Облачная веб-безопасность: настройте ADFS к Include Specific Groups во время аутентификации

Содержание

Введение

Этот документ описывает, как настроить Microsoft Active Directory Federated Services (ADFS) как Идентификационный Поставщик (IdP), который передает определенные подробные данные группы к сервису Облачной веб-безопасности (CWS) Cisco, а не полный список составов группы.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Облачная веб-Конфигурация безопасности с Порталом ScanCenter
- Аутентификация Языка разметки утверждений безопасности (SAML)
- Администрирование сервера Microsoft ADFS

Используемые компоненты

Сведения в этом документе основываются на версии 2.0 Microsoft ADFS, которая работает на Windows Server 2008 R2.

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.

Общие сведения

Когда процесс проверки подлинности между клиентским браузером происходит, сервер ADFS (IdP) и CWS (Поставщик услуг (SP)), вся информация зашифрована и добавлена к Строке URL в клиентском браузере. Это означает, что Строка URL более длинна, когда дополнительные сведения передаются CWS.

При настройке аутентификации SAML (с Microsoft ADFS) для использования с сервисом CWS необходимо настроить Полагающееся Партийное Доверие для введения информации о группе и имени пользователя. Облачная веб-Безопасность: Настройте пользователя/атрибуты группы с PingFederate и ADFS, Пока использование SAML описывает этот шаг более подробно.

Количество групп пользователь добавлено к увеличениям размер URL. Если пользователь принадлежит большому числу групп Active Directory (AD), URL растет до размера, посредством чего наложенное ограничение URL браузера достигнуто, и сбои процесса проверки подлинности.

Каждый браузер мог бы определить их собственную максимальную позволенную длину URL. RFC 2616 не задает максимальную длину, но практические ограничения наложены поставщиками браузера.

> **Примечание:** Не возможно явно определить максимальное число групп, потому что у группы нет фиксированного номера символов. Например, GroupA имеет меньше символов, чем Test_Group_A. Определить много групп, который остается ниже предела URL, зависит от счетчика символов Доменного имени + Имя группы.

Настройка

Можно настроить сервер Microsoft ADFS для включения определенных групп в процесс проверки подлинности. Как правило, вы выбрали бы только группы, используемые в веб-Правилах фильтрации CWS. Когда вы выполняете аудит политики, которая существует, он помогает определять группы, которые уже используются.

И новый и развертывания, которые уже существуют, должен придерживаться конфигурации оптимального метода, которая предоставляет эти преимущества:

- Поддерживает размер URL к минимуму
- Ускоряет процесс проверки подлинности между IdP (ADFS) и SP (CWS)
- Сохраняет пропускную способность на каждом запросе аутентификации

Конфигурация оптимального метода

Открытые Тресты Поставщика Требований и создают два Принятия, Преобразовывают Правила:

Шаблон правила Требования использования Передает атрибуты LDAP как Требования

Хранилище атрибута: AD;

Атрибут LDAP: маркерные группы - неполные названия;

Исходящий тип требования: группа

Шаблон правила Требования использования Передает атрибуты LDAP как Требования

Хранилище атрибута: AD;

Атрибут LDAP: учетное имя SAM;

Исходящий тип требования: Name

Создайте Выпуск, Преобразовывают Правила путем открытия Полагающихся Трестов Части, и создание два Преобразовывает Правила:

Используйте Преобразовывают входящий шаблон требования

Входящий тип Требования: Name

Формат: неуказанный

Исходящий тип требования: ID Названия

Формат: неуказанный

Выберите Pass через все значения требования

Используйте Passthrough или Фильтр входящее Требование

Входящий тип Требования: Группа

Выберите Pass через только значения требования, которые запускаются с определенного значения:

Задайте свои AD имена групп

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- В то время как вошли как конечный пользователь, перейдите к http://whoami.scansafe.net.
- Выходные данные должны перечислить только группы, заданные в ранее упомянутой процедуре, а не полном списке составов группы.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.