OpenShift 4.x Architecture Workshop

Enterprise Registry QUAY

QUAY

July 2019

Red Hat

What Is Quay?

- Market leading enterprise container registry
- Available on-premise, on public cloud and as a hosted service (SaaS)
- Key strengths:
  - Security
  - Robustness & speed
  - Automation
- Quay works with any container environment or orchestration platform

RED HAT QUAY

First hosted registry in the market with private repos

2nd biggest hosted registry overall

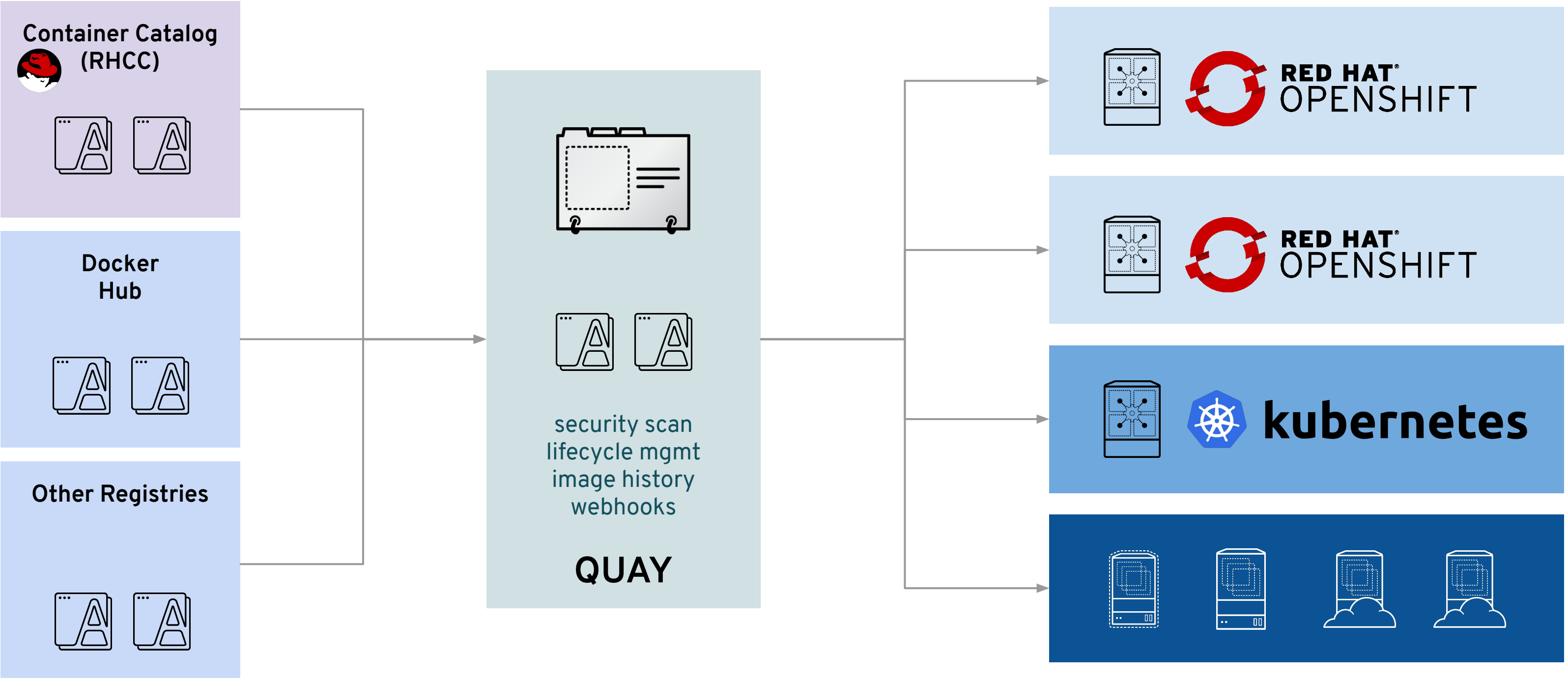
Red Hat Quay Feature Highlights

Security	Robustness and Speed	Automation
Support multiple authentication systems and identity providers	High availability & scalability	Build triggers
Vulnerability scanning	Geo-synchronous replication	Git hook compatible
Encrypted CLI passwords	Continuous, zero-downtime garbage collection	Robot accounts
Detailed logging for auditing	Torrent Distribution	Webhooks
Orgs & team support	Integration with multiple storage backends	Extensible API

