ADR 2023-11-09 SaaS Выбор API Gateway

In Progress

Запись об архитектурном решении: SaaS Выбор OpenSource API Gateway

Дата окончания согласования

Последняя дата согласования документа - 16.01.24

После этой даты документ будет согласован автоматически

Заказчик (PDM или PO)	Некрасов Дмитрий
Исполнитель	Пащенко Павел
Архитектор	Ледванов Олег
PDL	Ребров Борис
Бизнес-инициатива	CSE-9089 - API Gateway для интеграций с клиентской инфраструктурой ИССЛЕДОВАНИЕ
Архитектурная задача	~~CSE-9541~~ - ADR SaaS API Gateway [Выбор решения] ЗАКРЫТО
Статус	ADR_APPROVED

Контекст

В рамках реализации стратегии по продаже продуктов, возникла необходимость точечной интеграции it инфраструктуры b2b клиента с нашими продуктами и сервисами

Решение

Т.к. интеграция с системами b2b клиента подразумевает использование API интерфейсов, нам необходим API Gateway

API Gateway:

- Обеспечит единую точку входа,
- Упростит интеграцию,
- Будет принимать, обрабатывать и распределять запросы,
- Контролировать трафик,
- Осуществлять мониторинг
- Управлять доступом приложений к данным, бизнеслогике или функциональным возможностям сервисов.

blocked URL

Какие задачи требуется решить:

- Единая точка входа
- Безопасный доступ до внутренних endpoint'ов, либо через TLS, либо с использованием токенов доступа
- Валидация токенов keycloak, либо средствами api gateway, либо проброс токенов через api gateway в keycloak
- Контроль трафика по необходимости

К рассмотрению предлагается 3 самых популярных open source решения на рынке Kong, Tyk, KrakenD + платное решение от Yandex

API Gateway	Язык	Keycloak	Plugins	Поддерживаемые проколы	Метрики	Web-интерфейс	Требуется БД	Полнота документации

Kong	Lua	Через плагин kong-oidc, в бесплатной версии плагин из коробки не доступен, доступен только в enterprice, либо в кастомной сборке образа	Базовый язык Lua Есть инструменты для Go, Python, JavaScript	REST, gRPC, GraphQL	Prometheus	Есть из коробки (Kong Manager Open Source)	Да, Postgres	Отличная, с примерами
Tyk	Go	Из коробки нет - требуется платная лицензия	Базовый язык Go Есть инструменты для Python, JavaScript, Lua	REST, gRPC, GraphQL	Prometheus	Из коробки нет - требует ся платная лицензия	Да, Redis	Отличная, с примерами
KrakenD	Go	Из коробки (валидация полученного токена, internal redirect - только в платной версии)	Базовый язык Go Есть инструменты для Lua	REST, GraphQL gRPC - либо через костыль плагин, либо в enterprice решении	Prometheus	Есть из коробки (Online KrakenDesigner)	Не требуется	Отличная, с примерами
Nginx	C	OAuth2 и oidc доступны только в платной версии nginx+	Есть ряд готовых модулей, нативный язык C и C++, так же можно писать на Lua	REST, gRPC	Prometheus	gui настройки роутов нет, только дашборды и только в nginx plus	не требуется	Нормальная, с примерами
Envoy	C++	Из коробки есть возможность прямых редиректов на страницу авторизации Keycloak Из коробки есть возможность проводить валидацию jwt и oauth2 со стороны api gateway	C++, Lua	REST, gRPC	Prometheus	Нет gui	не требуется	Отличная, с примерами
Yandex API Gateway	-	Через подключаемый плагин yandex'a x-yc-apigateway-authorizer:jwt	Имеет ряд подключаемых расширений из коробки, нет кастомизации	REST, gRPC	Prometheus Через yandex monitoring	Есть из коробки (Консоль управления)	Не требуется	Нормальная, с примерами
Google cloud API	-	Через подключаемый плагин gcp x-google-jwks_uri	Имеет ряд подключаемых расширений из коробки, нет кастомизации	REST, gRPC	Prometheus Через cloud monitoring	Есть из коробки (Консоль управления)	Не требуется	Отличная, с примерами

Kong API Gateway

Kong Gateway (OSS) — это популярный шлюз API с открытым исходным кодом и усовершенствованным облачным API, созданный для универсального развертывания: он может работать на любой платформе. Может быть запущен как самостоятельное приложение, либо установлен в Kubernetes (в этом случае он представляется как специализированный Ingress-контроллер).

