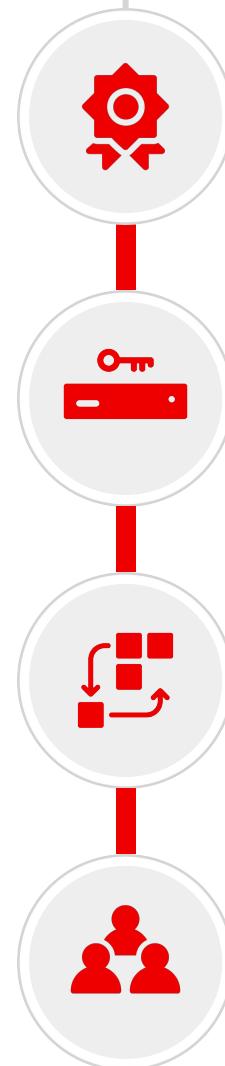




# RED HAT QUAY



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

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

## SCALABILITY

Seamless Git Integration  
Build Workers  
Webhooks

## BUILD AUTOMATION

Extensible API  
Webhooks, OAuth  
Robot Accounts

## INTEGRATION

Vulnerability Scanning  
Logging & Auditing  
Notifications & Alerting

## SECURITY

## REGISTRY

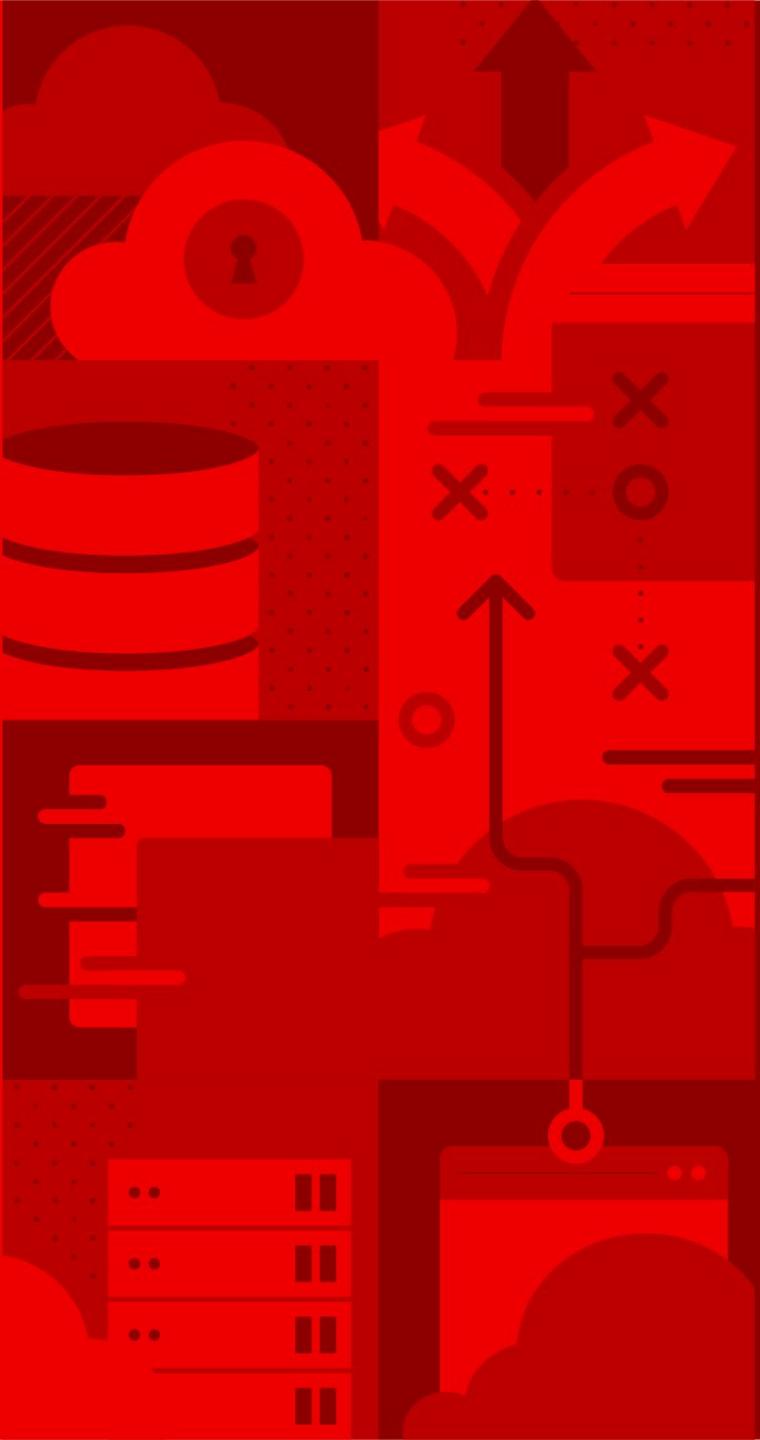
High Availability  
Full Standards / Spec Support  
Long-Term Protocol Support  
Application Registry  
Enterprise Grade Support  
Regular Updates

