"Статус HTTP 401 - Отказавшая Аутентификация: Ошибка, проверяющая SAML, обменивается сообщениями" когда Вы SSO Использования

Содержание

Введение

Этот документ описывает проблему, где вы получаете "Статус HTTP 401" сообщение об ошибках после периода бездействия при использовании Единой точки входа (SSO).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- SSO
- Сервис федерации Active Directory (AD FS)
- CloudCenter

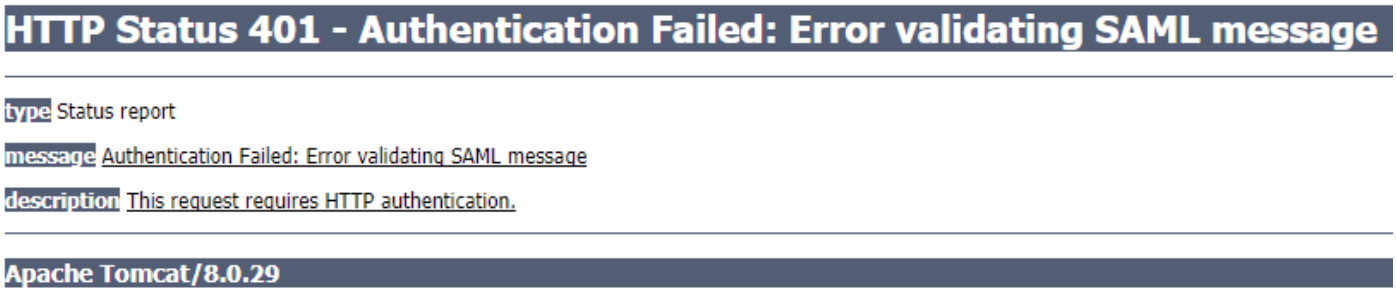
Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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

При использовании Единой точки входа можно получить "401" ошибка после периода бездействия вместо приглашения для регистрации снова как показано в образе.



Единственный путь к вам, чтобы быть в состоянии войти снова состоит в том, чтобы закрыть весь web-браузер и вновь открыть его.

Решение

Это вызвано несоответствием в значениях таймаута между CloudCenter и сервером SSO.

Будущее усовершенствование позволяет поддержку Параметров ForceAuthn, которая может позволить несоответствию между двумя значениями и CloudCenter выходить из системы корректно. Это усовершенствование может быть отслежено herehttps://bst.cloudapps. cisco . com/bugsearch/bug/CSCvg36752.

Единственный обходной путь должен удалить несоответствие. Существует три местоположения, где должны совпасть значения таймаута. Первые два находятся на самом CCM.

- Перейдите к**/usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml**.
- Модифицируйте **<session-timeout> time_In_Minutes </session-timeout>** для отражения таймаута, желаемого в минутах.
- Перейдите к**/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties**.
- Модифицируйте **saml.maxAuthenticationAge.seconds=timeout_in_seconds** для отражения таймаута, желаемого в секундах.

Третье находится на сервере SSO, и местоположение может варьироваться, который зависит от того, какой сервер SSO работает. Веб-значение срока действия SSO должно совпасть с двумя значениями, настроенными на CloudCenter.

Как только все три совпадают, когда таймаут произошел, вы роняетесь к экрану входа в систему, прежде чем позволено просмотреть страницу.