CUCM证书重新生成/更新过程

目录

简介

本文提供一个推荐，逐步程序重新生成用于Cisco Unified Communications Manager (CUCM)版本的证书8.x和以后。默认情况下安全以(ITL为特色)，并且Mixed-Mode (CTL)是也被覆盖为了避免所有不期望的中断。例如，如何避免不接受配置更改或固件的电话注册问题或电话。

> **警告：**总是推荐完成在维护窗口的证书重新生成。

概述

本文讨论这些服务的证书重新生成进程：

- CallManager
- CAPF (认证机关代理功能)
- IPsec
- Tomcat
- TV (托拉斯验证服务)
- ITLRecovery (仅CUCM 10.X和以后)
- 电话VPN托拉斯

- 电话sast托拉斯
- 电话托拉斯
- 电话CTL托拉斯

并且这些电话证书：

- LSCs (局部重要的证书)
- MICs (制造商已安装证书)

使用的组件

在本文和屏幕画面显示的所有输出根据CUCM版本9.1(2)SU2a，然而提交步骤可以与CUCM版本8.x一起使用和以后。是版本特定的差异在适当的部分被提及。

本文档中的信息根据在开始与原始的实验室环境的设备。如果您的网络实际，请确保您了解所有命令和执行的操作潜在影响。

什么时候重新生成证书

在CUCM的大多数证书，在新安装是发出后的自签名证书，默认情况下，用于五年。注意不可能当前修改五年时间范围是时间一个短程在CUCM的。然而， Certificate Authority (CA)能发行接近所有范围的证书时间。

也有被预先输入并且有一个更加长的有效性周期的一些信任证书(例如CAPF托拉斯和CallManager托拉斯)。例如， “制造CA的思科”证书在CUCM信任存储提供给特定功能，并且不会超时直到年2029年。

证书，在他们超时前，应该重新生成。当证书将超时您将收到在RTMT (系统日志浏览器)的警告若被设定，并且与通知的一电子邮件将被发送。

选派"CUCM01.der"证书证书到期通知的示例在“5月19日14:46"在信任存储“Tomcat托拉斯的"服务器CUCM02显示此处的星期一将超时：

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
SyslogSeverityMatchFound events generated:

SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent

ClusterID :

NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

如果服务证书(没有标志“的证书存储-信任”)已经超时重新生成他们是可能的。记住过期的证书也许有在您的CUCM功能的一影响，从属在簇配置。考虑事项在以下部分讨论。

由证书存储的服务影响

为系统的好功能是关键有在CUCM集群间更新的所有证书。如果您的证书是超时或无效他们也许极大影响系统的正常功能。您也许有潜在问题的列表，当其中任一特定证书无效或已到期显示此处。影响也许有所不同从属在您的系统设置。

CallManager.pem

- 已加密/验证电话不注册。
- TFTP没有委托(电话不接受签字的配置文件和ITL文件)。
- 电话服务也许受影响。
- 安全会话初始化协议(SIP)中继或媒体资源(会议桥，媒介终接点(MTP)， Xcoders，等等)不会注册也不会工作。
- AXL请求发生故障。

Tomcat.pem

- 电话不能访问在CUCM节点主机的HTTPs服务，例如公司目录。
- CUCM的Web GUI问题，例如无法访问从其他节点的服务页在集群。
- Extension Mobility或Extension Mobility交叉团星问题。

CAPF.pem

- 电话不为电话VPN， 802.1x或者电话代理验证。
- 不能发行电话的LSC证书。
- 已加密配置文件不工作。

IPSec.pem

- 灾难恢复系统(DR) /Disaster恢复框架(DRF)也许不正常运行。
- 对网关(GW)的IPSec隧道对其他CUCM集群不工作。

TV (托拉斯验证服务)

- 电话不能验证HTTPS服务。电话不能验证配置文件(这在CUCM能影响接近一切)。

电话VPN托拉斯

- 因为VPN的HTTPS URL不可能验证，电话VPN不会工作。

  注意：如果这不存在请勿担心。这仅是为特定配置。

电话sast托拉斯

- 上一个CTL/eTokens不能更新或修改CTL。

  注意：如果这不存在请勿担心。这仅是为特定配置。

电话托拉斯和电话CTL托拉斯

- 与Unity的虚拟语音邮件或Unity Connection不会工作。

  注意：如果这不存在请勿担心。这仅是为特定配置。

LSCs和MICs

- 电话不注册，电话不验证给VPN、电话代理或者802.1x打电话。

  注意：默认情况下MICs在多数电话型号。默认情况下LSCs由CAPF签字并且持续五年。软件客户端例如CIPC (Cisco IP Communicator)和Jabber不安排MIC安装。

