有关如何生成过期单点登录证书的技术说明

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[问题：登录失败，出现“用户名或密码无效”](#)
[解决方案](#)

简介

本文档介绍如何生成已过期的单点登录(SSO)证书。

先决条件

要求

思科建议您了解CloudCenter 4.7.2.1之前的版本

使用的组件

本文档中的信息基于4.7.2.1之前的所有CloudCenter版本

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。

问题：登录失败，出现“用户名或密码无效”

尽管使用了正确的密码和用户名，但登录失败，并显示“无效的用户名或密码”。这是由过期的单点登录证书引起的。 4.7.2.1包含证书未过期的修复。

解决方案

更新证书的步骤：

步骤1.将附加文件(samlKeystore**.jks)**上传到CCM。在HA模式下，将文件上传到两个CCM。

```
# cd /usr/local/tomcat/webapps/ROOT/WEB-INF/lib/ & mkdir ./security
# cp /tmp/samlKeystore.jks security/
```

步骤2.重新打包Cliqr安全库。在本例中，我们使用4.7.2版。

```
# cp cliqr-security-4.7.2.jar ~/
# jar uf cliqr-security-4.7.2.jar security/samlKeystore.jks
# chown -R cliqruser:cliqruser cliqr-security-4.7.2.jar
# rm -rf security/
```

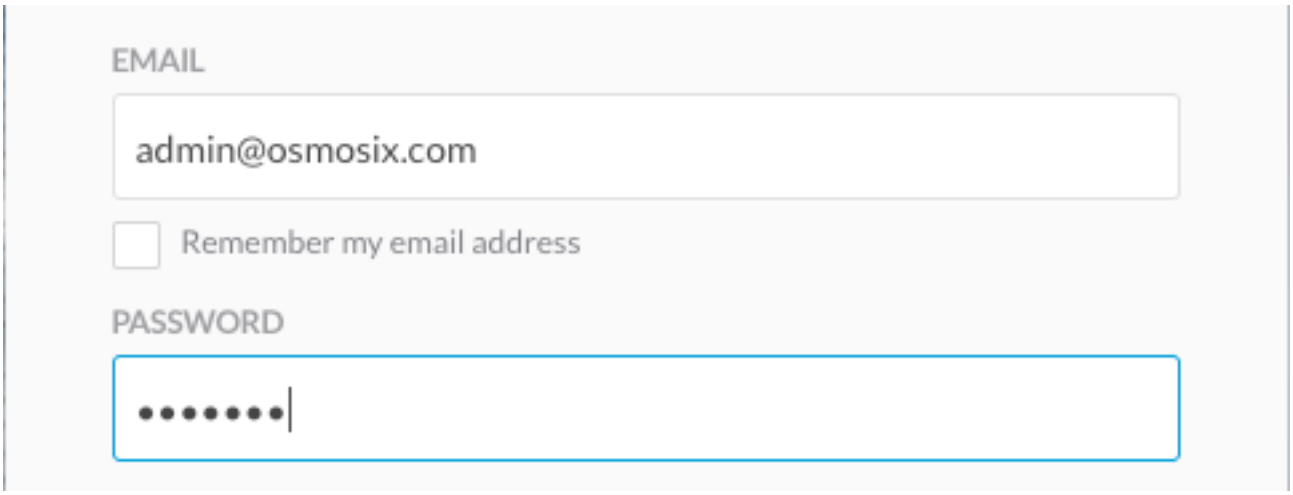
步骤3.在（主）CCM上重新启动Tomcat服务。

```
# /etc/init.d/tomcat restart
```

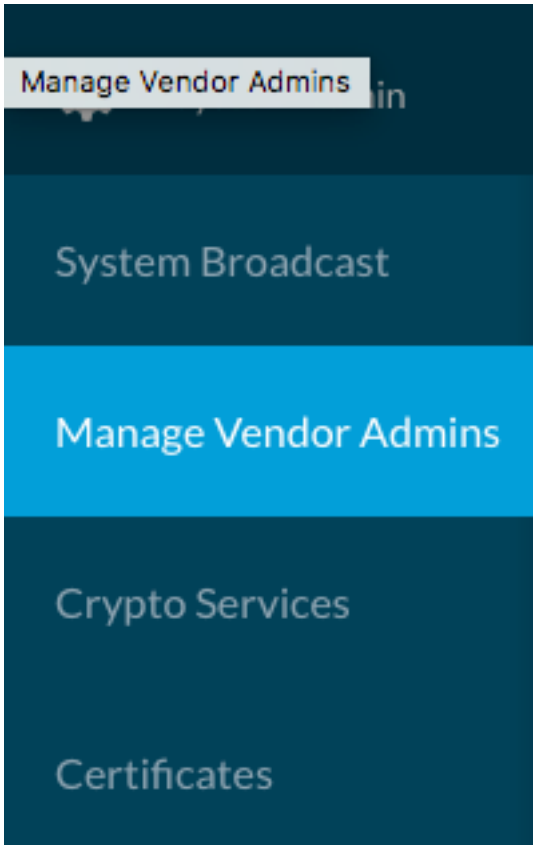
步骤4.在HA模式下，在辅助CCM上停止Tomcat服务。

```
# /etc/init.d/tomcat stop
```

