Mejora en la gestión de certificados de seguridad CUCM 11.x

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Administración de certificados](#)
[Versiones antiguas](#)
[Nuevas versiones](#)
[Preguntas Frecuentes](#)
[Verifiy](#)
[Registros del sistema](#)
[Registros IPT Platform CertMgr](#)

Introducción

Este documento describe el avance realizado en la gestión de certificados para Cisco Unified Communications Manager (CUCM) implementado en la versión 11.x.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- CUCM, versión 11.5.1.10000-6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

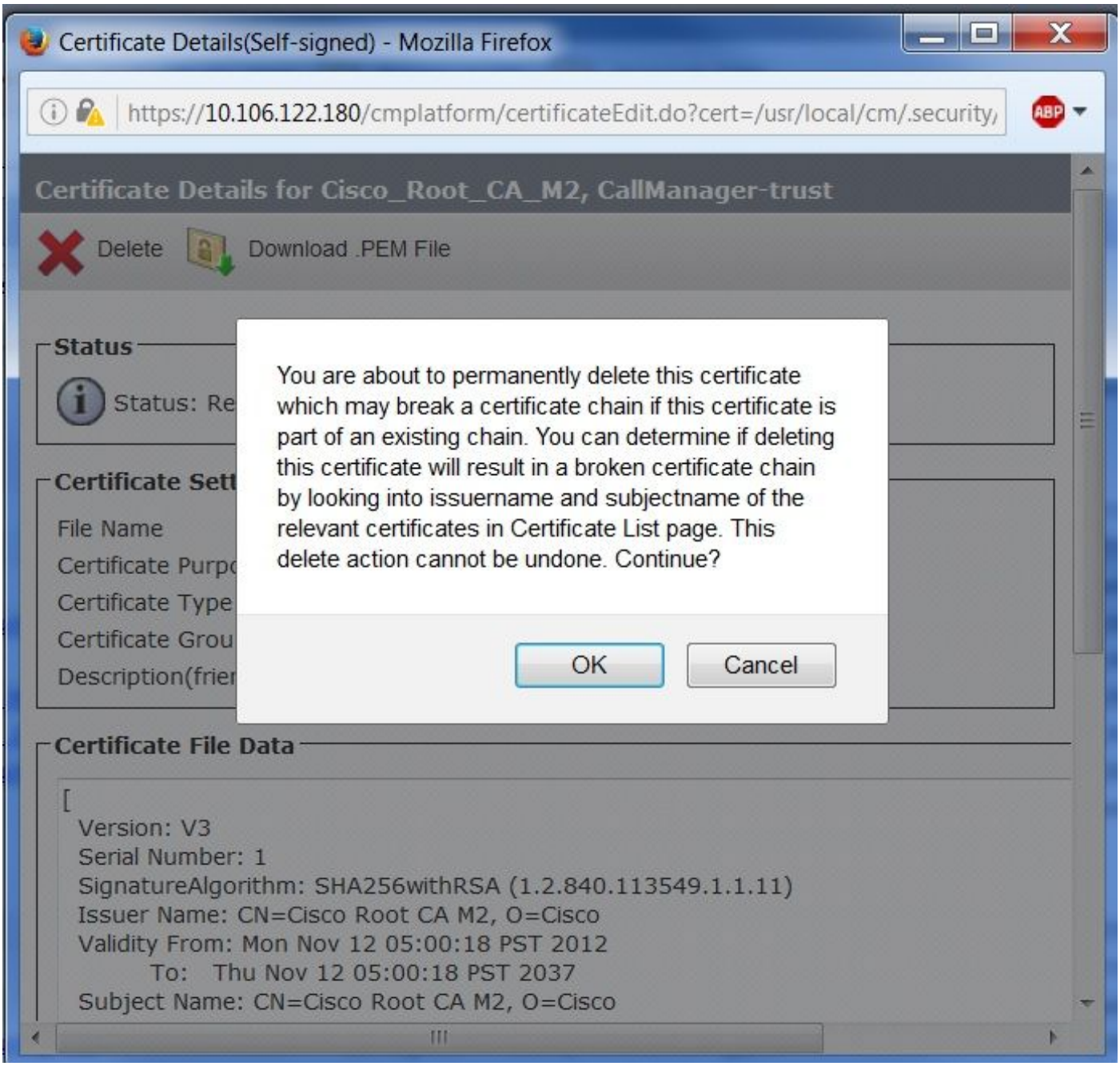
La gestión de certificados de CUCM ayuda a las Comunicaciones Unificadas o a los

administradores de seguridad a aprovechar las ventajas de administrar los certificados de forma más eficaz. Entre las ventajas de la mejora realizada se incluye una reducción del tiempo durante la eliminación de los certificados no deseados caducados en CUCM y IM&Presence.

Administración de certificados

Versiones antiguas

Antes de la versión 11 de CUCM, este mensaje aparecía si se elimina un certificado.