创建DR备份

在您进行象这样前的所有重大更改推荐创建DR备份。CUCM DRF备份将备份在集群的所有证书。所有DR备份/恢复过程可以在思科“Cisco Unified Communications Manager的灾难恢复系统管理指南找到”。

> **警告：** 记住Cisco Bug ID CSCtn50405， CUCM DRF备份不备份证书。

确定团星是否在Mixed-Mode

为了确定是否运行CTL/Secure/Mixed模式集群，请选择**Cisco Unified CM管理>System >企业参数>团星安全模式(不安全0的==;混合模式1的==)**。

如果团星在Mixed-Mode

如果运行在Mixed-Mode的一CUCM集群，这意味着CTL文件需要更新，在所有证书更改后。关于怎样的步骤执行此在思科的安全指南文档内。然而，请务必您有从Mixed-Mode功能的原始开始的至少一eToken，并且eToken密码知道。

> **注意**：(在ITL文件的情况下执行)， CTL的更新不自动地发生。它需要由管理员手工完成用CTL客户端或CLI命令。

在CUCM 10.X和以后您能放集群到在两种方式的Mixed-Mode ：

- CLI命令-，如果然后使用此方法您的CTL文件签字与发布服务器的CallManager.pem证书。

```
admin:show ctl
The checksum value of the CTL file:
0c05655de63fe2a042cf252d96c6d609(MD5)
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1156
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7 PUBLICKEY 140
```

```
8 SIGNATURE 128
9 CERTIFICATE 694 E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
A5 A3 8C 9C (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

- CTL客户端-，如果然后使用此方法您的CTL文件签字与其中一硬件eTokens。 `admin:show ctl`

```
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

注意： 您能移动在使用的方法之间与CUCM混合模式与Tokenless CTL。

从属在使用的方法巩固您的集群，需要使用一个适当的CTL更新步骤。请重新运行CTL客户端或输入从CLI的**使用情况ctl更新CTLfile**命令。

默认情况下验证安全在团星

ITL问题避免是重要，因为ITL问题能造成许多功能发生故障或电话将拒绝遵守对配置的所有更改。 ITL问题可以避免用这两个方式。

使用“准备回退的团星对前8.0"功能

此功能“成为空白”您的在所有服务器的ITL，因此电话将委托所有TFTP server。电话服务(例如，Extension Mobility)不会工作，当此参数设置对真。然而，用户能继续做和收到基本电话。

注意： 对此参数的一更改导致所有电话RESET。

一旦此功能设置，所有TFTP服务器需要重新启动(为了供应新的ITL)和所有电话需要重置为了迫使他们请求新的“空白” ITL。一旦证书更改完成，并且所有必要的服务被重新了启动，此功能可以设置回到“错误”， TFTP服务重新启动的和电话重置(因此电话能得到有效ITL文件)。然后所有功能将继续运作，他们以前。

再生证书按特定顺序

此步骤提供一TFTP server有效/更新是可用的从委托TFTP server的ITL文件。

1. 终止在主要的TFTP server的TFTP服务。
2. 做变动在主要的TFTP服务器的证书(当必要时)。
3. 重置电话(为了从附属TFTP server获得一个新的ITL文件) -从属在哪证书被重新生成，这也许自动地发生。
4. 一旦电话返回，请开始主要的TFTP服务器的TFTP服务。
5. 做证书变动在附属TFTP server。
6. 重置电话(为了从主要的TFTP server获得一个新的ITL文件)。

警告：同时请勿编辑在两个TFTP服务器的证书。这给电话号码TFTP server委托并且要求本地管理员从所有电话手工删除ITL。

删除和再生证书在CUCM

仅服务证书(没有标志“的证书存储-信任”)可以被重新生成。证书在信任存储(标志“的证书存储-信任”)需要删除，因为他们不可能被重新生成。

警告：注意Cisco Bug ID CSCut58407 -，当CAPF/CallManager/电视托拉斯删除时，设备不应该重新启动。

在所有证书修改以后，各自服务需要被重新启动承担更改。这在被覆盖在Certificates部分以后重新生成/删除。

警告： 注意Cisco Bug ID CSCto86463 -删除的证书再现，无法从CUCM删除证书。这是删除的证书继续在删除以后再现的问题。跟随在缺陷的应急方案。

通过CLI重新生成证书

警告：证书的重新生成触发ITL文件的一次自动更新在集群内的，触发簇范围软电话重置允许电话触发他们的本地ITL更新。这集中于CAPF和CallManager证书重新生成，但是能发生在CUCM内的其他证书存储，例如Tomcat。

