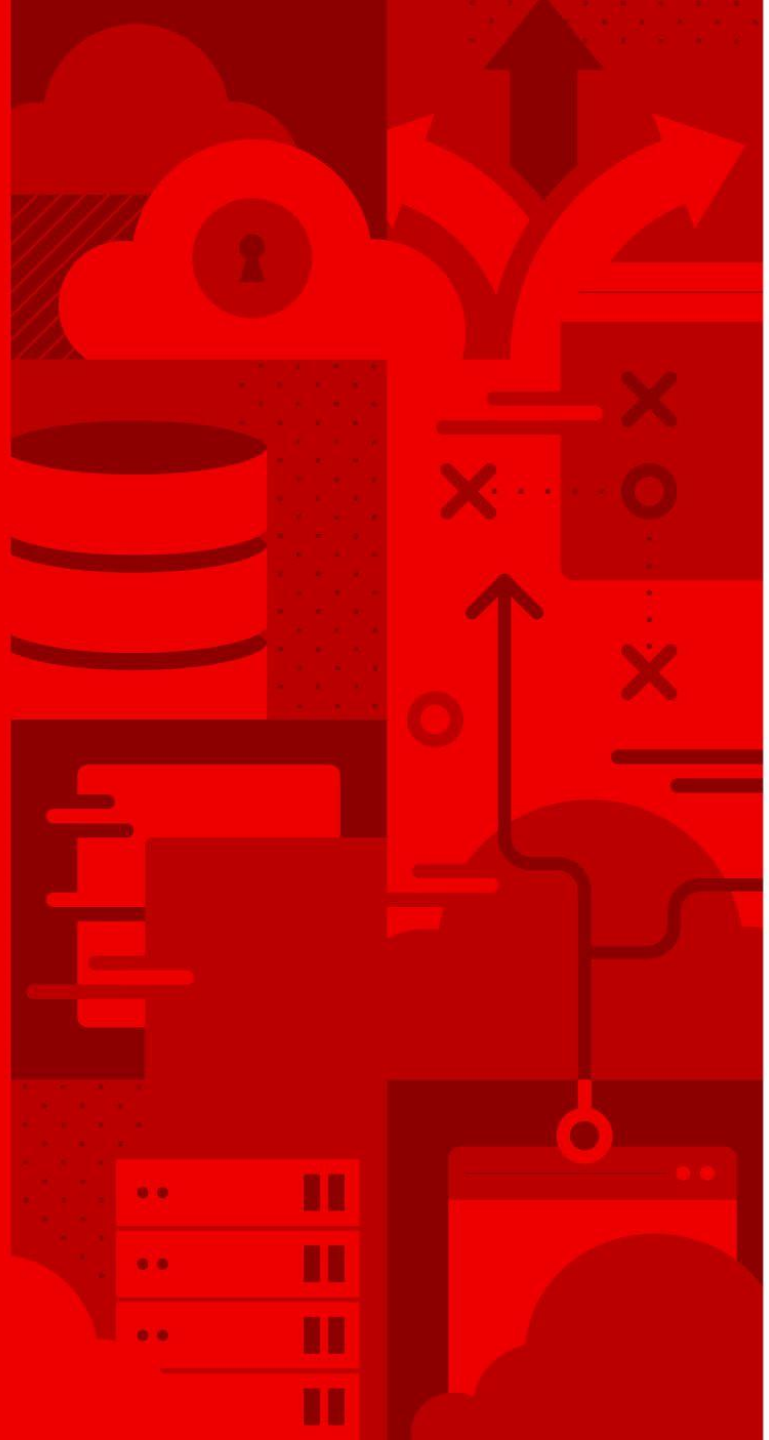


Nihol

Обзор платформы Red Hat OpenShift

Докладчик: Вадим Гоян

Ташкент - 2023

Red Hat

Что значит “Сделай Kubernetes сам”

Принесите своё собственное промежуточное программное обеспечение, базы данных и прочее ПО. Создайте каталог служб, чтобы обеспечить возможность самостоятельного развертывания и самообслуживания

Возьмите Kubernetes или другой оркестровщик (Mesos, Swarm) из апстрима и поддерживайте его работоспособность сами. Выполните всю работу, необходимую для его интеграции в ИТ-среду вашего предприятия (сети, хранение, реестр, безопасность, ведение журнала, метрики и т. д.)

Возьмите существующие инструменты для CI / CD и добавьте сборку и управление образом контейнера, непрерывное развертывание и т. д.

Возьмите Docker-контейнер из апстрима, поддерживайте его, обеспечивайте безопасность и обслуживайте его самостоятельно.

Поддерживайте и развивайте собственный апстрим дистрибутив Linux или используйте существующие коммерческие предложения Linux - RHEL или от сторонних производителей.

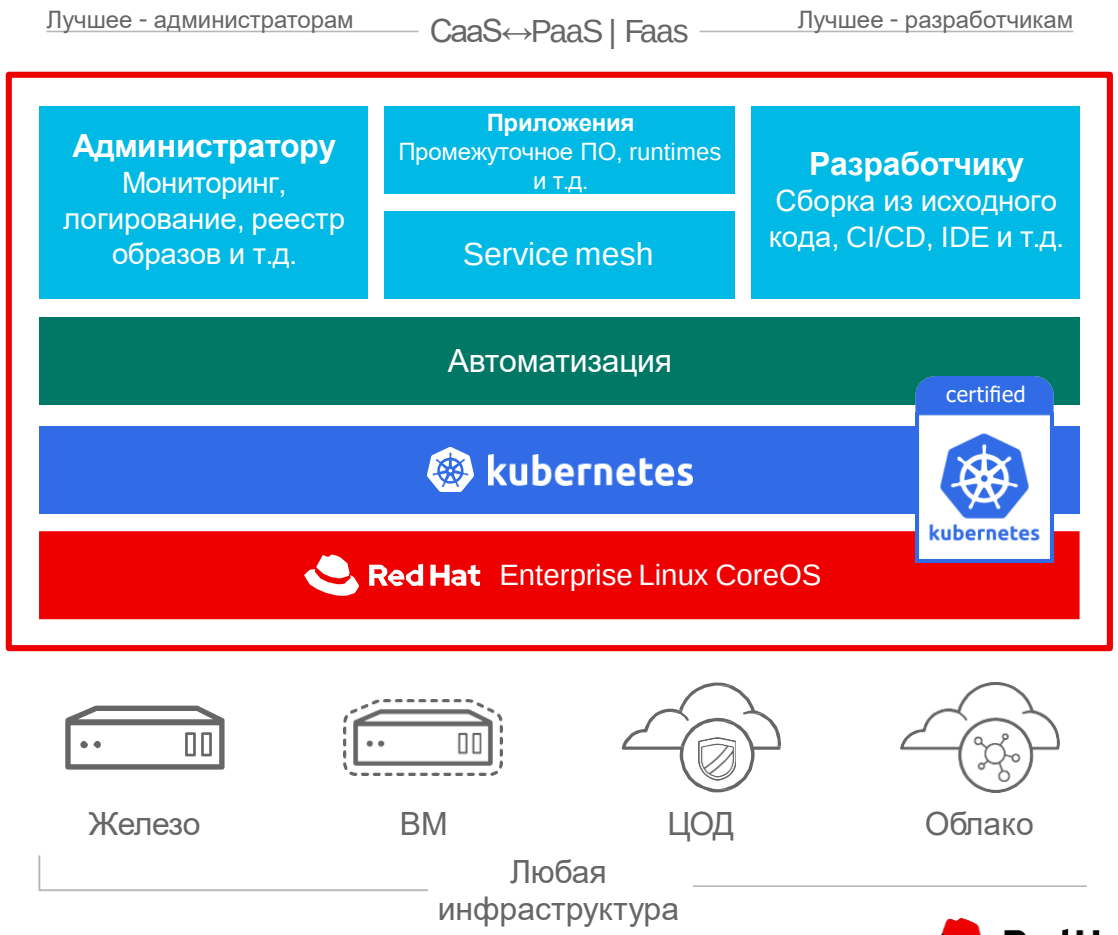
OpenShift 4 — коробочное решение

Red Hat OpenShift 4

Включает в себя все нужные компоненты из коробки:

1. Все компоненты интегрированы друг с другом
2. Стабильное и однородное развёртывание как в облаке, так и в вашем ЦОД
3. Полная автоматизация установки всех компонентов решения
4. Обновления в один клик
5. Автомасштабирование и интеграция с платформами

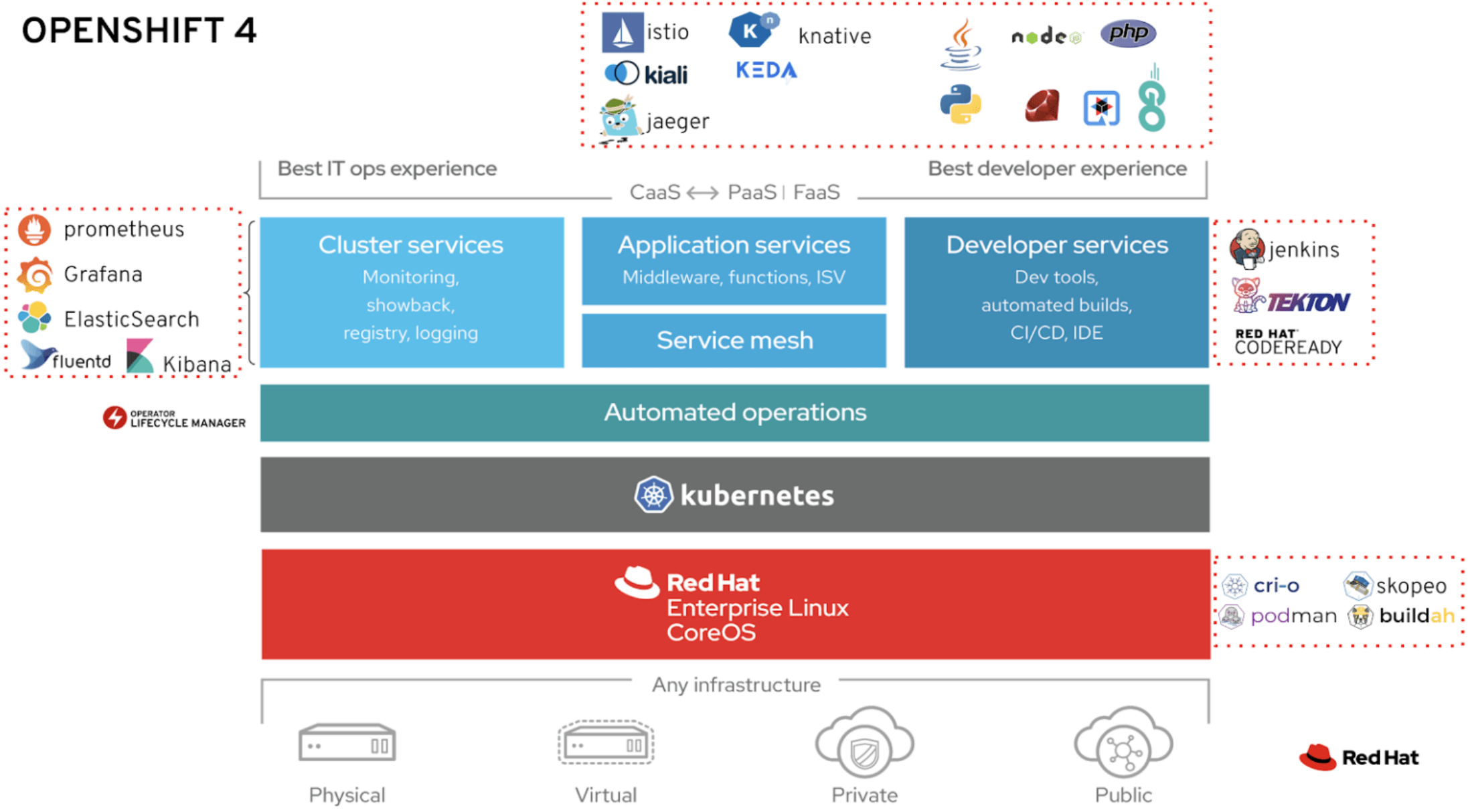
Любая инфраструктура



Red Hat

Nihol

OPENSHIFT 4



Стабильная и стандартная платформа для вашего предприятия

- Автоматизация
- Совместный доступ
- Безопасность “из коробки”
- Контроль сетевого доступа
- Автоматизация обновлений
- Мониторинг и логирование
- Расширяемая архитектура