Quay Use Cases

- Large-scale and distributed environments (thousands of users and images)
- Customer has multiple OpenShift/Kubernetes clusters (content ingress)
- Customer needs OpenShift/Kubernetes in multiple geographical regions
- Customer needs governance for container images (scanning)
- Customer has high image maintenance and automation requirements
- Large number of build and high requirements on image delivery throughput

Content Ingress with Quay



Container Catalog (RHCC)

Docker Hub

Other Registries

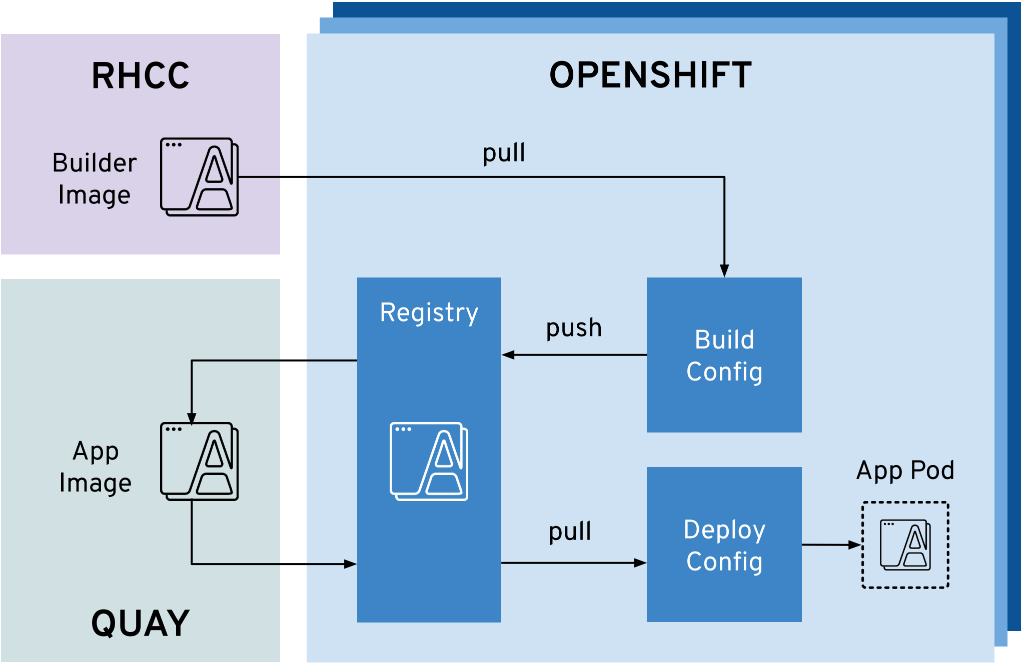
security scan
lifecycle mgmt
image history
webhooks

