

Minimalistic CI/CD stack

CI/CD tools

CI/CD demo in a Kubernetes environment
Possibilities for improvement

CONTENT

Installation details

Tool overview:

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

Process Demo

- stand infrastructure

- minimal stack for CI/CD

- Managing Let's Encrypt Certificates
- Fully automated CI/CD
- with Telegram notifications
- Canary Deployments and A/B Testing
- Playability
- on ARM architecture (Raspberry Pi)
- helmet support
- Ability to scale infrastructure
- Detailed monitoring and logging
- Ability to add security tools to the stack

- demonstration of CI/CD using a simple web application as an example

Purpose of presentation

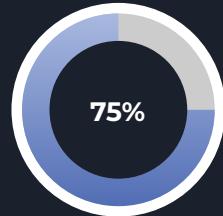
Demo of a minimalist CI/CD stack in a Kubernetes environment, suggesting implementation and use cases



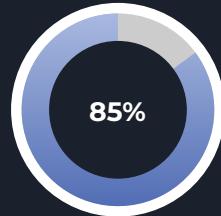


The target audience

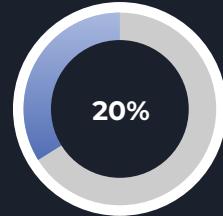
Developers и QA



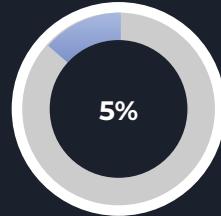
Knowledge in own
subject area



The need for a development and
testing bench



General knowledge in
Kubernetes and Docker

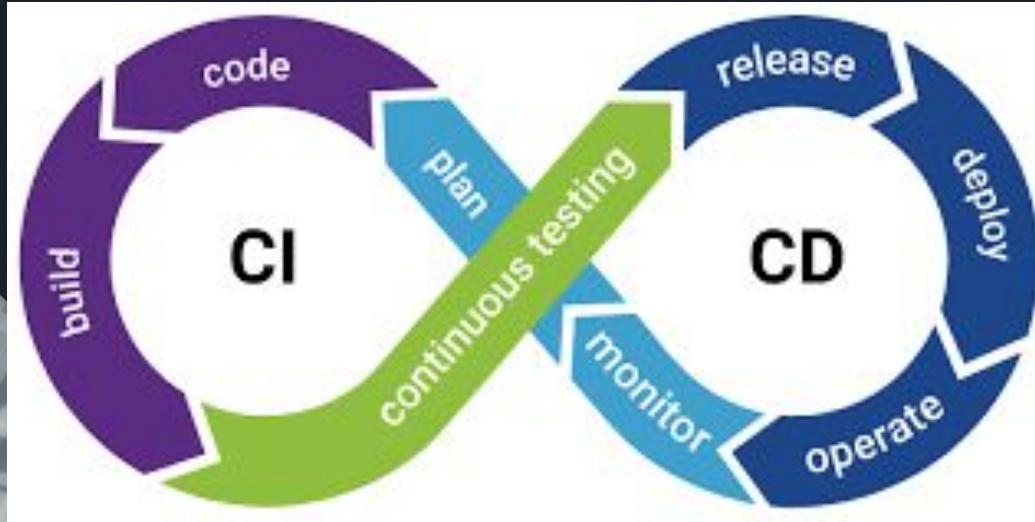


General Knowledge in Linux
Administration





What is CI/CD?

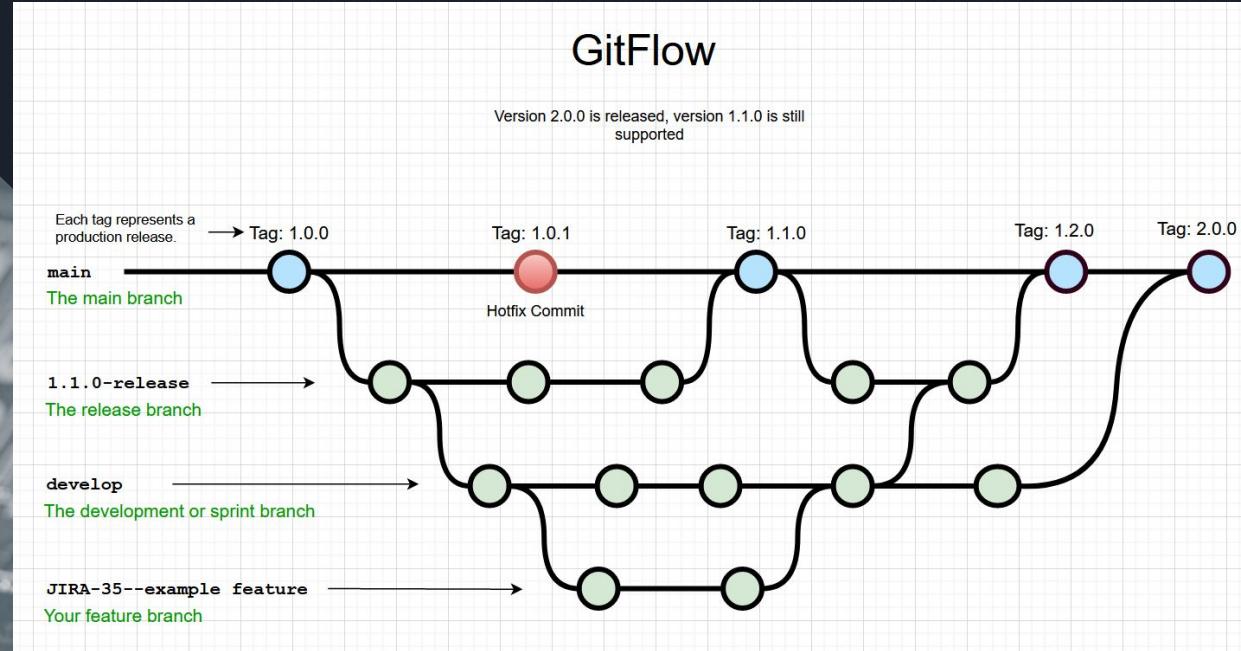


In software development, CI/CD is a combination of continuous integration and continuous software deployment in the development process with a high level of automation. CI/CD integrates the development, testing and deployment of an application. Nowadays, DevOps programmers tend to use CI / CD for almost all tasks.



Gitflow

(one of the options)



GitFlow is a Git branching model that uses feature branches and multiple master branches. Under this model, developers create a feature branch and defer merging it into the main trunk until the feature is complete.