RED HAT OPENSHIFT

Железо, VMware vSphere, Red Hat Virtualization, Red Hat OpenStack Platform, Amazon Web Services, Microsoft Azure, Google, IBM Cloud

Поддерживаемые платформы для установки

Full Stack Automation (IPI)

- amazon web services
- Microsoft Azure
- Google Cloud Platform
- vmware vSphere
- RED HAT OPENSTACK PLATFORM
- Bare Metal
- RED HAT VIRTUALIZATION

New addition in OCP 4.6

Pre-existing Infrastructure (UPI)

- amazon web services
- Microsoft Azure
- Google Cloud Platform
- vmware vSphere
- RED HAT OPENSTACK PLATFORM
- Bare Metal
- IBM Z
- IBM Power Systems

Now supports deploying to VMware vSphere 7.0

Автоматизация с уровня ОС

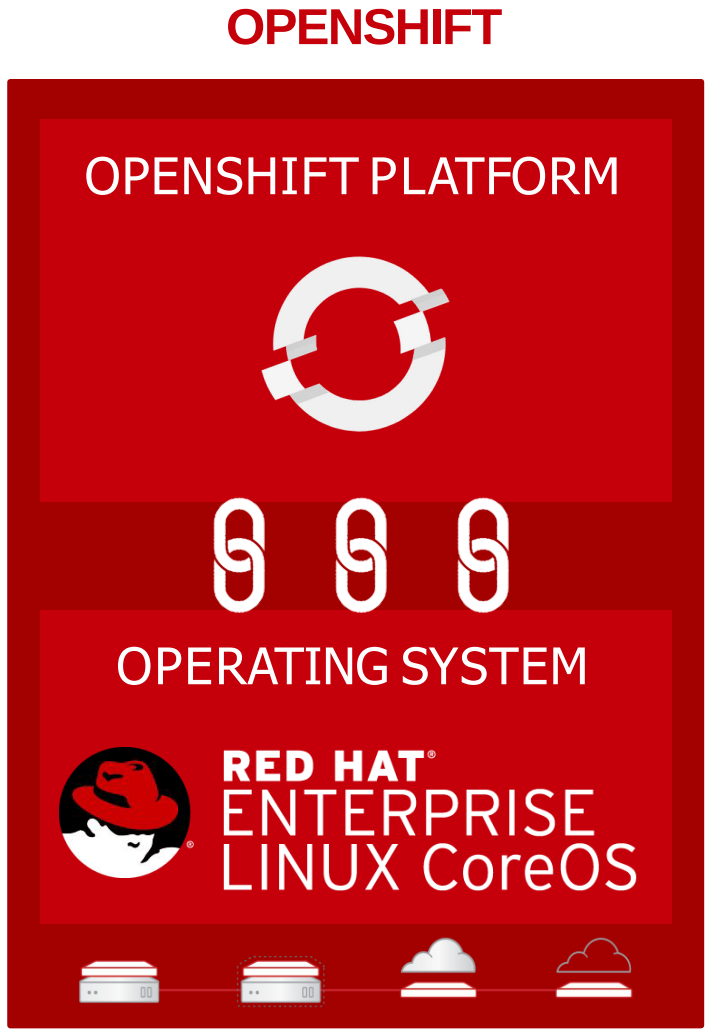
Red Hat Enterprise Linux CoreOS создавалась под OpenShift

CoreOS тестируется на совместимость с платформой и является неотъемлемой её частью.

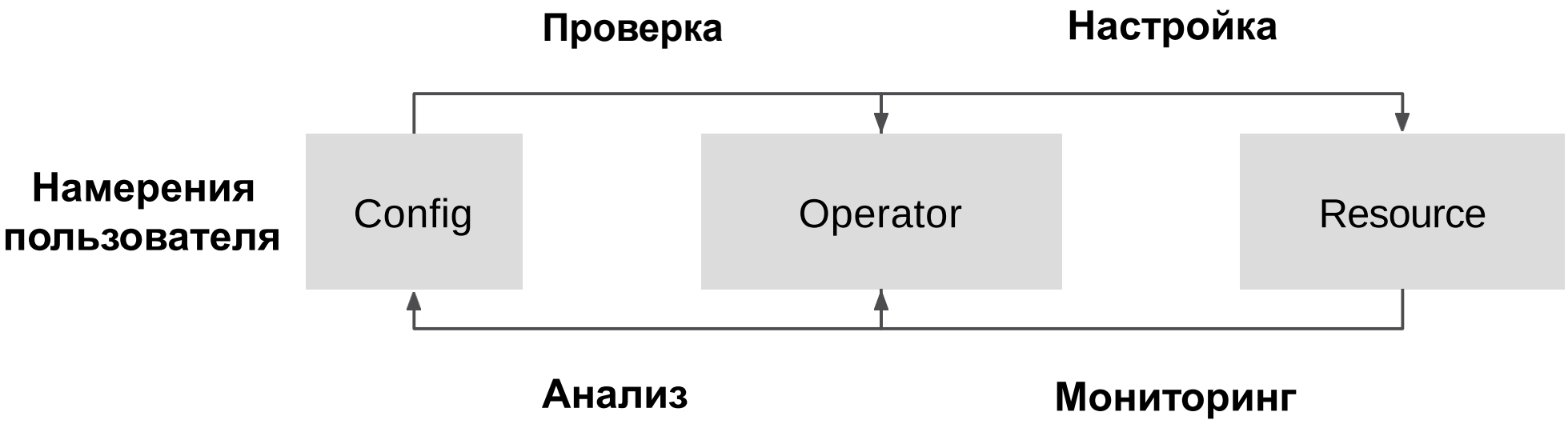
Red Hat Enterprise Linux CoreOS управляется кластером

Жизненный цикл ОС привязан к жизненному циклу кластера. OpenShift управляет не только самом ОС, но и конфигурациями приложений на ней, например:

- CRI-O
- Kubelet
- Список разрешённых контейнерных registry
- Конфигурации SSH



OpenShift - no Ops платформа. Как это работает?



Оператор действует как живой инженер. Он смотрит на развёрнутое приложение, анализирует его и принимает решения о реконфигурации.

OperatorHub

Используется администраторами для поиска и установки операторов

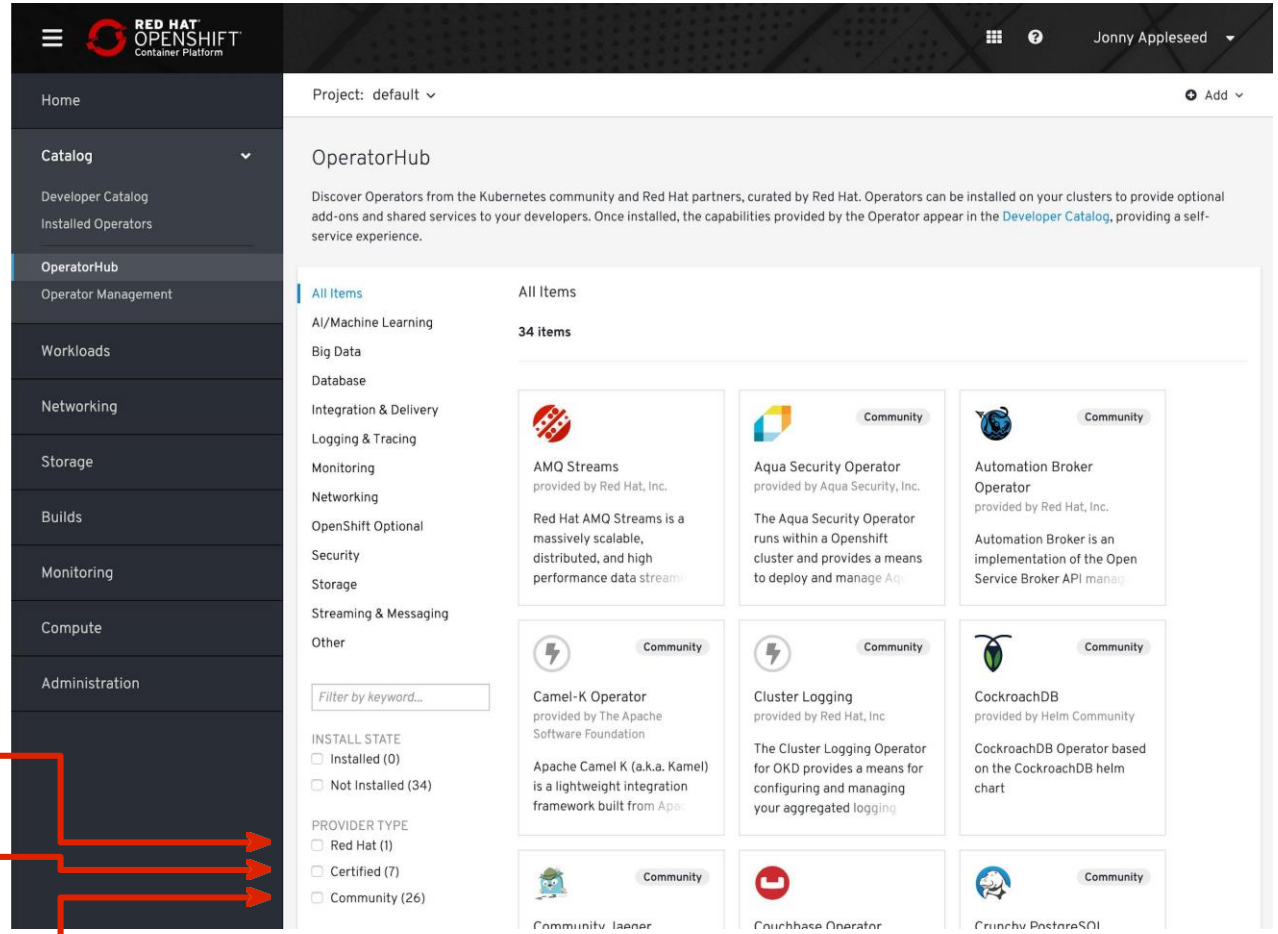
Операторы в OperatorHub поддерживают OLM

Marketplace Operator ответственен за UI OperatorHub на OpenShift

Red Hat Operators

OpenShift Certified Operators

Community Operators



Источник:
https://docs.openshift.com/container-platform/4.4/operators/olm-understanding-operatorhub.html