Он написан на языке программирования Lua и поддерживает гибридную и мульти облачную инфраструктуру, а также оптимизирован для микросервисов и распределенных архитектур.

По своей сути Kong создан для обеспечения высокой производительности, расширяемости и портативности. Kong легкий, быстрый и масштабируемый.

Kong поддерживает балансировку нагрузки (с различными алгоритмами), ведение журналов, аутентификацию (поддержка OAuth2.0), ограничение скорости, преобразования, мониторинг в реальном времени, обнаружение сервисов, кэширование, обнаружение и восстановление сбоев, кластеризацию и многое другое. Важно отметить, что Kong поддерживает кластеризацию узлов и бессерверные функции.

Так же поддерживает настройку прокси-серверов для сервисов и обслуживает их через SSL или использует WebSockets. Он может балансировать нагрузку трафика через реплики вышестоящих сервисов, отслеживать доступность сервисов и соответствующим образом корректировать балансировку нагрузки.

Kong поставляется с интерфейсом командной строки, который позволяет управлять "кластером Kong" из командной строки, а так же можно использовать как запросы к API, так и веб-интерфейсы Kong Manager или Konga.

Kong обладает широкими возможностями расширения с помощью плагинов и различных видов интеграции. Им можно управлять с помощью RESTful API для максимальной гибкости.

Многие расширения предустановлены в официальном контейнере, но они также могут быть найдены в Kong Plugin Hub.

На что обратить внимание

- Базовый язык Lua
- Плагин для работы с keycloak древний (не обновлялся больше 2х лет), в бесплатной версии его не возможно установить из коробки
- Бесплатная версия gui имеет ряд ограничений (не все плагины можно ставить из коробки, не возможно менеджерить нескольк глобальных workflow(tenant),
- В бесплатной версии не возможно ставить api заглушки, работать с GraphQL, валидировать запросы согласно внутренним схемам
- В бесплатной версии только Basic Authorization & Authentication
- В бесплатной версии нет выделенной тех поддержки
- В бесплатной версии отсутствуют автоматическое создание документации

Tyk API Gateway

Tyk (произносится как Taik) — это мощный, легкий и полнофункциональный API-шлюз с открытым исходным кодом, написанный с нуля с использованием языка программирования Go.

Это облачное решение с высокой производительностью, легко расширяемой и подключаемой архитектурой, основанной на открытых стандартах.

Он может работать независимо и требует только Redis в качестве хранилища данных. Он позволяет пользователям безопасно публиковать и управлять различными сервисами (поддерживает GraphQL «из коробки»).

Tyk оснащен множеством функций, включая различные методы аутентификации, квоты и ограничение скорости, контроль версий, уведомления и события, мониторинг и аналитику. Он также поддерживает обнаружение сервисов, преобразования «на лету» и виртуальные endpoints, а также позволяет создавать заглушки API перед выпуском.

Помимо вышесказанного, Tyk поддерживает документацию по API и предлагает инструмент (портал) для разработчиков API, систему, подобную CMS (системе управления контентом), где вы можете публиковать свои управляемые API, а сторонние разработчики регистрироваться в ваших API и могут управлять своими собственными ключами - требуется платная лицензия

Важно отметить, что существует только одна версия шлюза Tyk API, и она на 100% имеет открытый исходный код. Независимо от того, являетесь ли вы пользователем Community Edition или корпоративным пользователем, вы получаете один и тот же шлюз API. Он поставляется со всеми возможными деталями, необходимыми для полного удобства использования, без блокировки функций и черного ящика.

С Tyk мы точно узнаем, как обрабатываются наши данные.

