

Kubernetes 101: **ОСНОВЫ**

Андрей Ветров

Senior Systems Engineer,
VMware



Непрерывная доставка

Source: Pivotal – The Journey to Cloud Native

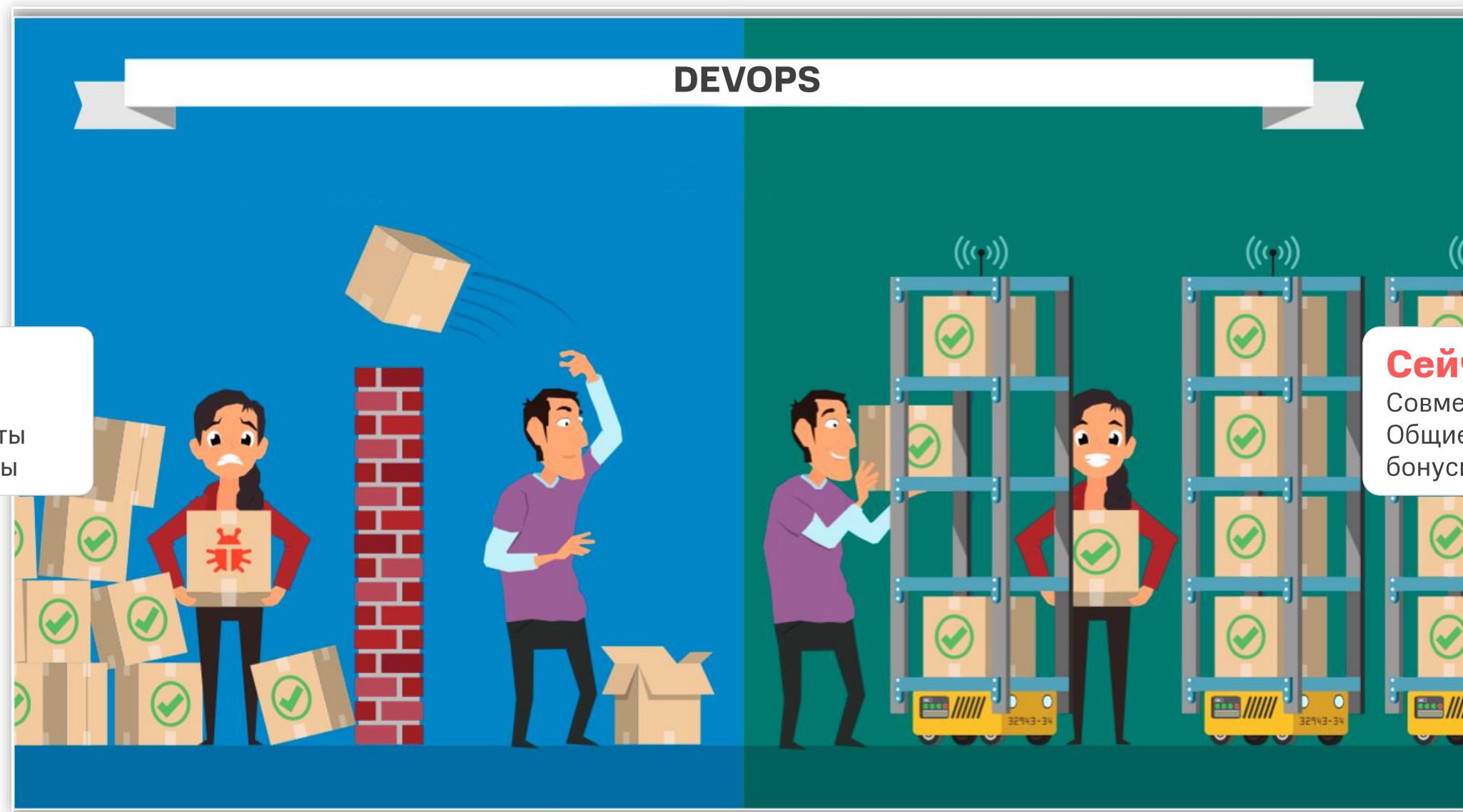


Раньше:
Выпуск новой версии 1 раз в полгода
Много проблем в реальной среде

Сейчас:
Выпуск новой версии 1 раз в неделю
Требования высоких стандартов кода от бизнеса

DevOps

Source: Pivotal – The Journey to Cloud Native



Раньше:

Не моя проблема
Раздельные инструменты
Непрозрачные процессы

Сейчас:

Совместная ответственность
Общие инструменты, процессы,
бонусы и культура

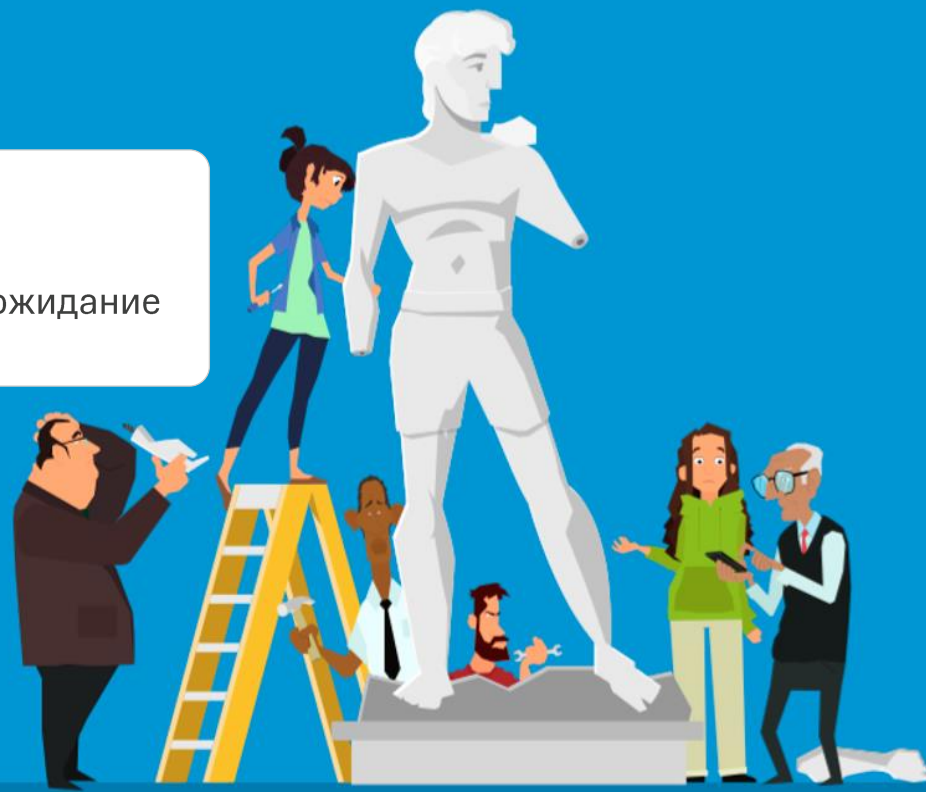
Микросервисы

Source: Pivotal – The Journey to Cloud Native

МИКРОСЕРВИСЫ

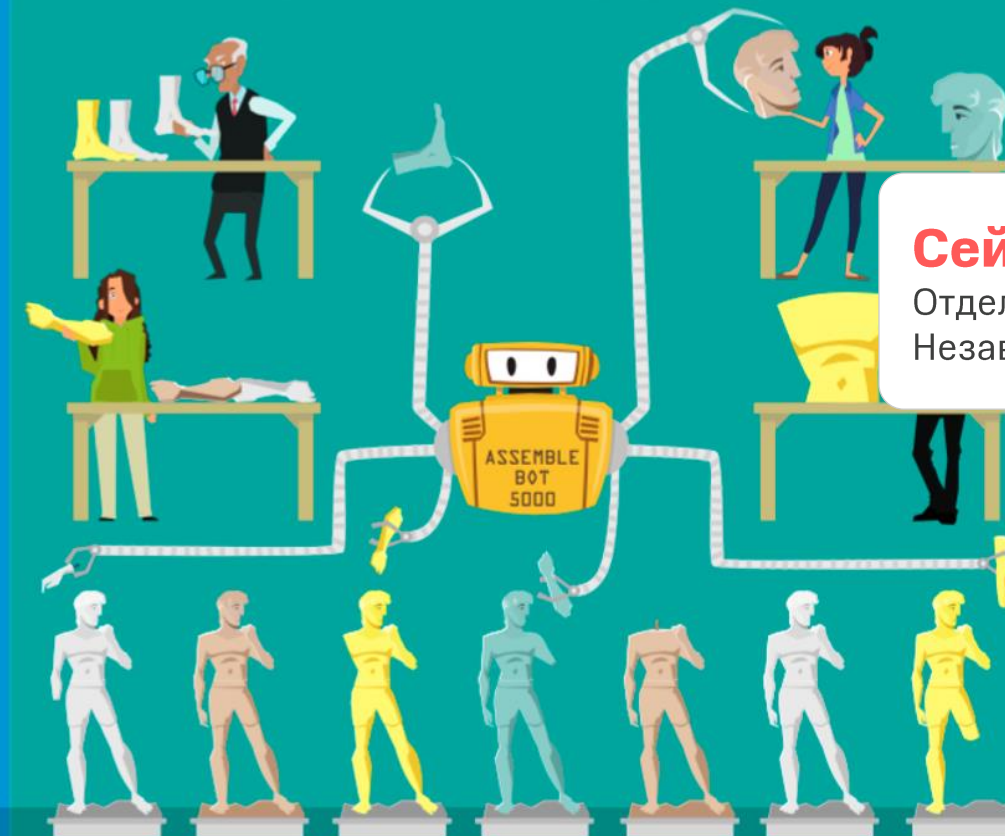
Раньше:

Монолитные приложения
Долгий цикл разработки: ожидание тестов и команды



Сейчас:

