重新生成CUCM证书

目录

简介

本文档介绍在Cisco Unified Communications Manager(CUCM)版本8.X及更高版本中重新生成证书的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- *实时监控工*具(RTMT)
- CUCM证书

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM 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。

背景信息

本文档介绍如何在Cisco Unified Communications Manager(CUCM)版本8.X及更高版本中重新生成证书的分步过程。但是，这没有反映12.0后国际交易日志恢复的变化情况。

安装RTMT

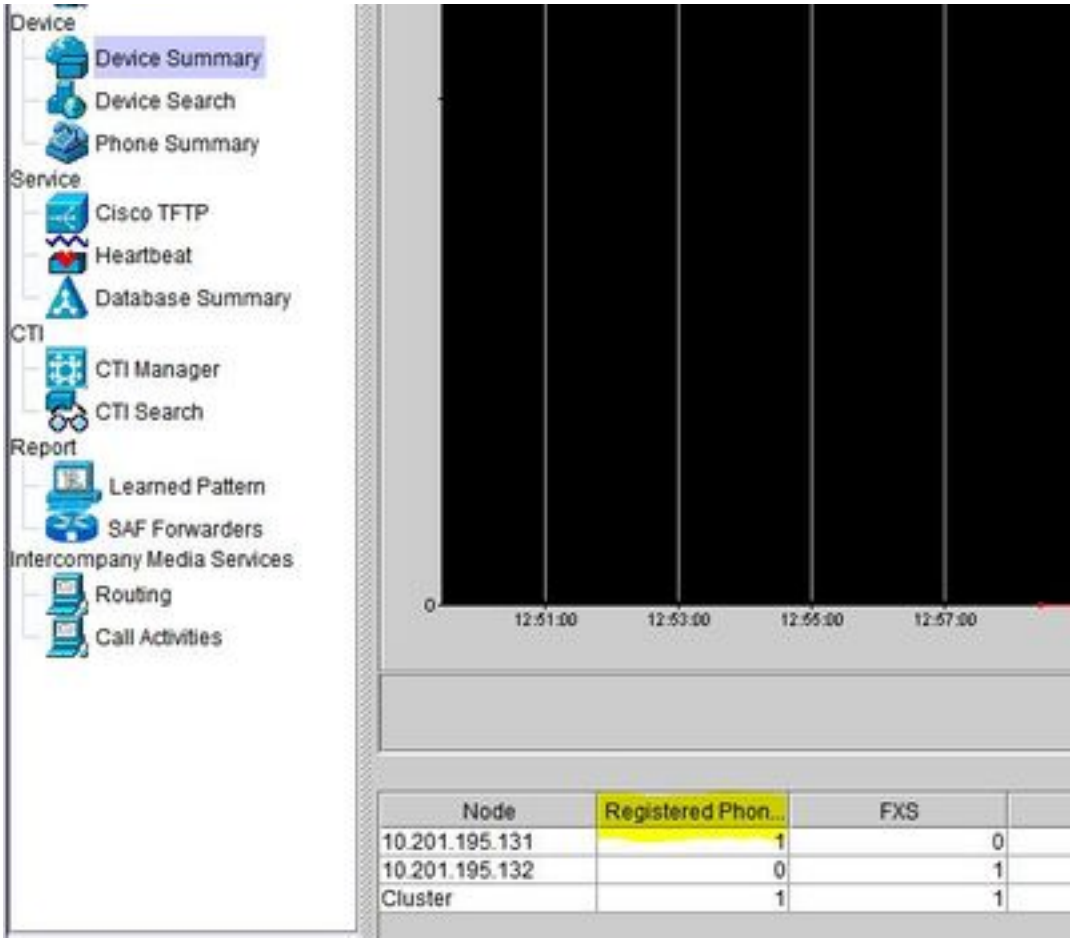
- 从Call Manager下载并安装RTMT工具。 导航到Call Manager(CM)Administration: **应用程序>插件>查找> Cisco Unified Real-Time Monitoring Tool - Windows >下载** 安装和启动

使用RTMT监控终端

- 启动RTMT并输入IP地址或完全限定域名(FQDN)，然后输入用户名和密码以访问该工具：
- 选择**Voice/Video**选项卡。选择**Device Summary**。 此部分标识注册终端的总数以及每个节点的数量端点重置时监控，以确保在重新生成下一个证书之前进行注册