OpenShift это про операторы

Cluster Settings

Details | Cluster Operators | Global Configuration

Filter | Name | Search by name... /

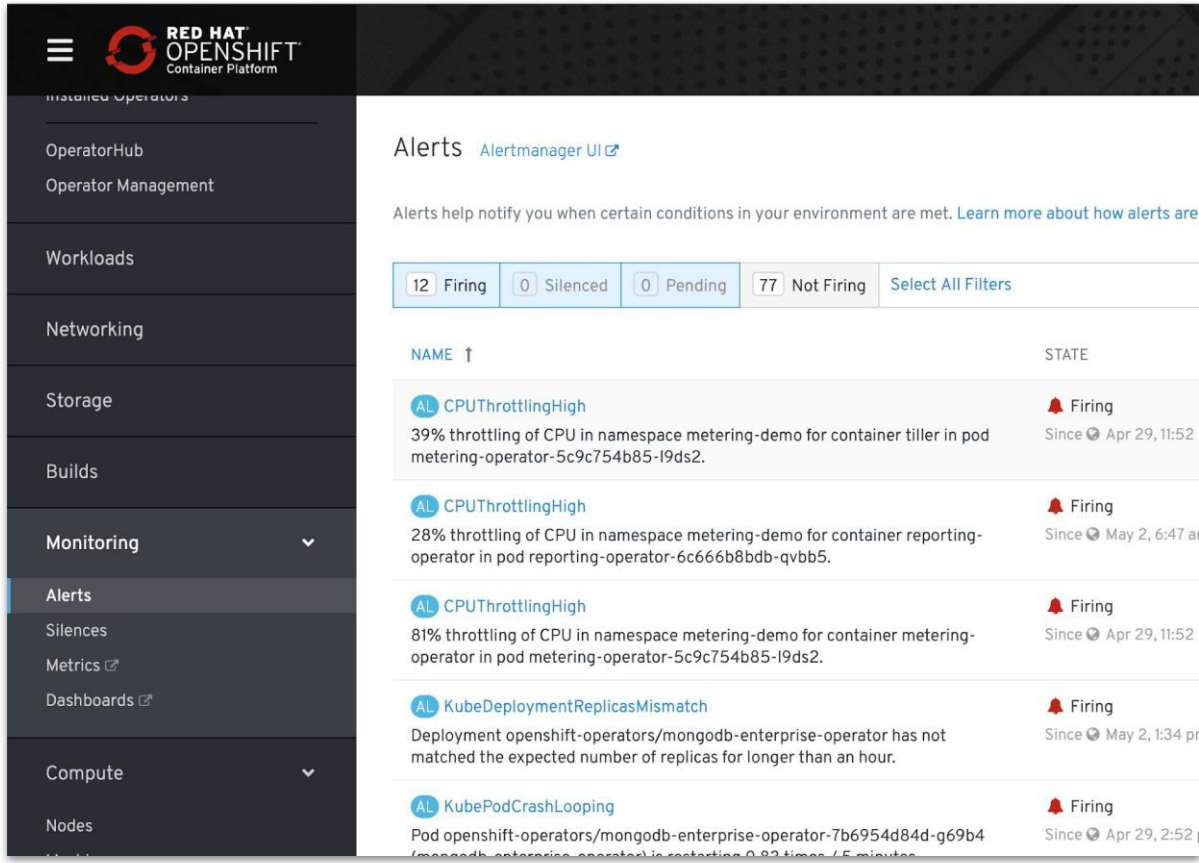
Name	Status	Version
CO authentication	Available	4.5.0-0.nightly-2020-04-21-103613
CO cloud-credential	Available	4.5.0-0.nightly-2020-04-21-103613
CO cluster-autoscaler	Available	4.5.0-0.nightly-2020-04-21-103613
CO config-operator	Available	4.5.0-0.nightly-2020-04-21-103613
CO console	Available	4.5.0-0.nightly-2020-04-21-103613

- Жизненный цикл операторов платформы связан с кластером.
- Каждый оператор отвечает за определенные конфигурации
- Оператор сообщает состояние о своем компоненте
  - Available
  - Progressing (applying a configuration update)
  - Degraded (loss of service over a period)
- Пример на картинке включает в себя:
  - DNS
  - Network
  - CSI
  - Monitoring
  - Ingress

Мониторинг кластера в OpenShift

Предоставляется “из коробки”, разворачивается в процессе установки

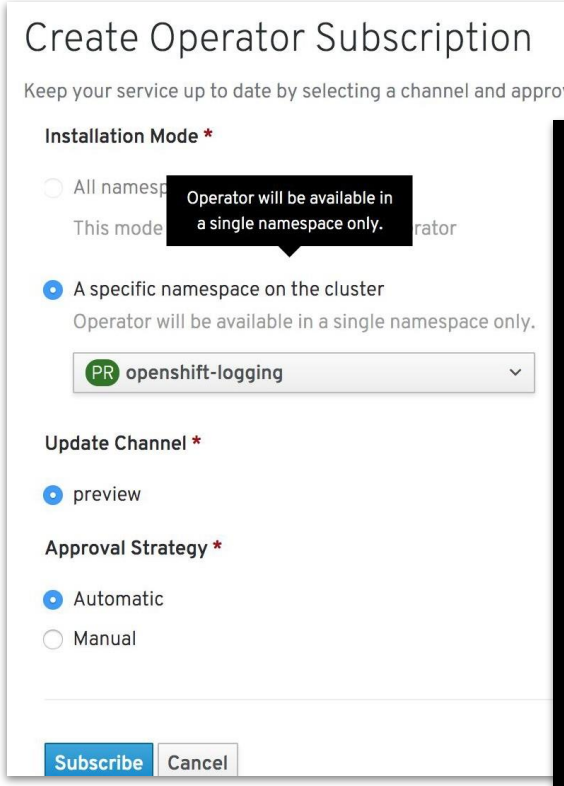
- Метрики для мониторинга etcd и других аспектов кластера “из коробки”
- Настраивайте нужные алерты отдельно в т.ч. Для ваших приложений
- Смотрите сводные графики с помощью Grafana
- Метрики для траблшутинга сети
- Configuration via ConfigMaps and Secrets



Логирование в OpenShift

Доступно в виде операторов

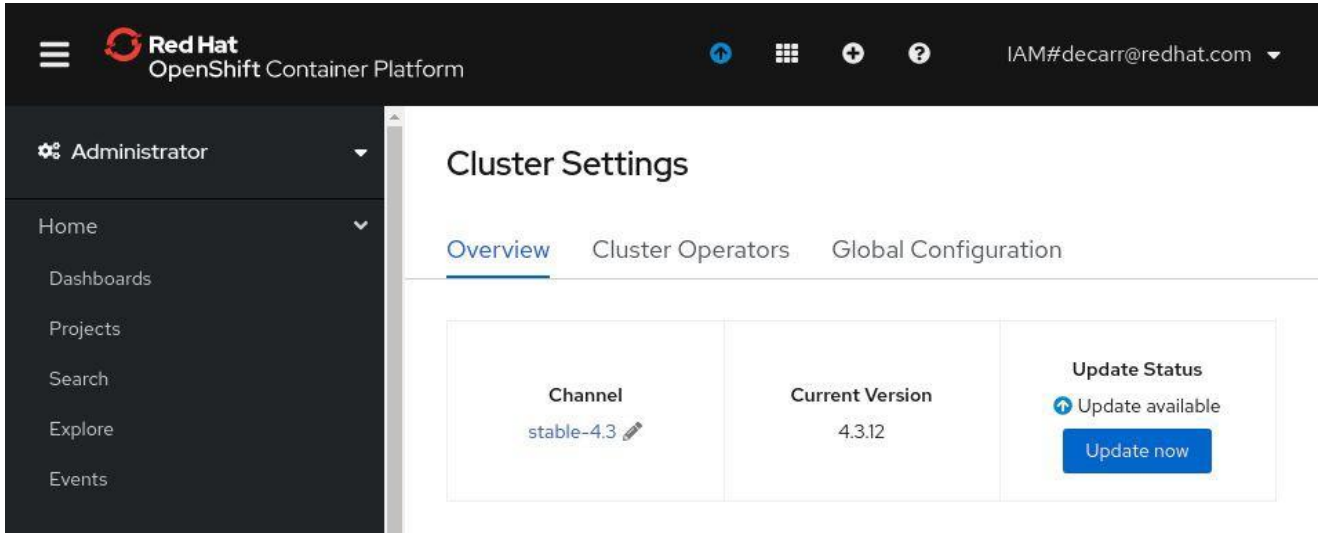
- EFK (Elasticsearch + Fluentd + Kibana) собирает логи хостов и приложений
  - Elasticsearch: хранит логи, позволяет создавать сложные запросы на поиск
  - Fluentd: собирает логи в Elasticsearch
  - Kibana: web интерфейс
- Контроль доступа
  - Администратор кластера может смотреть любые логи
  - Пользователи видят логи своих проектов
- Автоматический аудит всех событий API
- Log forwarding API



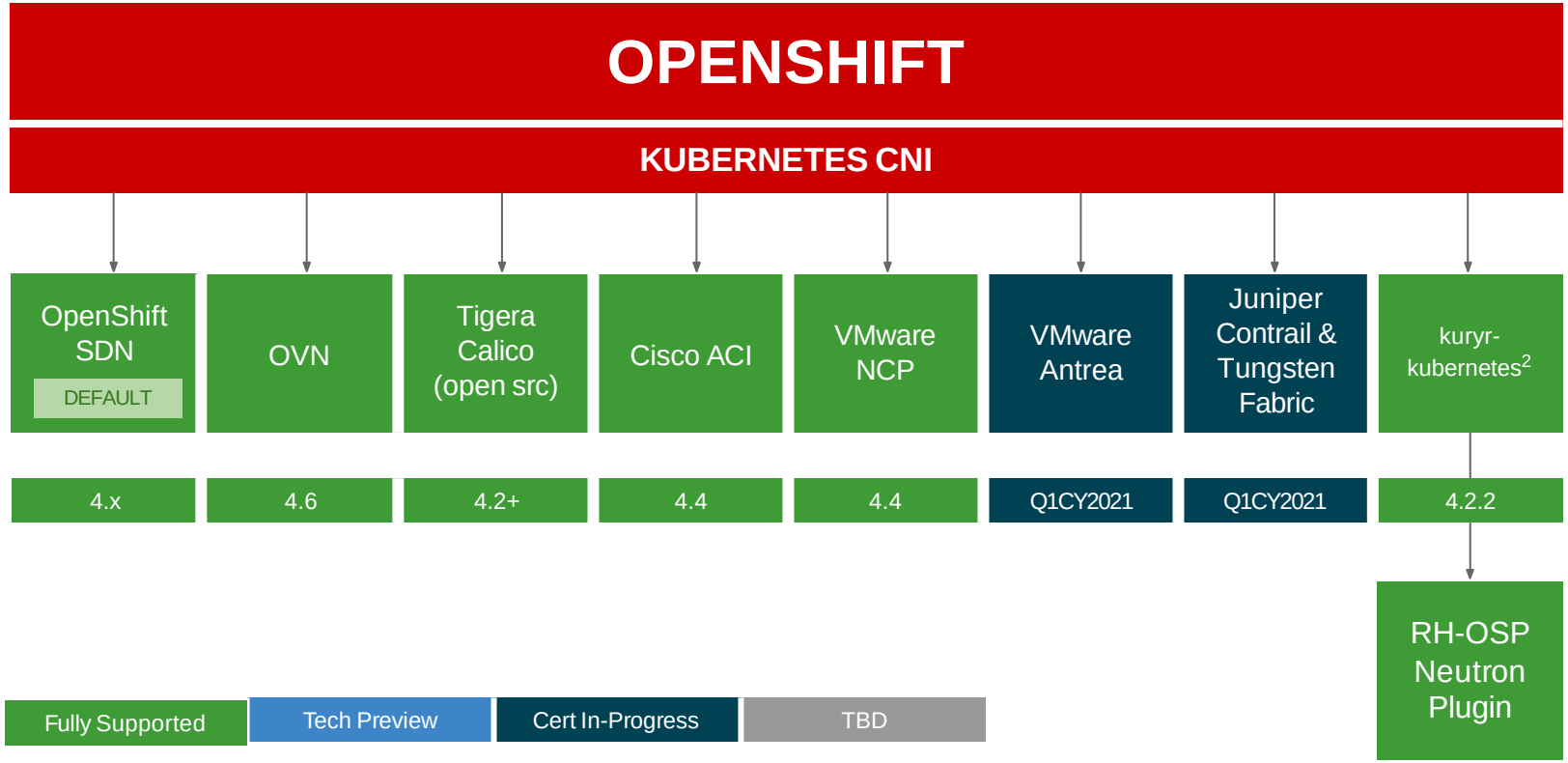

```yaml
# configure via CRD
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"
  namespace: "openshift-logging"
spec:
  managementState: "Managed"
  logStore:
      type: "elasticsearch"
      elasticsearch:
      nodeCount: 3
      resources:
      limits:
            cpu: 800m
            memory: 1Gi
      requests:
      cpu: 800m
  memory: 1Gi
  storage:
      storageClassName: gp2
      size: 100G
      redundancyPolicy: "SingleRedundan
  visualization:
      type: "kibana"
      kibana:
      replicas: 1
```

Обновления в один клик

- Обновление всех компонентов платформы
- Выбор версии под контролем администратора
- Поддерживается как изолированные среды, так и среды с подключением к интернету
- Обновление без простоев
- Проверка совместимостей перед запуском обновлений
- Обновление проходит поэтапно, даже при ошибке кластер не перестанет работать.