Отдельные небольшие сервисы
Независимое развертывание



Контейнеры

Source: Pivotal – The Journey to Cloud Native

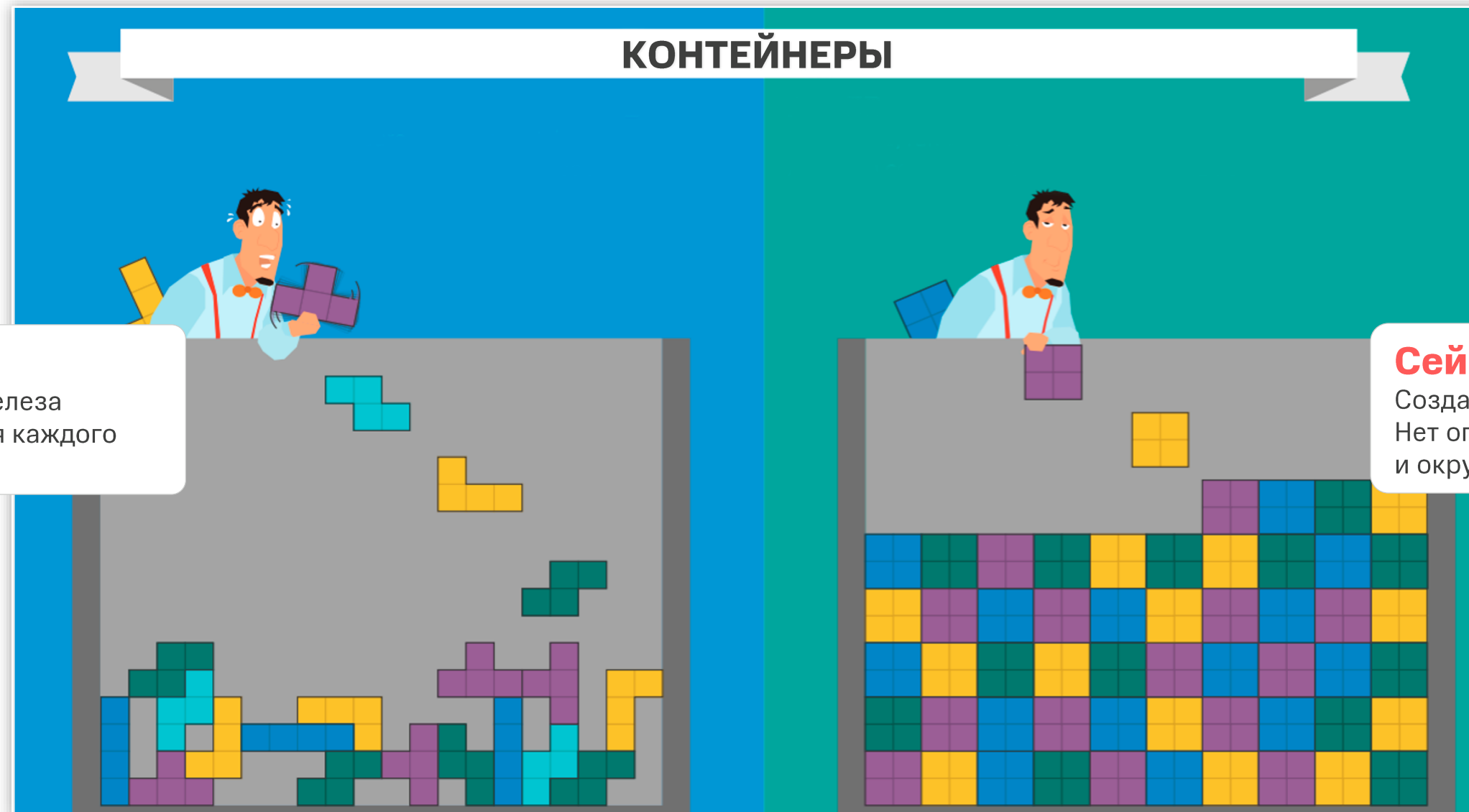
КОНТЕЙНЕРЫ

Раньше:

Совместимость ПО и железа
Сборка кода заново для каждого окружения

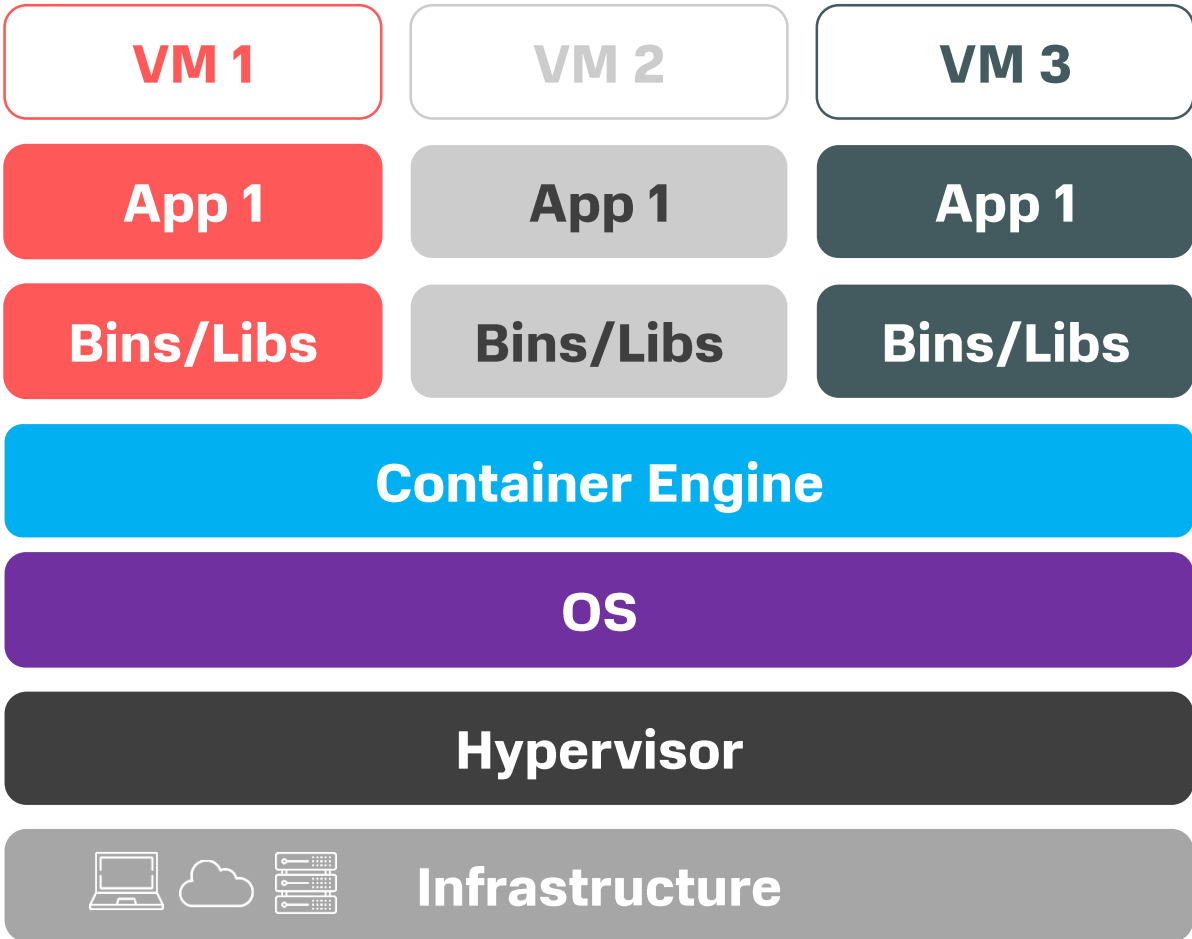
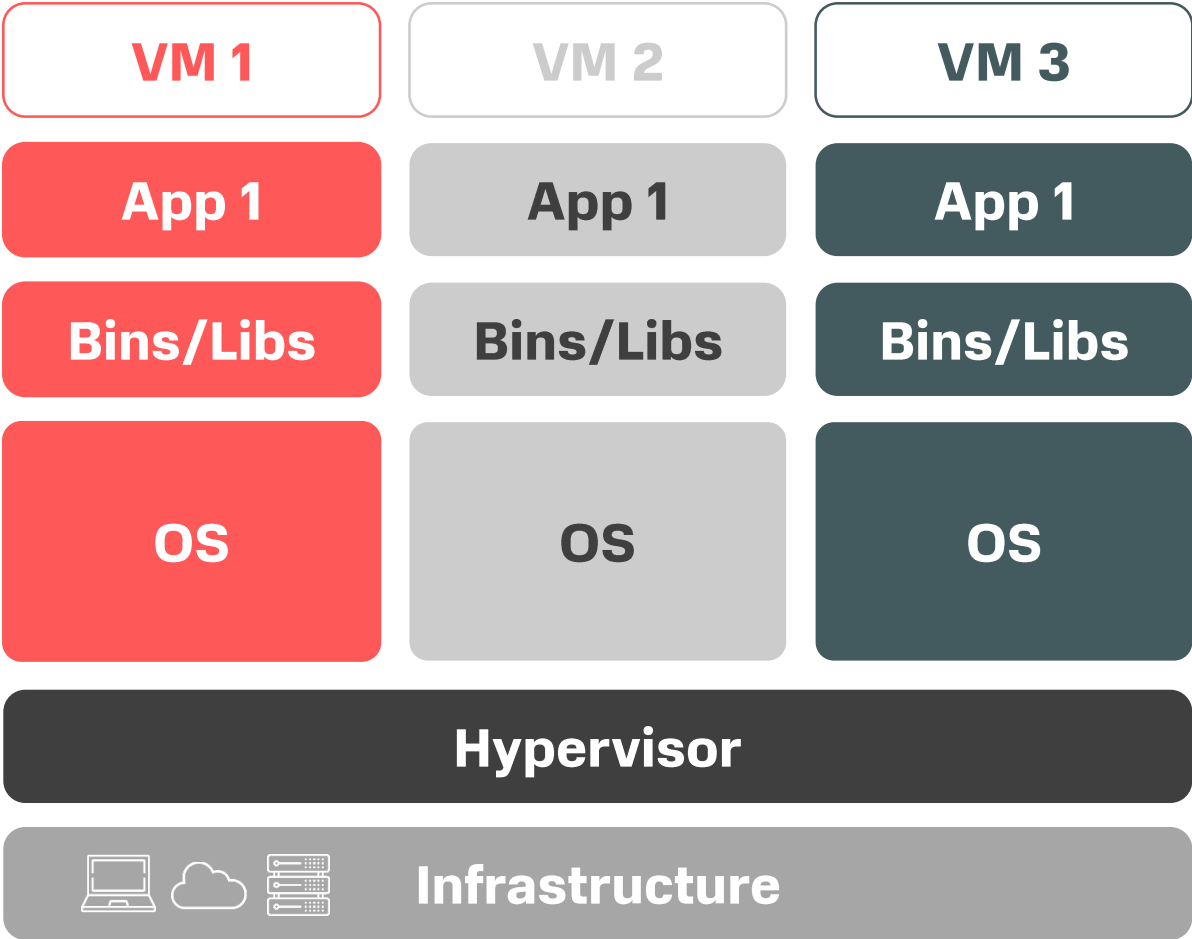
Сейчас:

