ARENADATA
Корпоративная платформа хранения
и обработки больших данных

Общество с ограниченной ответственностью
«Аренадата Софтвер»

Описание технической архитектуры программного обеспечения для электронно-вычислительных машин Arenadata One (AOne)

Москва
2025

Оглавление

1 Функциональная схема

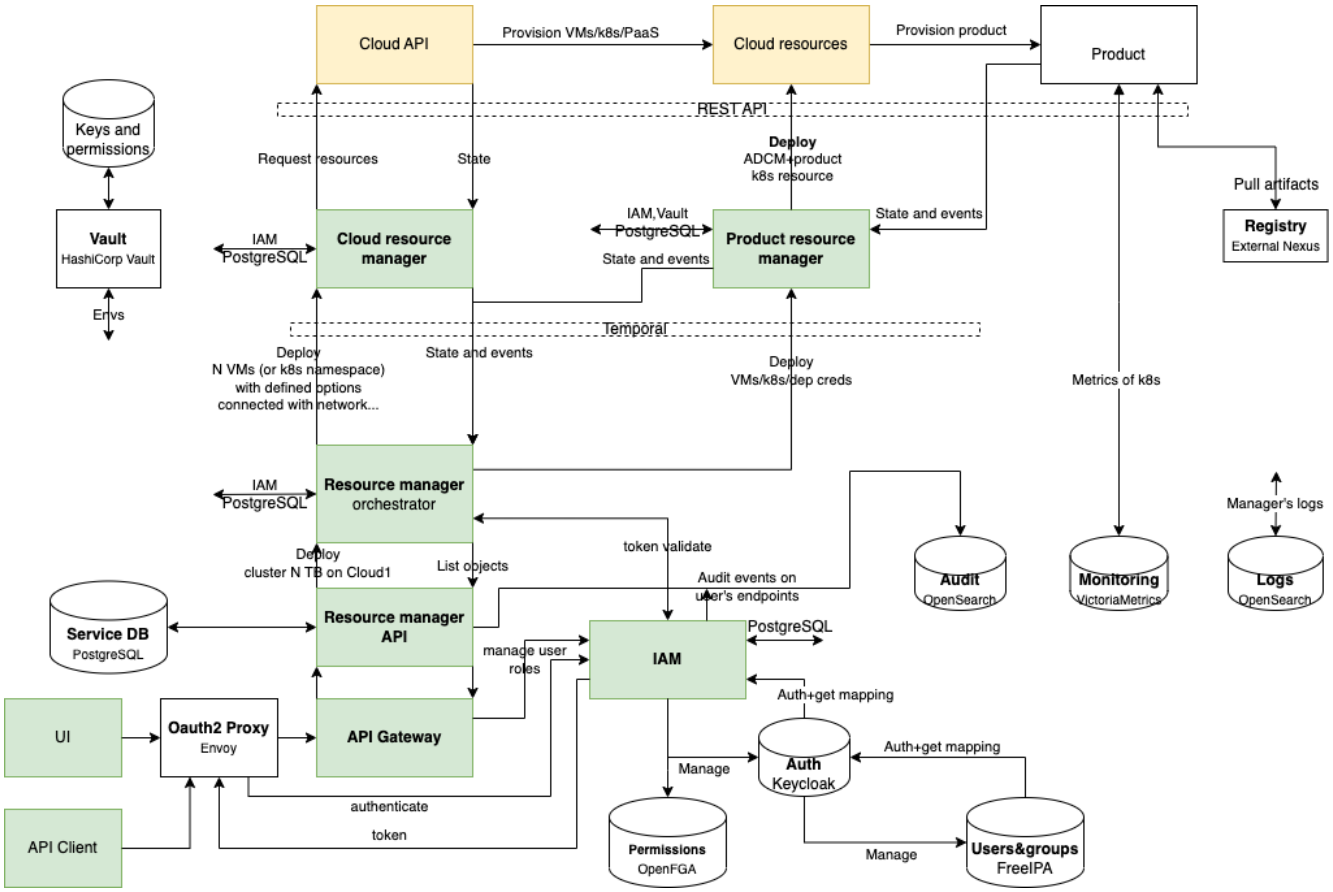

Рис. 1. Функциональная схема AOne

На рисунке 1 представлена функциональная схема ПО Arenadata One (AOne) с набором компонент. Желтым цветом обозначена инфраструктура облачного провайдера, зеленым – используемое ПО, белым – разрабатываемые сервисы.

