重新生成CUCM证书

目录

简介

本文档介绍如何重新生成在Cisco Unified Communications Manager(CUCM)版本8.x及更高版本中使用的证书。

背景信息

本文档还将介绍根据默认安全(SBD)功能启用的身份信任列表(ITL)和混合模式环境的证书信任列表(CTL)，以避免任何意外断电。例如，如何避免电话注册问题或不接受配置更改或固件的电话。

> **注意**：始终建议在维护窗口中完成证书重新生成。

先决条件

要求

Cisco 建议您了解以下主题：

- CallManager
- CAPF（思科证书颁发机构代理功能)
- IPsec
- Tomcat
- TVS（信任验证服务）
- ITLRecovery（仅适用于 CUCM 10.X 及更高版本）
- phone-vpn-trust
- phone-sast-trust
- phone-trust
- phone-ctl-trust
- LSC（本地重要证书）
- MIC（制造商安装的证书）

使用的组件

本文档中的信息基于以下软件版本：

- CUCM版本9.1(2)SU2a，
- CUCM版本8.x及更高版本

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

何时重新生成证书

在 CUCM 中，全新安装后使用的大多数证书都是自签名证书，默认情况下颁发期限为五年。请注意，在CUCM上，当前无法将五年时间范围修改为更短的时间范围。但是，证书颁发机构 (CA) 几乎可以颁发任何时间范围的证书。

CUCM中的证书分为两个角色：

- 服务证书：可以重新生成这些证书，但不会使用单词 — trust进行标记。每个节点都有自己的服务证书，这意味着每个发布和子节点都有CallManager、Tomcat、IPsec、TVS和CAPF证书。
- 信任证书：无法重新生成这些证书，并使用单词 — trust进行标记。这些证书可以是服务证书、默认安装的证书或来自其他服务器的证书的副本。

还有一些预先加载并且有效期更长的可信证书（例如 CAPF-trust 和 CallManager-trust）。例如，思科制造CA证书在CUCM信任库上针对特定功能提供，直到2029年才会到期。

证书必须在到期之前重新生成。当证书即将到期时，您将在RTMT（系统日志查看器）中收到警告，如果配置了这些警告，将会发送一封包含通知的电子邮件。

下面显示了一个证书过期通知的示例，该通知详细说明了信任存储的tomcat-trust上服务器CUCM02上的CUCM01.der证书在5月19日（星期一）14:46到期：

```
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
```

请记住，过期证书可能会影响您的CUCM功能，具体取决于集群的配置。下一部分将介绍相关注意事项。

证书库对服务的影响

对于系统的良好功能而言，跨CUCM集群更新所有证书至关重要。如果您的证书过期或无效，它们可能会严重影响系统的正常运行。此处显示当任何特定证书无效或过期时可能出现的潜在问题的列表。影响差异可能取决于您的系统设置。

CallManager.pem

- TFTP 不受信任（电话不接受签名的配置文件和/或 ITL 文件）。
- 电话服务可能会受到影响。
- 安全会话发起协议(SIP)中继或媒体资源(会议网桥、媒体终端点(MTP)、转码器等)不注册或工作。
- AXL 请求失败。

Tomcat.pem

- 电话不能访问 CUCM 节点上托管的 HTTP 服务，例如企业目录。
- CUCM 的 Web GUI 问题，例如无法从集群中的其他节点访问服务页面。
- 分机移动性或跨集群分机移动问题。
- 如果集成了UCCX(Unified Contact Center Express)，由于CCX 12.5的安全更改，因此需要在UCCX tomcat-trust存储中上传CUCM Tomcat证书（自签名）或Tomcat根和中间证书（用于CA签名），因为它会影响Finesse桌面登录

CAPF.pem

- 电话无法向电话 VPN、802.1x 或电话代理进行身份验证。
- 无法为电话颁发 LSC 证书。
- 加密的配置文件无法工作。

IPSec.pem

- 灾难恢复系统(DRS)/灾难恢复框架(DRF)无法正常工作。
- 与通往其他 CUCM 集群的网关 (GW) 之间的 IPsec 隧道无法工作。

信任验证服务(TVS)

