

在安全证书管理CUCM 11.x的增强

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[证书管理](#)

[旧有版本](#)

[新版本](#)

[常见问题](#)

[验证](#)

[系统日志](#)

[IPT平台CertMgr日志](#)

简介

本文描述在版本11.x (CUCM)证书管理方面做的前进实现的Cisco Unified Communications Manager的。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM

使用的组件

本文档中的信息基于以下软件版本：

- CUCM版本11.5.1.10000-6

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

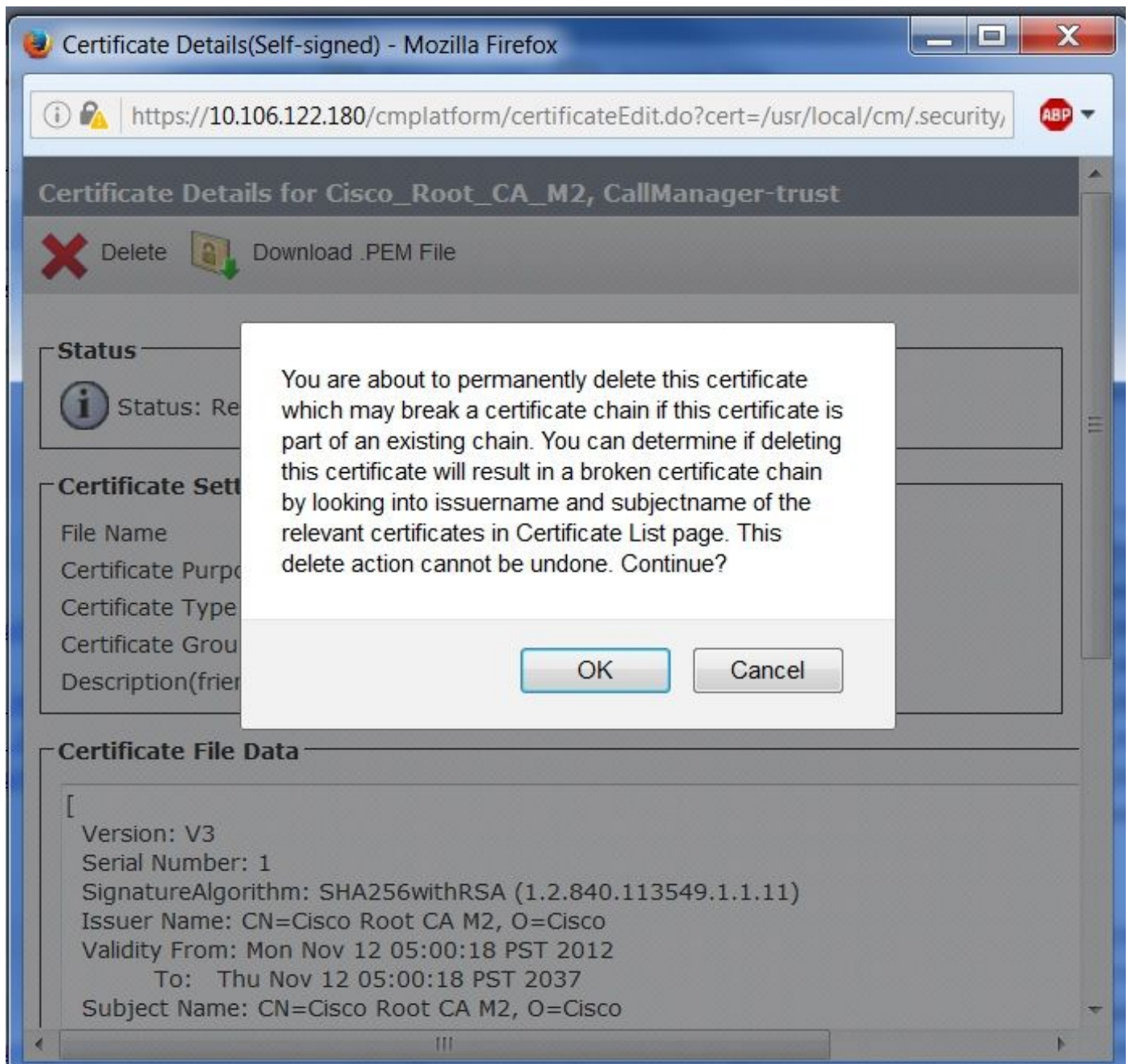
背景信息

CUCM证书管理帮助统一通信或安全管理员效率更高采取advantagesmanage证书。被做的增强的优点包括减小的时光在删除不需要期间过期的证书在CUCM和IM&Presence。