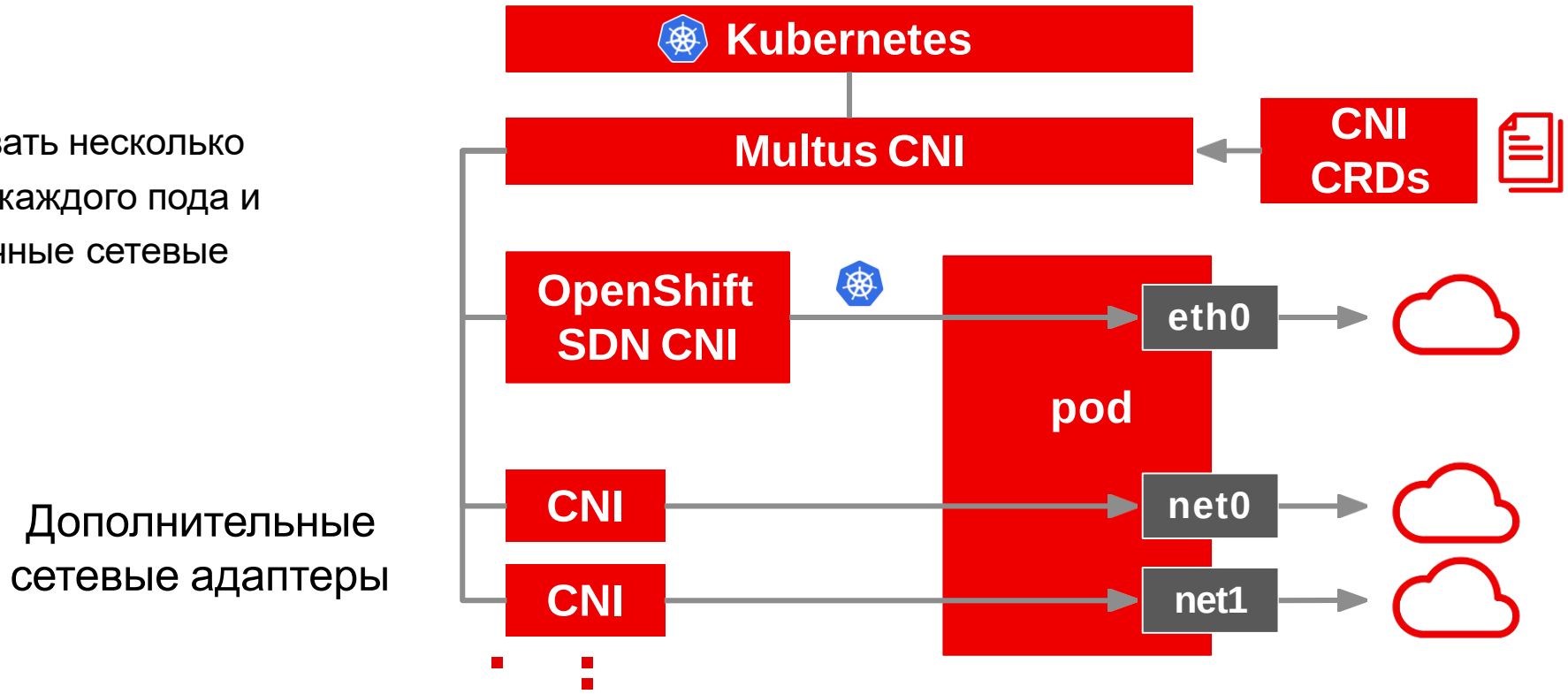
OpenShift Networking Plug-ins



Источник:
https://access.redhat.com/articles/5436171
https://access.redhat.com/articles/4763741

Multus

Multus позволяет создавать несколько сетевых адаптеров для каждого пода и назначать на них различные сетевые плагины



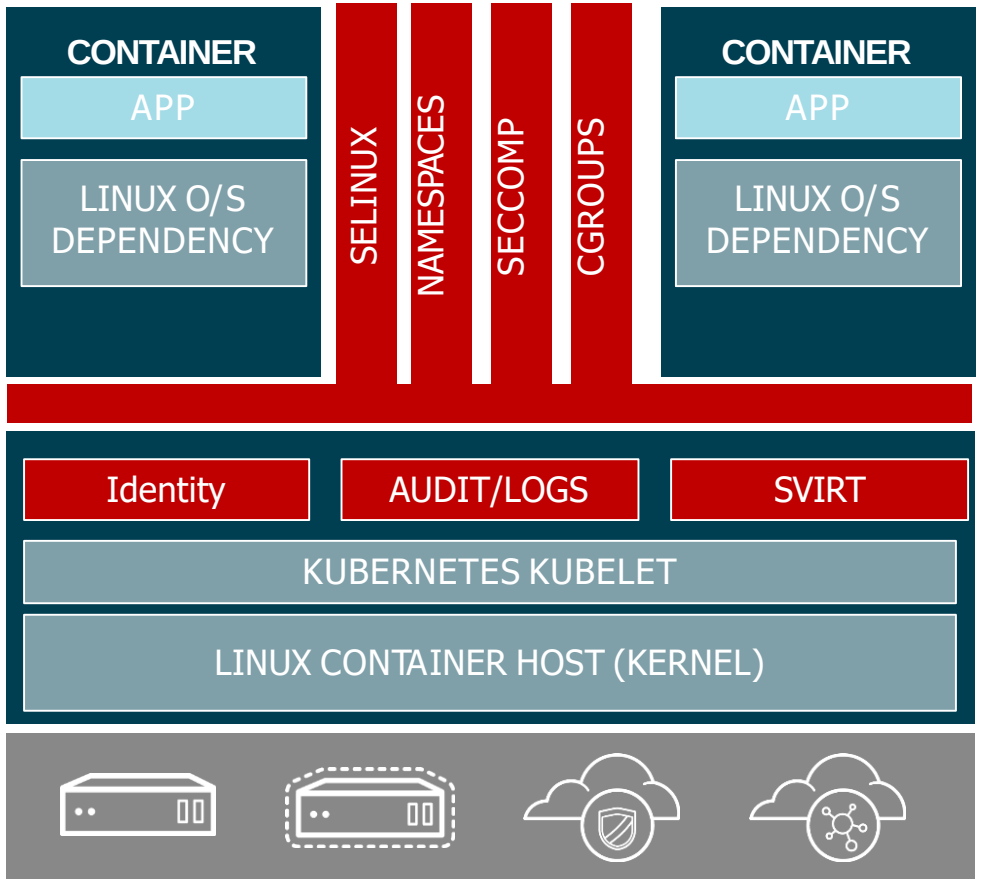
Поддерживаемые CNI плагины

- host device
- IPAM(dhcp)
- MACVLAN
- IPVLAN
- Bridge with VLAN
- Static IPAM
- DHCP IPAM
- Route Override
- whereabouts
- SR-IOV
- ...

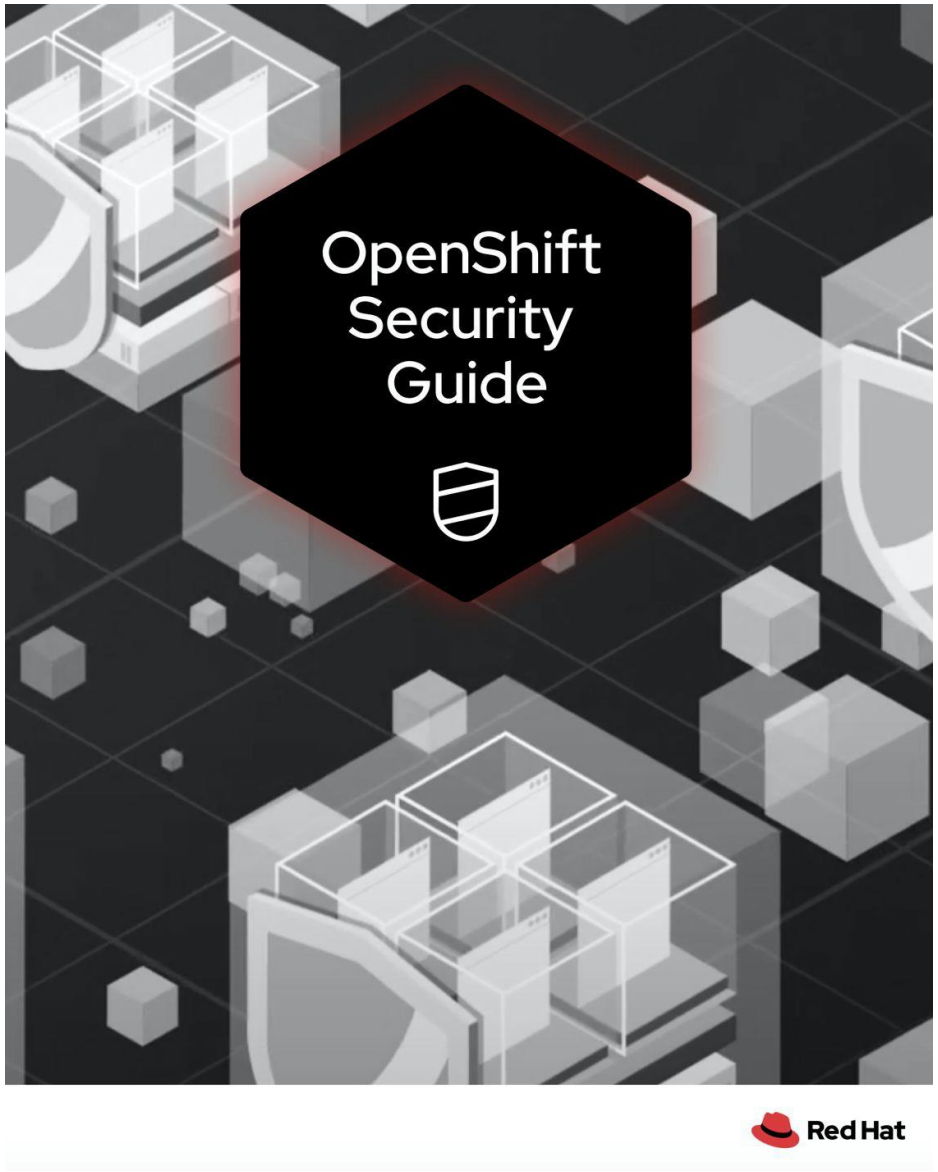
Источник:
https://access.redhat.com/articles/4763741

Безопасность начинается с хоста

- Безопасность хоста = безопасность контейнера
- SELinux, Seccomp и root capabilities позволят вам спать спокойно
- Защищайте не только хост от контейнеров, но и контейнеры друг от друга
- RHEL CoreOS обладает меньшим количеством векторов атак