QUAY

Quay as Upstream Registry with OpenShift

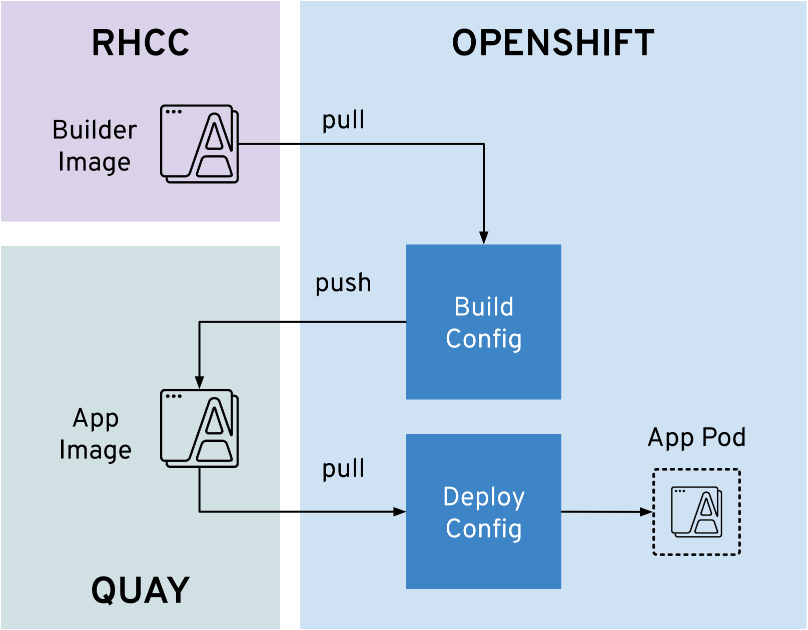
- Images pulled from Quay into the integrated OpenShift registry

- Images are pushed to the integrated OpenShift registry, and synced externally with Quay



Quay as OpenShift Registry

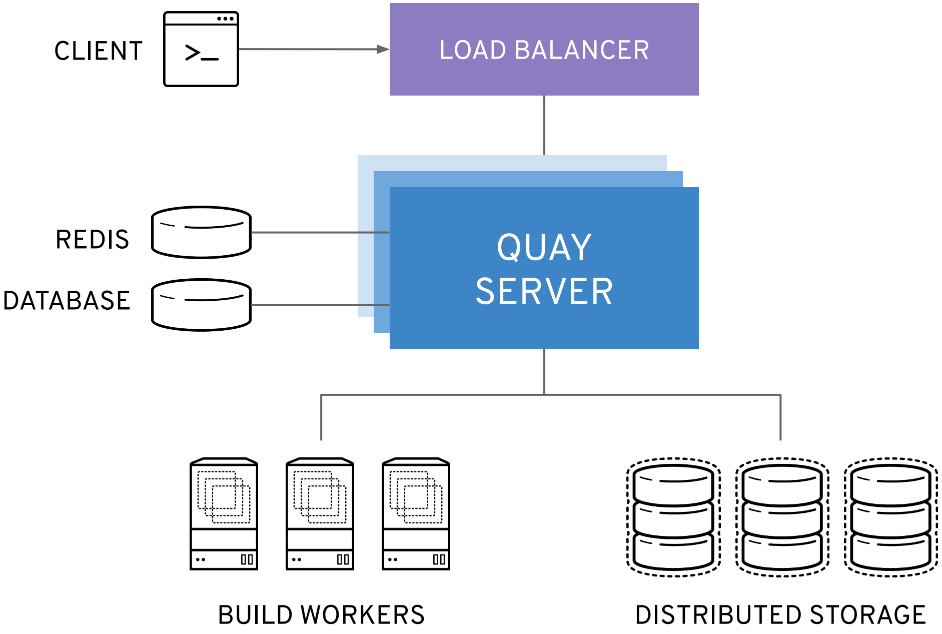
- Images are pushed directly by builds to Quay
- Images are pulled directly from Quay