Создал один раз, запустить
Нет ограничений к оборудованию и окружению



VM vs Containers

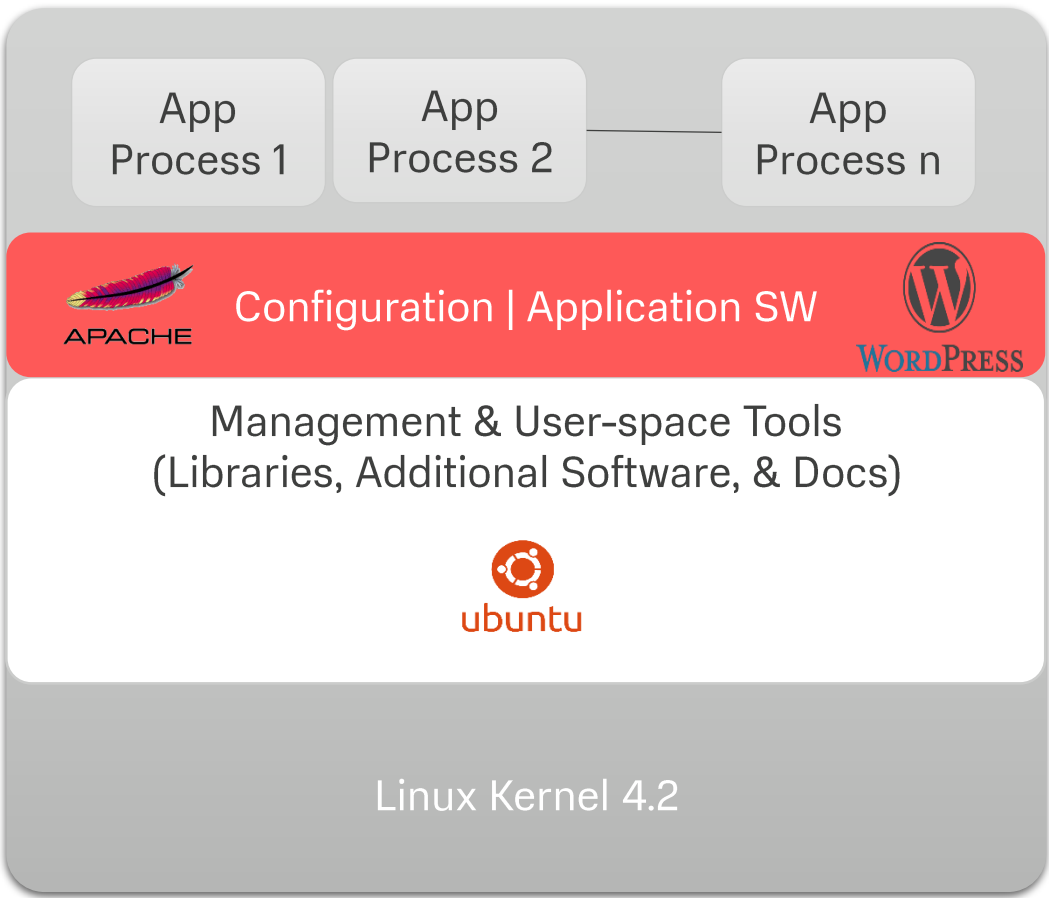
Вспомним про Docker



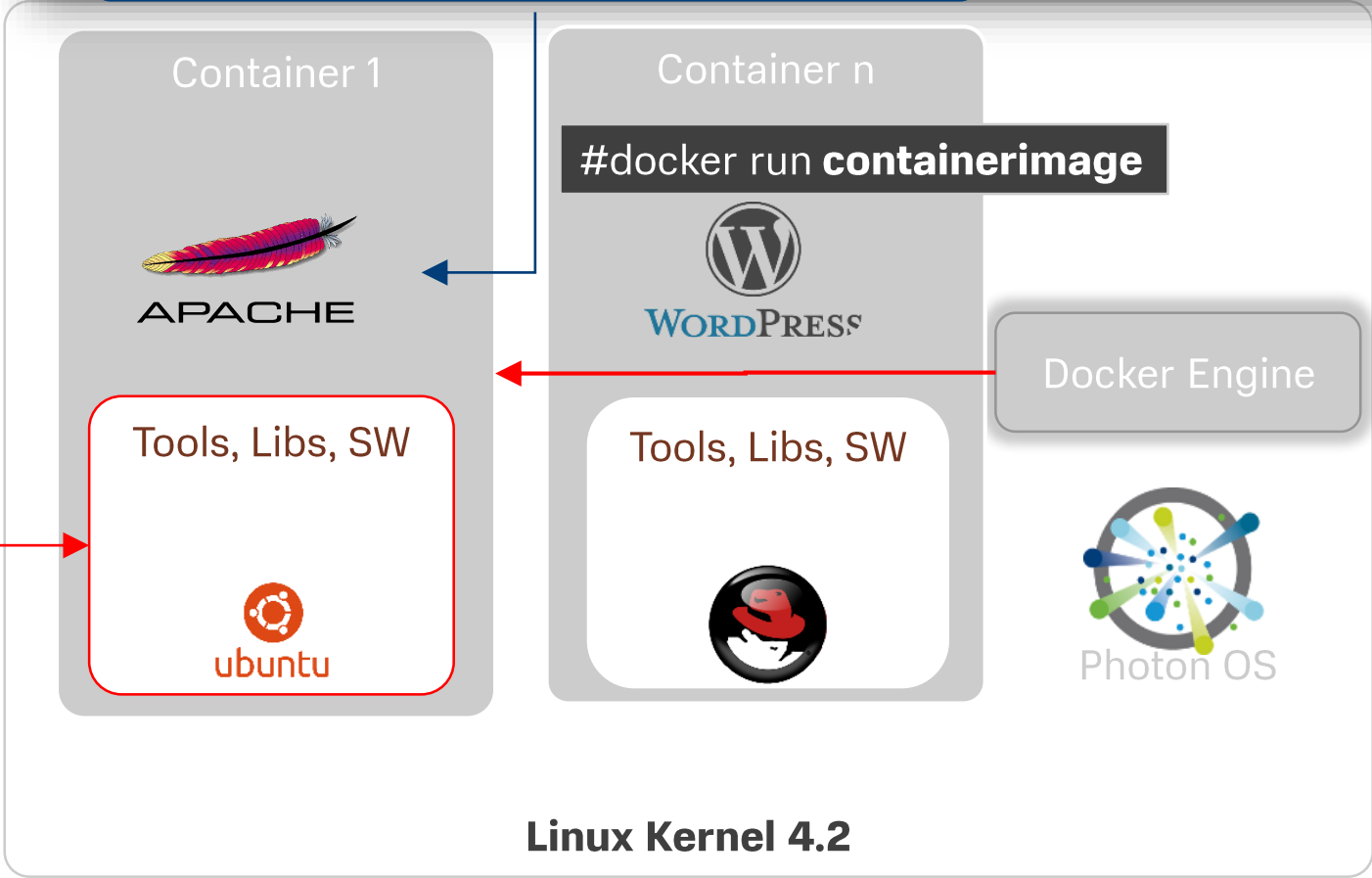
Зачем нужны контейнеры?

Container image создается через Dockerfile

```
15 lines (9 sloc) | 389 Bytes
1 # A basic apache server. To use either add or bind mount content under /var/www
2 FROM ubuntu:12.04
3
4 MAINTAINER Kimbro Staken version: 0.1
5
6 RUN apt-get update && apt-get install -y apache2 && apt-get clean && rm -rf /var/lib/apt/1
7
8 ENV APACHE_RUN_USER www-data
9 ENV APACHE_RUN_GROUP www-data
10 ENV APACHE_LOG_DIR /var/log/apache2
11
12 EXPOSE 80
13
14 CMD ["/usr/sbin/apache2", "-D", "FOREGROUND"]
```



Standard Linux Host

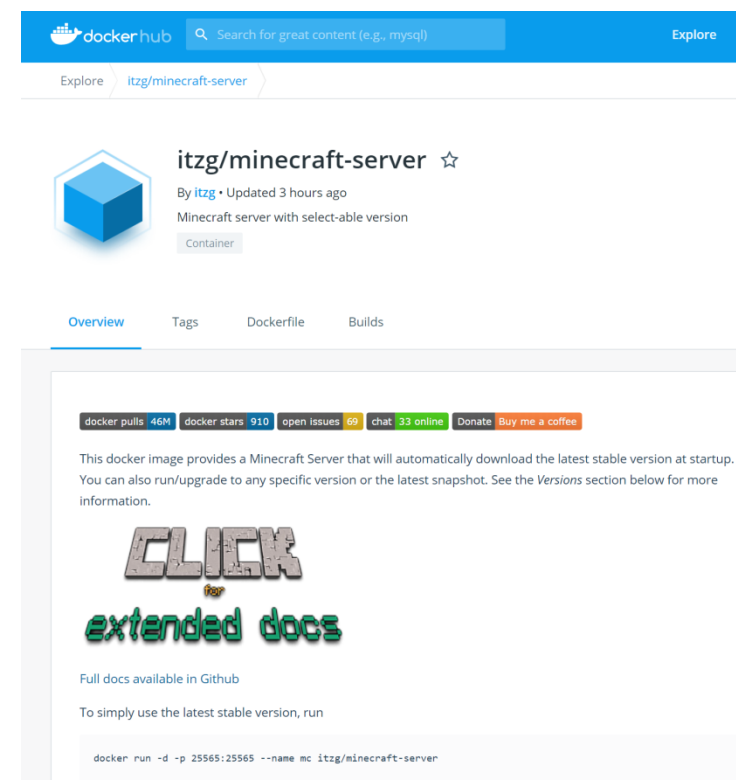


Linux Container Host

Вспомним про Docker

```
docker run -d -p 25565:25565 --name mc itzg/minecraft-server
```

```
docker run -d -e VERSION=1.7.9 ...
```



The screenshot shows the Docker Hub page for the `itzg/minecraft-server` image. It includes the Docker Hub logo, search bar, and navigation tabs for Overview, Tags, Dockerfile, and Builds. The main content area features the image name, a star icon, and a description: "Minecraft server with select-able version". Below this, there are statistics for pulls (46M), stars (910), open issues (69), and chat (33 online). A "CLICK extended docs" button is visible. At the bottom, there is a code block for the `docker run` command: `docker run -d -p 25565:25565 --name mc itzg/minecraft-server`.

