А. В. Тихонов

ИСПОЛЬЗОВАНИЕ КОМПОНЕНТА OPENSTACK KEYSTONE

Рассматривается схема управления доступом для облачного решения построенного на OpenStack в контексте частного облака кафедры.

Введение

При организации доступа к облаку кафедры для широкого круга пользователей, необходимо разграничить права доступа к сервису, а так же установить квоты для использования ресурсов. В выбранном комплексе программных средств OpenStack за организацию доступа отвечает программный модуль Keystone.

I. Keystone - OpenStack Identity Service

Keystone — это кодовое имя проекта (сервиса) OpenStack Identity, который при посредстве API-интерфейса OpenStack предоставляет такую функциональность, как токены, политики и каталоги. Как и остальные проекты платформы OpenStack, компонент Keystone представляет собой уровень абстрагирования. Keystone интегрирует функции OpenStack для аутентификации, для управления политиками и для обслуживания каталогов (включая регистрацию всех арендаторов и пользователей, аутентификацию пользователей и предоставление токенов для авторизации пользователей, создание политик, охватывающих всех пользователей и все сервисы, а также управление каталогом оконечных точек сервисов). Базовым объектом системы управления идентификацией является "пользователь"— в данном случае это цифровое представление человека, системы или сервиса, использующего какие-либо сервисы OpenStack. Нередко пользователь сопоставляется контейнеру под названием "арендатор"(tenant). Такой контейнер заключает в себе ресурсы и объекты идентифицируемой сущности. Арендатор может представлять собой клиента, учетную запись, подразделение организации и так далее.

II. Использование сервиса Keystone для разрграничения прав доступа студентов и преподавателей

Для начала нам предстоит разделить группы пользователей. В нашем случае, для начала, это будут Студенты и Преподаватели. Так, каждый пользователь будет членом соответствующего проекта. Таким образом мы создадим два проекта Students и Professors. И так нам надо будет создать как минимум по одному пользователю для каждого проекта. Это будут StudentAdmin и ProfessorAdmin соответственно. При создании пользователей мы выберем проект для каждого (Primary Project). Так же в уже созданных проектах, мы можем выставить ограничения (Quota) для каждого проекта. Это позволит более рационально распределить использование ресурсов и избежать перегруженности сервиса в целом.

III. Аутентификация компонентов OpenStack

Помимо сервиса организации доступа пользователей, компонент Keystone, так же осуществляет аутентификацию сервисов в процессе исполнения. Любой компонент OpenStack должен осуществлять аутентификацию. Сначала это приложение должно подключиться к сервису аутентификации и предоставить свои мандаты. После этого оно получает аутентификационный токен, который сможет передавать другому компоненту OpenStack при выполнении любых операций с объектами. В некоторых случаях конфигурация такого приложения может не иметь всех параметров соединения. В этих случаях оно также сможет получить эти параметры из Keystone. Например, приложение может послать в Keystone запрос о том, к каким проектам оно имеет право обращаться, и подать заявку на URL-адрес нужного сервиса.

IV. Выводы

Keystone жизненно необходимый компонент OpenStack который организует не только доступ пользователей к сервису в целом, но так и аутентификацию всех компонентов облачного решения при обращении друг к другу.

1. Официальная документация OpenStack https://docs.openstack.org/developer/keystone/
2. Свободная Энциклопедия https://en.wikipedia.org/wiki/OpenStack

Тихонов Артем Владимирович, магистрант кафедры информационных технологий автоматизированных систем БГУИР, ultravozhik@gmail.com.

Научный руководитель: Навроцкий Анатолий Александрович, заведующий кафедрой информационных технологий автоматизированных систем БГУИР, кандидат физико-математических наук, доцент, navrotsky@bsuir.by