Red Hat

Quay!

A Deep Dive

Laine Minor
Senior Solutions Architect
Application Deployment

Hi! I'm Laine Minor.

I'm an Application Deployment Solutions Architect, covering Wisconsin and Minnesota.

I live in a suburb of Lansing, Michigan.

Fun fact: At last count, I have 16.5 tattoos.

minor@redhat.com

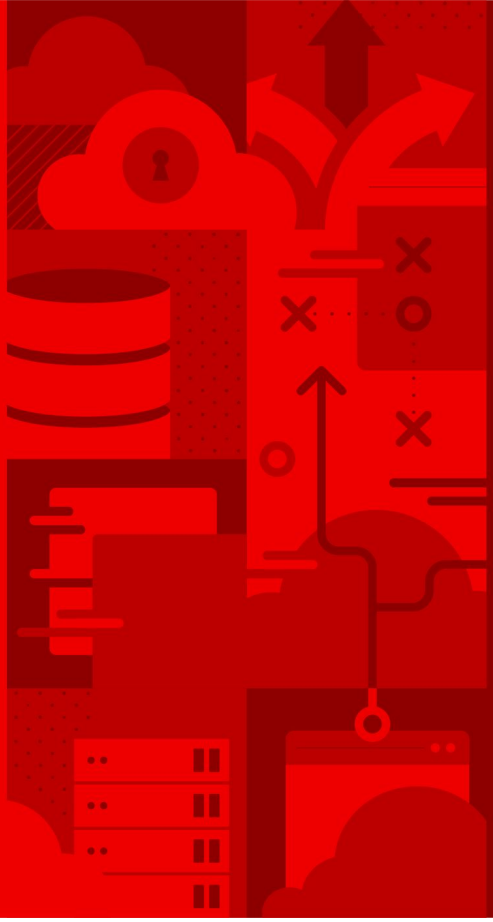
@lainieftw

Red Hat

Agenda

- Review: OpenShift and Containers
- Review: OpenShift and Kubernetes – Core (Relevant) Technical Pieces
- Quay: The Deep Dive Part(s)!
- Demo/Tour of Quay

Red Hat

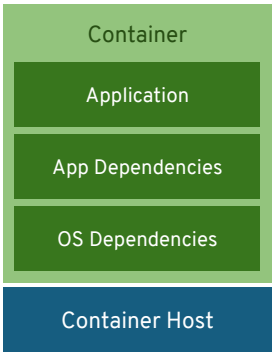


First, let's touch base on OpenShift and containers in general...

Red Hat

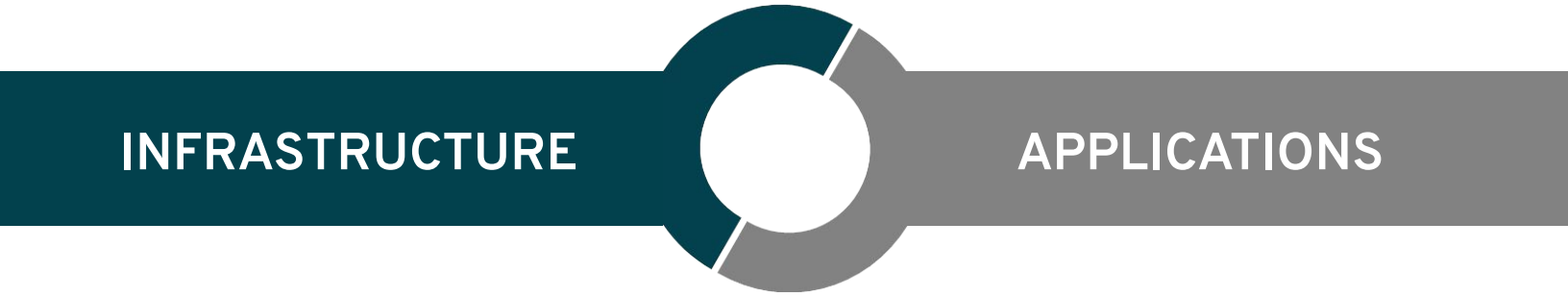
What is a container?

A container is an application, the application's dependencies/libraries/other binaries, and the configuration files that the application needs to run, all bundled into **one portable unit**.



Red Hat

Okay, but *why* containers?



- Application processes on a shared kernel
- Simpler, lighter, and denser than VMs
- **Portable** across different environments
- Dynamic **scalability** on demand

- Package apps with all dependencies
- Deploy to any environment in **seconds**
- Cloud-native application development
- **Flexibility** with language & runtime

Red Hat

What is Kubernetes?

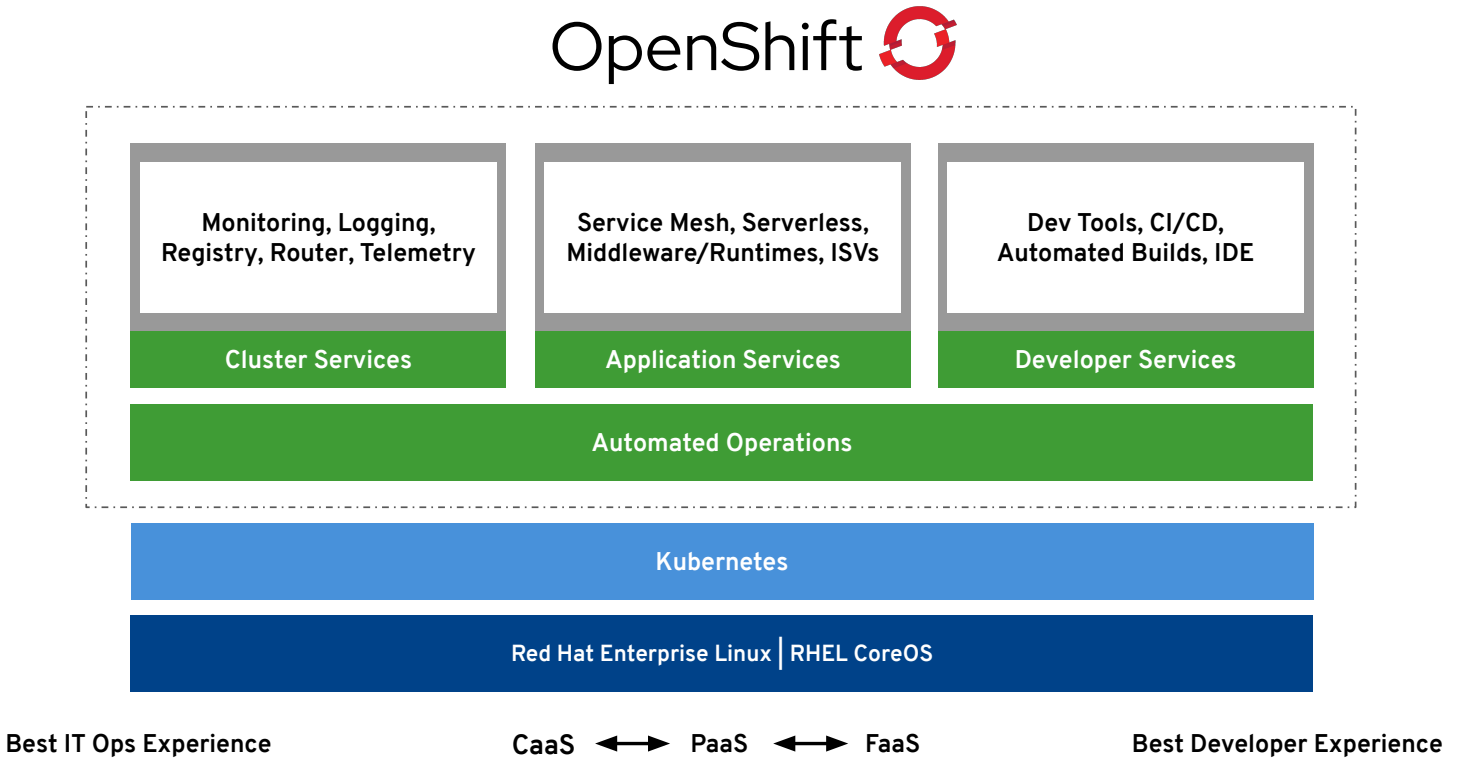
Kubernetes is open source container orchestration – it automates **deployment**, **scaling**, and **management** of containers.

Red Hat

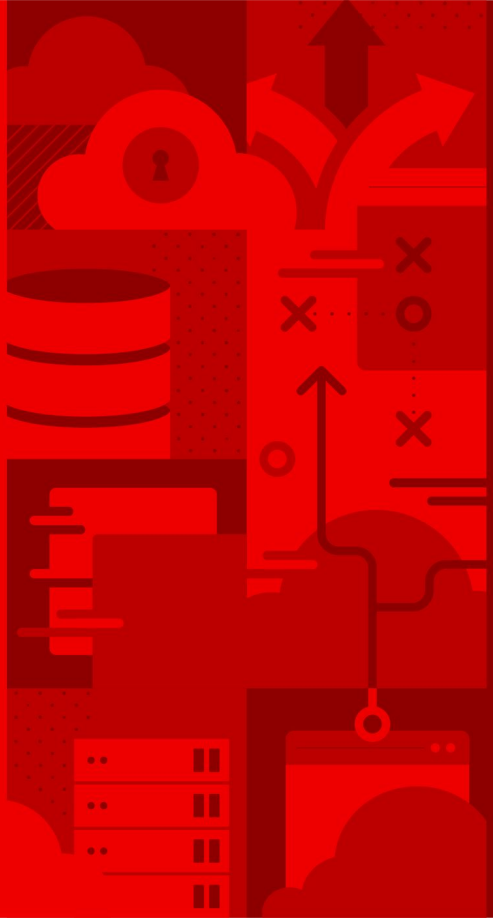
OpenShift

Red Hat OpenShift is a Kubernetes-based, enterprise-ready container application platform.

