Типовая архитектура UIDM

Концептуальная архитектура UIDM

Концептуальная архитектура решения представлена ниже.

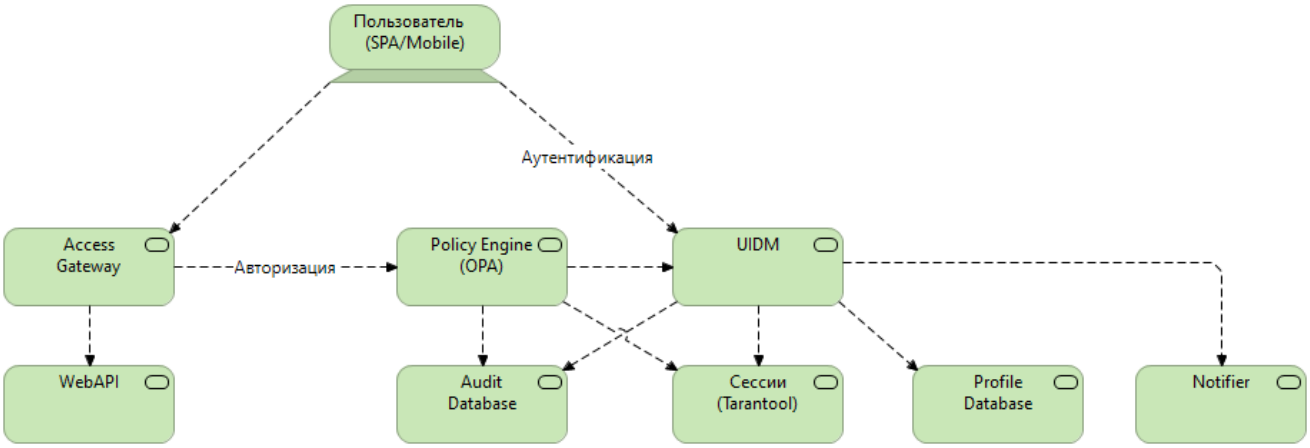


Figure 1. Концептуальная схема

Диаграмма содержит укрупненные блоки, в состав которых входят одни или несколько сервисов.

Каждый сервис зарезервирован в режиме Active-Active, точный коэффициент резервирования рассчитывается в зависимости от нагрузки.

Описание компонентов

- UIDM - центральный сервис аутентификации. Выполняет аутентификацию, предоставляет API для аутентификации, самообслуживания и администрирования. Состоит из порядка 10 сервисов, которые приведены ниже
- Profile Database - основная СУБД с пользователями и техническими данными, нужными для работы UIDM. Размер БД пропорционален количеству пользователей. В качестве РСУБД может использоваться Postgresql или Oracle
- Audit Database - СУБД с аудит-логом. Содержит все действия всех пользователей. В качестве РСУБД может использоваться Postgresql или Oracle, но могут использоваться и внешние NoSQL хранилища на усмотрение заказчика
- Сессии - оперативное хранилище выданных токенов и сессий пользователей и систем. Используется Tarantool
- Notifier - служебный сервис для шаблонизации и доставки исходящих уведомлений и одноразовых паролей. Интегрируется с каналами, например Email, SMS, Push, Voice. Протоколы доставки могут быть кастомными
- Policy Engine - центральный сервис авторизации. Вычисляет, разрешен ли доступ пользователей к веб-ресурсам. Используется движок, основанный на Open Policy Engine
- Access Gateway - шлюз доступа, через который проходят все запросы к веб-ресурсам.

Прерывает запрос и отправляет в Policy Engine для принятия авторизационного решения. Могут быть использованы разные шлюзы на усмотрение заказчика

- WebAPI - пример защищаемого веб-приложения

Полный список сервисов

Прикладные сервисы

Сервис	Назначение
api-gateway	Прерывает запросы, делегирует в Policy Engine, преобразовывает протоколы, упрощает интеграцию сторонним сервисам (BFF). RooX разрабатывает гейтвеи на технологии Spring Boot, но решение не ограничивается только ей
audit-search-api	Фасад перед БД аудита, используется для прикрытия обращений к БД Аудита REST API
certificate-service	Сервис управления пользовательскими сертификатами
customer-webapi	Сервис управления пользовательскими данными и организациями от лица пользователей
federation-webapi	Сервис данных федеративной аутентификации, хранит привязки пользователя к сторонним сервисам и предоставляет API к ним
identity-sync-service	Сервис фоновой синхронизации Active Directory и UIDM
oauth2-consumer-server	Обработчик протокола OAuth2 от лица Service Provider, используется в случаях, когда заказчик имеет только SPA
sso-server	Основной сервис аутентификации
opa	Вычислитель авторизационных решений
token-storage	Фасад перед хранилищем токенов
audit-writer	Запись событий аудита в БД из очереди сообщений асинхронного аудита
webapi-notifier	Сервис шаблонизации и доставки уведомлений
webapi-server-otp-settings	Сервис управления настройками 2 фактора

