



CONTAINER REGISTRIES

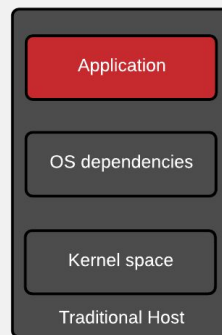
REGISTRY SERVERS

Better than virtual appliance market places :-)

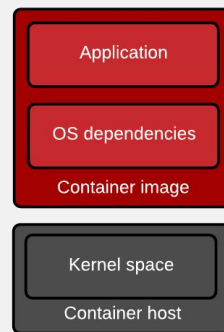
Defines a standard way to:

- Find images
- Run images
- Build new images
- Share images
- Pull images
- Introspect images
- Shell into running container
- Etc, etc, etc

-  Optimized for agility
-  Optimized for stability



Application & infrastructure
updates tightly coupled



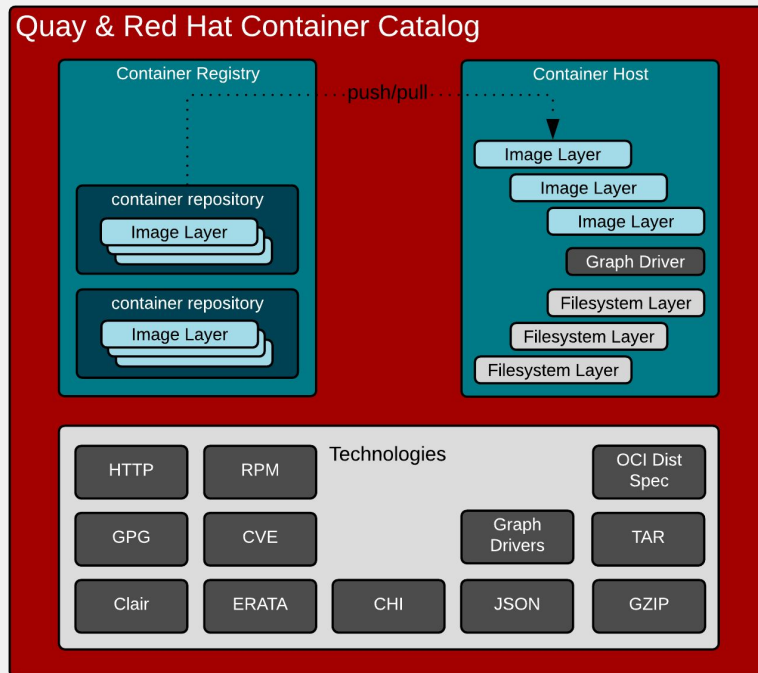
Application & infrastructure
updates loosely coupled

CONTAINER REGISTRY & STORAGE

Mapping image layers

Covering push, pull, and registry:

- Rest API (blobs, manifest, tags)
- Image Scanning (clair)
- CVE Tracking (errata)
- Scoring (Container Health Index)
- Graph Drivers (overlay2, dm)
- Responsible for maintaining chain of custody for secure images from registry to container host

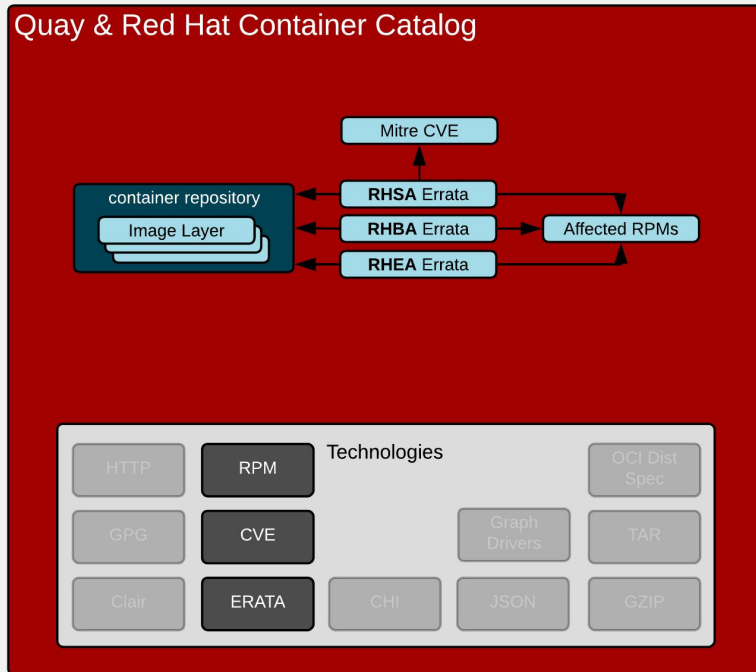


START WITH QUALITY REPOSITORIES

Repositories depend on good packages

Determining the quality of repository requires meta data:

- Errata is simple to explain, hard to build
 - Security Fixes
 - Bug Fixes
 - Enhancements
- Per container images layer (tag), often maps to multiple packages



