安全外部电话服务配置示例

目录

简介

本文描述如何配置安全外部电话服务。此配置能工作与所有第三方服务，但是对于演示，本文使用一个远程Cisco Unified Communications Manager (CUCM)服务器。

贡献用何塞比利亚洛沃斯， Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM
- CUCM证书
- 电话服务

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM 10.5.X/CUCM 11.X
- 小型客户机控制协议(SCCP)和会话初始化协议(SIP)电话向CUCM登记
- 实验室其使用的附属的替代方案名称(SAN)证书。
- 外部目录在SAN certs。
- 对于在此示例的所有系统Certificate Authority (CA)将是相同的，所有certs使用是CA符号。
- Domain Name server(DNS)和网络时间协议(NTP)需要是属性设置和工作。

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。如果您的网络实际，请保证您了解所有更改潜在影响。

相关产品

本文档也可用于以下硬件和软件版本：

- CUCM 9.X/10.X/11.X

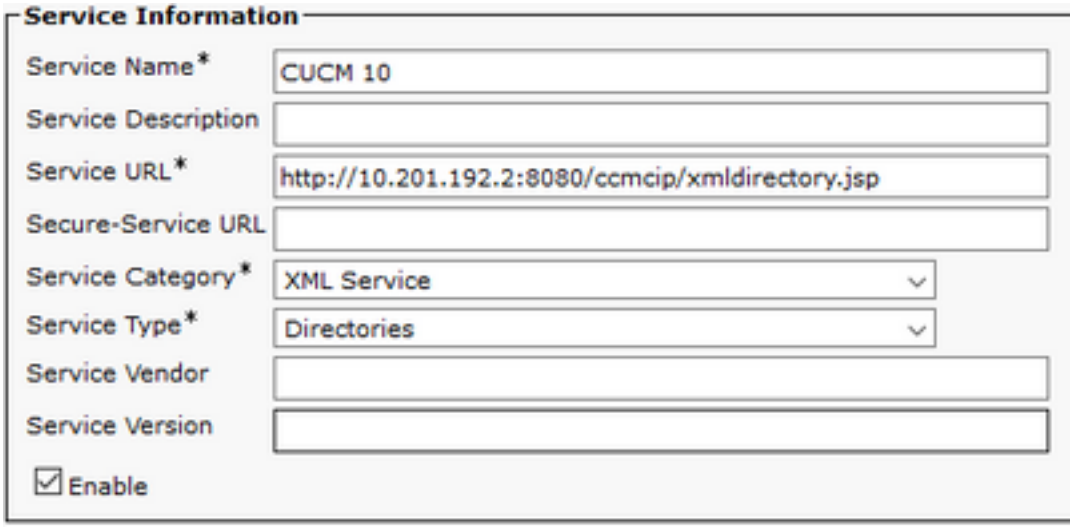
配置步骤

步骤1.设置在系统的服务URL。

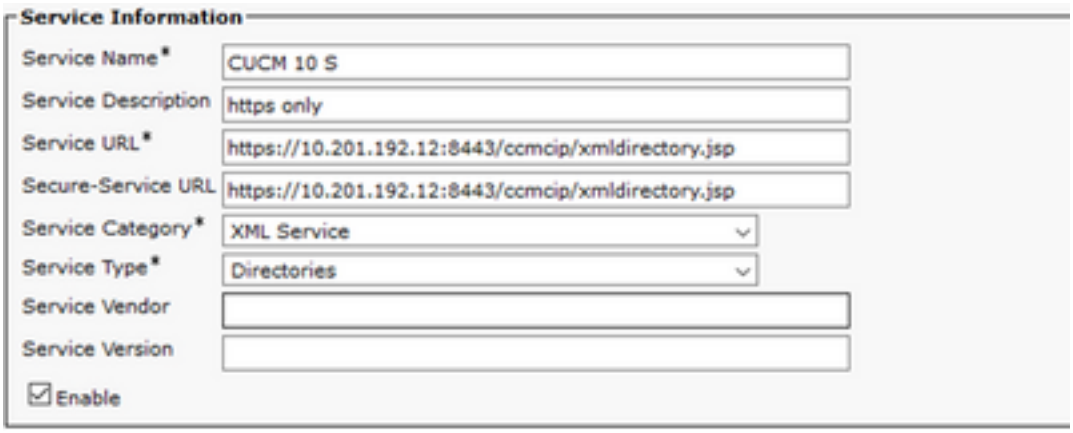
设置超文本传输协议(HTTP)和超文本传输协议安全(HTTPS)作为概念证明。最终想法是使用仅安全HTTP流量。