Хранилища

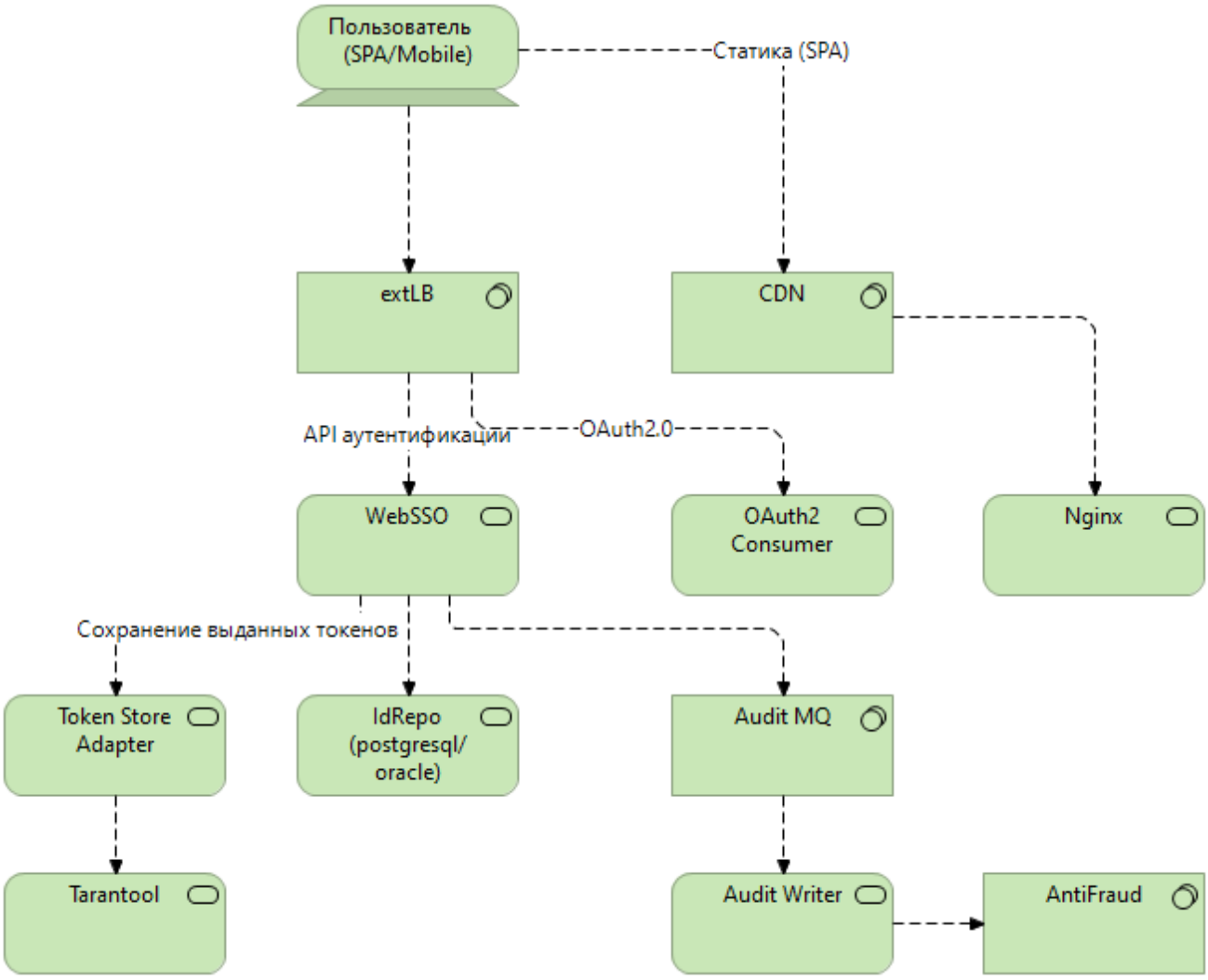
Хранилище	Назначение
tarantool	Хранилище токенов на базе Tarantool
postgresql/oracle	Хранилище постоянных данных UIDM (профили, блокировки, аудит)
opendj	Legacy-хранилище токенов на базе LDAP. Больше не внедряется.

