在Unified Communications Manager重新生成证书

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 安装实时监控工具(RTMT)
- 使用RTMT监控终端
- 确定集群安全模式
  - ITL和CTL
- 证书存储区的影响
  - CallManager.pem/CallManager-ECDSA.pem
  - Tomcat.pem/Tomcat-ECDSA.pem
  - CAPF.pem
  - IPSec.pem
  - 信任验证服务(TVS)

证书再生过程

- Tomcat证书
- IPSEC证书
- CAPF证书
- CallManager证书
- TVS证书
- ITR恢复证书

删除过期的信任证书

确认

故障排除

简介

本文档介绍在Unified Communications Manager中重新生成证书的步骤、效果以及成功的要求。

先决条件

要求

Cisco 建议您了解以下主题：

- 实时监控工具(RTMT)
- Cisco Unified Communications Manager安全指南
- CUCM证书
- 混合模式
- 证书颁发机构代理功能

使用的组件

思科建议您安装以下工具：

- 实时监控工具(RTMT)
- 基于Cisco Unified Communications Manager(CUCM)版本15.0+的信息。

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。

背景信息

本文档介绍如何在Cisco Unified Communications Manager(CUCM)15.X及更高版本中重新生成证书的分步过程。请参阅特定版本的安全指南。

不考虑生命周期终止的旧版本。

通信管理器(CUCM)12.0+版ITL通过ITR恢复证书签署。

Communications Manager(CUCM)版本12.0+在混合模式下使用ITLRecovery证书签署CTL。

混合模式是一种启用增强安全功能的模式，同时保持与传统端点或非安全端点的兼容性。

思科IP电话依赖CTL文件来了解集群安全模式（非安全或混合模式）。 CTL文件通过在Unified Communications Manager记录中包含Unified Communications Manager证书来跟踪集群安全模式。只有在集群处于混合模式后才会生成CTL。

ITL文件还包含集群安全模式指示。

身份证书：表示用户或设备（应用/服务器）身份的证书。 它包含颁发证书的证书颁发机构(CA)的

公钥，并且包含诸如证书所有者的详细信息和证书的有效期等信息。



ITL签名者比较

安装实时监控工具(RTMT)

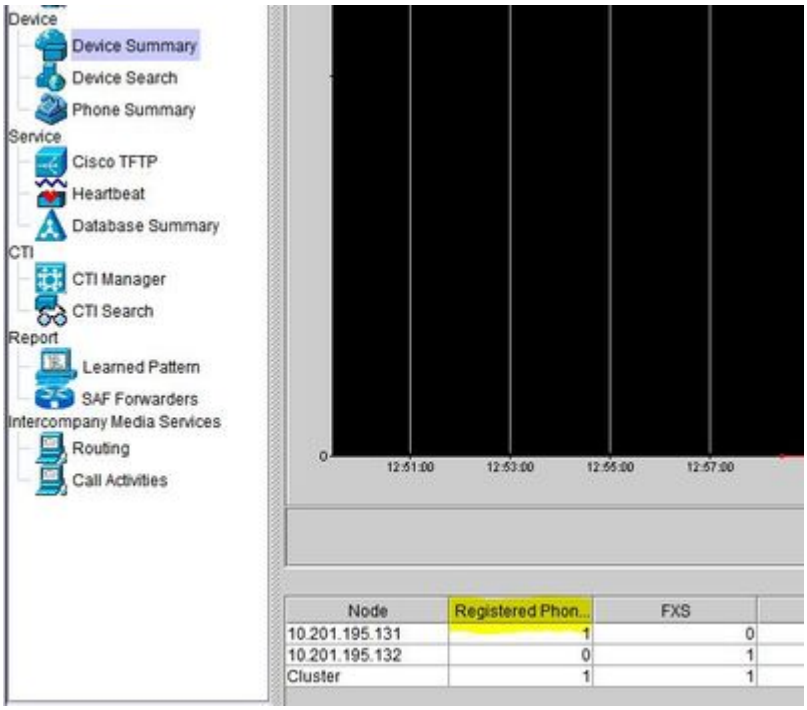
- 从Call Manager下载并安装RTMT工具。
  - 导航到Call Manager(CM)Administration:Application > Plugins > Find > Cisco Unified Real-Time Monitoring Tool - Windows > Download。安装启动。

