TLS VCS Web接口的握手失败

目录

简介

Cisco视频通信服务器(VCS)使用客户端证书认证和授权进程。因为允许安全一块已添加层，并且可以用于在目的的单个符号此功能是非常有用的对一些环境。然而，如果不正确地配置，它能锁定管理员在VCS Web接口外面。

在本文的步骤用于禁用在Cisco VCS的客户端基于认证的安全。

问题

如果客户端基于认证的安全在VCS启用和不正确地配置，用户也许不能访问VCS Web接口。尝试访问Web接口会见传输层安全(TLS)握手失败。

这是触发问题的配置更改：

解决方案

完成这些步骤为了禁用客户端基于认证的安全和返回系统到管理员能访问VCS的Web接口的状态：

1. 连接对VCS作为根通过安全壳SSH。
2. 请勿输入此命令作为根为了硬编码Apache使用客户端基于认证的安全：
   ```
   echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
   ```
   Note:在此命令被输入后， VCS不可能为客户端基于认证的安全重新配置，直到**removecba.conf文件**删除，并且VCS重新启动。
3. 您必须重新启动VCS为了此配置更改能生效。当您准备重新启动VCS时，请输入这些命令：
   ```
   tshell
   xcommand restart
   ```
   Note:这重新启动VCS并且下降所有呼叫/注册。
4. 一旦VCS重新加载，客户端基于认证的安全禁用。然而，它没有禁用用一个理想方式。登陆对与一个读写管理帐户的VCS。导航对在VCS的**System > System**页。

在VCS的系统管理页，请保证客户端基于认证的安全设置对“不需要的”：

一旦此变动做，请保存更改。

5. 一旦完整，请输入此命令作为在SSH的根为了重新设置Apache到正常：
   ```
   rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
   ```
   警告：如果跳到此步骤，您不能重新启用客户端基于认证的安全。
6. 再次重新启动VCS为了验证步骤工作。即然您访问Web访问，您能重新启动从Web接口的VCS在**维护>重新启动下**。

祝贺!您的VCS以客户端禁用的基于cerificate的安全当前运行。