VCS Web界面上的TLS握手失败

目录

简介

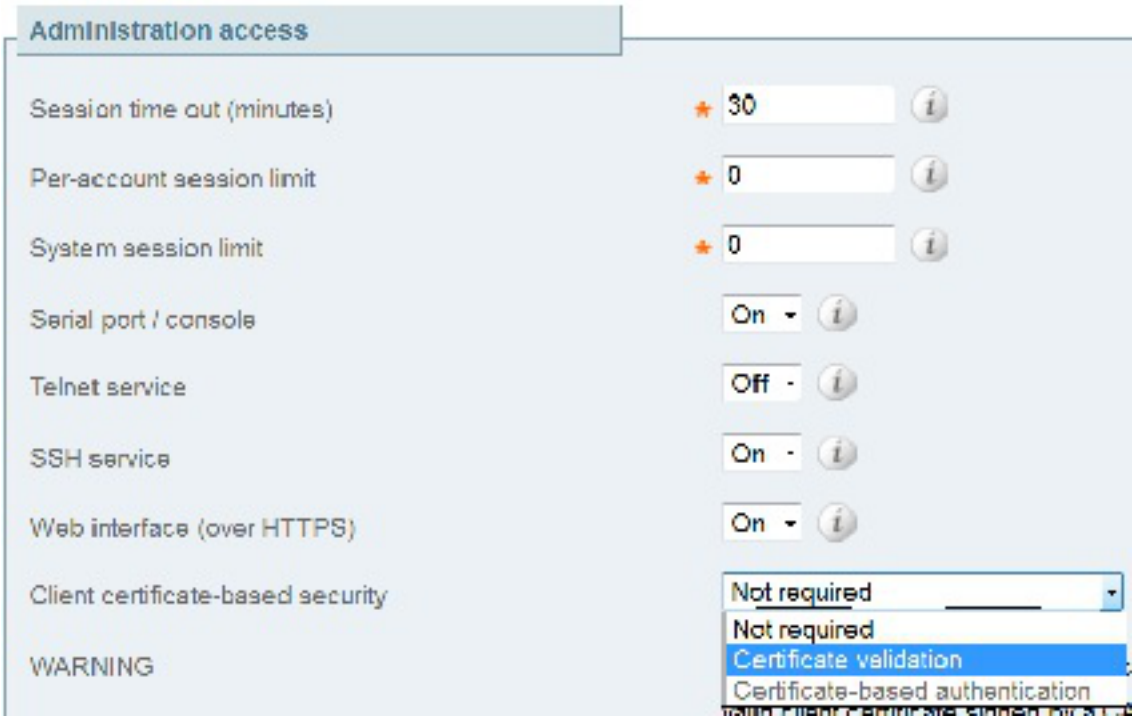
思科视频通信服务器(VCS)使用客户端证书进行身份验证和授权过程。此功能对于某些环境非常有用，因为它允许增加一层安全性，并可用于单点登录。但是，如果配置错误，它会将管理员锁定在VCS Web界面之外。

