Отказоустойчивость в облаке

Александр Зубарев
Директор Центра информационной безопасности ВШИТиАС САФУ

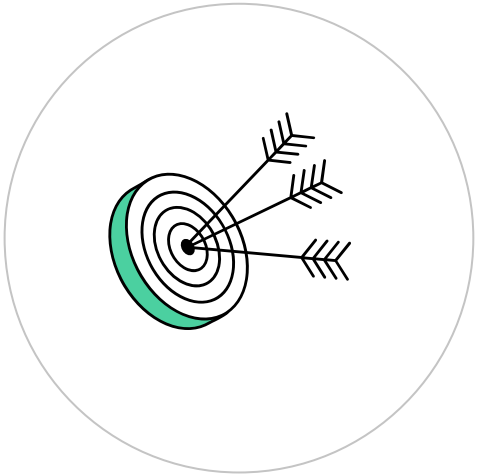
Александр Зубарев

О спикере:

- председатель цикловой комиссии информационной безопасности инфокоммуникационных систем, АКТ (ф) СПбГУТ
- эксперт CCNA Routing & Switching, security
- мастер-эксперт по компетенции WSR «Кибербезопасность»
- преподаватель высших квалификационных категорий
- преподаватель кафедры информационной безопасности в САФУ

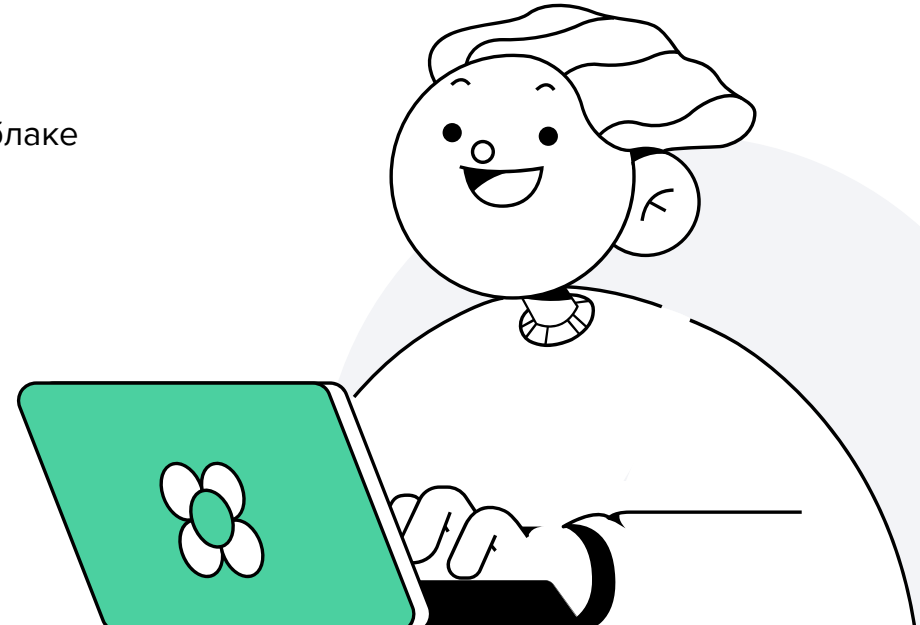
Цели занятия

- Узнать, почему важно строить отказоустойчивые системы
- Рассмотреть основные сценарии отказа инфраструктуры
- Познакомиться с механизмами повышения доступности приложения в Яндекс Облаке



План занятия

1. Что такое отказоустойчивость и зачем она нужна
2. Из чего складывается отказоустойчивость
3. Почему сервис может быть недоступен
4. Как снизить риски сбоя сервиса
5. Как сделать отказоустойчивый сервис в Яндекс Облаке
6. Итоги
7. Домашнее задание
8. Дополнительные материалы



Что такое отказоустойчивость и зачем она нужна

1

У любого сервиса есть SLA.
SLA — это набор метрик и их допустимых значений между пользователем сервиса и провайдером сервиса.