电话无法对 HTTPS 服务进行身份验证。电话无法对配置文件进行身份验证（这几乎会对 CUCM 上的一切造成影响）。

phone-vpn-trust

电话VPN不起作用，因为无法对VPN的HTTPS URL进行身份验证。

> **注**：如果不存在此项，请不要担心。这种情况仅适用于特定配置。

phone-sast-trust

以前的CTL/eTokens无法更新或修改CTL。

> **注**：如果不存在此项，请不要担心。这种情况仅适用于特定配置。

Phone-trust 和 phone-ctl-trust

带有Unity或Unity Connection的可视语音邮件不起作用。

> **注**：如果不存在此项，请不要担心。这种情况仅适用于特定配置。

，

LSC 和 MIC

电话未注册。电话不对电话VPN、电话代理或802.1x进行身份验证。

> **注意**：默认情况下，MIC在大多数电话型号上。LSC 则默认由 CAPF 签名，有效期为五年。CIPC（思科 IP Communicator）和 Jabber 等软件客户端未安装 MIC。

创建 DRS 备份

建议您在执行任何此类重大更改之前先创建一份 DRS 备份。CUCM DRF备份文件备份集群中的所有证书。所有DRS备份/恢复过程均可在《Cisco Unified Communications Manager的Cisco Disaster Recovery System Administration Guide》中找到。

> **注意**:请记住Cisco Bug ID CSCtn50405,CUCM DRF Backup不会备份证书。

确定混合模式

要确定是否运行CTL/安全/混合模式集群，请选择**Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode(0 == Non-Secure; 1 == Mixed Mode)**。

如果集群处于混合模式

如果您运行的 CUCM 集群处于混合模式，这意味着需要在所有证书更改后再更新 CTL 文件。思科

的安全指南文档中介绍了有关如何执行此操作的程序。但是，请确保混合模式功能的原始启动中至少有一个eToken，并且已知eToken密码。

> **注**:CTL的更新不会自动发生（与ITL文件的情况一样）。而是需要由管理员使用 CTL 客户端或 CLI 命令手动完成。

在 CUCM 10.X 及更高版本中，您可以通过两种方式将集群设置为混合模式：

- CLI 命令 - 如果使用此方法，则会使用发布方服务器的 CallManager.pem 证书签署 CTL 文件。

```
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 — 如果使用此方法，则使用其中一个硬件eTokens对CTL文件进行签名。

```
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：您可以在使用无令牌的CTL的CUCM混合模式使用的方法之间移动。

根据您用于保护集群安全的方法，需要使用相应的 CTL 更新程序。重新运行 CTL 客户端，或从 CLI 输入 **utils ctl update CTLfile 命令。**

验证集群的默认安全设置

避免ITL问题非常重要，因为它可能会导致许多功能失败或电话拒绝遵守任何配置更改。 可以通过以下两种方法避免 ITL 问题。

利用“准备集群以回滚到8.0之前的版本”功能

此功能会清空ITL文件中的ITL条目，因此电话信任任何TFTP服务器。 当此参数设置为True时，任何来自/发送到电话的HTTPS请求都将失败。建议不要启用此功能，因为它会限制电话功能，如分机移动、公司目录等。 但是，您可以拨打和接听基本电话。

注：此功能不适用于混合模式集群，因为此参数仅清除ITL而不是CTL条目。

注：此功能仅防止ITL问题，但不会修复。如果问题已在电话中，则不会删除国际交易日志，而需要手动删除国际交易日志。

注意：更改此参数将导致重置所有电话。

设置此功能后，需要重新启动所有TFTP服务器（以提供新的ITL），并需要重置所有电话以强制它们请求新的空白ITL。完成证书更改并重新启动所有必要的服务后，可将此功能重新设置为 **False**，重新启动TFTP服务，并重置电话（以便电话获取有效的ITL文件）。然后，所有功能将继续像以前一样工作。

按特定顺序重新生成证书

以下程序可以从受信任的可用 TFTP 服务器为另一台 TFTP 服务器提供有效的/更新后的 ITL 文件。

1. 在主 TFTP 服务器上停止 TFTP 服务。
2. 更改主TFTP服务器的证书（根据需要）。
3. 重置电话（以便从辅助TFTP服务器获取新的ITL文件） — 根据重新生成的证书，可以自动执行此操作。
4. 电话返回后，启动主 TFTP 服务器的 TFTP 服务。
5. 在辅助 TFTP 服务器上进行证书更改。
6. 重置电话（以便从主 TFTP 服务器获取新的 ITL 文件）。

注意：不要同时编辑两个TFTP服务器上的证书。这会让电话没有可信任的 TFTP 服务器，而需要本地管理员从所有电话上手动删除 ITL。

一次重新生成一种类型的证书

这是最常用的程序，也是推荐的程序，因为它可防止电话失去信任。有关这一过程的介绍，请参见

Cisco Unified Communications Manager(CUCM)证书重新生成过程指南。

在 CUCM 中删除并重新生成证书

只能重新生成服务证书（未使用 — trust标记的证书存储）。需要删除信任库中的证书（标记为 — trust的证书库），因为它们无法重新生成。

> **注意**：请注意Cisco Bug ID CSCut58407 — 删除CAPF/CallManager/TVS-trust时，设备无法重新启动。

完成所有证书修改后，需要重新启动各自的服务以接受更改。重新生成/删除证书后部分将对此进行介绍。

> **注意**：请注意Cisco Bug ID CSCto86463 — 删除的证书重新出现，无法从CUCM中删除证书。在此问题中，已删除的证书不断在删除后重新出现。请按照缺陷解决方法操作。

