CUCM电话证书的(LSC/MIC) Q.A

目录

简介

本文包括某些Cisco Unified Communications Manager (CUCM)电话证书的问题和解答。 这是电话证书的一张快速视图。

制造商预装证书(MIC) ：

当名称指示，电话事先装配与MIC，并且这不可能由管理员删除/修改。Certificate Authority (CA)证书CAP-RTP-001、制造CA SHA2的CAP-RTP-002、Cisco_Manufacturing_CA和思科在CUCM被事先装配委托MIC。 MIC能？t，一旦正确性超时作为MIC CA伪善言辞是关于生成，使用，

局部重要的证书(LSC) ：

LSC拥有Cisco IP电话的公共密钥，由Cisco Unified Communications Manager认证机关代理功能(CAPF)专用密钥签字。默认情况下它在电话没有安装。管理员完全控制LSC。CAPF CA证书可以被重新生成能反过来发出新建的LSC到电话，每当要求。

什么是电话证书的普通的用途？

这是电话证书的一些普通的用途

在CAPF和电话之间安装的/升级，删除或者排除故障

打电话建立与CAPF安装/升级的连接，删除或者排除故障在电话的证书。电话Certficate用于建立与CAPF的连接，当认证模式在证书颁发机构现有的证书设置的对由现有的证书(对LSC的优先)或代理功能(CAPF)时信息下(对MIC的优先)。

由现有的证书(对LSC的优先) ： 电话使用LSC验证与CAPF。如果LSC没有安装，它将使用MIC。如果有与使用的证书的问题安装失效与原因“无效LSC”。示例， LSC的签字的CA不是可用的在CAPF托拉斯。更新认证模式使用其他证书方法或由这样失败事例的空字符串。

由现有的证书(对MIC的优先) ：电话使用MIC验证与CAPF。

在CallManager和电话之间Trasnsport层安全(TLS)连接的

电话使用LSC或MIC建立与CallManager的TLS连接。CallManager将验证电话提交的Certficate通过检查CallManager托拉斯。各自CAPF证书必须取得到在CallManager托拉斯中为LSC和思科制造CA？MIC的s。

在电话和认证服务器之间802.1x验证的

CAPF/Manufacturing CA certs上传到认证服务器类似思科安全访问控制服务器(ACS)或身份服务引擎(ISE)。认证服务器使用上传的证书验证电话，当它存在其证书(LSC或MIC)。

证书在电话和思科可适应安全工具(ASA)之间的基于验证VPN的

CAPF/Manufacture CA certs在ASA上传，当电话现在LIC/MIC， ASA通过检查它验证它时信任。

当LSC和MIC存在时，有没有任何方式为连接明确地选择LSC或MIC ？

没有中的选项是否LSC或MIC连接的。如果LSC安装，电话使用LSC。 如果LSC没有安装，电话使用MIC。

控制台条目，当LSC不存在：

SECD ：- PXY_NO_LSC ：[SCCP]的LSC，不会尝试MIC

控制台条目，当LSC存在：

SECD ：- PXY_CERT_CIPHER ：[SCCP]， [TLSv1]， cert [LSC]

LSC或MIC的选择是仅可能的在CAPF和电话安装/升级之间，删除或者排除故障。

什么是原因有获取的配置文件的LSC安装的电话不得到登记，当移

动对新的集群？

这能为电话发生已经有的那些从旧有团星的一LSC。当MIC和LSC存在时， LSC用于建立TLS连接。TLS不能设立，因为新的CUCM doesn ？t有此LSC的CA在其呼叫管理器信任。

控制台日志显示哪证书用于设立TLS。在条目之下显示LSC使用。

3469没有00:01:31.935298 SECD ：- PXY_CERT_CIPHER ：[SCCP]， [TLSv1]， cert [LSC]，密码器[AES256-SHA:AES128-SHA]

SSL3_Alert与？未知CA ？在控制台日志的这样失败的案件：--

3486个ERR 00:01:31.938954 SECD ：-STATE_SSL3_ALERT ：SSL3警报[read] ：[fatal] ：[未知CA

其中一个方式解决此问题是，获得电话注册使用非？安全配置文件然后删除现有LSC。使用获取的配置文件，安装从新的集群的LSC然后注册电话。也是可能的有有使用MIC注册的获取的配置文件的电话，无需安装LSC。