Инфраструктурные сервисы, предоставляются заказчиком

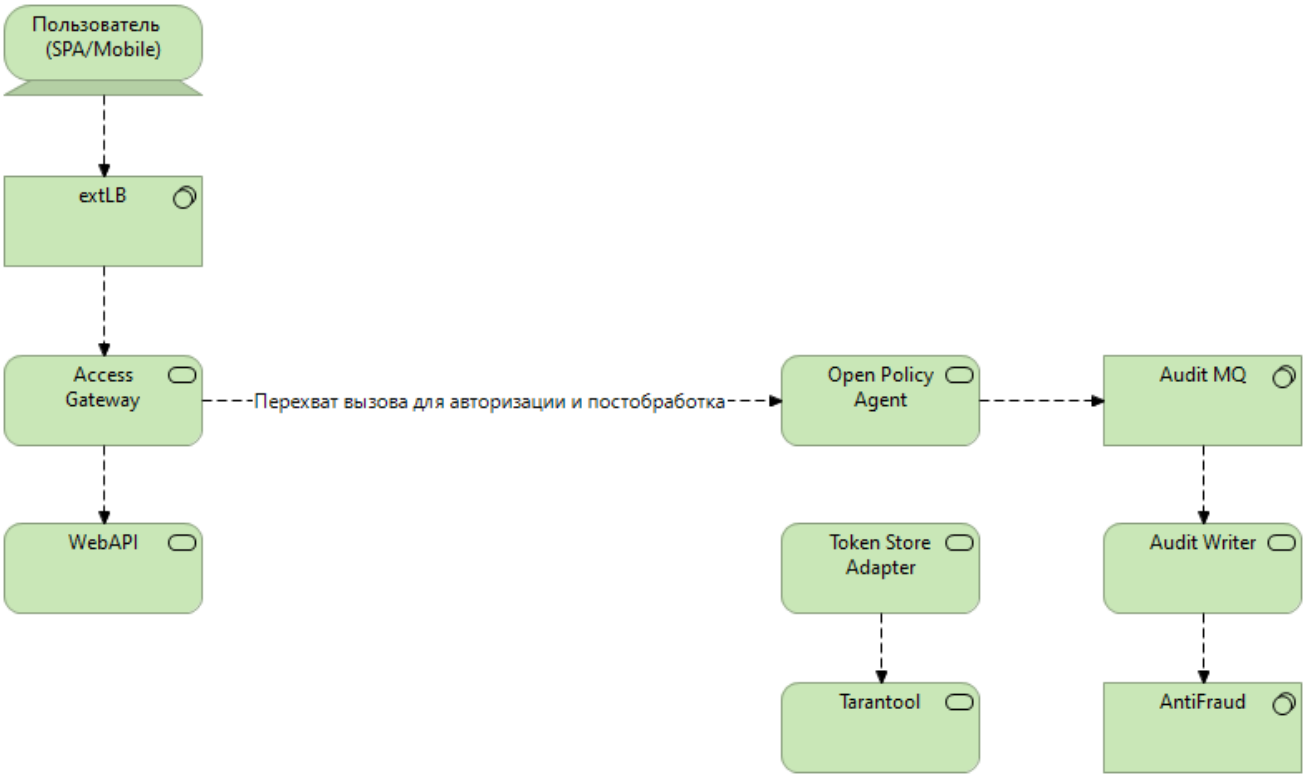
Сервис	Назначение
extLb	Внешний балансировщик, выставляет сервисы в открытый Интернет. Так же выполняет SSL Offload. В настоящее время, как правило, содержит WAF
intLB	Внутренний балансировщик. Управляет трафиком между сервисами, выполняя масштабирование, резервирование и проверку доступности. В K8S инсталляциях, как правило, используется ingress
sms gateway, email service	Транспорты для доставки сообщений клиентам. Заказчик обычно уже содержит такие сервисы или подрядчиков, так что в проекте внедрения выполняется интеграция с имеющимися сервисами доставки
CDN	Сеть доставки статического контента. Используется для обслуживания виджетов логина для систем с высокой нагрузкой
monitoring	Сервис мониторинга
tracing	Сервис централизованного логгирования

Уточненные диаграммы для отдельных сценариев

Сценарий аутентификации



Сценарий авторизации с централизованным вычислением политик



Сценарий отправки сообщения (EMAIL, SMS, PUSH, VOICE)