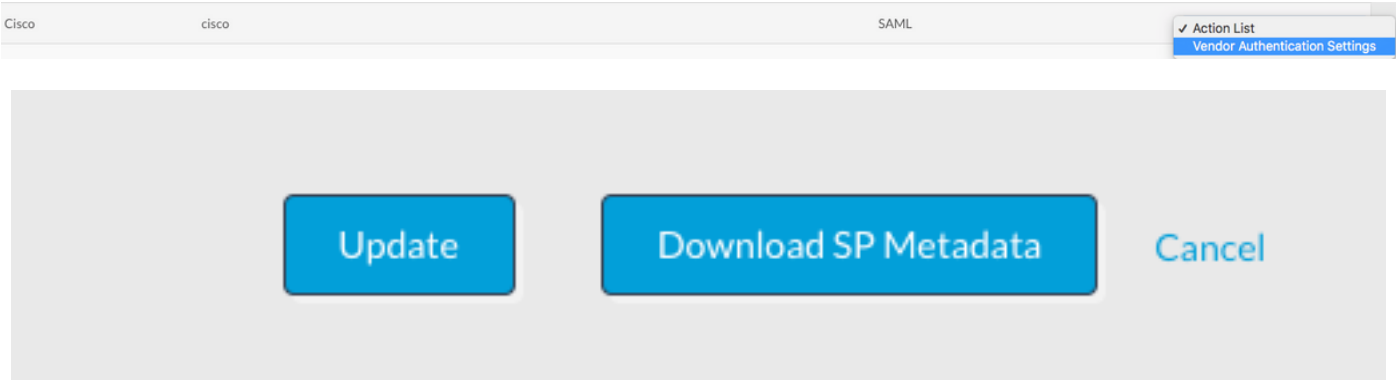
步骤5.使用admin@osmosix.com用户登录CCM。



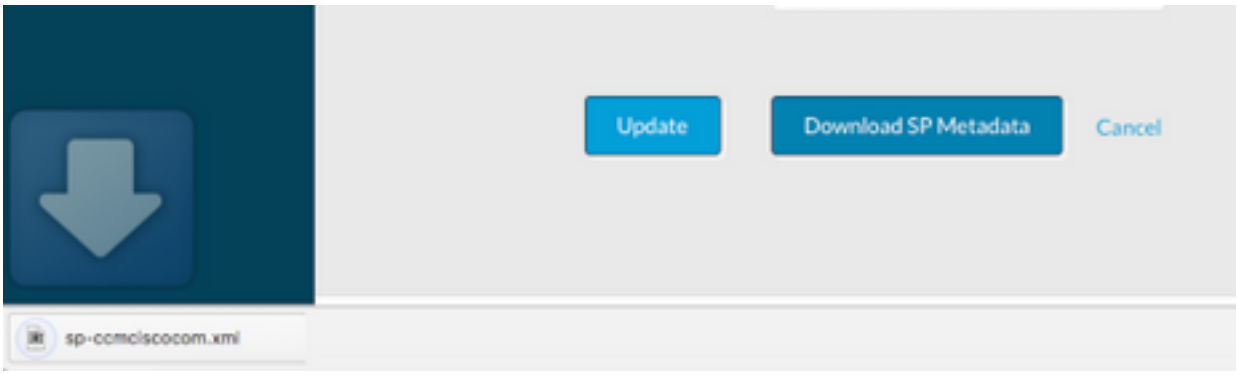
步骤6.单击“管理**供应商管理员**”。



步骤7.为租**户选**择Authentication settings，转到屏幕底部并单击**Update按钮**。这将更新相应的元数据文件。



步骤8.按下“下载SP元数据”按钮下载XML文件。



步骤8.1.对于HA模式，将xml文件从CCM1复制到CCM2，确保权限与CCM1相同。XML的位置

？在/usr/**local/osmosix/metadata/sp/中**。

```
From CCM1
# cd /usr/local/osmosix/metadata/sp
# scp <metadatafile>.xml root@CCM2:/usr/local/osmosix/metadata/sp
```

步骤8.2.在第二个CCM上启动Tomcat服务

```
From CCM2
# /etc/init.d/tomcat restart
```

步骤9.将XML文件上传到IDP。

步骤10.如果需要IDP的.cer文件，请打开XML文件，并将私钥和证书的值复制到文本文件中。将文本文件格式化为：

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
<value for private key>
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<value for certificate>
-----END CERTIFICATE-----
```

步骤11.通过登录验证解决方案。

注意：如果有多个租户，请为每个租户重复步骤4 - 8。