证书管理

旧有版本

在CUCM版本11之前，如果证书删除，此消息出现。



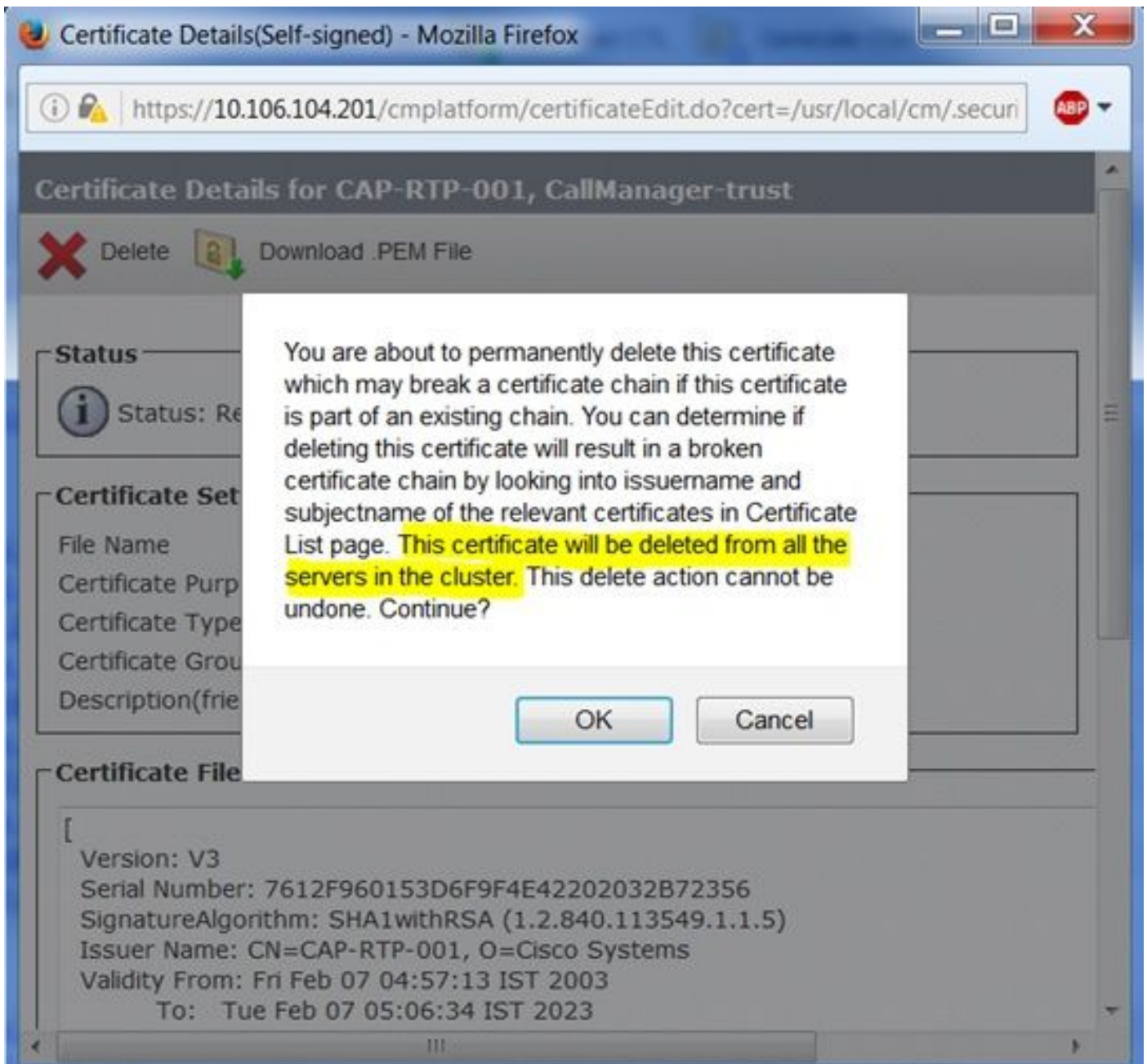
证书从删除操作被发起的节点仅被删除。

如果同一证书在其他节点没有删除，删除的证书被增加在最初删除的节点的上一步。这归结于呼叫 Certificate 修改提示的证书监控服务。作为在CUCM更旧的版本的最佳实践，证书修改提示服务在证书删除前的所有CUCM节点被终止。在更旧的版本的另一个缺点是需求登陆到每个节点的OS管理部分为了删除单个不需要或过期的证书，变得繁琐和费时特别是为一大集群。

新版本

开始在CUCM版本11.0或以上，从当前节点删除的所有不需要或过期的证书从在集群内的其他节点

也删除。



增强包括寻址这些缺陷：

[CSCto86463](#) -删除的证书再现，无法从CUCM删除证书

[CSCus28550](#) -删除从所有节点的一证书的Cert管理的增进

常见问题

Q. 什么是在此增强包括的证书种类？

A. 对于Cisco Unified Communications Manager：

- Tomcat托拉斯
- CallManager托拉斯
- 电话SAST托拉斯

Cisco Unified Communications Manager IM &在线状态：

- Tomcat托拉斯

Q. 什么在此增强的后端发生？

A. 当证书在任何一个CUCM节点中删除：

- 证书从本地节点删除
- 平台事件触发同一证书的删除对其他节点。

验证

一旦证书通过在节点的OS管理页面删除，请登陆对其他节点并且检查证书是否存在。如果一删除的证书没有从所有节点删除，请检查通过证书删除实例生成的日志。

- [系统日志](#)
- IPT平台CertMgr日志

在一个普遍的工作的方案中，这些是预计日志。

系统日志

平台事件在其他节点被看到(除证书删除启动)的节点之外。在本例中，名为CUCMSUB1.pem的Tomcat托拉斯证书从发行商删除， displaying此在用户的Syslog。

```
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)
```

IPT平台CertMgr日志

在CertMgr日志，记录确认证书在删除的队列从数据库条目。

```
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) -
为证书的删除触发的sql命令在CertMgr日志能被看到。
```

```
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")
```

从CertMgr日志，条目确认证书从文件系统(与pem或der扩展的证书删除)。

```
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
```

如果证书删除仍然没有反射对节点的其余在集群的或日志显示错误，请继续开有CUCM团队的TAC案例。