Dockerfile – это сценарий, который состоит из последовательности команд и аргументов, необходимых для создания образа.

```
minecraft.dockerfile
1 FROM adoptopenjdk/openjdk13:alpin
2
3 LABEL maintainer "itzg"
4
5 RUN apk add --no-cache -U \
6     openssl \
7     imagemagick \
8     lsof \
9     su-exec \
10    shadow \
11    bash \
12    curl iputils wget \
13    git \
14    jq \
15    mc
```

Docker-compose.yml – это описание мультиконтейнерного docker-приложения.

```
docker-compose.yml
1
2 version: '3'
3 # Other docker-compose examples in /examples
4
5 services:
6   minecraft:
7     image: itzg/minecraft-server
8     ports:
9       - "25565:25565"
10    volumes:
11      - "mc:/data"
12    environment:
13      EULA: "TRUE"
14      CONSOLE: "false"
15      ENABLE_RCON: "true"
16      RCON_PASSWORD: "testing"
17      RCON_PORT: 28016
18    restart: always
19  rcon:
20    image: itzg/rcon
21    ports:
22      - "4326:4326"
23      - "4327:4327"
24    volumes:
25      - "rcon:/opt/rcon-web-admin/db"
26
27 volumes:
```

Новые «вызовы» при использовании контейнеров

Контейнеры у разработчиков

Ну что, «ни единого разрыва»? ;0

Containers

Контейнеры в проде

- Load Balancing
- Security
- High Availability
- Application Updates
- Scaling up/down
- Repeatable Deployments
- Replication
- Scheduling
- Containers



RENA
MONROVIA

Что такое Kubernetes (K8s)

Kubernetes — это open-source-платформа для управления и автоматизации развертывания, масштабирования и управления контейнеризированными приложениями кластера рабочих узлов (worker nodes).

Ключевые возможности:

- Скорость и повторяемость развертывания
- Масштабирование «на лету»
- Простой выкат новых релизов
- Оптимизация затрат ресурсов



