Note en tech sur la façon dont générer le certificat simple expiré d'ouverture de session

Contenu

Introduction

Ce document décrit comment générer un certificat simple de l'ouverture de session (SSO) qui a expiré.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la release antérieurement 4.7.2.1 de CloudCenter

Composants utilisés

Les informations dans ce document sont basées sur toutes les versions de CloudCenter avant 4.7.2.1

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème : La procédure de connexion échoue avec « le nom d'utilisateur ou mot de passe non valide »

La procédure de connexion échoue avec « le nom d'utilisateur ou mot de passe non valide » en dépit du mot de passe et du nom d'utilisateur corrects étant utilisés. Ceci est provoqué par par un certificat simple expiré d'ouverture de session. 4.7.2.1 inclut une difficulté à où les Certificats n'expirent pas.

Solution

Étapes pour mettre à jour le certificat :

Étape 1. Téléchargez le fichier relié (**samlKeystore.jks) au** CCM. En cas de mode ha, téléchargez le fichier aux les deux CDSM.

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

Étape 2. Remballez la bibliothèque de Sécurité de Cliqr. Dans cet exemple, nous utilisons la version 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/
```

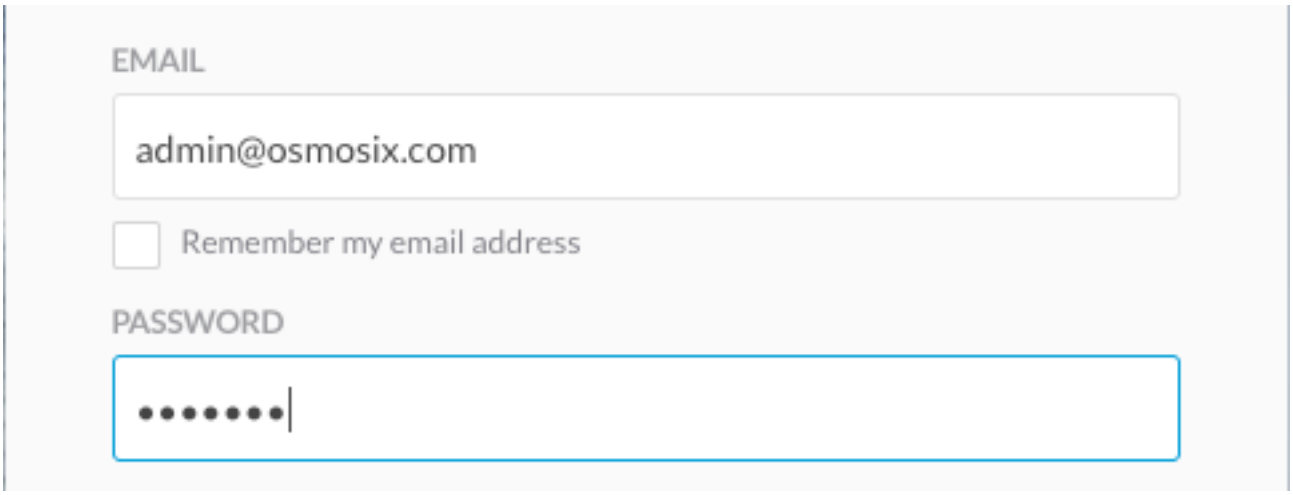
Étape 3. Service de Tomcat de reprise sur le CCM (primaire).

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

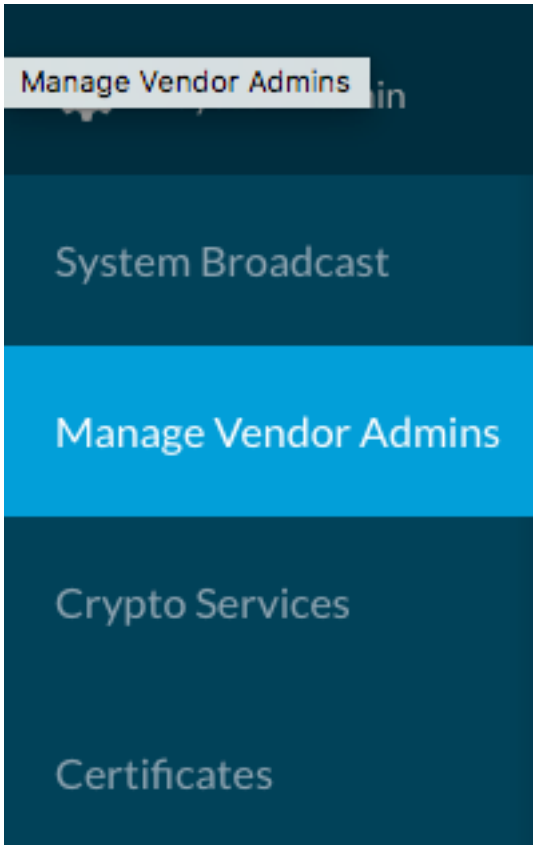
Étape 4. En cas de mode ha, arrêtez le service de Tomcat sur le CCM secondaire.

