

Минималистичный стек CI/CD

Инструменты CI/CD
Демонстрация CI/CD в среде Kubernetes
Возможности улучшения

СОДЕРЖАНИЕ

Детали инсталляции

Обзор инструментов:

- RKE/Rancher
- MetalLB
- cert-manager
- local-path-provisioner
- Gitea
- registry
- Drone CI
- Argo CD
- Argo Rollouts
- helm

Демо процесса

- инфраструктура стенда

- минималистичный стек для CI/CD

- Управление сертификатами Let's Encrypt
- Полностью автоматизированный CI/CD с уведомлениями Telegram
- Канареевые развертывания и A/B-тестирование
- Возможность воспроизведения на архитектуре ARM (Raspberry Pi)
- Поддержка helm
- Возможность масштабирования инфраструктуры
- Детализированный мониторинг и логирование
- Возможность добавлять инструменты безопасности в стек

- демонстрация CI/CD на примере простого web-приложения



Цель презентации

Демо минималистичного стека CI/CD в среде
Kubernetes, предложение вариантов
внедрения и использования

Прототип

Демонстрация

Эксплуатация

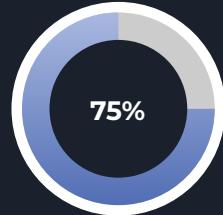
Доработка



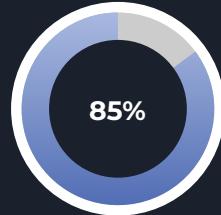


Целевая аудитория

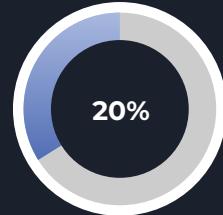
Developers и QA



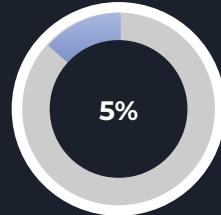
Знания в собственной
предметной области



Потребность в стенде разработки и
тестирования



Общие знания в
Kubernetes и Docker

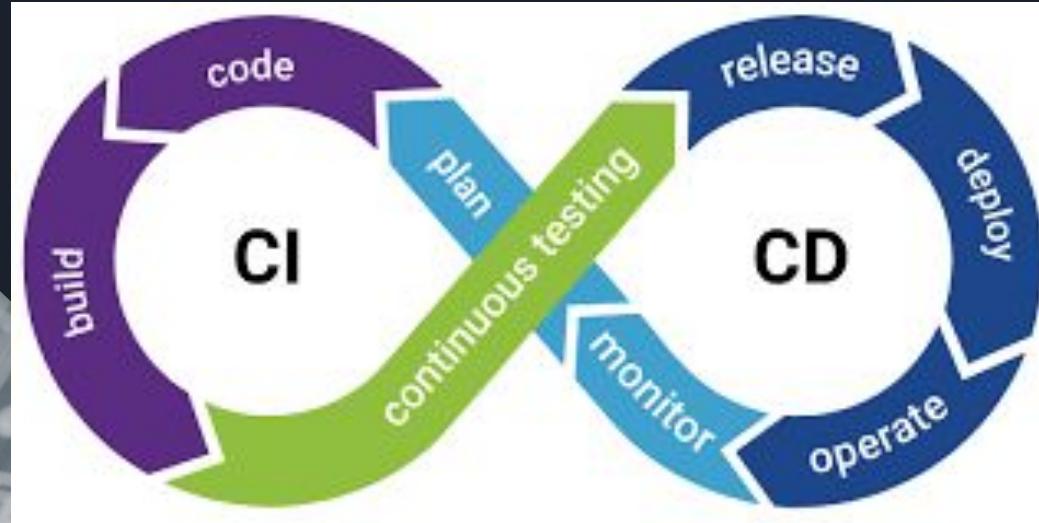


Общие знания в
администрировании Linux





Что такое CI/CD?

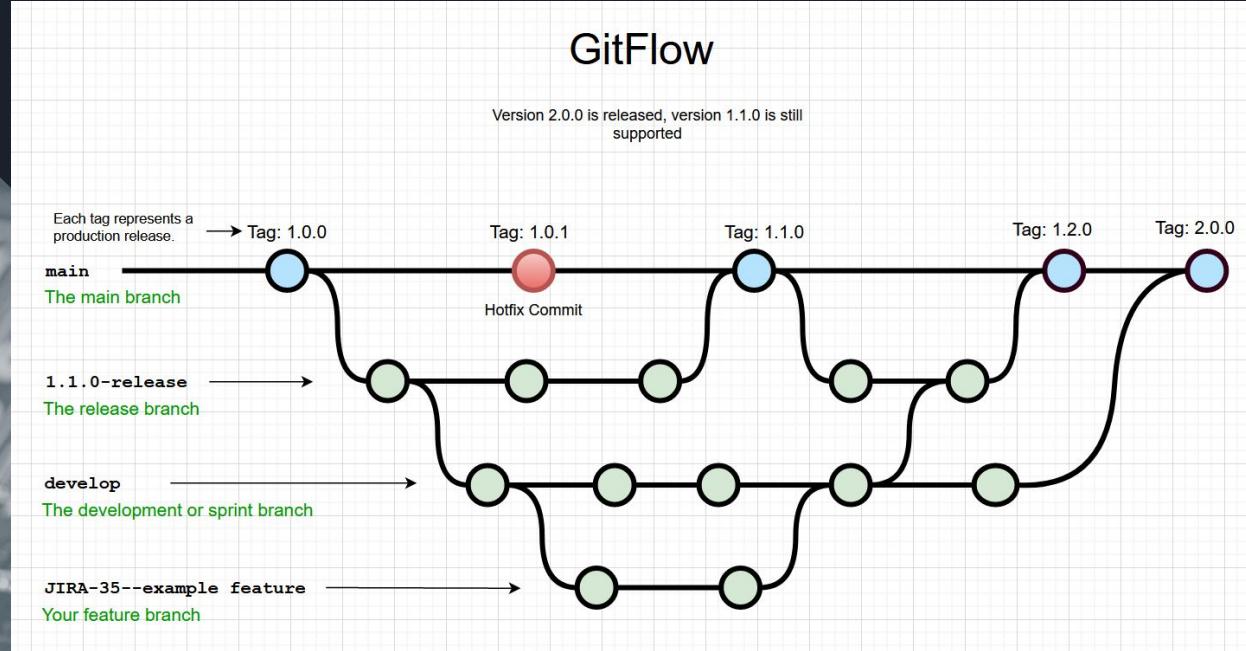


В разработке ПО, CI/CD — это комбинация непрерывной интеграции и непрерывного развертывания программного обеспечения в процессе разработки с высоким уровнем автоматизации. CI/CD объединяет разработку, тестирование и развертывания приложения. В настоящий момент DevOps-программисты стремятся применять CI/CD практически для всех задач.



GitFlow

(один из вариантов)



GitFlow — модель ветвления Git, в которой используются функциональные ветки и несколько основных веток. В соответствии с этой моделью разработчики создают функциональную ветку и откладывают ее слияние с главной магистральной веткой до завершения работы над функцией.



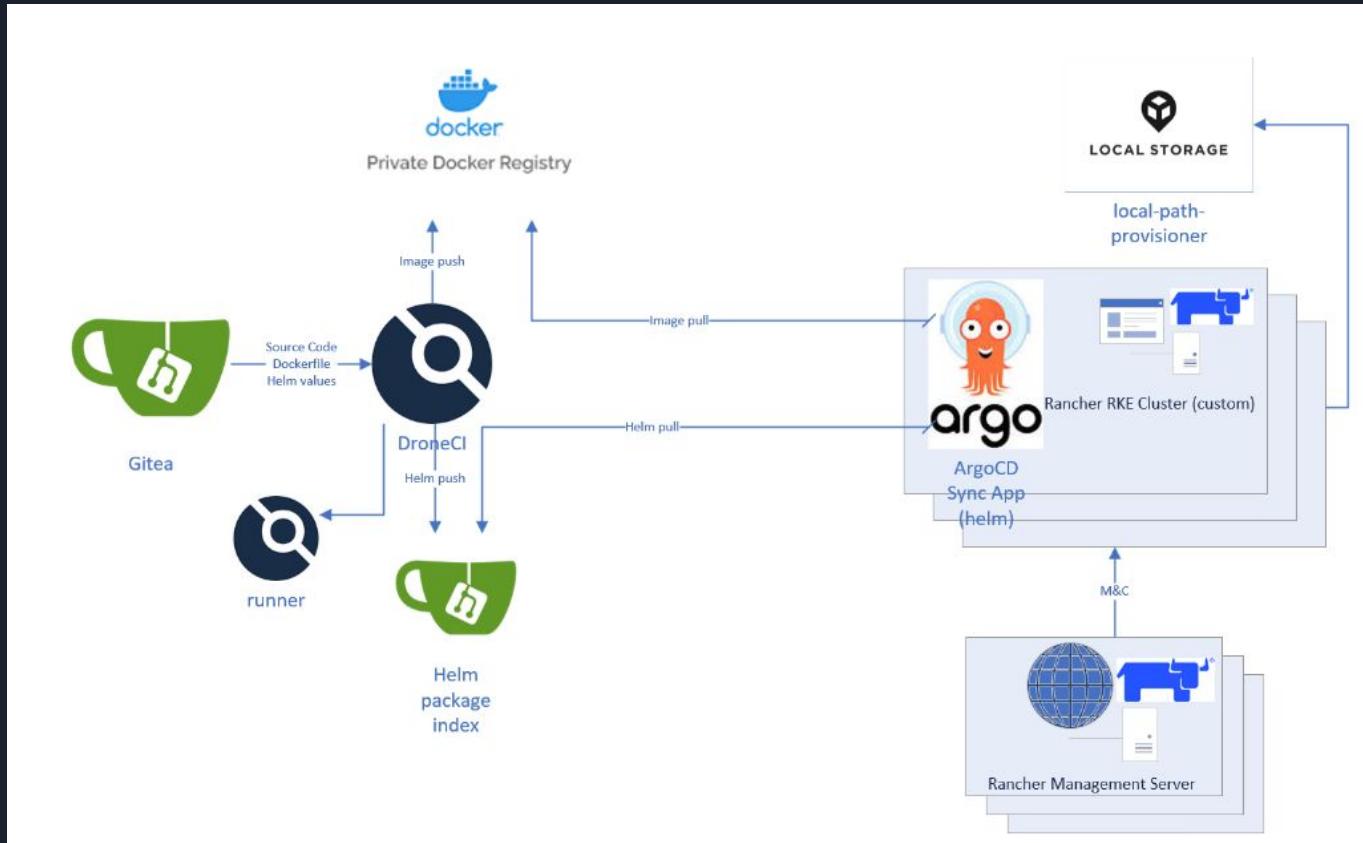
Требования к инфраструктуре

Для генерации стенда потребуется:

- не менее 4-х физических ядер CPU и 24 ГБ RAM для ноды кластера Kubernetes
- Rancher Desktop для Management Server (на ноутбуке)
- роутер с возможностью DNAT и VPN
- реальный IP-адрес на ноде кластера
- доменное имя и DNS-провайдер.

Всё используемое в стеке ПО с открытым исходным кодом, бесплатно и может быть получено в процессе генерации стенда через Интернет.

Схема CI/CD (упрощенная)





Инфраструктура стенда

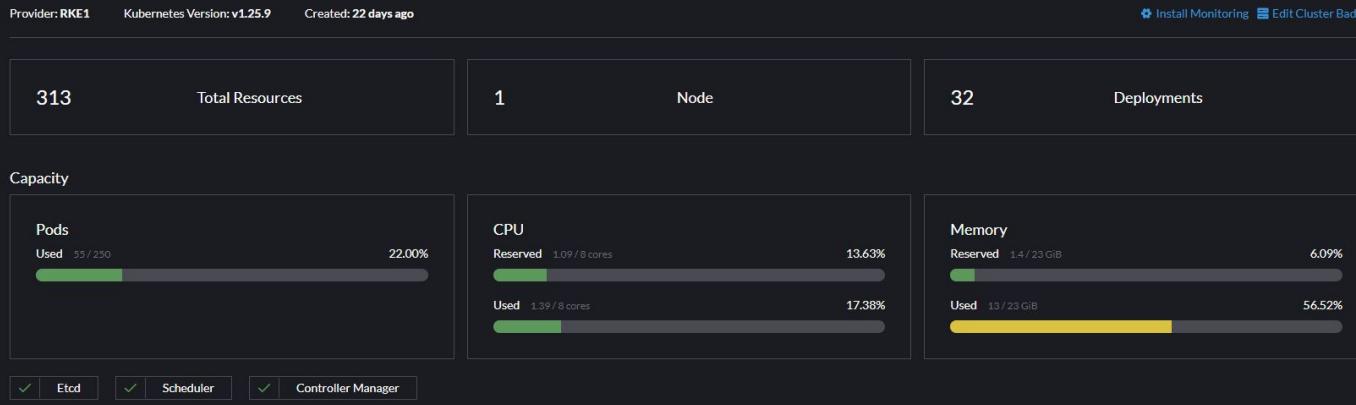
Rancher Desktop (для М&С)

Rancher RKE1 Cluster

The screenshot displays two windows side-by-side. On the left is the Rancher Desktop application window, showing a sidebar with General, Port Forwarding, Images, Troubleshooting, and Diagnostics options. The main area is titled 'Welcome to Rancher Desktop' and includes a version info section (Version: 1.8.1), a statistics collection checkbox, and a network status indicator (Network status: online). On the right is the Rancher UI Cluster Dashboard, showing a tree view of the cluster structure under the 'local' node. It lists Workloads (CronJobs: 0, DaemonSets: 1, Deployments: 13, Jobs: 0, StatefulSets: 0, Pods: 14), Apps, Service Discovery, Storage, Policy, and More Resources. Below the tree view, a table lists running pods across three namespaces: cattle-fleet-system, cattle-system, and cattle-ui-plugin-system. The table columns include Pod name, Status, Image, and Count.

Namespace	Pod Name	Status	Image	Count
cattle-fleet-system	fleet-controller-686c7dcfcf-wjokc	Running	rancher/fleet:v0.6.0	1/1
cattle-fleet-system	gitjob-79f557d76fb467	Running	rancher/gitjob:v0.1.37	1/1
cattle-system	rancher-769656fb94-rcm7t	Running	rancher/rancherv2.7.3	1/1
cattle-system	rancher-webhook-7d5f881677-5vjq	Running	rancher/rancher-webhook:v0.3.3	1/1

Cluster Dashboard



Инструменты

Gitea - управление исходным кодом

Задачи Запросы на слияние Этапы Обзор

my-project

Репозитории Проекты Пакеты Участники Команды Настройки

Поиск Сортировать

Новый репозиторий
Новая миграция

my-project-php Приватный
my-project-php
site
Обновлено 45 минут назад

my-project-helm Приватный
my-project-helm
Обновлено 5 дней назад

apache-bullseye-base Приватный
Обновлено 2 недели назад

Участники 1 >
Команды 1 >
Онтопс
1 Участники · 3 Репозитории
Создание команды

Gitea — ПО для хостинга IT-проектов и совместной разработки на базе Git. Поддерживает отслеживание ошибок, вики и обзора кода. Gitea поддерживает самостоятельный хостинг, но также существует и бесплатный сервис. Википедия

Языки программирования: Go, JavaScript

Лицензия: лицензия MIT

Написана на: Go и JavaScript

Сайт: gitea.io

Инструменты

Drone CI - сборка,
тестирование и публикация
артефактов

The screenshot shows the Drone CI dashboard interface. At the top, there's a header with a search icon and a 'Dashboard' button. Below the header is a section titled 'RECENT ACTIVITY' displaying three recent pull requests:

- my-project/my-project-php: v1.0.42 - Merge pull request 'stage' (#15) from stage into main. Reviewed-on: <https://git.simshp.ru/my-project/my-project-php>. 1 hour ago.
- my-project/my-project-helm: v2.3.0 - Изменен(а) на 'my-project/Chart.yaml'. 5 days ago.
- my-project/apache-bullseye-base: v8.119-1 - change Dockerfile. 14 days ago.