На что обратить внимание

- Базовый язык Go
- Бесплатная версия содержит только gateway oss (работа с gateway только через api), все остальные плюшки в виде аналитики, дашбордов, мониторинга, gui - требуется платная лицензия
- В бесплатной версии не возможно менеджерить несколько глобальных workflow(tenant), SSO, RBAC, Developer portal, Developer API Analyst
- В бесплатной версии нет выделенной тех поддержки
- В бесплатной версии отсутствуют автоматическое создание документации

KrakenD API Gateway

Написан на Go и создан с акцентом на производительность, представляет собой высокопроизводительный, простой и легко подключаемый API-шлюз с открытым исходным кодом, разработанный с архитектурой без сохранения состояния.

Он может работать где угодно и для запуска не требует базы данных. Он имеет простую конфигурацию и поддерживает неограниченное количество конечных точек и серверов.

KrakenD поддерживает мониторинг, кэширование, пользовательские квоты, ограничение скорости, качество обслуживания (одновременные вызовы, автоматический выключатель endpoint'а и настройку тайм-аутов), преобразование, агрегацию (объединение источников), фильтрацию (внесение в белый и черный списки) и декодирование.

Он предлагает такие функции прокси, как балансировка нагрузки, трансляция протоколов и Oauth, а также функции безопасности, такие как SSL и политики безопасности.

Можно настраивать поведение API шлюза вручную или с помощью KrakenDesigner, графического пользовательского интерфейса, который позволяет визуально разрабатывать API с нуля.

Более того, расширяемая архитектура KrakenD позволяет добавлять дополнительные функции, плагины, встроенные скрипты и промежуточное ПО без изменения исходного кода.

По словам разработчиков, пропускная способность KrakenD превосходит другие API-шлюзы от Tyk и Kong. Плюс он имеет встроенную поддержку GraphQL

На что обратить внимание

- Базовый язык Go
- Кастомные плагины пишутся только на Go
- Конфигурирование API - GitOps ориентировано, т.е. выкатка изменений в api происходит через ci\cd процесс
- В бесплатной версии есть поддержка mTLS из коробки,
- В бесплатной версии есть поддержка работы с Keycloak из коробки
- В бесплатной версии есть gui api designer
- В бесплатной версии нет выделенной тех поддержки, отсутствуют аналитические дашборды и автоматическое создание документации, функции редиректа на страницу авторизации keycloak

Nginx в качестве API Gateway

Nginx - это программное обеспечение с открытым исходным кодом для создания легкого и мощного веб-сервера. Также его используют в качестве почтового или обратного прокси-сервера. Nginx решает проблему падения производительности с ростом трафика и является самым популярным веб-сервером в России и вторым в мире

Nginx обслуживает соединения, обрабатывает запросы, которые поступают к серверу, а также используется:

- для обработки запросов с сайтов, где много статического неизменного контента;
- обслуживания серверов, на которые поступает много запросов одновременно;

- в качестве прокси, почтового сервера или для распределения нагрузки на серверную часть.
- SSL/TLS терминация: Nginx способен выполнять терминацию SSL/TLS, обеспечивая шифрование и дешифрование данных между клиентами и серверами. Это снижает нагрузку на бэкэнд-серверы и улучшает безопасность.

На что обратить внимание

- Базовый язык C
- Огромное количество готовых плагинов на все случаи жизни, можно писать кастомные на C++ или Lua, или использовать платный Nginx plus и писать модули на любом языке
- В бесплатной версии есть поддержка TLS из коробки,
- Нет api healthcheck
- В бесплатной версии нет:
  - поддержки работы с Keycloak из коробки
  - gui api designer,
  - выделенной тех поддержки,
  - отсутствуют аналитические дашборды и автоматическое создание документации,
  - функции редиректа на страницу авторизации keycloak

Envoy

Это L4\L7 балансировщик написанный на C++, ориентированный на высокую производительность и доступность, может выступать в качестве единой точки входа для приложений.

С одной стороны, это в некотором роде аналог nginx и haproxy, соизмеримый с ними по производительности.

