CUCM电话证书(LSC/MIC)的问题解答

目录

简介

本文档介绍Cisco Unified Communications Manager(CUCM)电话证书的一些问题和答案。 以下是电话证书的快速视图。

制造商安装的证书(MIC):

如名称所示，电话预装有MIC，管理员无法删除/修改此MIC。证书颁发机构(CA)证书CAP-RTP-001、CAP-RTP-002、Cisco_Manufacturing_CA和Cisco Manufacturing CA SHA2预安装在CUCM中以信任MIC。一旦MIC的有效期过，MIC就无法使用重新生成，

本地有效证书(LSC):

LSC拥有Cisco IP电话的公钥，该公钥由Cisco Unified Communications Manager证书颁发机构代理功能(CAPF)私钥签名。默认情况下，电话上未安装该软件。管理员对LSC拥有完全控制权。CAPF CA证书可以重新生成，然后可以在需要时向电话发出新LSC。

电话证书的常见用途是什么？

以下是电话证书的一些常见用途

在CAPF和电话之间安装/升级、删除或故障排除

电话与CAPF建立连接，以在电话上安装/升级、删除或排除证书故障。当Authentication Mode下的Certification Authority Proxy Function(CAPF)Information设置为By Existing Certificate(Precedence to LSC)或By Existing Certificate(Precedence to MIC)时，电话证书用于建立与CAPF的连接。

按现有证书（优先于LSC）： 电话使用LSC向CAPF进行身份验证。如果未安装LSC，则使用MIC。如果使用的证书有问题，安装失败，原因为“LSC无效”。例如，LSC的签名CA在CAPF信任中不可用。对于此类故障情况，使用其他证书方法或空字符串更新身份验证模式。

按现有证书（优先级到MIC）：电话使用MIC向CAPF进行身份验证。

在CallManager和电话之间进行传输层安全(TLS)连接

电话使用LSC或MIC与CallManager建立TLS连接。CallManager将通过检查CallManager-trust来验证电话提供的证书。LSC的CallManager-trust和MIC的思科制造CA中必须提供相应的CAPF证书。

在电话和身份验证服务器之间进行802.1x身份验证

CAPF/制造CA证书上传到身份验证服务器，如思科安全访问控制服务器(ACS)或身份服务引擎(ISE)。 身份验证服务器使用上传的证书在电话显示其证书（LSC或MIC）时对其进行身份验证。

用于电话和适用于VPN的思科自适应安全设备(ASA)之间的基于证书的身份验证

CAPF/制造CA证书上传到ASA中，当电话显示LIC/MIC时，ASA通过检查其信任来验证它。

当存在LSC和MIC时，是否有方法明确选择LSC或MIC进行连接？

没有选项可为连接选择LSC还是MIC。如果安装了LSC，电话使用LSC。如果未安装LSC，电话使用MIC。

LSC不存在时的控制台条目：

SECD:-PXY_NO_LSC:[SCCP]没有LSC，将尝试MIC

存在LSC时的控制台条目：

SECD:-PXY_CERT_CIPHER:[SCCP]、[TLSv1]、证书[LSC]

LSC或MIC只能在CAPF和电话安装/升级、删除或故障排除之间选择。

迁移到新集群时，具有安全配置文件的LSC安装电话未注册的原因是什么？

对于已从旧集群拥有LSC的电话，可能会发生这种情况。当MIC和LSC同时存在时，LSC用于建立TLS连接。无法建立TLS，因为新CUCM在其CallManager信任中没有此LSC的CA。

控制台日志显示用于建立TLS的证书。下面的条目显示使用LSC。

3469非00:01:31.935298秒：-PXY_CERT_CIPHER:[SCCP]、[TLSv1]、证书[LSC]、密码[AES256-SHA:AES128-SHA]

控制台日志中此类失败案例的SSL3_Alert（“未知CA”）：-

3486错误00:01:31.938954秒：-STATE_SSL3_ALERT:SSL3警报[读取]:[致命]:[未知CA

解决此问题的方法之一是，使用非安全配置文件注册电话，然后删除现有LSC。从新集群安装LSC，然后使用安全配置文件注册电话。也可以使用MIC注册具有安全配置文件的电话，而无需安装LSC。

