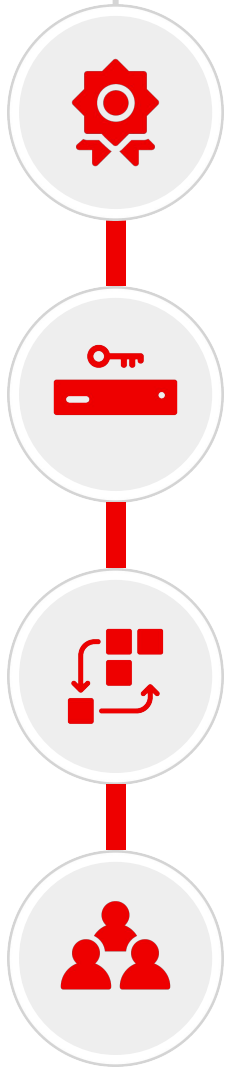
Red Hat Quay

RED HAT QUAY

Secure Enterprise Registry

Red Hat

Red Hat Quay



Industry-leading, **trusted, and open source registry platform** operating at scale since 2014

Built to **efficiently manage content** under governance and security **controls** globally

Runs **everywhere**, easy to **integrate** and **automate** but works best with **OpenShift**

Developed in **collaboration** with a broad open source, customer, and ecosystem **community**

Red Hat Quay Key Features

SCALABILITY

Massive Scale Testing Quay.io
Real Time Garbage Collection
Automated Squashing

BUILD AUTOMATION

Seamless Git Integration
Build Workers
Webhooks

INTEGRATION

Extensible API
Webhooks, OAuth
Robot Accounts

REGISTRY

High Availability
Full Standards / Spec Support
Long-Term Protocol Support
Application Registry
Enterprise Grade Support
Regular Updates

SECURITY

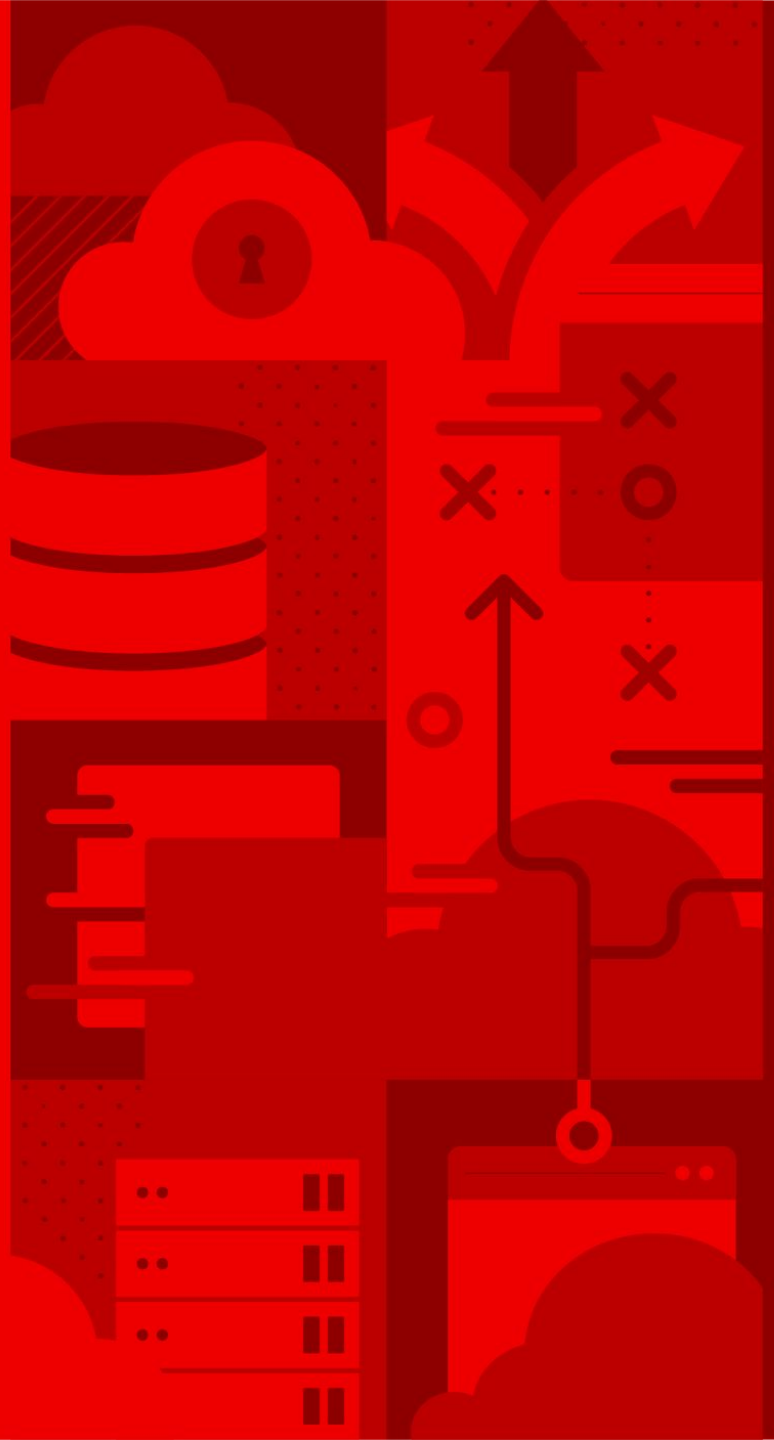
Vulnerability Scanning
Logging & Auditing
Notifications & Alerting

CONTENT DISTRIBUTION

Geo-Replication
Repository Mirroring
Air-Gapped Environments

ACCESS CONTROL

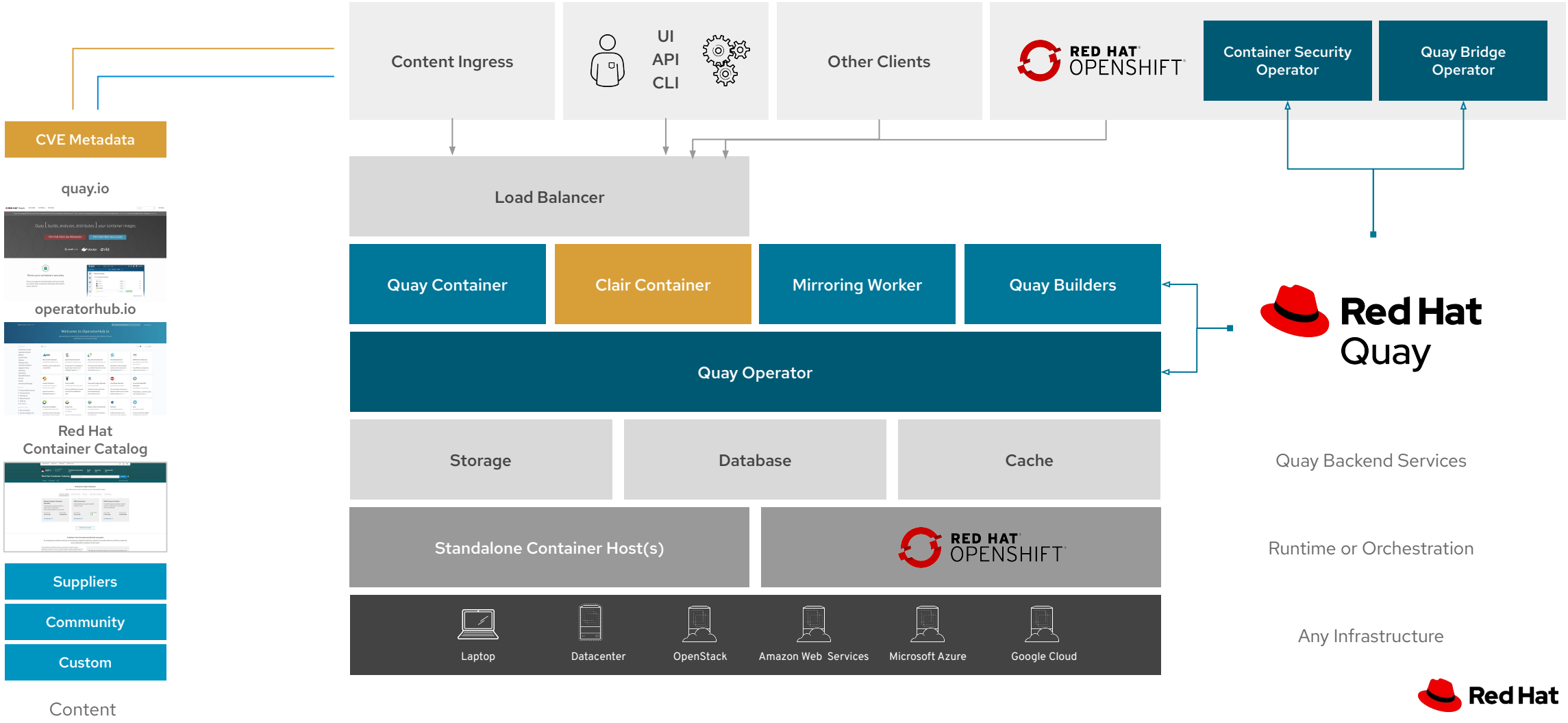
Authentication Providers
Fine-Grained RBAC
Organizations & Teams



