NAC(CCA) ：如何在CAM/CAS升级到4.1.6以后解决认证错误

目录

简介

本文描述如何改正在Clean Access管理器(CAM) /Clean接入服务器(CAS)的证书错误有版本4.1.6的。

先决条件

要求

思科建议您有升级进程的知识思科网络准入控制(美洲台)设备的。

使用的组件

本文档中的信息根据与CAM/CAS的Cisco NAC设备版本4.1.6。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

步骤

这些证书错误在*/perfigo/logs/perfigo-redirect.log0.log.0*或*/perfigo/logs/perfigo-log0.log.0*被找到。

这是验证错误的示例：

```
SEVERE: RMISocketFactory:Creating RMI socket failed to host
        10.1.20.10:sun.security.validator.ValidatorException:
        Certificate chaining error
Aug 1, 2008 1:41:22 PM com.perfigo.wlan.web.admin.ConnectorClient connect
SEVERE: Communication Exception : java.rmi.ConnectIOException: Exception
        creating connection to: 10.1.20.10; nested exception is:
 javax.net.ssl.SSLHandshakeException:
        sun.security.validator.ValidatorException: Certificate chaining error
```

这些错误是在4.1.6做的安全性增强结果。在4.1.6， CAS和CAM彼此作为客户端和服务器并且必须互相委托。每一个要求根和中间证书从其他。例如，如果CAS有Verisign认证和CAM有一Perfigo (临时)证书， CAS和CAM需要Verisign一系列(根和半成品)和Perfigo根。

完成这些步骤为了改正证书错误：

1. 备份不是临时证书的所有已安装证书。在CAM，请打开Web接口，并且去**Administration > CCA Manager> SSL > X509证书**。在CAS，请去直接地Web接口通过https:// <CAS IP>/admin，然后去**Administration > SSL > X509证书**。从选择选择**出口CSR/Private密钥/证书**操作下拉列表。点击在预装证书旁边当前查找的**出口**，并且保存此文件。点击在当前安装的专用密钥旁边查找的**出口**，并且保存此文件。
2. 在备份，如果CAS和CAM已经不使用临时证书后，生成他们。在CAM，请打开Web接口，并且去**Administration > CCA Manager> SSL > X509证书**。在CAS，请去直接地Web接口通过https:// <CAS IP>/admin，然后去**Administration > SSL > X509证书**。选择**生成**从下拉列表的**临时证书**。填写列出的字段，并且单击**生成**。**注意：** 这不再要求重新启动生效。
3. 从CAS和CAM取消所有信任证书权限。此步骤使更加容易管理和改进安全。在CAM，去**Administration > CCA Manager> SSL >信任证书权限**。在CAS，请去**Administration > SSL >信任证书权限**。创建过滤器排除Perfigo证书。从添加过滤器下拉列表选择**辨别名称**。选择**包含不**从在辨别名称旁边出现的下拉列表。在文本字段键入Perfigo，然后单击**过滤器**。从在删除选择的按钮旁边查找的下拉列表选择100。在删除选择的下拉列表之下单击复选框为了选择所有证书权限(CA)列表的。点击**选择的删除**为了删除在列表的所有CA。请继续点击方框，并且点击**选择的删除，**直到所有CA删除。
4. 在您删除所有CA后，必须导入根和中间证书。在CAM，去**Administration > CCA Manager> SSL >信任证书权限**。在CAS，请去**Administration > SSL >信任证书权限**。单击**浏览**，并且首先选择根证明。**注意：** 应该设置主题和发布者对同一个值。点击**导入**，并且CA在如下列表应该出现。执行所有半成品证书的同一个步骤。
5. 安装该CAS和CAM的证书您备份在第一步。在CAM，请打开Web接口，并且去**Administration > CCA Manager> SSL > X509证书**。在CAS，请去直接地Web接口通过https:// <CAS IP>/admin，然后去**Administration > SSL > X509证书**。从下拉列表选择**进口证明书**。单击从step1**浏览**，并且选择保存的证书。点击**加载**。单击**浏览**再，并且选择从step1保存的专用密钥。从文件类型下拉列表选择**专用密钥**，然后单击**加载**。单击**验证并且安装上传的证书**。**注意：** 此错误消息不将由这些步骤修复：

   ```
   SEVERE: SSLFilter:access deniedCN=cas1.domain.com,
           OU=Information Technologies, O=Company, ST=State,
           C=US:Netscape cert type does not permit use for SSL client
   ```

   如果日志包含此消息，您必须与证书供应商联系。必须补发证书Netscape Cert类型字段设置为SSL服务器和SSL客户端。

相关信息

- Cisco NAC设备支持页面
- 技术支持和文档 - Cisco Systems