Ворота в пустыне

Походюн Александр

Role Based Access Control, RBAC

Управление доступом на основе ролей.

Для определения модели RBAC используются следующие соглашения:

- S = Субъект (Subject) = Человек или автоматизированный агент (множество пользователей);
- R = Роль (Role) = Рабочая функция или название, которое определяется на уровне авторизации (множество ролей);
- P = Разрешения (Permissions) = Утверждения режима доступа к ресурсу (множество прав доступа на объекты системы);
- SE = Сессия (Session) = Соответствие между S, R и/или P

JSON Web Token

Токен JWT состоит из трех частей:

- заголовок (header);
- полезная нагрузка (payload);
- подпись или данные шифрования.

Пример JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhcHAiOiJlbm5lcmdpaWEtbXZzIiwic2NvcGVzIjozLCJoYXNoIjoiN2JjNjk1ZWU4OTU2ODhhYjI4ZTM2MjYxNDFjZmNlMWIiLCJpYXQiOjE1Njc2NTMwMzcsImV4cCI6MTU2NzY1MzkzN30.bz2ywYI1Z5cgm9b1gTI0cDGLv4DToAfWh0KGwOUVG8g

header.payload.signature

Попробуем все объединить

От RBAC берем роли и разрешения и в качестве субъекта не пользователь а микросервис. Сессию заменяем на jwt токен. Метод шифрования симметричный, но ключ знает только микросервис.

Важно не забыть:

- Смена ключа не должна вызывать трудностей;
- В случае смены ключа или изменения роли или разрешений, токен должен быть невалидным;
- Для локальной разработки все должно быть просто (иначе нафига нам, такой тюниг в саратовском зоопарке).

Конфиг

Объект конфигурации содержит следующие части:

- roles - массив ролей;
- permissions - массив разрешений;
- apps - массив приложений (клиентов).

```
const PERMISSION_CREATE_COLLECTION = 'create_collection';
const PERMISSION_READ_COLLECTION = 'read_collection';
const ROLE_GUEST = 'guest';
const ROLE_ADMIN = 'admin';

const APP_SLUG_ENNERGIIA_MVS = 'ennergiia-mvs';
const APP_ID_ENNERGIIA_MVS = 'PYxUNTdw';
const APP_SECRET_ENNERGIIA_MVS = 'ecFeRutc69pd7QqL';

const config = {
  permissions: [

    { id: PERMISSION_CREATE_COLLECTION, title: 'Создание новых коллекций' },
    {
      id: PERMISSION_READ_COLLECTION,
      title: 'Получение информации о коллекции'
    },
  ],
  roles: [
    { id: 'guest', title: 'Гость', permissions: [PERMISSION_READ_COLLECTION] }
  ],
  apps: [
    {
      slug: APP_SLUG_ENNERGIIA_MVS,
      id: APP_ID_ENNERGIIA_MVS,
      secret: APP_SECRET_ENNERGIIA_MVS,
      title: 'Мобильная версия сайта Энергии',
      roles: [ROLE_GUEST, ROLE_ADMIN]
    }
  ]
};
```

Демо

Спасибо за внимание!