Quay Architecture

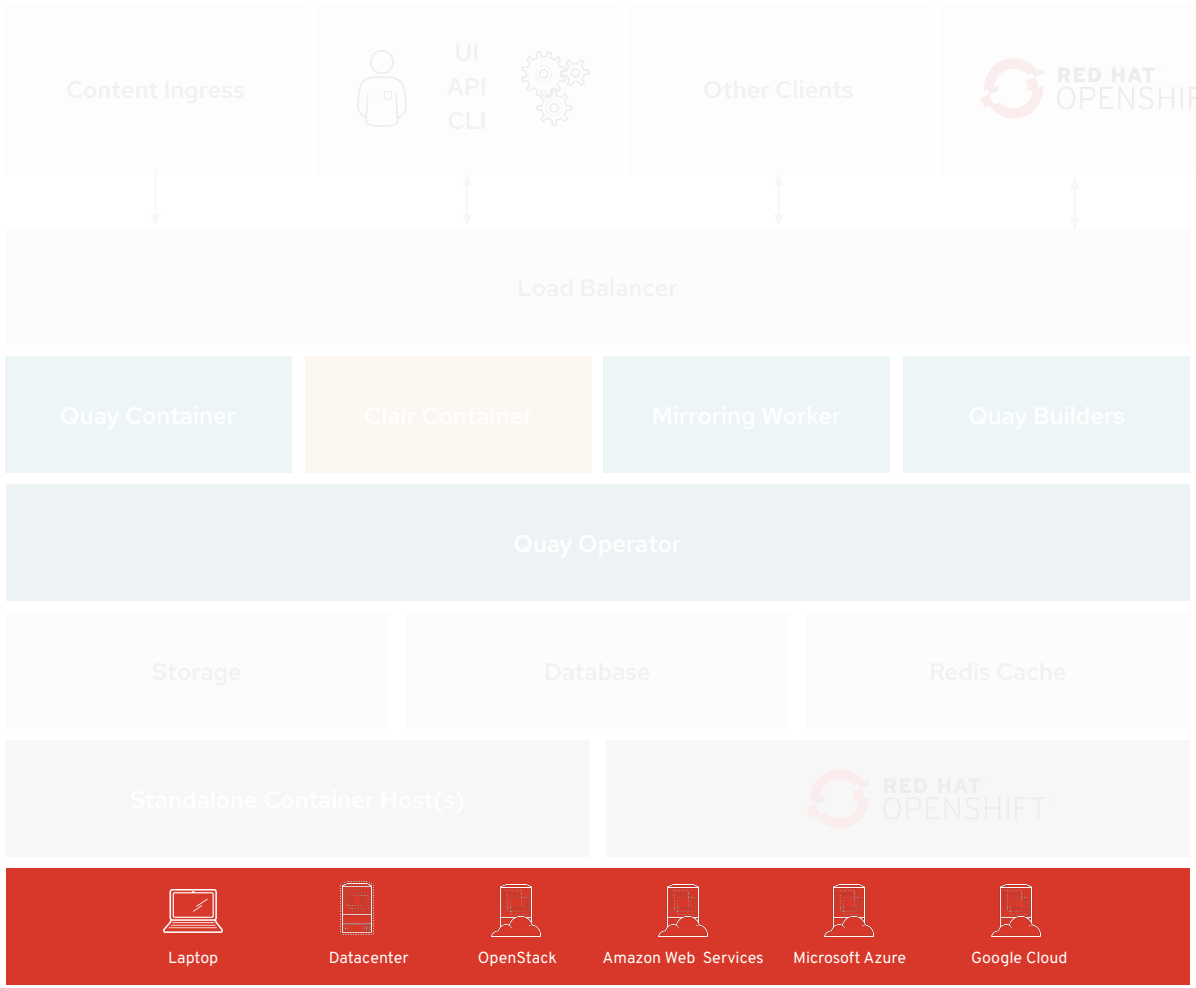
Red Hat

Red Hat Quay Architecture



Red Hat

Prerequisite: Infrastructure



Quay runs on any* physical or virtual infrastructure both on-premise or public cloud**

Quay scales from an all-in-one setup on a developer laptop over running highly available on OpenShift up to geographically dispersed setup across multiple availability zones and regions

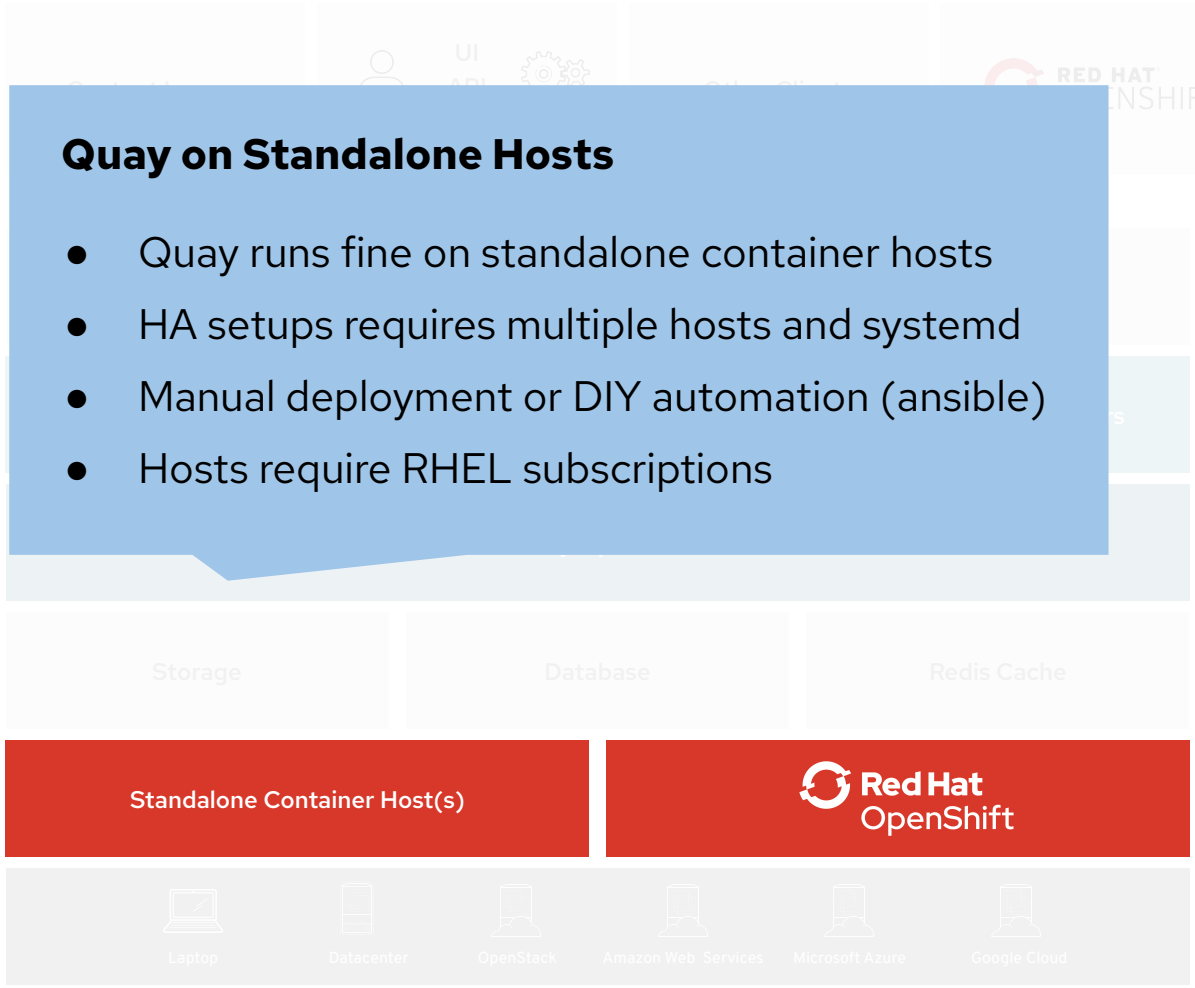
Recommendation: if Quay runs on public cloud -> use the public cloud services for Quay backend services to ensure proper HA and scalability

* Further details can be found in the Quay 3.x tested configuration matrix: https://access.redhat.com/articles/4067991

** Further details can be found in the Quay Support Policy: https://access.redhat.com/support/policy/updates/rhquay/policies

Red Hat

Prerequisite: Container Runtime or Orchestration



Quay on Standalone Hosts

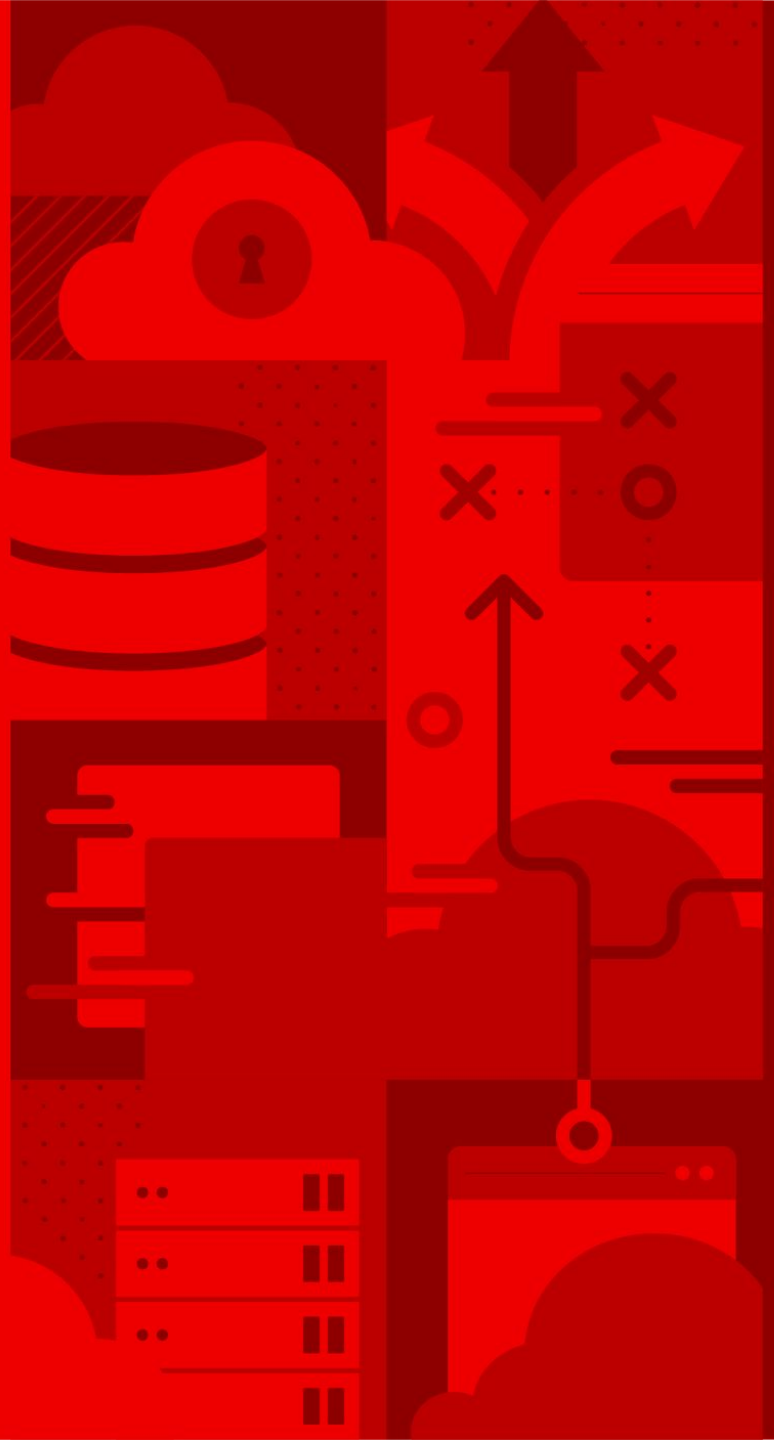
- Quay runs fine on standalone container hosts
- HA setups requires multiple hosts and systemd
- Manual deployment or DIY automation (ansible)
- Hosts require RHEL subscriptions

Benefits of running Quay on OpenShift:

- Run Quay where you run all other container workloads and services
- Seamless deployment and day2 management of Red Hat Quay via the Quay operator and OLM
- Leverage all orchestration and management capabilities of Red Hat OpenShift incl. Operator Lifecycle Mgt (OLM), monitoring, dashboards, ...
- Quay can run on OpenShift infra nodes (no further subscriptions required)

Full list of tested and supported configurations can be found inside the Red Hat Quay Tested Integrations Matrix: https://access.redhat.com/articles/4067991

Red Hat



Quay and OpenShift

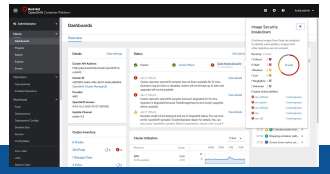
Red Hat

Red Hat Quay works best with OpenShift

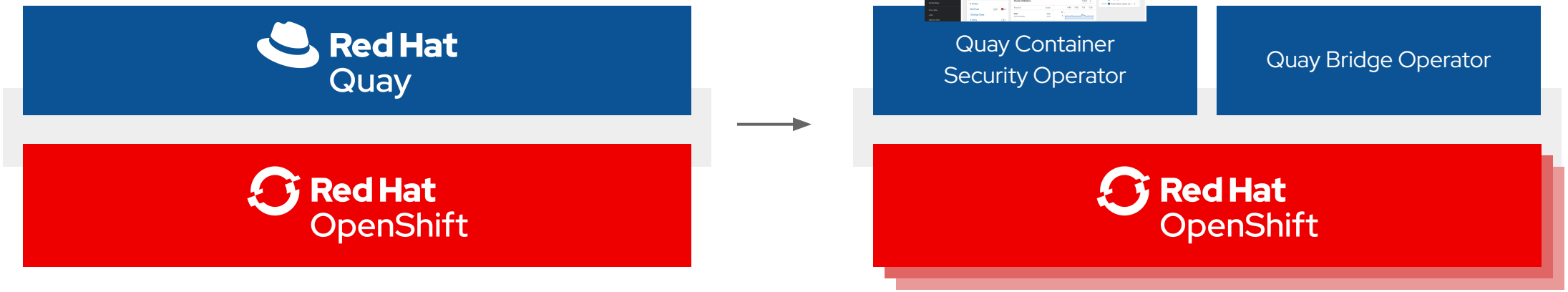
Red Hat Quay runs on any infrastructure but **runs best on OpenShift**

The **Quay Operator** ensures seamless deployment and management of Quay running on OpenShift

CSO brings Quay / Clair vulnerability data into the OpenShift Console



The **Quay Bridge Operator** ensures seamless integration and user experience for using Quay **with** OpenShift



Quay serves content to **one or many OpenShift clusters**, wherever they're running.

With or without using the OpenShift internal registry but leveraging all OpenShift capabilities.

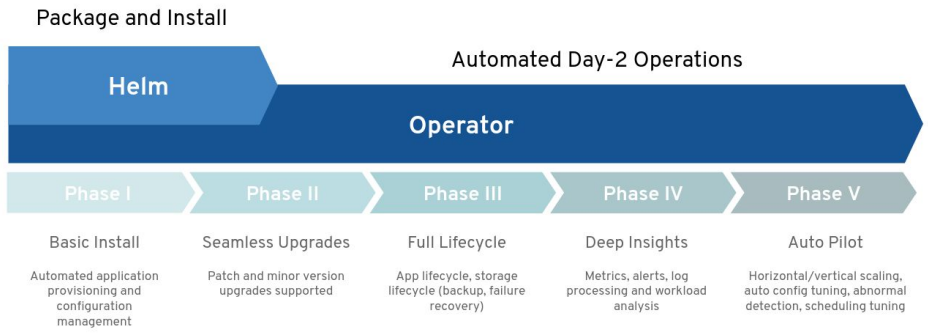
Red Hat

Benefits of running Quay on OpenShift

- **Zero to Hero** - Simplified deployment of Quay and associated components means that you can starting using the product immediately
- **Scalability -** Leverage cluster compute capacity to manage expected demand
- **Simplified Networking** - Diverse ingress options using well established patterns for any application deployed on the platform
- **Centralized configuration management** - Configurations stored in etcd provide a centralized source of truth
- **Repeatability** - Consistency regardless of the number of replicas of Quay / Clair
- **Expanded Options** - Additional solutions that are specifically designed to take advantage of an OpenShift deployment

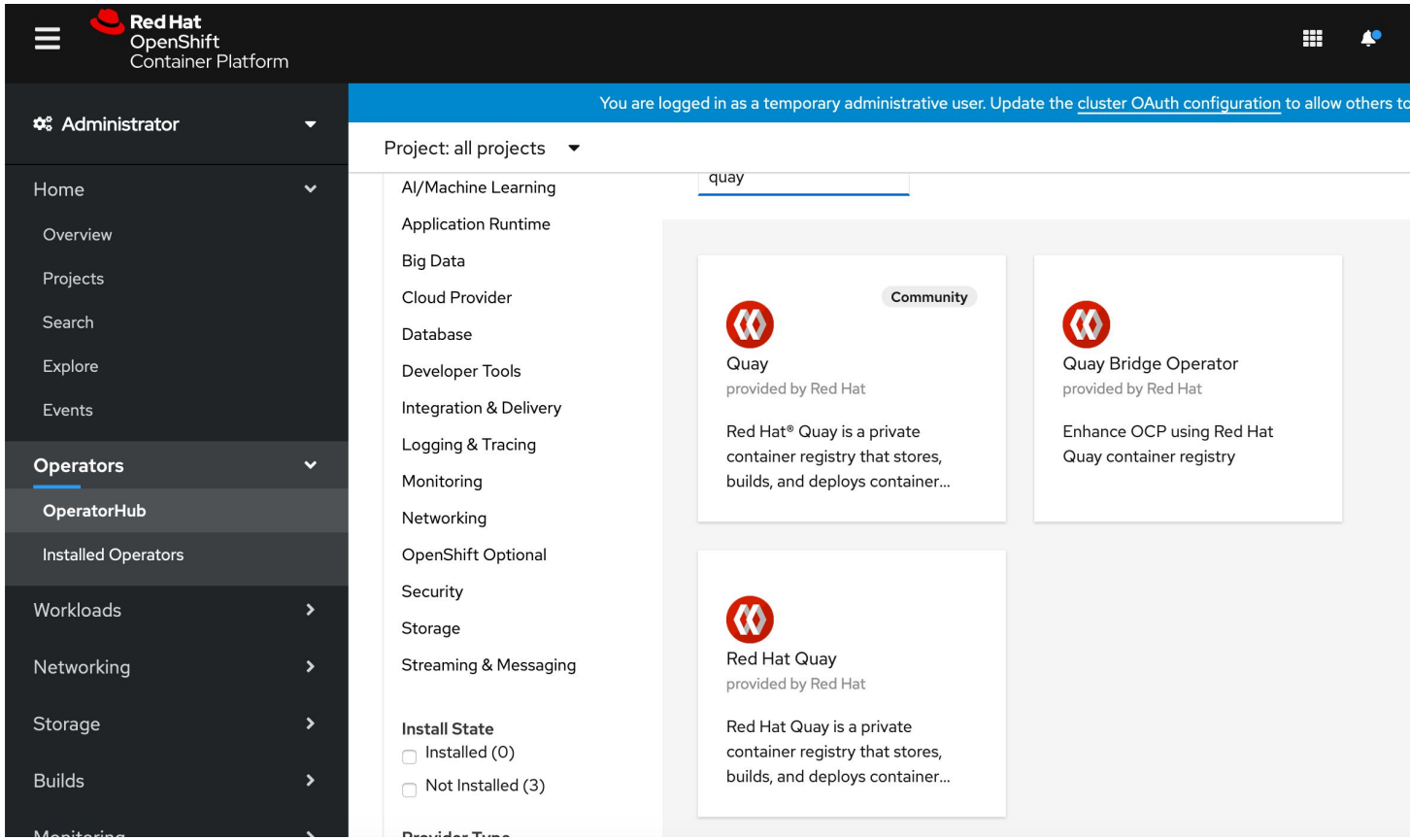
Red Hat

Quay - Focus on Operators



Focus and direction for the Quay product are kubernetes operators and running Quay on OpenShift / kubernetes given the advantages of operators compared with its alternatives

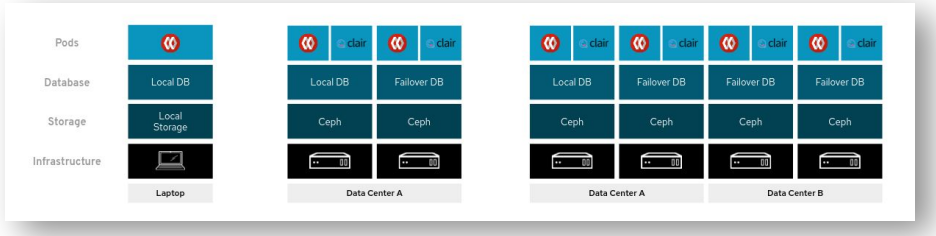
Maintaining another deployment and management tooling for non-k8s deployments is not feasible and not aligned to our prioritization and roadmap (Quay v4 will run on k8s by default)

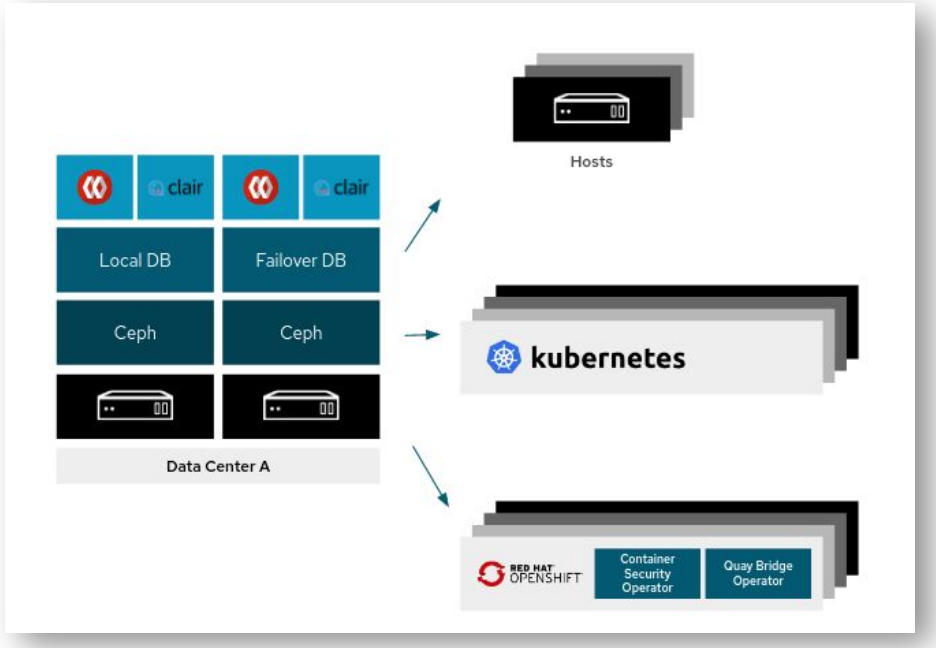


Red Hat

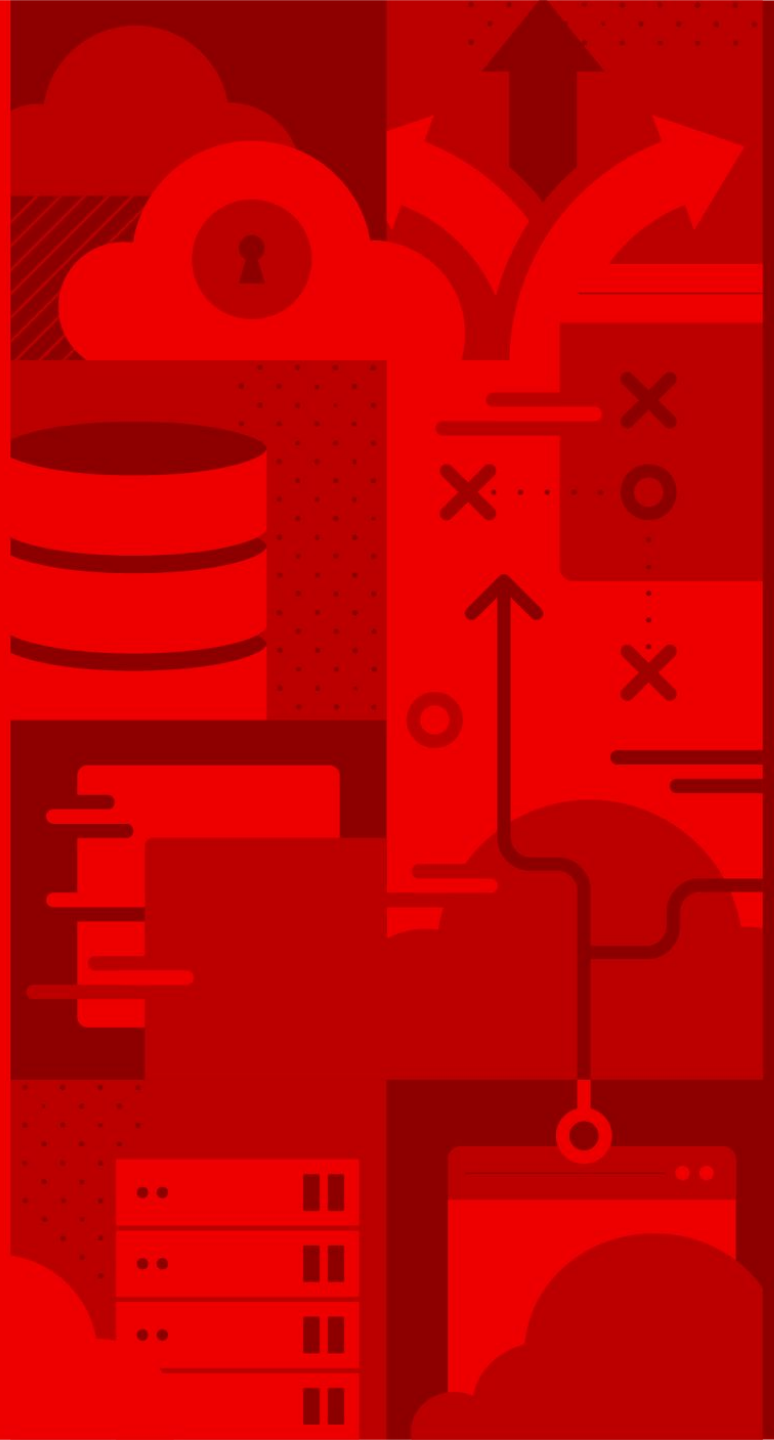
Quay Deployment Examples

- Quay can run on standalone container hosts or OpenShift (recommended)
- A Quay deployment can be distributed across multiple DCs or even OCP clusters (geo-repl)
- Typically Quay is used for **more than one / many OpenShift clusters**
- Components which can run **on-cluster**: Quay, Clair, mirroring workers
- Components which should / must run **off cluster** (today): Quay builders, databases (if not an operator), storage





Red Hat

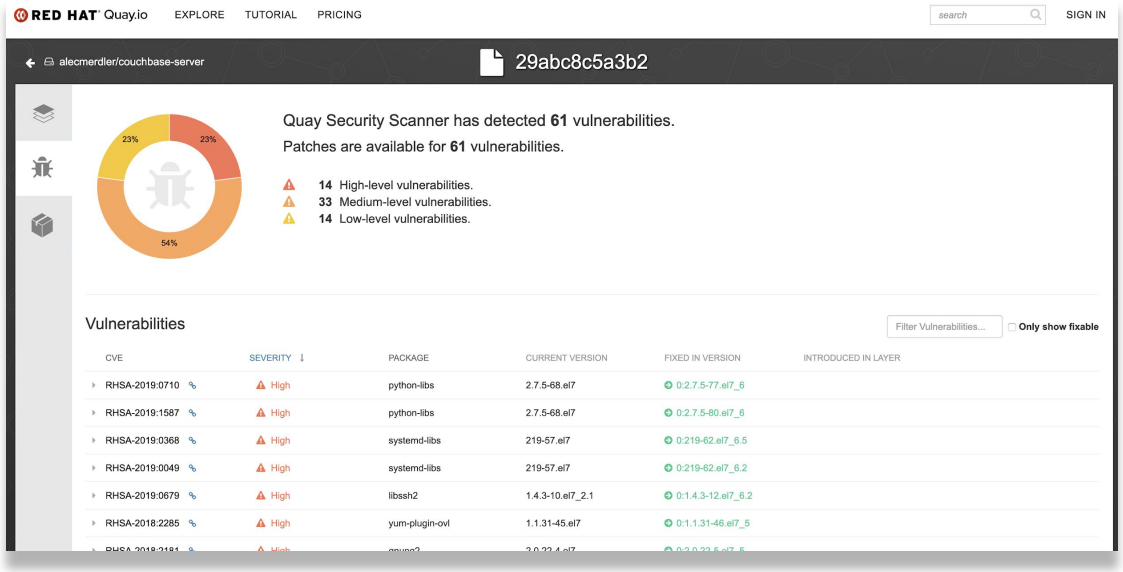


Built-In Vulnerability Scanning via Clair

Red Hat

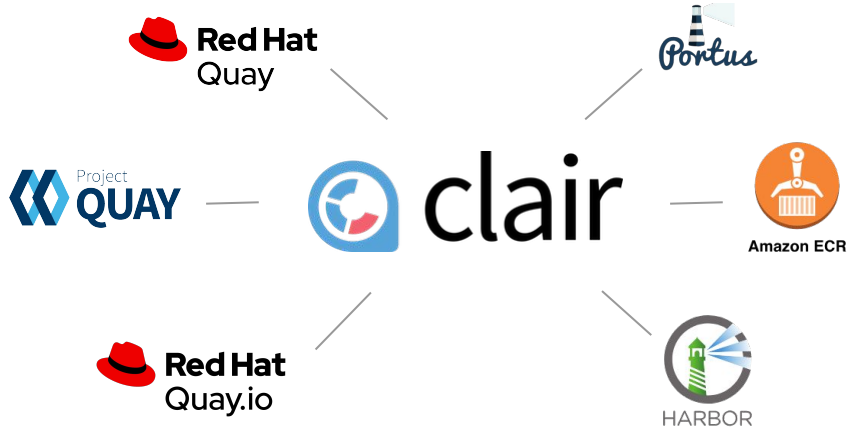
Clair Overview

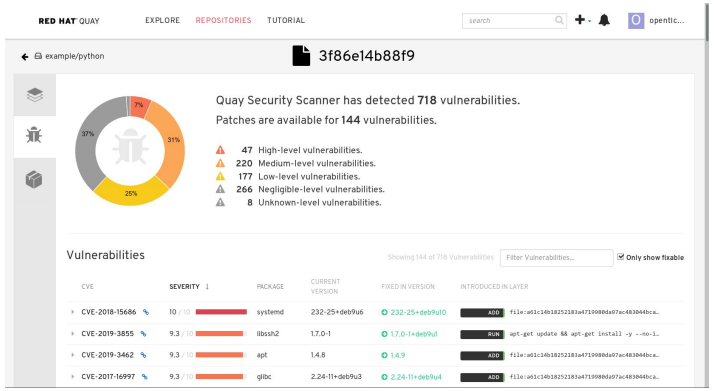
- Clair is an open source tool for static analysis of vulnerabilities in application containers
- Developed by CoreOS for Quay and it's massive scale usage at Quay.io
- Used by various other projects and third party products
- Upstream Repositories: https://github.com/quay/clair



Red Hat

clair v4





Clair v4 (Tech Preview with Quay 3.3)

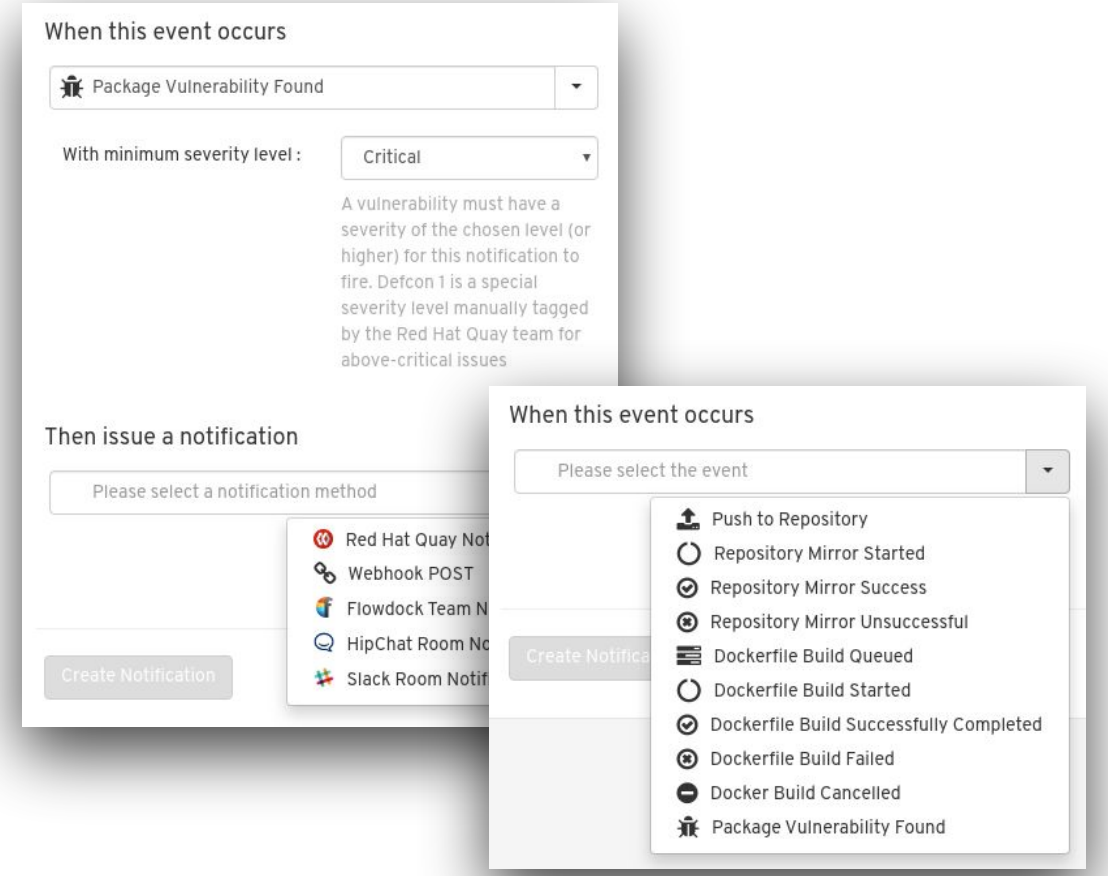
Clair v4 is the newest version of Clair after a massive refactoring in order to make several big enhancements possible. This includes:

- Support for programming language package managers (3.3: python)
- immutable data model & new manifest-oriented API
- Refocus on latest container specifications (OCI) (Content addressability)

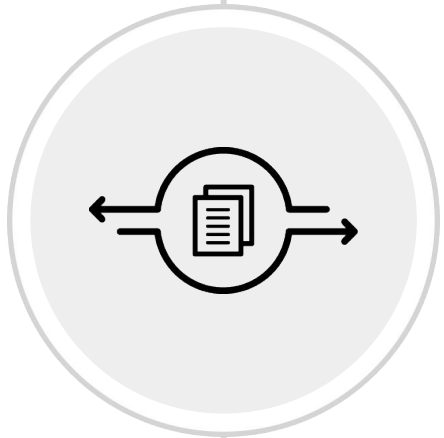
Red Hat

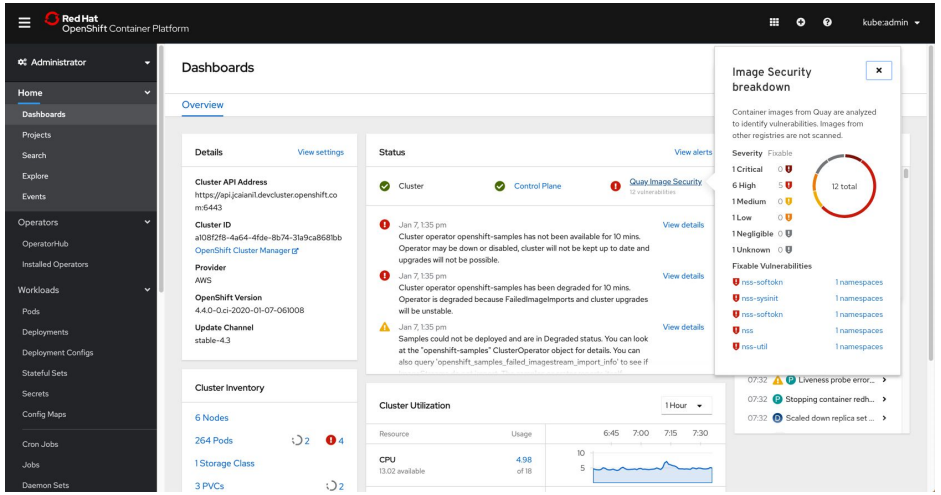
Notifications for Vulnerabilities found by Clair

- **Quay triggers different notifications for various repository events** (depends on enabled features)
- This includes the event type **“Package Vulnerability Found”**
- Additional Filter can be applied for **Severity Level**
- **Various Notification Methods**
- Custom Notification Title (optional)



Red Hat





RED HAT® QUAY

Scans images running on OpenShift and exposes data via API

clair

Red Hat OpenShift Container Platform

Operator monitors pod objects and updates vulnerability data

Container Security Operator - Vulnerability Data in OpenShift

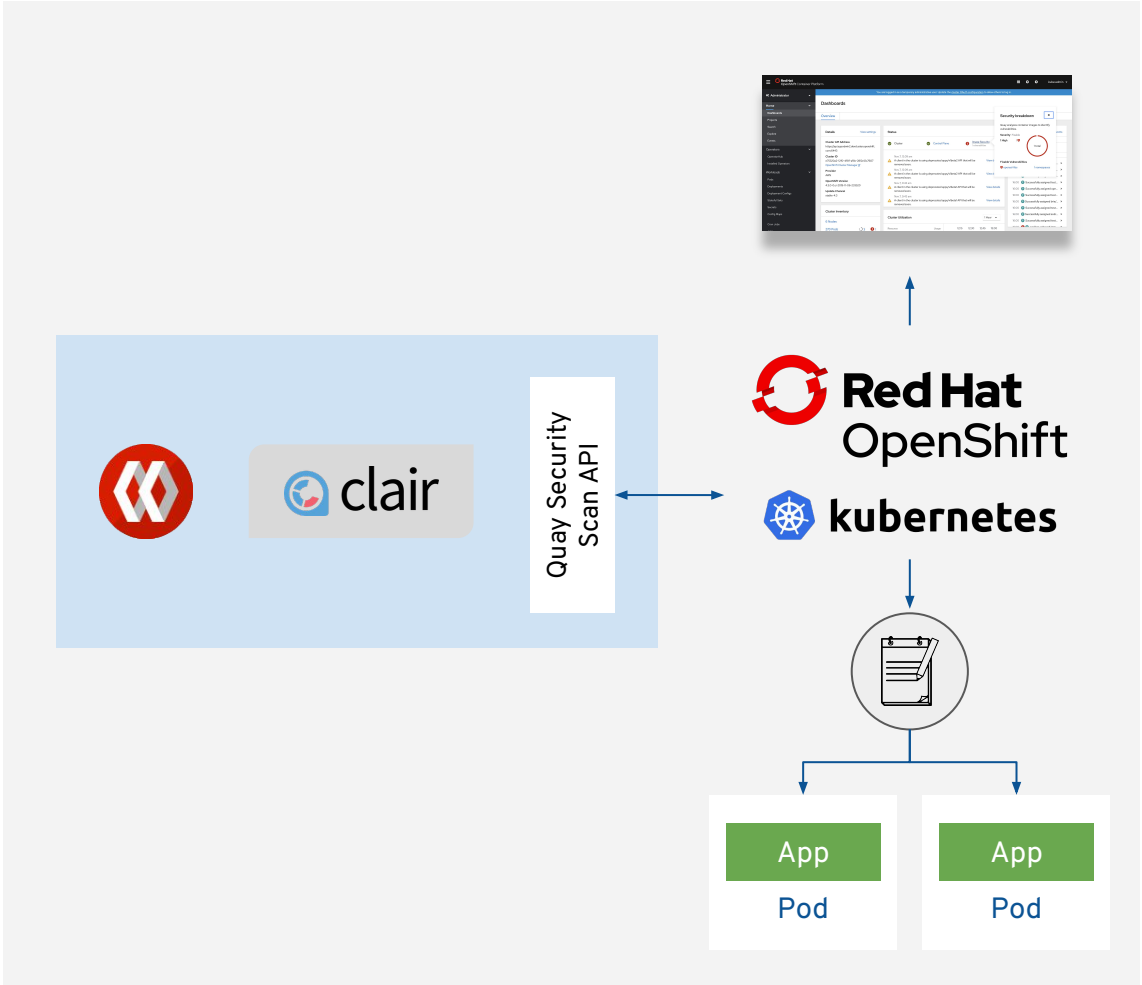
Operator which runs on OpenShift and fetches vulnerability from Quay / Clair if Kubernetes pod objects change

Synchronous Updates of vulnerability information

Prerequisite to leverage / show vulnerability data in OpenShift Console

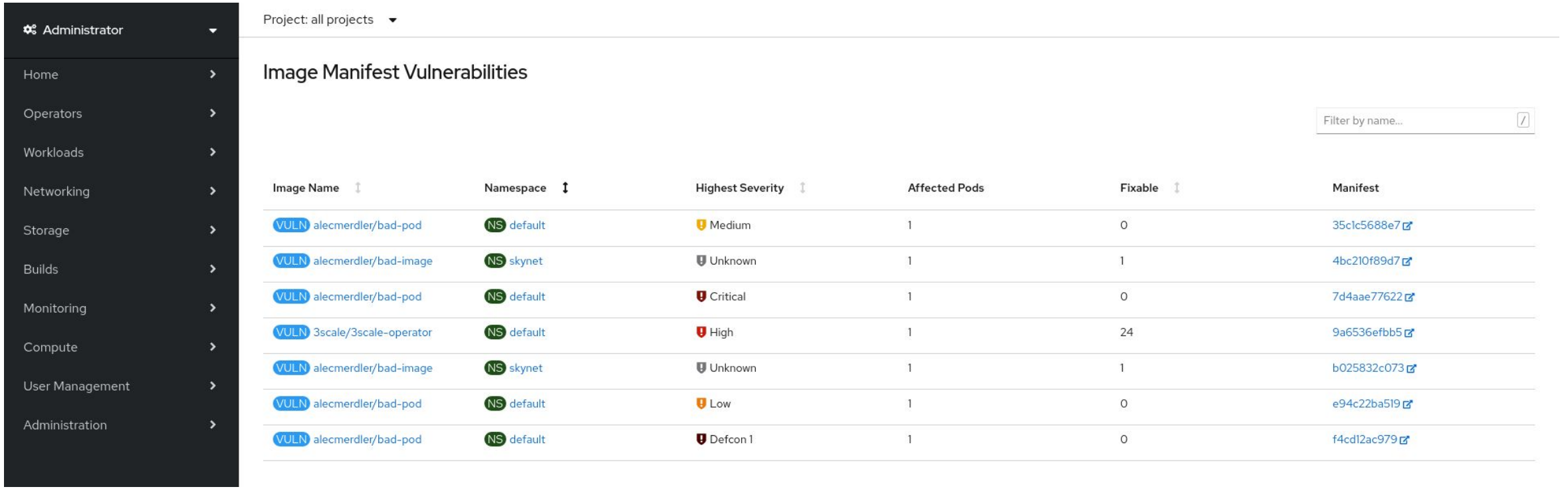
Red Hat

Container Security Operator (CSO)



- Container Security Operator (CSO) runs on OpenShift and watches pod objects
- Pod object changes triggering a data fetch from Quay/Clair and stores vulnerability information in CRs (by image manifest ID)
- CRs gets deleted if pod gets deleted
- Configurable interval to update vulnerability data from Quay / Clair (default: 5min)
- Data available via k8s CLI / APIs
- Supposed to be used by partner security products as well (consistent data ingress)

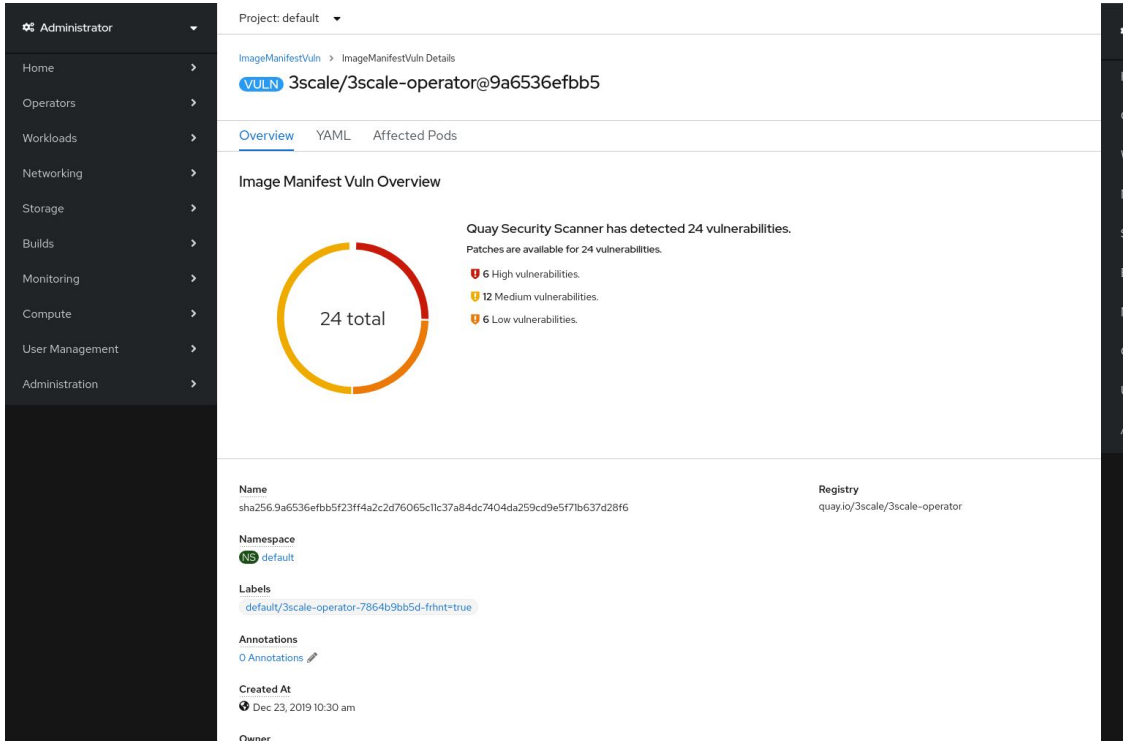
Vulnerability Data inside the OpenShift Console

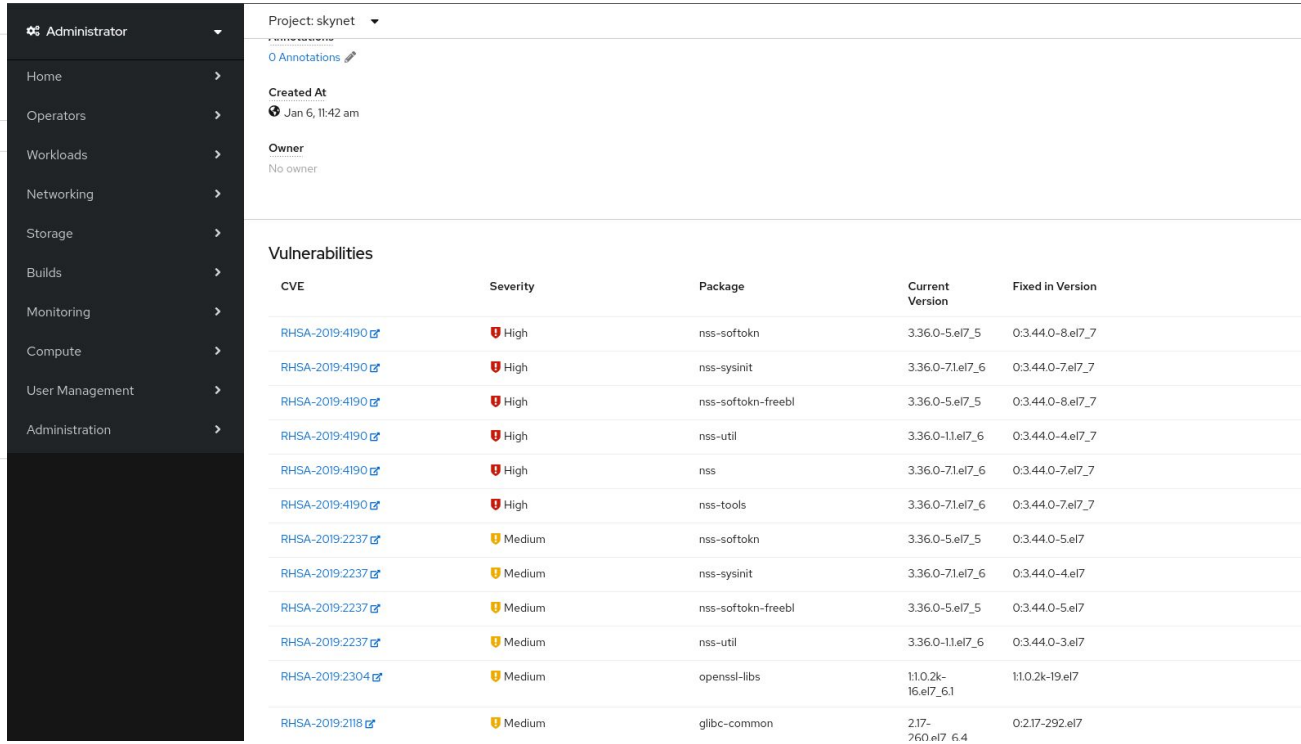


ImageManifestVuln list view

Red Hat

Vulnerability Data inside the OpenShift Console

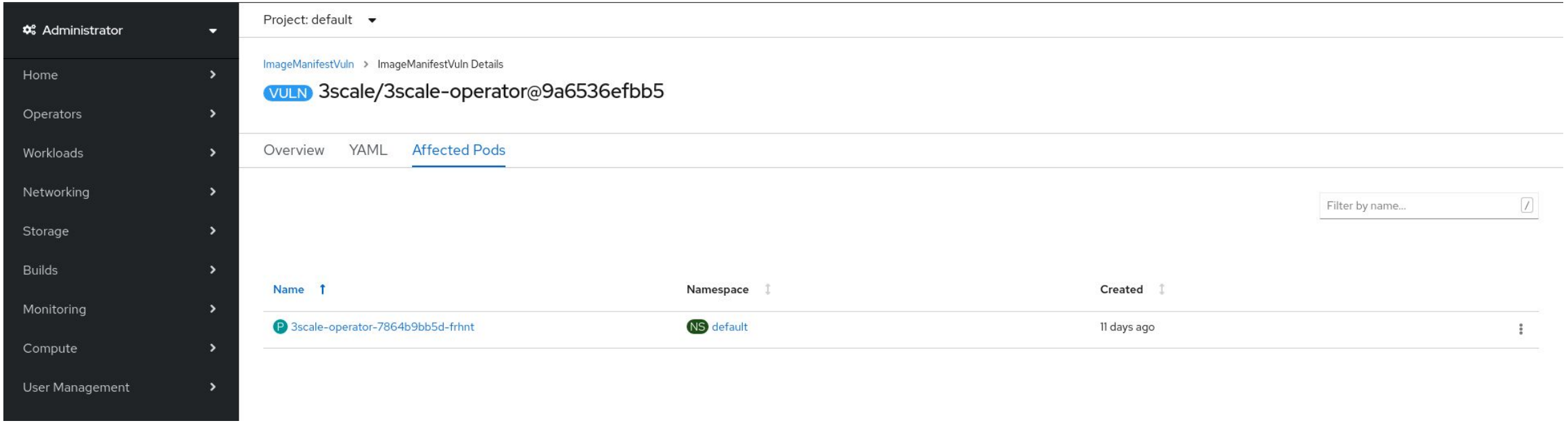




ImageManifestVuln detail view

Red Hat

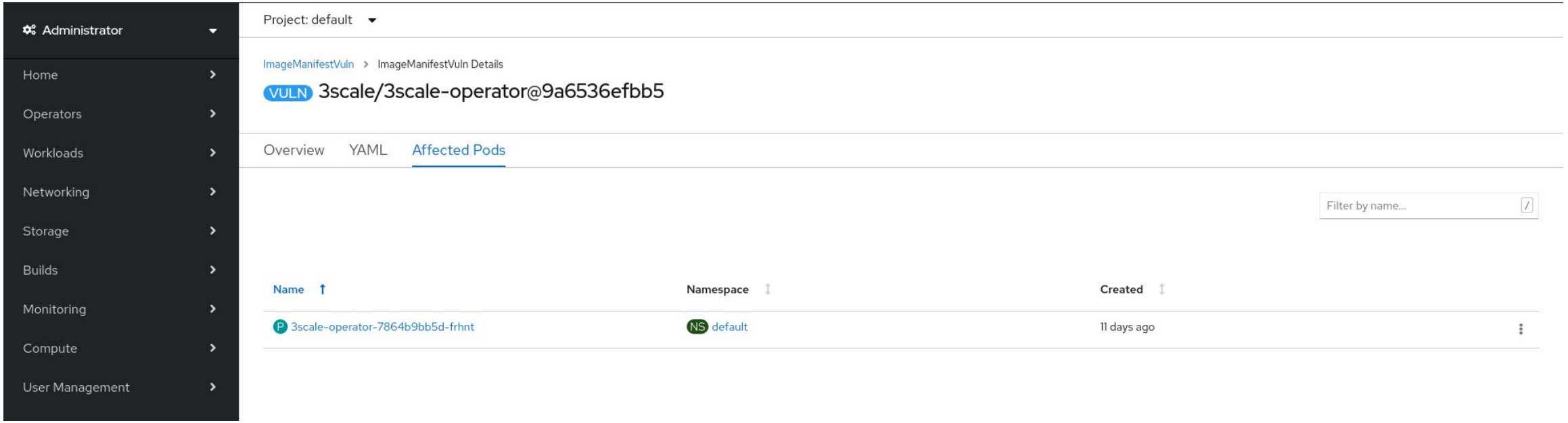
Vulnerability Data inside the OpenShift Console



ImageManifestVuln detail view (affected pods)

Red Hat

Vulnerability Data inside the OpenShift Console



Kebab action on Pods list view

Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat