Technische opmerking over het genereren van het verloopcertificaat voor één aanmelding

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Probleem: Aanmelden mislukt met "Ongeldige gebruikersnaam of wachtwoord"](#)
[Oplossing](#)

Inleiding

In dit document wordt beschreven hoe u een verlopen aanmelding (Single Sign-On)-certificaat kunt genereren.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van CloudCenter release vóór 4.7.2.1

Gebruikte componenten

De informatie in dit document is gebaseerd op alle CloudCenter-versies vóór 4.7.2.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Probleem: Aanmelden mislukt met "Ongeldige gebruikersnaam of wachtwoord"

Aanmelden mislukt met "Ongeldige gebruikersnaam of wachtwoord" ondanks het juiste wachtwoord en de juiste gebruikersnaam die gebruikt wordt. Dit wordt veroorzaakt door een verlopen single aanmelding certificaat. 4.7.2.1 voorziet in een regeling voor de plaats waar de certificaten niet vervallen.

Oplossing

Stappen om het certificaat bij te werken:

Stap 1. Upload het aangehechte bestand (**samlKeystore.jks**) naar het CCM. Upload het bestand naar beide CCM's in het geval van de HA-modus.

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

Stap 2. Vervang de Clientbeveiligingsbibliotheek. In dit voorbeeld gebruiken we versie 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/
```

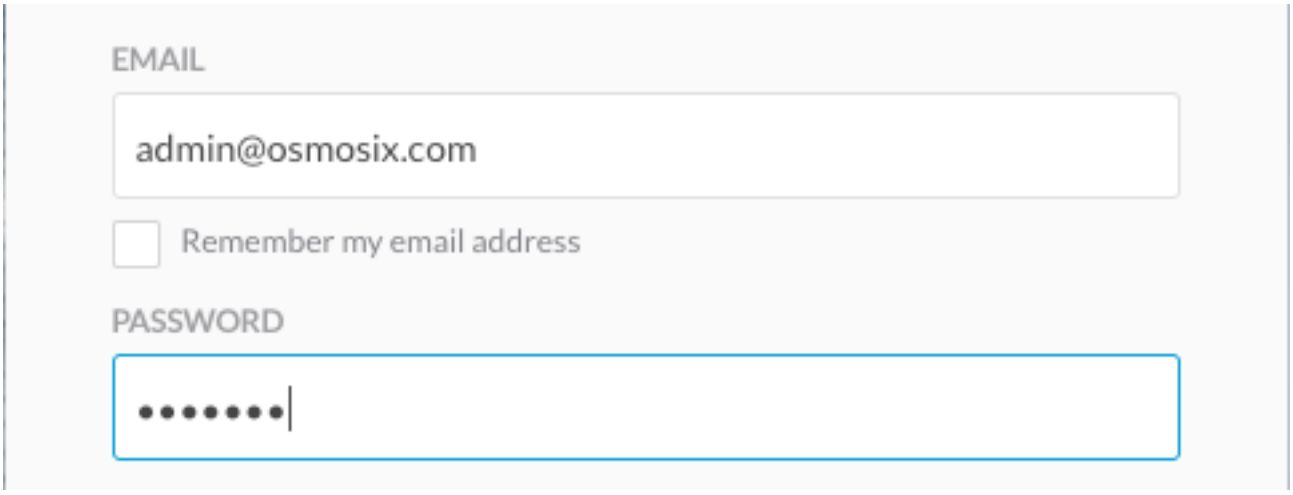
Stap 3. Start de Tomcat-service opnieuw op het (primaire) CCM.

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

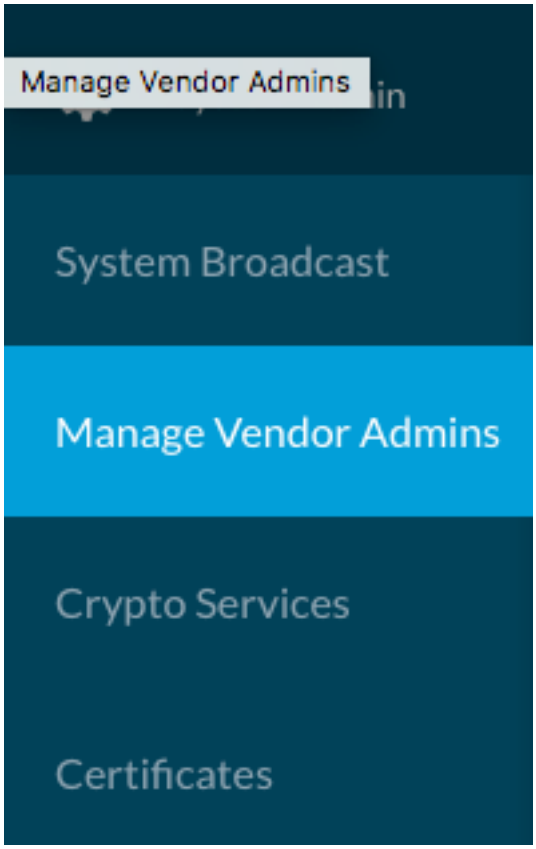
Stap 4. In het geval van de HA-modus, stop de Tomcat-dienst op het secundaire CCM.

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

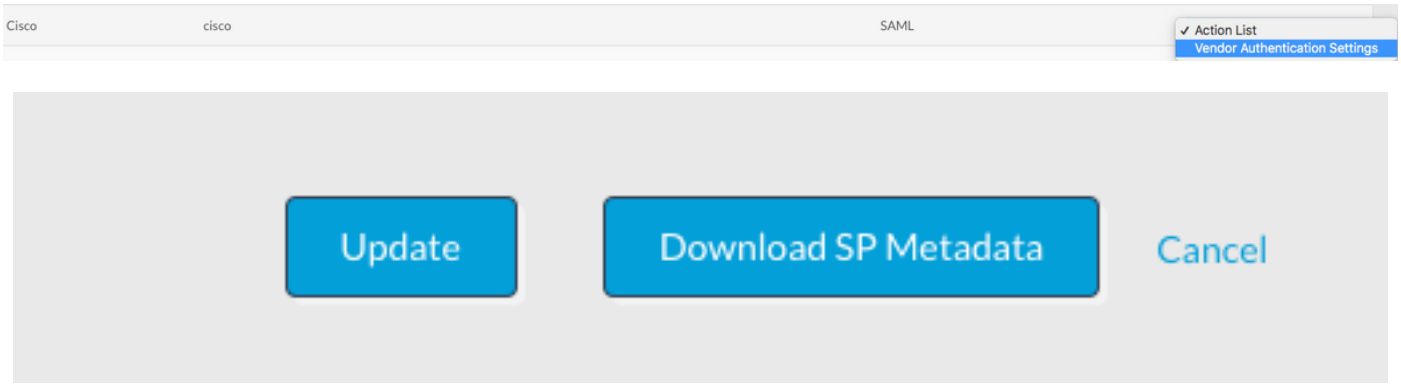
Stap 5. Meld u aan bij de CCM met de admin@osmosix.com-gebruiker.



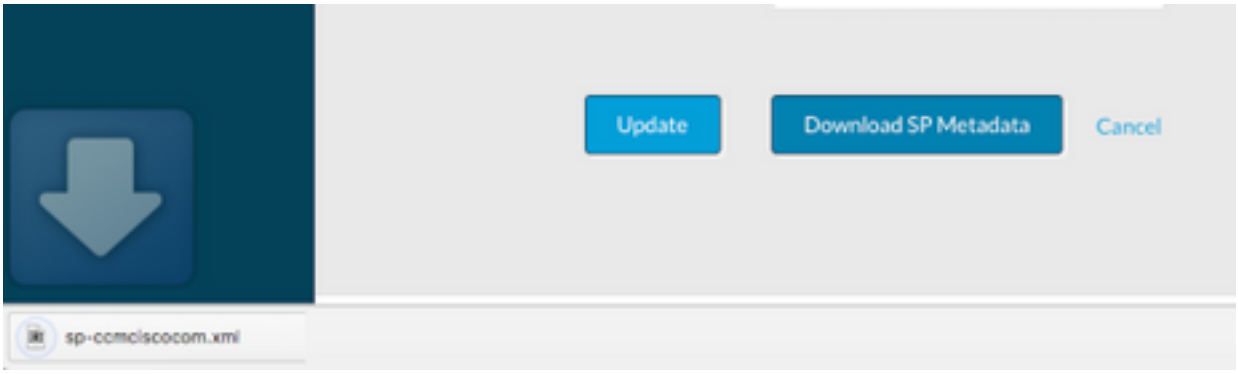
Stap 6. Klik op **Verkrachters beheren**.



Stap 7. Selecteer **Verificatieinstellingen** voor de huurder, ga naar de onderkant van het scherm en klik op de **knop Update**. Dit werkt het corresponderende metagegevensbestand bij.



Stap 8. Druk op de knop SP Metagegevens downloaden om het XML-bestand te downloaden.



Stap 8.1.Voor de HA-modus, kopieert u het bestand xml van CCM1 naar CCM2, zorg er dan

voor dat de permissies hetzelfde zijn als CCM1. Locatie van de XML? is in **/usr/local/osmosix/metadata/sp/**.

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

Stap 8.2. Start de Tomcat-dienst op het tweede CCM

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

Stap 9. Upload het XML bestand naar IDP.

Stap 10. Als u een .cer-bestand voor uw IDP nodig hebt, opent u het XML-bestand en kopieert u de waarden van de Private Key and certificaatbestand naar een tekstbestand. Opmaak het tekstbestand als volgt:

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

Stap 11. Vestig de oplossing door in te loggen.

Opmerking: Herhaal stap 4 - 8 voor elke huurder bij meerdere huurders.