启用在CUCM的已加密配置功能

目录

简介

本文描述使用在Cisco Unified Communications Manager (CUCM)的已加密配置电话文件。

背景信息

使用电话的已加密配置文件是可用的在CUCM的一个可选安全功能。

您没有要求运行在混合模式的CUCM集群为了此功能能正常运行，因为认证机关代理功能(CAPF)证书信息在标识托拉斯列表(ITL)文件内包含。

> **Note**:这是所有的默认位置CUCM版本8.X和以上。对于在版本8.X之前的CUCM版本，您必须保证集群在混合模式运行，如果希望使用此功能。

已加密配置功能概述

此部分描述发生的进程，当已加密配置电话文件在CUCM内时使用。

当您启用此功能，重置电话，并且下载配置文件时，您收到一个要求有**.cnf.xml.sgn分机的**文件：

然而，在已加密配置功能在CUCM后启用， TFTP服务不再生成有**.cnf.xml.sgn分机的**一个完全配置文件**。**反而，如下一个示例所显示，它生成部分配置文件。

> **Note**:当您第一次时使用此方法，电话与局部重要的证书(LSC)或制造安装的证书比较电话证书的MD5哈希在配置文件的(MIC)的MD5哈希。

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
```

```
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
<certHash></certHash>
<encrConfig>true</encrConfig>
</device>
```

如果电话识别问题，尝试启动有CAPF的一会话，除非CAPF认证模式*由认证字符串*配比，在必须手工输入字符串情况下。这是电话也许识别的一些问题：

- 哈希不配比。
- 电话不包含证书。
- MD5值是空白的(正如在前一个示例)。

Note:电话启动传输层安全(TLS)默认情况下会话对在端口3804的CAPF服务。

必须为电话知道CAPF证书，因此在ITL文件或证书信任列表(CTL)文件必须包括(如果集群在混合模式运行)。

在CAPF通信建立后，电话发送使用的信息对关于LSC或MIC的CAPF。CAPF解压缩从LSC或MIC的电话公共密钥，然后生成MD5哈希，并且存储公共密钥的值和在CUCM数据库的证书哈希。

```
admin:run sql select md5hash,name from device where name='SEPA45630BBFA40'
md5hash name
================================ ===============
6e566143c1c14566c9da943d949a79c8 SEPA45630BBFA40
```

在公共密钥在数据库后存储，电话重置并且请求新配置文件。电话尝试**再次**下载有**cnf.xml.sgn分机的**配置文件。

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
<certHash>6e566143c1c14566c9da943d949a79c8</certHash>
<encrConfig>true</encrConfig>
</device>
```

电话再比较**cerHash**，并且，如果不检测问题，下载有**.cnf.xml.enc.sgn分机的**已加密配置文件。

```
............c..)CN=cucm85;OU=It;O=Cisco;L=KRK;ST=PL;C=PL....Z.........)CN=cucm85;
```

```
OU=It;O=Cisco;L=KRK;ST=PL;C=PL..........
.........C.<...Y6.Lh.|(..w+..,.0.a.&.
O.........V....T...Z..R^..f....|.=.e.@...5..........G...[.........n.........=
.A..H.(....Z...{.!%[.. SEPA45630BBFA40.cnf.xml.enc.sgn....R.DD..M...........
Uu.C..@..........
..................m.b.......6y ..x.^b..-8.^..^'.4.<Wb.n.....5...we.0@..g..
V7.,..r.9
Qs>..).w....pt/...}A.']
.r.t%G..d_.;u.rEI.pr.F
.....M..r...o.N
.=..g.^P....Pz....J..E.S...d|Z).....J..&..I....7.r..g8.{f..o.....:.~..U...5G+V.
[...]
```

Enable (event)已加密配置功能

为了启用已加密配置电话文件，您必须创建一个新的(或编辑当前)电话安全配置文件和分配它到电话。完成这些步骤为了启用在CUCM的已加密配置功能：

1. 登录CUCM管理页面并且导航对**系统> Security >电话安全配置文件**：

2. 复制当前或者创建新，给安全配置文件打电话并且检查**TFTP加密的设置**复选框：

3. 分配配置文件到电话：

故障排除

完成这些步骤为了关于已加密配置功能排除故障系统问题：

1. 保证CAPF服务是活跃的并且适当地运作在CUCM集群的发行商节点。

2. 下载部分配置文件并且验证CAPF服务的端口和IP地址从电话是可及的。

3. 验证在端口3804的TCP通信对发行商节点。

4. 运行以前被提及的结构化查询语言(SQL)命令为了验证CAPF服务是否有由电话使用关于LSC或MIC的信息。

5. 如果问题仍然仍然存在，您也许要求从系统收集其他信息。重新启动电话并且收集此信息：

给控制台日志打电话Cisco Tftp日志思科CAPF日志从CUCM和电话的数据包捕获

参考这些资源关于如何从CUCM和电话运行数据包捕获的更多信息：

- 收集CUCM跟踪从TAC SR的CUCM 8.6.2
- 统一通信管理器设备型号的数据包捕获
- 收集数据包捕获从Cisco IP电话

在日志和数据包捕获，您必须保证在前面部分描述的进程正常运行。特别地，请验证那：

- 电话下载有正确CAPF信息的部分配置文件。
- 电话通过TLS接通对CAPF服务，并且那关于LSC或MIC的信息在数据库更新。
- 电话下载全双工已加密配置文件。