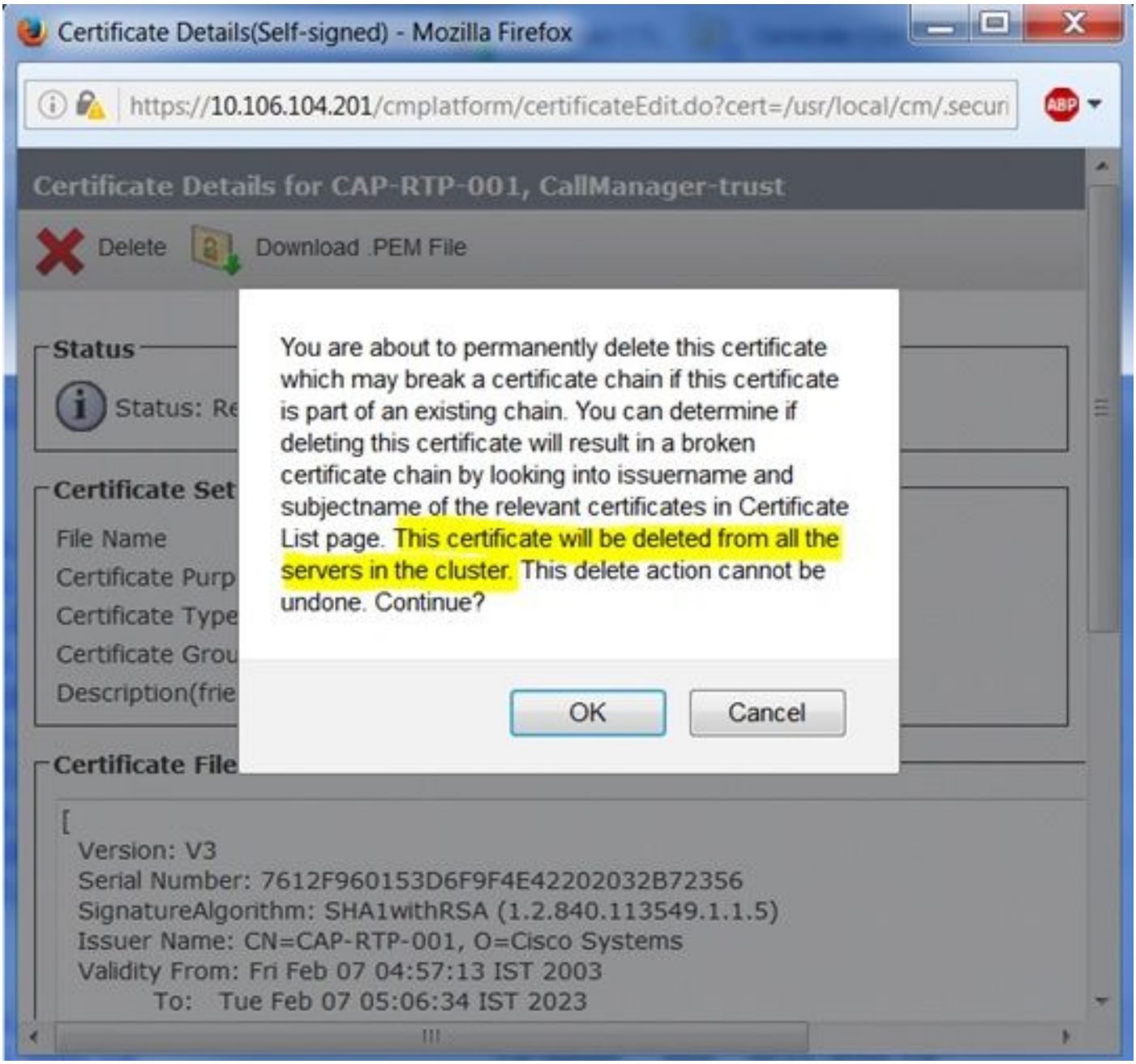
El certificado se elimina sólo del nodo en el que se inicia la operación de eliminación.

Si el mismo certificado no se elimina en otros nodos, el certificado eliminado se rellena nuevamente en el nodo donde se eliminó inicialmente. Esto se debe al servicio de supervisión de certificados llamado Notificación de cambio de certificado. Como práctica recomendada en versiones anteriores de CUCM, el servicio de Notificación de cambios de certificados se detiene

en todos los nodos de CUCM antes de la eliminación del certificado. Otra desventaja en las versiones anteriores es el requisito de iniciar sesión en la sección de administración del SO de cada nodo para eliminar un único certificado no deseado o vencido, que se vuelve tedioso y consume mucho tiempo, especialmente para un clúster grande.

Nuevas versiones

A partir de la versión 11.0 o posterior de CUCM, los certificados no deseados o caducados que se eliminen del nodo actual también se eliminarán de todos los demás nodos del clúster.



La mejora se incluyó para abordar estos defectos:

CSCto86463 - Los certificados eliminados reaparecen, no se pueden quitar certificados de CUCM

CSCus28550 - Mejora de la administración de certificados para eliminar un certificado de todos los nodos

Preguntas Frecuentes

P. ¿Cuál es el tipo de certificados incluidos en esta mejora?

A. Para Cisco Unified Communications Manager:

- tomcat-trust
- CallManager-trust
- phone-sast-trust

Para MI y presencia de Cisco Unified Communications Manager:

- tomcat-trust

P. ¿Qué ocurre en el motor de esta mejora?

A. Tan pronto como se elimina un certificado en cualquiera de los nodos CUCM:

- El certificado se elimina del nodo local
- El evento Platform activa la eliminación del mismo certificado a todos los demás nodos.

Verifiy

Una vez que se elimina un certificado a través de la página de administración del sistema operativo en un nodo, inicie sesión en otros nodos y verifique si el certificado está presente o no. Si no se elimina un certificado eliminado de todos los nodos, verifique los registros generados a través de la instancia de eliminación de certificados.

- Registros del sistema
- Registros IPT Platform CertMgr

En un escenario de trabajo común, estos son los registros esperados.

Registros del sistema

El evento de plataforma se ve en otros nodos (excepto en el nodo donde se inició la eliminación del certificado). En este ejemplo, se eliminó del editor un certificado de tomcat-trust denominado CUCMSUB1.pem, mostrándolo en el syslog del suscriptor.

```
Aug  6 20:20:47 CUCMSUB1 user 6 ilog_impl: Received request for platform-event (--no-wait
platform-event-clusterwide-certificate-delete HOSTNAME=CUCM-PUB UNIT=tomcat-trust
NAME=CUCMSUB1.pem)
```

Registros IPT Platform CertMgr

En los registros de CertMgr, los registros confirman que el certificado está en cola para su eliminación de las entradas de la base de datos.

```
2016-08-06 21:22:06,151 INFO [main] - IN -- CertDBAction.java - deleteCertificateInDB(certInfo)
-

2016-08-06 21:22:06,151 INFO [main] -
```

```
DBParameters ...

PKID :                    null

CN :                       L=BGL,ST=Karnataka,CN=CUCMSUB1,OU=TAC,O=Cisco,C=IN

serialNo :              4d6dc0cb7bc73e70c3ded20690d15fa8

hostName :          CUCMSUB1

issuerName :       L=BGL,ST=Karnataka,CN=CUCMSUB1,OU=TAC,O=Cisco,C=IN

Certificate :          Not Printing huge Certificate String..

IPV4Address :      10.106.99.196

IPV6Address :

TimeToLive :        NULL

TkCertificateDistribution :1

UNIT :                   tomcat-trust

TYPE :                    trust-certs

ROLE :                   null

RoleMoniker :    null

RoleEnum :null

SERVICE :                            null

ServiceMoniker :               null

ServiceEnum :0

2016-08-06 21:22:06,151 INFO [main] - DB - Certifciate Store Plugin Handler is
:com.cisco.ccm.certmgmt.db.CertDBImpl

2016-08-06 21:22:06,156 INFO [main] - IN -- CertDBImpl.java - deleteCertificate(certInfo) –
```

El comando SQL disparado para la eliminación del certificado se puede ver en los registros de CertMgr.

```
2016-08-06 21:22:08,980 DEBUG [main] - Delete query of CERTIFICATEPROCESSNODEMAP :DELETE FROM
CERTIFICATEPROCESSNODEMAP WHERE FKCERTIFICATE="cdd0365a-2d17-3483-4d00-1bf08f942cf5" AND
SERVERNAME = "CUCMSUB1"

2016-08-06 21:22:08,980 DEBUG [main] - execute(DELETE FROM CERTIFICATEPROCESSNODEMAP WHERE
FKCERTIFICATE="cdd0365a-2d17-3483-4d00-1bf08f942cf5" AND SERVERNAME = "CUCMSUB1")
```

Desde los registros de CertMgr, las entradas confirman que el certificado se elimina del FILE-SYSTEM (certificado con extensiones pem o der).

```
2016-08-06 21:22:09,009 DEBUG [main] - deleteDERandPEM: sCertDir =
/usr/local/platform/.security/tomcat/trust-certs --- sAlias = CUCMSUB1

2016-08-06 21:22:09,009 INFO [main] - IN -- TomcatCertMgr.java - removeFromKeyStore(..) -
```

```
2016-08-06 21:22:09,010 INFO [main] - IN -- RSACryptoEngine.java -
removeFromKeyStore(keystoreFile, keystorePass, alias) -

2016-08-06 21:22:09,010 INFO [main] - IN -- RSACryptoEngine.java - loadKeyStore(keystoreFile,
keystorePass) -

2016-08-06 21:22:09,086 INFO [main] - OUT -- RSACryptoEngine.java - loadKeyStore -

2016-08-06 21:22:09,103 DEBUG [main] - Removing certificate from keystore : CUCMSUB1
```

Si la eliminación del certificado todavía no se refleja en el resto de los nodos de un clúster o los registros muestran errores, abra un caso TAC con el equipo de CUCM.