导航到**Device>设备Settings> service>添加新的电话**

仅HTTP



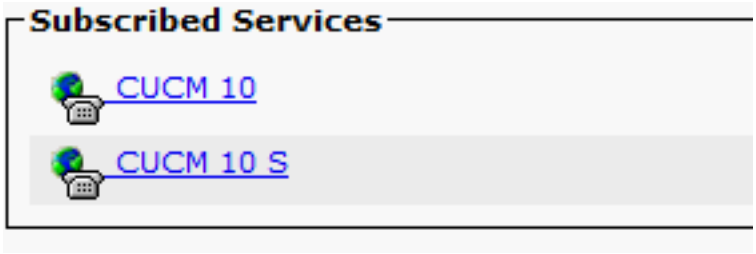
仅HTTPS



> 警告：如果添加**企业订阅的**检查，步骤两可以被跳到。然而，此更改重置所有电话，因此请保证您了解潜在影响。

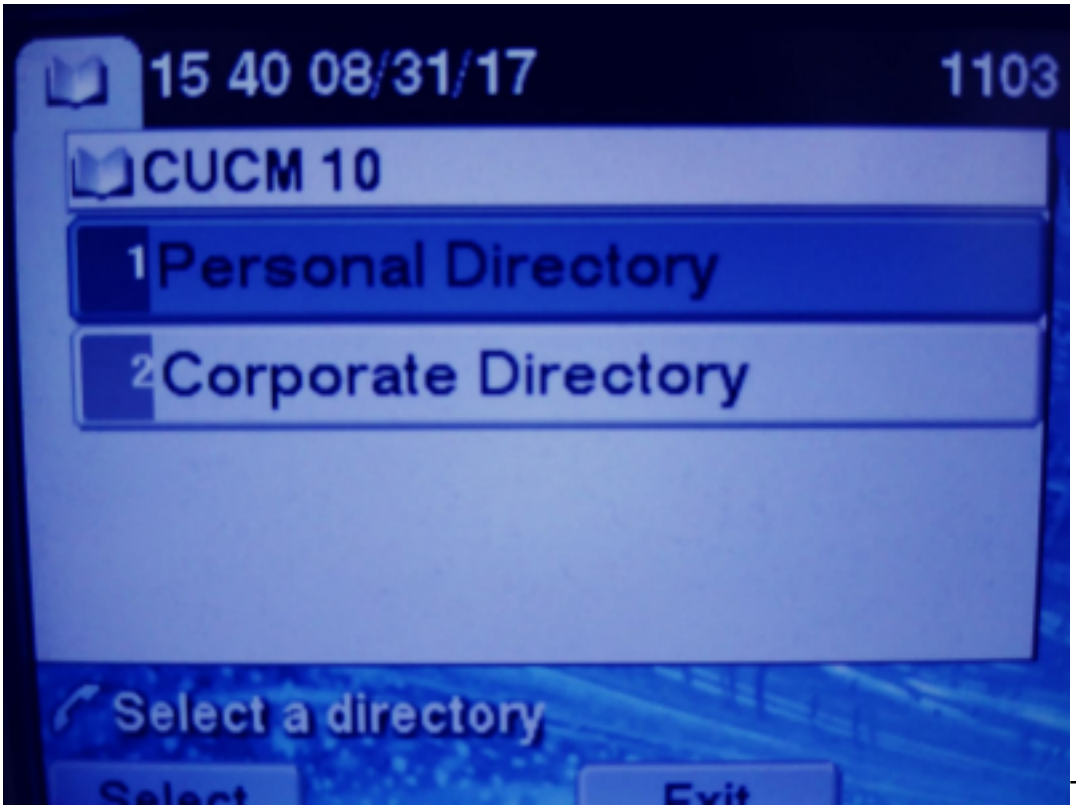
步骤2.订购电话服务。

对**Device>Phone>>Subscriber/Unsubscribe服务的**Natigate。



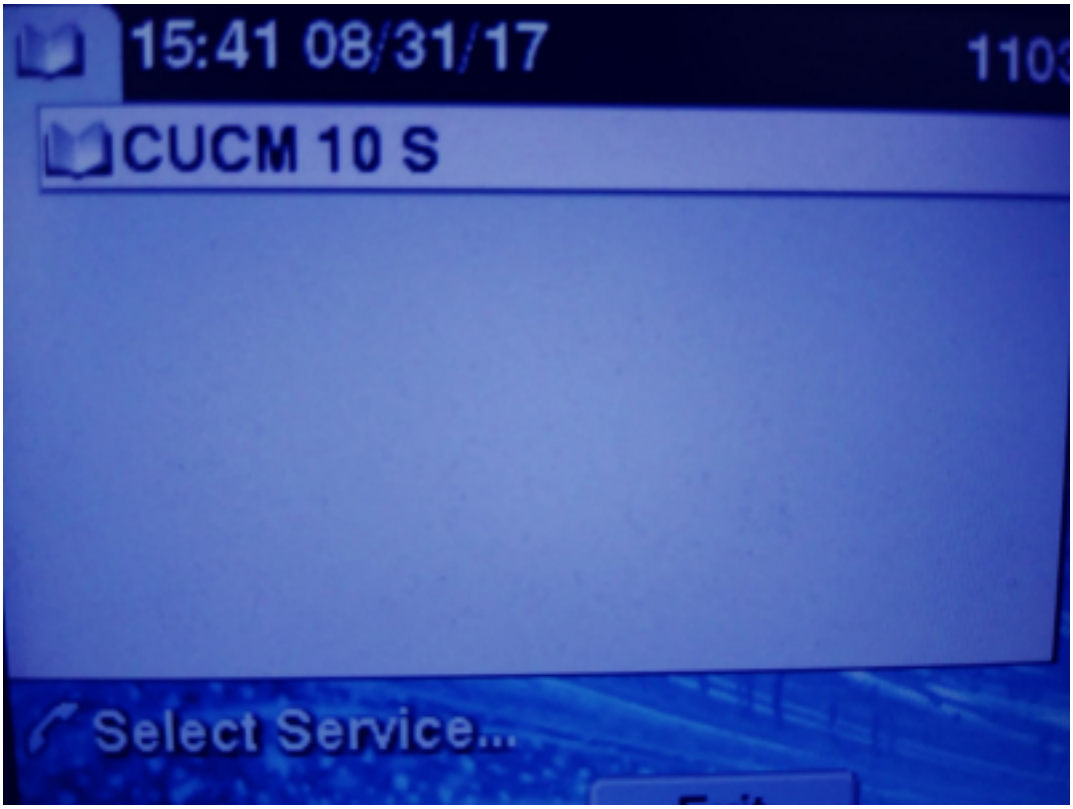
这时，如果应用程序提供HTTP，您一定能到达服务，但是https仍然不是。

HTTP



TTP

HTTPS



HTTPS将显示“主机没被找到的”错误由于这样的事实，服务不能为电话验证此的TV。