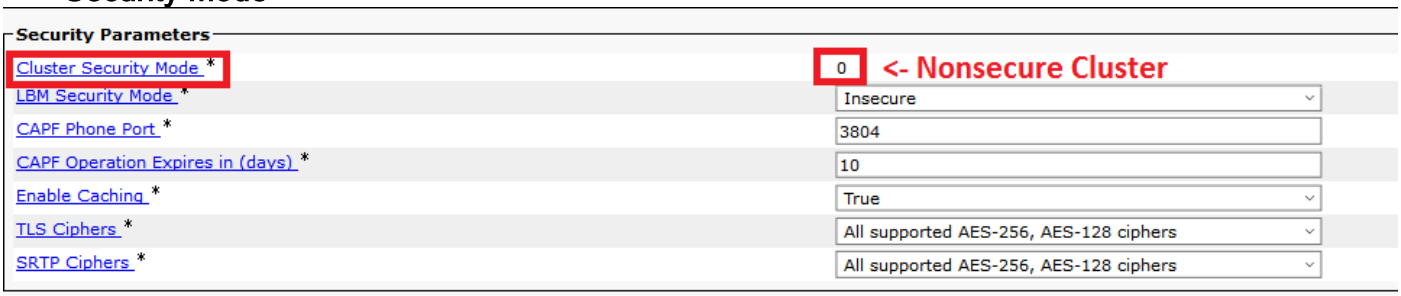
  提示：某些证书的重新生成过程可能会影响端点。由于需要重新启动服务和重新启动电话，请在正常工作时间后考虑一个行动计划。强烈建议通过RTMT验证电话注册。

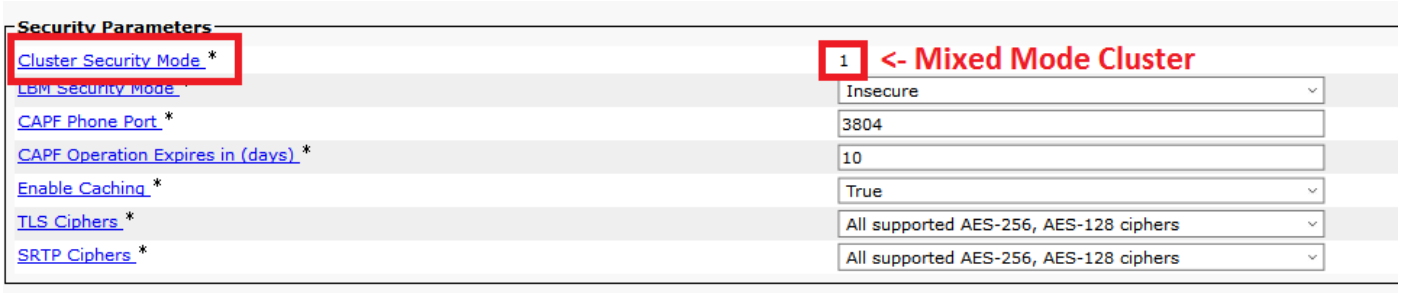
  警告：在此流程之后，当前ITL不匹配的终端可能会出现注册问题。 在更新过程完成且所有其他电话注册后，删除终端上的国际交易日志是一个典型的最佳做法解决方案。



确定集群是处于混合模式还是非安全模式

- 导航到CM Administration。 **System > Enterprise Parameters > Security Parameters > Cluster Security Mode**





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。以下显示的是无效或过期的特定证书的服务列表：

CallManager.pem

- 加密/身份验证电话未注册
- 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

- 电话无法访问CUCM节点上托管的HTTP服务，例如公司目录
- CUCM可能遇到各种网络问题，例如无法从集群中的其他节点访问服务页面
- 跨群集的分机移动(EM)或分机移动问题
- 单点登录(SSO)
- 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

- 电话不对电话VPN、802.1x或电话代理进行身份验证
- 无法为电话颁发本地重要证书(LSC)证书。
- 加密的配置文件不起作用

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)到其他CUCM集群的IPsec隧道不起作用

TVS（信任验证服务）

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。

ITL和CTL

- ITL包含Call Manager TFTP的证书角色、集群中的所有TVS证书以及运行时的证书授权代理功能(CAPF)。
- CTL包含在同一服务器、CAPF、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。