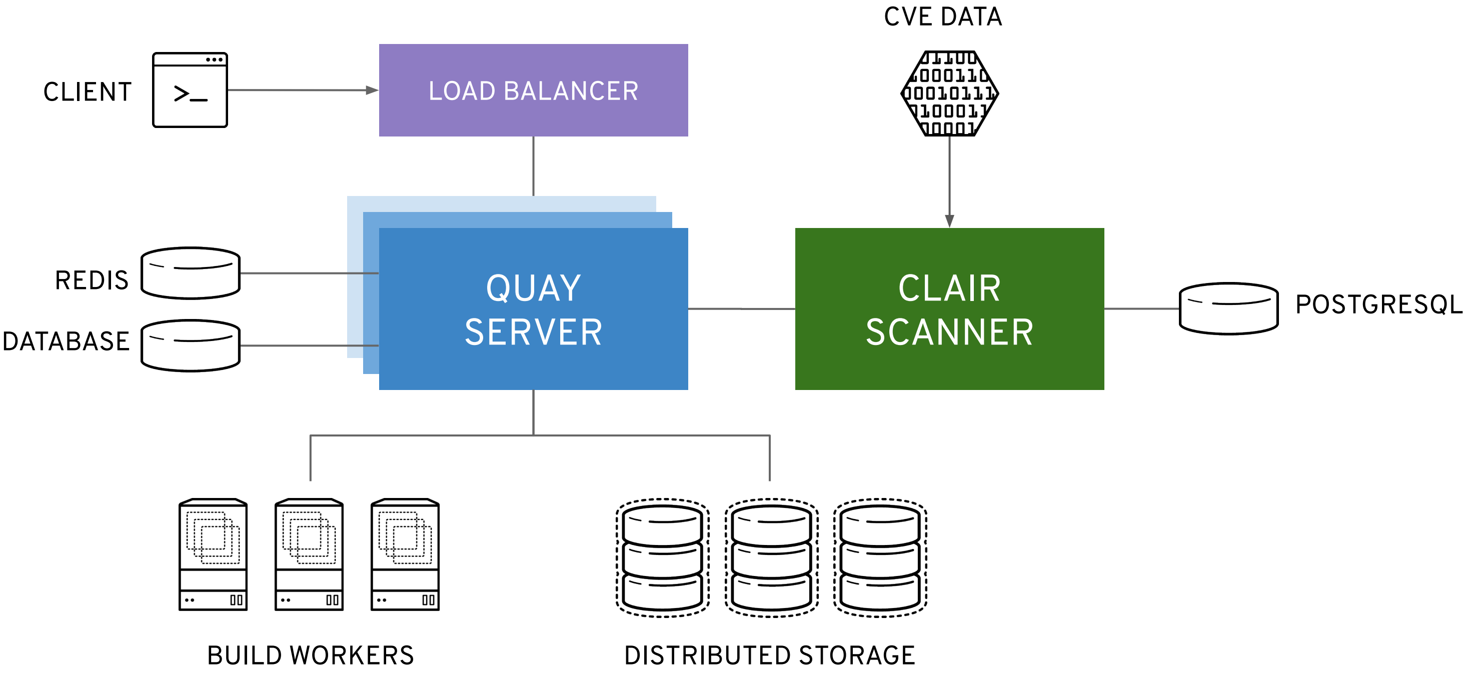
Red Hat

Quay Architecture

Quay Architecture



Quay Architecture with Image Scanning



Underlying Infrastructures Quay can run

- Quay can run on
  - standalone container host
  - (Tectonic) / Kubernetes / OpenShift
- Quay runs on any public cloud infrastructure as well
  - Quay.io runs on AWS
- Reference Architectures in planning