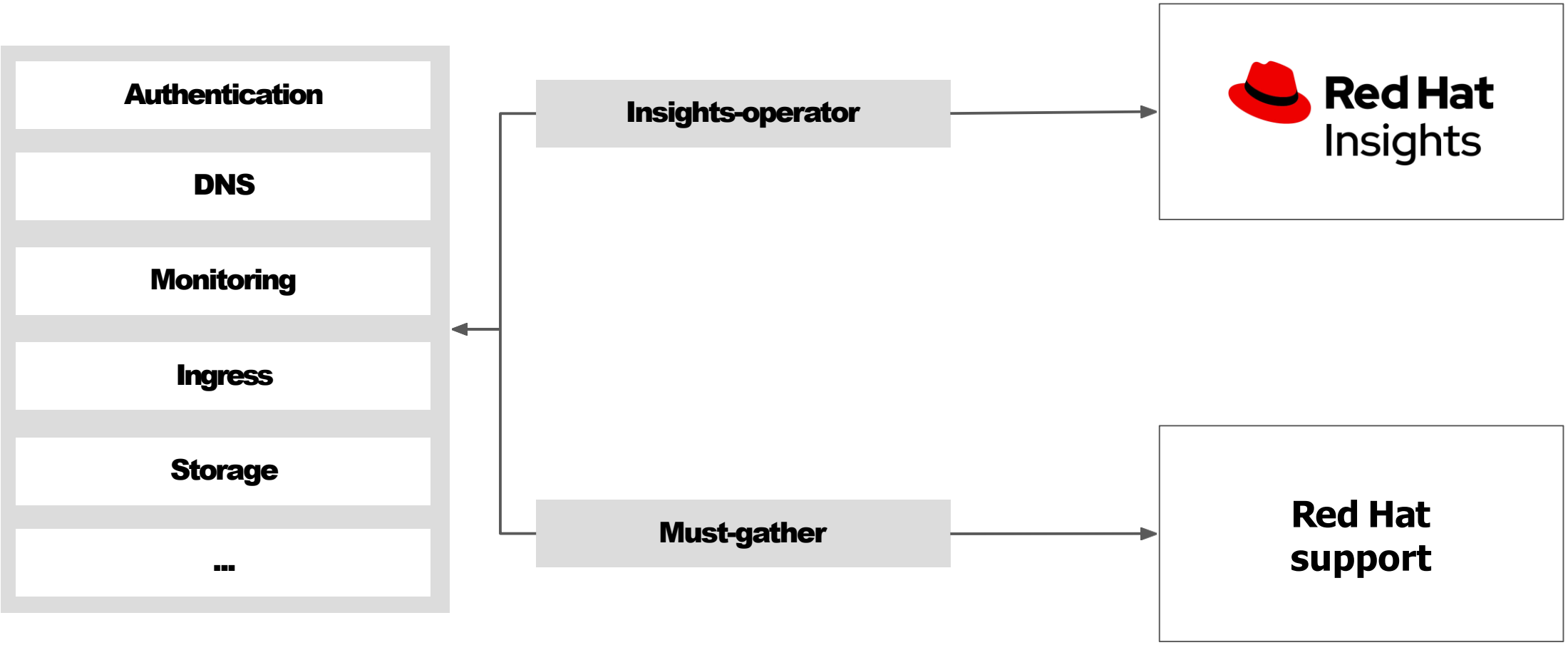


Openshift security guide

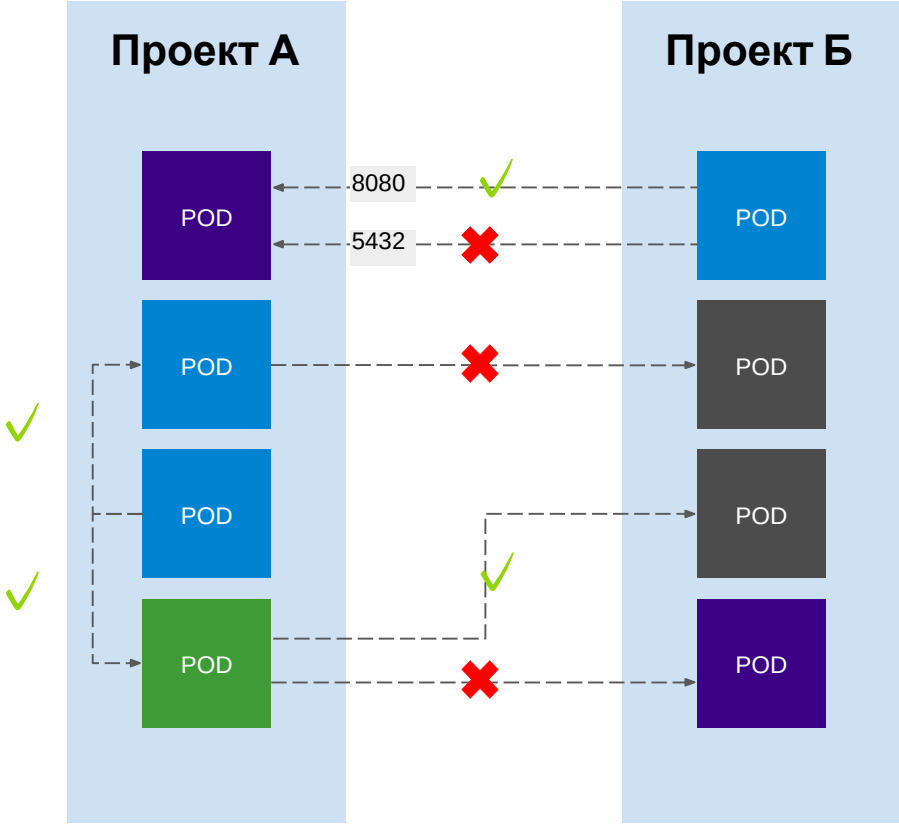


Источник
https://access.redhat.com/system/files/redhat_openshift_security_guide_2_for_screen_0.pdf

OpenShift and Red Hat Insights



NetworkPolicy

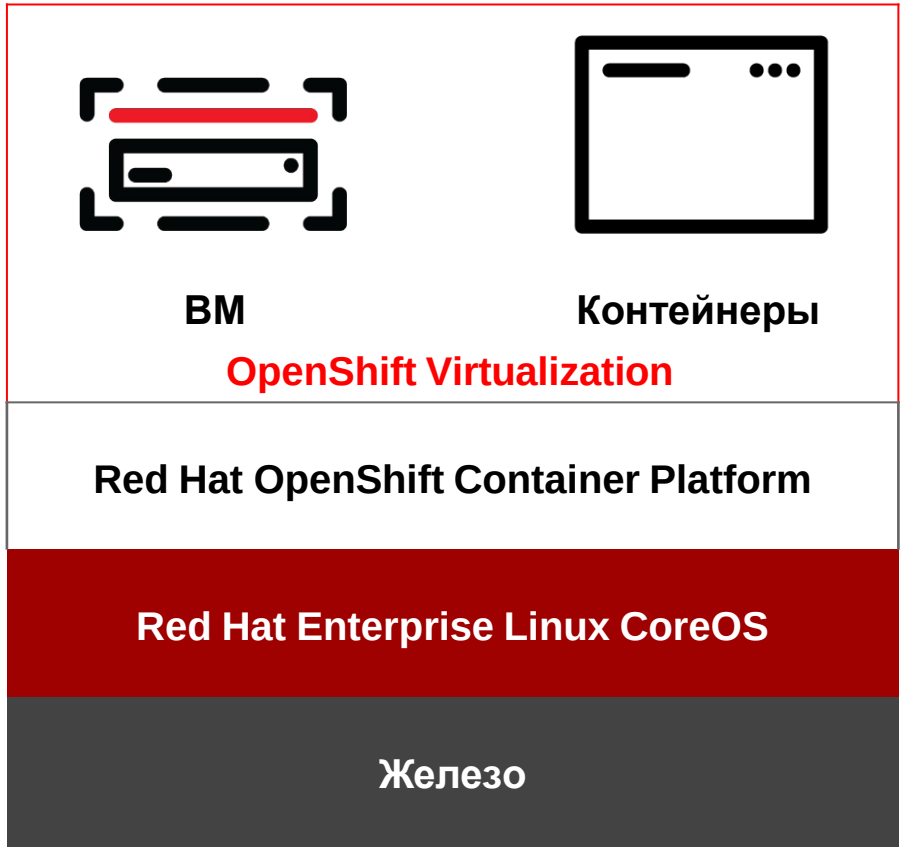


Примеры

- Разрешить весь трафик в проекте
- Разрешить трафик из зелёного в серое
- Разрешить трафик в фиолетовое по порту 8080

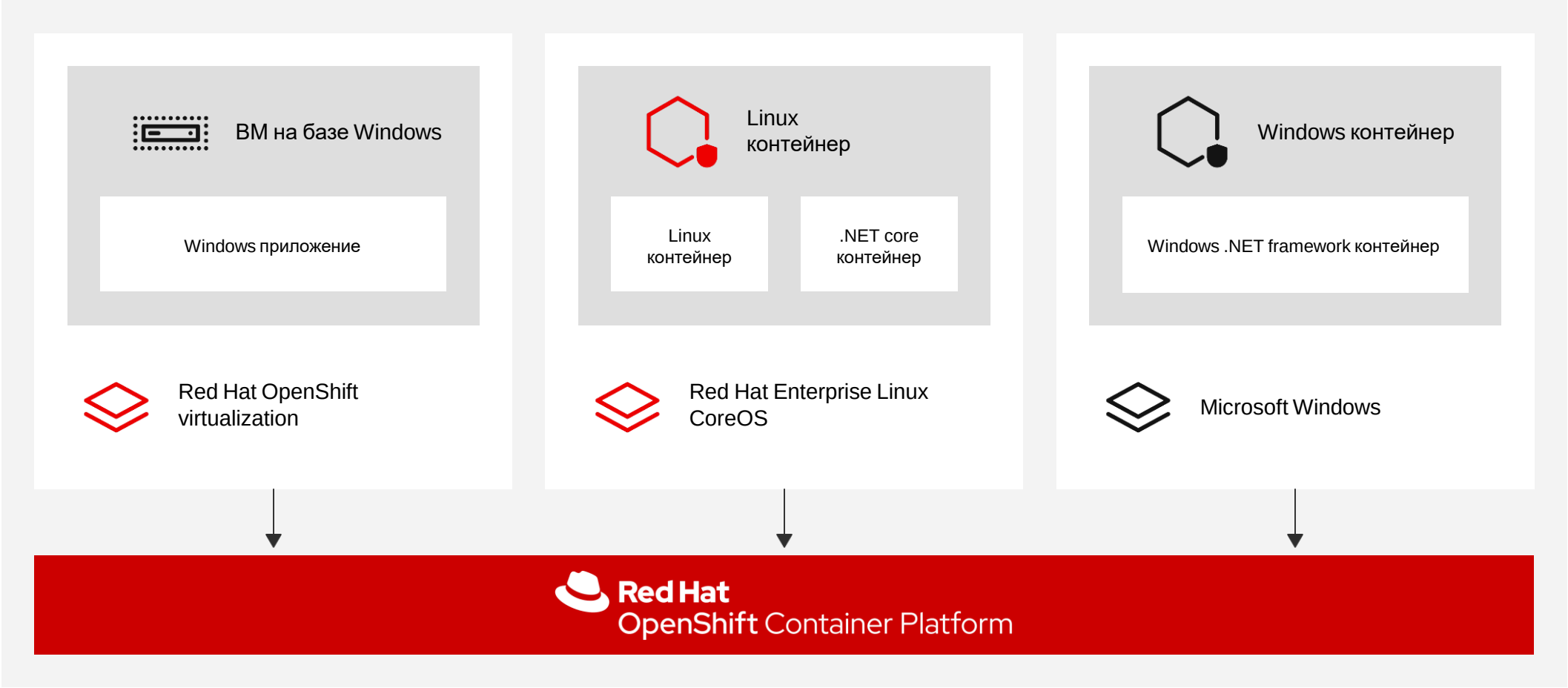
```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
  - ports:
    - protocol: tcp
      port: 8080
```

Виртуальные машины в OpenShift



- OpenShift Virtualization позволяет разворачивать “смешанные” приложения на одной платформе и управлять едиными средствами
- ВМ можно добавлять в имеющиеся приложения
- Модернизируете ваши приложения с течением времени, а пока управляйте всем из единого окна