С другой, он больше ориентирован под микросервисную архитектуру и обладает функционалом не хуже балансировщиков на java и go, таких как zuul или traefik.

Задачи в которых Envoy незаменим:

- Балансировка трафика в сложных и динамичных системах. Сюда попадает service mesh, но это не обязательно только он.
- Необходимость функционала распределенной трассировки, сложной авторизации или другого, который есть в *envoy* из коробки или удобно реализовывается, а в nginx/haproxy нужно обложиться lua и сомнительными плагинами.

На что обратить внимание

- Базовый язык C++
- L4\L7балансировщик
- Огромное количество готовых плагинов на все случаи жизни
- Из коробки есть поддержка TLS ,
- Из коробки есть валидация jwt токенов,
- Из коробки есть прямые редиректы на страницу авторизации Keycloak
- Из коробки есть api healthcheck
- Конфигурирование API - GitOps ориентировано, т.е. выкатка изменений в api происходит через ci\cd процесс
- Из коробки нет:
  - gui api
  - отсутствуют аналитические дашборды и автоматическое создание документации

Yandex API Gateway

Сервис для управления API-шлюзами, поддерживающий спецификацию OpenAPI 3.0 и набор расширений для взаимодействия с другими облачными сервисами

API-шлюз — это интерфейс взаимодействия с сервисами внутри Yandex Cloud или в интернете.

API-шлюз задается декларативно при помощи спецификации. Спецификация — это файл в формате JSON или YAML с описанием API-шлюза по стандарту OpenAPI 3.0.

В сервисе API Gateway спецификация дополнена расширениями, которые можно использовать для интеграции с другими облачными платформами.

Сервис API Gateway интегрирован с системой управления доменами сервиса Certificate Manager. Можно использовать домены с подтвержденными правами при обращении к API.

При этом для обеспечения TLS-соединения будет использован привязанный к домену сертификат.

С API Gateway запросы к API сервисов обрабатываются с минимальной задержкой. При пиковой нагрузке сервис автоматически масштабируется, чтобы минимизировать задержку ответов.

Можно спецификации по клику в консоли управления и интегрируйте ваши приложения с сервисами Yandex Cloud.

Канареечные релизы в API Gateway позволяют применять изменения OpenAPI-спецификации API-шлюза не сразу для всем входящим запросам, а постепенно только к определённой их доле.

Можно ограничивать количество запросов к APIшлюзу в единицу времени для защиты от DDoSатак и для контроля потребления облачных ресурсов.

Оплачивайте только хранение и операции с данными в бессерверном режиме. На сервис действуют специальные тарифы: первые 100 000 запросов к API-шлюзам в месяц предоставляются бесплатно

Тарификация (https://cloud.yandex.ru/docs/api-gateway/pricing)

Запросы к API-шлюзам. Оплачивается только фактическое количество вызовов.

Услуга	Цена за 1 млн запросов, вкл. НДС
Запросы к API-шлюзам, до 100 000 запросов в месяц	Не тарифицируется
Запросы к API-шлюзам, свыше 100 000 запросов в месяц	120,0000

Исходящий трафик

При использовании сервиса оплачивается исходящий трафик из Yandex Cloud в интернет. Передача трафика между сервисами Yandex Cloud по внутренним адресам, как и входящий трафик из интернета, не тарифицируется.

Каждый месяц не тарифицируются первые 100 ГБ исходящего трафика.

Минимальная единица тарификации — 1 МБ.

Категория ресурса	Цена за ГБ
Исходящий трафик, первые 100 ГБ в месяц	Не тарифицируется
Исходящий трафик, свыше 100 ГБ в месяц	1,5300

На что обратить внимание

- Обязательно необходимо купить
- Необходимо оплачивать расходы на использование шлюза

GCP API Gateway

Сервис для управления API-шлюзами, поддерживающий спецификацию OpenAPI 2.0 и набор расширений для взаимодействия с другими облачными сервисами

Предоставляет полностью управляемое решение с оплатой по факту использования для размещения API.

Обеспечивает безопасный доступ к серверным службам через четко определенный REST API, который единообразен для всех ваших служб, независимо от их реализации.