Azure

Google Cloud

openstack

aws

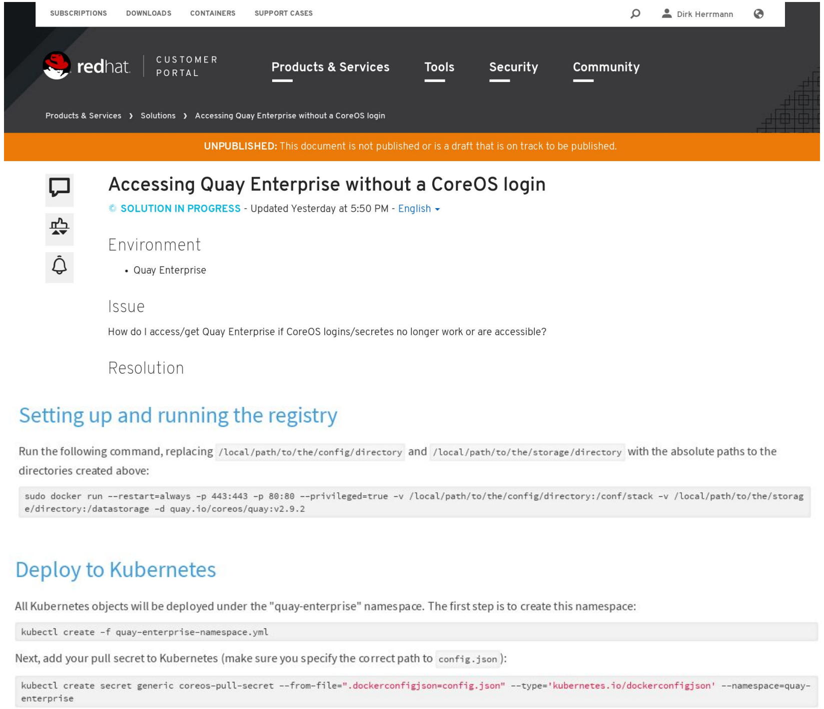
Underlying Infrastructure

- Quay is shipped as container images
  - Images are distributed via Quay.io (will move to RHCC later)
  - Required secret to pull them in customer portal (requires login)

https://access.redhat.com/solutions/3533201

- Install procedure documentation at

https://access.redhat.com/documentation/en-us/red_hat_quay/2.9/



UNPUBLISHED: This document is not published or is a draft that is on track to be published.

Accessing Quay Enterprise without a CoreOS login

SOLUTION IN PROGRESS - Updated Yesterday at 5:50 PM - English

Environment

- Quay Enterprise

Issue

How do I access/get Quay Enterprise if CoreOS logins/secretes no longer work or are accessible?

Resolution

Setting up and running the registry

Run the following command, replacing `/local/path/to/the/config/directory` and `/local/path/to/the/storage/directory` with the absolute paths to the directories created above:

```
sudo docker run --restart=always -p 443:443 -p 80:80 --privileged=true -v /local/path/to/the/config/directory:/conf/stack -v /local/path/to/the/storag
e/directory:/datastorage -d quay.io/coreos/quay:v2.9.2
```

Deploy to Kubernetes

All Kubernetes objects will be deployed under the "quay-enterprise" namespace. The first step is to create this namespace:

```
kubectl create -f quay-enterprise-namespace.yml
```

Next, add your pull secret to Kubernetes (make sure you specify the correct path to `config.json`):

```
kubectl create secret generic coreos-pull-secret --from-file=".dockerconfigjson=config.json" --type='kubernetes.io/dockerconfigjson' --namespace=quay-
enterprise
```

Running Quay on OpenShift

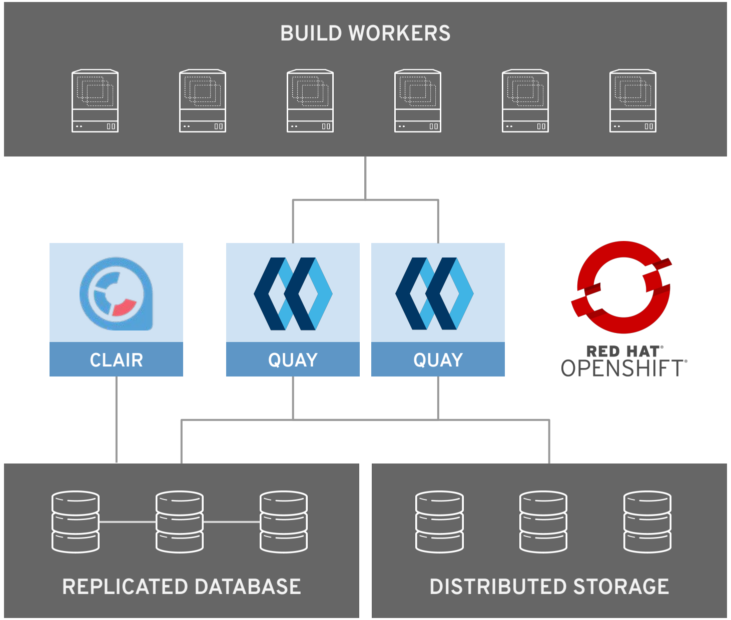
Quay on OpenShift: Recommended Setup

On OpenShift Cluster:

- Quay Enterprise
- Clair

Outside OpenShift cluster:

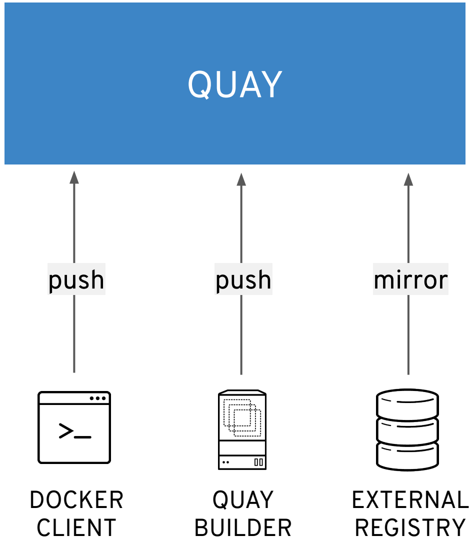
- Database
- Storage
- Builders



Getting Images into QUAY

Getting Images into Quay Registry

- Multiple ways to get images into Quay
  - Push images to Quay
  - Quay builders
  - Repository mirroring (coming soon)
- Any compliant Docker client can push images into Quay
  - OpenShift build config
  - Docker CLI
  - Skopeo (recommended)



Clair

Clair Vulnerability Scanning

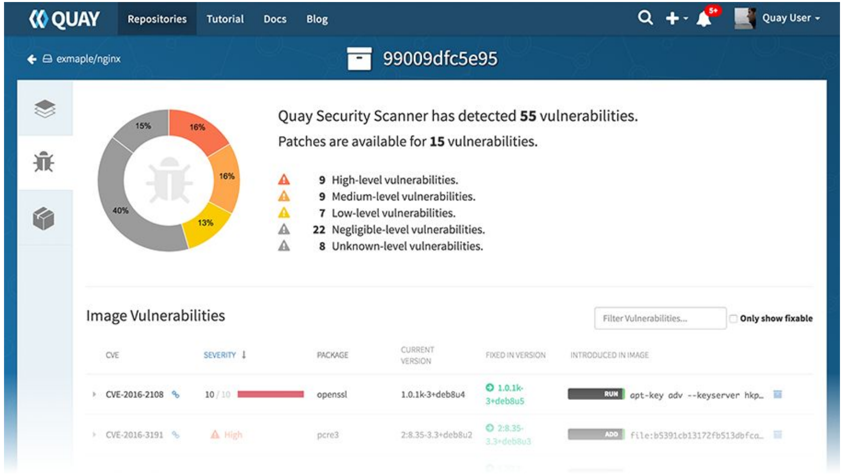
clair

Complete Visibility into known vulnerabilities and how to fix them

Description: Quay integrates with Clair to continually scans your containers for vuln’s.

How it Works:

- Static analysis of vulnerabilities
- Multiple drivers and data sources
- Synchronous update of vuln metadata
- New vuln’s trigger notifications
- Rich Clair API
- Can run single-instance or HA



99009dfc5e95

Quay Security Scanner has detected **55** vulnerabilities.

Patches are available for **15** vulnerabilities.

⚠ 9 High-level vulnerabilities.
⚠ 9 Medium-level vulnerabilities.
⚠ 7 Low-level vulnerabilities.
⚠ 22 Negligible-level vulnerabilities.
⚠ 8 Unknown-level vulnerabilities.

Image Vulnerabilities

Filter Vulnerabilities... □ Only show fixable

CVE	SEVERITY ↓	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN IMAGE
CVE-2016-2108	10 / 10	openssl	1.0.1k-3+deb8u4	1.0.1k-3+deb8u5	RUN apt-key adv --keyserver hkp…
CVE-2016-3191	⚠ High	pcre3	2:8.35-3.3+deb8u2	2:8.35-3.3+deb8u3	ADD file:b5391cb13172fb513dbfca…

Red Hat

Thank you !