Одна из метрик* SLA для любого сервиса — его доступность

* Помимо доступности, в SLA сервиса могут быть и другие метрики

Отказоустойчивость — способ увеличения доступности сервиса

Когда нужна отказоустойчивость

Когда недоступность сервиса ведёт к финансовым потерям:

- в связи с упущенной выручкой и прибылью
- потерей пользователей/клиентов
- негативной репутацией (пользователи ждут 100% uptime)
- нарушением требований регуляторов
- нарушением критических бизнес-процессов компании

Но отказоустойчивость — это дополнительные затраты на сервис, поэтому важно применять её тогда, когда это целесообразно

Когда отказоустойчивость необязательна

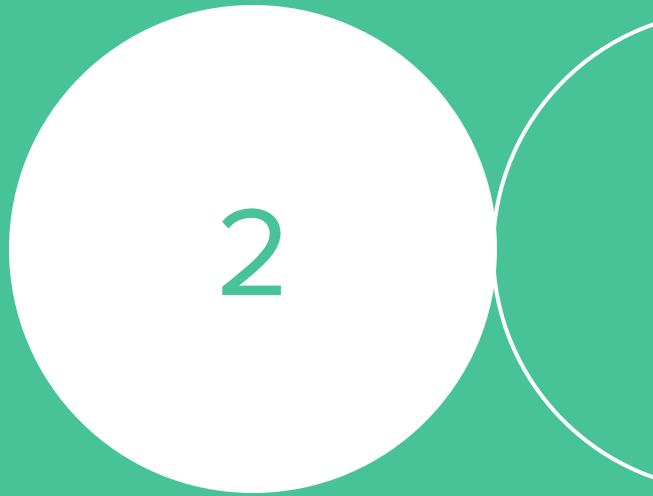
Бывают ситуации, когда отказоустойчивость может быть избыточной:

- среды разработки и тестирования
- задачи, у которых нет SLA по доступности, например батч-задачи

Важно во всех сервисах, где доступность приложения — часть SLA, договориться о метриках доступности, даже если высокая доступность не требуется

Из чего складывается отказоустойчивость

Примеры



Из чего состоит отказоустойчивость

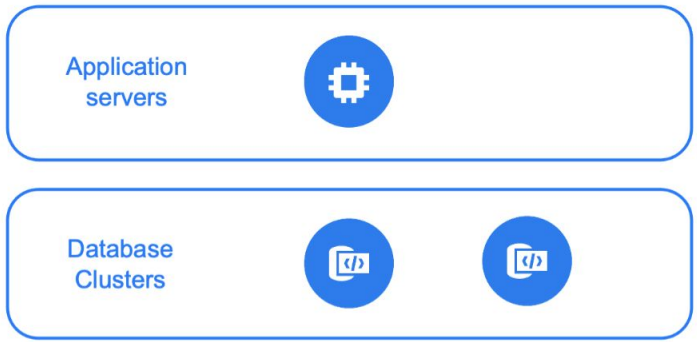
- Избыточность (redundancy)
- Мониторинг узлов
- Реакция на сбой (failover)
- Возвращение узла в кластер (failback)

Нужно понимать, из каких компонентов состоит сервис,
чтобы сделать эти компоненты отказоустойчивыми