Любая нагрузка будем как дома



Разрабатывайте эффективнее

Сборка → Тесты → Продуктив

- Самообслуживание
- Стандартные среды
- Автоматическая сборка приложений
- Конвейеры сборки-доставки (CI/CD)
- Управление конфигурациями
- Логирование и мониторинг

Создание ← Анализ ← Мониторинг

SPRING & JAVA™ EE	MICROSERVICES	FUNCTIONS
LANGUAGES	DATABASES	APPLICATION SERVICES
LINUX	RED HAT OPENSHIFT	WINDOWS

Helm Chart и Kubernetes Operators

“Упаковка” и установка

Автоматизация операций “Второго дня”

Helm Chart

Kubernetes Operator

Установка

Автоматизация установки приложения по предоставленным конфигурациям

Обновление

Установка патчей и обновление в рамках минорных версий

Автоматизация жизненного цикла

Сопровождение, настройка, резервное копирование, восстановление после отказа

Аналитика

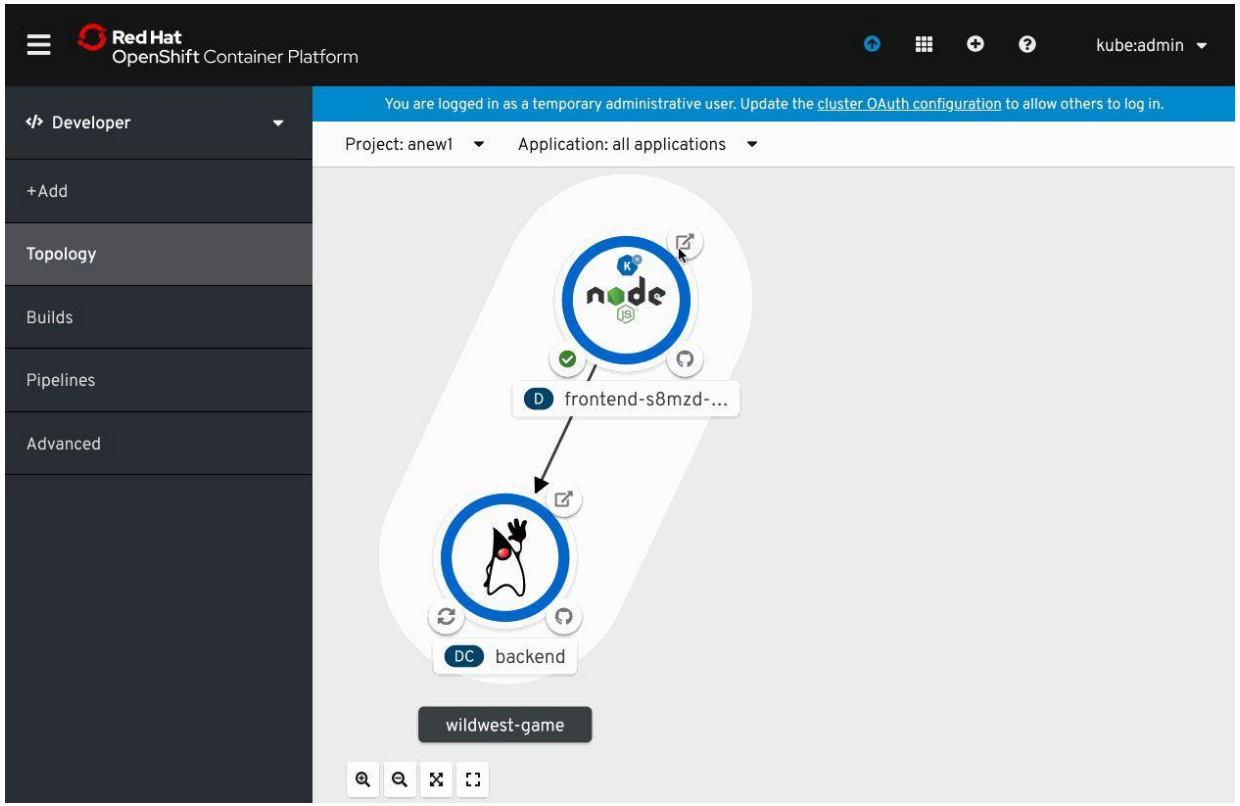
Метрики, оповещения, сбор и передача логов, анализ работы приложения

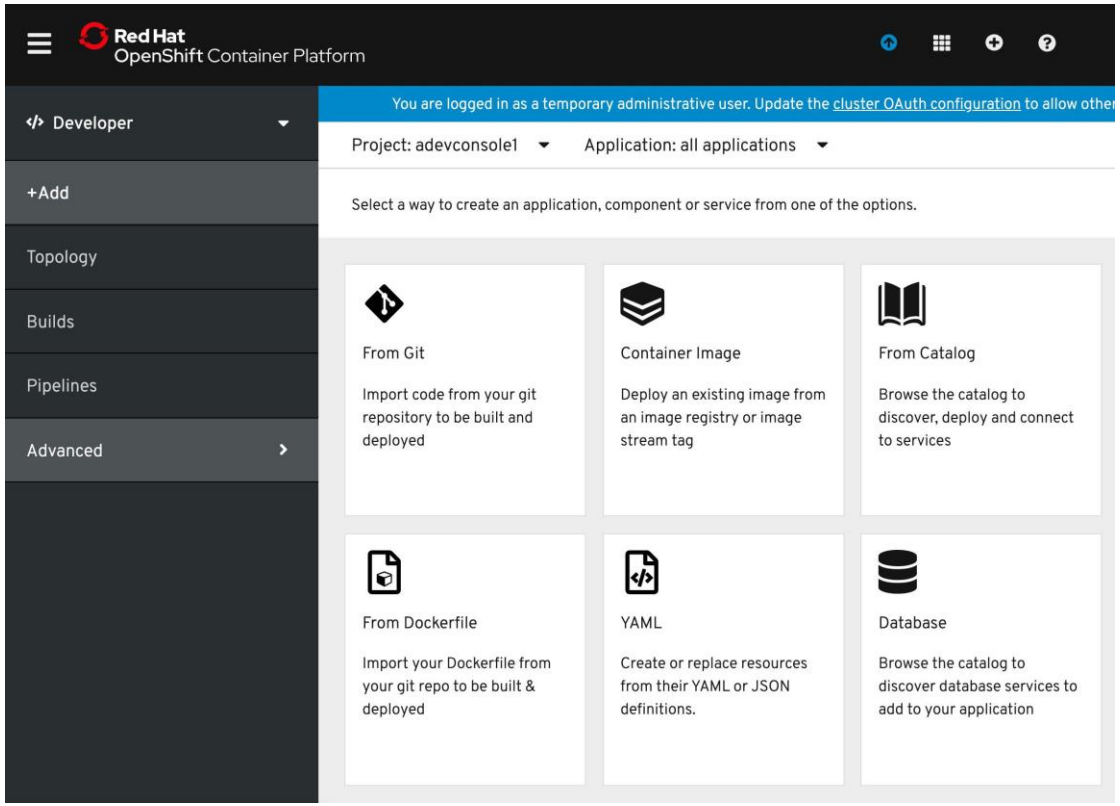
“Автопилот”

Масштабирование, автоматическое изменение конфигураций, настройка по расписанию, реакция на аномальное поведение