通过 CLI 重新生成证书

> **注意**：重新生成证书会触发集群内ITL文件的自动更新，从而触发集群范围的软件电话重置，使电话能够触发本地ITL的更新。这主要用于CAPF和CallManager证书重新生成，但可能发生在CUCM内的其他证书存储中，例如Tomcat。

重新生成CAPF：重新生成时，CAPF证书会自动将自身上传到CAPF-trust和CallManager-trust。此外，CAPF始终具有唯一的Subject Name报头，因此先前使用的CAPF证书将被保留并用于身份验证。

```
set cert regen CAPF
```

> **注意**：如果CAPF证书过期，使用LSC的电话无法注册到CUCM，因为CUCM拒绝其证书。不过，您仍然可以使用新的 CAPF 证书为电话生成新的 LSC。当您重新启动电话时，它会下载配置，然后联系CAPF以更新LSC。更新LSC后，电话会尽可能注册。只要新的 CAPF 证书在 ITL 文件中并且电话已下载和信任签署它的证书 (callmanager.pem)，此方法就可以奏效。

重新生成CallManager：重新生成时，CallManager会自动将自身上传到CallManager-trust。

```
set cert regen CallManager
```

重新生成IPsec：在重新生成时，IPsec证书会自动将自身上传到ipsec-trust。

```
set cert regen ipsec
```

重新生成Tomcat：重新生成时，Tomcat证书会自动将自身上传到tomcat-trust。

```
set cert regen tomcat
```
重新生成TVS:

```
set cert regen TVS
```
预计发生的情况

通过 CLI 重新生成证书时，系统会要求您验证此更改。输入**yes**，然后选择**Enter**。

```
admin:set cert regen CAPF

WARNING: This operation will overwrite any CA signed certificate previously imported
for CAPF

Proceed with regeneration (yes|no)? yes

Successfully Regenerated Certificate for CAPF.

You must restart services related to CAPF for the regenerated certificates to become active.
```
通过 CLI 删除证书

删除 CAPF-trust 证书

```
set cert delete CAPF <name of certificate>.pem
```
删除 CallManager-trust 证书

```
set cert delete CallManager <name of certificate>.pem
```
删除 ipsec-trust 证书

```
set cert delete ipsec <name of certificate>.pem
```
删除 Tomcat-trust 证书

```
set cert delete tomcat <name of certificate>.pem
```
删除 TVS-trust 证书

```
set cert delete TVS <name of certificate>.pem
```
通过 Web GUI 重新生成证书

重新生成CAPF:

CAPF 证书在重新生成后会自动将自身上传到 CAPF-trust 和 CallManager-trust。此外，CAPF 证书始终有一个唯一的“使用者名称”标题，因此以前使用的 CAPF 证书将保留并用于身份验证。

```
OS Admin > Security > Certificate Management > Find > Click CAPF certificate > Regenerate
```
重新生成CallManager:

在重新生成时，CallManager证书会自动将自身上传到CallManager-trust。

```
OS Admin > Security > Certificate Management > Find > Click CallManager certificate > Regenerate
```

重新生成IPsec:

Ipsec 证书在重新生成后会自动将自身上传到 ipsec-trust。

```
OS Admin > Security > Certificate Management > Find > Click ipsec certificate > Regenerate
```

重新生成Tomcat:

Tomcat 证书在重新生成后会自动将自身上传到 tomcat-trust。

```
OS Admin > Security > Certificate Management > Find > Click tomcat certificate > Regenerate
```

重新生成TVS:

```
OS Admin > Security > Certificate Management > Find > Click TVS certificate > Regenerate
```

通过 Web GUI 删除证书

```
OS Admin > Security > Certificate Management > Find > Click X certificate within the
'-trust' store > Remove/Delete
```