Примеры плохой архитектуры

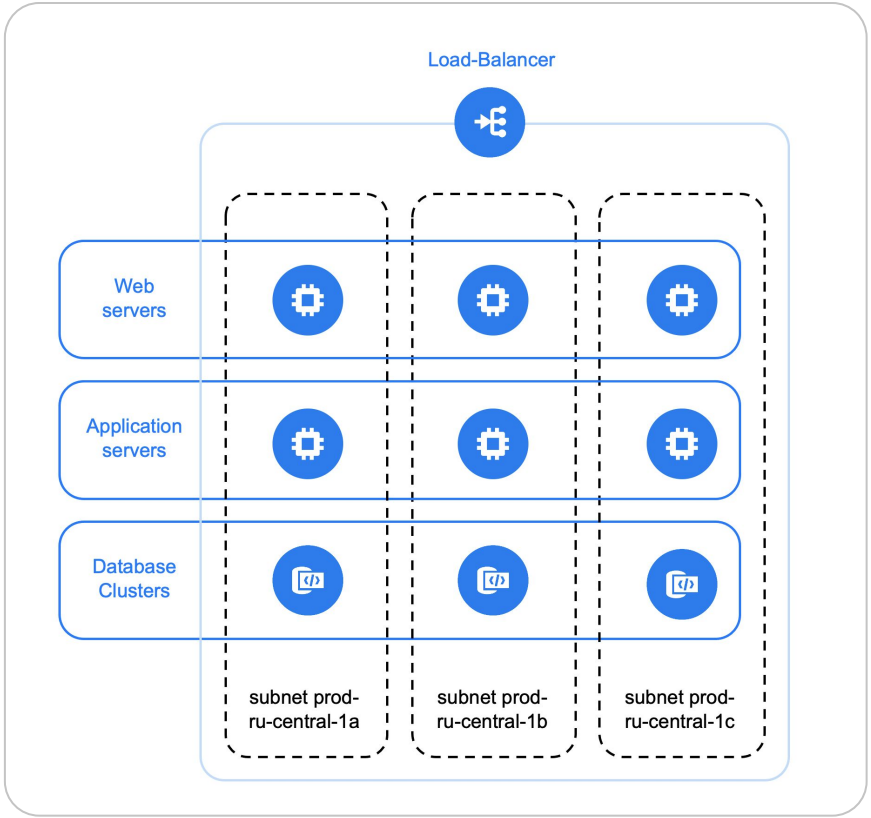
- Всё приложение крутится на одной ВМ

- Данные реплицированы, но есть точка отказа



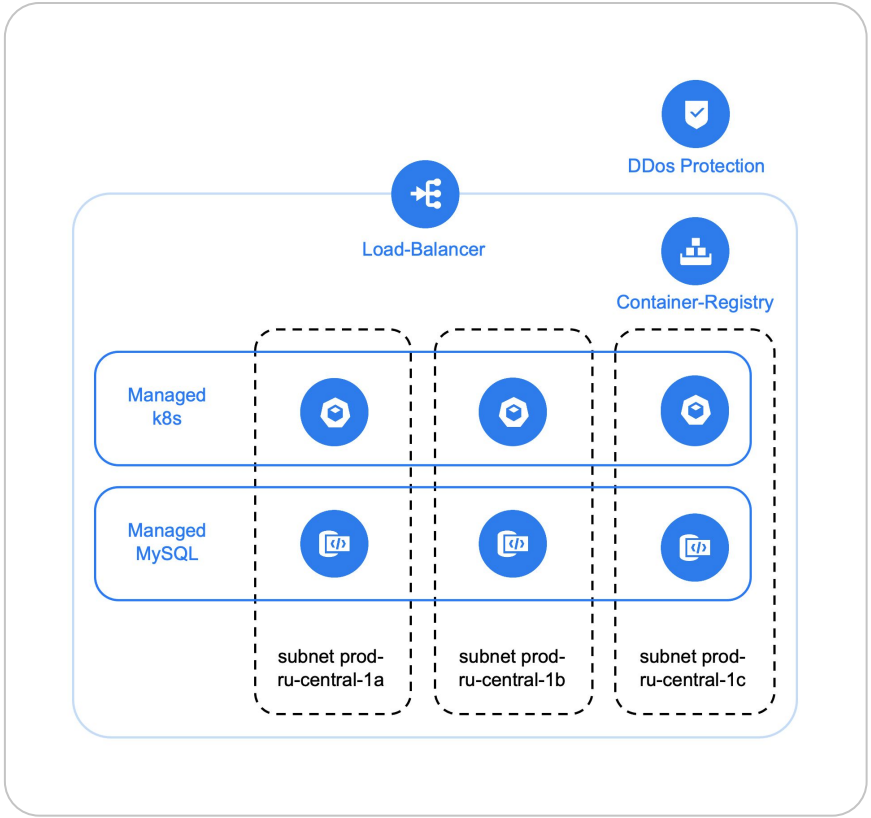
Пример хорошей архитектуры

- Веб-серверы находятся за внешним балансировщиком нагрузки
- Веб-серверы балансируют трафик на серверы приложений
- Серверы приложений «ходят» в мастера и реплики БД



Пример архитектуры на базе k8s

- Балансировщик защищён услугой DDoS Protection
- Ноды кластера находятся за балансировщиком нагрузки
- Ingress controller принимает входящий трафик от балан-сировщика и направляет на сервисы
- Сервисы «ходят» в мастера и реплики БД

