 받았음을 보여줍니다.

디코딩: 참

op: 삭제

단위: tomcat 트러스트

keystoreUnit:tomcat-trust

로그 파일: /var/log/active/platform/log/cert-mgmt.log

resultFile:/var/log/active/platform/log/certde-info.xml

키 디렉터리: /usr/local/cm/.security/tomcat/keys

certDir: /usr/local/cm/.security/tomcat/trust-certs/Certificate.pem

이 로그는 인증서가 데이터베이스에서 삭제되었음을 보여줍니다.

2016-07-06 01:31:55,374 INFO [main] - IN — CertDBAction.java - deleteCertificateInDB(certInfo) -