Nota Técnica em como gerar único expirado Sinal-no certificado

Índice

Introdução

Este documento descreve como gerar um único Sinal-no certificado (SSO) que expirou.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento da liberação previamente 4.7.2.1 de CloudCenter

Componentes Utilizados

A informação neste documento é baseada em todas as versões de CloudCenter antes de 4.7.2.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Problema: O início de uma sessão falha com “Nome de usuário inválido ou senha”

O início de uma sessão falha com “Nome de usuário inválido ou senha” apesar da senha e do username corretos que estão sendo usados. Isto é causado por um único expirado Sinal-no certificado. 4.7.2.1 inclui um reparo a onde os Certificados não expirem.

Solução

Etapas para atualizar o certificado:

Etapa 1. Transfira arquivos pela rede o arquivo anexado (**samlKeystore.jks) ao** CCM. Em caso do modo HA, transfira arquivos pela rede o arquivo a ambos os CCM.

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

Etapa 2. Repackage a biblioteca da Segurança de Cliqr. Neste exemplo, nós estamos usando a versão 4.7.2.

```
# 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/
```

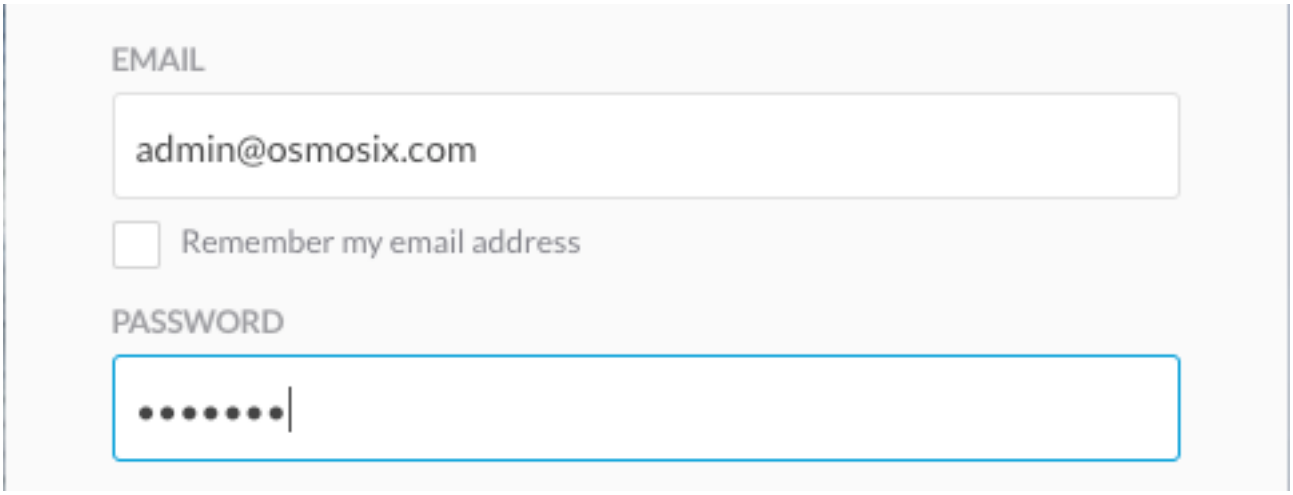
Etapa 3. Serviço de Tomcat do reinício no CCM (preliminar).

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

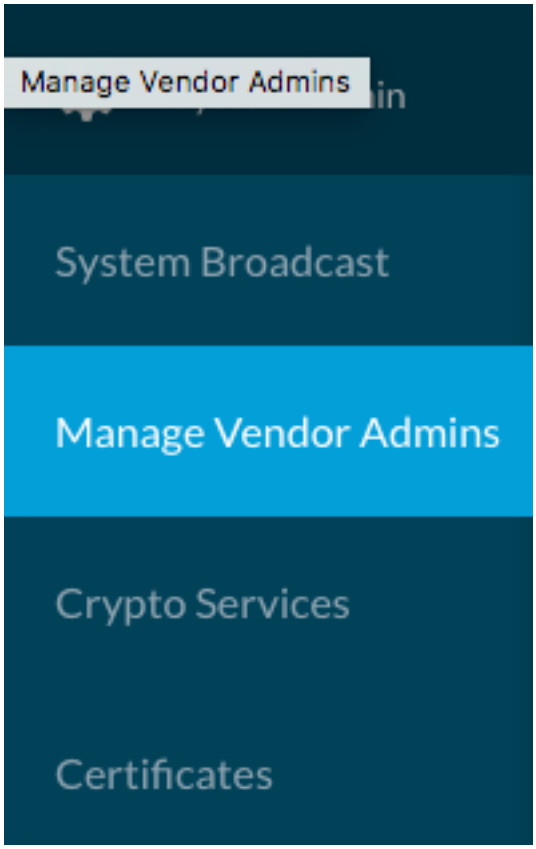
Etapa 4. Em caso do modo HA, pare o serviço de Tomcat no CCM secundário.