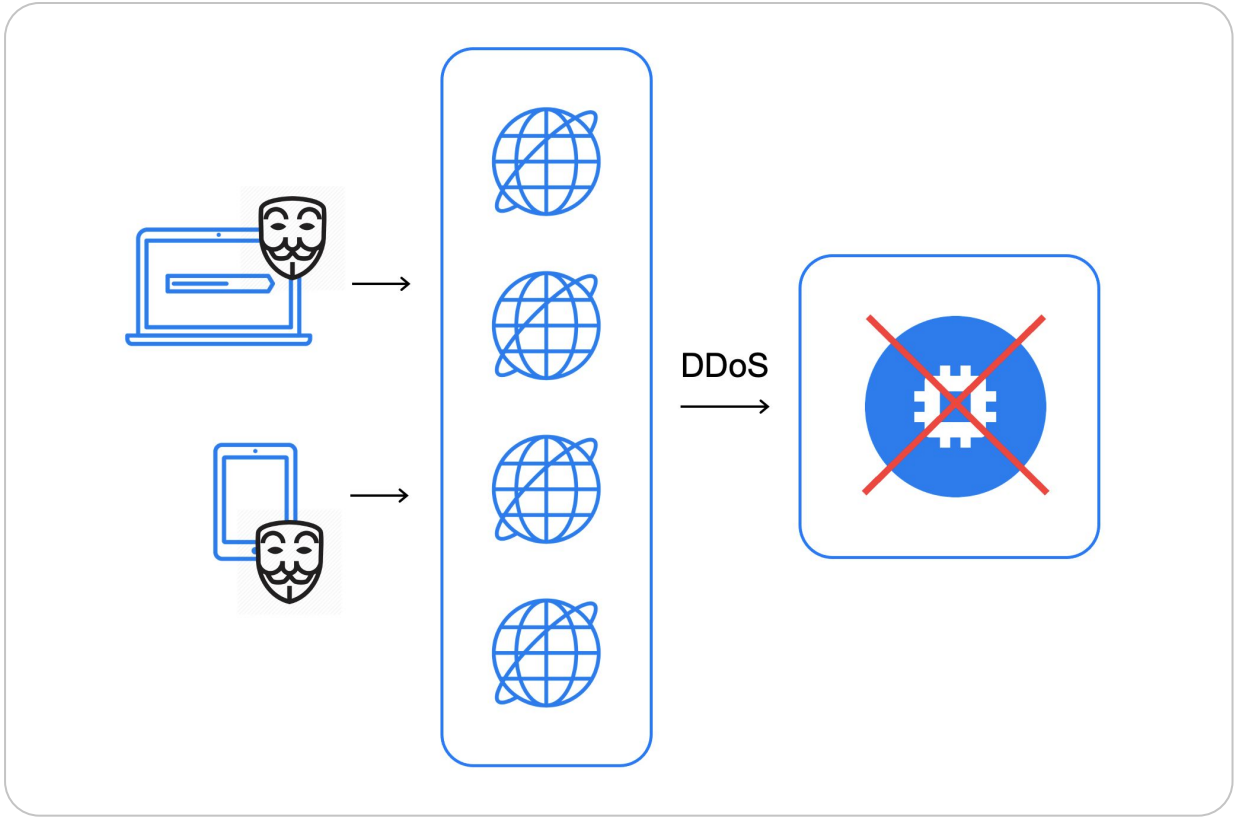


Почему сервис может быть недоступен

3

Атака

- DoS
- DDoS



Проблемы из-за инфраструктуры

Сбой на стороне инфраструктуры

- Отказ физического сервера / стойки
- Отказ зоны доступности / дата-центров (ДЦ)
- Сетевые проблемы
- Проблемы с дисковой подсистемой

Решение — превышение квот и лимитов работы инфраструктуры

- Понимание разницы между квотами и лимитами

  Примеры лимитов в Яндекс Облаке:

  - сеть: лимит по flow
  - диск: лимит на производительность

Проблемы из-за настроек сервиса

Сбой на стороне приложения

- Утечки памяти, утечки на ядре ОС
- Конец свободного места в файловой системе
- Баг в новом релизе софта
- Баг в сторонней библиотеке

