Технические примечания о том, как генерировать истекший сертификат единой точки входа

Содержание

Введение

Этот документ описывает, как генерировать сертификат Единой точки входа (SSO), который истек.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с Выпуском CloudCenter предшествующие 4.7.2.1

Используемые компоненты

Сведения в этом документе основываются на всех версиях CloudCenter прежде 4.7.2.1

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Проблема: Вход в систему отказывает с "недопустимым именем пользователя или Паролем"

Вход в систему отказывает с "недопустимым именем пользователя или Паролем" несмотря на правильный пароль и используемое имя пользователя. Это вызвано сертификатом Единой точки входа с истекшим сроком. 4.7.2.1 включает исправление туда, где не истекают сертификаты.

Решение

Шагает для обновления сертификата:

Шаг 1. Загрузите прикрепленный файл **(samlKeystore.jks)** к CCM. В случае режима HA загрузите файл к обоим CCM.

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

Шаг 2. Повторно упакуйте библиотеку Cliqr Security. В данном примере мы используем версию 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/
```

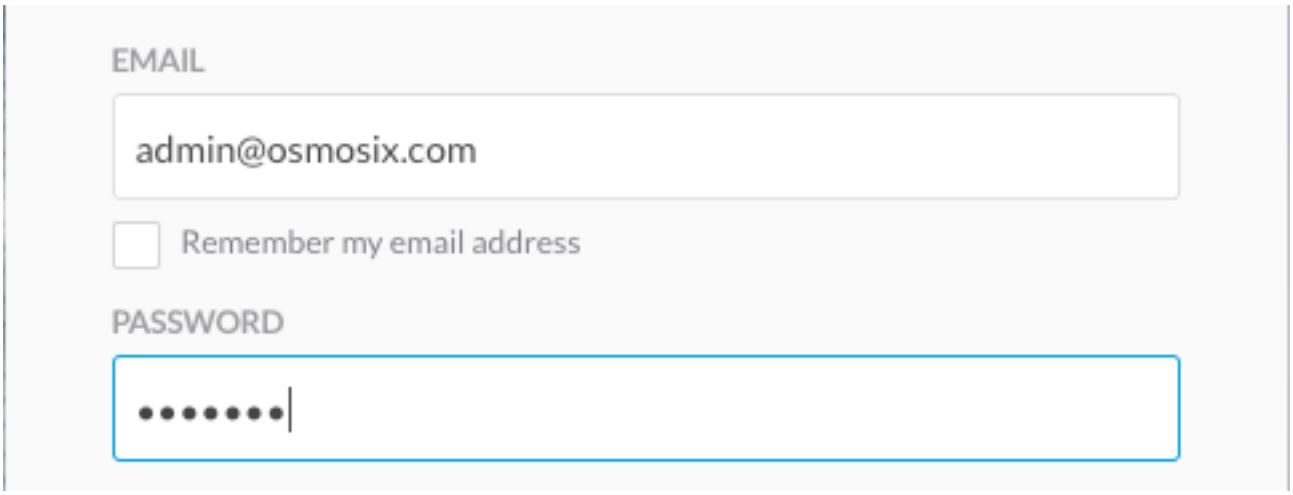
Шаг 3. Сервис Tomcat перезапуска на (основном) CCM.

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

