Настройка SSO SAML с примером конфигурации проверки подлинности Kerberos

Содержание

Введение

Этот документ описывает, как настроить Сервис Федерации Active Directory и Active Directory (AD FS) Версия 2.0, чтобы позволить ему использовать проверку подлинности Kerberos Клиентами Jabber (Только Microsoft Windows), который позволяет пользователям входить с их Входом в систему Microsoft Windows и не предлагаться для учетных данных.

> **Внимание. :** Этот документ основывается на лабораторной среде и предполагает, что вы знаете о влиянии изменений, которые вы вносите. См. документацию соответствующего продукта для понимания влияния изменений, которые вы вносите.

Предварительные условия

Требования

Cisco рекомендует иметь:

- AD Версия 2.0 FS , установленная и настроенная с продуктами Cisco Collaboration как Полагающийся Партийное Доверие
- Продукты совместной работы, такие как IM Cisco Unified Communications Manager (CUCM) и Присутствие, Cisco Unity Connection (UCXN) и CUCM включили для использования Единой точки входа (SSO) Языка разметки утверждений безопасности

(SAML)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Active Directory 2008 (имя хоста: ADFS1.ciscolive.com)
- AD версия 2.0 FS (имя хоста: ADFS1.ciscolive.com)
- CUCM (имя хоста: CUCM1.ciscolive.com)
- Версия Microsoft Internet Explorer 10
- Версия 34 Mozilla Firefox
- Версия 4 скрипача Telerik

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.

Настройка

Настройте AD FS

1. Настройте AD Версию 2.0 FS с Сервисным главным именем (SPN) для включения компьютера клиента, на котором Jabber установлен для запроса билетов, который в свою очередь позволяет компьютеру клиента связаться с AD сервисом FS.

   См. AD FS 2.0: Как Настроить SPN (servicePrincipalName) для Учетной записи сервиса для получения дополнительной информации.

2. Гарантируйте, что конфигурация проверки подлинности по умолчанию для AD сервиса FS (в **C:\inetpub\adfs\ls\web.config**) является **Интегрированной Проверкой подлинности Windows**. Гарантируйте, что это не было изменено на **Основанную на форме Аутентификацию**.

3. Выберите **Windows Authentication** и нажмите **Advanced Settings** под правой панелью. В Расширенных настройках снятие **Включает аутентификацию Привилегированного режима**, удостоверьтесь, что Расширенная Защита **Выключено**, и нажмите **OK**.

4. Гарантируйте, что AD Версия 2.0 FS поддерживает и протокол Kerberos и LAN Manager NT (NTLM) протокол, потому что все клиенты He-Windows не могут использовать

Kerberos и полагаться на NTLM.

В правой панели выберите **Providers** и удостоверьтесь**, Выполняют согласование**, и **NTLM** присутствуют при Включенных Поставщиках:

Примечание: AD FS передает Выполнить согласование заголовок защиты, когда Интегрированная Проверка подлинности Windows используется для аутентификации запросов клиента. Выполнить согласование заголовок защиты позволяет клиентам выбрать между проверкой подлинности Kerberos и аутентификацией NTLM. Выполнить согласование процесс выбирает проверку подлинности Kerberos, пока одно из этих условий не истинно:

- Одна из систем, которая вовлечена в аутентификацию, не может использовать проверку подлинности Kerberos.

- Вызывающее приложение не предоставляет достаточные сведения для использования проверки подлинности Kerberos.

- Чтобы позволить Выполнить согласование процессу выбрать протокол Kerberos для сетевой проверки подлинности, клиентское приложение должно предоставить SPN, главное имя пользователя (UPN) или Network Basic Input/Output System (NetBIOS) учетное имя как целевое имя. В противном случае Выполнить согласование процесс всегда выбирает протокол NTLM как предпочтительный метод аутентификации.

Настройте браузер

Microsoft Internet Explorer

1. Гарантируйте, что **Internet Explorer > Усовершенствованный> Включает Интегрированную Проверку подлинности Windows**, проверен.

2. Добавьте AD URL FS под **Безопасностью> зоны Интранет> узлы**.

3. Добавьте CUCM, IMP и имена хоста Unity к **Безопасности> Надежные узлы**.

4. Гарантируйте, что **Интернет > Security Exporer>> Security Локального Intranet Параметры настройки> Проверка подлинности пользователя - Вход в систему** настроен для использования вошедшего учетные данные для интранет-сайтов.

Mozilla Firefox

1. Открытый Firefox и вводит **about:config** в строку адреса.

2. Нажмите **я буду осторожен, я обещаю!**

3. Дважды нажмите Привилегированное название **network.negotiate-auth.allow-non-fqdn** к **истинному** и **network.negotiate-auth.trusted-uris** к **ciscolive.com, adfs1.ciscolive.com** для изменения.

4. Близкий Firefox и вновь открылся.

Проверка

Чтобы проверить, что SPNs для AD сервера FS должным образом созданы, введите **setspn** команду и просмотрите выходные данные.

Проверьте, имеют ли клиентские компьютеры билеты Kerberos:

Выполните эти шаги для проверки, какая аутентификация (Kerberos или аутентификация NTLM) используется.

1. Загрузите программное средство Скрипача к своему клиентскому компьютеру и установите его.

2. Закройте все окна Microsoft Internet Explorer.

3. Выполните Программное средство Скрипача и проверьте, что **Вариант трафика Перехвата** включен под Меню Файл. Скрипач работает как транзитный прокси между клиентским компьютером и сервером и слушает весь трафик.

4. Открытый Microsoft Internet Explorer, просмотрите в свой CUCM и щелкните по некоторым ссылкам для генерирования трафика.

5. Вернитесь к главному окну Fiddler и выберите один из Кадров, где Результат **200** (успех), и вы видите Kerberos как Механизм аутентификации

6. Если Тип проверки подлинности является NTLM, то вы видите**, Выполняют**

согласование - NTLMSSP в начале кадра, как показано здесь.

Устранение неполадок

Если вся конфигурация и шаги проверки завершена, как описано в этом документе, и у вас все еще есть проблемы входа в систему, то необходимо консультироваться с Active Directory Microsoft Windows / AD Администратор FS.