Интегрирован с Google Cloud, поэтому возможно использовать те же инструменты разработки, мониторинга, ведения журналов и трассировки, которые используем с любым другим продуктом Google Cloud.

Если подключаемся к серверной службе, размещенной за пределами Google Cloud, вы все равно возможно воспользоваться всеми службами Google Cloud, включая службы аутентификации и авторизации, используемые для управления доступом к вашим API.

API Gateway позволяет обеспечить безопасный доступ к сервисам через четко определенный REST API, который единообразен для всех наших сервисов, независимо от их реализации.

Согласованный API:

- Упрощает использование сервисов разработчиками.
- Позволяет изменить реализацию серверной службы, не затрагивая общедоступный API.
- Позволяет воспользоваться функциями масштабирования, мониторинга и безопасности, встроенными в Google Cloud Platform (GCP).

Используя API Gateway, разработчики используют REST API для реализации приложений. Поскольку все API размещаются на API Gateway, разработчики видят единый интерфейс для всех серверных служб.

Развернув свои API на API Gateway, мы можем обновить серверную службу или даже переместить службу из одной архитектуры в другую без необходимости изменения API.

Пока API нашего сервиса остается согласованным, разработчикам не придется модифицировать развернутые приложения из-за базовых изменений в серверном интерфейсе.

Тарификация (https://cloud.google.com/api-gateway/pricing)

API Gateway взимает плату за вызовы Service Control . Каждый вызов API, обработанный API Gateway, регистрируется API Service Control как отслеживаемая операция и указывается в вашем счете как отдельная позиция для Service Control.

Цена API Gateway зависит от количества вызовов вашего API, как описано в следующей таблице:

Вызовы API в месяц на один платежный аккаунт	Стоимость миллиона вызовов API
0-2М	$0,00
2М-1Б	3,00 доллара США
1Б+	1,50 доллара США

Стоимость передачи данных

Передача данных в Google Cloud бесплатна.

Общее использование сети применяется к данным, которые выходят из Google. API-шлюз использует передачу данных уровня Premium в Интернет, цены указаны ниже.

Цены на передачу данных соответствуют ценам на Google Cloud Network – уровень Premium.

Цены указаны за ГБ в месяц.

Источник и назначение трафика	0–10 ТБ	10 ТБ-150 ТБ	150 ТБ+
Северная Америка в Северную Америку	0,105 доллара США	$0,080	$0,060
Европа в Европу	0,105 доллара США	$0,080	$0,060
Азиатско-Тихоокеанский регион в Азиатско-Тихоокеанский регион	0,120 доллара США	$0,085	$0,080
Южная Америка в Южную Америку	0,120 доллара США	$0,085	$0,080
Океания в Океанию	0,120 доллара США	$0,085	$0,080
Межконтинентальный (исключая Океанию и Китай)	0,120 доллара США	$0,085	$0,080
Межконтинентальный рейс в/из Океании	0,190 доллара США	$0,160	0,150 доллара США
Любой трафик в Китай	0,190 доллара США	$0,160	0,150 доллара США

На что обратить внимание

- Обязательно необходимо купить
- Необходимо оплачивать расходы на использование шлюза

Предложение по выбору API Gateway

Исходя из задач, которые требуется решать на текущий момент, по всем параметрам подходит open source решение Envoy

Последствия

При отказе от использования api gateway, возрастет время на интеграцию внешних пользователей, усложнится поддержка интеграций, есть риски нарушения безопасности при обмене информацией

Ссылки

https://habr.com/ru/companies/ru_mts/articles/716512/

https://geekflare.com/api-gateway/

https://www.tecmint.com/open-source-api-gateways-and-management-tools/

https://tyk.io/

https://www.krakend.io/

https://konghq.com/

https://habr.com/ru/articles/663056/

https://habr.com/ru/articles/665558/

https://nordicapis.com/6-open-source-api-gateways/

https://geekflare.com/api-gateway/

https://www.way2smile.ae/blog/top-10-open-source-api-gateways/

https://habr.com/ru/articles/482578/