步骤3.上传外部服务证书对CUCM。

上传外部服务作为**仅Tomcat信任**。保证服务重置在所有节点。

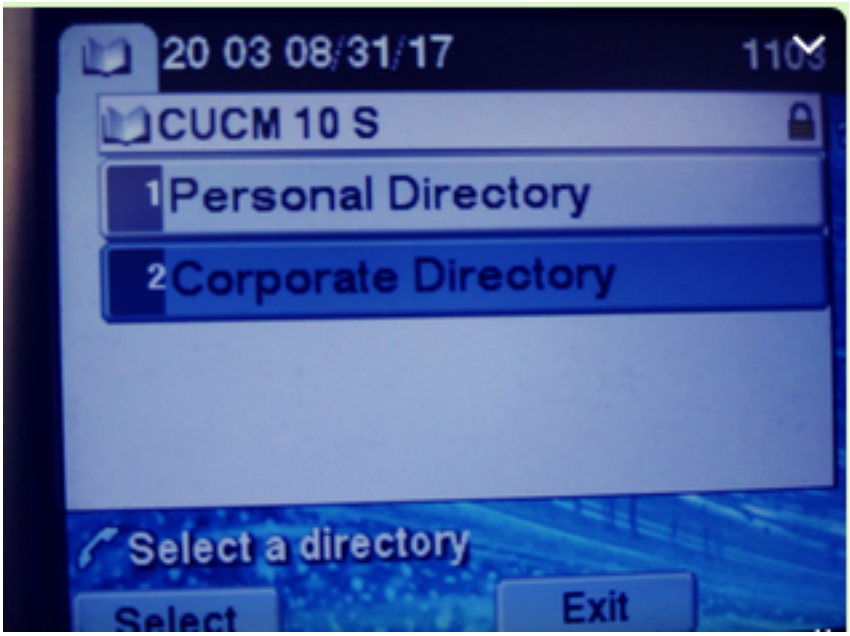
此种certs在电话没有存储，电话必须与TV服务相当协商发现是否建立HTTPS连接。

导航对**OS admin> Certificate>证书加载。**

从重置在所有节点的CUCM Tomcat服务的SSH。

```
admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
arted properly, execute the same command again.
Service Manager is running
```

在这些步骤以后，电话一定能访问HTTPS服务，不用问题



常见请询问问题(FAQ)