是否需要为电话安装LSC才能使用经过身份验证或加密的安全配置文件进行注册？

否。如果未安装LSC，电话使用MIC建立与CUCM的TLS连接。

4878 WRN 15:47:34.756063秒：-PXY_NO_LSC:[SCCP]没有LSC，尝试MIC。

要安装/升级/删除LSC，是否必须对各自设备安全配置文件中的设备安全模式进行身份验证或加密？

它不是强制性的，可以使用默认标准非安全配置文件完成，在设备安全模式下也是不安全的。

在电话中安装LSC是否必须集群处于混合模式？

这不是强制性的。即使集群安全模式处于非安全模式，也可以执行LSC安装/删除。

如何快速测试电话使用的LSC是否有问题？

转到Phone Admin Page，删除其中一部电话中的LSC。这会强制电话使用MIC。如果MIC一切正常，则继续LSC故障排除。

如何获取电话证书进行故障排除？

在Device/Phone（设备/电话）下设置Certificate Operation（证书操作）以进行故障排除。依次点击保存(Save)和应用配置(Apply Config)。 请等待查看证书操作状态以排**除成功故障**。从实**时监控工具**(RTMT)收集思科证书颁发机构代理功能日志。 包含来自电话的证书。

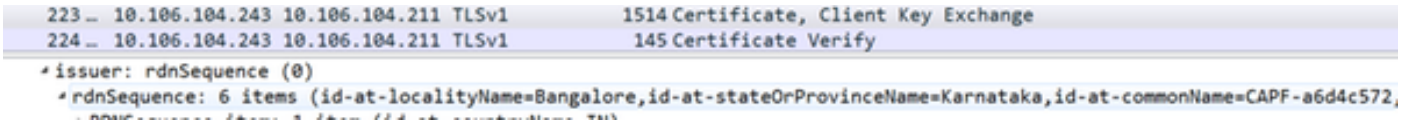
如果电话的LSC或MIC用于与CallManager建立TLS连接，如何从数据包捕获中验证？

收集包含电话重启的数据包捕获。

检查证书、客户端密钥交换消息。验证从IP电话发送的证书。

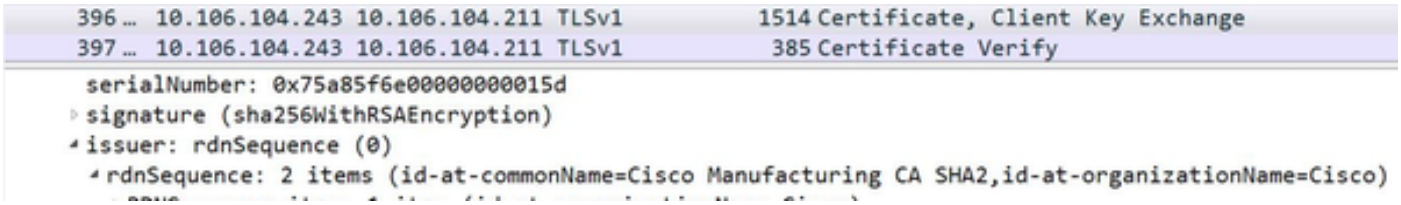
示例LSC:

对于LSC，CAPF CN在颁发者字段中显示。CallManager-trust中必须存在各自的CAPF根。



示例MIC:

对于MIC，请在颁发者字段中输入思科制造CA。CallManager-trust中必须存在各自的根CA。



认证机构代理功能(CAPF)信息下的身份验证模式有何意义？CUCM和电话之间的TLS连接有何意义？

它只是电话和CAPF之间用于安装/升级/删除和故障排除操作的一种身份验证方法。它对CUCM和电话之间的TLS连接没有任何意义。

重新生成CAPF证书后，电话要考虑的基本LSC操作是什么？

本节介绍不使用离线CA发出LSC的空闲场景。

与CallManager的TLS连接

确保在从CallManager-trust中删除之前的CAPF证书之前在电话上安装新LSC。删除之前的CAPF证书，然后重新启动CallManager服务，会导致具有此CAPF证书颁发的LSC的电话的注册问题。

LSC操作与CAPF-Trust

确保在从CAPF-trust删除之前的CAPF证书之前在电话上安装新LSC。LSC操作(如使用“现有证书”(Precedence to LSC)的身份验证模式**安装/删除)失败，错误为Invalid LSC** 对于具有由此CAPF证书颁发的LSC的电话。

在电话和身份验证服务器之间进行802.1x身份验证

确保在上传新CAPF证书并电话获取新CAPF颁发的LSC之前，不要从身份验证服务器删除之前的CAPF证书。

在ASA和电话之间

确保在电话获取新LSC并将新CAPF CA证书上传到ASA之前，不要从ASA删除之前的CAPF证书。

请参阅证书再生，*了解重新生成CAPF证书的步骤。*

相关信息

- 思科IP电话证书和安全通信
- 802.1X IP电话设计指南
- 思科统一通信管理器安全指南