Уведомление приложений о событиях RooX UIDM (webhooks)

Оглавление

RooX UIDM позволяет уведомлять серверные приложения о некоторых событиях, которые произошли в нем.

Список событий

- **Сессия прекращена**. Отправляется когда сессия была прекращена по любой причине, в том числе когда истекло время жизни, когда пользователь явно запросил завершение или пользователь был заблокирован.
- **Приложение заблокировано целиком**. Всю приложение заблокировано администратором. Приложение в терминах OAuth — client_id.
- **Уровень аутентификации понижен**. Пользователь вышел из сессии с повышенным уровнем аутентификации.

Защищаемый сервис может подписаться на эти события и получать HTTP-запросы от RooX UIDM с информацией о событиях. Для этого необходимо сообщить один или несколько callback URL, на которые RooX UIDM будет отправлять оповещения. Список URL для оповещения настраивается администратором.

Применение

Основной сценарий использования — это локальный кеш токенов в защищаемом приложении.

Существует такая схема интеграции RooX UIDM — веб-приложение, когда веб-приложение поднимает свою веб-сессию когда пользователь залогинился в RooX UIDM. Технически это реализуется через кеш токенов (lookup таблицу). Первый запрос проверяется на RooX UIDM, а затем последующие запросы обрабатываются приложением локально.

При этом теряется возможность централизованного вычисления политик и централизованного аудита, но некоторые клиенты находят схему удобной ввиду минимизации сетевых обращений.

Встает вопрос безопасного завершения сессии.

Когда сессия завершается в приложении, то есть пользователь явно вызывает функцию "Выйти", тогда приложение имеет возможность инвалидировать кеш. Но сессия может завершиться на стороне RooX UIDM по таймауту или из-за блокировки. Для инвалидации кеша в RooX UIDM в таких случаях предусмотрен механизм отправки вебхуков по HTTP.

Поддерживаемые события

Сессия прекращена

Технически сессия поддерживается через токены доступа (access token). При инвалидации токена конкретного пользователя RooX UIDM отправляет соответствующее оповещение на callback URL. Защищаемый сервис, получив такое оповещение, должен немедленно инвалидировать локальную сессию пользователя. Если защищаемый сервис использует кеширование результатов авторизации, кеш результатов авторизации данного пользователя также должен быть инвалидирован.

ЗАМЕТКА

Если токены прекратили существование из-за блокировки сессии целиком, то события по каждому токену отправляться не будут. Вместо этого придет одно событие о блокировке приложения целиком (ниже). Такое поведение выбрано из соображений производительности.

Формат оповещения о инвалидации токена

```
POST <callback_url>
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded

event=token_revoked&
global=false&
cn=<cn>&
access_token=<access_token>&
sub=<sub>&
cid=<customerId>
```

Параметры

- callback_url — URL для оповещения из списка, заданного администратором RooX UIDM, строка
- event — имя события, строка
- global — флаг полной блокировки сервиса, bool, в этом оповещении всегда false
- cn — номер телефона пользователя (msisdn), строка
- access_token — инвалидированный access token, строка
- sub — идентификатор принципала, строка в формате prefix_id, например `bis_199412412152222`
- customerId — идентификатор клиента в терминах защищаемого приложения

Блокирование приложения целиком

При блокировании приложения целиком RooX UIDM отправляет соответствующее оповещение на callback URL. Приложение в терминах OAuth — client_id. Защищаемый сервис, получив такое оповещение, должен немедленно инвалидировать сессии всех пользователей. Если защищаемый сервис использует кеширование результатов авторизации, кеш результатов авторизации всех пользователей также должен быть инвалидирован.

Формат оповещения о блокировке сервиса

```
POST <callback_url>
Cache-Control: no-cache
```

```
Content-Type: application/x-www-form-urlencoded

event=service_blocked&
global=true
```

Параметры

- callback_url — URL для оповещения из списка, заданного администратором RooX UIDM, строка
- event — имя события, строка
- global — флаг полной блокировки сервиса, bool, в этом оповещении всегда true

Понижение уровня авторизации токена

При понижении уровня авторизации токена конкретного пользователя RooX UIDM отправляет соответствующее оповещение на callback URL. Если защищаемый сервис использует кеширование результатов авторизации, кеш результатов авторизации всех пользователей также должен быть инвалидирован.

Формат оповещения о понижении уровня авторизации токена

```
POST <callback_url>
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded

event=token_auth_level_decreased&
global=false&
cn=<cn>&
access_token=<access_token>&
sub=<sub>&
cid=<customerId>
```

Параметры

- callback_url — URL для оповещения из списка, заданного администратором RooX UIDM, строка
- event — имя события, строка
- global — флаг полной блокировки сервиса, bool, в этом оповещении всегда false
- cn — номер телефона пользователя (msisdn), строка
- access_token — измененный access token, строка
- sub — идентификатор принципала, строка в формате prefix_id, например `bis_199412412152222`
- customerId — идентификатор клиента в терминах защищаемого приложения

Конфигурация

В настройках OAuth2.0 клиента установить свойство `callbackURIs`. Свойство является массивом, поэтому задается через синтаксис индексатора

Пример файла конфигурации клиента, использующего вебхуки

```
```

```
clientName=onlinebank_web

callbackURIs[0]=https://127.0.0.1:2003/callbacks
```

Опционально: настроить параметры HTTP (действуют системно для всех oauth-клиентов)

Таблица 1. Параметры HTTP

Параметр	Описание	Значение по умолчанию
com.rooxteam.sso.oauth.notification.httpclient.connection.timeout	Таймаут подключения к приемнику вебхуков, мс	5000
com.rooxteam.sso.oauth.notification.httpclient.socket.timeout	Таймаут чтения/записи, мс	5000
com.rooxteam.sso.oauth.notification.httpclient.connection_pool_size	Количество одновременных запросов ко всем приемниках суммарно	2147483647
com.rooxteam.sso.oauth.notification.httpclient.connection_pool_size.per_route	Количество одновременных запросов к каждому сконфигурированному URL приемника	256 Все параме требуют перезапуск сервиса roo

Особенности и ограничения

1. Конечная точка приемника может требовать basic-аутентификацию RFC7617. Для ее конфигурирования требуется прописать Callback URL в формате `https://username:password@domain/path`, например, `https://callbacks:password@domain.com/uidm_callbacks`
2. Поддерживаются схемы HTTP, HTTPS. Рекомендуется использовать HTTPS из соображений безопасности. Могут использоваться или сертификаты, выданные одним из зарегистрированных УЦ, либо самоподписанные. При использовании самоподписанных сертификатов, их необходимо добавить в системный keystore. Обратитесь к документации по JVM.
3. В настоящий момент не поддерживается настройка разных URL для разных событий. При возникновении такой необходимости используйте обратный прокси и маршрутизацию по параметру event.
4. RooX UIDM выполняет ровно один HTTP-запрос на каждое событие, повторов нет. Статус код ответа сервиса и тело игнорируются.