使用RTMT监控终端

- 启动RTMT并输入IP地址或完全限定域名(FQDN)，然后输入username和password以访问工具：
  - 选择Voice/Video选项卡。
  - 选择设备摘要。
    - 此部分标识注册终端的总数以及每个节点的数量。
    - 在端点重置期间进行监控，以确保在重新生成下一个证书之前进行注册。

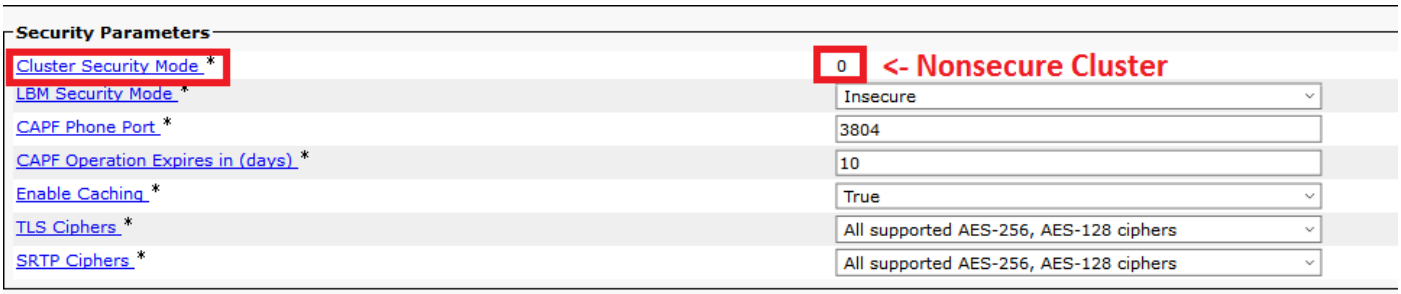
提示：某些证书的重新生成过程可能会影响终端。由于需要重新启动服务和重新启动电话，请在正常工作时间后考虑一个行动计划。强烈建议在此过程之前、期间和之后通过RTMT验证电话注册。只有在服务器上运行服务时，才需要重新启动服务。

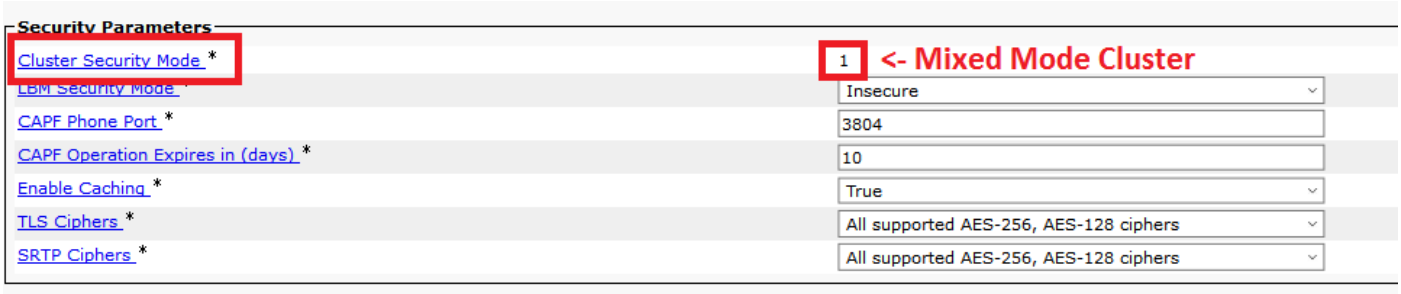
警告：当前具有ITL不匹配（错误ITL）的终端在此过程后可能会出现注册问题。对于具有不良ITL的设备，在重新生成过程完成后，在所有其他电话注册后，删除终端上的ITL是典型的最佳做法解决方案。请审查关于如何删除ITL/CTL（安全）证书的特定电话型号。



确定集群安全模式

- 导航到CM管理：System > Enterprise Parameters > Security Parameters > Cluster Security Mode。





ITL和CTL

- 初始信任列表(ITL)包含Call Manager TFTP、ITLRecovery和集群中所有TVS证书的证书角色

。如果服务正在运行，它还可以包含证书颁发机构代理功能(CAPF)。从12.0版开始，国际交易日志由ITLRecovery证书签署。您可以通过登录CLI并输入命令show itl来查看这一点。在12.0版之前，ITL由Call Manager证书签署。
- CTL包含在同一服务器、CAPF、ITLRecovery、TFTP服务器和自适应安全设备(ASA)防火墙上运行的系统管理员安全令牌(SAST)、Cisco CallManager和Cisco TFTP服务的条目。CTL中未引用TVS。如果服务Cisco CTL提供商正在运行，则向终端提供CTL。
- 从CUCM 14SU(3)开始，Cisco CTL提供商服务不再支持CTL令牌，无令牌是默认支持的方法。

证书存储区的影响

对于成功的系统功能而言，跨CUCM集群更新所有证书至关重要。如果证书过期或无效，可能会严重影响系统的正常功能。影响可能因系统设置而异。以下是适用于无效或过期的特定证书的服务：

CallManager.pem/CallManager-ECDSA.pem

- 经过加密/身份验证的电话无法注册。
- 简单文件传输协议(TFTP)不可信（电话不接受签名配置文件和/或ITL文件）。
- 电话服务可能会受到影响（自动注册、分机移动、跨集群分机移动）
- 安全会话发起协议(SIP)中继或媒体资源(SIP TLS、会议网桥、媒体终端点(MTP)、Xcoder等，Exp-C TLS遍历区域)不注册或工作。
- AXL 请求失败。

Tomcat.pem/Tomcat-ECDSA.pem

- 电话不能访问 CUCM 节点上托管的 HTTP 服务，例如企业目录。
- CUCM可能遇到各种Web问题，例如无法从集群中的其他节点访问服务页面。
- Extension Mobility(EM)或Extension Mobility Cross Cluster。
- 灾难恢复
- 单点登录(SSO)
- Expressway遍历区域关闭（启用TLS验证）。
- 如果集成了Unified Contact Center Express(UCCX)，由于CCX 12.5的安全更改，则需要在UCCX tomcat-trust存储中上传CUCM Tomcat证书（自签名）或Tomcat根证书和中间证书（用于CA签名），因为它会影响Finesse桌面登录。

CAPF.pem

- 此证书用于向终端（除在线和离线CAPF模式外）、电话VPN、802.1x、电话代理、应用用户CAPF配置文件颁发LSC。
- 从Unified Communications Manager版本11.5(1)SU1开始，由CAPF服务颁发的所有LSC证书

都使用SHA-256算法签名。
- CTI、JTAPI和TAPI的身份验证和加密设置。

IPSec.pem

- 灾难恢复系统(DRS)/灾难恢复框架(DRF)无法正常工作。
- 到网关(GW)或其他CUCM集群的IPsec隧道不起作用。

信任验证服务(TVS)

默认情况下，信任验证服务(TVS)是安全的主要组件。TVS使思科统一IP电话能够在建立HTTPS时对应用服务器（例如EM服务、目录和MIDlet）进行身份验证。

TVS提供以下功能：

- 可扩展性 — Cisco Unified IP电话资源不受要信任的证书数量的影响。
- 灵活性 — 信任证书的添加或删除会自动反映在系统中。
- 默认安全性 — 非媒体和信号安全功能是默认安装的一部分，不需要用户干预。
- 通过证书验证进行电话服务请求和验证。

ITLRecovery（信任验证服务）

- 8.X - 11.5恢复ITL不匹配的电话、电话迁移和EMCC到CUCM 12.0+。
- 12.0+用于SSO、EMCC和ITL/CTL的主签名者。
- 12.5+ ITL恢复仅由发布方生成

证书管理器ECDSA支持

在Unified Communications Manager版本11.0中，证书管理器支持生成自签名ECDSA证书和ECDSA证书签名请求(CSR)。 Unified Communications Manager的早期版本仅支持RSA证书。但是，从Unified Communications Manager版本11.0开始，CallManager-ECDSA证书已随现有RSA证书一起添加。

CallManager和CallManager-ECDSA证书共享通用证书信任库 — CallManager-Trust。Unified Communications Manager将这些证书上传到此信任库。

第三方CA签名身份证书

注意：第三方可能指内部证书颁发机构(CA)或外部来源，如Go-Daddy、Verisign等。身份证书是特定卷（Tomcat、Call Manager等）的服务器证书。 已签名的证书将至少具有对身份证书签名的根CA。大多数情况下为中间或倍数。证书路径可能如下所示：根 — 中间 — 身份证书。

1. 从发布者开始，然后由每个用户成功导航到集群中的每个服务器（在Web浏览器的单独选项卡中，除非您正在创建多SAN CSR）。导航到Cisco Unified OS Administration > Security > Certificate Management。
2. 选择生成 CSR。
3. 选择Certificate Purpose下拉列表，然后选择证书。
4. 选择Distribution类型。单服务器或多服务器(SAN)。
    - 多服务器(SAN)在SAN部分中包括所有CUCM和CUP节点。
5. 选择生成。
6. 下载CSR并提供给您的证书颁发机构。
7. 收到签名证书后，通过链式订单上传证书。
    - 将ROOT作为信任证书上传。
    - 将Intermediate作为信任证书上传。
    - 上传Signed Certificate作为证书类型。
    - 重新启动弹出窗口中确定的相应服务。

证书再生过程

注意：在重新生成证书之前，需要打开并注册所有终端。否则，未连接的电话需要删除ITL。

Tomcat证书

重新生成Tomcat和Tomcat-ECDSA的过程相同，包括服务重新启动。

识别是否正在使用第三方证书：

1. 导航到集群中的每台服务器（在Web浏览器的单独选项卡中），从发布者开始，然后由每个订阅者继续。导航到Cisco Unified OS Administration > Security > Certificate Management > Find。
    - 如果Tomcat指示系统生成的自签名证书，请从“说明”(Description)列中进行观察。如果Tomcat是第三方签名，请使用提供的链接，并在Tomcat重新生成后执行这些步骤。
    - 第三方签名证书，请参阅CUCM上传CCMAdmin Web GUI证书。
2. 选择查找以显示所有证书：
    - 选择Find Tomcat Pem。
    - 打开后，选择Regenerate并等待，直到您看到Success弹出窗口，然后关闭弹出窗口或返回并选择Find/List。

3. 继续处理每个后续用户，在步骤2中执行相同的过程并在集群中的所有用户上完成。
4. 在所有节点重新生成Tomcat证书后，在所有节点上重新启动tomcat服务。从发布服务器开始，继续订阅服务器。
    - 要重新启动Tomcat，您需要为每个节点打开CLI会话并执行命令utils service restart Cisco Tomcat。
    - 如果集群配置为SSO或使用OAuth，则必须重新启动带utils服务的SSOSP服务，然后重新启动Cisco SSOSP Tomcat。

```
admin:
admin:utils service restart Cisco Tomcat
 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

5.在CCX环境中使用以下步骤（如果适用）：

- 如果使用自签名证书，请将Tomcat证书从CUCM集群的所有节点上传到Unified CCX Tomcat信任库。
- 如果使用CA签名证书或专用CA签名证书，请将CUCM的根CA证书上传到Unified CCX Tomcat信任库。
- 按照CCX的证书重新生成文档所述重新启动服务器。

其他参考:

- UCCX解决方案证书管理指南
- Unified CCX运行状况检查实用程序

IPSEC证书

注意：CUCM/即时消息和在线状态(IM&P)在10.X版本之前，DRF主代理在CUCM发布方和IM&P发布方上运行。DRF本地服务分别在用户上运行。版本10.X及更高版本中，DRF主代理仅在CUCM发布服务器上运行，而CUCM订阅服务器和IM&P发布服务器和订阅服务器上运行DRF本地服务。

注意：灾难恢复系统在主代理和本地代理之间使用基于安全套接字层(SSL)的通信对CUCM集群节点之间的数据进行身份验证和加密。DRS将IPSec证书用于其公钥/私钥加密。请注意，如果从Certificate Management页面删除IPSEC truststore(hostname.pem)文件，则DRS不会按预期工作。如果手动删除IPSEC-trust文件，则必须确保将IPSEC证书上传到IPSEC trust-store。有关详细信息，请参阅《Cisco Unified Communications Manager安全指南》中的证书管理帮助页面。

1. 导航到集群中的每台服务器（在Web浏览器的单独选项卡中），从发布者开始，每个订阅者都成功完成。导航到Cisco Unified OS Administration > Security > Certificate Management > Find。
    - 选择IPSEC PEM证书。
    - 打开后，选择Regenerate并等待，直到您看到Success弹出窗口，然后关闭弹出窗口或返回并选择Find/List。
2. 继续使用后续用户；在步骤1中执行相同的步骤并在集群中的所有用户上完成。
3. 在所有节点重新生成IPSEC证书后，重新启动服务。
    - 导航到Publisher Cisco Unified Serviceability。
        1. Cisco Unified Serviceability > Tools > Control Center - Network Services。
        2. 选择Restart on Cisco DRF Master Service。
        3. 服务重新启动完成后，请在发布器上的Cisco DRF本地服务上选择Restart，然后继续使用订阅服务器，然后在Cisco DRF本地服务上选择Restart。
        4. 在所有节点上重新启动tomcat服务。从发布服务器开始，继续订阅服务器。
            - 要重新启动Tomcat，您需要为每个节点打开CLI会话并执行命令utils service restart Cisco Tomcat。

CAPF证书

注意：从CUCM 14开始，只能在发布服务器上找到CAPF证书。

警告：请确保您已确定集群是否处于混合模式，然后继续。请参阅识别集群安全模式部分。

1. 导航到Cisco Unified CM Administration > System > Enterprise Parameters。
    - 选中Security Parameters部分并验证Cluster Security Mode是否设置为0或1。如果值为0，则集群处于非安全模式。如果值为1，则集群处于混合模式，您需要在更新证书之后和重新启动服务之前更新CTL文件。
2. 导航到集群中的发布服务器导航到Cisco Unified OS Administration > Security > Certificate Management > Find。
    - 选择CAPF PEM证书。
    - 打开后，选择Regenerate并等待，直到您看到Success弹出窗口，然后关闭弹出窗口，或者返回并选择Find/List。
    - 如果集群处于混合模式或正在对802.1X使用CTL，则必须在继续之前更新CTL。
        - 登录到发布器的CLI并输入命令utils ctl update CTLFile。
        - 重置所有加密和经过身份验证的电话，使CTL文件更新生效。
3. 发布服务器重新生成CAPF证书后，重新启动服务。
    - 导航到发布者Cisco Unified Serviceability。
        1. Cisco Unified Serviceability > Tools > Control Center — 功能服务。
        2. 选择publisher，并在Cisco Certificate Authority Proxy Function Service上选择Restart（仅在处于活动状态时可用）。
4. 导航到Cisco Unified Serviceability > Tools > Control Center - Network Services。
    - 从发布服务器开始，然后继续订阅服务器，选择Restart on Cisco Trust Verification Service。

- 导航到Cisco Unified Serviceability > Tools > Control Center - Feature Services。
- 从发布服务器开始，然后继续订阅服务器，重新启动Cisco TFTP服务，其状态显示已启动。

5. 重新启动所有电话：
   - 选项1 - Cisco Unified CM Administration > System > Enterprise Parameters
   - 选择Reset，您将看到一个弹出窗口，其中显示语句“You are about to reset all devices in the system.此操作无法撤消。是否继续？”，选择OK，然后选择Reset。
     - 此方法重置Call Manager中的所有组件。
   - 选项2 - Cisco Unified CM管理 > 批量管理 > 电话 > 更新电话 > 查询
     - 搜索Device Name begins with SEP > Next > Reset Phones > Run Immediately。

电话现在已重置。通过RTMT工具监控其操作，以确保重置成功且设备重新注册到CUCM。等待电话注册完成，然后继续下一个证书。此电话注册过程可能需要一些时间。请注意，在重新生成过程之前具有不良ITL的设备不会重新注册到集群，直到ITL被删除。

CallManager证书

重新生成CallManager和CallManager-ECDSA的过程相同，包括服务重新启动。

⚠ 警告：请确保您已确定集群是否处于混合模式，然后继续。请参阅识别集群安全模式部分。

⚠ 警告：请勿在8.x-11.5版本中同时重新生成CallManager.PEM和TVS.PEM证书，或者如果ITL由Call Manager证书签名。这会导致终端上已安装的ITL出现不可恢复的不匹配，需要从集群中的所有终端删除ITL，或从DRS恢复以重新开始证书更新。

---

1. 导航到Cisco Unified CM Administration > System > Enterprise Parameters:
   - 选中Security Parameters部分并验证Cluster Security Mode是否设置为0或1。如果值为0，则集群处于非安全模式。如果值为1，则集群处于混合模式，您需要在重新启动服务之前更新CTL文件。请参阅令牌和无令牌链路。
2. 导航到集群中的每台服务器（在Web浏览器的单独选项卡中），从发布者开始，然后是每个订用者。导航到Cisco Unified OS Administration > Security > Certificate Management > Find。
   - 选择CallManager pem Certificate。
   - 打开后，选择Regenerate并等待，直到您看到Success弹出窗口，然后关闭弹出窗口或返回并选择Find/List。
3. 继续使用后续用户；执行步骤2中的相同步骤，并在集群中的所有用户上完成。
   - 如果集群处于混合模式，或者正在对802.1X使用CTL，则必须在继续之前更新CTL。
     - 登录到发布器的CLI并输入命令utils ctl update CTLFile。
     - 重置所有加密和经过身份验证的电话，使CTL文件更新生效。
4. 登录Publisher Cisco Unified Serviceability:
   - 导航到Cisco Unified Serviceability > Tools > Control Center - Feature Services。
   - 从发布服务器开始，然后继续订阅服务器，只重新启动Cisco CallManager服务，其状态显示已启动。

5. 导航到Cisco Unified Serviceability > Tools > Control Center - Feature Services。
    - 从发布服务器开始，然后继续订阅服务器，重新启动Cisco CTIManager Service，其状态显示已启动。
6. 导航到Cisco Unified Serviceability > Tools > Control Center - Network Services。
    - 从发布服务器开始，然后继续订阅服务器，重新启动思科信任验证服务。
7. 导航到Cisco Unified Serviceability > Tools > Control Center - Feature Services。
    - 从发布服务器开始，然后继续订阅服务器，重新启动Cisco TFTP服务，其状态显示已启动。
8. 如果您的集群配置为使用SSO或OAuth，则需要重新启动Cisco HAProxy服务。
    - 要重新启动Tomcat SSOSP，您需要为每个节点打开CLI会话并执行命令utils service restart Cisco HAProxy。
9. 重新启动所有电话：
    - 选项1 - Cisco Unified CM Administration > System > Enterprise Parameters
        - 选择Reset，您将看到一个弹出窗口，其中显示语句“You are about to reset all devices in the system.此操作无法撤消。是否继续？”，选择OK，然后选择Reset。
        - 此方法重置Call Manager中的所有组件。
    - 选项2 - Cisco Unified CM管理>批量管理>电话>更新电话>查询
        - 搜索设备名称以SEP > Next > Reset Phones > Run Immediately开头

电话现在已重置。通过RTMT工具监控其操作，以确保重置成功且设备重新注册到CUCM。等待电话注册完成，然后继续下一个证书。此电话注册过程可能需要一些时间。请注意，在重新生成过程之前具有不良ITL的设备不会重新注册到集群，直到ITL被删除。

TVS证书

警告：请勿在8.x-11.5版本中同时重新生成CallManager.PEM和TVS.PEM证书，或者如果ITL由Call Manager证书签名。这会导致终端上已安装的ITL出现不可恢复的不匹配，需要从集群中的所有终端删除ITL，或从DRS恢复以重新开始证书更新。

注意：TVS代表Call Manager对证书进行身份验证。最后重新生成此证书。

导航到集群中的每台服务器（在Web浏览器的单独选项卡中），从发布者开始，然后是每个订用者。导航到Cisco Unified OS Administration > Security > Certificate Management > Find。

- 选择TVS pem证书。
- 打开后，选择Regenerate并等待，直到您看到Success弹出窗口，然后关闭弹出窗口，或者返回并选择Find/List。

1. 继续使用后续用户；在步骤1中执行相同的步骤并在集群中的所有用户上完成。
    - 所有节点重新生成TVS证书后，重新启动服务：

- 登录到Publisher Cisco Unified Serviceabilty。
  - 导航到Cisco Unified Serviceability > Tools > Control Center - Network Services
  - 在发布服务器上，选择Restart on Cisco Trust Verification Service。
- 服务重新启动完成后，继续用户并重新启动Cisco Trust Verification Service。

2. 从发布服务器开始，然后继续订阅服务器，重新启动Cisco TFTP服务，其中状态显示已启动。
3. 重新启动所有电话：
   - 选项1 - Cisco Unified CM管理>系统>企业参数
     - 选择Reset，您将看到一个弹出窗口，其中显示语句“You are about to reset all devices in the system.此操作无法撤消。是否继续？”，选择OK，然后选择Reset。
     - 此方法重置Call Manager中的所有组件。
   - 选项2 - Cisco Unified CM Administration > Bulk Administration<s/trong> > Phones<s/trong> > Update Phones > Query
     - 搜索Device Name begins with SEP > Next > Reset Phones > Run Immediately。

电话现在已重置。通过RTMT工具监控其操作，以确保重置成功且设备重新注册到CUCM。等待电话注册完成，然后继续下一个证书。此电话注册过程可能需要一些时间。请注意，在重新生成过程之前具有不良ITL的设备不会重新注册到集群，直到ITL被删除。

ITR恢复证书

注意：当设备失去其受信任状态时，将使用ITLRecovery证书。证书显示在ITL和CTL中（当CTL提供程序处于活动状态时，Cisco bug ID CSCwf85275）。
从12.5+开始，ITLRecovery是由发布者生成的单个证书并分发给订阅者。
如果设备丢失其信任状态，您可以使用命令utils itl reset localkey用于非安全集群，使用utils ctl reset localkey命令用于混合模式集群。阅读Call Manager版本的安全指南，熟悉如何使用ITLRecovery证书以及恢复受信任状态所需的流程。
如果集群已升级到支持密钥长度2048的版本，且集群服务器证书已重新生成到2048年，并且ITLRecovery尚未重新生成，且当前密钥长度为1024，则ITL恢复命令将失败，并且不使用ITLRecovery方法。

---

1. 导航到Publisher Cisco Unified OS Administration > Security > Certificate Management > Find。
   - 选择ITLRecovery pem Certificate。
   - 打开后，选择Regenerate并等待，直到您看到Success弹出窗口，然后关闭弹出窗口，或者返回并选择Find/List。