Nihol

Самообслуживание



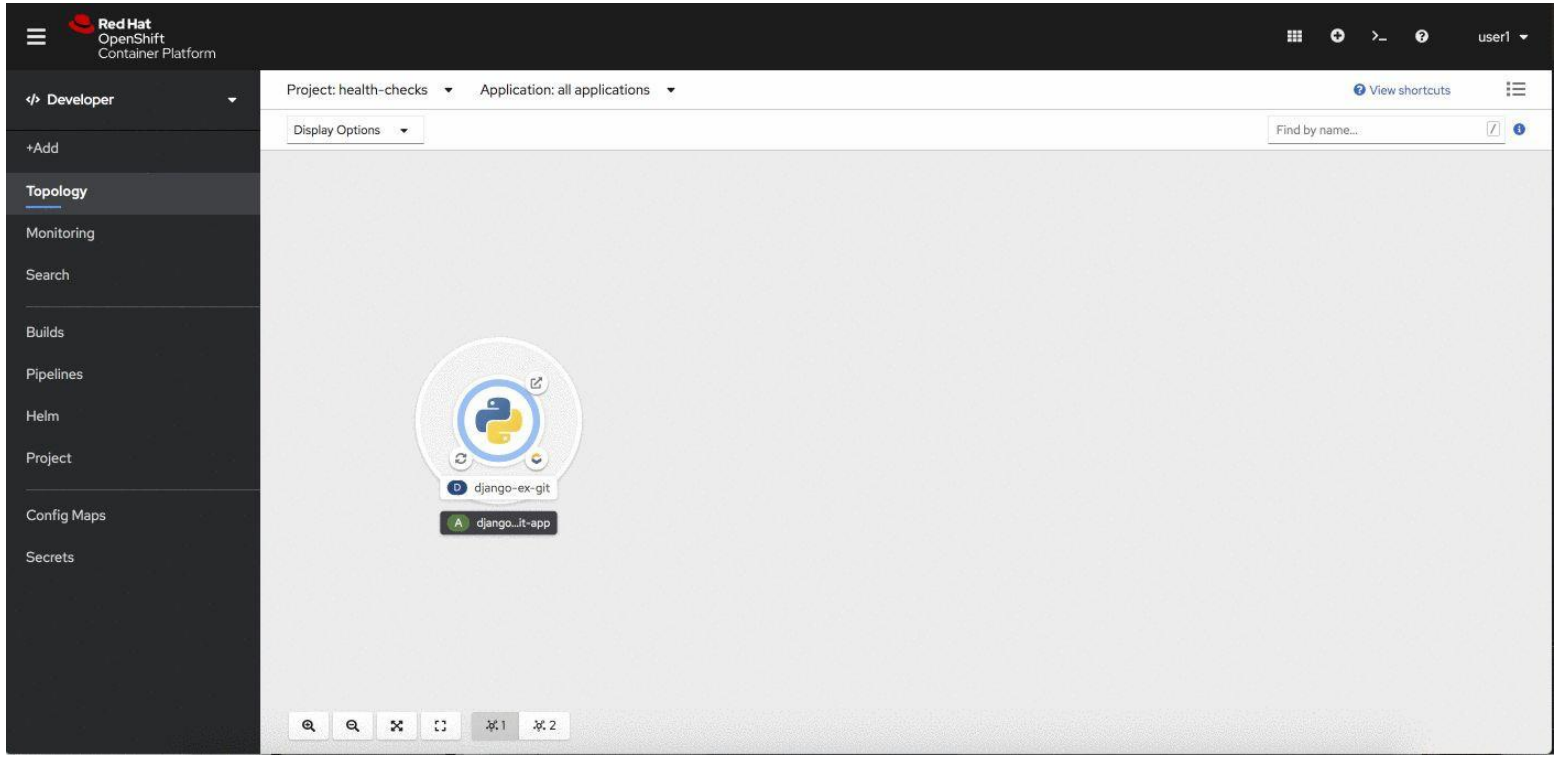


Red Hat

Работа с Health Check

Возможность добавлять health checks из web консоли

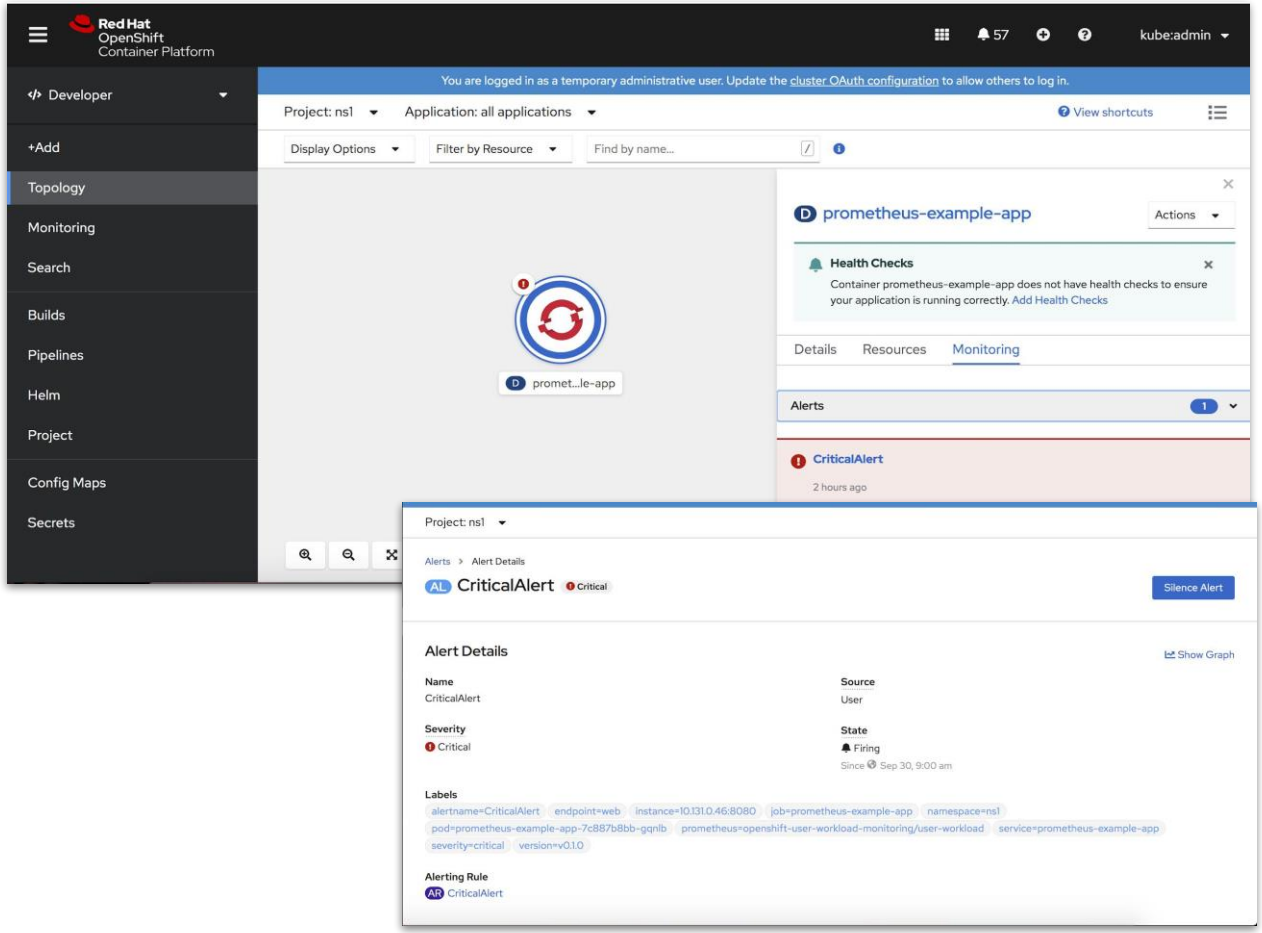
- Находятся в Advanced Option
- Оповещение о том, что вы не настроили health checks
- Можно добавлять и редактировать Health Checks
- Health checks реализуют liveliness, readiness и startup probes



Создание своих метрик

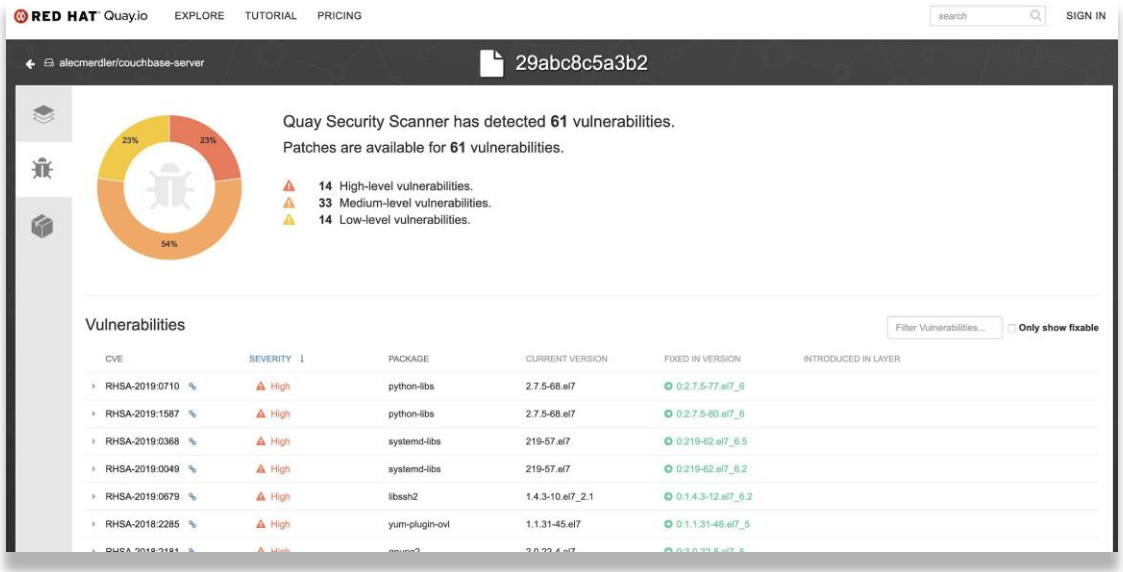
Используйте наш стек мониторинга для того, чтобы следить за вашими нагрузками

- Создавайте ваши правила для мониторинга приложений и инфраструктурных сервисов, которых нет “из коробки”
- Организуйте доступ до метрик и алертов через одну консоль, с использованием разграничений прав доступа.

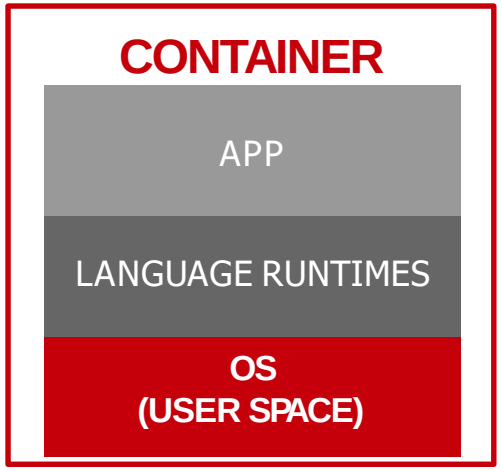


Что такое Clair?

- Инструмент для статического анализа образов на уязвимости с открытым исходным кодом
- Используется в Quay.io
- Применяется в других проектах (например, Amazon ERC и Harbor)



Red Hat Universal Base Image



Основанный на RHEL, Red Hat Universal Base Image доступен без дополнительной платы

Разработка

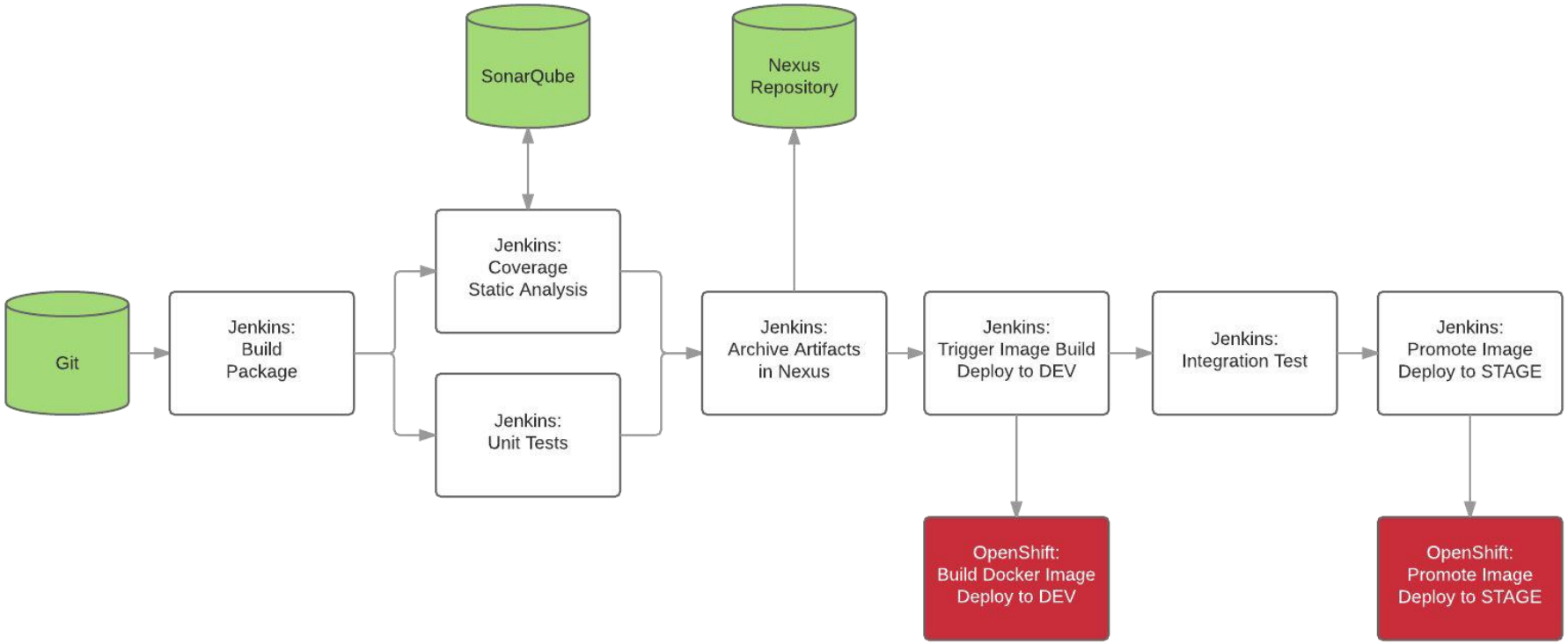
- Минимальный объём (~90 to ~200MB)
- Широкий выбор языков программирования

Использование

- Поддерживается как RHEL при работе на RHEL
- Та же производительность, безопасность и жизненный цикл, что и RHEL
- Можно использовать подписки для поддержки

Конвейеры сборки доставки на основе Jenkins

Расширяемый конвейер сборки-доставки Jenkins поможет вам создать вам вашу реализацию DevOps на предприятии



Сопутствующие технологии

OpenShift Service Mesh

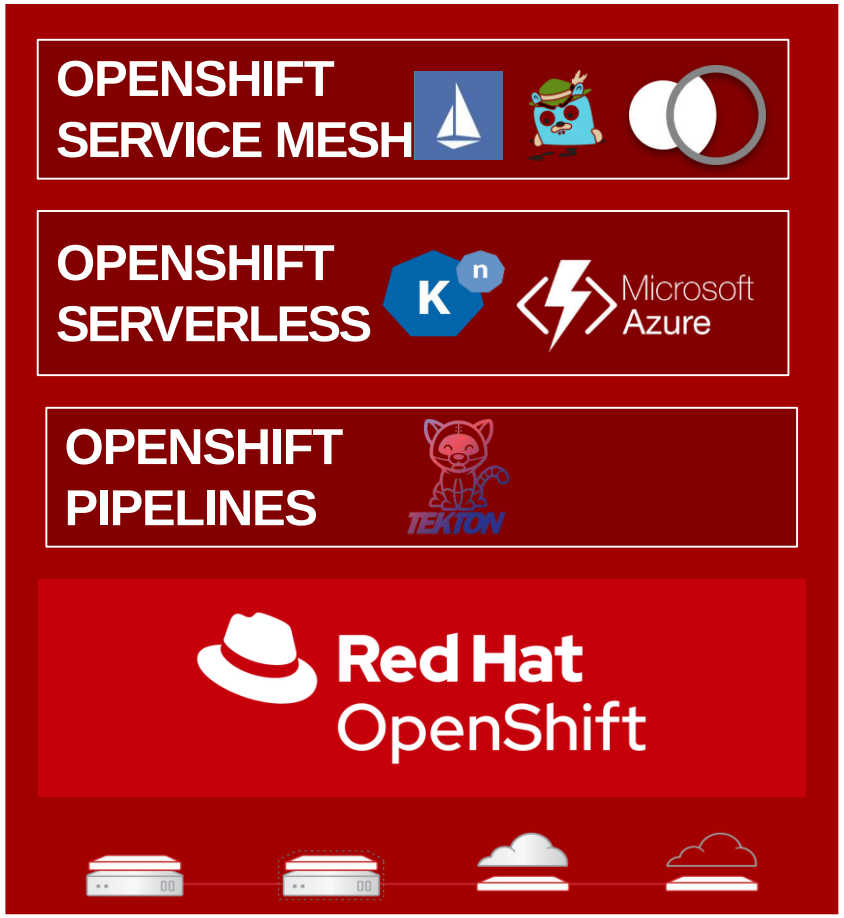
- Контроль сетевого взаимодействия микросервисов на базе Istio, Kiali (интерфейс) и Jaeger (Трассировка)