Red Hat


OpenShift
Monitoring, Logging, Registry, Router, Telemetry
Service Mesh, Serverless, Middleware/Runtimes, ISVs
Dev Tools, CI/CD, Automated Builds, IDE
Cluster Services
Application Services
Developer Services
Automated Operations
Kubernetes
Red Hat Enterprise Linux | RHEL CoreOS
Best IT Ops Experience
CaaS
PaaS
FaaS
Best Developer Experience

Red Hat



OpenShift and Kubernetes: Core (Relevant) Technical Pieces

Red Hat

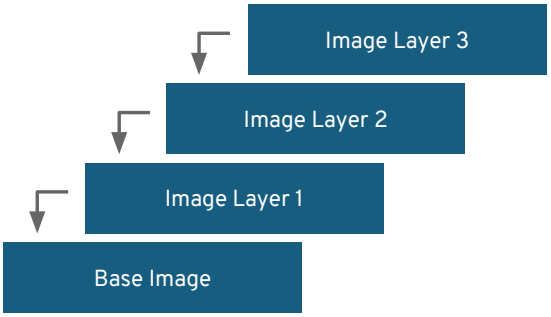
a container is the smallest compute unit

Red Hat

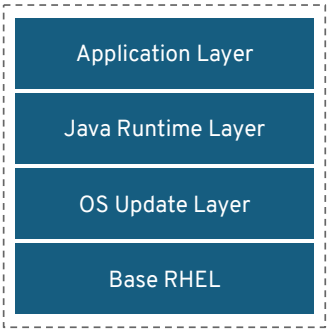
containers are created from container `images`