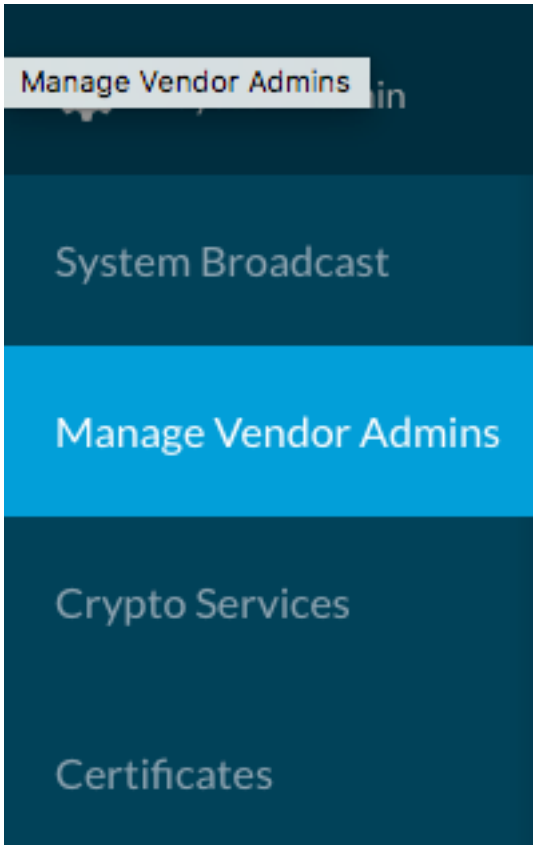
Шаг 4. . В случае режима HA остановите сервис Tomcat на вторичном CCM.

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

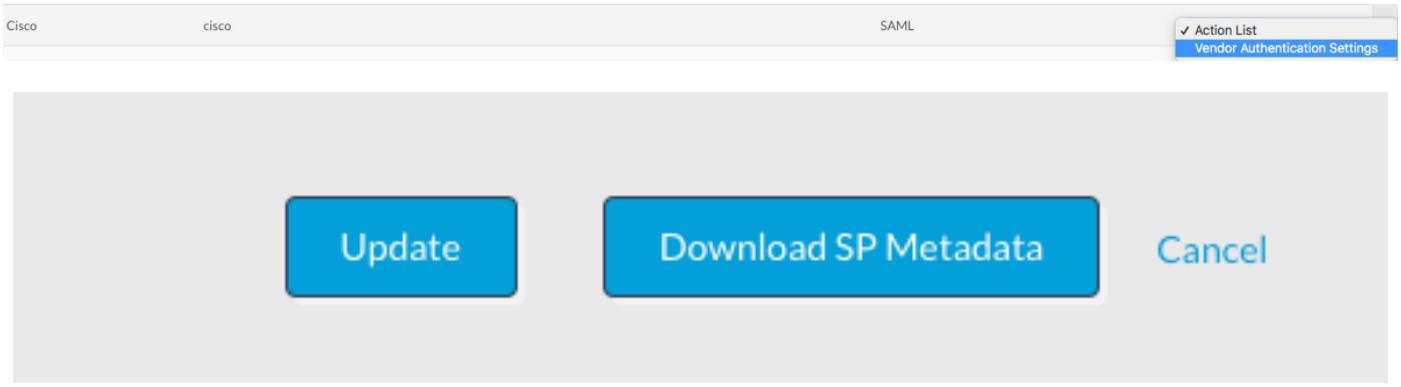
Шаг 5. . Войдите к CCM с admin@osmosix.com пользователем.



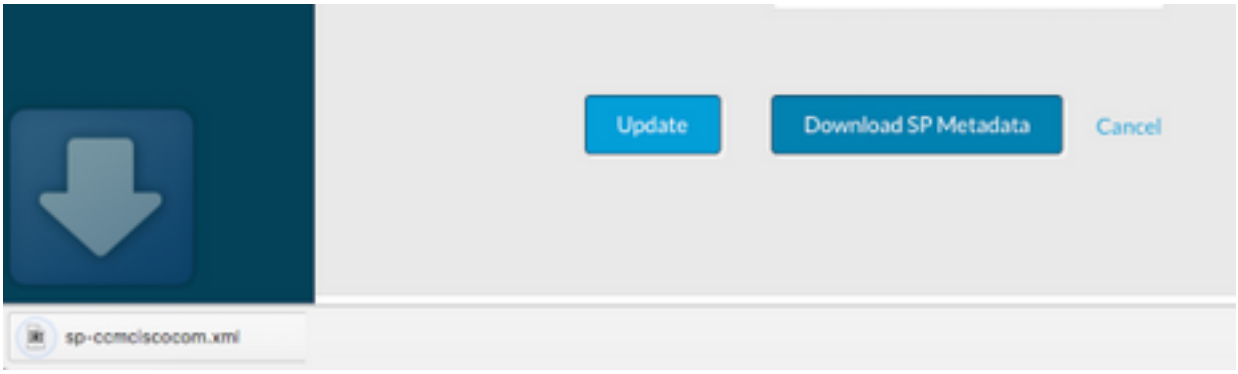
Шаг 6. Щелкните **по Manage Vendor Admins**.



Шаг 7. Выберите **Настройки аутентификации** для арендатора, перейдите к нижней части экрана и щелкните **по кнопке Update**. Это обновляет соответствующий файл метаданных.



Шаг 8. Нажмите кнопку Download the SP Metadata для загрузки XML-файла.



Шаг 8. 1. Для режима HA скопируйте файл xml от CCM1 до CCM2, удостоверьтесь, что

разрешения совпадают с CCM1. Местоположение XML находится в**/usr/local/osmosix/metadata/sp/**.

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

Шаг 8. 2. Запустите сервис Tomcat на втором CCM

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

Шаг 9. Загрузите XML-файл к IDP.

Шаг 10. Если вы нуждаетесь в .cer файле для своего IDP, открываете XML-файл и копируете значения Секретного ключа и Сертификата в текстовый файл. Отформатируйте текстовый файл как их:

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

Шаг 11. Проверьте решение путем регистрации.

> **Примечание:** В случае множественных арендаторов, Повторных шагов 4 - 8 для каждого арендатора.