本文档中的步骤用于在Cisco VCS上禁用基于客户端证书的安全性。

问题

如果VCS上启用了基于客户端证书的安全，并且配置不正确，用户可能无法访问VCS Web界面。尝试访问网络界面时遇到传输层安全(TLS)握手失败。

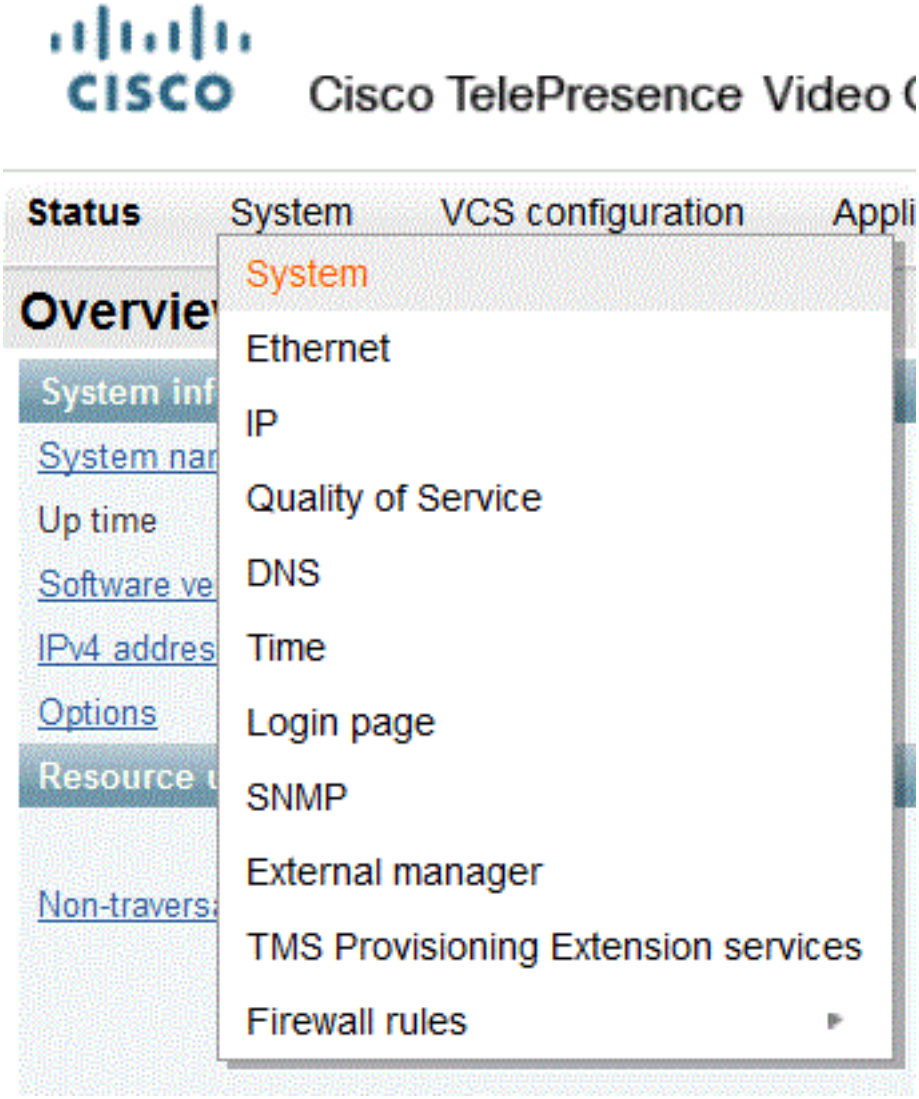
以下是触发问题的配置更改：



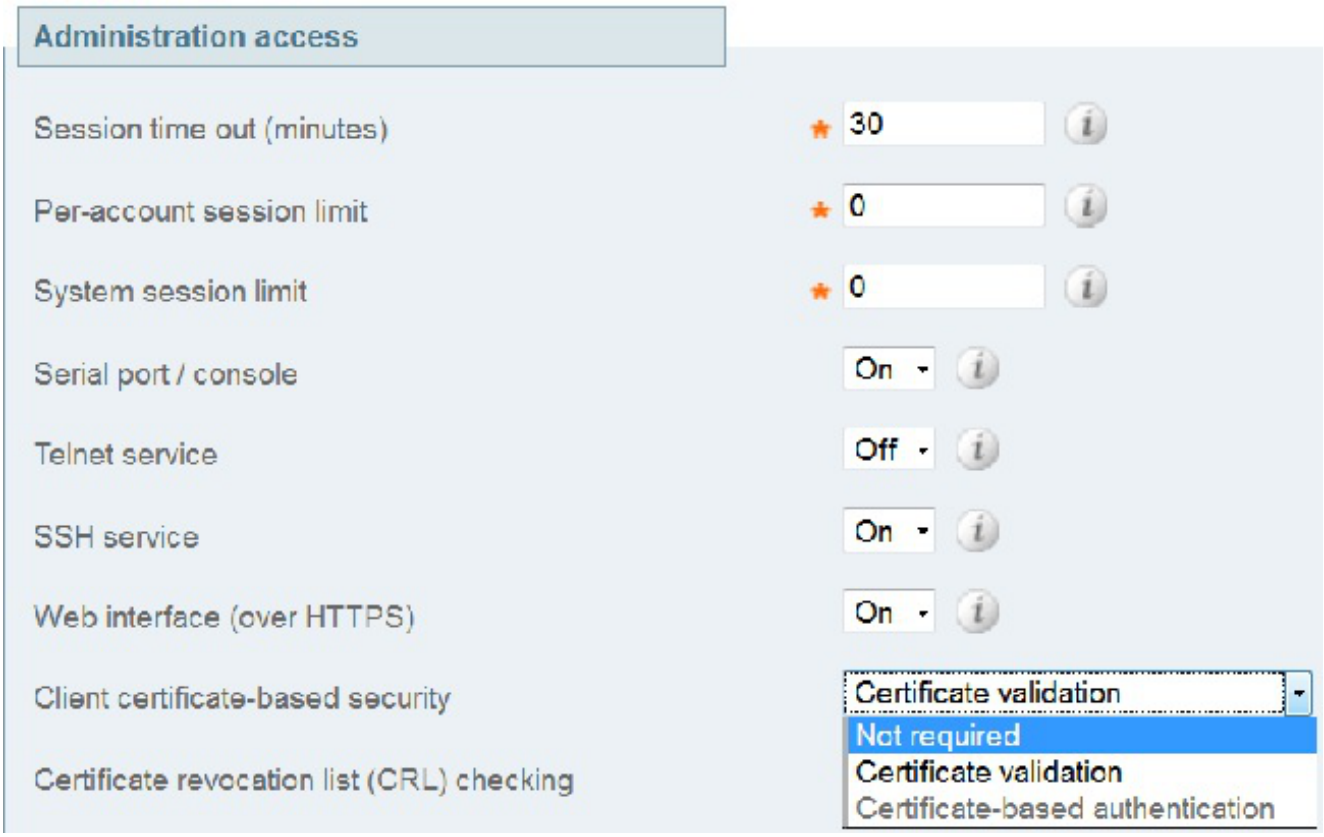
解决方案

要禁用基于客户端证书的安全并使系统恢复到管理员能够访问VCS Web界面的状态，请完成以下步骤：

1. 通过Secure Shell(SSH)以根连接到VCS。
2. 输入此命令作为根，以便硬编码Apache不能使用基于客户端证书的安全：
   ```
   echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
   ```
   注意：输入此命令后，在删除removecba.conf文件并重新启动VCS之前，无法将VCS重新配置为基于客户**端证书的**安全性。
3. 必须重新启动VCS，此配置更改才能生效。准备好重新启动VCS时，输入以下命令：
   ```
   tshell
   xcommand restart
   ```
   注意：这将重新启动VCS并丢弃所有呼叫/注册。
4. 一旦VCS重新加载，基于客户端证书的安全功能将被禁用。但是，它并非以理想方式禁用。使用读写管理员帐户登录VCS。导航至VCS**上的System > System**页面。



在VCS的系统管理页面上，确保Client certificate-based security（基于客户端证书的安全）设置为“Not required”（不需要）：



进行此更改后，保存更改。

5. 完成后，在SSH中以root身份输入以下命令，以将Apache重置为正常：
   ```
   rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
   ```
   警告：如果跳过此步骤，则永远无法重新启用基于客户端证书的安全性。
6. 再次重新启动VCS，以验证该过程是否正常运行。现在，您可以通过Web访问，从Maintenance > **Restart**下的Web界面重新启动VCS。

Congratulations!您的VCS现在在禁用基于客户端证书的安全的情况下运行。