Red Hat

container `images` are built in layers



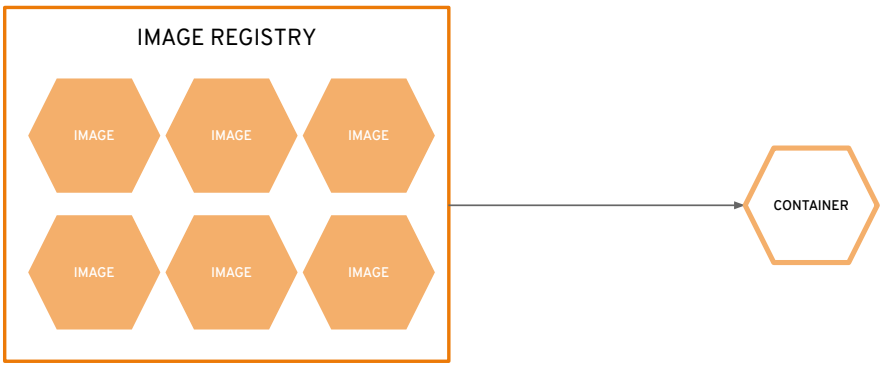
Container Image Layers



Example Container Image

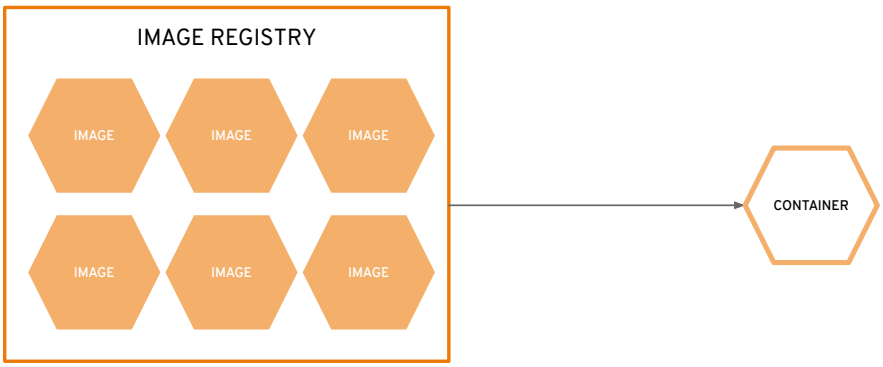
Red Hat

...and are stored in an `image registry`



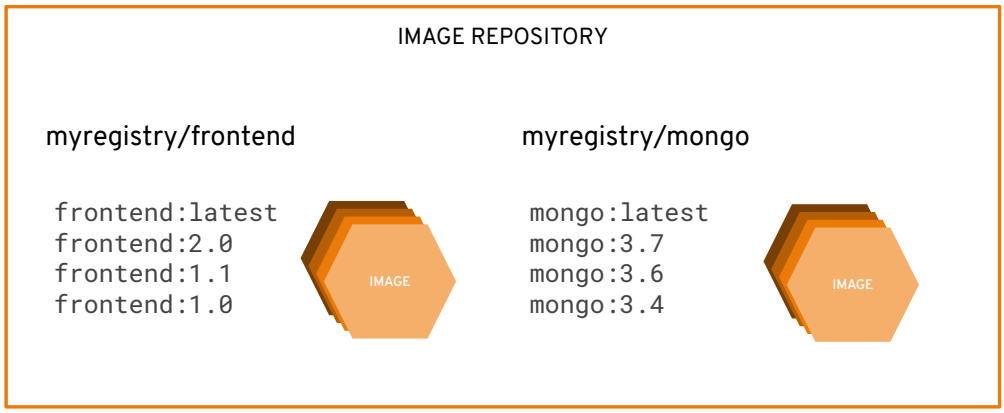
Red Hat

an `image registry` is the basic *concept* behind image storage and management



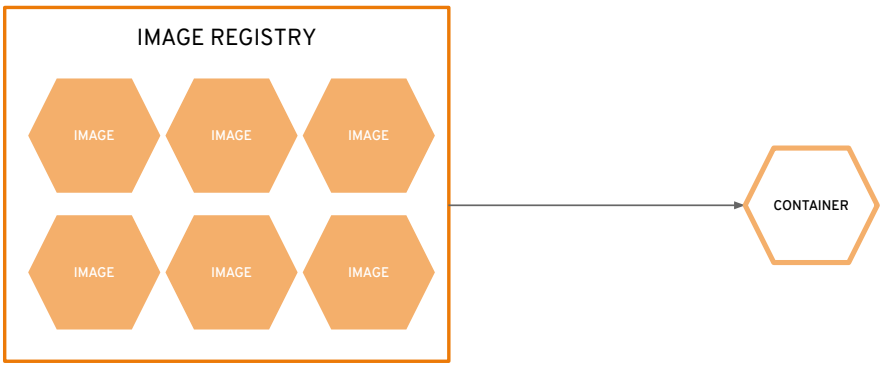
Red Hat

an `image repository` contains all versions (`tags`) of an image



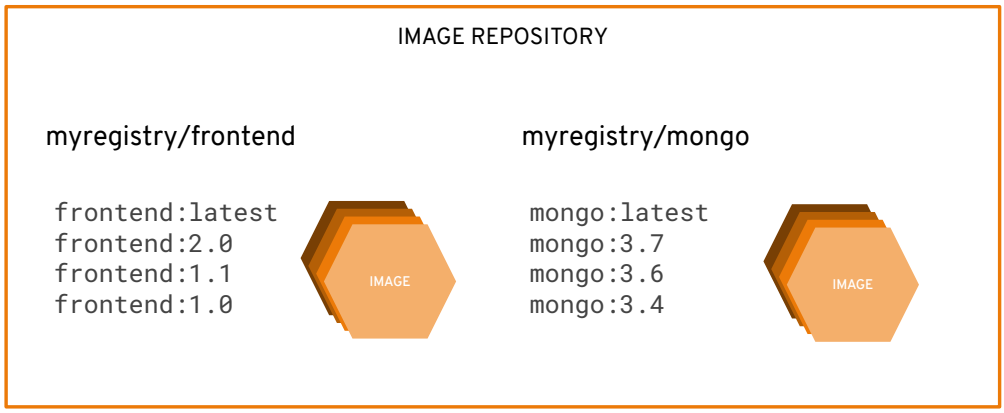
Red Hat

`image registry` = concept

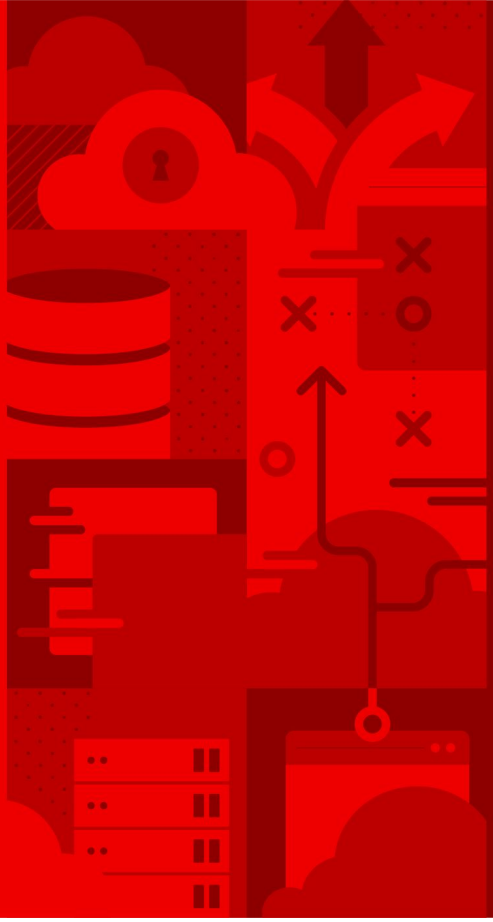


Red Hat

`image repository` = *implementation*



Red Hat

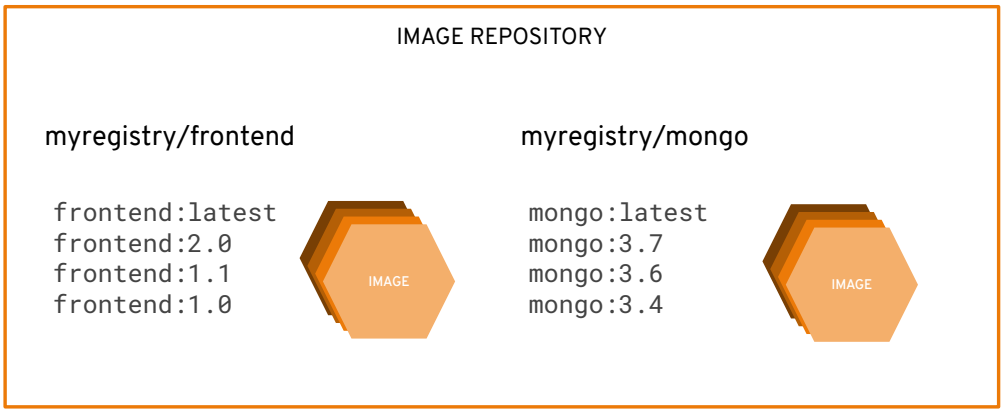


Red Hat Quay

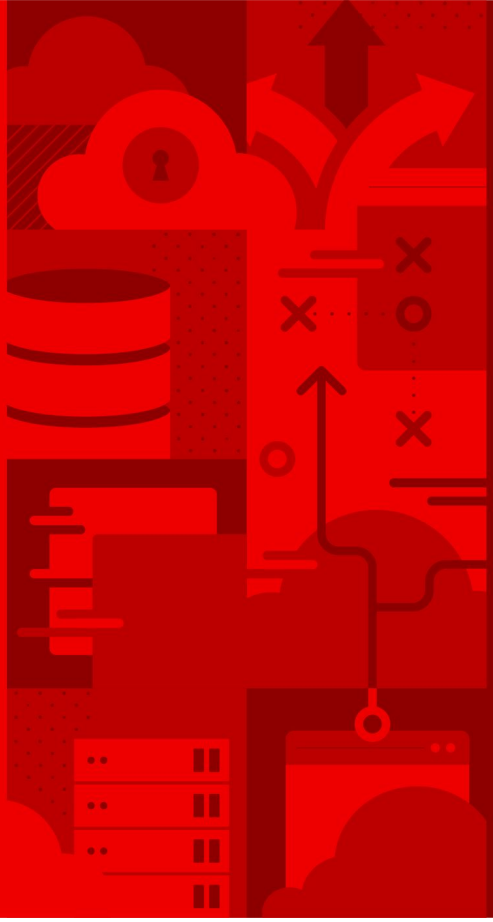
What is it?

Red Hat

Red Hat Quay



Red Hat



Red Hat Quay

What value does it provide?

Red Hat

Red Hat
Quay

Trusted, open source container registry platform that runs everywhere, but runs best on Red Hat OpenShift

Scalability, from a developer laptop to a container host or Kubernetes, on-premise or on public cloud

Global governance and security controls, with image vulnerability scanning, access controls, geo-replication, etc.

Offered as a **self-managed enterprise container registry product** and as a **hosted multi-tenant SaaS solution**

Red Hat

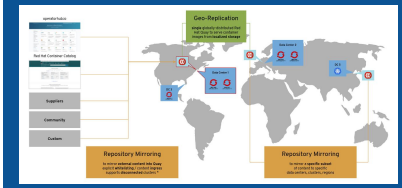
Okay, but...what *business* problems does Quay solve?

- Large-scale or distributed environments (think thousands of users, and/or thousands of images)
- Images shared across multiple OpenShift clusters
  - Dev + Prod
  - Dev + Prod + Prod 2 + Prod n
  - East + West + Europe
  - AWS + Azure + On-prem
  - ...etc
- Governance/security of container images
- High image maintenance and automation requirements
- “Source of truth” tailored to container images

Red Hat

Or said another way, it works great in a “DevSecOps” software delivery process:

BUILD

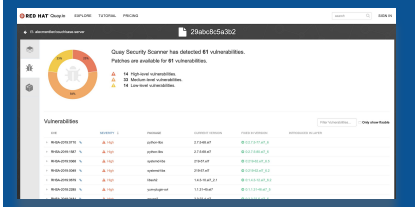


Content ingress point for explicitly whitelisted (trusted) content

Access to Scan Results in all stages of your development pipeline

Fine-Granular RBAC Model

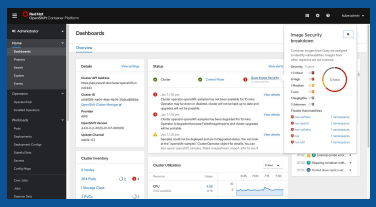
DEPLOY



built-in vulnerability scanning at the place where it makes most sense and scales best

Advanced Logging and Auditing

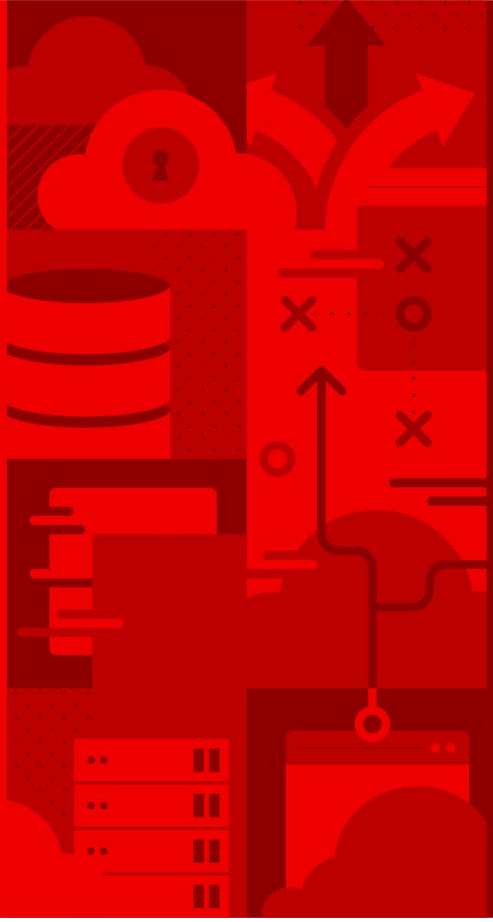
RUN



Vulnerability scan results exposed to the platform and its users

Alerting via Notifications or Webhooks to trigger actions

Red Hat

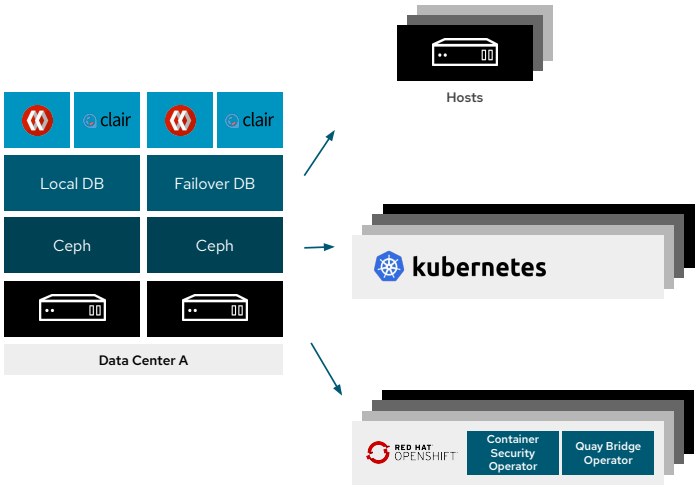


Red Hat Quay

Deployment Models

Red Hat

Quay Deployment Examples



Red Hat Quay can serve content to:

- Any container runtime or host
- Any orchestration platform

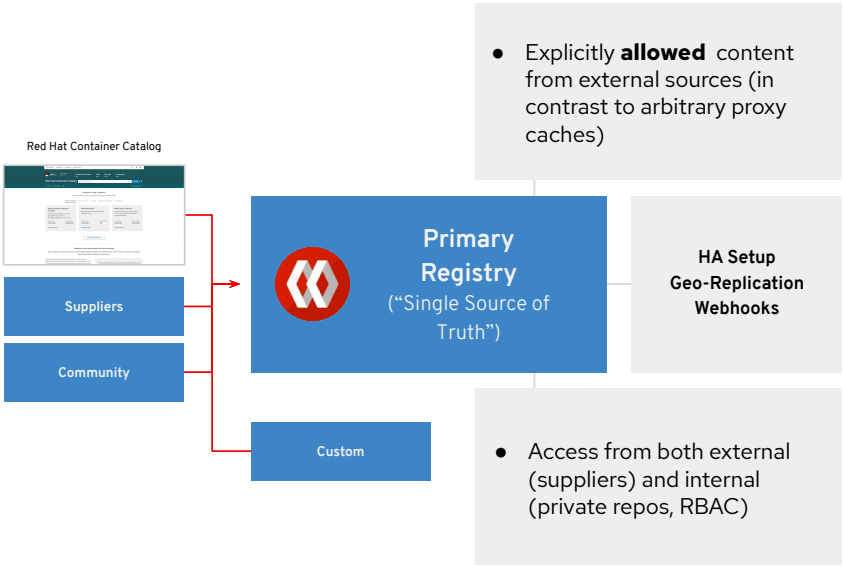
Typically Quay is serving content to many clients

- With different technologies / runtimes
- In different datacenters, VPCs or even regions

The only requirement is that the client is compatible with the protocols and specs Quay supports (Docker Registry API, OCI distribution spec).