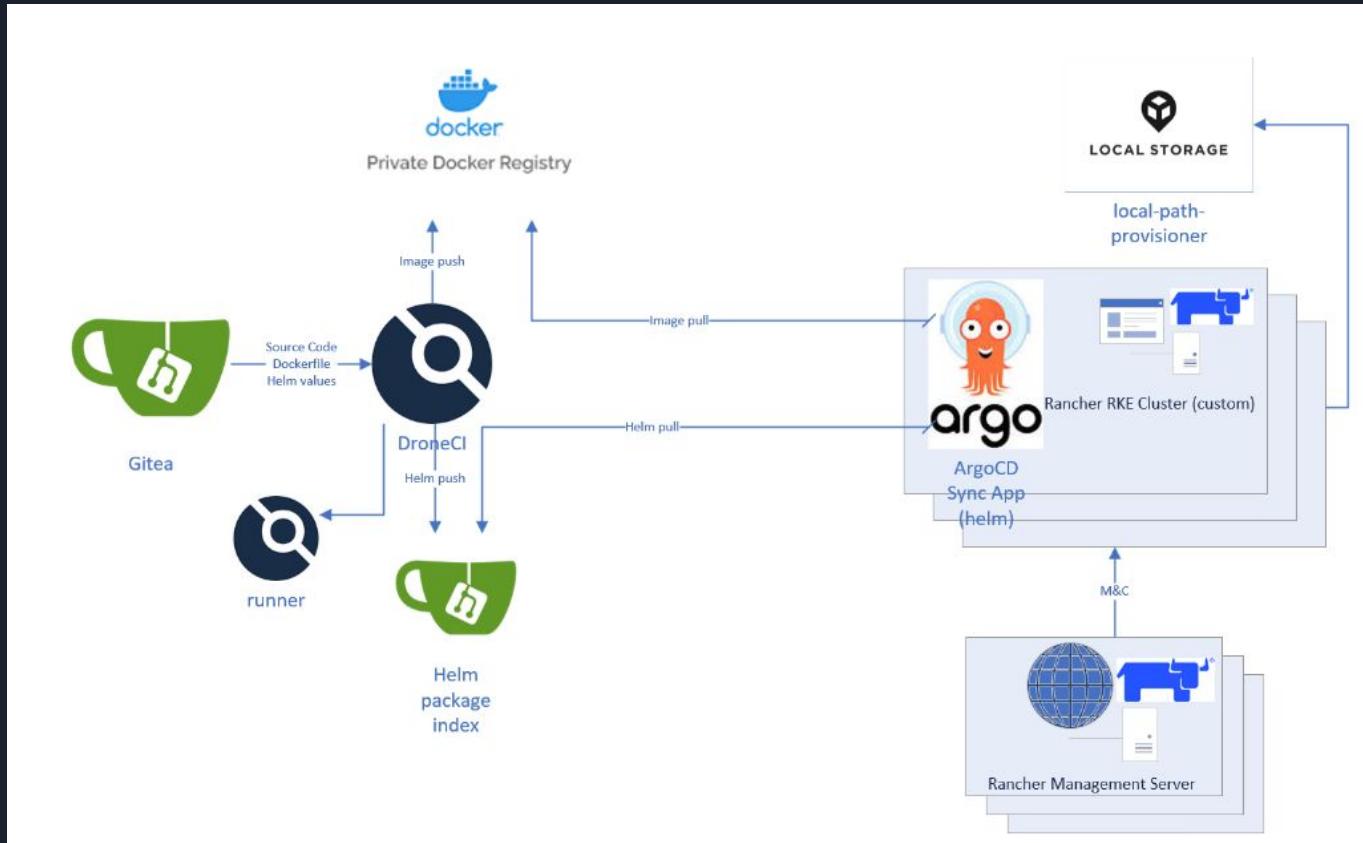
Infrastructure requirements

To generate a stand you will need:

- at least 4 physical CPU cores and 24 GB of RAM for a Kubernetes cluster node
- Rancher Desktop for Management Server (on a laptop)
- router with DNAT and VPN capability
- real IP address on the cluster node
- domain name and DNS provider.

All software used in the stack is open source, free of charge and can be obtained in the process of generating a stand via the Internet.

CI/CD scheme (simplified)



Booth infrastructure

Rancher Desktop (для М&С)

Rancher RKE1 Cluster

Cluster Dashboard

Provider: RKE1 Kubernetes Version: v1.25.9 Created: 22 days ago [Install Monitoring](#) [Edit Cluster Badge](#)

313	Total Resources
1	Node
32	Deployments

Capacity

Pods Used: 55 / 250 22.00%	CPU Reserved: 1.09 / 8 cores 13.63% Used: 1.39 / 8 cores 17.38%	Memory Reserved: 1.4 / 23 GiB 6.09% Used: 13 / 23 GiB 56.52%
----------------------------------------	----------------------------------------------------------------------------------	-------------------------------------------------------------------------------

[Etcd](#) [Scheduler](#) [Controller Manager](#)

Rancher Desktop

Rancher

Welcome to Rancher Desktop

Rancher Desktop provides Kubernetes and image management through the use of a central dashboard.

- Project Discussions: #rancher-desktop in Rancher Users Slack
- Project Links: Homepage Issues

Version: 1.8.1

Allow collection of anonymous statistics to help us improve Rancher Desktop. Send anonymized usage info, error reports, etc. to help improve Rancher Desktop. Your data is only used to help us improve Rancher Desktop and is not shared with anyone else, and no information about what specific resources or endpoints you are deploying is collected.

Network status: online

Cluster

Workloads

- CronJobs: 0
- DaemonSets: 1
- Deployments: 13
- Jobs: 0
- StatefulSets: 0
- Pods: 14

Apps

Service Discovery

Storage

Policy

More Resources

Cluster Tools

All Namespaces

Namespace: cattle-fleet-system

fleet-controller-686c7dcfcf-wjokc	rancher/fleet:v0.6.0	1/1
gitjob-79f557d76fb467	rancher/gitjob:v0.1.37	1/1

Namespace: cattle-system

rancher-769656fb94-rcm7t	rancher/rancherv2.7.3	1/1
rancher-webhook-7d5f881677-5vjq	rancher/rancher-webhook:v0.3.3	1/1

Namespace: cattle-ui-plugin-system

Tools

Gitea - management source code

The screenshot shows the Gitea web interface. At the top, there's a navigation bar with links for 'Задачи', 'Запросы на слияние', 'Этапы', and 'Обзор'. The main header says 'my-project' with a 'Privatnyy' button. Below the header, there are tabs for 'Репозитории', 'Проекты', 'Пакеты', 'Участники', 'Команды', and 'Настройки'. A search bar with 'Поиск...' placeholder and a 'Поиск' button is present. On the left, there's a sidebar with 'Новый репозиторий' and 'Новая миграция' buttons. The main content area displays three repository cards:

- my-project-php** [Privatnyy]
site
Обновлено 45 минут назад
- my-project-helm** [Privatnyy]
my-project-helm
Обновлено 5 дней назад
- apache-bullseye-base** [Privatnyy]
Обновлено 2 недели назад

On the right side, there are two sections: 'Участники' (Participants) and 'Команды' (Teams). The 'Участники' section shows one participant with a profile picture and the name 'Owners'. The 'Команды' section shows one team with the name 'Owners' and '1 Участники · 3 Репозитории'. There's also a 'Создание команды' (Create team) button.

Gitea is a Git-based IT project hosting and collaborative development software. Supports bug tracking, wiki and code review. Gitea supports self-hosting, but there is also a free service. Wikipedia

Programming languages: Go, JavaScript

License: MIT license

Written in: Go and JavaScript

Website: gitea.io

Tools

Drone CI - build,
testing and publication
artifacts

The screenshot shows the Drone CI dashboard with a dark theme. On the left, there's a sidebar with icons for Dashboard, Recent Activity, and Repositories. The main area has a header "Dashboard" and a "SYNC" button. Below it is a section titled "RECENT ACTIVITY" with three items:

- 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...>. 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 this is a "REPOSITORIES" section with three entries:

- my-project/my-project-php: ed0521e6 Merge pull request 'stage' (#15) from stage into main. Reviewed-on: <https://git.simshp.ru/my-pro...>. 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.

At the bottom of the dashboard, there are filters: Active Only, Sort by Recent activity, All Organizations, and a Filter input field.

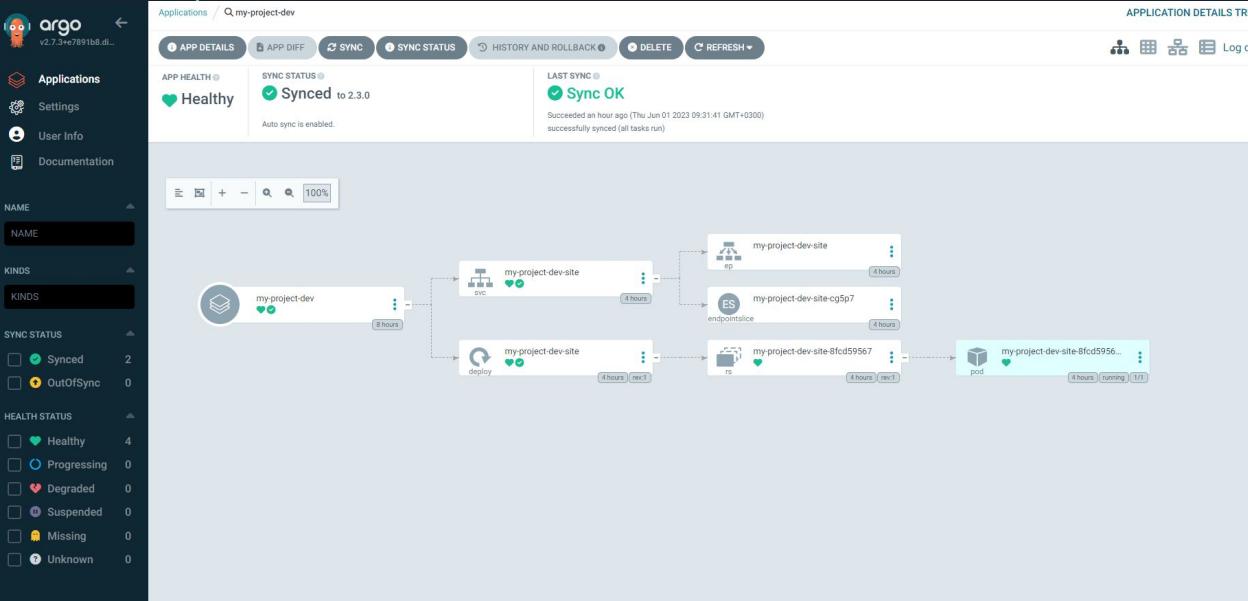
Software build and test automation

Drone is a self-service continuous integration platform for development teams.

Website: drone.io

Tools

Argo CD- application delivery to Kubernetes clusters



Argo CD is a declarative GitOps continuous delivery tool for Kubernetes.

Definitions, configurations, and application environments should be declarative and versioned. Application deployment and lifecycle management should be automated, auditable, and easy to understand.

Website: argo-cd.readthedocs.io



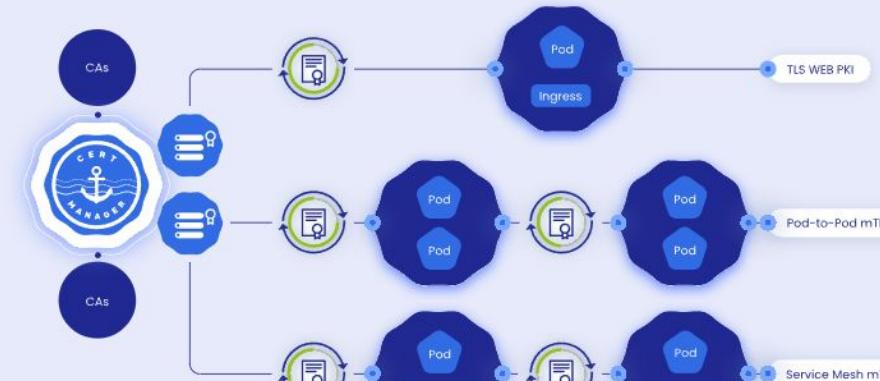
Related programs

cert-manager

Cloud native certificate management

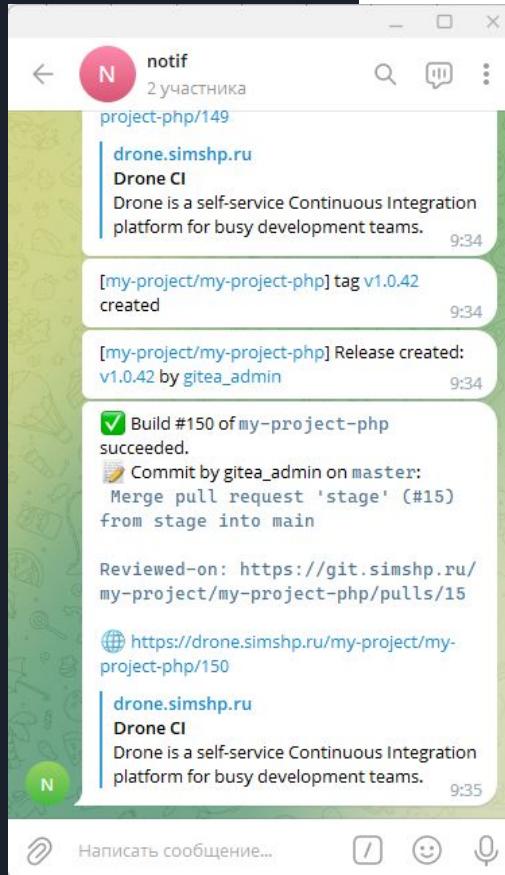
X.509 certificate management for
Kubernetes and OpenShift

Certificate Management for
Kubernetes



Telegram

Related programs



CI/CD Event Notifications



Argo Rollouts - Kubernetes Progressive Delivery Controller

Related programs
(after finalizing the helm-chart)

Canary deployments and A/B
testing

The screenshot shows the Argo Rollouts UI interface. At the top, there's a navigation bar with a logo, a search bar, and status indicators for the namespace (NS: rollouts-demo) and version (v1.0.0+75eeb71.dirty). Below the navigation bar, there are three main sections, each representing a different deployment strategy:

- bluegreen-demo**: Strategy: BlueGreen. It shows a revision (bluegreen-demo-6cbcccd9f99) with a weight of 100% (3 green checkmarks) and a revision (bluegreen-demo-6cbcccd9f99) with a weight of 0% (grey box). Buttons for "RESTART" and "PROMOTE-FULL" are present.
- canary-demo**: Strategy: Canary. It shows a revision (canary-demo-68f96454b6) with a weight of 20% (1 green checkmark) and a revision (canary-demo-645d5dbc4c) with a weight of 80% (4 green checkmarks). Buttons for "RESTART" and "PROMOTE-FULL" are present.
- rollouts-demo**: Strategy: Canary. It shows a revision (rollouts-demo-7bf84f9696) with a weight of 80% (4 green checkmarks) and a revision (rollouts-demo-789746c88d) with a weight of 20% (1 green checkmark). Buttons for "RESTART" and "PROMOTE-FULL" are present.



Related programs

Helm

package manager
for Kubernetes

Helm is the best way to
discover, share, and use
software built for Kubernetes.





Related programs
(infrastructure component)

MetalLB

MetalLB is a bare metal implementation of a load balancer for Kubernetes clusters using standard routing protocols.

MetalLB is installed on a Kubernetes cluster and provides a network load balancer implementation. In short, it allows you to create LoadBalancer-type Kubernetes services on clusters that don't run on a cloud provider, and therefore can't just connect to paid products to provide load balancers.



Companion programs for the cluster

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

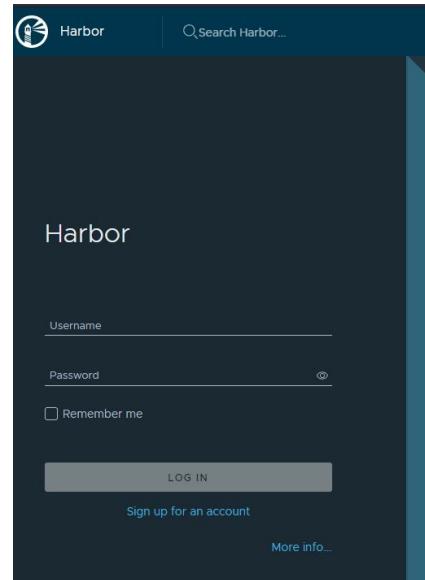


Stack Upgrades

Harbor (instead of registry)

Harbor is an open source registry that secures artifacts with policy and role-based access control, ensures image scanning and security, and image signing.

Harbor, a CNCF graduate project, provides compliance, performance, and interoperability to help you manage artifacts consistently and securely across native cloud computing platforms such as Kubernetes and Docker.





Stack Upgrades

SonarQube

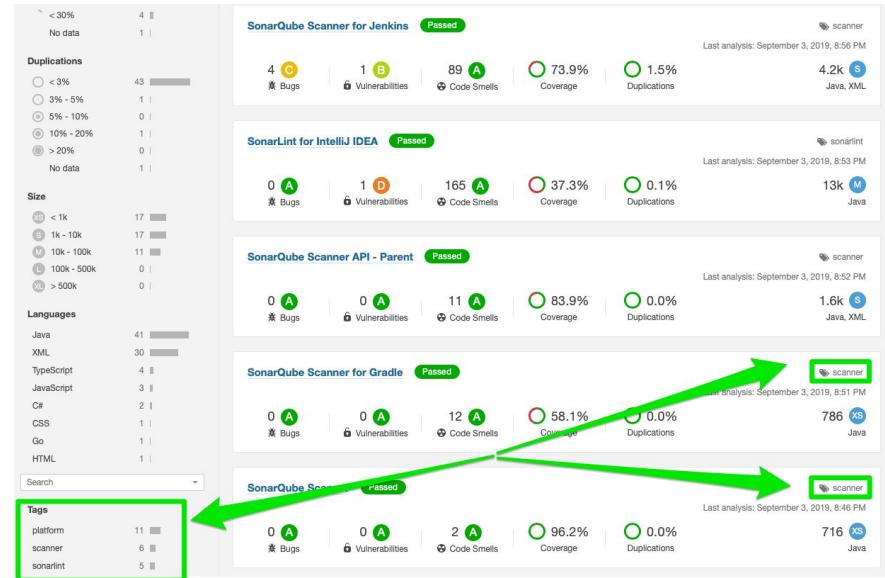
SonarQube is an open source platform for continuous analysis and measurement of code quality. Supports code analysis and error detection according to the rules of programming standards.

Programming language: Java

License: GNU LGPLv3

Operating system: Cross-platform

Latest version: 9.4





Stack Upgrades

Vault

Manage Secrets and Protect
Sensitive Data with Vault

Protect, store and control access to
tokens, passwords, certificates,
encryption keys and other sensitive data
using the user interface, CLI or HTTP API

Ability to integrate with all CI/CD stack tools



Demo

Questions?

Thank you!
Minimalist CI/CD stack

Application | my-project-dev

APP DETAILS | APP DIFF | SYNC | SYNC STATUS | HISTORY AND ROLLBACK | DELETE | REFRESH

APP HEALTH | Healthy

SYNC STATUS | Synced to 2.3.0 | Sync OK | LAST SYNC | Succeeded 2 hours ago (Thu Jan 01 2023 09:31:41 GMT+0000) successfully synced (all tasks run)

Auto sync is enabled.

APPLICATION

```
graph LR; A[my-project-dev] --> B[my-project-dev-site]; B --> C[my-project-dev-site-clone]; C --> D[my-project-dev-site-deploy]
```