OpenShift Serverless

- Функция-как-сервис (FaaS) для того, чтобы автоматически изменять (в т.ч. до нуля) кол-во микросервисов на основе событий. Построено на базе Knative framework

OpenShift Pipelines (Tech Preview)

- Kubernetes-native конвейер сборки-доставки (CI/CD) на основе Tekton. Тесно интегрирован с OpenShift и его средствами для разработчиков



Удобство для разработчиков

CodeReady Workspaces

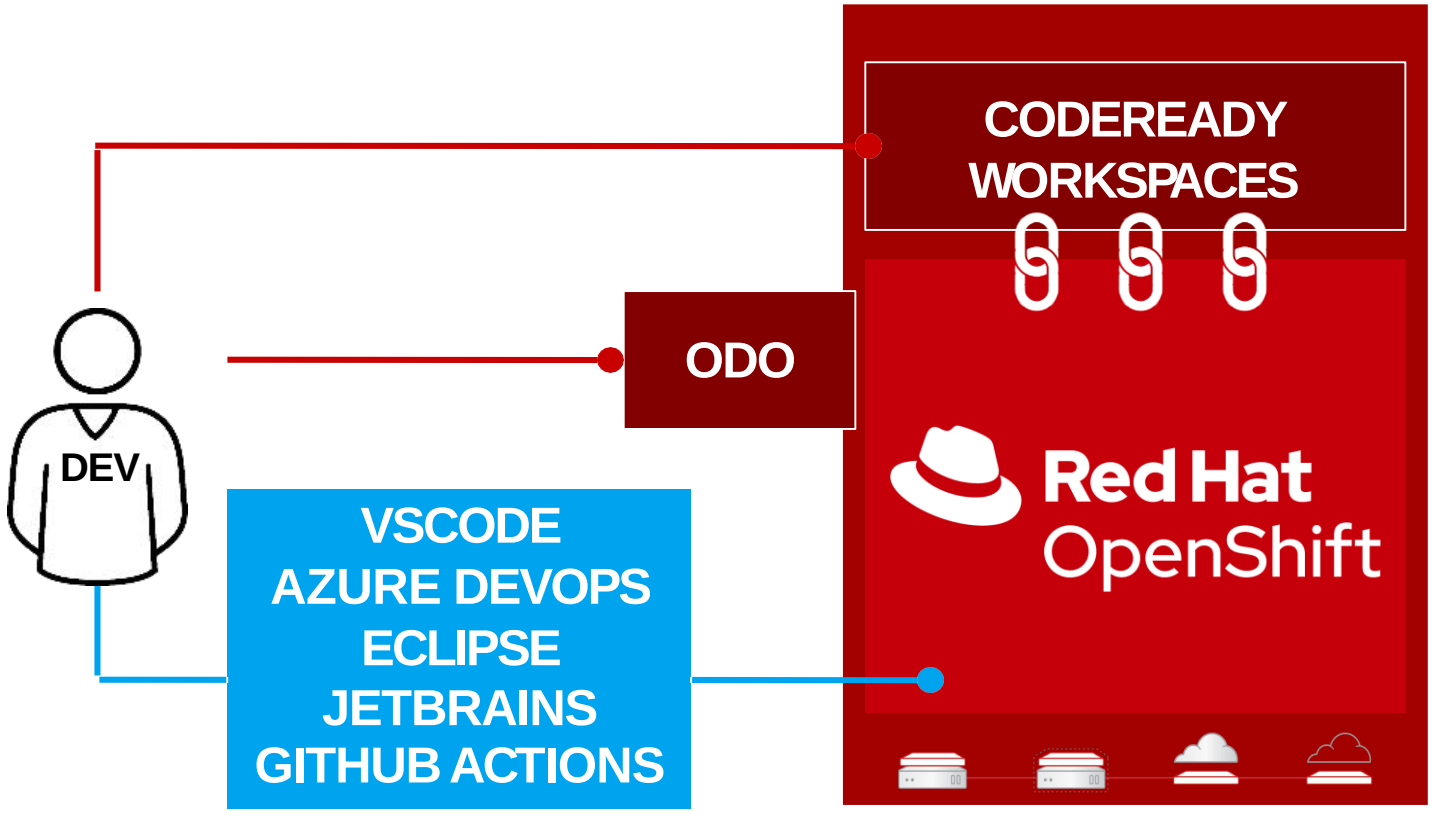
Kube-native web-based IDE для разработчиков. Пишите код откуда угодно

OpenShift ODO

CLI для разработчика, построенный по известному синтаксису git-push

OpenShift Plugins

Расширения для VScode, Azure DevOps, Eclipse IDE, JetBrains, GitHub Actions



CodeReady Workspaces

Container Workspaces

Полная имитация обычного рабочего места

Интеграции

Используйте встроенные средства OpenShift для большей продуктивности

Защита исходного кода

Код всегда в контейнере на вашей платформе, а не на ноутбуке разработчика

На основе Eclipse Che project (>10M pulls)	Составная часть платформы	Поддерживает расширения (plug-ins)	Встроенная поддержка stateful, stateless и serverless

Зачем? Чтобы быстро вводить в строй новых разработчиков и заменить VDI

Nihol

Много сценариев, любая инфраструктура, одна платформа

STATELESS, EVENT-DRIVEN MICROSERVICES	STATEFUL TRANSACTIONAL DATABASE	AI/ML INTELLIGENT APPS
RUNTIMES, INTEGRATION	RUNTIMES, AUTOMATION, CONTAINER STORAGE	AUTOMATION (DM, PAM), OPEN DATA HUB
SERVERLESS APPLICATIONS	TRADITIONAL MONOLITHIC	INTERNET OF THINGS
KNATIVE, OCF + MW INTEGRATIONS	EAP, APP MIGRATION/MODERNIZATION	AGILE INTEGRATION (FUSE, KAFKA)
CUSTOMER / PARTNER FACING	HIGH PERFORMANCE	PROCESS AUTOMATION / CASE MGMT APPS
RUNTIMES, AGILE INTEGRATION (3SCALE)	RUNTIMES, INTEGRATION	AUTOMATION, AGILE INTEGRATION (3SCALE)

RED HAT® OPENSHIFT

Red Hat OpenShift Container Storage

Red Hat

OpenShift Roadmap

Q4 2021

DEV
- OpenShift Builds v2 TP
- Simplify access to RHEL subs in builds

APP
- OpenShift Serverless Functions TP
- OpenShift Serverless on OSD as installed software
- Console internationalization GA
- Foundation for User Preferences
- Better Operator version & update mgmt

PLATFORM
- Azure Stack Hub
- IPv6 (single/dual stack on control plane)
- GA Userspace Interface API & Library
- Gateway API + Contour Tech Preview
- External DNS Management
- SmartNIC: OVS HW Offload
- OVN Egress Router
- MetalLB Support (L2)
- ipfailover Support
- Vertical Pod Autoscaling
- Pod Disruption Budget v1/beta to stable
- Scheduling profiles
- Service Mesh federation
- Windows BYOH
- ARM Support (Dev Preview)
- RHEL 8 Server Compute/Infra Nodes
- Multi-Instance-GPU support

HOSTED
- OSD consumption billing, autoscaling
- Expanded ROSA and OSD Add-ons
- ARO government region (MAG) support
- Cost management for IBM and GCP

1H 2022

DEV
- OpenShift Builds v2 GA
- Automate access to RHEL subs in builds
- Pipelines-as-code
- DevSecOps tasks in OpenShift Pipelines
- Rootless builds

APP
- OpenShift Serverless End-to-End Encryption
- OpenShift Serverless Knative Kafka Broker
- Application delivery dashboard in Dev Console
- Support for OCI chart repositories in Console
- Operator SDK for Java (Tech Preview)

PLATFORM
- OVN as default networking plugin
- IBM Cloud, Alibaba IPI/UPI
- Edge: Single node lightweight Kube cluster
- SmartNIC support for perf., OVS hardware offload
- Gateway API + Contour
- BGP Advertised Services (FRR)
- ACM scale to 2000 single node clusters
- CoreOS dynamic first boot images for fast scaling
- Windows with containerd runtime support
- Subject claim URI scheme for OIDC IdPs
- Move to out-of-tree cloud providers
- FIPS compliance for OpenShift sandboxed Containers
- OCP Virt. VMs in Service Mesh
- Cert-manager operator
- NetFlow/sFlow/IPFIX Collector
- Network Observability & Analysis Tooling
- ARM Support (GA)

HOSTED
- Cost management forecasting and budgeting

2H 2022

DEV
- OpenShift Builds v2 & Buildpacks GA
- Tekton Hub on OpenShift
- OpenShift sandboxed containers in Pipelines

APP
- OpenShift Serverless Functions GA
- Global Operators Model & new Operator API
- Operator Maturity increase via SDK
- Dynamic Plugins for the OCP Console

PLATFORM
- Azure China & AWS China
- AWS Outposts, Equinix Metal, & Microsoft Hyper-V
- Utilize cgroups v2
- Enable user namespaces
- Additional Windows Containers capabilities*
- Ingress Traffic Mirroring/Splitting
- Network Topology and Analysis Tooling
- SmartNIC Integrations
- Network Policy v2
- eBPF
- OVN no-overlay option

HOSTED
- Cost mgmt integration to Subs Watch, ACM
- ROSA AWS console integration
- Cluster Suspend / Resume

Red Hat Advanced Cluster Management for Kubernetes

- Единое окно для управления кластерами
- Настройка и анализ кластеров с помощью политик
- Упрощенное управление приложениями во всех кластерах
- Единая точка мониторинга за вашими кластерами
- GitOps для всех ваших кластеров

Red Hat Advanced Cluster Security for Kubernetes

- Kubernetes-native решение
- Shift-left подход
- Сканирование образов и конфигураций в любой момент жизненного цикла
- Ранжирование угроз
- Анализ сетевого взаимодействия и автоматизация сетевых политик
- Реакция на угрозы в реальном времени

DevOps → DevSecOps ← Security

Nihol

Red Hat Quay

Реестр контейнерных образов с открытым исходным кодом, который работает везде, но лучше всего в связке с OpenShift

Работает как на ноутбуке разработчика, так и в сценариях гео-распределённых сред с большими нагрузками

Контроль и безопасность обеспечивается с помощью сканирования образов, контроля доступа, гео-репликации и т. д.

Доступен как отдельный продукт в вашем ЦОД, так и в виде SaaS сервиса от Red Hat

Red Hat

Nihol

Спасибо за внимание!

Узбекистан, г. Ташкент, 100187, ул. Интизор, 26,
Группа компаний NIHOL

(998-71) 208-58-44, 208-58-45, 208-58-48, 266-58-46,

266-58-47

info@nihol.uz

Red Hat
Data Services