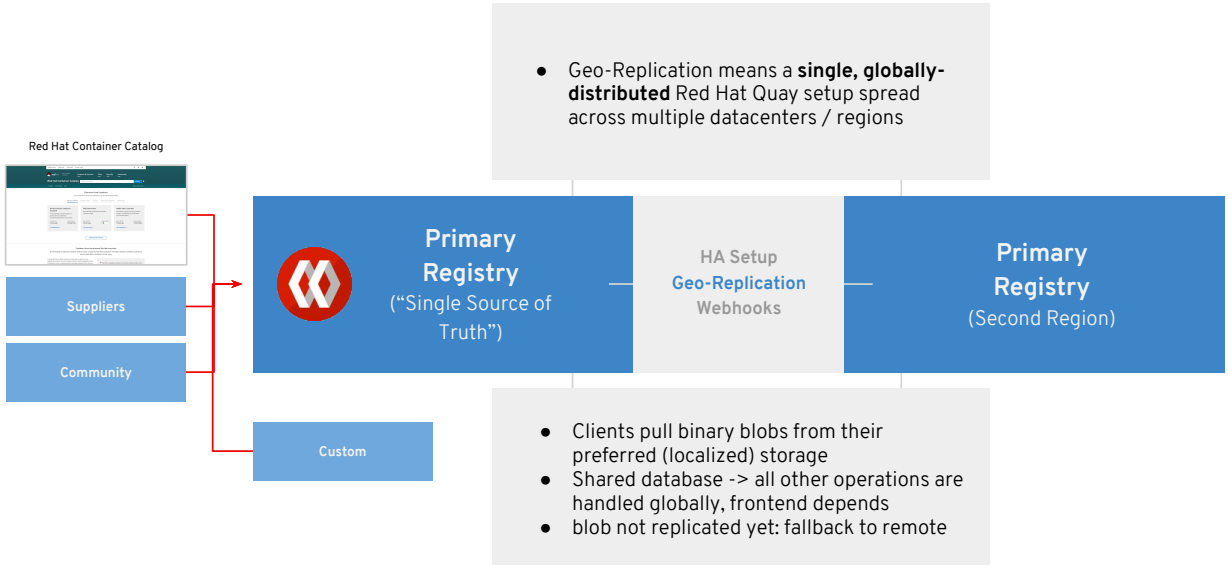
Red Hat

Model #1 - Buffer/Source of Truth



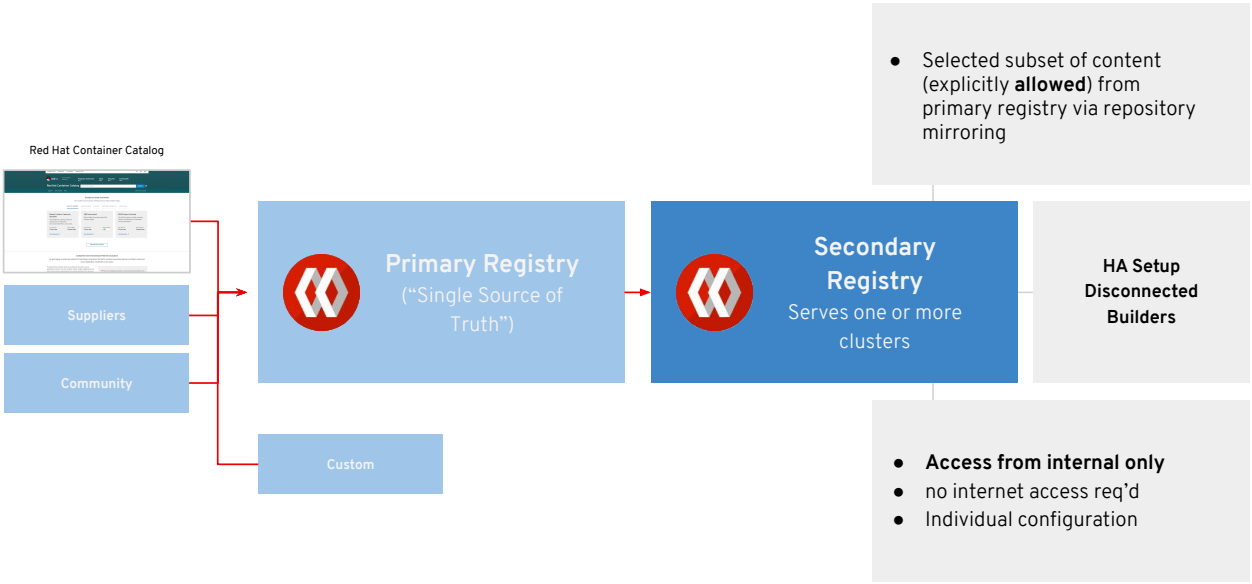
Red Hat

Model #2 - Source of Truth + Geo-Replication/Multi-Region



Red Hat

Model #3 – Source of Truth + Mirror(s)



Red Hat

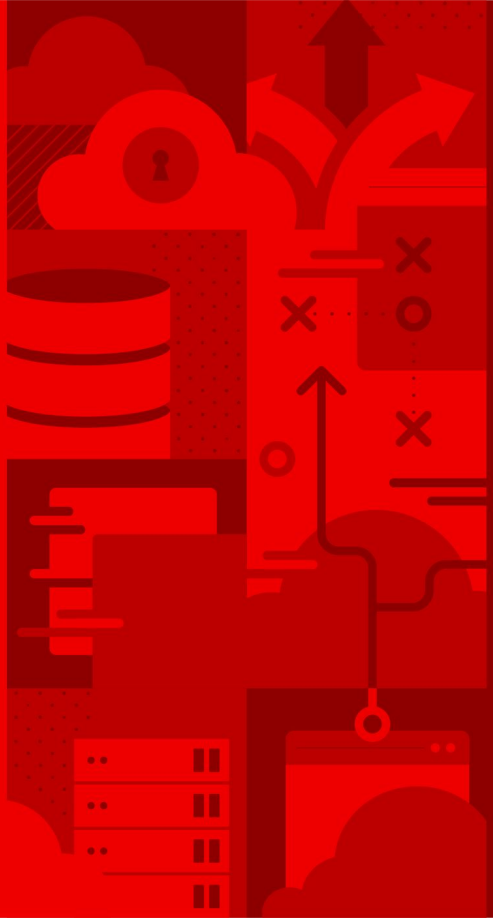
Quay Repository Mirroring vs. Geo-Replication

Feature / Capability	Geo- Replication	Repository Mirroring
Feature is designed for	a shared, global registry	Distinct, different registries
If replication / mirroring hasn't been completed yet then...	The remote copy is used (slower)	No image is served
Access to all storage backends in both regions required	Yes (all Quay nodes)	No (distinct storage)
Users can push images from both sites to the same repository	yes	no
whole registry content and configuration is identical across all regions (shared database)	yes	no
users can select individual namespaces / repositories to be mirrored	no	yes
users can apply filters (tag, tag range, etc.) to synchronization rules	no	yes
allows individual / different RBAC configurations in each region	no	yes

Quay Repository Mirroring vs. Geo-Replication

Feature / Capability	Geo- Replication	Repository Mirroring
Feature is designed for	a shared, global registry	Distinct, different registries
If replication / mirroring hasn't been completed yet then...	The remote copy is used (slower)	No image is served
Access to all storage backends in both regions required	Yes (all Quay nodes)	No (distinct storage)
Users can push images from both sites to the same repository	yes	no
whole registry content and configuration is identical across all regions (shared database)	yes	no
users can select individual namespaces / repositories to be mirrored	no	yes
users can apply filters (tag, tag range, etc.) to synchronization rules	no	yes
allows individual / different RBAC configurations in each region	no	yes