重新生成/删除证书后

在证书库中删除或重新生成证书后，需要重新启动各自的服务以接受更改。

证书库	要重新启动的服务	如何
Tomcat	Tomcat	CLI:utils service restart Cisco Tomcat 从CCX环境中执行所需的步骤（如果适用） https://www.cisco.com/c/en/us/support/docs/customer- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/
CallManager	CallManager;TFTP;CTI管理器	Web Gui：导航到**Cisco Unified Serviceability > Tools >**
CAPF	CAPF（仅在发布方服务器上）	Web Gui：导航到**Cisco Unified Serviceability > Tools >** Web Gui：导航至**Cisco Unified Serviceability > Tools >**
TVS	信任验证服务（在各自的服务器上）	Web Gui：导航到**Cisco Unified Serviceability > Tools >**
ipsec	Cisco DRF Local（在所有节点上）；Cisco DRF Primary（在发布服务器上）	CLI: utils service **restart Cisco DRF Local** CLI:utils服**务重新启动Cisco DRF Primary**

如何识别不再使用的信任证书

在删除信任存储中的过期证书之前，必须确定使用的证书和未使用的证书。请记住以下要点，以选择必须删除的证书：

- 大多数 — trust证书都是已使用的服务证书的副本。建议首先在所有节点中重新生成所有过期的服务证书，CUCM会自动更新 — trust副本。

- 不再使用tomcat-trust VeriSign_Class_3_Secure_Server_CA_-_G3。如果使用Smart Call Home功能，请按照下一指南上传新证书：https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/smart-call-home/215210-troubleshooting-certficate-exipry-alert.html

- 制造信任证书在安装期间预加载到任何CUCM，默认情况下，CUCM用于信任任何思科IP电话。建议不要删除以下证书：
  CAP-RTP-001

  CAP-RTP-002

  思科根CA 2048

  思科根CA M2

  ACT2_SUDI_CA

  Cisco_Manufacturing_CA

  Cisco_Manufacturing_CA_SHA2

- 如果更改了域或主机名，则具有旧域或主机名的旧证书将列为“信任”。如果这些主机名和域不再使用，则这些证书将不被使用并且可以删除。

- 如果证书的公用名来自其他服务器（非CUCM集群），请验证来自其他服务器的证书是否有效。由于CUCM无法重新生成证书，这必须在其他服务器上完成，然后将证书作为 — trust导入CUCM。

通过电话安装/更新 LSC

如果已重新生成 CAPF 证书，则需要以新 CAPF 证书签名的 LSC 来更新集群中所有电话的 LSC 证书。

1. 导航到**CUCM Serviceability > Service Activation**。在发布方服务器上，激活思科 CTL 提供程序和思科证书颁发机构代理功能。

2. 在**CUCM CCMAdmin**下，导航到**设备>电话。**选择要在其中调配 LSC 的 IP 电话。

3. 在**证书操作**下的“设备配置”(Device configuration)页面中，导航到**安装/升级(Install/Upgrade)>“按空字符串”(By Null String)**。

4. 在 CCMAdmin 中保存电话配置，然后选择**应用配置。**

如果电话安装 LSC 时遇到问题，请在电话上完成以下操作：

当电话重置时，在物理电话下导航到**Settings >(6)Security Configuration >(4)LSC > **#**（此操作将解锁GUI并允许我们继续下一步）> Update**（在您执行上一步之前更新不可见）。现在，单击**Submit。**

请勿将任何证书分配给电话，除非它是无线电话 (7921/25)。为了对自身进行身份验证，无线电话使用第三方证书颁发机构 (CA)。

其他证书的续订流程

Cisco Unified Communications Manager(CUCM)的证书重新生成过程：本指南介绍按类型重新生成证书的流程，这是最常用的推荐流程。

CUCM 12.x及更高版本上ITLRecovery的证书重新生成过程：本指南介绍在12.x CUCM集群上重新生成ITLRecovery证书的过程。

CUCM CA-Signed Certificates的重新生成：本指南介绍CUCM中CA签名证书的流程以及上传证书时显示的最常见错误。

使用CA签名的多服务器主体备用名进行统一通信集群设置配置示例：本指南提供了Tomcat多san证书再生的示例。

重新生成Unified Communications Manager IM & Presence Service自签名证书：本指南提供重新生成过程以及针对IM&P节点重新启动的服务。

UCCX解决方案证书管理指南：该指南提供了UCCX中证书的集成要求以及重新生成证书的过程。

Expressway C和E的再生过程在以下视频中描述：

将服务器证书安装到Expressway

为MRA/群集Expressway生成CSR

如何配置Expressway-C和Expressway-E之间的证书信任

结论

倘若您遇到问题或需要有关此程序的帮助，请联系思科技术支持中心 (TAC) 寻求帮助。在这种情况下，请保持DRF备份可用，因为它被用作最后手段，以便在TAC无法通过其他方法恢复服务时恢复服务。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。