它要求有为了电话安装的LSC能获得它注册使用已验证或已加密获取的配置文件？

不能。如果LSC没有安装，电话使用MIC建立对CUCM的TLS连接。

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

在各自设备安全性配置文件的设备安全性模式验证或加密的安装/升级/删除LSC是否是必须的？

不是必须，它可以太执行使用默认标准不安全的配置文件在设备安全性模式是非安全的地方。

是否是必须团星在安装在电话的LSC的混合模式？

这不是必须。LSC安装/删除可以完成，既使当在不安全的集群安全模式。

如何迅速测试，如果有与电话使用的LSC的问题？

通过去删除LSC在一个电话中电话管理员页面。这强制电话使用MIC。如果所有与MIC然后优良继续进行故障排除LSC。

如何获得排除故障的电话证书？

设置证书操作排除故障在设备/电话下。命中数保存然后运用设置。 等待发现证书操作状态**排除故障成功**。收集**思科认证机关**从实时监控工具(RTMT)的**代理功能**日志。它包含从电话的证书。

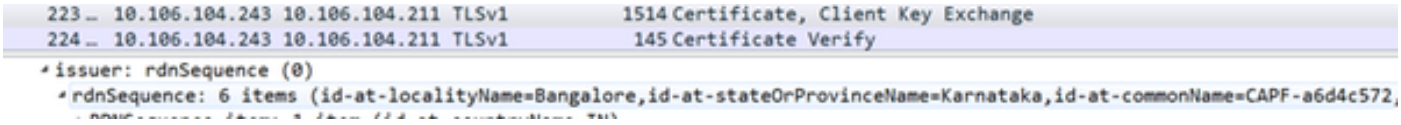
如何从数据包捕获验证，如果电话的LSC或MIC是使用的建立与CallManager的TLS连接？

收集包括电话重新启动的数据包捕获。

检查证书，客户端密钥交换交换消息。验证从IP电话发送的证书。

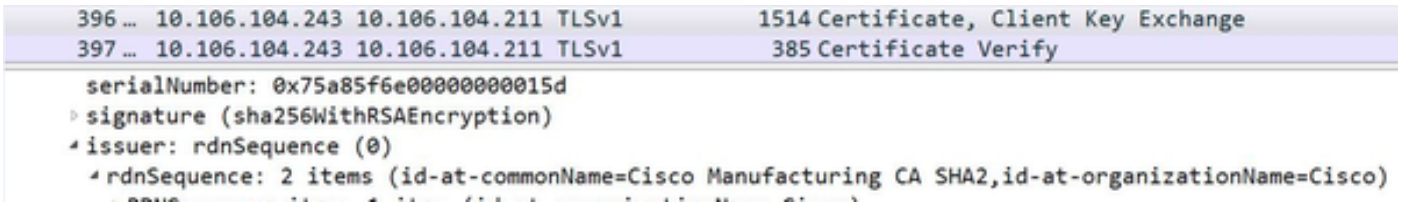
示例LSC ：

对于LSC， CAPF CN在发布者字段被看到。各自CAPF根必须是存在CallManager托拉斯中。



示例MIC ：

MIC，制造CA的思科在发布者字段。各自根CA必须是存在CallManager托拉斯中。



什么是认证模式的意义在证书颁发机构代理功能(CAPF)信息下？TLS连接的任何意义CUCM和电话之间？

它是在电话和CAPF之间的一认证方法安装的/升级/删除和排除故障操作。它doesn ？t有TLS连接的所有意义CUCM和电话之间。

什么是电话的基本LSC操作能考虑在CAPF证书以后被重新生成？

此部分包括脱机CA没有用于发出LSC的空闲方案。

与CallManager的TLS连接

保证在删除从CallManager托拉斯的上一个CAPF证书前安装在电话的新的LSC。删除CallManager服务重新启动跟随的上一个CAPF证书请导致对那些有此CAPF证书发出的LSC的电话的注册问题。

与CAPF托拉斯的LSC操作

保证在删除从CAPF托拉斯的上一个CAPF证书前安装在电话的新的LSC。那些有此CAPF证书发出的LSC的LSC操作类似安装/删除使用认证模式**由现有的证书(优先对LSC)**失效与错误**无效LSC**电话的。

在电话和认证服务器之间802.1x验证的

保证不删除从认证服务器的上一个CAPF证书，直到新的CAPF证书上传并且给LSC由新的CAPF发出的获得打电话。

在ASA和电话之间

保证不删除从ASA的上一个CAPF证书直到电话有新的LSC和上传的新建的CAPF CA证书ASA。

*参考*证书重新生成关于将被跟随的步骤重新生成CAPF证书。

相关信息

- Cisco IP电话证书和安全通信
- 802.1X设计指南的IP电话
- Cisco Unified Communications Manager安全指南