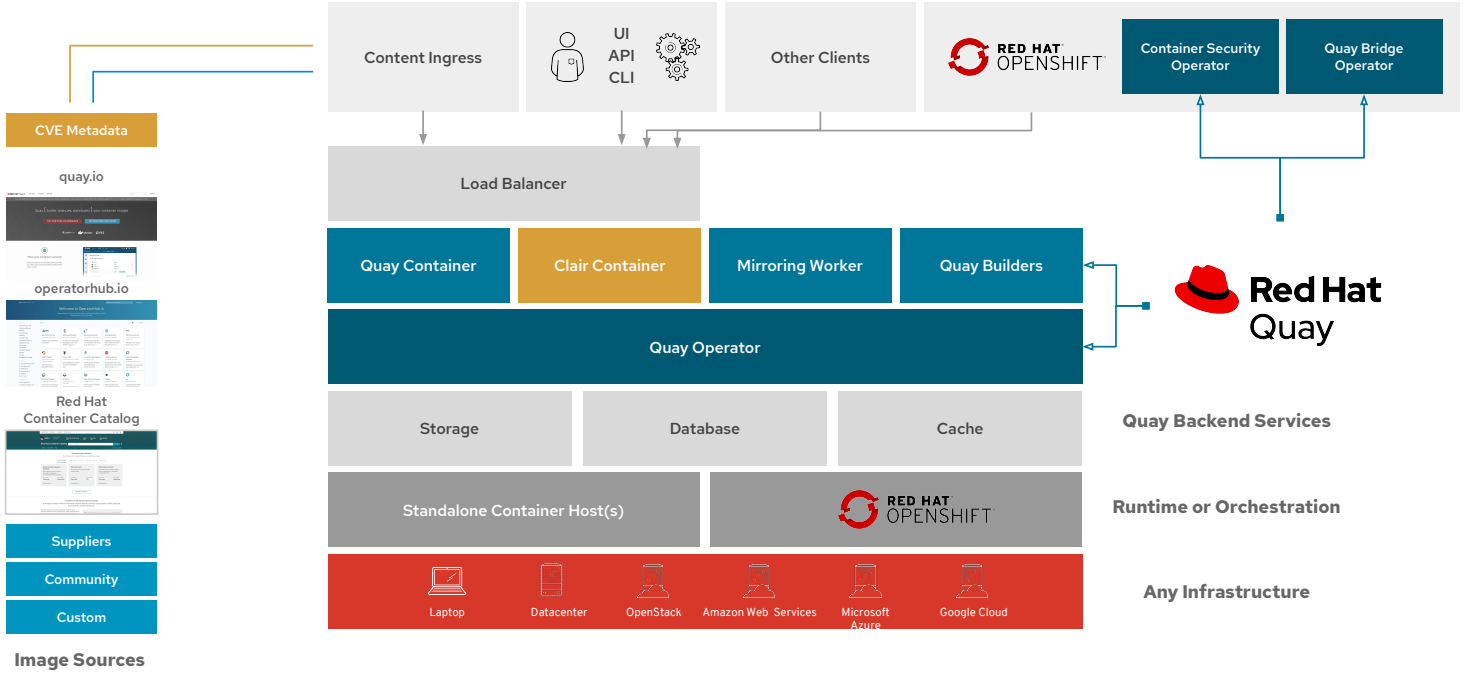
Red Hat



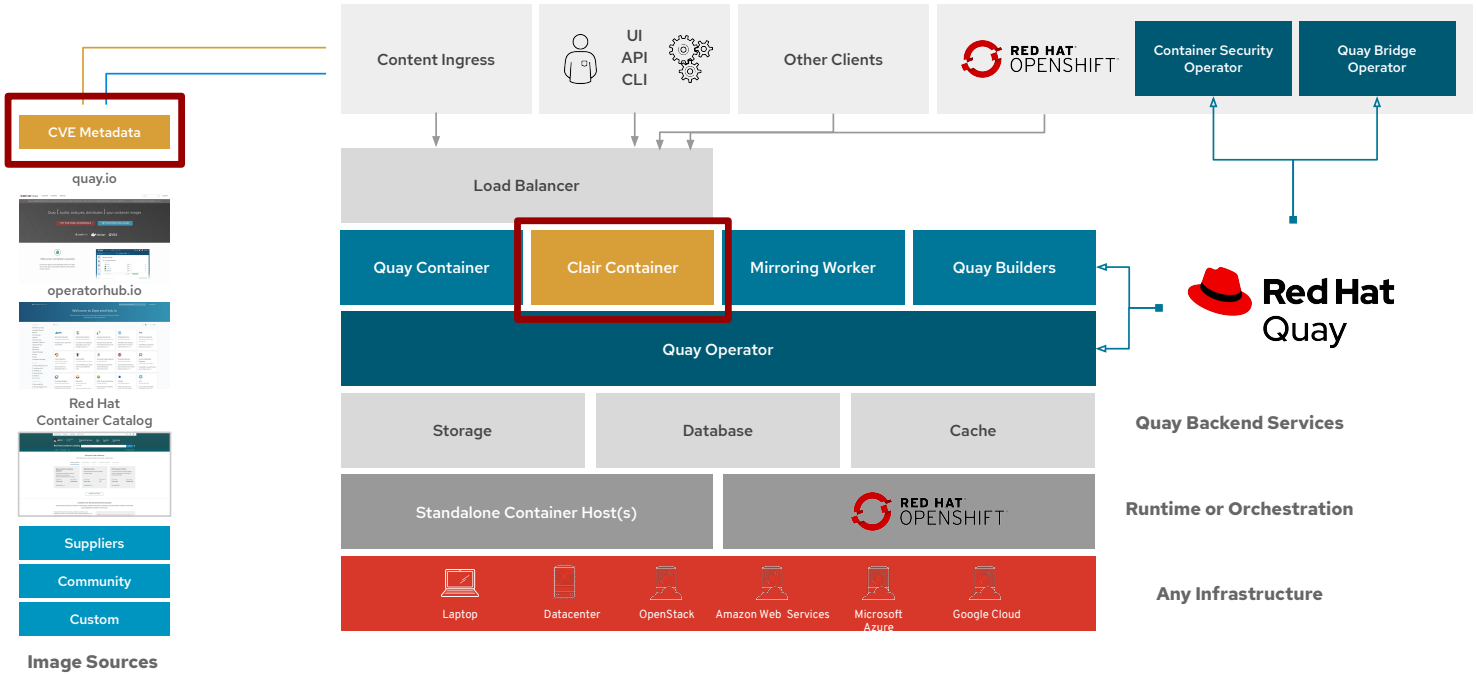
Red Hat Quay

What are the pieces? (Quay Architecture)

Red Hat


CVE Metadata
quay.io
operatorhub.io
Red Hat
Container Catalog
Suppliers
Community
Custom
Image Sources
Content Ingress
UI
API
CLI
Other Clients
RED HAT OPENSHIFT
Container Security Operator
Quay Bridge Operator
Load Balancer
Quay Container
Clair Container
Mirroring Worker
Quay Builders
Quay Operator
Red Hat Quay
Storage
Database
Cache
Quay Backend Services
Standalone Container Host(s)
RED HAT OPENSHIFT
Runtime or Orchestration
Laptop
Datacenter
OpenStack
Amazon Web Services
Microsoft Azure
Google Cloud
Any Infrastructure

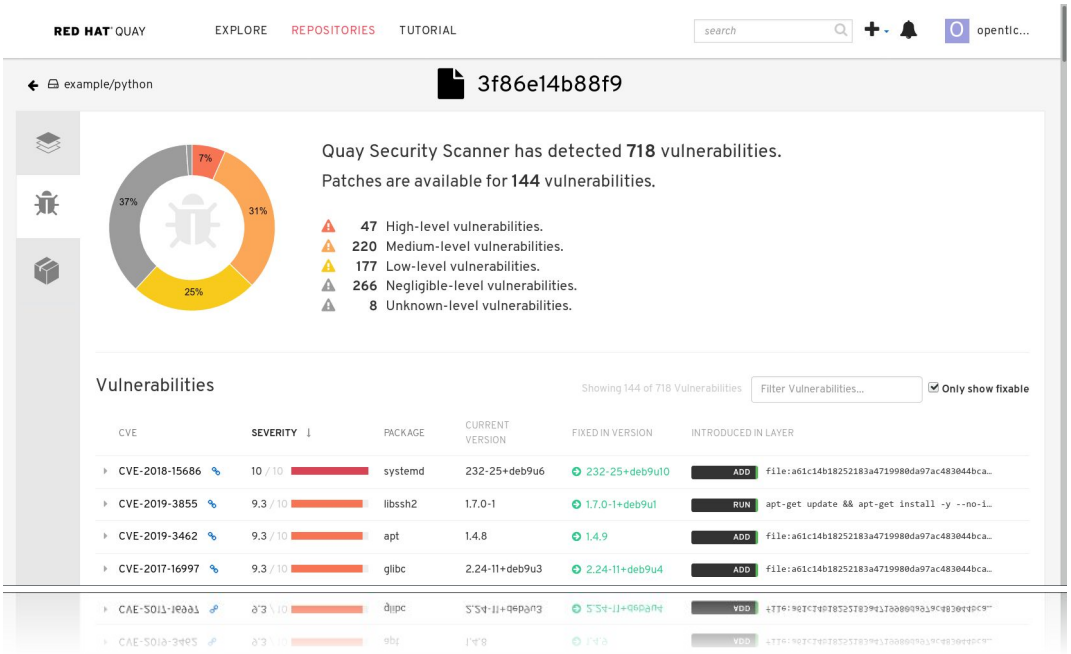
Red Hat


CVE Metadata
quay.io
operatorhub.io
Red Hat
Container Catalog
Suppliers
Community
Custom
Image Sources
Content Ingress
UI
API
CLI
Other Clients
RED HAT OPENSHIFT
Container Security Operator
Quay Bridge Operator
Load Balancer
Quay Container
Clair Container
Mirroring Worker
Quay Builders
Quay Operator
Red Hat Quay
Storage
Database
Cache
Quay Backend Services
Standalone Container Host(s)
RED HAT OPENSHIFT
Runtime or Orchestration
Laptop
Datacenter
OpenStack
Amazon Web Services
Microsoft Azure
Google Cloud
Any Infrastructure