再生CAPF

在重新生成， CAPF证书自动地上传对CAPF托拉斯和CallManager托拉斯。并且， CAPF总是有一个唯一主题名称报头，因而以前使用的CAPF证书将保留并且使用验证。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015
```

```
[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

注意： 如果CAPF证书获得超时，使用LSC的电话不能注册到CUCM，因为CUCM拒绝他们的证书。然而，您能仍然生成电话的一新的LSC有新的CAPF证书的。当您重新启动它下载配置的电话时然后与CAPF联系为了更新LSC。在LSC更新后，电话注册作为它请应该。这工作，只要一新的CAPF证书在下载的ITL文件和电话并且委托签署它的证书(callmanager.pem)。

再生CallManager

在重新生成， CallManager自动地上传对CallManager托拉斯。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

再生IPsec

在重新生成， IPsec证书自动地上传对ipsec托拉斯。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015
```

```
[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

再生Tomcat

在重新生成， Tomcat证书自动地上传对Tomcat托拉斯。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

再生TV

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
```

```
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

所期待的是

当您通过CLI时重新生成证书，您请求验证此更改。键入**是**并且按回车。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

通过CLI删除证书

删除CAPF托拉斯证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
```

```
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
```
This etoken was used to sign the CTL file.

删除CallManager托拉斯证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

删除ipsec托拉斯证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

删除Tomcat托拉斯证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)
```

```
Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

删除电视托拉斯证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

通过Web GUI重新生成证书

重新生成CAPF

在重新生成， CAPF证书自动地上传对CAPF托拉斯和CallManager托拉斯。并且， CAPF证书总是有一个唯一主题名称报头，因而以前使用的CAPF证书保留并且使用验证。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015
```

```
[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

再生CallManager

在重新生成， CAPF证书自动地上传对CallManager托拉斯。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

再生IPsec

在重新生成， IPsec证书自动地上传对ipsec托拉斯。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
```

```
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

再生Tomcat

在重新生成，Tomcat证书自动地上传对Tomcat托拉斯。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

再生TV

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
```

```
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

删除证书通过Web GUI

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

在证书以后重新生成/删除

在您删除或重新生成从证书存储后的一证书，各自服务需要被重新启动为了承担更改。

存储	重新启动的服务	如何(C == CLI;W == Web GUI)
Tomcat	Tomcat	C ：utils service restart Cisco Tomcat G ： Cisco Unified维护性> Tools > Co Center -功能Services> (请选择服务器 择"Cisco CallManager" >重新启动
CallManager	CallManager;TFTP	并且 G ： Cisco Unified维护性> Tools > C Center -功能Services> (请选择服务器 择"Cisco Tftp" >重新启动
CAPF	CAPF (在只有发行商)	G ： Cisco Unified维护性> Tools > C Center -功能Services> (请选择服务器 择"Cisco Certificate Authority Proxy Function" >重新启动
TV	委托验证服务(在各自的服务器)	G ：Cisco Unified维护性> Tools > Co Center -网络服务> (请选择服务器) >选 "Cisco Trust Verification Service" >重 动
ipsec	思科DRF本地(在所有节点);思科DRF万事达(在发行商)	C ：使用情况服务重新启动思科DRF本 并且 C ：使用情况服务重新启动思科DRF万

在电话的安装/更新LSC

如果CAPF证书被重新生成了，则所有电话的LSC证书在集群需要更新与新的CAPF证书签字的LSC。

1. 选择**CUCM维护性>服务激活**。激活思科CTL供应商和思科认证机关代理功能在发布服务器。
2. 从CUCM Ccmadmin，请选择**Device > Phone**。选择您要设置LSC的IP电话。
3. 在证书操作下的设备配置页，请选择**由空字符串安装/升级>**。
4. 保存在Ccmadmin的电话配置并且选择**运用设置**。

如果电话有与LSC的安装的困难，请完成在电话的这些操作：

当电话重置时，去实体电话并且选择**设置> (6)安全配置> (4) LSC > ** #** (此操作取消锁定GUI并且允许我们继续到下一步) **>更新**(更新不会可视，直到您执行上一步) **>提交**。

请勿分配任何证书到电话，除非它是一个无线电话(7921/25)。无线电话使用第三方证书权限(CA)为了验证。

结论

如果遇到问题或需要与此步骤的援助，请与协助的Cisco技术支持中心(TAC)联系。在这种情况下，请保持您的DRF备份联机，因为将用于作为最后一招为了恢复服务，如果TAC无法通过其他方法如此执行。