Mejora en Administración CUCM 11.x del Security Certificate

Contenido

Introducción

Este documento describe el adelanto hecho en administración de certificados para el administrador de las Comunicaciones unificadas de Cisco (CUCM) implementado en la versión 11.x.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM

Componentes Utilizados

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

- Versión 11.5.1.10000-6 CUCM

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

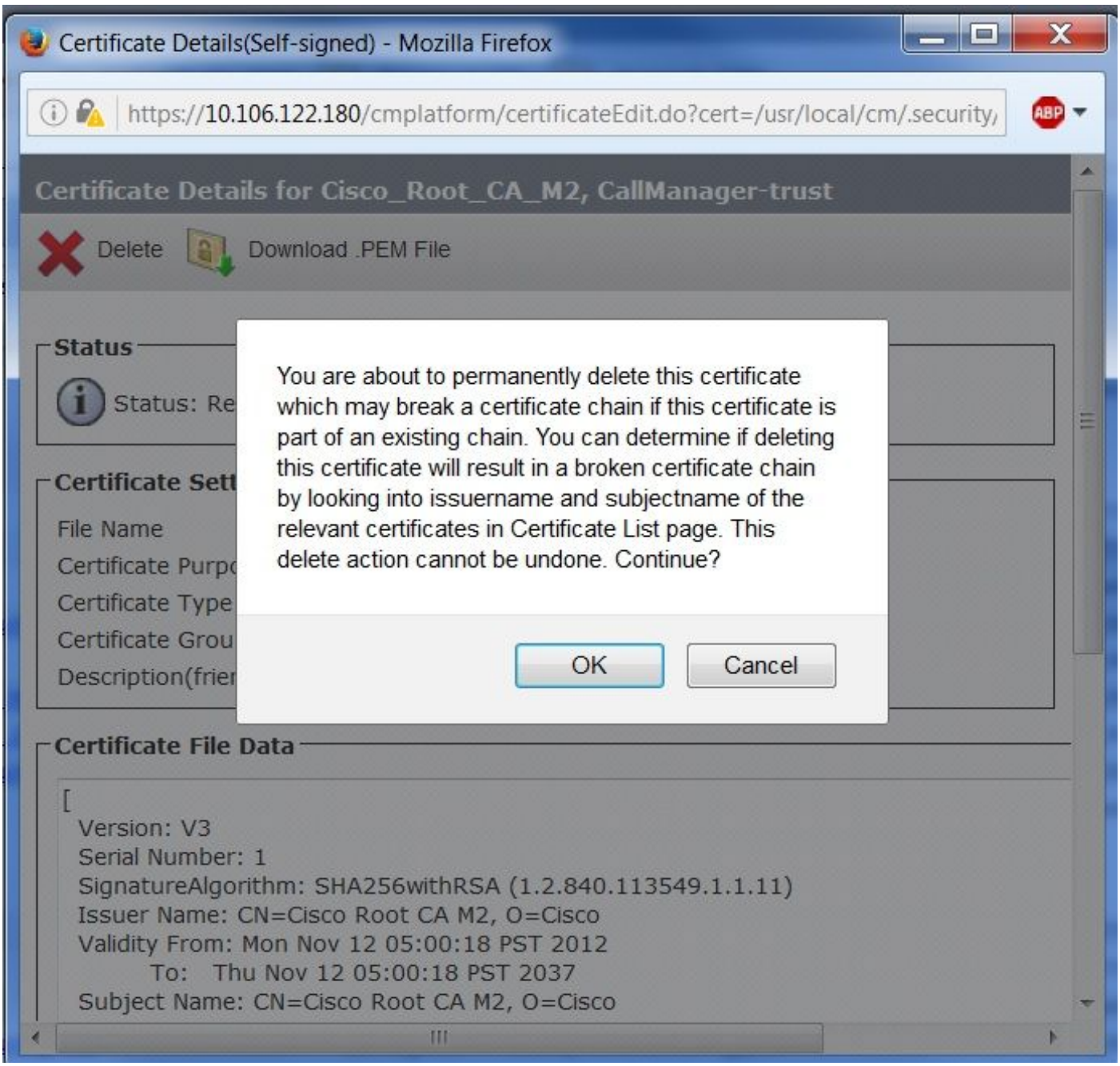
Antecedentes

Las Comunicaciones unificadas o los administradores de seguridad de las ayudas de la administración de certificados CUCM toman los Certificados del advantagesmanage más eficientemente. Las ventajas de la mejora hecha incluyen un rato disminuido durante el retiro de indeseado de los certificados vencidos en CUCM e IM&Presence.

Administración de certificados

Versiones antiguas

Antes de la versión 11 CUCM, este mensaje apareció si se borra un certificado.



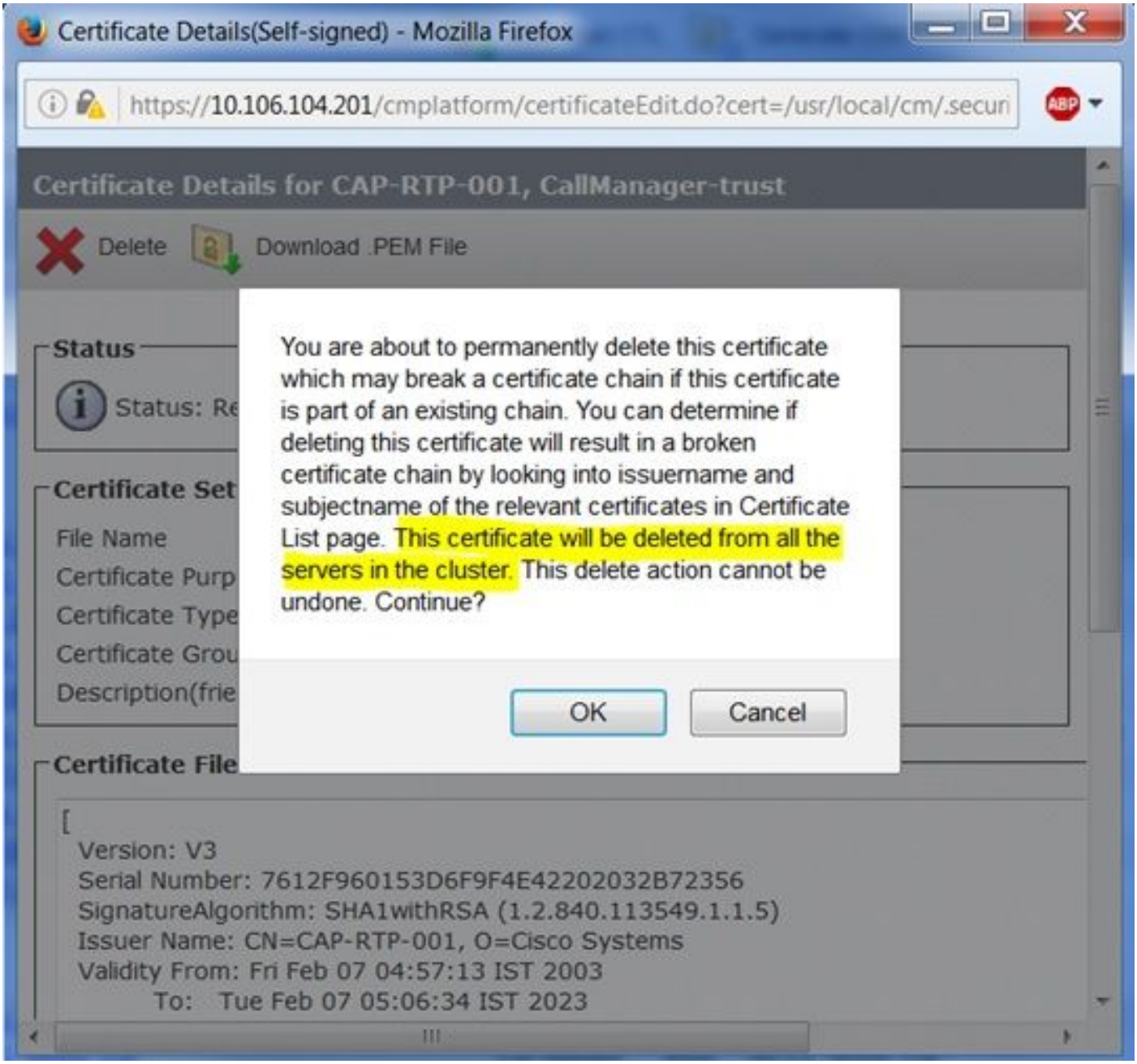
El certificado consigue borrado solamente del nodo en el cual se inicia la operación de eliminación.

Si el mismo certificado no se borra en otros Nodos, el certificado borrado consigue poblado detrás en el nodo donde fue borrado inicialmente. Esto es debido al servicio de supervisión del

certificado llamado notificación de cambio de Certificate. Como mejor práctica en las versiones anteriores de CUCM, el servicio de la notificación de cambio del certificado se para en todos los Nodos CUCM antes de la cancelacíon del certificado. Otra desventaja en las versiones anteriores es el requisito de iniciar sesión a la sección de la administración OS de cada nodo para borrar un solo indeseado o certificado vencido, que llegan a ser aburridos y largos especialmente para un cluster grande.

Nuevas versiones

Comenzando en la versión 11.0 o posterior CUCM, cualesquiera indeseados o certificado vencido que se borren del nodo actual también se borran del resto de los Nodos dentro del cluster.



La mejora fue incluida para dirigir estos defectos:

CSCto86463 - Los Certificados borrados reaparecen, incapaz de quitar los Certificados de CUCM

CSCus28550 - Mejora de administración CERT para borrar un certificado de todos los Nodos

Preguntas Frecuentes

Q. ¿Cuáles son el tipo de Certificados incluidos en esta mejora?

A. Para el administrador de las Comunicaciones unificadas de Cisco:

- Tomcat-confianza
- CallManager-confianza
- Teléfono-SAST-confianza

Para el administrador de las Comunicaciones unificadas de Cisco IM y presencia:

- Tomcat-confianza

Q. ¿Qué sucede en la parte para esta mejora?

A. Tan pronto como un certificado se borre en de los Nodos CUCM:

- El certificado se borra del nodo local
- El evento de la plataforma acciona la cancelacíon del mismo certificado al resto de los Nodos.

Verificación

Una vez que un certificado se borra vía la página de administración OS en un nodo, inicie sesión a otros Nodos y marque si el certificado está presente o no. Si un certificado borrado no se borra de todos los Nodos, marque los registros generados con el caso de la cancelacíon del certificado.

- Registros del sistema
- Registros de CertMgr de la plataforma IPT

En un escenario de trabajo común, éstos son los registros previstos.

Registros del sistema

el Plataforma-evento se considera en otros Nodos (con excepción del nodo donde la cancelacíon del certificado fue iniciada). En este ejemplo, un certificado de la Tomcat-confianza nombrado CUCMSUB1.pem fue borrado del editor, diplaying esto 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 de CertMgr de la plataforma IPT

En los registros de CertMgr, los expedientes confirman que el certificado está en la cola para la cancelacíon 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 - Certificate 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 accionado para la cancelacíon del certificado puede ser considerado 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")
```

De los registros de CertMgr, las entradas confirman que el certificado está borrado del SISTEMA DE FICHEROS (certificado con las Extensiones PEM o del 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 cancelacíon del certificado todavía no se refleja al resto de los Nodos en un cluster o los registros muestran los errores, proceda a abrir un caso TAC con el equipo CUCM.