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

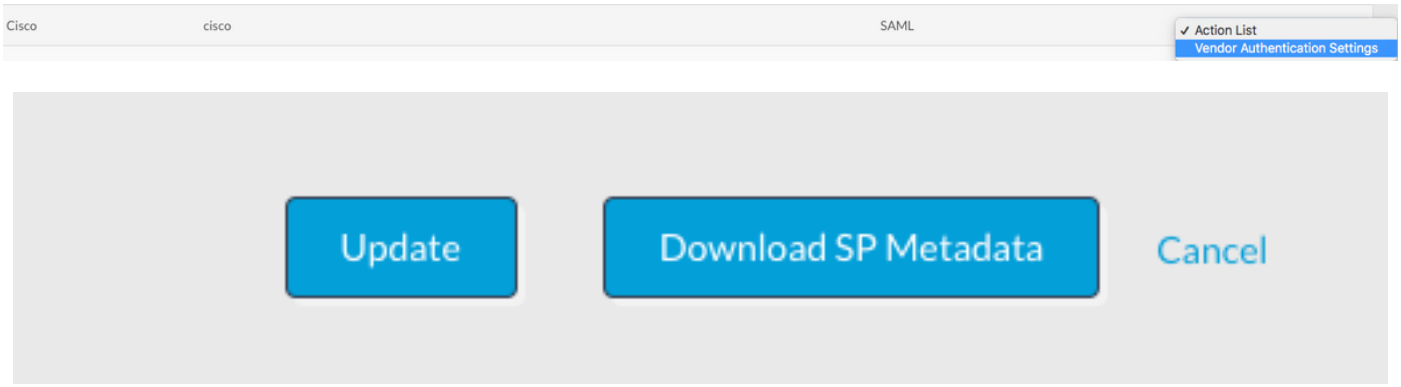
Étape 5. Procédure de connexion au CCM avec l'utilisateur d'admin@osmosix.com.



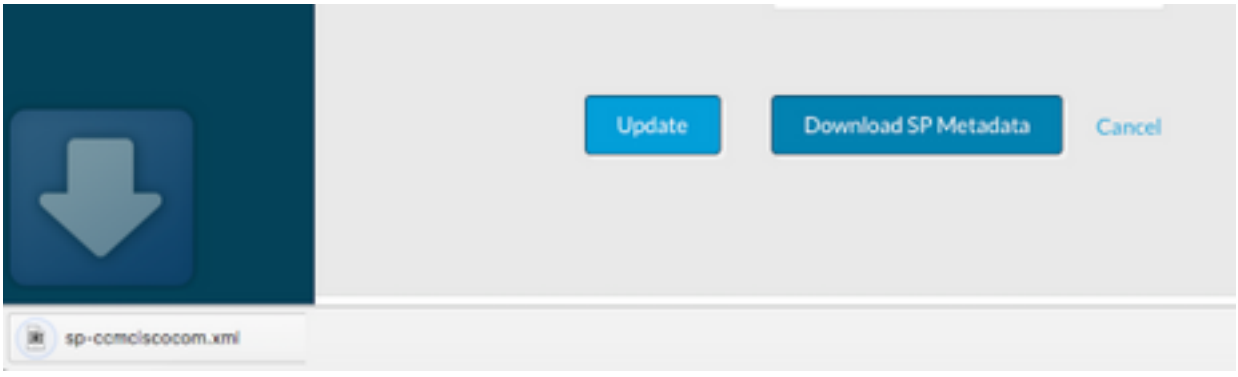
Étape 6. Cliquez sur **gèrent** en fonction des **admins de constructeur**.



Étape 7. Sélectionnez les **configurations d'authentification** pour le locataire, allez au bas de l'écran et cliquez sur en fonction le **bouton de mise à jour**. Ceci met le dossier à jour correspondant de métadonnées.



Étape 8. Appuyez sur le téléchargement que les métadonnées de fournisseur de services se boutonnent pour télécharger le fichier XML.



Le mode de l'étape 8.1.For ha, copient le fichier de xml de CCM1 sur CCM2, s'assurent que les autorisations sont identiques que CCM1. Emplacement du XML ? est dans **/usr/local/osmosix/metadata/sp/**.

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

Étape 8.2. Commencez le service de Tomcat sur CCM deuxième

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

Étape 9. Téléchargez le fichier XML à l'IDP.

Étape 10. Si vous avez besoin d'un fichier de .cer pour votre IDP, ouvrez le fichier XML, et copiez les valeurs de la clé privée et les délivrez un certificat dans un fichier texte. Formatez le fichier texte en tant que ces derniers :

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

Étape 11. Validez la solution en ouvrant une session.

Remarque: En cas de plusieurs locataires, répétez les étapes 4 - 8 pour chaque locataire.