Перегрузка

- Резкий всплеск активности — Хабраэффект, Чёрная пятница
- Постоянный рост нагрузки
- Следствие сбоя на стороне инфраструктуры

Как снизить риски сбоя сервиса

4

Атака

DoS

- Анализируйте приложение на уязвимости.
  Примеры сканеров: Burp Suite, Acunetix, Nessus
- Можно заказать pentest от Лаборатории Касперского, Group-IB, BI.ZONE
- Используйте web application firewall: Imperva, F5, NGINX Plus, Wallarm, Cloudflare

DDoS

- Яндекс Облако, Qrator Labs, Cloudflare, Akamai
- Автомасштабирование: Instance Groups, Managed Kubernetes

Сбой на стороне инфраструктуры

Сбой сервера

- Балансировка нагрузки с использованием healthchecks
- Anti-affinity-правила — гарантия того, что копии сервиса запускаются

Сбой дата-центра

- Балансировка нагрузки на несколько дата-центров
- Disaster recovery

Сбой из-за лимитов

Сеть

- Читайте документацию
- Используйте средства для уменьшения паразитной нагрузки
- Горизонтально масштабируйте нагрузку

Диски

- Читайте документацию
- Увеличивайте размер диска и число дисков
- Горизонтально масштабируйте нагрузку

Сбой на стороне приложения

ОС

- Мониторинг ОС (потребление RAM, CPU, свободного места)
- Обновление ОС и ядра
- Масштабирование места на диске

Сбой на стороне приложения

Баги

- Dev/stage-среды
- Юнит-тесты, интеграционные тесты
- Возможность сделать rollback
- Современные методики деплоя
- Учения
- Feature-флаги

Перегрузка

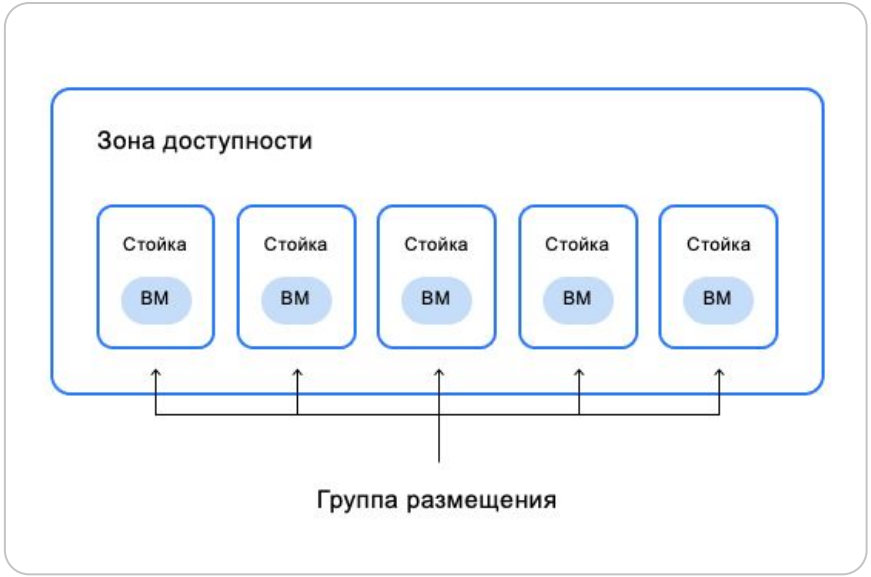
1. Реализовывайте сайзинг — приложение должно уметь обрабатывать нагрузку:
   - при падении нескольких узлов
   - при падении дата-центра
2. Готовьтесь к возможной неравномерной балансировке
3. Делайте мониторинг нагрузки
4. Делайте нагрузочное тестирование перед вводом в продакшн
5. Приложение должно уметь горизонтально масштабировать входящую нагрузку: автоматически или вручную
6. Аккуратно комбинируйте резервирование и автомасштабирование: алгоритмы автоскейлинга могут не успеть масштабировать нагрузку при высоких её всплесках

Как сделать отказоустойчивый сервис в Яндекс Облаке

5

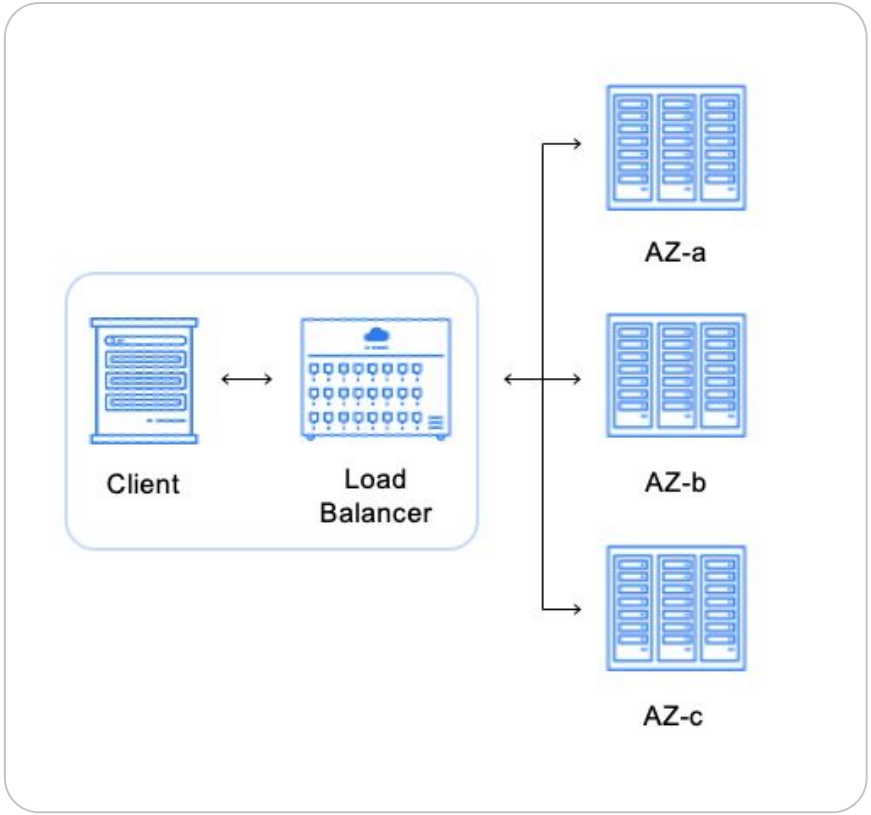
Yandex Compute Cloud

- ВМ и диск — сущность зоны доступности
- Группа размещения (placement groups) позволяет гарантировать, что ВМ будут находиться в разных стойках



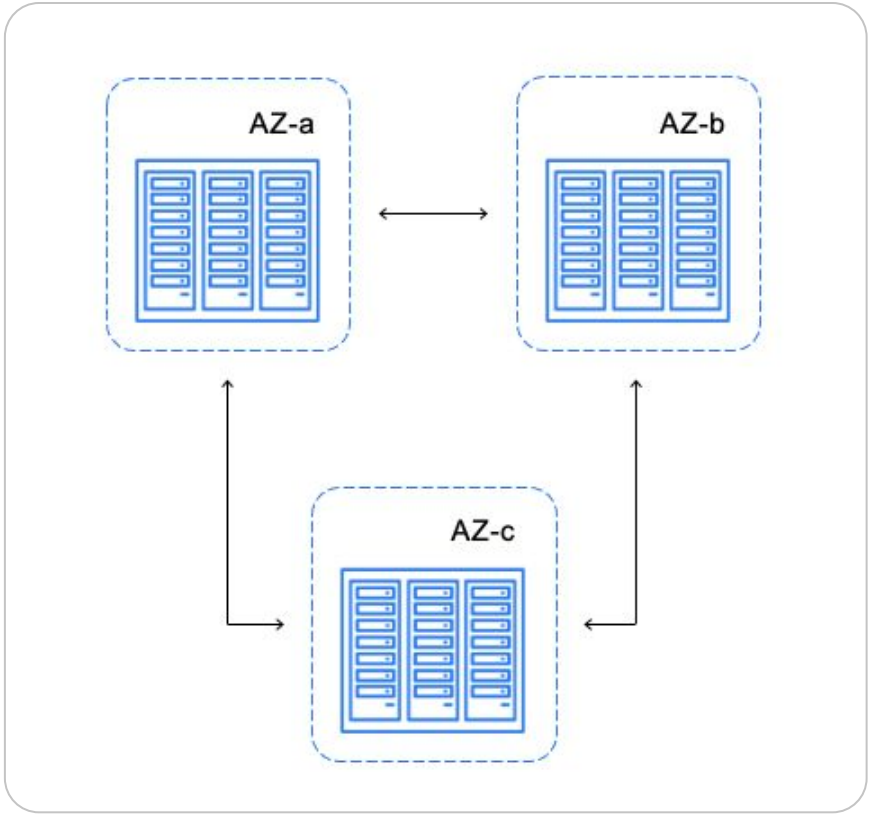
Yandex Load Balancer

- Есть стабильный статический IP-адрес
- Можно подключить Anti-DDoS
- Есть cross-AZ-балансировка нагрузки
- Трафик на зоны доступности приходит с помощью ECMP
- Трафик внутри зоны доступности использует consistent hashing



Virtual Private Cloud

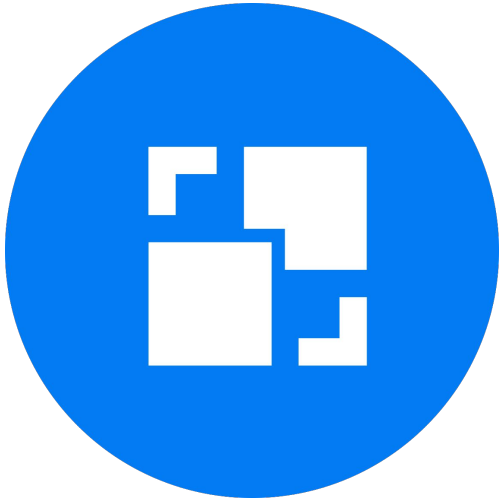
- Зона доступности — независимый дата-центр
- VPC обеспечивает полную IP-связность между зонами доступности
- Есть latency между зонами
- Сервис позволяет защитить виртуальные машины с помощью Anti-DDoS



Instance Groups

Управляемый сервис для работы
с группой виртуальных машин.

- Горизонтальное масштабирование на несколько AZ
- Автоматическое масштабирование
- Rolling update
- Интеграция с Load Balancer



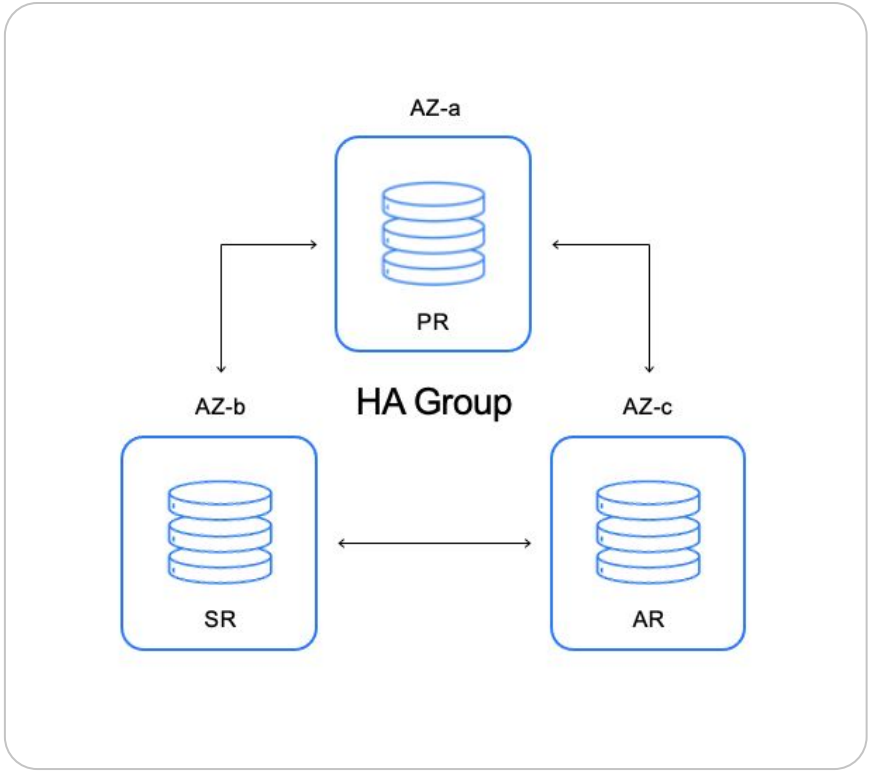
Yandex Managed Kubernetes

- Managed Kubernetes:
  - отказоустойчивые мастеры
  - много нативной функциональности для доступности и масштабирования контейнеров
  - интеграция с балансировщиком нагрузки
- Автомасштабирование узлов
- Интеграция с Container Registry, Load Balancer

Managed Databases

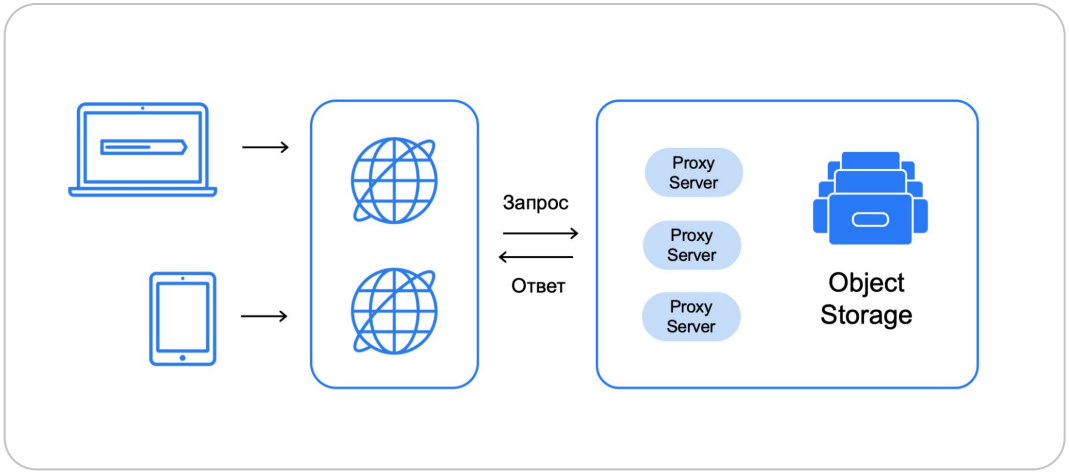
Виды конфигураций:

- кластер (минимум 2 узла) — разные AZ
- возможность масштабирования вверх



Yandex Object Storage

- Бесконечно масштабируемый по нагрузке Object Storage
- Данные реплицированы на 3 ЦОД
- Есть поддержка SSL и кастомного домена
- Есть интеграция с CDN



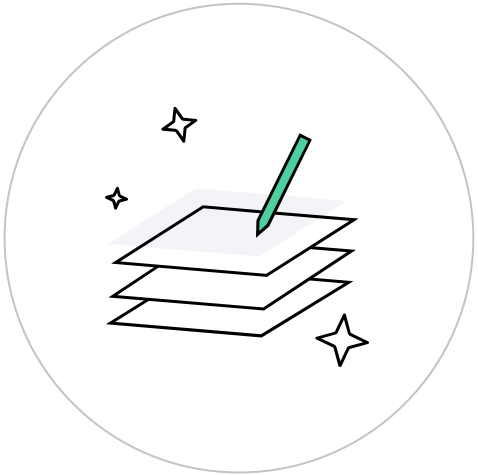
Итоги занятия

- Узнали, что такое отказоустойчивость и зачем она нужна
- Рассмотрели сценарии, от которых надо защищать приложение
- Прошлись по базовым сервисам Яндекс Облака,
  которые позволяют увеличить доступность вашего сервиса

Домашнее задание

Давайте посмотрим ваше домашнее задание

1. Вопросы по домашней работе задавайте в чате группы
2. Задачи можно сдавать по частям
3. Зачёт по домашней работе ставят после того, как приняты все задачи



Дополнительные материалы

- Public Cloud. Гайд по масштабированию
- Настройка отказоустойчивой архитектуры в Яндекс Облаке
- Google SRE Books

Задавайте вопросы и пишите отзыв о лекции

Александр Зубарев
Директор Центра информационной безопасности ВШИТиАС САФУ