Keycloak – это open-source сервер аутентификации и управления учетными записями (IDM) от JBoss, построенный на базе спецификаций OAuth 2.0, Open ID Connect, JSON Web Token (JWT) и SAML 2.0.

Пользователи проходят аутентификацию с помощью Keycloak, а не отдельных приложений. Это означает, что приложениям не нужно иметь дело с формами входа, аутентификацией пользователей и сохранением пользователей. После входа в Keycloak пользователям не нужно повторно входить в систему для доступа к другому приложению.

Это также относится к выходу из системы. Keycloak обеспечивает единый выход, что означает, что пользователям нужно выйти из системы только один раз, чтобы выйти из всех приложений, использующих Keycloak.

Включение входа в систему с помощью социальных сетей легко добавить через консоль администратора. Это всего лишь вопрос выбора социальной сети, которую вы хотите добавить. Никакого кода или изменений в вашем приложении не требуется.

Keycloak также может аутентифицировать пользователей с помощью существующих поставщиков удостоверений OpenID Connect или SAML 2.0. Это также всего лишь вопрос настройки поставщика удостоверений через консоль администратора.

Keycloak имеет встроенную поддержку для подключения к существующим серверам LDAP или Active Directory. Вы также можете внедрить своего собственного провайдера, если у вас есть пользователи в других хранилищах, таких как реляционная база данных.

Через консоль администратора администраторы могут централизованно управлять всеми аспектами сервера поиска ключей. Они могут включать и отключать различные функции. Они могут настраивать посредничество при идентификации и федерацию пользователей. Они могут создавать приложения и службы и управлять ими, а также определять детализированные политики авторизации. Они также могут управлять пользователями, включая разрешения и сеансы.

Через консоль управления учетными записями пользователи могут управлять своими собственными учетными записями. Они могут обновлять профиль, менять пароли и настраивать двухфакторную аутентификацию. Пользователи также могут управлять сеансами, а также просматривать историю учетной записи. Если вы включили вход в социальную сеть или посредничество при идентификации, пользователи также могут связать свои учетные записи с дополнительными поставщиками, чтобы они могли проходить аутентификацию в одной учетной записи с разными поставщиками удостоверений.

Поиск ключей основан на стандартных протоколах и обеспечивает поддержку OpenID Connect, OAuth 2.0 и SAML.

Если авторизация на основе ролей не удовлетворяет вашим потребностям, Keycloak также предоставляет детализированные услуги авторизации. Это позволяет вам управлять разрешениями для всех ваших служб из консоли администратора Keycloak и дает вам возможность точно определять нужные вам политики.

Для запуска keycloak на машине разработчика удобно использовать docker-compose.

Пример настроек конфигурации keycloak в docker-compose:

keycloak:

image: jboss/keycloak

container\_name: keycloak

environment:

DB\_VENDOR: POSTGRES

DB\_ADDR: postgres

DB\_DATABASE: crm

DB\_SCHEMA: keycloak

DB\_USER: postgres

DB\_PASSWORD: postgres

KEYCLOAK\_USER: admin

KEYCLOAK\_PASSWORD: admin

ports:

- "8484:8080"

depends\_on:

- postgres

Назначение основных разделов Keycloack:

1. Realms – сферы или области. Область управляет набором пользователей, учетных данных, ролей и групп. Пользователь принадлежит к области и входит в нее. Области изолированы друг от друга и могут управлять и аутентифицировать только тех пользователей, которых они контролируют.
2. Clients (клиенты) – это объекты, которые могут запрашивать Keycloak для аутентификации пользователя. Чаще всего клиентами являются приложения и службы, которые хотят использовать Keycloak для обеспечения собственной безопасности и предоставления решения для единого входа. Клиентами также могут быть организации, которые просто хотят запросить идентификационную информацию или токен доступа, чтобы они могли безопасно вызывать другие службы в сети, защищенные с помощью Keycloak.
3. Users (пользователи) – это организации, которые могут входить в вашу систему. У них могут быть атрибуты, связанные с ними самими, такие как электронная почта, имя пользователя, адрес, номер телефона и день рождения. Им может быть назначено членство в группе и им могут быть назначены определенные роли. Вы создаете пользователей в области, в которой вы собираетесь размещать приложения, необходимые этим пользователям.
4. Role (роли) – определяют тип или категорию пользователя. Admin, user, manager и employee – это все характерные роли, которые могут существовать в организации. Приложения часто назначают доступ и разрешения определенным ролям, а не отдельным пользователям, поскольку работа с пользователями может быть слишком мелкой и сложной в управлении.
5. Groups (группы) – управляют группами пользователей. Атрибуты могут быть определены для группы. Вы также можете сопоставить роли с группой. Пользователи, которые становятся членами группы, наследуют атрибуты и сопоставления ролей, определенные группой.
6. Authentication Flows (потоки аутентификации) – это рабочие потоки, которые пользователь должен выполнять при взаимодействии с определенными аспектами системы. Поток входа в систему может определять, какие типы учетных данных требуются. Процесс регистрации определяет, какую информацию профиля пользователь должен ввести и нужно ли использовать что-то вроде reCAPTCHA для фильтрации ботов. Процесс сброса учетных данных определяет, какие действия должен выполнить пользователь, прежде чем он сможет сбросить свой пароль.
7. User federation provider – Keycloak может хранить пользователей и управлять ими. Часто в компаниях уже есть службы LDAP или Active Directory, которые хранят информацию о пользователях и учетных данных. Вы можете использовать Keycloak для проверки учетных данных из этих внешних хранилищ и извлечения идентификационной информации.
8. Identity provider federation – Keycloak можно настроить для делегирования аутентификации одному или нескольким IDPL. Вход в социальную сеть через Facebook или Google+ является примером федерации поставщиков удостоверений. Вы также можете подключить Keycloak для делегирования аутентификации любому другому OpenID Connect или SAML 2.0 IDP.