Below the recent activity is a 'REPOSITORIES' section listing three repositories:

- my-project/my-project-php: ed0521e6 - Merge pull request 'stage' (#15) from stage into main. Reviewed-on: <https://git.simshp.ru/my-project/my-project-php>. 1 hour ago.
- my-project/my-project-helm: 9fe6d59f - Изменен(а) на 'my-project/Chart.yaml'. 5 days ago.
- my-project/apache-bullseye-base: edad1ba3 - change Dockerfile. 14 days ago.

Автоматизация сборки и
тестирования программного
обеспечения

Drone - это платформа непрерывной
интеграции самообслуживания для
групп разработчиков.

Сайт: drone.io

Инструменты

Argo CD -
доставка приложения
в кластеры Kubernetes

The screenshot shows the Argo CD web interface for the application 'my-project-dev'. On the left, there's a sidebar with navigation links like 'Applications', 'Settings', 'User Info', and 'Documentation'. The main area displays the application details for 'my-project-dev'. It shows the sync status as 'Synced' to version 2.3.0, with the last sync occurring an hour ago. Below this, a detailed view of the application's components is shown in a tree structure:

- my-project-dev**: Contains a service ('svc') and a deployment ('deploy'). The deployment has a revision labeled 'rev1'.
- my-project-dev-site**: Contains an endpoint ('ep'), an Elasticsearch pod ('es'), and a replicaset ('rs'). The replicaset also has a revision labeled 'rev1'.
- my-project-dev-site-8fcfd59567**: Contains a pod ('pod') which is currently running.

Each component has a green heart icon indicating it is healthy. The interface includes various buttons for managing the application, such as 'APP DETAILS', 'APP DIFF', 'SYNC', 'SYNC STATUS', 'HISTORY AND ROLLBACK', 'DELETE', and 'REFRESH'.

Argo CD - декларативный инструмент непрерывной доставки GitOps для Kubernetes.

Определения, конфигурации и среды приложений должны быть декларативными и контролироваться версиями. Разворачивание приложений и управление жизненным циклом должны быть автоматизированными, проверяемыми и простыми для понимания.

Сайт: argo-cd.readthedocs.io



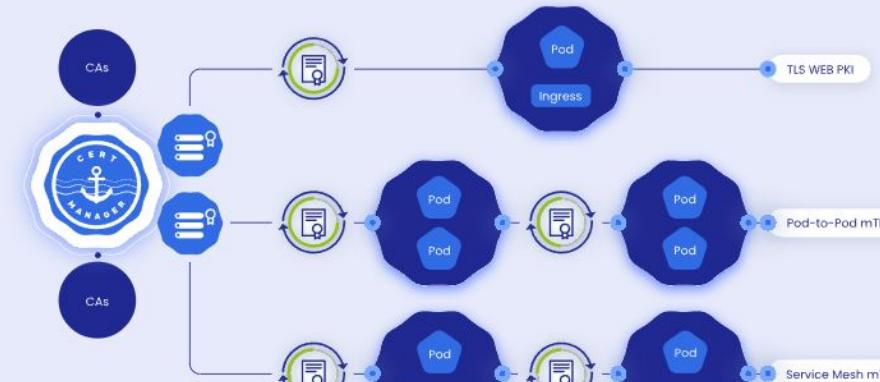
Сопутствующие программы

cert-manager

Cloud native certificate management

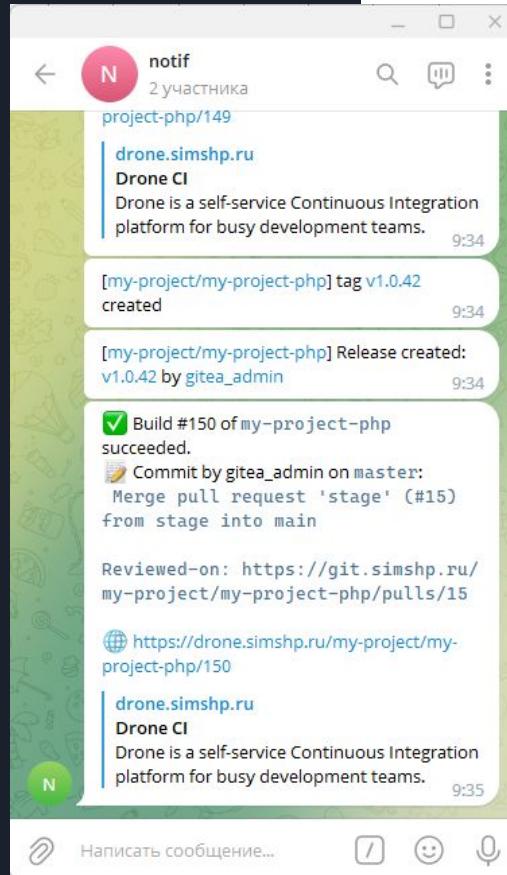
X.509 certificate management for
Kubernetes and OpenShift

Управление сертификатами
для Kubernetes



Telegram

Сопутствующие программы



Уведомления о событиях
CI/CD



Argo Rollouts - Kubernetes Контроллер прогрессивной доставки

Сопутствующие программы
(после доработки helm-чарта)

Канареевые деплои и A/B-
тестирование

Rollouts

NS: rollouts-demo v1.0.0+75eeb71.dirty

Search...

Revision	Strategy	Weight	Status
bluegreen-demo-6cbcccd9f99	BlueGreen	100	Green
canary-demo-68f96454b6	Canary	20	Green
rollouts-demo-7bf84f9696	Canary	80	Green
bluegreen-demo-6cbcccd9f99	BlueGreen	100	Green
canary-demo-645d5dbc4c	Canary	40	Green
rollouts-demo-789746c88d	Canary	60	Green

bluegreen-demo

Strategy: BlueGreen

bluegreen-demo-6cbcccd9f99 Revision 1

canary-demo

Strategy: Canary

Weight: 20

canary-demo-68f96454b6 Revision 9

rollouts-demo

Strategy: Canary

Weight: 80

rollouts-demo-7bf84f9696 Revision 5

bluegreen-demo-6cbcccd9f99

canary-demo-645d5dbc4c

rollouts-demo-789746c88d

RESTART PROMOTE-FULL

RESTART PROMOTE-FULL

RESTART PROMOTE-FULL



Сопутствующие программы

Helm

менеджер пакетов
для Kubernetes

Helm — лучший способ
искать, делиться и
использовать программное
обеспечение, созданное для
Kubernetes.





Сопутствующие программы
(инфраструктурный компонент)

MetalLB

MetalLB — это реализация балансировщика нагрузки для кластеров Kubernetes на «голом железе», использующая стандартные протоколы маршрутизации.

MetalLB устанавливается в кластере Kubernetes и обеспечивает реализацию балансировщика сетевой нагрузки. Короче говоря, он позволяет создавать сервисы Kubernetes типа LoadBalancer в кластерах, которые не работают в облачном провайдере, и, следовательно, не могут просто подключаться к платным продуктам для предоставления балансировщиков нагрузки.



Сопутствующие программы для кластера

observability, tracing, security

Cluster Tools

All charts have at least one version that is installable on clusters with Linux and Windows nodes unless otherwise indicated.



Alerting Drivers

v102.0.0

The manager for third-party webhook receivers used in Prometheus Alertmanager

Install



CIS Benchmark

v4.0.0

The cis-operator enables running CIS benchmark security scans on a kubernetes cluster

Install



Istio

v102.2.0+up1.17.2

A basic Istio setup that installs with the istioctl. Refer to <https://istio.io/latest/> for details.

Install



Logging

v102.0.0+up3.17.10

Deploys on Windows

Collects and filter logs using highly configurable CRDs. Powered by Banzai Cloud Logging Operator.

Install



Longhorn

v102.2.0+up1.4.1

Longhorn is a distributed block storage system for Kubernetes.

Install



Monitoring

v102.0.0+up40.1.2

Deploys on Windows
Collects several related Helm charts, Grafana dashboards, and Prometheus rules combined with documentation and scripts to provide easy to operate end-to-end Kubernetes cluster monitoring with Prometheus using the Prometheus Operator.

Install



NeuVector

v102.0.1+up2.4.3

Helm feature chart for NeuVector's core services

Install



OPA Gatekeeper

v102.0.0+up3.10.0

Modifies Open Policy Agent's upstream gatekeeper chart that provides policy-based control for cloud native environments

Install

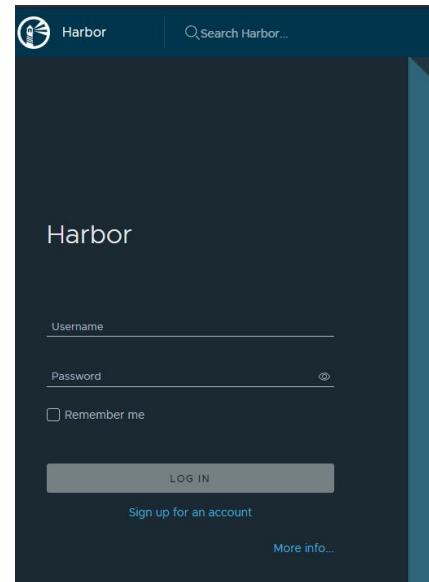


Возможности улучшения стека

Harbor (вместо registry)

Harbor - это реестр с открытым исходным кодом, который защищает артефакты с помощью политик и контроля доступа на основе ролей, обеспечивает сканирование изображений и отсутствие уязвимостей, а также подписывает образы.

Harbor, выпускной проект CNCF, обеспечивает соответствие, производительность и функциональную совместимость, чтобы помочь вам последовательно и безопасно управлять артефактами на собственных вычислительных платформах облаков, таких как Kubernetes и Docker.





Возможности улучшения стека

SonarQube

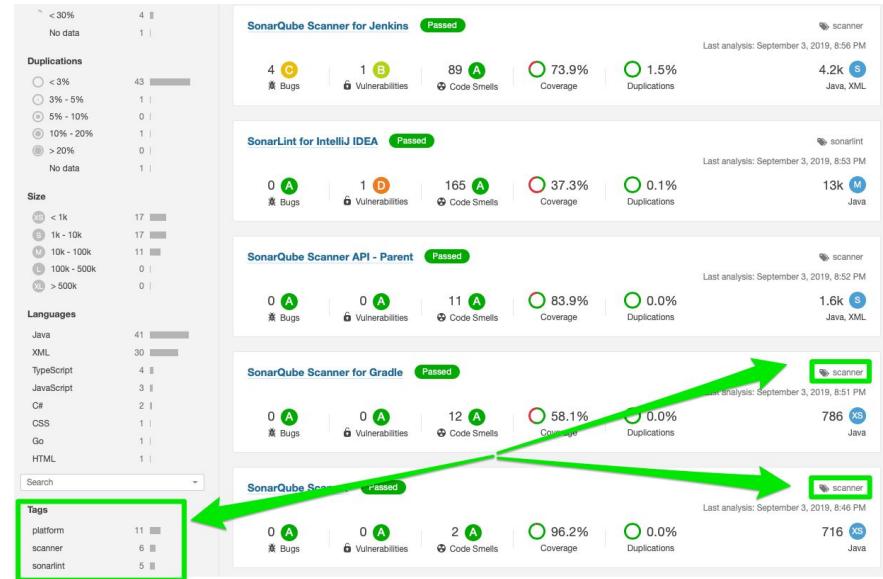
SonarQube — платформа с открытым исходным кодом для непрерывного анализа и измерения качества программного кода. Поддерживает анализ кода и поиск ошибок согласно правилам стандартов программирования.

Язык программирования: Java

Лицензия: GNU LGPLv3

Операционная система:
Кроссплатформенное

Последняя версия: 9.4





Возможности улучшения стека

Vault

Управление секретами и
защита чувствительных
данных с помощью Vault

Защита, хранение и контроль доступа
к токенам, паролям, сертификатам,
ключам шифрования и другим
конфиденциальным данным с
помощью пользовательского
интерфейса, CLI или HTTP API

Возможность интеграции со всеми
инструментами стека CI/CD





ДeMO

Вопросы?

Спасибо!

Минималистичный стек CI/CD

