
Яндекс

Дорога в облака.
Путь Яндекса.

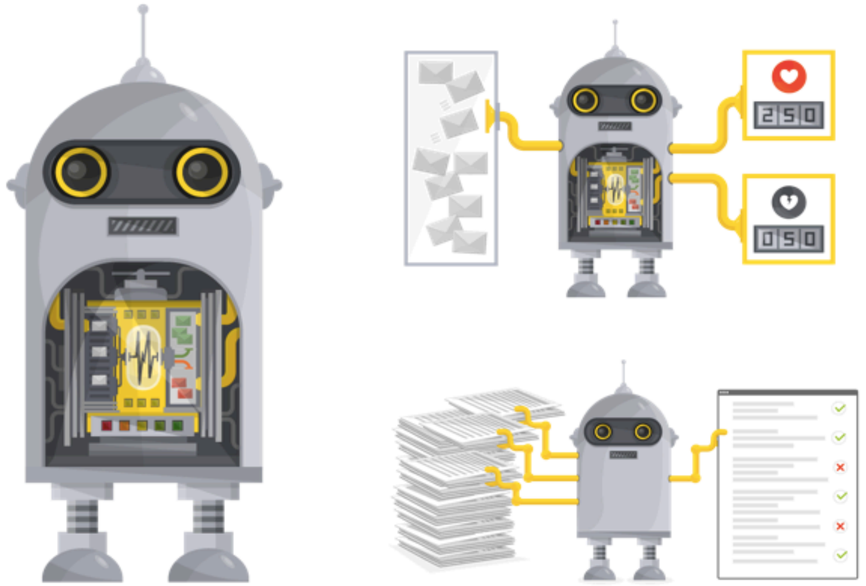
О чём поговорим

- Бизнес-цели отказа от железных машин в пользу облачной платформы
- Новые вызовы для информационной безопасности
- Правила жизни в облаках

Курс на облака

Для чего мы используем облака

- Выполнение расчётов, задач, обработка больших данных
- Запуск сервисов



Цели бизнеса

- Эффективная утилизация оборудования
- Повышение отказоустойчивости сервисов (непрерывность)
- Возможность горизонтального масштабирования
- Снижение затрат на администрирование

Что делать?

Необходима технологическая прослойка между сервисом/выполняемой задачей и оборудованием, чтобы сделать их работу непрерывной при эффективном расходовании ресурсов

Как этого добиться?

Создание единой среды для запуска сервисов и задач (единое ядро, единая сборка nginx и пр.)

- Сбор и анализ потребностей
- Дизайн единого решения
- Реализация и «великое переселение»

Гибкость vs. Безопасность

- «Полная виртуализация» (kvm): условно безопасно, но очень большие затраты

- «Легковесная контейнеризация» (а-ля linux cgroups): максимальная эффективность, но очень много проблем безопасности

- Мы в итоге пошли по второму пути :)

Структура облака

Основные компоненты облака

- Интерфейс для потребителей
- Управление ресурсами
- Управление окружением
- Железные машины

Курс на безопасные облака?

Максимальная изоляция

Риск: из контейнера можно получить доступ к соседнему контейнеру или к хост-машине

Дополнительная изоляция:

- Изоляция для инженера облака и изоляция для инженера ИБ — совсем разные подходы

Отсутствие изоляции может быть бизнес-необходимостью

Межкомпонентная аутентификация

- Риск: несанкционированный доступ к управляющим компонентам платформы
- Все компоненты, API, транспорты и пр. должны иметь взаимную аутентификацию
- Без снижения скорости выполнения задач

Сетевая безопасность

- Риск: сеть плоская, так как в случае тысяч постоянно мигрируемых контейнеров «динамическая сегментация» будет стоить дорого

- Доступ разграничивается не на L3, а на L7 (межсервисная аутентификация)

- Требует высокого уровня зрелости в написании сервисов

Единый балансер

- Риск: «Честные» сертификаты управляются отдельными командами, а не единым механизмом

- Для доступа в мир отдельные балансеры с расположенными на них сертификатами

Балансеры на внутренних инструментов

- Риск: разграничение доступов пользователей внутренних сервисов
- SLB per service

Доступ DevOps к приложению

- Риск: избыточные доступы разработчиков при отладке приложений
- ssh-доступ только к своему контейнеру (не на хост-машину)
- Разные режимы и набор компонент при запуске приложения и его отладке

Адаптация окружения

- Риск: избыточные привилегии и доступные компоненты при использовании недоверенных сервисов (например, third-party)

- Безопасное окружение (сетевая изоляция, ограничение системных вызовов, пр.)

Требования к сервисам

- Риск: недоверенная среда при запуске сервиса, влияние уязвимых сервисов друг на друга
- Все компоненты, API и пр. должны иметь взаимную аутентификацию
- Security Audit

Мониторинг событий

- Риск: доступ злоумышленника к компонентам платформы опасен для всех запускаемых сервисов
- Сбор логов с хостов, критичных компонент платформы, приложений
- Анализ событий и инцидентов

Жизнь в облаке

Жизнь в облаке

- Важно чётко определить правила жизни в «коммунальной квартире»
- Правила для потребителей: высокий уровень зрелости и внедрение SDLC
- Платформа предоставляет все необходимые инструменты обеспечения безопасности

Самое сложное и интересное

Анализировать облачную платформу, разрабатывать дизайн инструментов безопасности и добиваться их реализации вместе с активной доработкой самой платформы


Welcome To
The Future

Контакты

- Наталья Куканова, Vice CISO
- sterh@yandex-team.ru