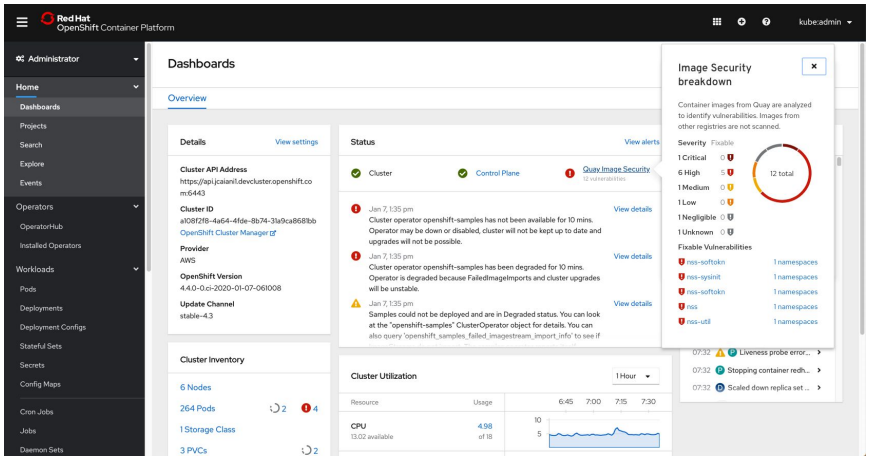
Red Hat

Clair: Integrated Container Vulnerability Scanning

Quay integrates with Clair to **continually scan** your containers for vulnerabilities.



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

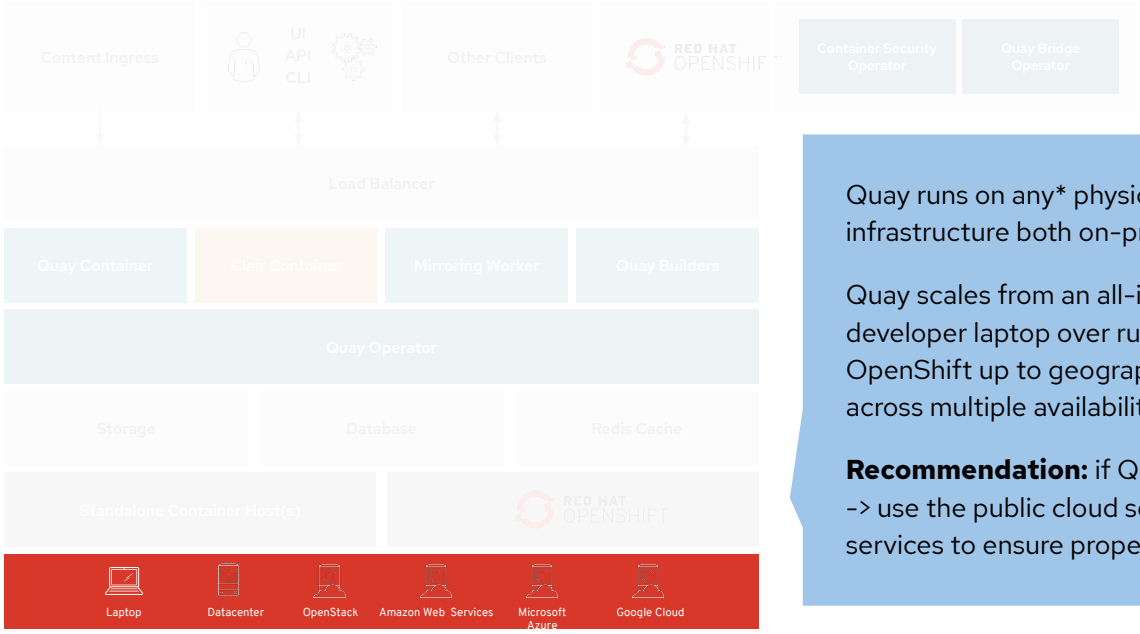
See Clair Vulnerability Data in the OpenShift Console!

We extended the vulnerability information shown inside the OpenShift Console brought to Kubernetes via the Container Security Operator. This includes:

- Image Vulnerabilities Lists in the Administrator section
- Pod View for image vulnerabilities specific to a particular pod
- Enhanced information shown now including severity, advisories and versions
- Affected pods view to show all pods affected by a particular CVE

Red Hat

Underlying 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

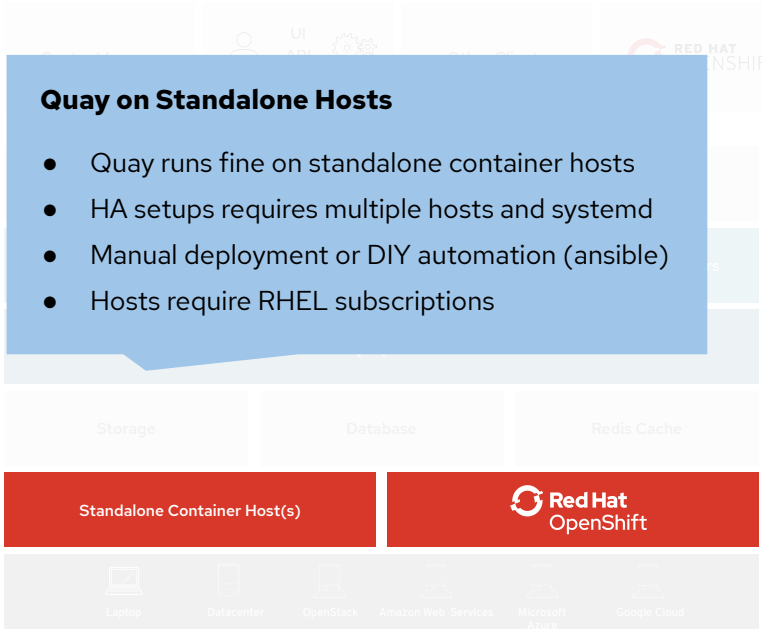
Recommendation: if Quay runs on public cloud -> use the public cloud services for Quay backend services to ensure proper HA and scalability

* 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

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:

- Automated Scaling and updates
- Quay Operator can manage Quay and all dependencies
- Automated deployment and day2 management of Red Hat Quay with customisation options
- Integrate with existing OpenShift processes like GitOps, Monitoring, Alerting, Logging, ...
- Quay can run on OpenShift infra nodes

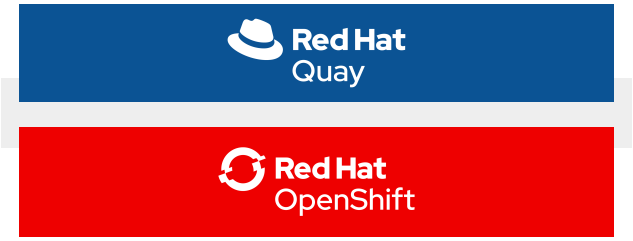
Full list of tested and supported configurations can be found inside the Red Hat Quay Tested Integrations Matrix: https://access.redhat.com/articles/4067991

Red Hat

Red Hat Quay + OpenShift = ♥

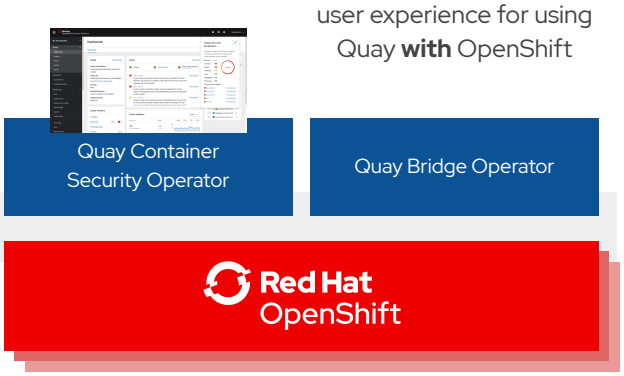
Red Hat Quay runs on any infrastructure but **runs best on OpenShift**

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



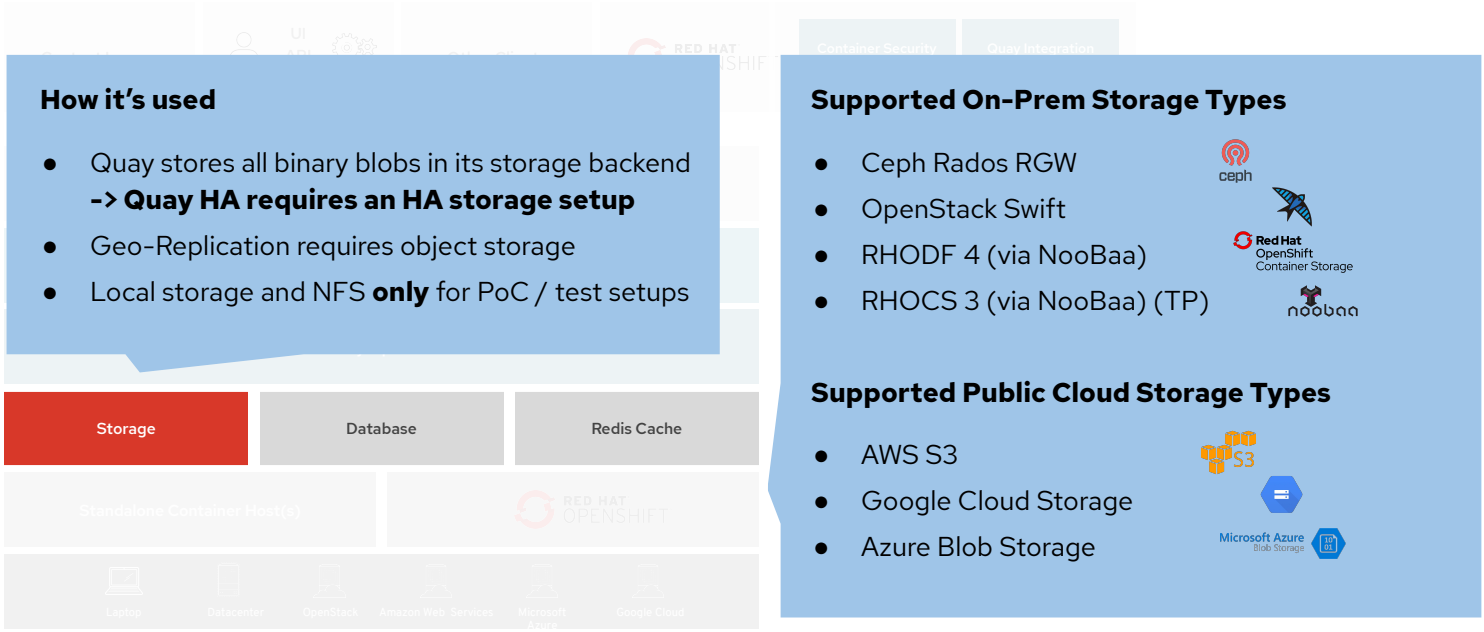
CSO brings Quay / Clair vulnerability data into the OpenShift Console

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



Red Hat

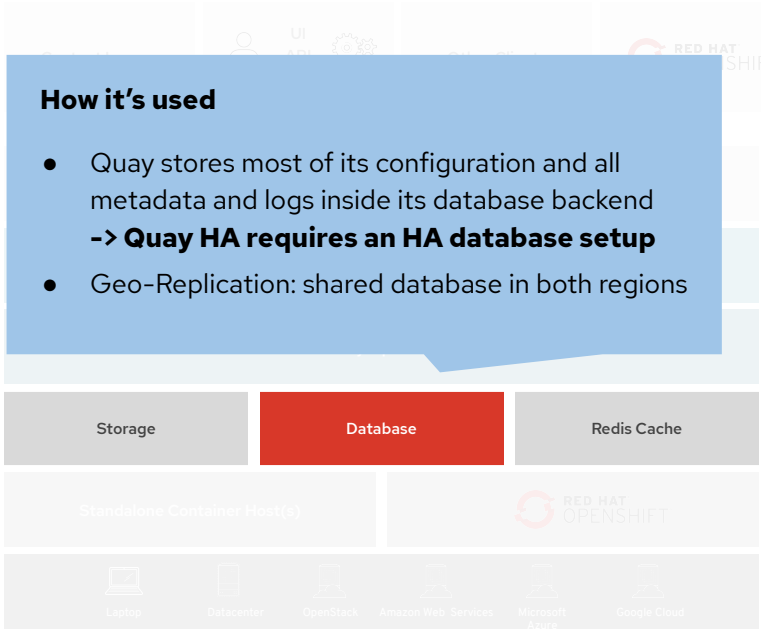
Storage Backend



Note: Technically any S3 compatible storage solution works with Quay and is used by several customers. Support limitations might apply though.
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

Database Backend



How it's used

- Quay stores most of its configuration and all metadata and logs inside its database backend **-> Quay HA requires an HA database setup**
- Geo-Replication: shared database in both regions

- **PostgreSQL** is the preferred database backend since it can be used for both Quay and Clair
- Quay works fine with MySQL too (5.7+)
- If Quay runs on **public cloud infrastructure** we recommend to use the PostgreSQL services provided by your cloud provider
- Typically runs off-cluster but if DB runs on k8s / **OpenShift** we recommend to use an **operator** such as Crunchy Data PostgreSQL Operator
- Logs can be pushed into **ElasticSearch** instead

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

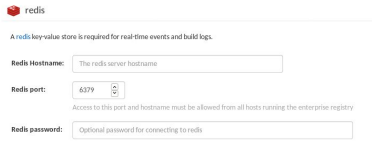
Red Hat

Redis Cache

How it's used

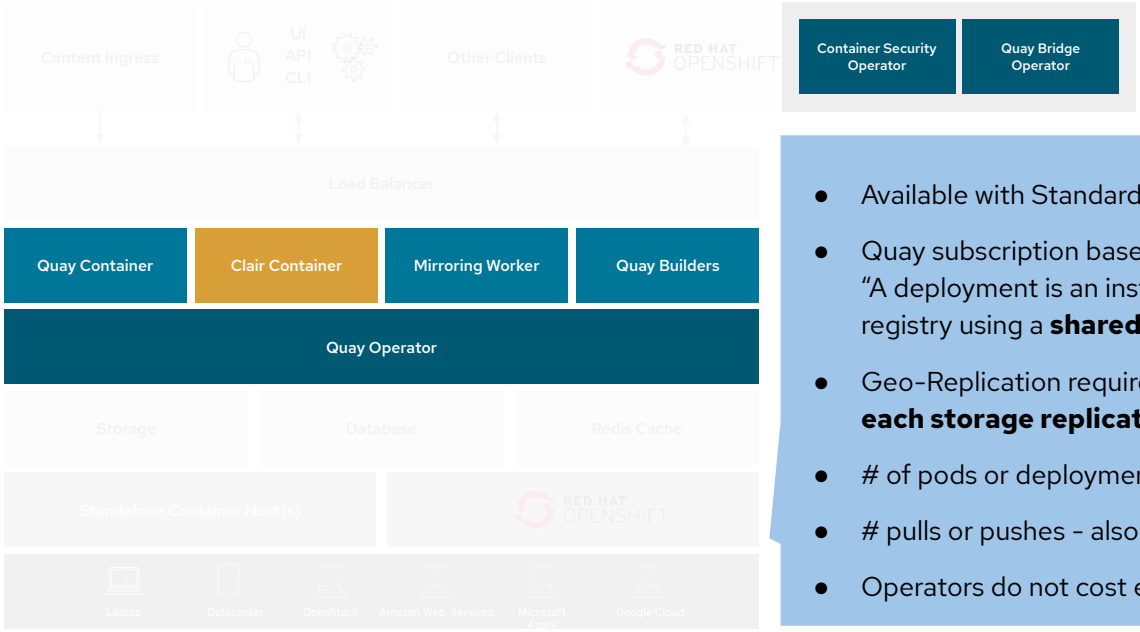
- Quay stores builder logs and the Quay tutorial inside a Redis cache
- Data stored is ephemeral in nature -> Redis does not need to be HA although it's stateful

- Redis via **Red Hat Software Collections** or any other redis works, too
- If Redis goes down you will lose access to:
  - Live build logs
  - Tutorial



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

How Subscriptions Work

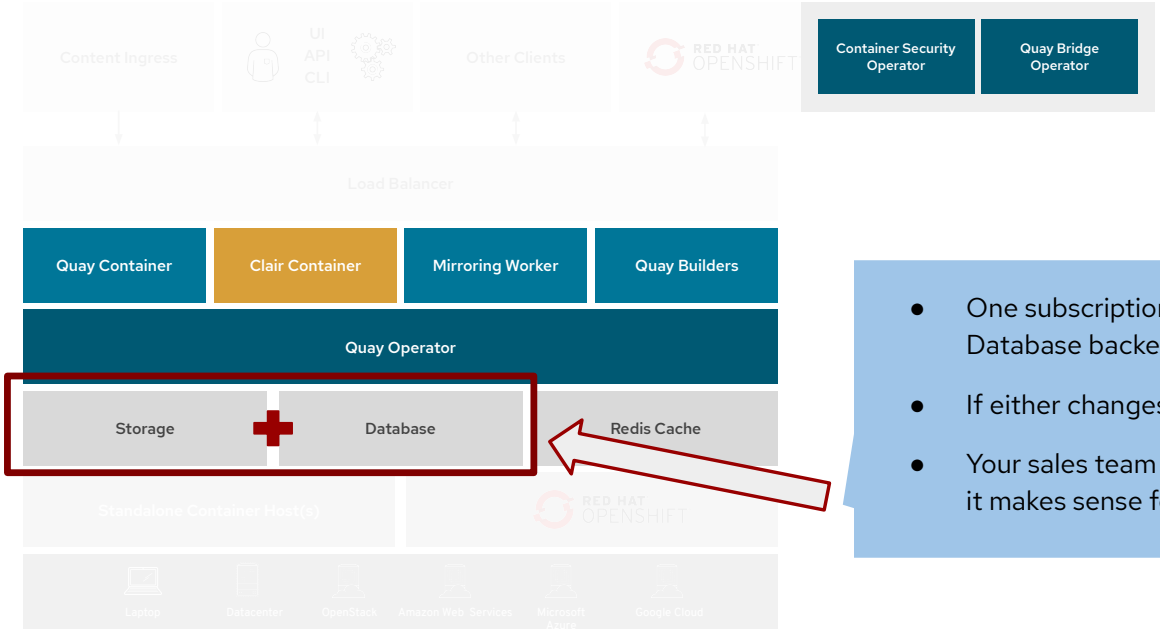


- Available with Standard or Premium Support
- Quay subscription based on a "deployment": "A deployment is an installation of a single Quay registry using a **shared data backend**."
- Geo-Replication requires a subscription for **each storage replication** (database is shared)
- # of pods or deployments of Quay - irrelevant!
- # pulls or pushes - also irrelevant!
- Operators do not cost extra

