«МИЦЕЛИЙ»

Руководство администратора

СОДЕРЖАНИЕ

1 Предварительные требования

В разделе приведены предварительные требования, которые необходимо выполнить для корректной установки ПО.

Технические требования

Технические требования к серверу для «Мицелий»:

- CPU: 4 ядра, 2 Ггц;
- RAM: 4 Гб;
- HDD: 50 Гб.

Требования к программному обеспечению

Необходимое программное обеспечение для работы «Мицелий»:

- docker – необходим для работы Docker, в котором будут разворачивать сервисы;
- docker.io – docker-cli необходим для загрузки образов;
- docker-compose – необходим для развертывания сервисов;
- nginx – необходим для маршрутизации внешних запросов к сервисам.

2 Установка

В составе дистрибутива продукта поставляется пакет инсталляции (в виде архива или иным образом), содержащий набор артефактов:

- key.pem – ключ для удаленного ssh подключения к демонстрационному стенду
- docker-compose.yml – файлы для развертывания сервисов
- docker образы сервисов, сохраненные в архивы
- nginx.conf – конфигурация Nginx.

Компоненты системы, упакованные в Docker:

- Keycloak - OIDC провайдер, необходим для первичной аутентификации запросов
- Сервис Grants обеспечивает:
    - предоставление списка ролей пользователя, прошедшего аутентификацию;
    - предоставление открытых данных сертификатов, для проверки подписи JWT-токена;
    - формирование JWT-токена для авторизации в сервисе источнике данных для указанной роли пользователя, прошедшего аутентификацию;
    - хранение данных пользователя необходимых для выпуска JWT-токена;
    - хранение ролей доступных пользователю для авторизации;
    - хранение настроек контроля доступа для сервисов-источников.
- Сервис Security Proxy обеспечивает:
    - контроль доступа к данным, предоставляемым GraphQL API сервисом-источником данных, на основе правил авторизации;
    - проверка корректности разметки GraphQL API сервисов-источника данных;
    - Предоставление контрактов защищаемого сервиса внешним потребителям, не ограничивая доступ к контрактам для неавторизованных запросов;
    - проксирование запросов, прошедших авторизацию к сервису-источнику данных.
- Star Wars – демонстрационный сервис-поставщик данных, защищаемый для демонстрационных целей системой «Мицелий»;
- Postgres – БД, хранит в себе данные Сервиса Grants.

3 Развертывание

Для развертывания поставляемого решения выполните следующие команды:

Установка системных зависимостей

```
#!/bin/bash

apt install docker
apt install docker.io
apt install nginx
apt install docker-compose
apt install jq
```

Подготовка директорий

```
#!/bin/bash

mkdir /opt/data/
mkdir /opt/data/keycloak
mkdir /opt/data/postgres
mkdir /opt/data/services
mkdir /opt/data/distributive
```

Установка сервисов

```
#!/bin/bash

cd /opt/data/
tar -xvf micelium_distributive
cd distributive
docker load < grants.tar
docker load < keycloak.tar
docker load < postgres.tar
docker load < sec.tar
docker load < sw.tar
mv services/docker-compose.yaml ../services/
mv postgres/docker-compose.yaml ../postgres/
mv keycloak/docker-compose.yaml ../keycloak/
mv -f nginx.conf /etc/nginx/sites-available/default
systemctl restart nginx
cd ../postgres
docker-compose up
```

```
sql_address=$(docker volume inspect install_postgres_data | jq '.[].Mountpoint')
cp ../distributive/dumps_grants.sql $sql_address
docker exec -it install_postgres_1 bash
psql -U keycloak -d keycloak < dumps_grants.sql

cd ../keycloak
docker-compose up -d
cd ../services
docker-compose up -d
```

Проверкой будет поход на %АДРЕС_СЕРВЕРА%/security_proxy, в случае успеха в браузере отобразится graphql playground сервиса security proxy