2. 在ITLRecovery重新生成ITLRecovery证书后，需要重新启动服务。
   - 如果集群处于混合模式或正在对802.1X使用CTL，则必须在继续之前更新CTL。
     - 登录到发布器的CLI并输入命令utils ctl update CTLFile。
   - 登录到Publisher Cisco Unified Serviceability。
     - 导航到Cisco Unified Serviceability > Tools > Control Center - Network Services。

        - 在发布服务器上，选择Restart on Cisco Trust Verification Service。
    - 服务重新启动完成后，继续用户并重新启动Cisco Trust Verification Service。
3. 从发布服务器开始，然后继续订阅服务器，重新启动Cisco TFTP服务，其中状态显示已启动。
4. 重新启动所有电话：
    - 选项1 - Cisco Unified CM Administration > System > Enterprise Parameters
        - 选择Reset，您将看到一个弹出窗口，其中显示语句“You are about to reset all devices in the system.此操作无法撤消。是否继续？”，选择OK，然后选择Reset。
        - 此方法重置Call Manager中的所有组件。
    - 选项2 - Cisco Unified CM管理 > 批量管理 > 电话 > 更新电话 > 查询
        - 搜索Device Name begins with SEP > Next > Reset Phones > Run Immediately。

删除过期的信任证书

警告：删除证书可能会影响您的系统操作。如果证书是现有链的一部分，它还可以断开证书链。从Certificate List窗口中相关证书的用户名和使用者名称验证此关系。

注意：受信任证书是唯一可以删除的证书类型。无法删除由系统生成的自签名证书。识别需要删除、不再需要或已过期的信任证书。请勿删除包括CallManager.pem、tomcat.pem、ipsec.pem、CAPF.pem和TVS.pem在内的五个基本证书。可以适时删除信任证书。重新启动的下一个服务旨在清除这些服务中的旧证书信息。

1. 导航到Cisco Unified Serviceability > Tools > Control Center - Network Services。
    - 从下拉列表中选择CUCM Publisher。
        - 对于CUCM 11.5及更低版本，
        - 选择Stop Certificate Change Notification。CUCM 12.0版及更高版本不需要此要求。
        - 对集群中的每个Call Manager节点重复上述步骤。
    - 如果您有IMP服务器：
        - 从下拉菜单中，逐一选择IMP服务器，然后选择Stop Platform Administration Web Services和Cisco Intercluster Sync Agent。IMP版本12.0及更高版本不需要此要求。
2. 导航到Cisco Unified OS Administration > Security > Certificate Management > Find。
    - 查找过期的信任证书。(对于版本10.X及更高版本，您可以按到期进行过滤。对于低于10.0的版本，请手动识别证书或使用RTMT警报（如果收到）。)
    - 同一信任证书可以出现在多个节点中。必须从每个节点单独删除它。
    - 选择要删除的信任证书（根据您的版本，您会弹出一个窗口，或者导航到同一页面上的证书）
        - 选择Delete（您将看到以“您将要永久删除此证书”开头的弹出窗口）。
        - 选择“确定”。
3. 对每个要删除的信任证书重复此过程。

4. 完成后，需要重新启动与删除的证书直接相关的服务。在本节中，您无需重新启动电话。Call Manager和CAPF会对终端造成影响。
    - Tomcat-trust:通过命令行重新启动Tomcat服务（请参阅Tomcat部分）。
    - CAPF-trust:重新启动Cisco Certificate Authority代理功能（请参阅CAPF部分）。 请勿重新启动终端。
    - CallManager信任：CallManager Service/CTIManager（请参阅CallManager一节）。请勿重新启动终端。
        - 影响终端并导致重新启动。
    - IPSEC信任：DRF主/DRF本地（请参阅IPSEC部分）。
    - TVS（自签名）没有信任证书。
5. 重新启动之前在步骤1中停止的服务。

确认

要从CLI列出CUCM上存在的证书，请使用以下命令输出：

```
run sql select c.servername, tcs.name, dist.moniker, c.ipv4address, c.certificate from certificate as c
```

故障排除

此配置不支持故障排除过程。

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）。