Red Hat

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

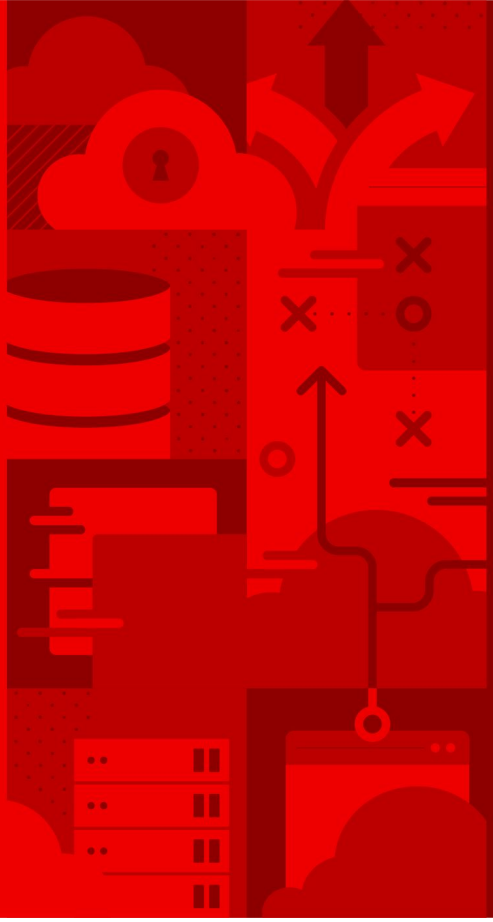
Or, said another way...



- One subscription = Storage backend + Database backend
- If either changes, it's an additional subscription.
- Your sales team can help you figure this out as it makes sense for your use cases!

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

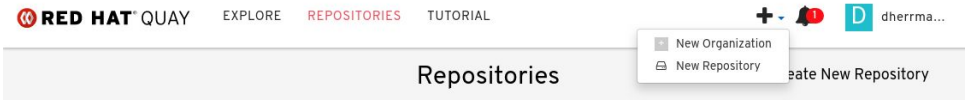


Red Hat Quay

How does it work? (Running Quay + Features)

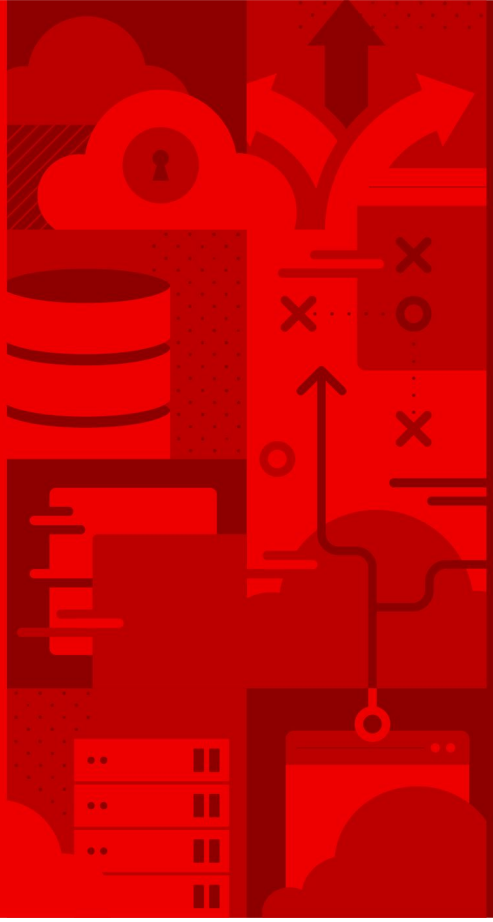
Red Hat

Quay Organizations, Teams, and Robot Accounts



- **Organizations** provide a way of sharing repositories under a common namespace that does not belong to a single user, but rather to many users in a shared setting (such as a division in a company).
- Organizations are organized into a set of **Teams** which provide access to a subset of the repositories under that namespace
- **Robot accounts** are managed inside the Robot Accounts tab and can belong only to **one** organization (but multiple **Teams**) while **Teams** and **Users** can belong to multiple organizations. These are handy for things like mirroring.
- Usage (audit) logs are shown on an organization level for all repositories inside the organization

Red Hat



Red Hat Quay

DEMO TIME!

Red Hat

Red Hat Quay Further Information

Product Docs

- Red Hat Quay Release Notes
- Deploy Red Hat Quay - Basic
- Deploy Red Hat Quay on OpenShift
- Deploy Red Hat Quay on OpenShift with Quay Setup Operator
- Deploy Red Hat Quay - High Availability
- Manage Red Hat Quay
- Upgrade Red Hat Quay
- Use Red Hat Quay
- Red Hat Quay API Guide

Knowledge Base

- Inside the Red Hat Customer Portal many knowledge base articles and solutions can be found around Red Hat Quay
- How to find them: enter your search term and select "Red Hat Quay" as the product
- Optional: preferred content type
- Sample Search URL

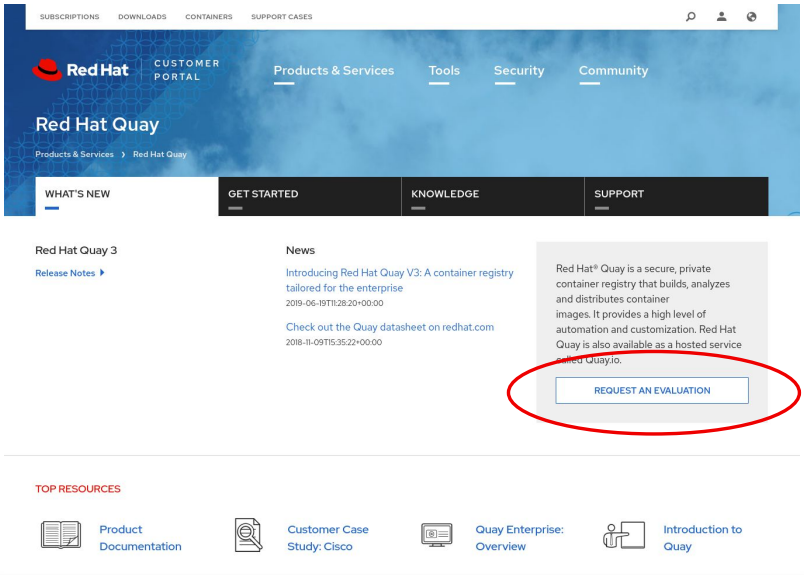
Other Information

- Community Mailing list (Quay SIG)
- Project Quay Community Page
- Source Code (Project Quay)
- Feature Development and Bugtracking in public Quay Jira
- Project Quay on Twitter
- Red Hat Quay.io (Hosted SaaS)

Red Hat

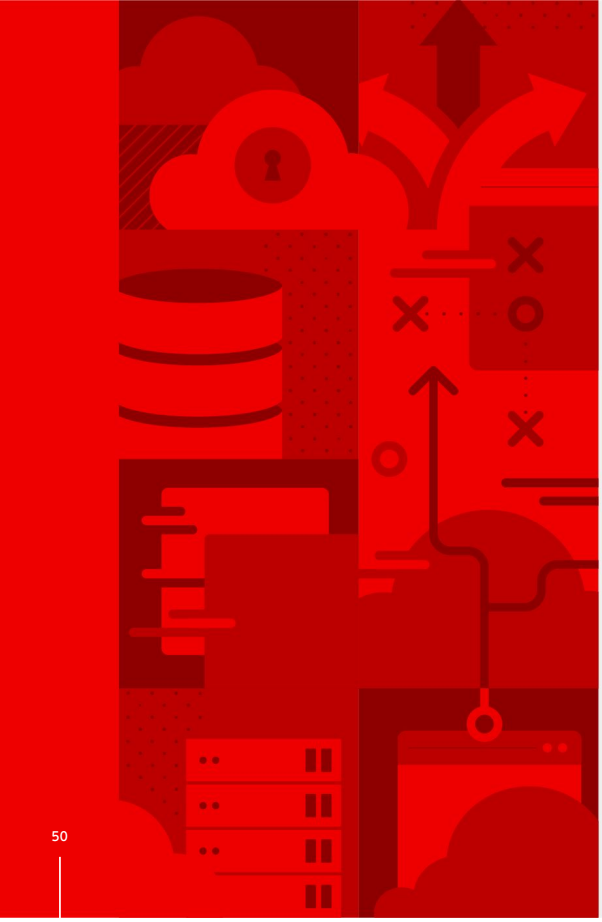
Try it out!

https://access.redhat.com/products/red-hat-quay



On all Quay product pages you can find an evaluation form which grants you access to the software for a 90 day trial period.

Alternatively you can signup **for free** on Quay.io



Thank you!

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat