Как настроить авторизацию пользователей в веб-интерфейсе установщика

Инструкция для администраторов

Оглавление

Типы авторизации в установщике

1. Сопоставление IP-пользователь — пользователь определяется по IP адресу.
2. Прокси-авторизация. Предполагается, что установщик работает за прокси-сервером, который занимается авторизацией, а установщик получает данные о пользователе из заголовков.
3. Через OIDC сервер. Пользователь перенаправляется к OIDC серверу для авторизации.

Типы авторизации перечислены в порядке убывания приоритета. Все 3 типа авторизации могут быть настроены одновременно. Например, если данные о пользователе будут получены из заголовков, то перенаправления к OIDC серверу не будет. Чтобы отключить какой-то из типов авторизации, достаточно не указывать его в файле конфигурации.

Настройки авторизации

Вся найстрока производится в файле конфигурации `deployerParams.yaml`. По умолчанию файл находится в папке `/home/deployer/`. Файл содержит 4 основных блока:

- `oidc` — блок настройки OIDC сервера.
- `byIpUsers` — блок настройки авторизации по IP. Если пользователь подключится с заданного IP адреса, то ему будет назначено заданное имя пользователя. Сделано для подключения сторонних систем, например, ботов или CI/CD.
- `proxyAuth` — блок настройки прокси-авторизации: когда авторизацией занимается вышестоящий сервис, а в установщик приходят только заголовки с уже определёнными значениями.
- `overrideUsers` — переопределение атрибутов пользователей. Эти значения имеют приоритет перед данными, полученными из OIDC или заголовков.

В установщике есть 2 роли пользователей:

- **admin** — полный доступ.
- **viewer** — только чтение.

> ⚠ **Внимание**
>
> Никакие из приведённых выше настроек не являются значениями по умолчанию. По умолчанию все поля отсутствуют в файле конфигурации, а установщик работает без авторизации.

Настройка OIDC сервера

Содержит следующие поля:

Название поля	Описание	Пример значения
host	URL OIDC сервера	`https://biz.wm1.on-premise.ru/auth/realms/EXCH.ON-PREMISE.RU/protocol/openid-connect`
skipTls	Игнорировать ошибку сертификата при подключении к OIDC серверу	`false`
clientId	ID OIDC клиента	`api`
clientSecret	Секрет OIDC клиента	`otBrIQrxqvXj9VUtOkR1TcuBsmDzx8`
authPath	Путь API клиентской авторизации	`/auth`
tokenPath	Путь API работы с токенами	`/token`
infoPath	Путь API информации о пользователе	`/userinfo`
scope	OAuth-scope OIDC сервера	`email`
disableRefresh	Не проверять актуальность OAuth токена по истечении срока действия	`false`
infoFields	Мапинг полей в ответе OIDC API информации о пользователе	
infoFields: email	Содержит email пользователя в ответе OIDC API информации о пользователе	`email`
infoFields: username	**Обязательное поле** — содержит имя пользователя в ответе OIDC API информации о пользователе	`preferred_username`
infoFields: firstName		`given_name`

Название поля	Описание	Пример значения
	Содержит имя в ответе OIDC API информации о пользователе	
infoFields: lastName	Содержит фамилию в ответе OIDC API информации о пользователе	`family_name`
infoFields: role	Содержит роль пользователя в ответе OIDC API информации о пользователе. Если окажется пустым, то будет подставлена defaultRole (описана ниже)	`deployerAccess`

Пример конфигурации:

```
auth:
  oidc:
    host: https://biz.ws.vkwm1.on-premise.ru/auth/realms/EXCH.ON-PREMISE.RU/protocol/openid-
connect
    skipTls: false
    clientId: api
    clientSecret: otBrIQrxqvXj9VUtOk5iR1TcuBsmDzx8
    authPath: /auth
    tokenPath: /token
    infoPath: /userinfo
    scope: email
    disableRefresh: false
    infoFields:
      email: email
      username: preferred_username
      firstName: given_name
      lastName: family_name
      role: deployerAccess
```

Настройка авторизации по IP

Содержит следующие поля:

- `cidr` — IP/Subnet клиента.
- `username` — **Обязательное поле**. Идентификатор (имя пользователя), который будет назначен клиенту. Атрибуты пользователя будут взяты из блока `overrideUsers`.

Пример конфигурации:

```
auth:
   byIpUsers:
```

```
    - cidr: 172.20.70.190
      username: ivanivanov
```

Настройка прокси-авторизации

Содержит два основных блока:

- `headers` — маппинг заголовков в атрибуты пользователя.
- `allowCIDRs` — список IP/подсетей, с которых разрешён приём заголовков авторизации.

В блоке `headers` содержатся следующие поля:

Название поля	Описание	Пример значения
email	Содержит email пользователя.	`email`
username	**Обязательное поле** — содержит идентификатор (имя) пользователя	`preferred_username`
firstName	Заголовок, содержащий имя	`given_name`
lastName	Заголовок, содержащий фамилию	`family_name`
role	Заголовок, содержащий роль пользователя. Если окажется пустым, то будет подставлена defaultRole (описана ниже)	`deployerAccess`

Пример конфигурации:

```
auth:
  proxyAuth:
    headers:
      email: x-email
      username: x-username
      firstName: x-given-name
      lastName: x-family-name
      role: x-role
    allowCIDRs:
      - 172.20.70.190
```

Переопределение атрибутов пользователей

Состоит из имен пользователей, атрибуты которых необходимо переопределить. Например у нас есть пользователь `ivanivanov` :

Название поля	Описание	Пример значения
email	Содержит email пользователя.	`ivanivanov@mail.ru`
firstName	Заголовок, содержащий имя	`ivan`
lastName	Заголовок, содержащий фамилию	`ivanov`
role	Заголовок, содержащий роль пользователя. Если окажется пустым, то будет подставлена defaultRole (описана ниже)	`admin`

Пример конфигурации:

```
auth:
  overrideUsers:
    as:
      email: ivanivanov@mail.ru
      firstName: ivan
      lastName: ivanov
      role: admin
```

Дополнительные настройки авторизации

Кроме четырех блоков описанных выше, есть еще несколько полей для настройки авторизации:

- `defaultRole` — Роль по умолчанию, на случай, если из внешней системы получена пустая роль.
- `auditLogPath` — Путь к audit-логу установщика. Если поле пустое, то audit-лог не будет записываться.
- `realIpHeader` — Заголовок с реальным IP клиента, если установщик работает за прокси-сервером.
- `realIpFrom` — Список IP/посдсетей, с которых разрешён приём заголовка с реальным IP клиента. Если список пуст, то заголовок будет принят с любого адреса.

Пример конфигурации:

```
auth:
  ...
  defaultRole: admin
auditLogPath: audit.log
realIpHeader: x-real-IP
realIpFrom:
  - 172.20.70.190
```

Пример полной конфигурации

Скачать файл конфигурации

```
auth:
  oidc:
    host: https://biz.ws.vkwm1.on-premise.ru/auth/realms/EXCH.ON-PREMISE.RU/protocol/openid-
connect
    skipTls: false
    clientId: api
    clientSecret: otBrIQrxqvXj9VUtOk5iR1TcuBsmDzx8
    authPath: /auth
    tokenPath: /token
    infoPath: /userinfo
    scope: email
    disableRefresh: false
    infoFields:
      email: email
      username: preferred_username
      firstName: given_name
      lastName: family_name
      role: deployerAccess
  byIpUsers:
    - cidr: 172.20.70.190
      username: as
  proxyAuth:
    headers:
      email: x-email
      username: x-username
      firstName: x-given-name
      lastName: x-family-name
      role: x-role
    allowCIDRs:
      - 172.20.70.190
  overrideUsers:
    as:
      email: as@mail.ru
      firstName: a
      lastName: s
      role: admin
  defaultRole: admin
auditLogPath: audit.log
realIpHeader: x-real-IP
realIpFrom:
  - 172.20.70.190
```

Как получить логи авторизации через OIDC-провайдер

Информацию об авторизации можно увидеть в логах установщика:

```
journalctl -fu deployer
```

Либо на стороне OIDC-провайдера. Например, на сервере с Keycloak выполнить команду:

```
journalctl -fu onpremise-container-keycloak1
```

Как закрыть доступ до установщика с помощью TLS

Добавьте ключ и сертификат в строку запуска установщика:

```
./onpremise-deployer_linux -tlsCert fullchain.pem -tlsKey privkey.pem
```

Если установщик запускается через systemd:

1. Откройте для редактирования файл `/etc/systemd/system/deployer.service`:

   ```
   vim /etc/systemd/system/deployer.service
   ```

2. В строчке `Exec` добавьте:

   ```
   -tlsCert /etc/certs/fullchain.pem -tlsKey /etc/certs/privkey.pem
   ```

   Указав полный путь до ключей.

3. Выполните команды:

   ```
   systemctl daemon-reload
   systemctl restart deployer
   ```

Автор: Груздев Никита

30 июня 2025 г.