在证书交换后， HTTPS用“没找到的主机仍然失效”。

-请检查电话其寄存器并且保证您看到在节点的第三方证书的节点。

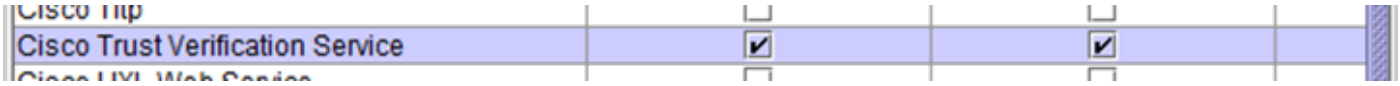
-重置在特定节点的Tomcat。

-请检查DNS，保证证书的普通的Name(CN)可以是解决的。

排除故障

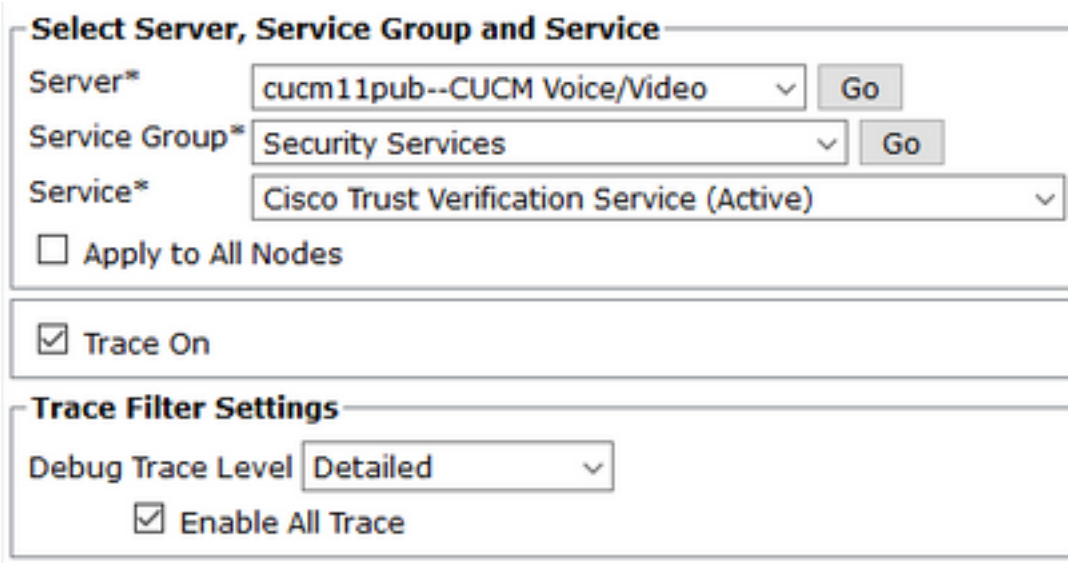
收集的CUCM TV日志必须提供您好信息

导航对**RTMT>System>Trace &记录中央印制厂>收集的日志文件**



注意：收集从所有节点的日志并且保证日志设置对详细的TV。

TV日志设置对详细



跟踪示例

```
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificate</table><tableid>46</tableid><action>I</action>
<user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>1504203457</cdrtim
e><pkid>e6148ee3-3eb5-e955-fa56-
2baa538a88fb</pkid><servername>cucm11pub</servername><subjectname>CN=10.201.192.12,OU=RCH,O=Cisc
o,L=RCH,ST=Tx,C=US</subjectname><issuername>CN=pablogon-
CA,DC=rcdncollab,DC=com</issuername><serialnumber>3d00000008230ded92f687ec03000000000008</serial
number><certificate></certificate><ipv4address>10.201.192.13</ipv4address><ipv6address></ipv6add
ress><timetolive>NULL</timetolive><tkcertificatedistribution>1</tkcertificatedistribution><ifx_r
eplcheck>6460504654345273346</ifx_replcheck></new></msg>
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificate" has been changed
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Looking up the
roles for
11:17:38.291 |   debug Pkid : fead9987-66b5-498f-4e41-c695c54fac98
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - DBChange Notification
received
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificatetrustrolemap</table><tableid>50</tableid><actio
n>I</action><user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>150420
3457</cdrtime><pkid>5ae6e1d2-63a2-4590-bf40-1954bfa79a2d</pkid><fkcertificate>e6148ee3-3eb5-
e955-fa56-
2baa538a88fb</fkcertificate><tktrustrole>7</tktrustrole><ifx_replcheck>6460504654345273346</ifx_
replcheck></new></msg>
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificatetrustrolemap" has been changed
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:46.811 |   debug updateLocalDBCache : Refreshing the local DB certificate cache
11:34:00.131 |   debug Return value after polling is 1
11:34:00.131 |   debug FD_ISSET i=0, SockServ=14

11:34:00.131 |   debug Accepted TCP connection from socket 0x00000014
```