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

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，然后是每个订用者。 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)列中观察。如果Tomcat是第三方签名的，请按照提供的链接进行操作，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**Tomcat 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**。
3. 继续处理每个后续用户，按照步骤2中的相同过程完成集群中的所有用户。
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。从发布者开始，然后是订阅者。 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**。

```
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.如果适用，需要从CCX环境中执行以下步骤：

- 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：DRF 10.X版之前的CUCM/即时消息和在线状态(IM&P) Master 代理在CUCM Publisher和IM&P Publisher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，DRF Master 代理仅在CUCM发布服务器上运行，在CUCM订用程序和IM&P发布服务器和订用服务器上运行DRF本地服务。

注意：灾难恢复系统使用 Master 代理和本地代理，用于CUCM集群节点之间的数据身份验证和加密。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信任文件，则必须确保将IPSEC证书上传到IPSEC信任存储。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，然后是每个订用者。导航到**Cisco Unified OS Administration > Security > Certificate Management > Find**: 选择**IPSEC 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**。
2. 继续使用后续用户；按照步骤1中的相同步骤操作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**。 **Cisco Unified Serviceability > Tools > Control Center - Network Services**。选择**Restart** on **思科DRF** Master服务。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**，然后继续使用用户，然后在**Cisco DRF本地服务**上选择**Restart**。

发布器中的IPSEC.pem证书必须有效，且必须作为IPSEC信任库存在于所有订阅器中。在标准部署中，发布服务器中不存在用户IPSEC.pem证书作为IPSEC信任库。为了验证有效性，请将PUB的IPSEC.pem证书中的序列号与SUB中的IPSEC-trust进行比较。它们必须匹配。

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**别集群处于混合模式或非安全模式部分**。

1. 导航至**Cisco Unified CM管理>系统>企业参数**。
   检查“安全参数”部分，验证集群安全模式是否设置为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**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返回并选择**Find/List**
3. 继续使用后续用户；按照步骤2中的相同步骤操作并在集群中的所有用户上完成。 如果集群仅处于混合模式且已重新生成CAPF — 请在继续下一步之前更新CTL Token - Tokenless。如果集群处于混合模式，则还需要重新启动Call Manager服务才能重新启动其他服务。
4. 所有节点重新生成CAPF证书后，重新启动服务。
   导航到发布者**Cisco Unified Serviceability**。 **Cisco Unified Serviceability > Tools > Control Center - Feature Services**。从发布者开始，并在活动位置选择**Cisco Certificate Authority Proxy Function Service**上的**Restart**。
5. 导航至**Cisco Unified Serviceability > Tools > Control Center - Network Services**。 从发布者开始，然后继续订阅者，选择**Restart** on **Cisco Trust Verification** 服务。 导航至**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，仅在活动位置重新启动**Cisco TFTP服务**。
6. 重新启动所有电话： **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**You are about to reset all devices in the system。此操作无法撤消。继续？,**选择**确定，然后选择重置。**

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的设备在删除之前不会注册回集群。

CallManager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**确定集群处于混合模式或非安全模式**部分。

警告：请勿同时重新生成CallManager.PEM和TVS.PEM证书。 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。完成CallManager.PEM的整个过程，并在电话重新注册后，启动TVS.PEM的流程。

1. 导航到**Cisco Unified CM管理>系统>企业参数**: 检查“安全参数”部分，验证集群安全模式是否设置为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；按照步骤2中的相同步骤操作并在集群中的所有用户上完成。 如果集群仅处于混合模式，并且CallManager证书已重新生成 — 在继续下一步之前更新CTL Token - Tokenless
4. 登录到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，在活**动位置重新**启动Cisco CallManager服务。
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，仅在活**动时重新**启动Cisco CTIanager服务。
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，仅在活动位置重新启动**Cisco TFTP服务**。
8. 重新启动所有电话： **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**You are about to reset all devices in the system。此操作无法撤消。继续？,**选择**确定，然后选择重置**

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，在再生过程之前存在不良ITL的设备在ITL删除之前不会注册回集群。

TVS证书

警告： 请勿同时重新生成CallManager.PEM和TVS.PEM证书。 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。

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返回并选择**Find/List**。

1. 继续使用后续用户；按照步骤1中的相同步骤操作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 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**思科信任验证服务**。
2. 从发布服务器开始，然后继续订阅服务器，仅在活**动时重新**启动**Cisco TFTP** Service。
3. 重新启动所有电话： **Cisco Unified CM Administration > System > Enterprise Parameters**。选择**Reset**，您将看到一个弹出窗口，其中显示**You are about to reset all devices in the system。此操作无法撤消。继续？,**选择**确定，然后选择重置。**

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，在再生过程之前存在不良ITL的设备在ITL删除之前不会注册回集群。

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。证书出现在ITL和CTL中（当CTL提供程序处于活动状态时）。
> 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**ITLRecovery 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；按照步骤2中的相同步骤操作并在集群中的所有用户上完成。
3. 所有节点重新生成ITLRecovery证书后，需要按以下顺序重新启动服务： 如果您处于混合模式 — 在继续Token - Tokenless之前更新CTL。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**思科信任验证服务**。
4. 从发布服务器开始，然后继续订阅服务器，仅在活**动时重新**启动**Cisco TFTP** Service。
5. 重新启动所有电话： **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**You are about to reset all devices in the system。此操作无法撤消。继续？,**选择**确定，然后选择重置。**
6. 现在，电话在重置时上传新的ITL/CTL。

删除过期的信任证书

注意：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. 导航至**Cisco Unified Serviceability > Tools > Control Center - Network Services**。 从下拉列表中选择CUCM Publisher。选择**Stop Certificate Change Notification**。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，逐一选择您的IMP服务器，然后选择**Stop Platform Administration Web Services**和**Cisco Intercluster Sync Agent**。
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，您需要手动识别特定证书，或者通过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（取决于您获得弹出窗口或导航到同一页面上的证书的版本） 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信任：重新启动Cisco Certificate Authority代理功能（请参阅CAPF部分）不要重新启动终端。CallManager-trust:CallManager Service/CTIManager（请参阅CallManager部分）不重新启动终端。 影响终端并导致重新启动。IPSEC信任：DRF Master/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

验证过程对此配置不可用。

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）。