## CONTENT DISTRIBUTION

Geo-Replication  
Repository Mirroring  
Air-Gapped Environments

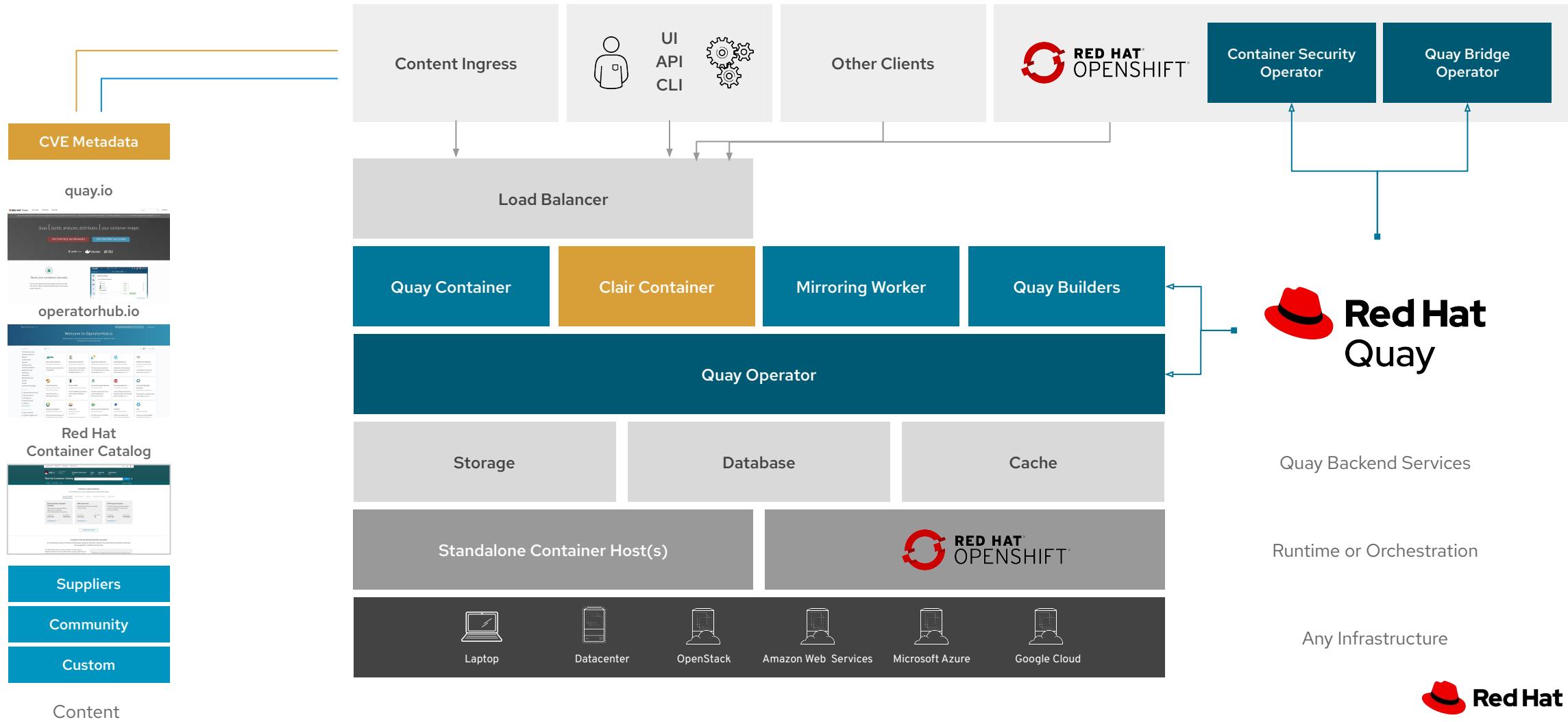
## ACCESS CONTROL

Authentication Providers  
Fine-Grained RBAC  
Organizations & Teams

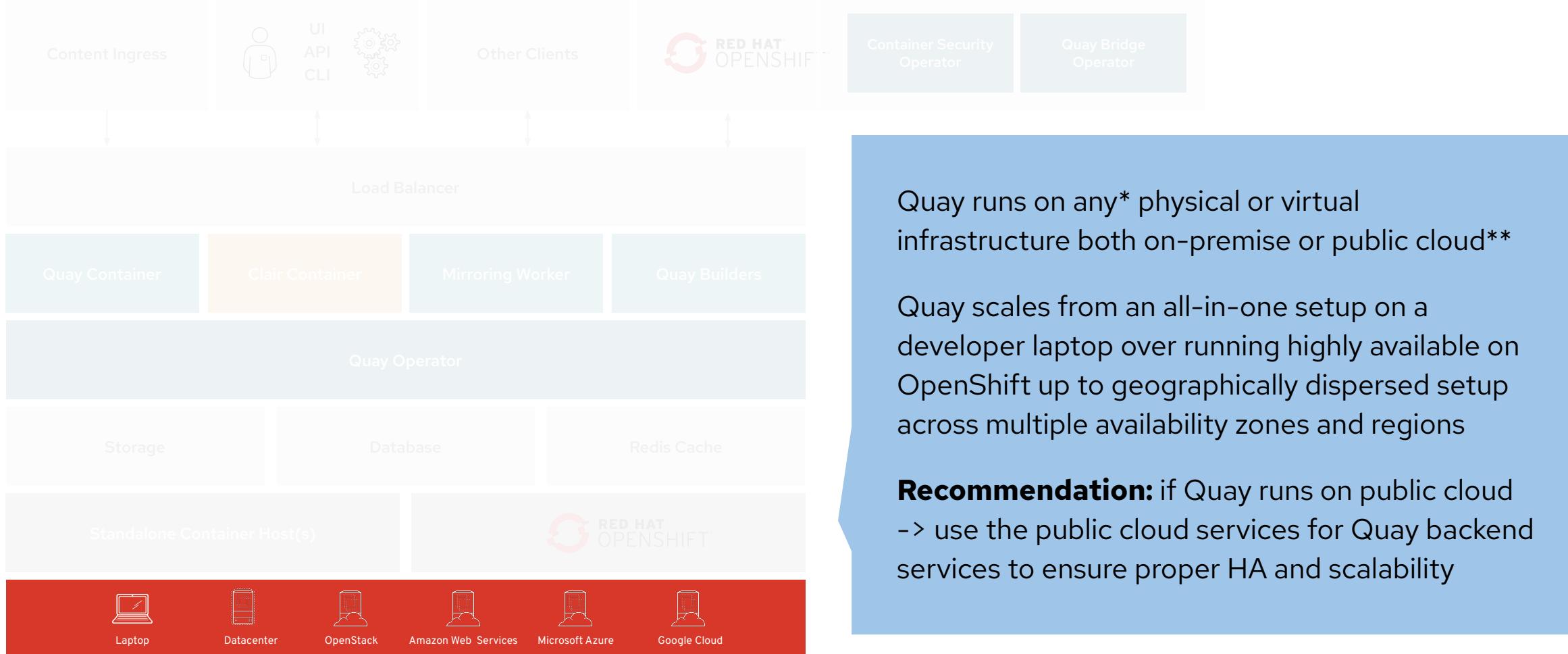


# Quay Architecture

# Red Hat Quay Architecture



# Prerequisite: Infrastructure

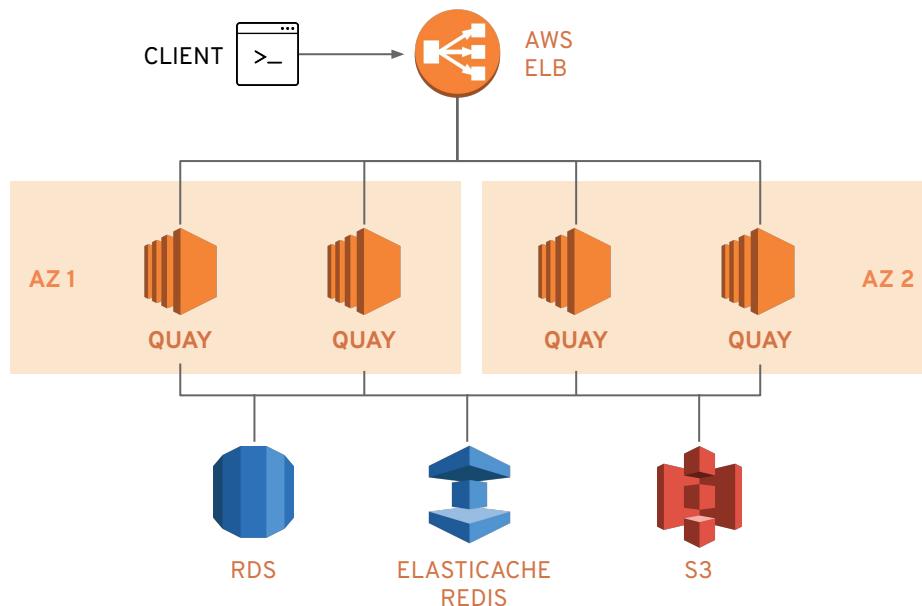


\* Further details can be found in the Quay 3.x tested configuration matrix: <https://access.redhat.com/articles/4067991>

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

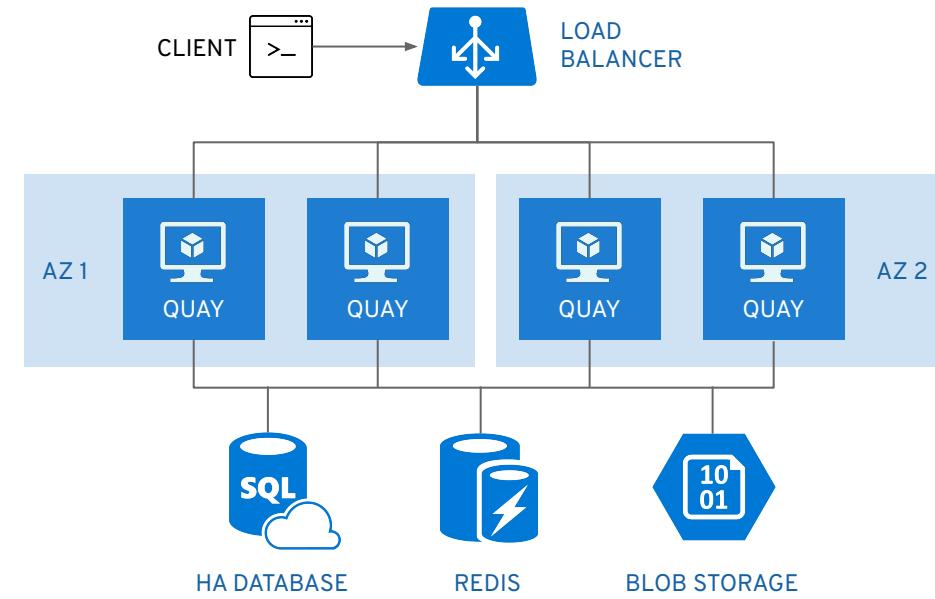
# Running Red Hat Quay on Public Cloud

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



If Quay runs on AWS you can use:

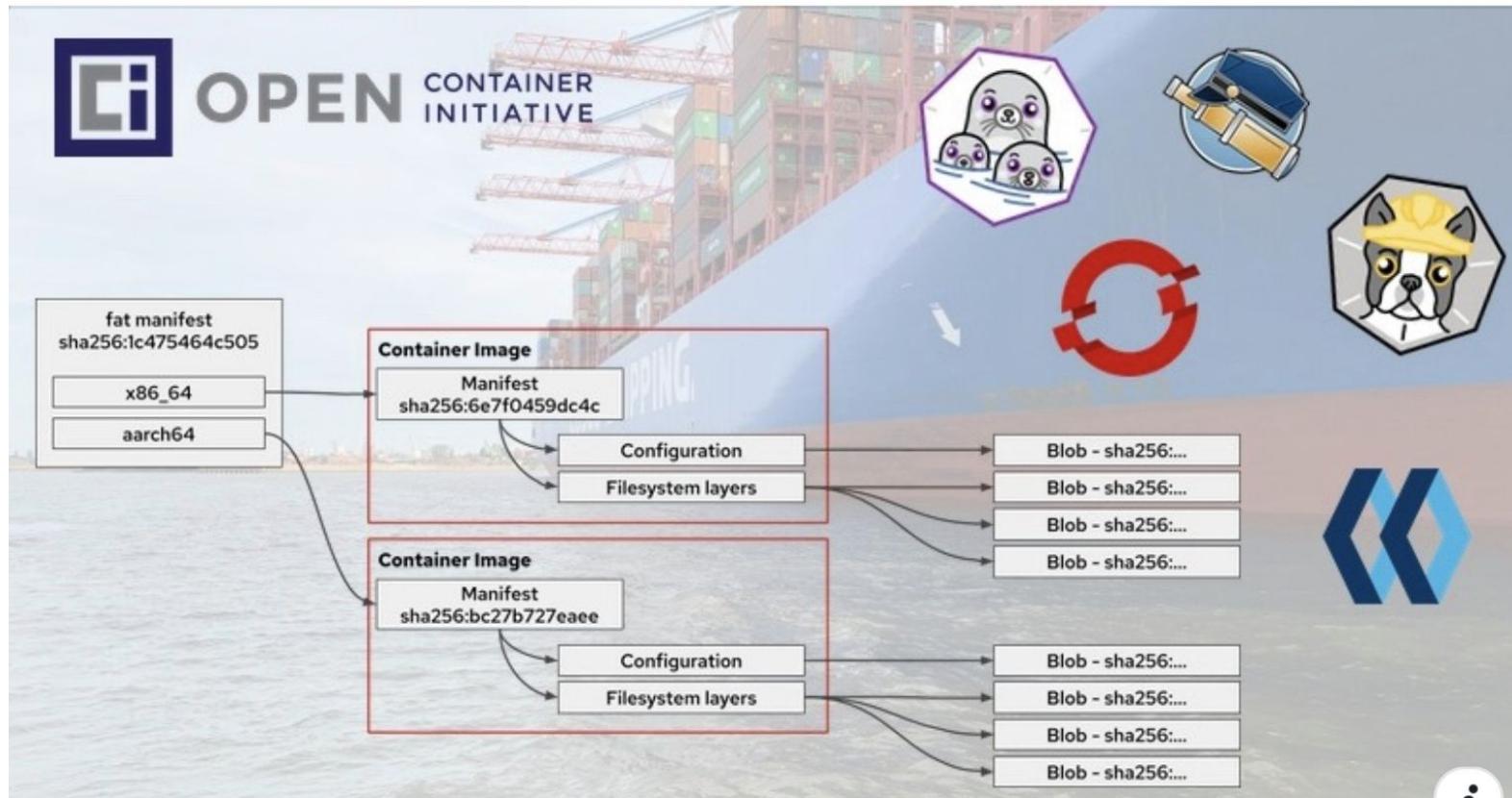
- AWS Elastic Load Balancer
- AWS S3 (hot) blob storage
- AWS RDS database
- AWS ElastiCache Redis
- EC2 VMs recommendation: M3.Large or M4.XLarge



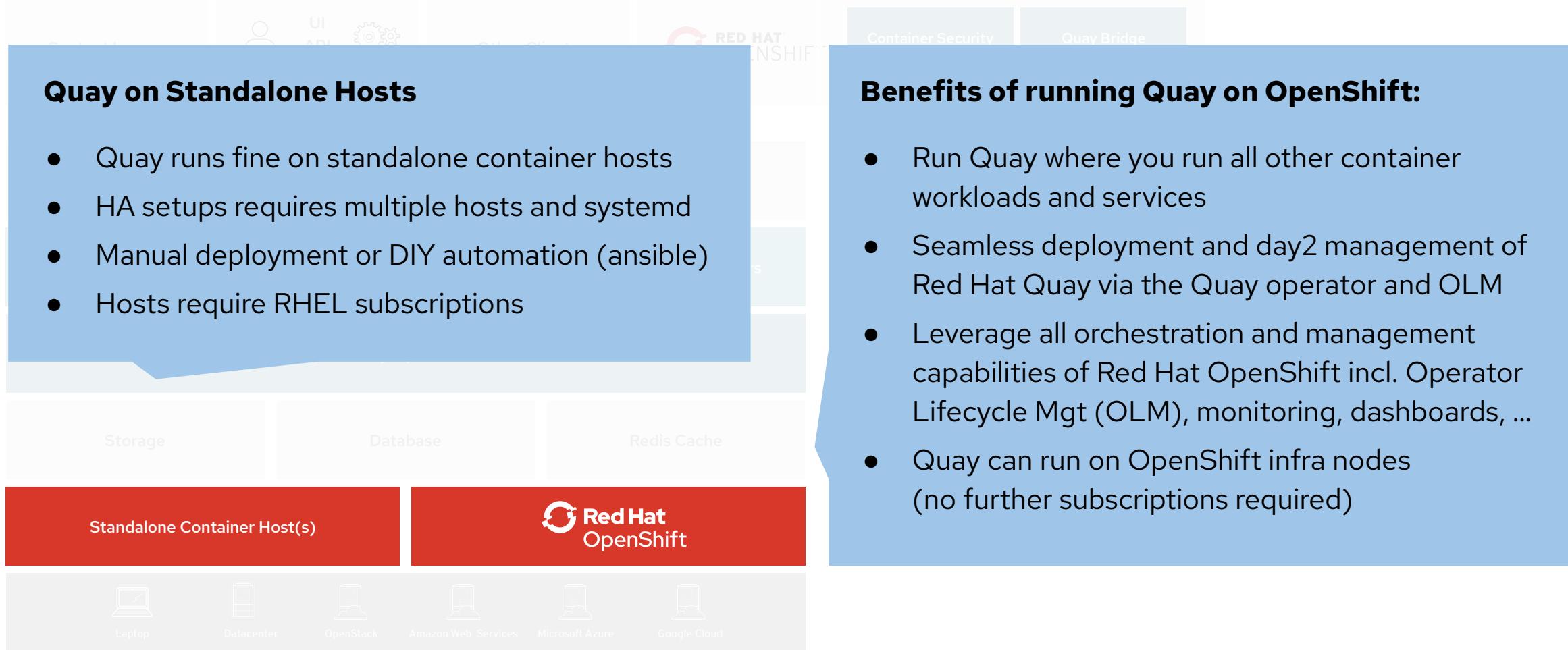
If Quay runs on MS Azure you can use:

- Azure managed services such as HA PostgreSQL
- Azure Blob Storage must be hot storage (not Azure Cool Blob Storage)
- Azure Cache for Redis

# Multi Architecture Containers



# Prerequisite: Container Runtime or Orchestration

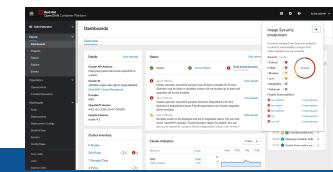


# Red Hat Quay works best with OpenShift

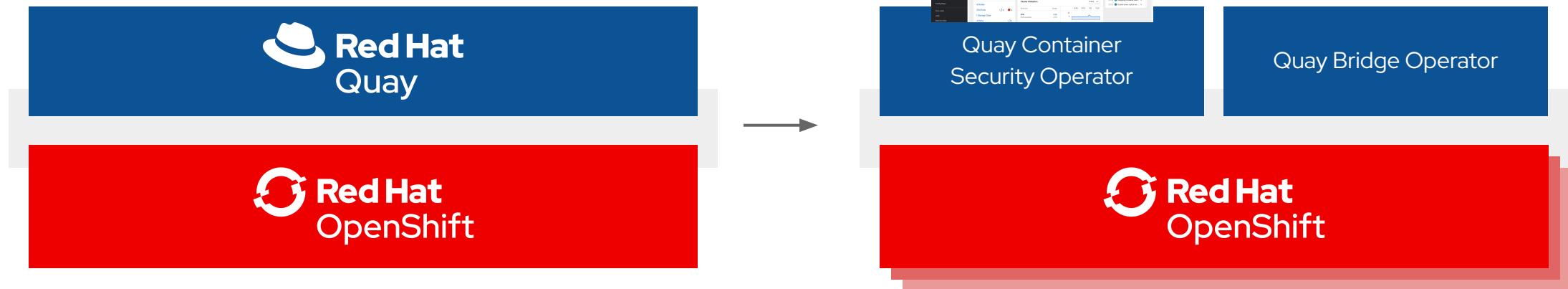
Red Hat Quay runs on any infrastructure  
but **runs best on OpenShift**

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.

# Benefits of running Quay on OpenShift



- **Zero to Hero** - Simplified deployment of Quay and associated components means that you can start 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

# Quay Sizing Recommendations

- Scalability of Quay is one of its key strengths since the same code base runs on a developer laptop with a PoC sizing, as a typical mid-size deployment with ~2,000 users serving content to dozens of kubernetes clusters up to thousands of clusters world-wide (Quay.io)
- As for any other product there are no “typical sizing recommendations” since sizing heavily depends on a multitude of factors (no of users / images / concurrent pulls and pushes, etc.)
- **Stateless** components can be **scaled-out** (will cause more load on backend services though)
  - Auto-scaling on k8s deployments currently tech-preview, future via Quay operator
  - Note: Scaling out stateless components will add load to stateful components
- **Minimum** requirements as documented in the Quay Product Docs:
  - Quay: min 4GB, recommended 6GB, 2 or more vCPUs
  - Clair: recommended 2GB RAM, 2 or more vCPUs
  - Clair database requirements for security metadata: min 200MB
  - Storage depends on no of images, recommended min 30GB

# Quay Sample Sizings

**Note:** Those are sample sizings of existing Quay deployments. Whether a specific deployment runs fine with the same metrics depends on too many other factors as well not shown here.

Metric	Minimum Setup	Mid/Large Setup	XXXXL (Quay.io)
No of Quay containers by default	1	4	15
No of Quay containers max at scale-out	N/A	8	30
No of Clair containers by default	1	3	10
No of Clair containers max at scale-out	N/A	6	15
No of mirroring pods <sup>1</sup> (to mirror 100 repos)	1	5-10	N/A
Database sizing		4-8 Cores / 6-32 GB RAM	32 cores 244GB, 1+ TB disk
Storage Backend Sizing	10-20 GB	1 - 20 TB	50+ TB up to PB
Redis Cache Sizing <sup>2</sup>		2 Cores / 2-4 GB RAM	4 cores / 28 GB RAM
Underlying node sizing (phys or virtual)	2-4 Cores / 6 GB RAM	4-6 Cores, 12-16 GB RAM	Quay: 13 cores 56GB RAM Clair: 2 cores 4 GB RAM

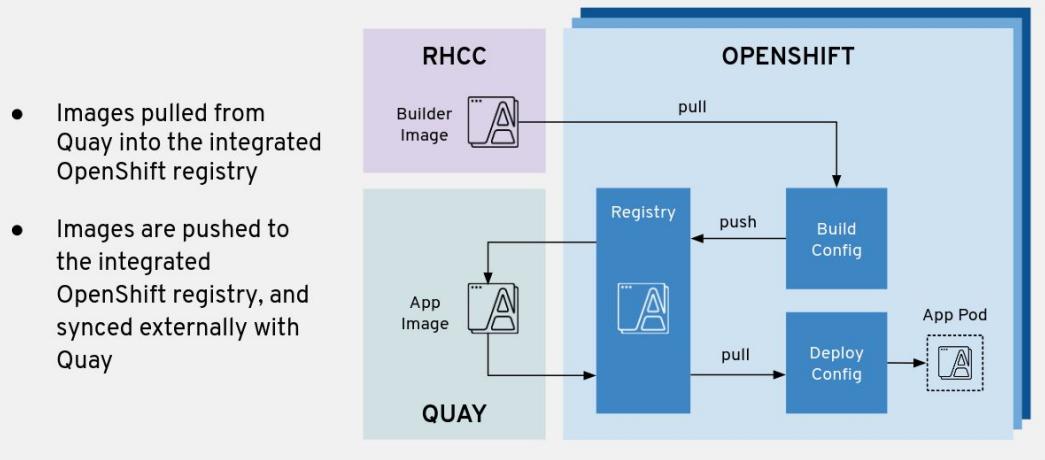
<sup>1</sup> see repository mirroring section for further details on sizing & related recommendations

<sup>2</sup> since Redis cache is only used for Quay builders the sizing can be very tiny if builders aren't used

# Using Quay With or Without Internal Registry

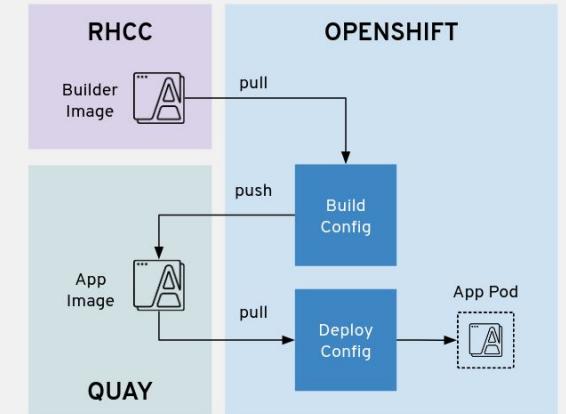
- Quay can be used as an external registry in front of an entire OpenShift cluster with its registry
- Quay also can be used directly without using the internal registry which requires a couple of changes (secrets, build and deployment configs) which are **partially** done automatically by QBO

## Quay as Upstream Registry with OpenShift



## Quay as OpenShift Registry

- Images are pushed directly by builds to Quay
- Images are pulled directly from Quay

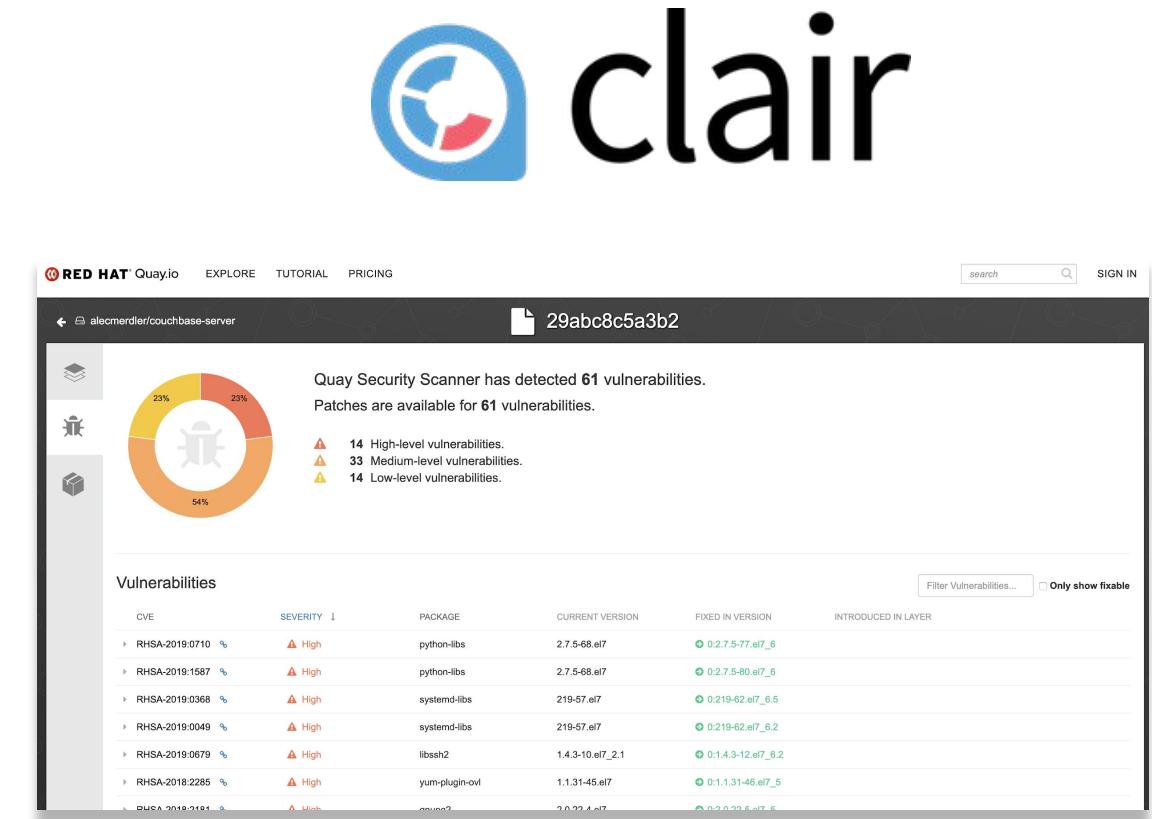




## Built-In Vulnerability Scanning via Clair

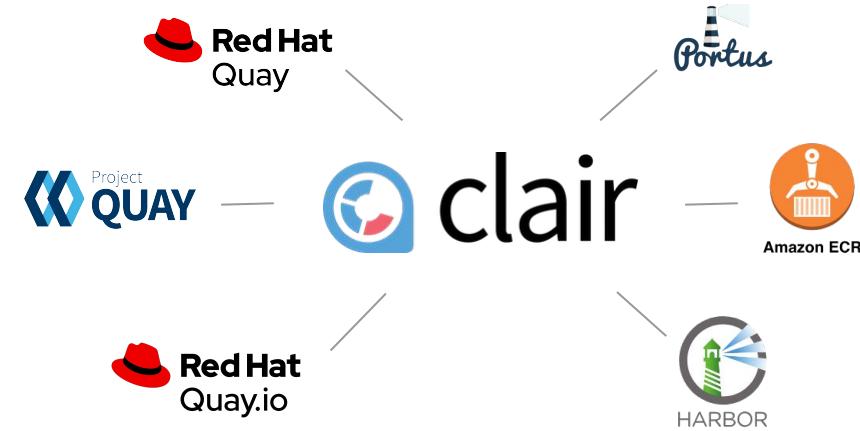
# Clair Overview

- 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>





The screenshot shows the Red Hat Quay interface with a search bar and navigation tabs for 'REPO', 'EXPLORE', 'REPOSITORIES', and 'TUTORIAL'. A search result for 'example/python' is shown with a digest '3f86e14b88f9'. The page indicates 718 vulnerabilities found, with patches available for 144. A pie chart breaks down the vulnerabilities by severity: 7% High-level, 31% Medium-level, 37% Low-level, 26% Negligible-level, and 8% Unknown-level. Below the chart, a table lists 144 vulnerabilities, including details like CVE ID, Severity, Package, Current Version, Fixed In Version, and Introduced In Layer. Examples include CVE-2018-15686 in systemd, CVE-2019-3855 in libssh2, CVE-2019-3462 in apt, and CVE-2017-16997 in glibc.



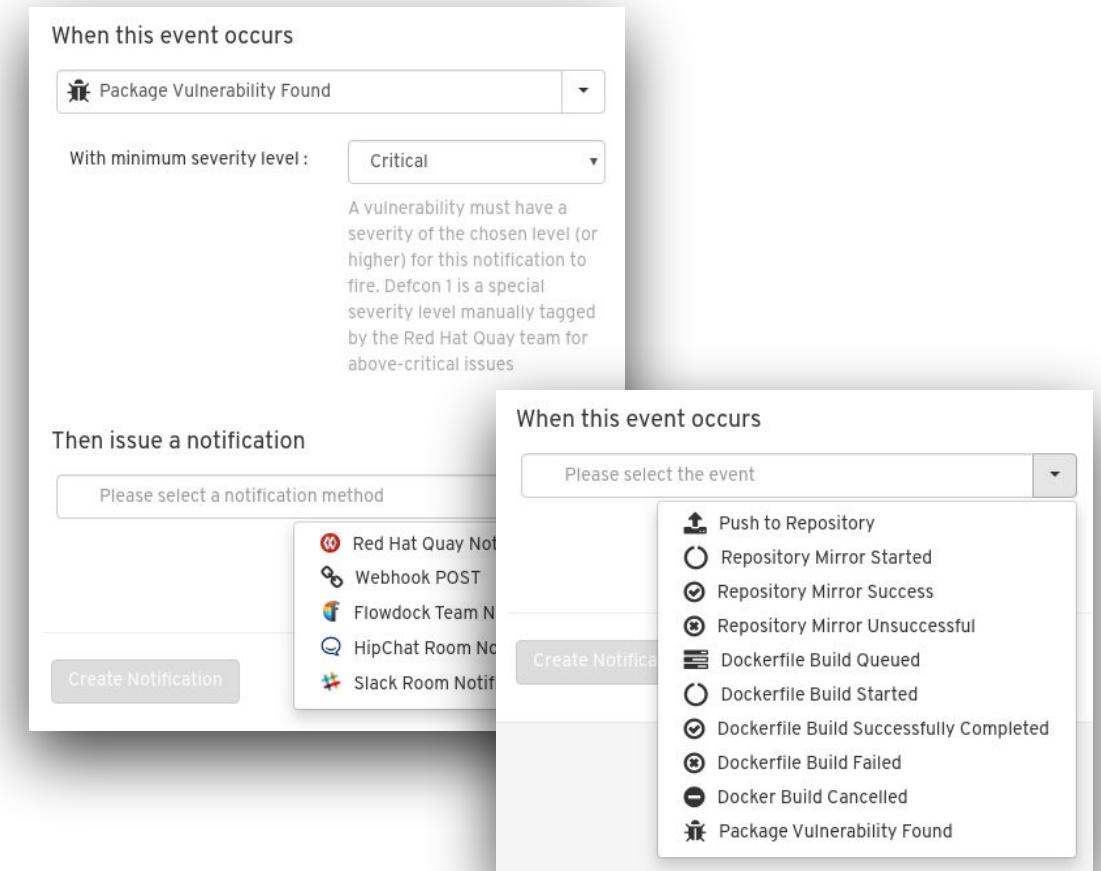
## Clair v4 (Tech Preview with Quay 3.3)

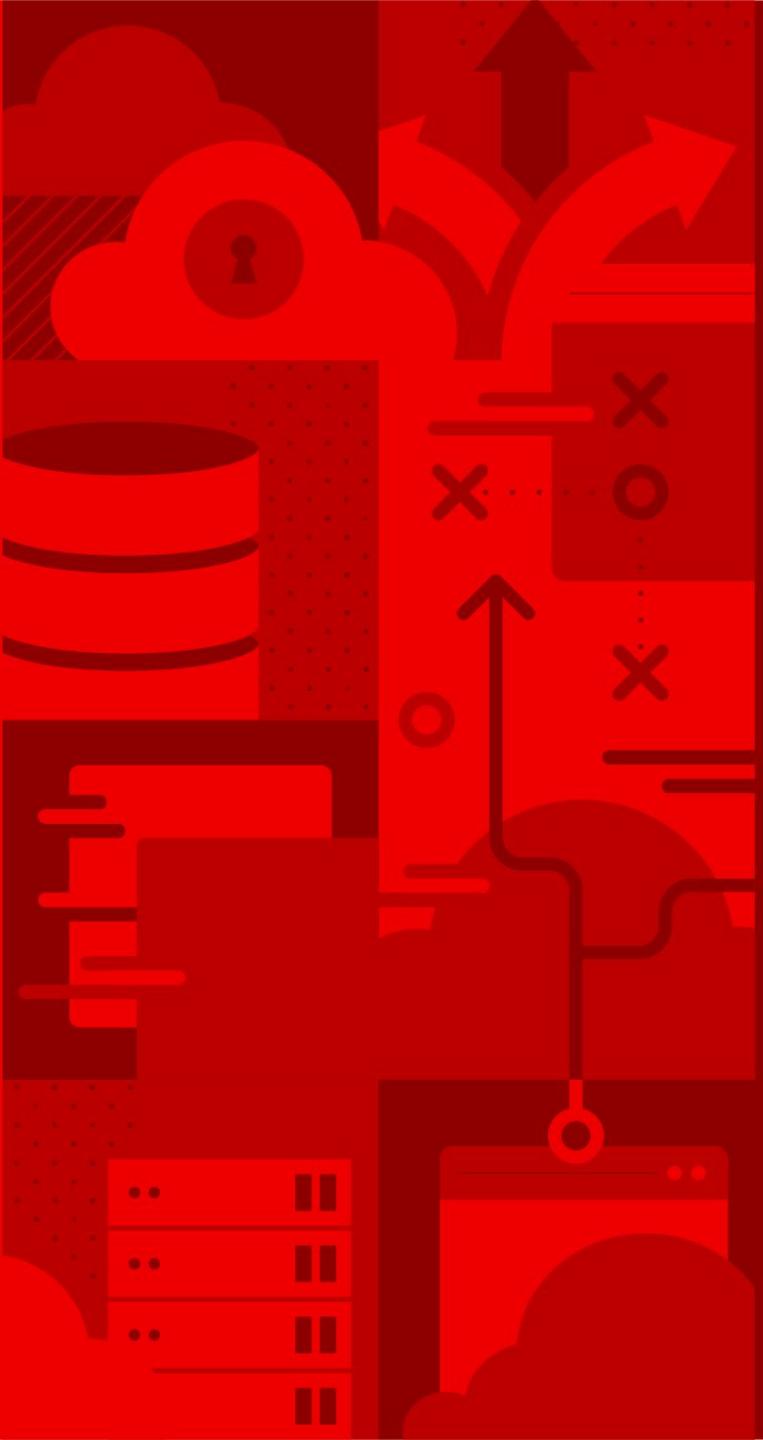
Clair v4 is the newest version of Clair after a massive refactoring in order to make several big enhancements possible. This includes:

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

# Notifications for Vulnerabilities found by Clair

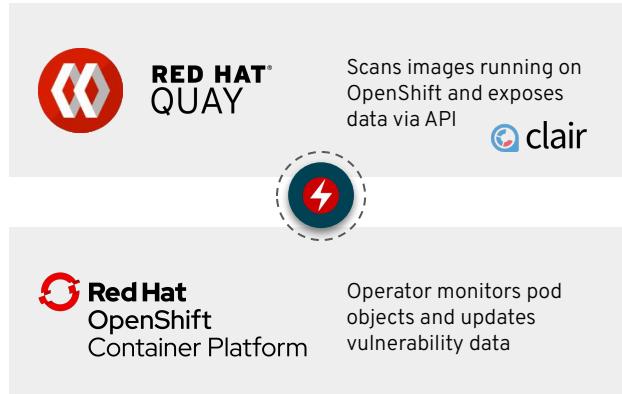
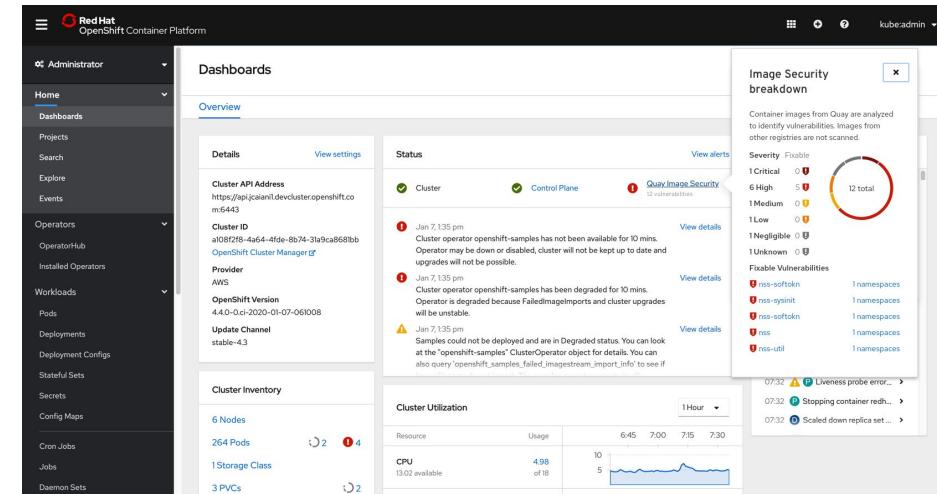
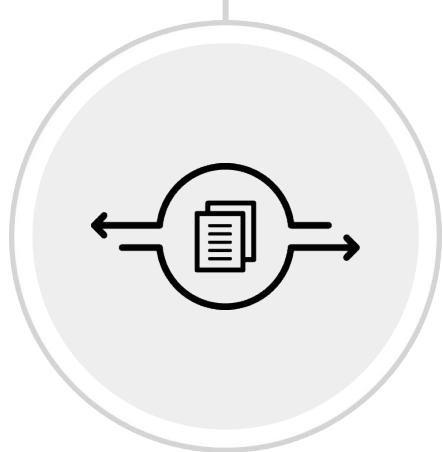
- **Quay triggers different notifications for various repository events** (depends on enabled features)
- This includes the event type “**Package Vulnerability Found**”
- Additional Filter can be applied for **Severity Level**
- **Various Notification Methods**
- Custom Notification Title (optional)





# Container Security Operator and OpenShift Console Integration

## Quay Container Security Operator (CSO)



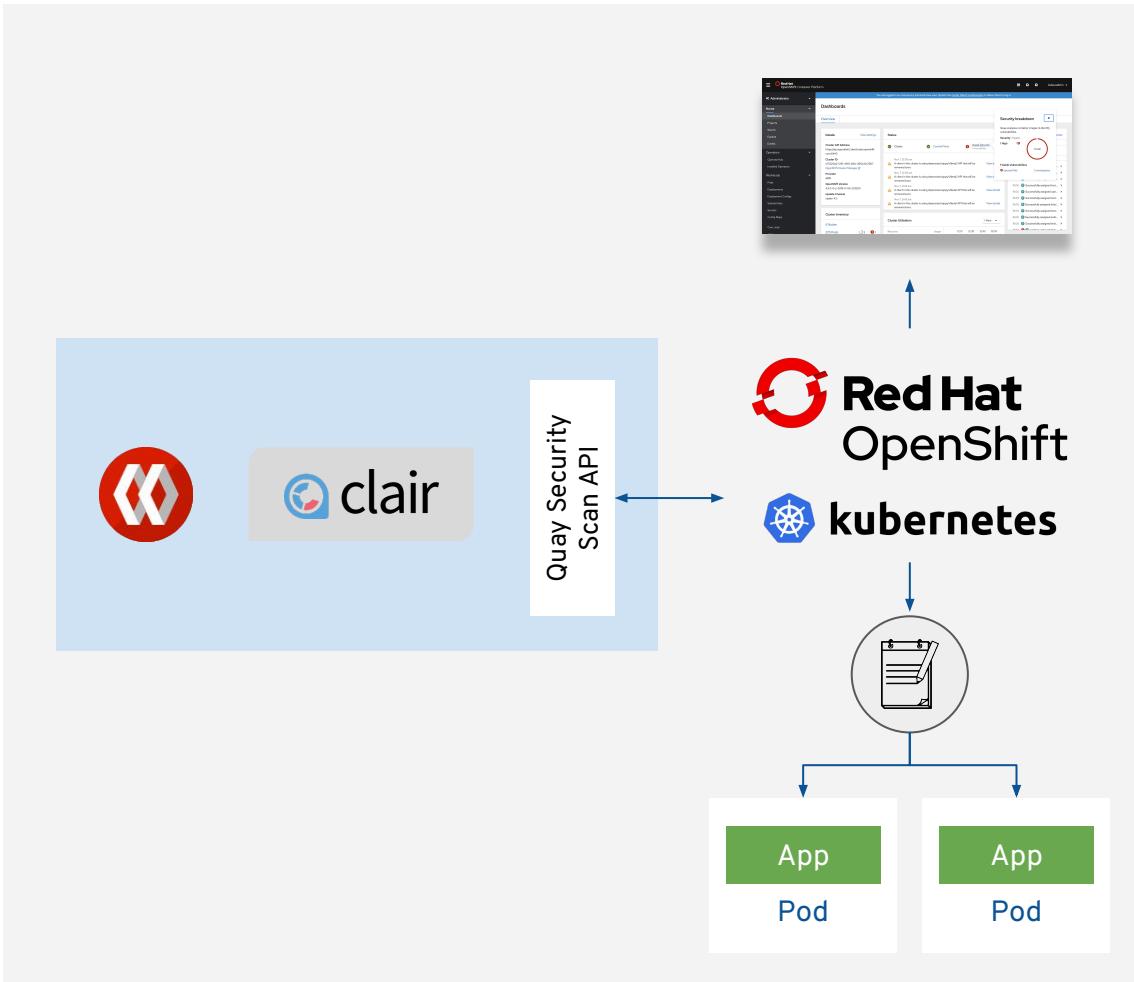
## Container Security Operator - Vulnerability Data in OpenShift

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

# 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)

# OpenShift Console Vulnerability Information Enhancements

Project: knative-eventing

ImageManifestVuln > ImageManifestVuln Details

**IMV openshift-knative/knative-e-evening-channel-controller@08aed83clbb**

**Details** **YAML** **Affected Pods**

**Image Manifest Vuln Details**

Quay Security Scanner has detected 7 vulnerabilities.  
Patches are available for 7 vulnerabilities.  
7 High vulnerabilities.

7 total

Name	Registry
sha256:08aed83clbb9f510d0f2c4dc64993fa333bad32d90bc08e4fcfc82fb	quay.io/openshift/knative/knative-e-evening-channel-controller

**Namespace** knative-eventing

**Labels** knative-eventing/imc-controller-69c4775c85-vg77q=true

**Annotations** 0 Annotations

**Created At** Mar 23, 4:40 pm

**Owner** No owner

**Vulnerabilities**

Vulnerability	Severity	Package	Current Version	Fixed in Version
RHSA-2019-4190	High	nss-softoken-freebl	3.44.0-5.el7	0.344.0-8.el7_7
RHSA-2019-4190	High	nss-util	3.44.0-3.el7	0.344.0-4.el7_7
RHSA-2019-4190	High	nss-tools	3.44.0-4.el7	0.344.0-7.el7_7
RHSA-2019-4190	High	nss-softoken	3.44.0-5.el7	0.344.0-8.el7_7
RHSA-2019-4190	High	nss	3.44.0-4.el7	0.344.0-7.el7_7
RHSA-2019-4190	High	nss-sysinit	3.44.0-4.el7	0.344.0-7.el7_7
RHSA-2020-0227	High	sqlite	3.717-8.el7	0.3717-8.el7_71

Project: knative-eventing

**Image Manifest Vulnerabilities**

Filter by name...

Image Name	Namespace	Highest Severity	Affected Pods	Fixable	Manifest
IMV openshift-knative/knative-e-evening-channel-controller	NS knative-eventing	High	1	7	08aed83clbb
IMV openshift-knative/knative-e-evening-sources-controller	NS knative-eventing	High	1	7	32f3ca637fd
IMV openshift-knative/knative-e-evening-controller	NS knative-eventing	High	1	7	cc4ec0d71b8
IMV openshift-knative/knative-e-evening-webhook	NS knative-eventing	High	1	7	e3bb2c01ddf

# 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](https://www.linkedin.com/company/red-hat)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



[twitter.com/RedHat](https://twitter.com/RedHat)