Компоненты AOne приведены далее в пп.1.1 - 1.14.

1.1 Resource manager API

Основная функциональность Resource manager API:

- Направление запросов REST API к временным рабочим процессам;
- Сохранение сведений о доступе, состоянии и параметрах ресурсов;
- Проверка и привязка зависимостей между ресурсами;
- Расширение метаданных для параметров ресурсов;
- Подготовка представления ресурсов для API;
- Сохранение связи между ресурсами и проектами;

- Сохранение манифестов ресурсов.

1.2 Resource manager

Основная функциональность Resource manager:

- Управление процессом развертывания облачных ресурсов;
- Управление процессом развертывания продукта на базе облачных ресурсов;
- Управление процессом управления развернутых продуктов.

1.3 Cloud resource manager

Основная функциональность Cloud resource manager:

- Создание ресурсов в облачном провайдере через Terraform/Python;
- Подготовка адресов и учетных данных для доступа к ресурсам;
- Удаление и очистка ресурсов на облачном провайдере;
- Получение состояния ресурсов от облачного провайдера;
- Получение состояния (квот) проекта от облачного провайдера.

1.4 Product resource manager

Основная функциональность Product resource manager:

- Развертывание продукта с определенной конфигурацией с использованием определенных ресурсов (облако/другие продукты);
- Корректировка параметров ранее развернутых продуктов;
- Удаление ранее развернутых продуктов из базовых ресурсов.

1.5 База данных PostgreSQL

База данных PostgreSQL отвечает за хранение данных менеджеров и сервисов в общем кластере, за репликацию данных.

1.6 Шина сообщений Temporal

Шина сообщений Temporal отвечает за распределение событий по сервисам, за контроль выполнения последовательностей операций.

1.7 Прокси-сервер Envoy

Прокси-сервер Envoy отвечает за аутентификацию, ограничения скорости и маршрутизацию запросов.

1.8 API Gateway

API Gateway отвечает за проксирование запросов к внутренним сервисам и поддержание стабильности API.

1.9 IAM

Основная функциональность IAM:

- Управление организациями;
- Управление группами и отношениями между пользователями и группами;
- Управление назначенными ролями;
- Представление профиля для каждого пользователя;
- Внедрение аутентификации с использованием паролей и OAuth2 для устройств.

1.9.1 FreeIPA

FreeIPA – хранилище пользователей, групп и их сопоставление. LDAP(s) может использоваться в качестве протокола связи с бэкэндом FreeIPA.

1.9.2 Keycloak

Keycloak отвечает за выпуск и проверку JWT, управление пользователями, федерацию с другими инстансами.

1.9.3 OpenFGA

OpenFGA отвечает за хранение и обеспечение соблюдения разрешений доступа пользователей.

1.10 HashiCorp Vault

HashiCorp Vault – Хранилище чувствительных данных. Отвечает за хранение и управление доступом к токенам, паролям, сертификатам и ключам шифрования для защиты секретов и других конфиденциальных данных.

1.11 OpenSearch (аудит)

OpenSearch – хранилище данных аудита. Отвечает за хранение событий аудита и предоставление их через API.

1.12 VectoriaMetrics

VectoriaMetrics – хранилище метрик. Отвечает за долгосрочное хранение метрик и предоставление доступа к ним через API.

1.13 OpenSearch (логи)

OpenSearch – хранилище логов. Отвечает за долгосрочное хранение журналов и предоставление доступа к ним через API.

1.14 Nexus

Nexus – хранилище артефактов. Отвечает за хранение артефактов, которые используются для развертывания сервисов и продуктов. На данный момент внешний.

2 Распределение компонент

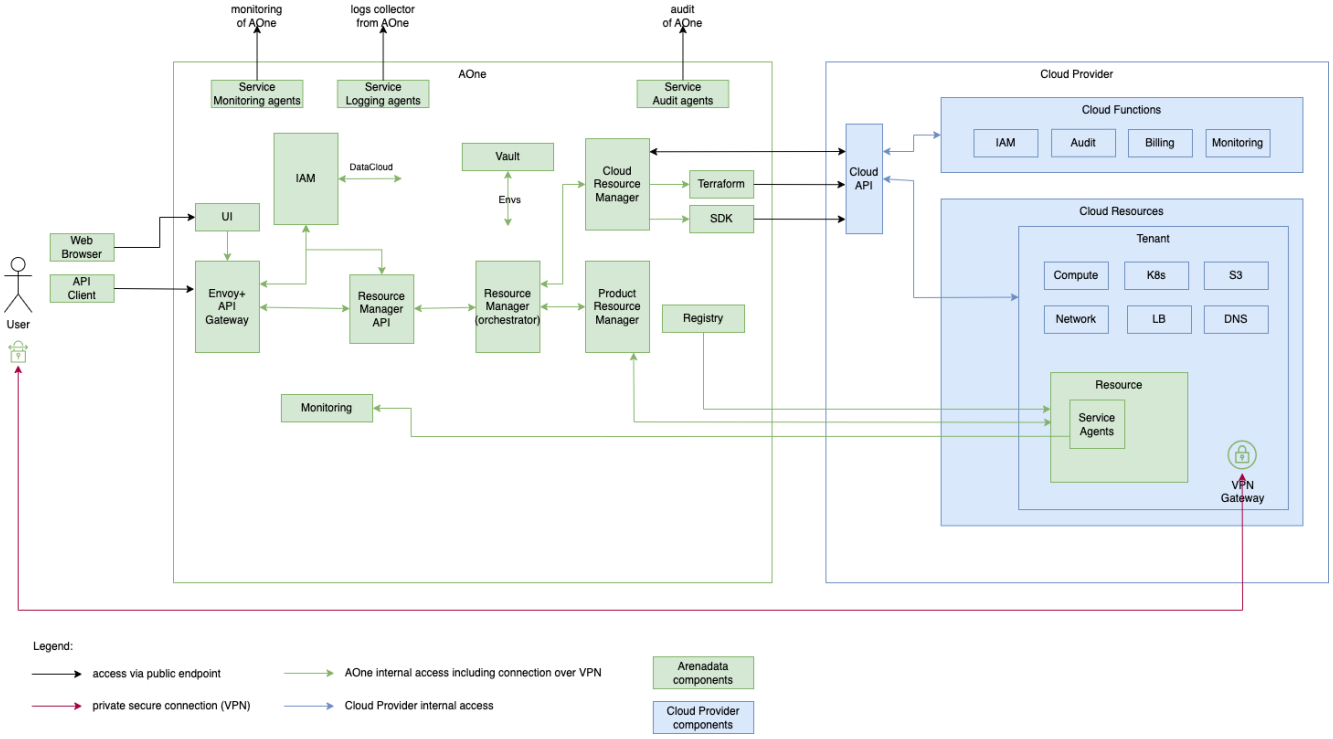

Рис. 2. Распределение компонент AOne

На рисунке 2 представлено распределение компонент системы и взаимодействие с облачным провайдером:

- Зеленые компоненты — сущности AOne;
- Синие компоненты — сущности облачного провайдера;
- Зеленая стрелка — внутренний доступ AOne, включая подключение через VPN;
- Синяя стрелка — внутренний доступ облачного провайдера;
- Красная стрелка — доступ через частное защищенное соединение (VPN);
- Черная стрелка — доступ через публичный адрес.