kubernetes

Сущности K8s

Namespace

- RBAC

Pod

- ServiceAccount

ReplicaSet

- User

Deployment

- Group

DeamonSet

- Role

Job / CronJob

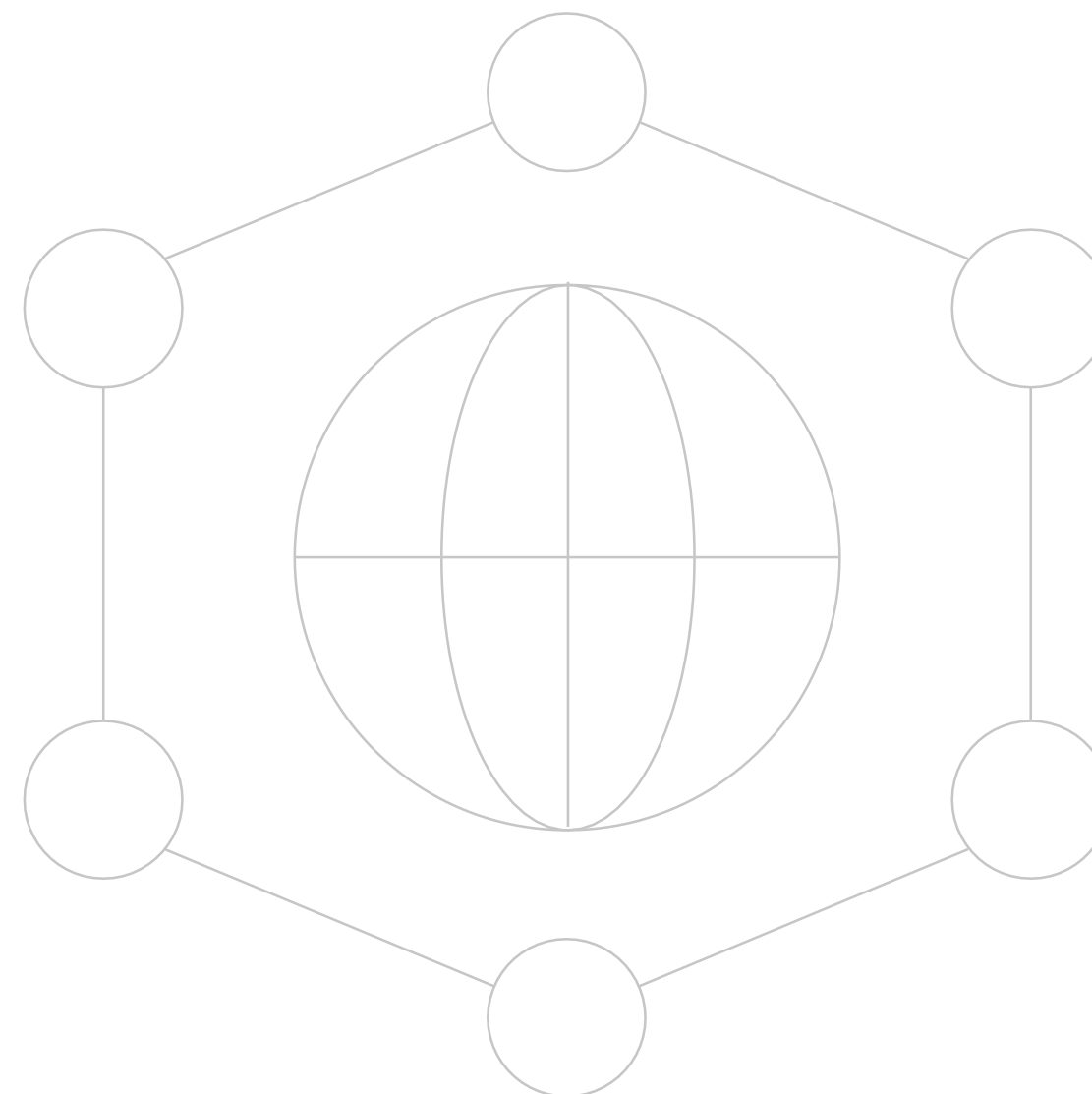
- RoleBinding

ConfigMap

- ClusterRole

Secret

- ClusterRoleBinding

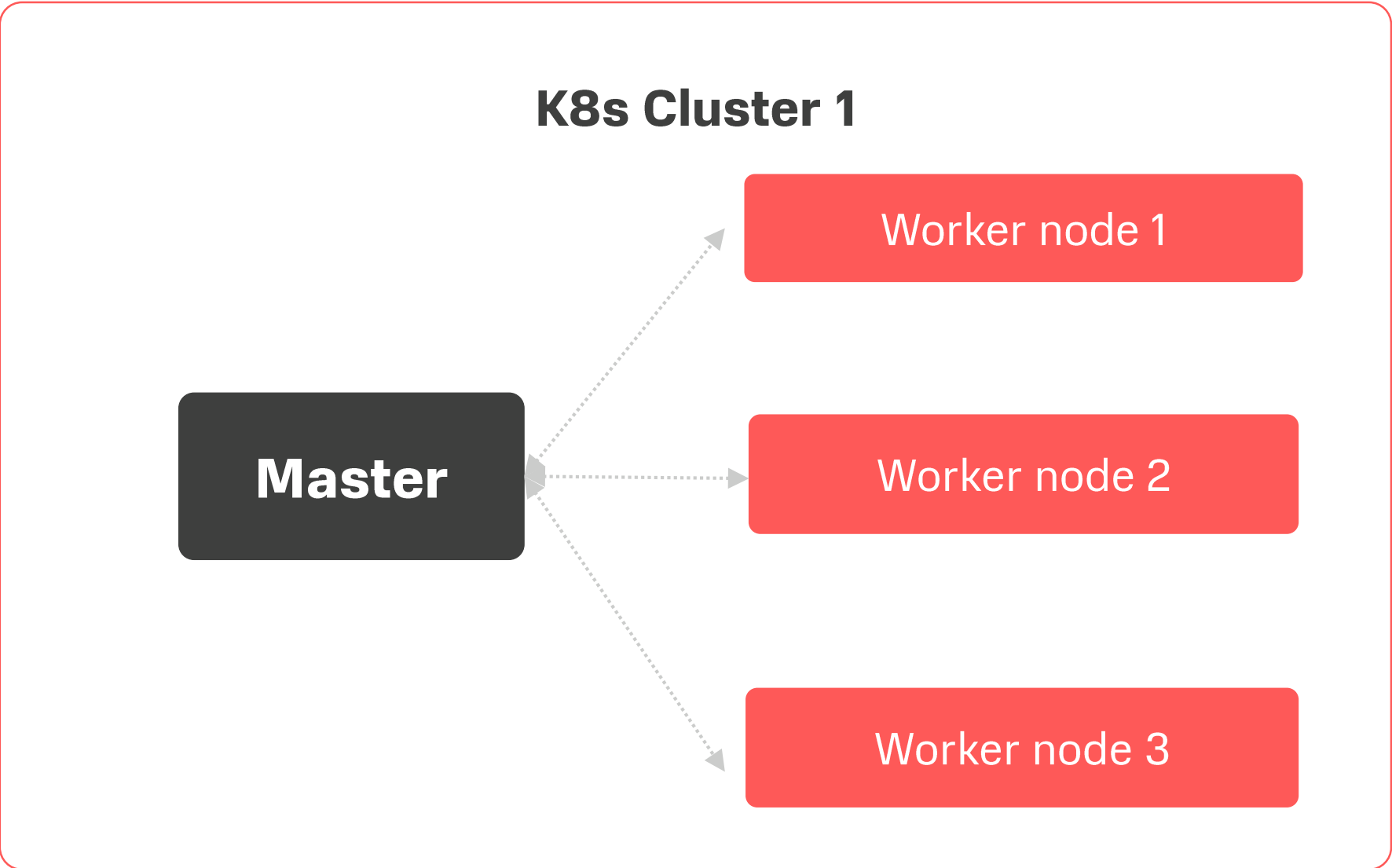


K8s Cluster

Master + worker nodes

Namespaces

Механизм разделения ресурсов в логические группы нагрузок



K8s Master

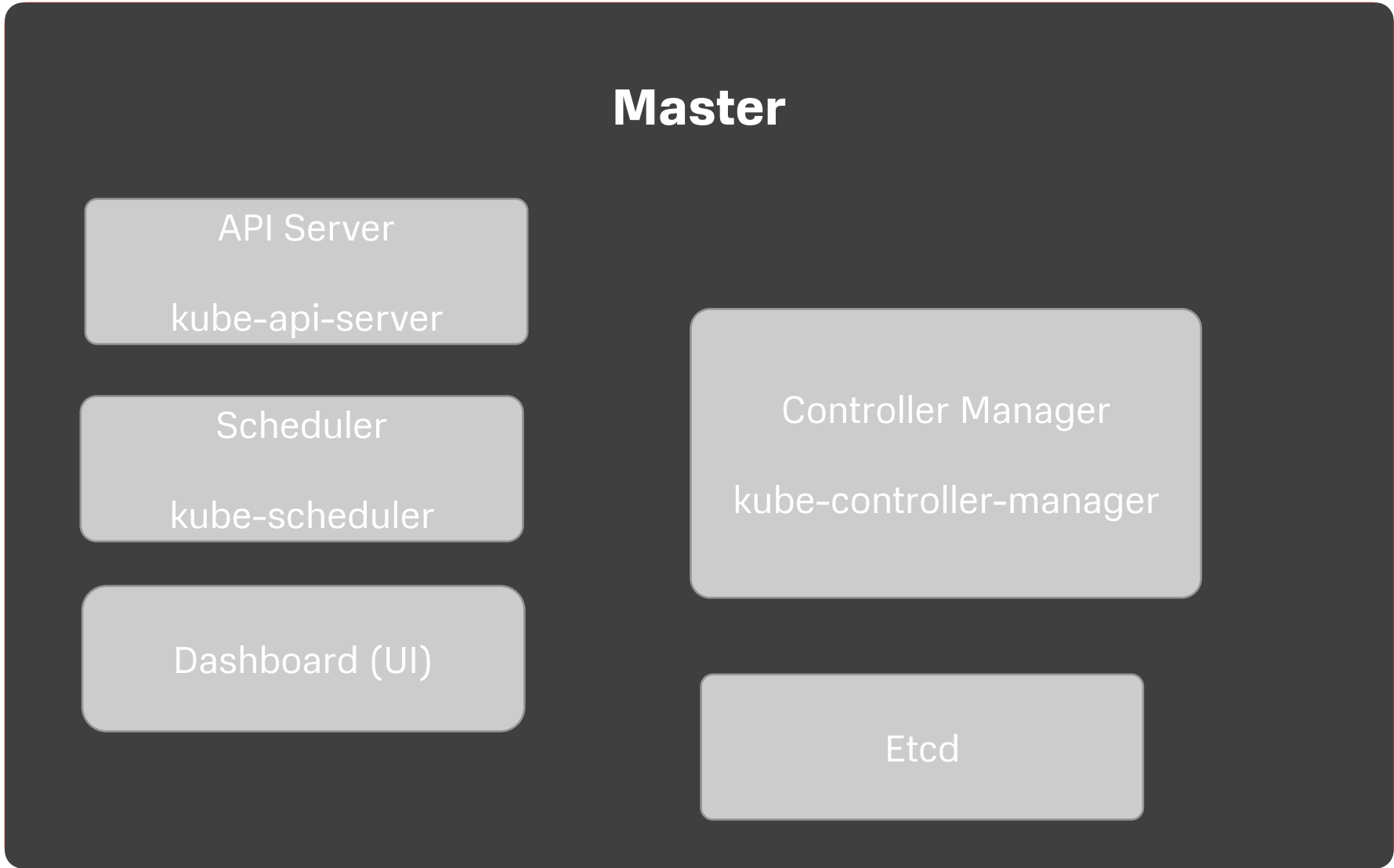
API Server

Scheduler

Dashboard (UI)

Controller Manager

Replication Controller



K8s etcd

- Используется как распределенное хранение ключей/секретов в Kubernetes
- Хранит конфигурационные данные для каждого узла кластера
- Может быть распределенным на несколько узлов
- Используется для *service discovery*
- Представляет состояние кластера

Key-Value Store



K8s Worker Node

Kubelet

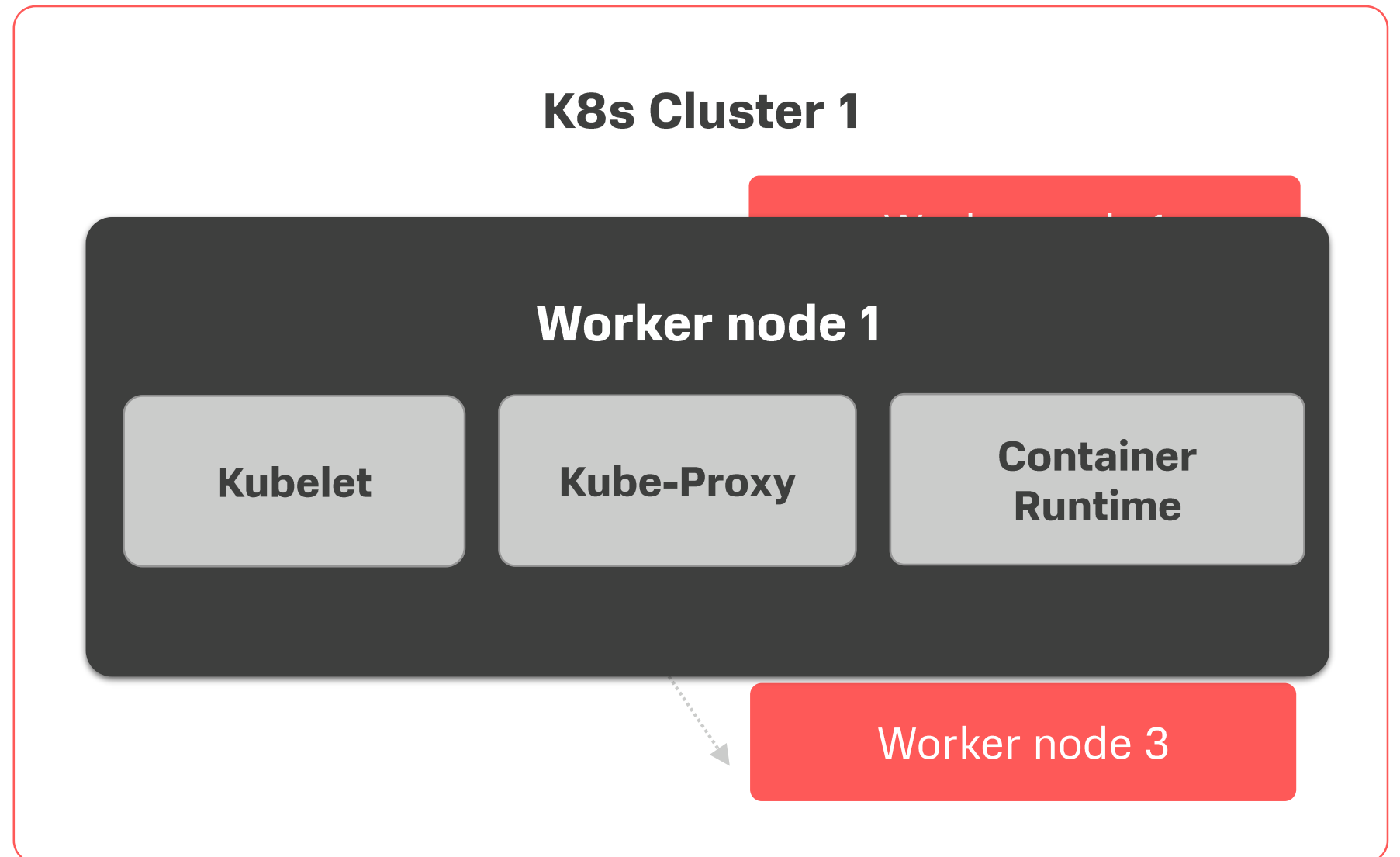
Агент на узлах, наблюдающий за PodSpecs, для определения, что требуется запустить

Kube-Proxy

Сервис, наблюдающий за конфигурацией services на API Server и применяющий east/west балансировку нагрузки на узлах, используя NAT в IPTables

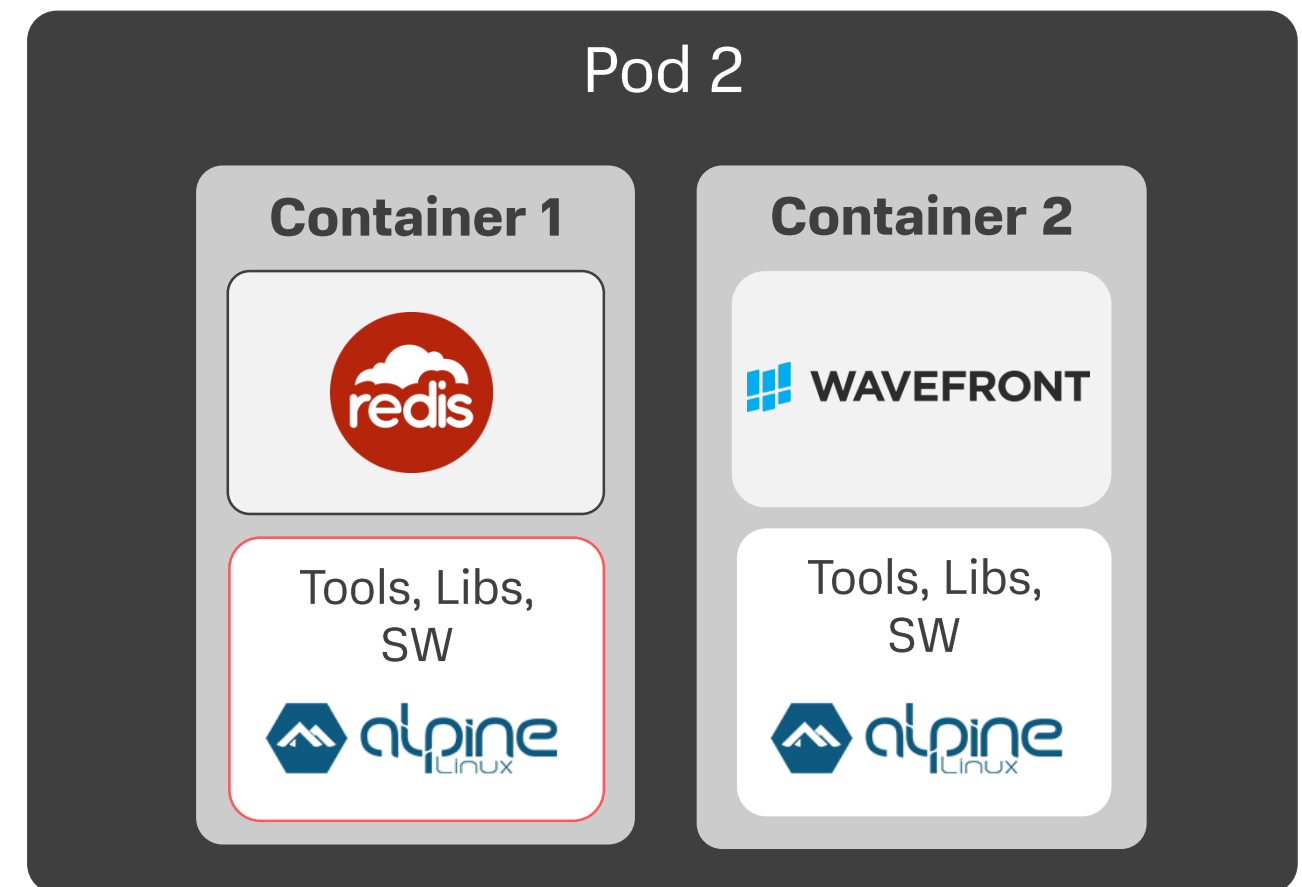
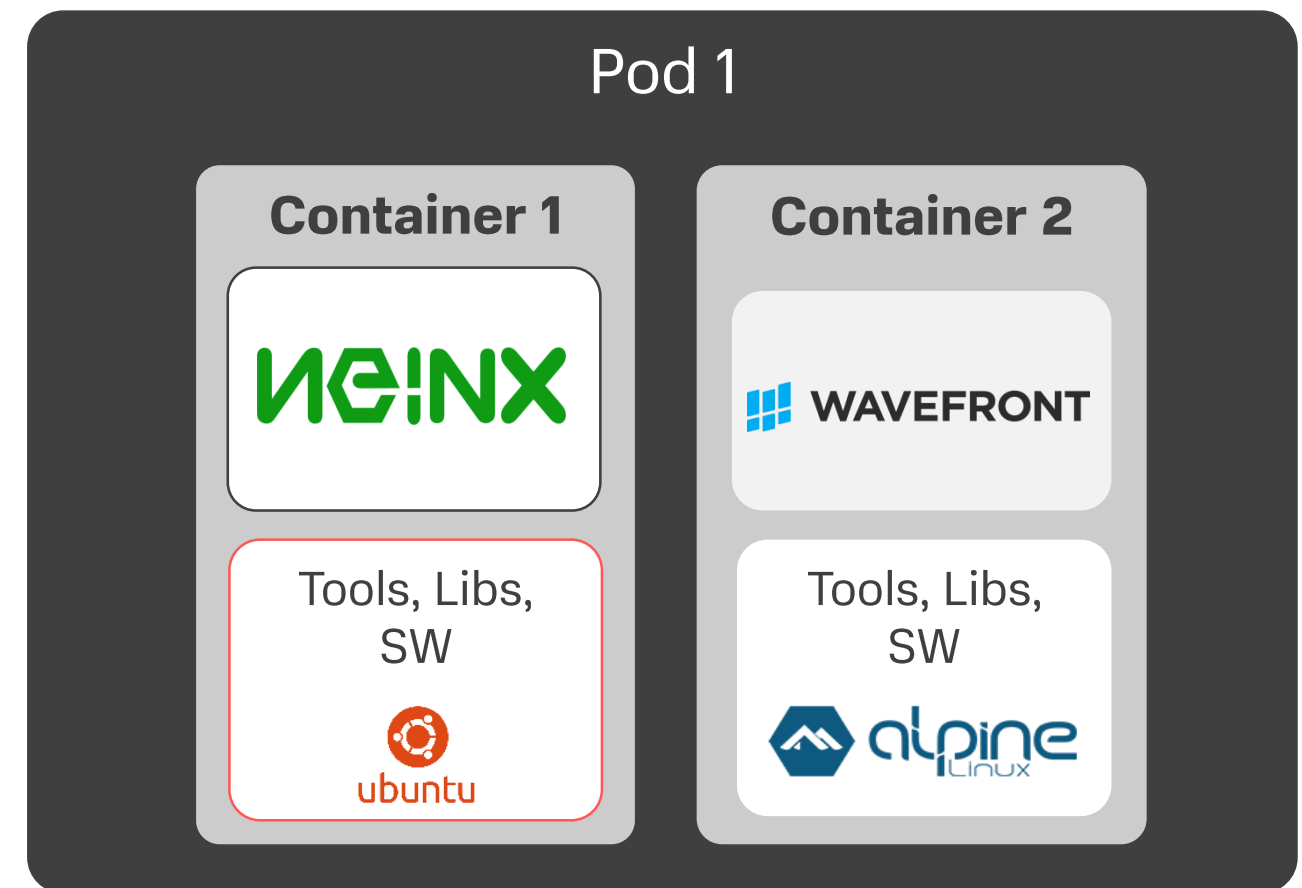
Container Runtime