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

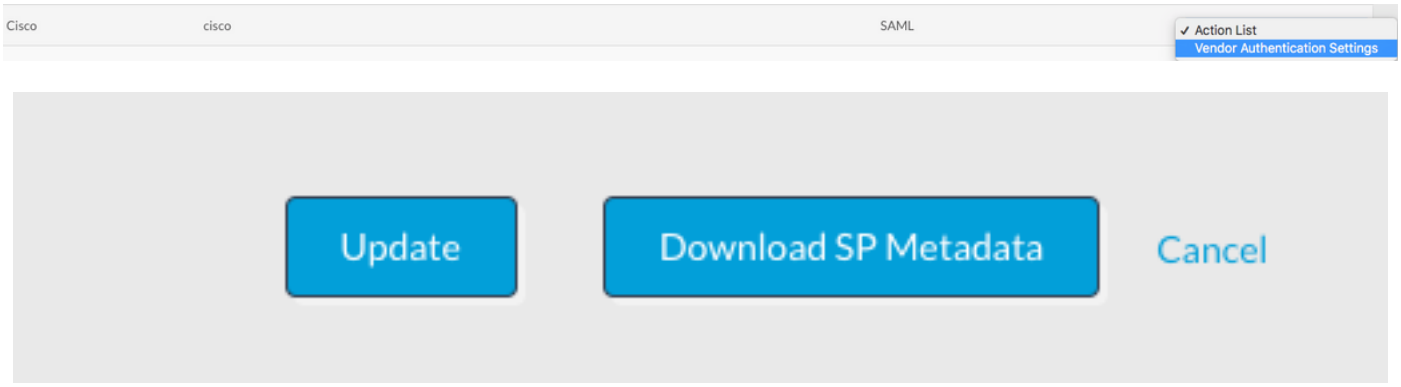
Etapa 5. Início de uma sessão ao CCM com usuário de admin@osmosix.com.



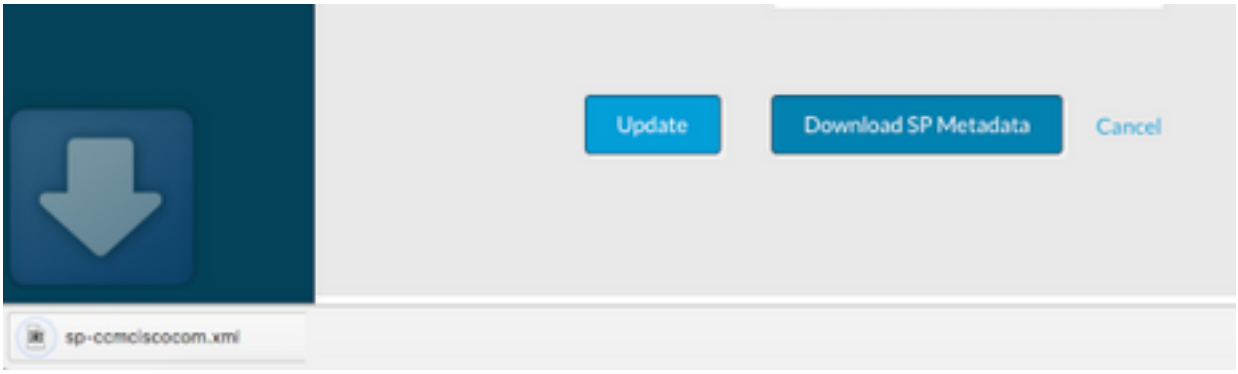
Etapa 6. Clique **controlam** sobre o **vendedor Admins**.



Etapa 7. Selecione **ajustes da autenticação** para o inquilino, vá à parte inferior da tela e clique sobre o **botão Update Button**. Isto atualiza o arquivo correspondente dos metadata.



Etapa 8. Pressione a transferência o botão dos Metadata SP para transferir o arquivo XML.



O modo da etapa 8.1.For HA, copia o arquivo do xml do CCM1 ao CCM2, certifica-se que as

permissões são as mesmas que o CCM1. Lugar do XML? está em **/usr/local/osmosix/metadata/sp/**.

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

Etapa 8.2. Comece o serviço de Tomcat no segundo CCM

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

Etapa 9. Transfira arquivos pela rede o arquivo XML a IDP.

Etapa 10. Se você precisa um arquivo de .cer para seu IDP, abra o arquivo XML, e copie os valores da chave privada e Certificate em um arquivo de texto. Formate o arquivo de texto como estes:

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

Etapa 11. Valide a solução entrando.

Nota: Em caso dos inquilinos múltiplos, repita etapas 4 - 8 para cada inquilino.