Docker/Rkt/...



Pods

- Узел (под) – это группа из одного или более контейнеров
- Контейнеры в поде разделяют один IP address и список портов и могут взаимодействовать друг с другом через localhost
- Контейнеры в поде также разделяют данные в volumes

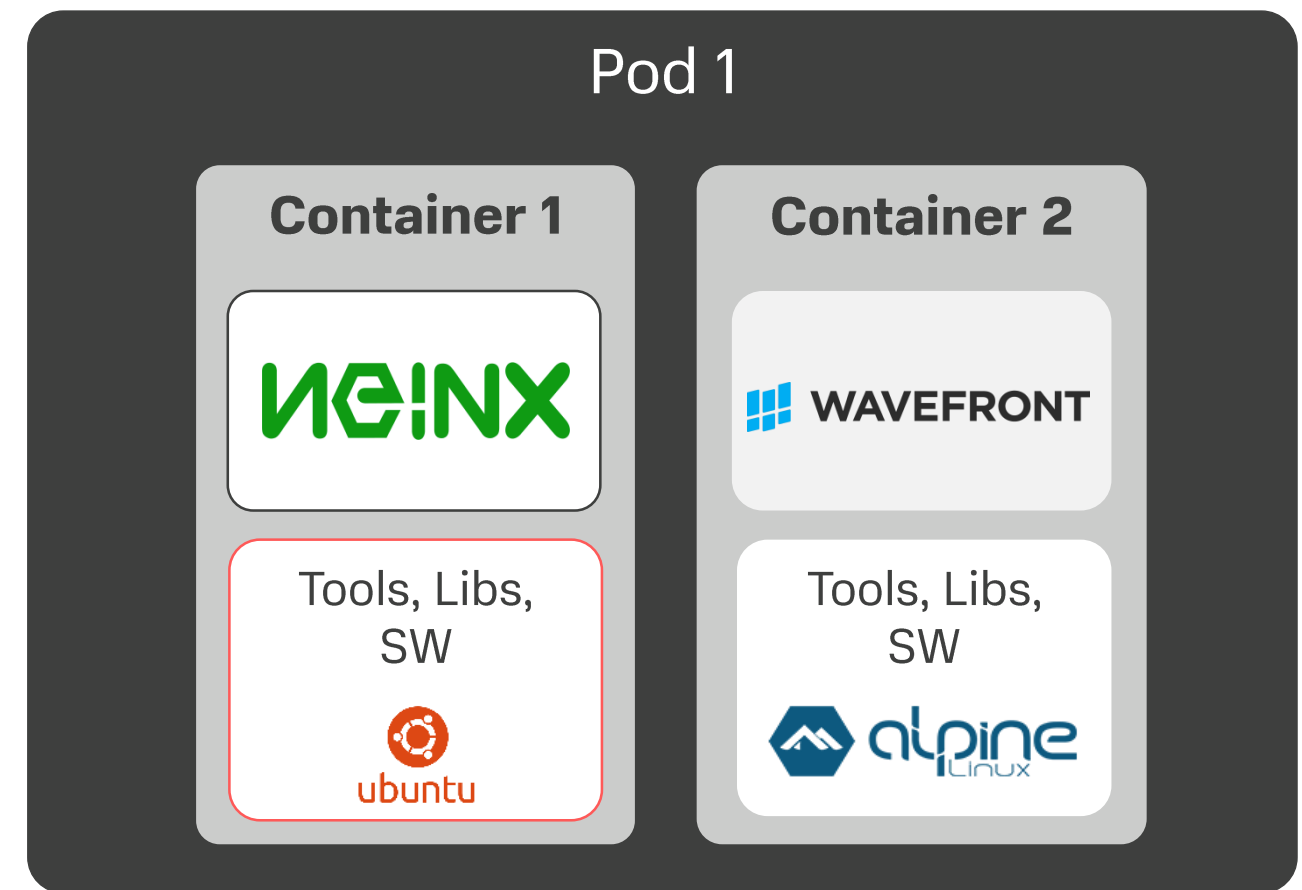


Labels

- Метка – это пара key/value, привязанная к подам и содержащая пользовательские атрибуты
- Можно использовать селекторы меток для выбора нужных подов и применения Services или Replication Controllers к ним
- Метки могут быть добавлены к объектам при создании и изменены в любой момент

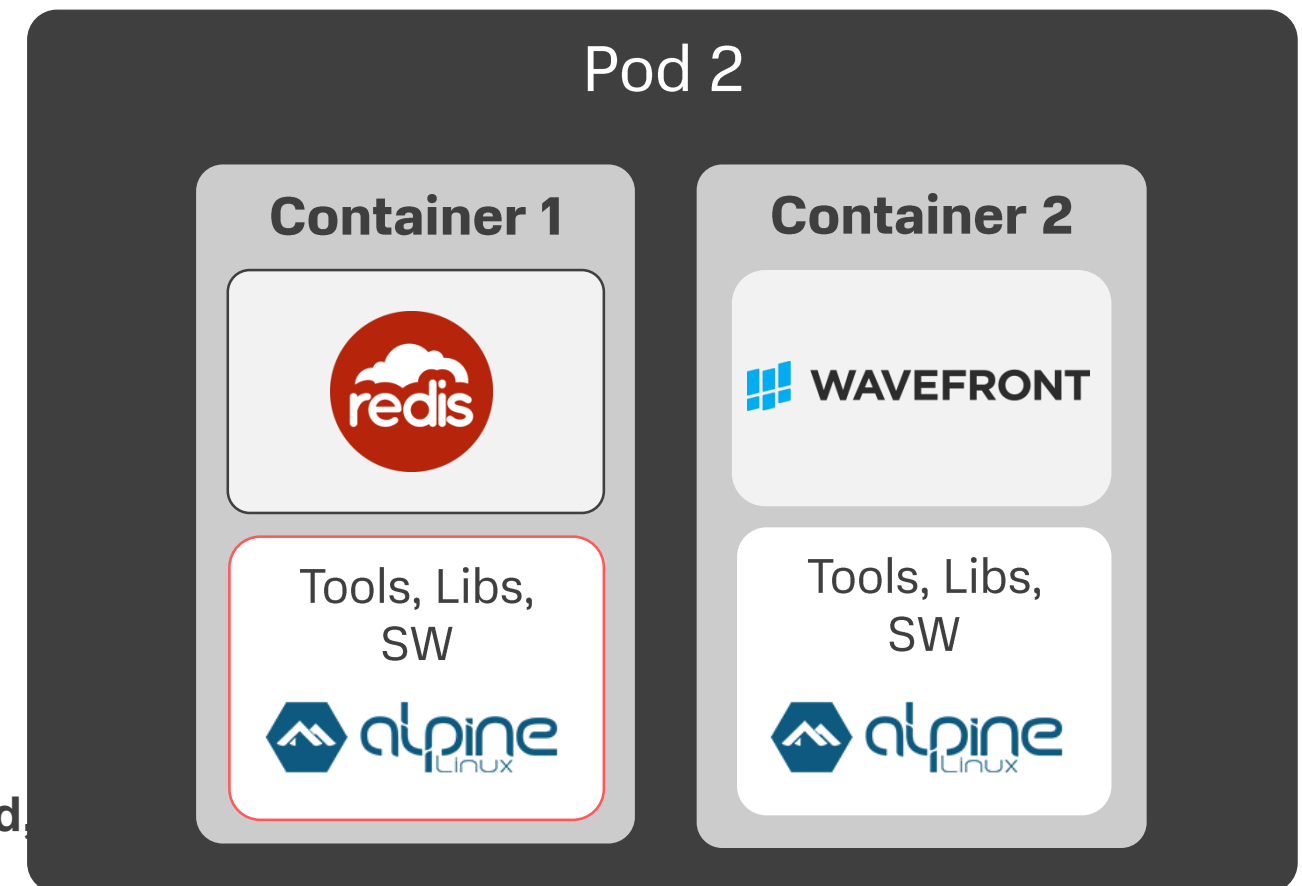
Labels:

**tier=frontend,
app=myapp**

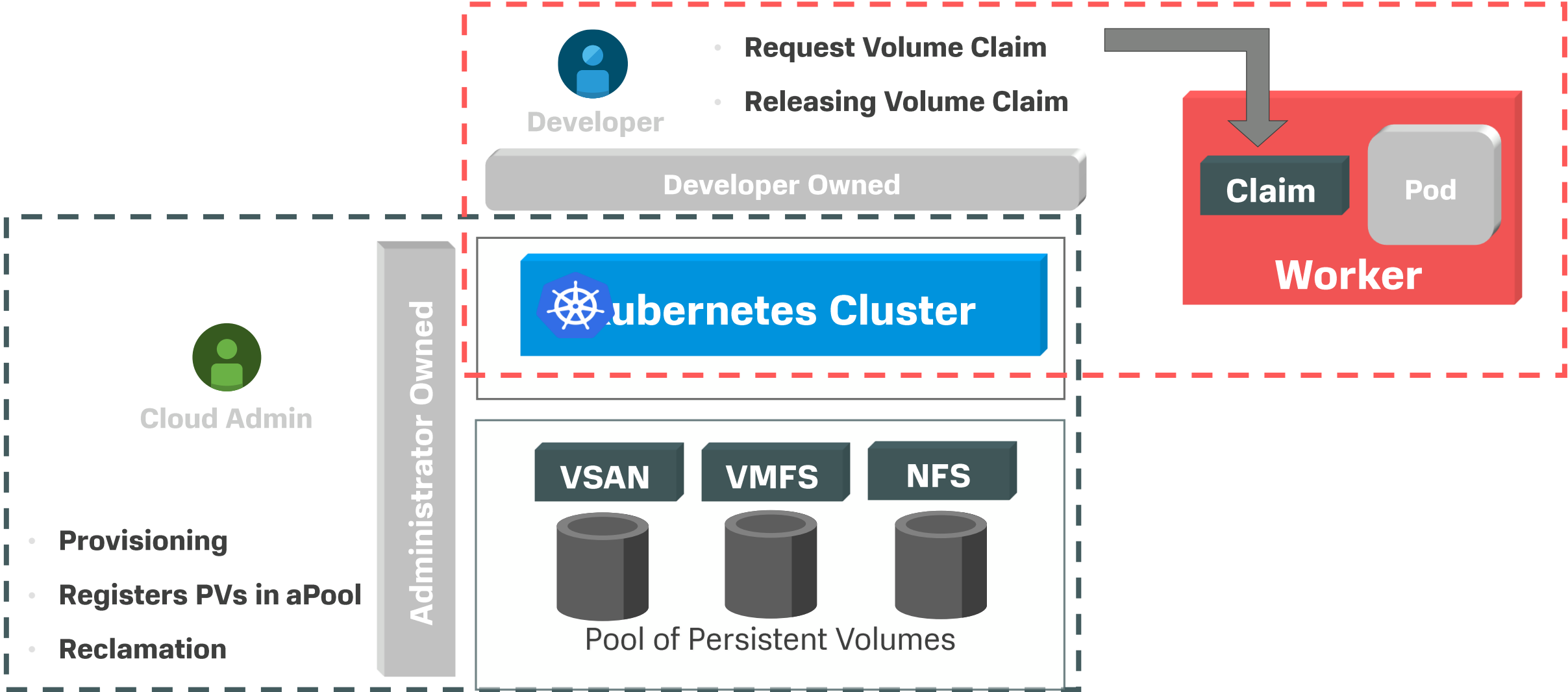


Labels:

**tier=backend,
app=myapp**



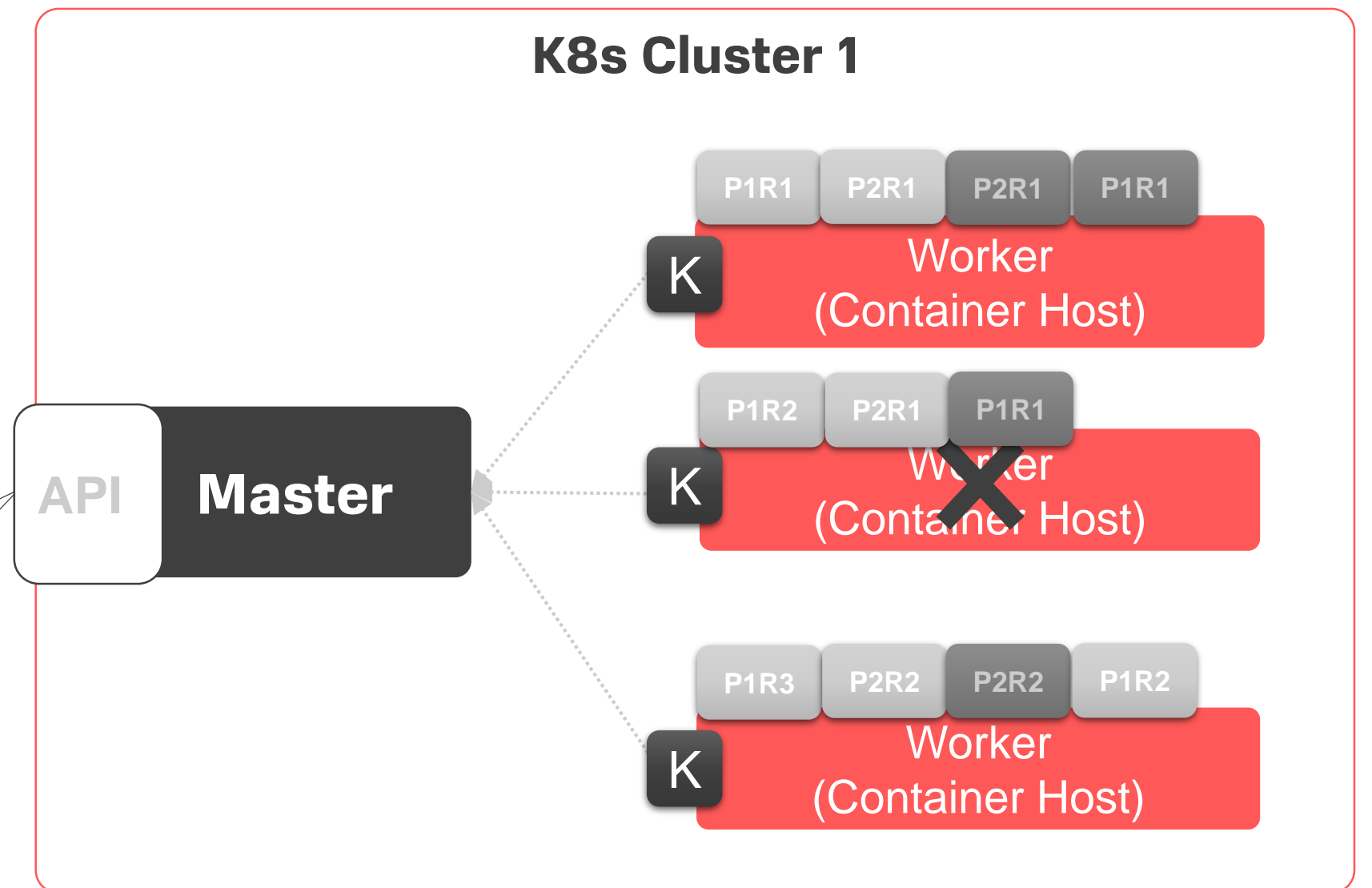
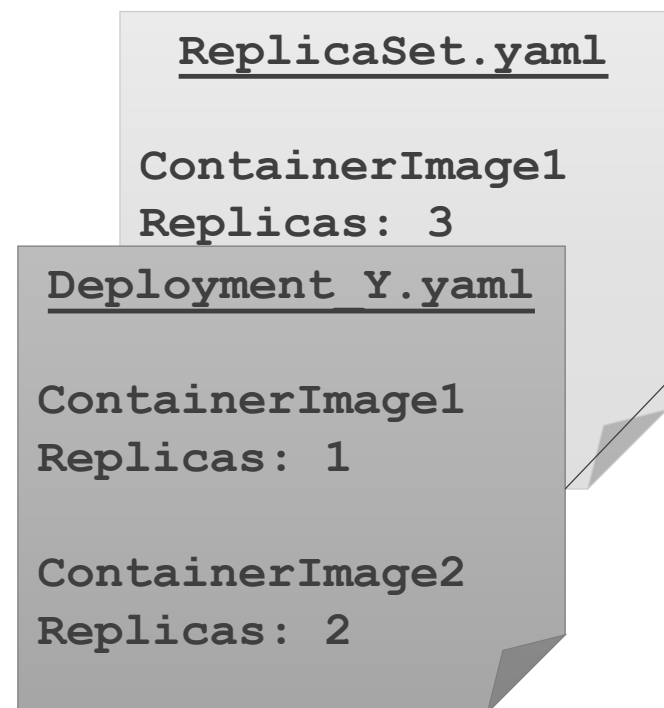
Persistent Volume Claim



Replication Controller

Преимущества реплик подов

- Автоматическое восстановление
- Ручное масштабирование
- Rolling Updates
- Контроль релизов



StatefulSet

Путь запуска **последовательно** реплик подов.
Позволяет работать подам в clustered mode

- Master/Slave приложения

Важно для приложений, которым нужны:

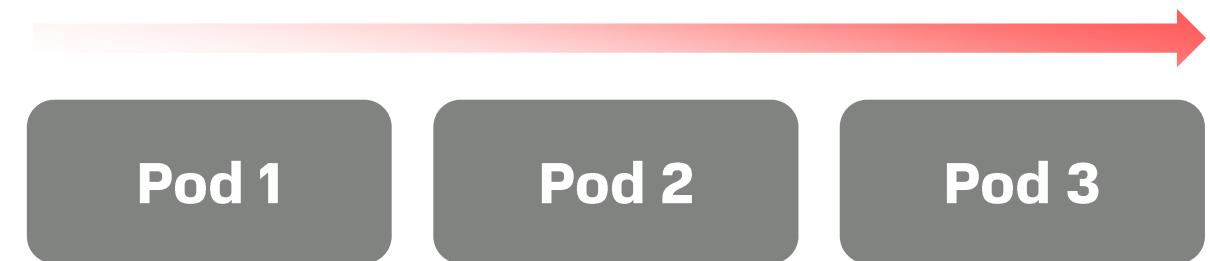
- Фиксированные и уникальные сетевые идентификаторы
- Фиксированное persistent storage
- Развертывание и масштабирование по запросу

Необходим Headless service

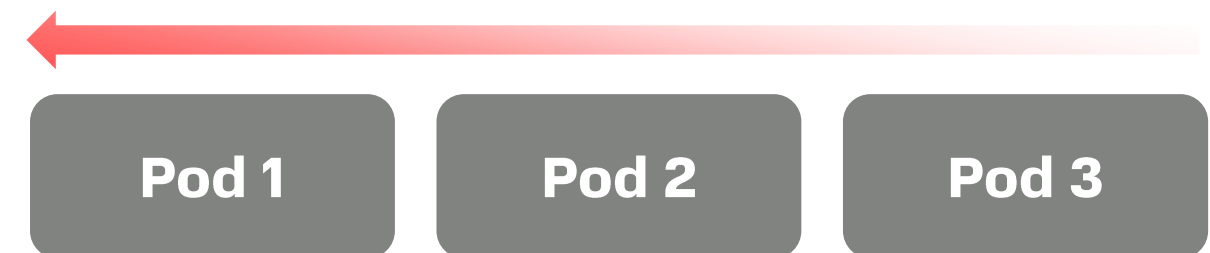
Примеры:

- Zookeeper, Cassandra, etcd, MySQL, etc

Создание последовательности подов

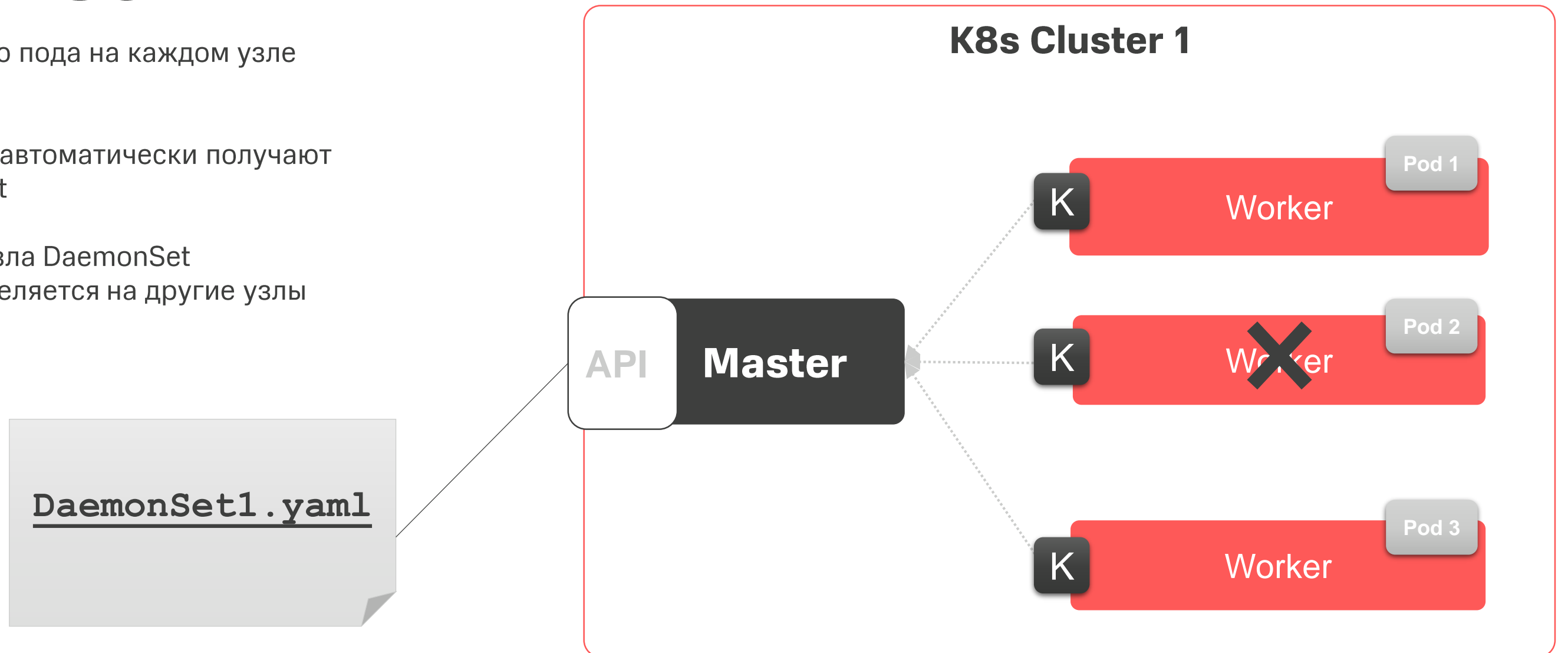


Удаление последовательности подов
в обратном порядке



DaemonSet

- Запускает копию пода на каждом узле в кластере
- Все новые узлы автоматически получают поды DaemonSet
- При удалении узла DaemonSet не перераспределяется на другие узлы



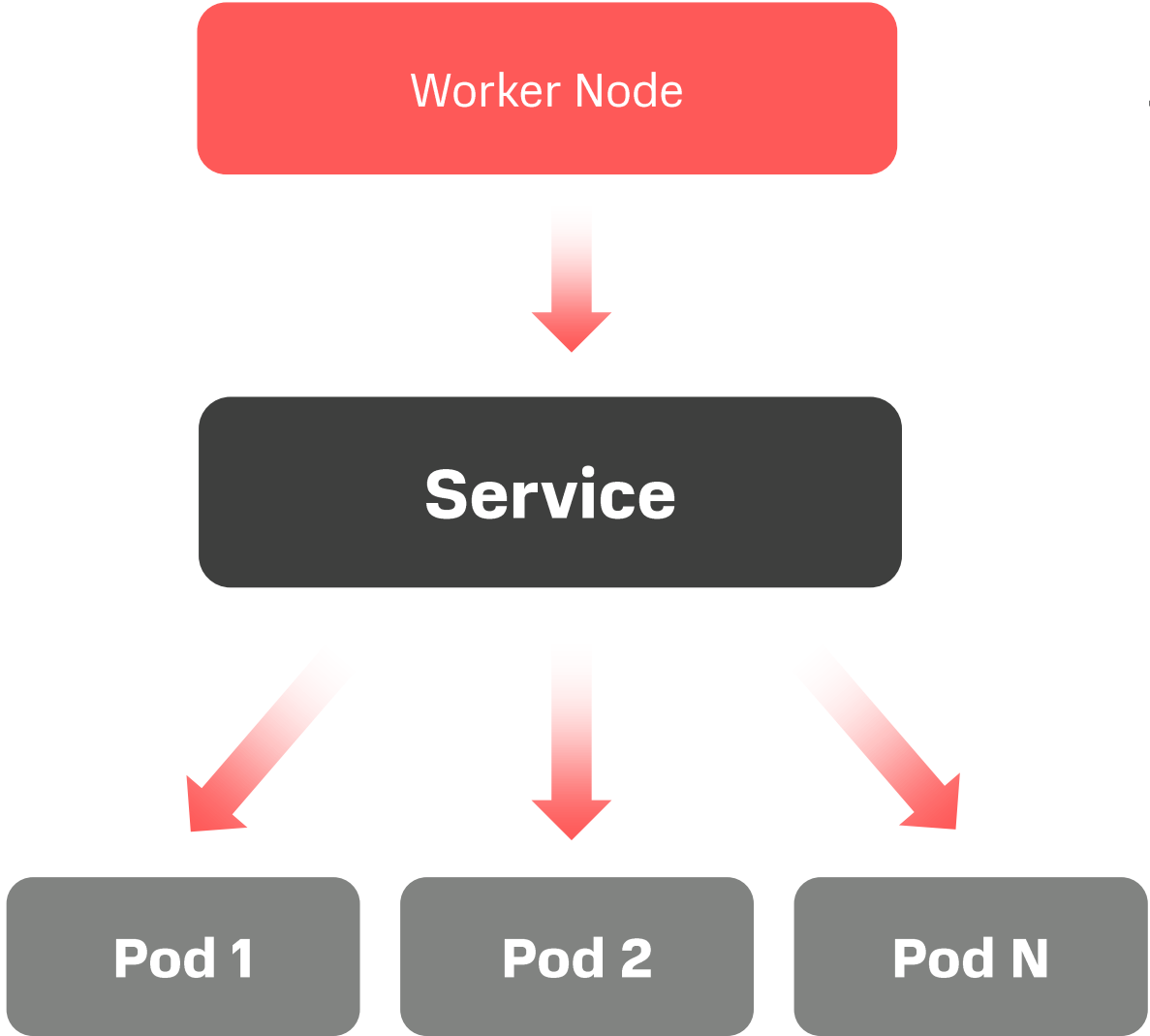
Services

Services Types

- ClusterIP
- NodePort
- Loadbalancer

Service Discovery

- DNS
- Environmental variables



Node IP:
192.168.10.10

IP: 10.2.3.14
DNS: service1.cluster.local
Port: 9443
NodePort: 31233
Protocol: TCP

Port: 9443

Закрепить материал

Лабораторные работы

Docker/Kubernetes <https://labs.play-with-k8s.com/>

Hands-On Labs <https://labs.hol.vmware.com/>

ModernAppsNinja Courses from VMware

<https://modernapps.ninja>

Learn Kubernetes. From Experts. For Free

<https://kube.academy/>

K8S <https://kubernetes.io/>

Cloud Native Apps: <https://blogs.vmware.com/cloudnative>

The screenshot shows the Play with Kubernetes interface. At the top, a timer displays 03:42:35. Below it is a 'CLOSE SESSION' button. The 'Instances' section shows a list of three instances: node1 (192.168.0.23), node2 (192.168.0.22), and node3 (192.168.0.21). A terminal window on the right shows the output of the 'kubeadm join' command on node2, indicating it has successfully joined the cluster. The terminal output includes various warnings and status messages, such as 'Initializing machine ID from random generator', 'Running pre-flight checks', and 'This node has joined the cluster: * Certificate signing request was sent to apiserver and a response was received. * The Kubelet was informed of the new secure connection details.' The terminal prompt is '[node2 ~]\$'.

Спасибо!