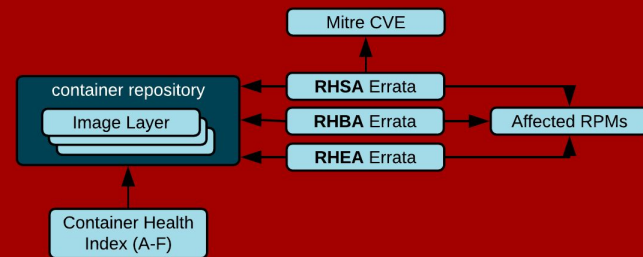
SCORING REPOSITORIES

Images age like cheese, not like wine

Based on severity and age of Security
Errata:

- Trust is temporal
- Even good images go bad over time because the world changes around you

Quay & Red Hat Container Catalog

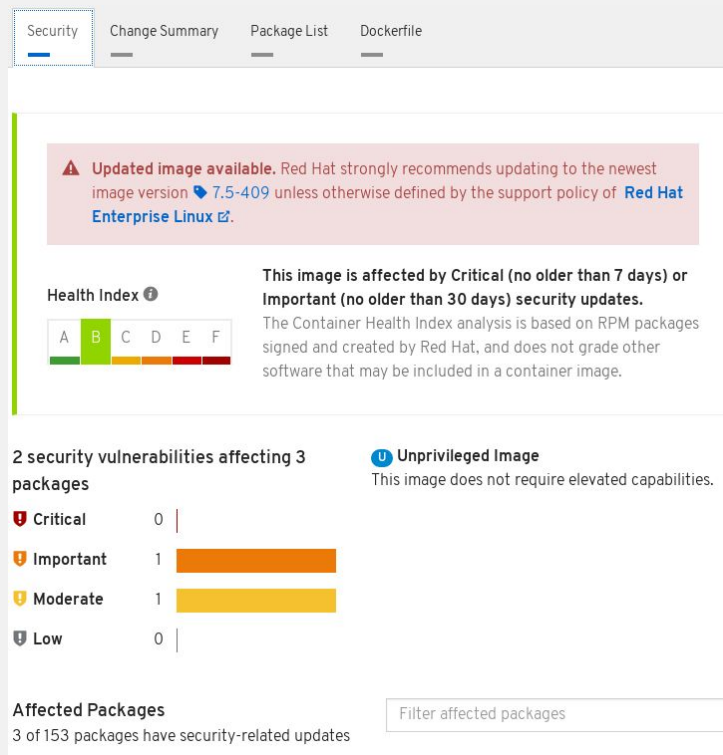


SCORING REPOSITORIES

Container Health Index

Based on severity and age of Security
Errata:

- Trust is temporal
- Images must constantly be rebuilt to maintain score of “A”

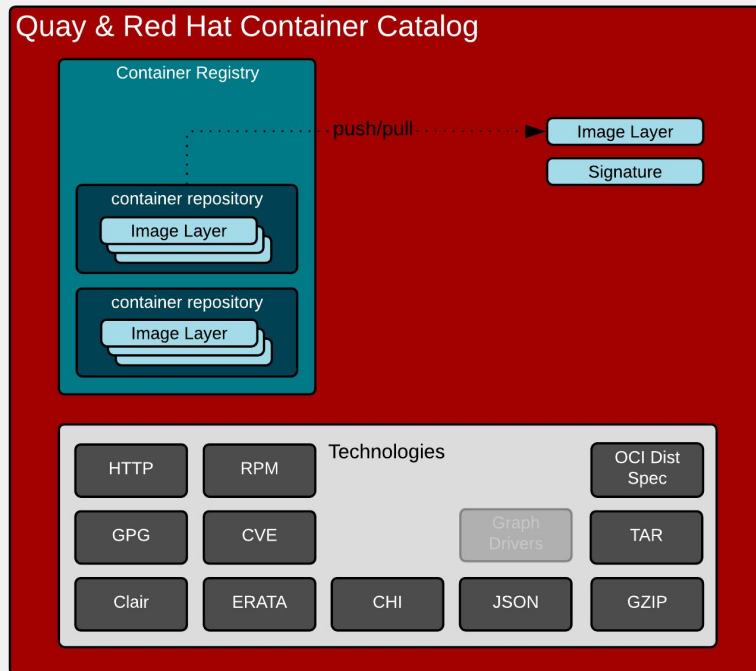


PUSH, PULL & SIGNING

Signing and verification before/after transit

Registry has all of the image layers and can have the signatures as well:

- Download trusted thing
- Download from trusted source
- Neither is sufficient by itself



PUSH, PULL & SIGNING

Mapping image layers

Command:

```
docker pull registry.access.redhat.com/rhel7/rhel:latest
```

Decomposition:

access.registry.redhat.com

/

rhel7

/

rhel

:

latest

Generalization:

Registry Server

/

namespace

/

repo

:

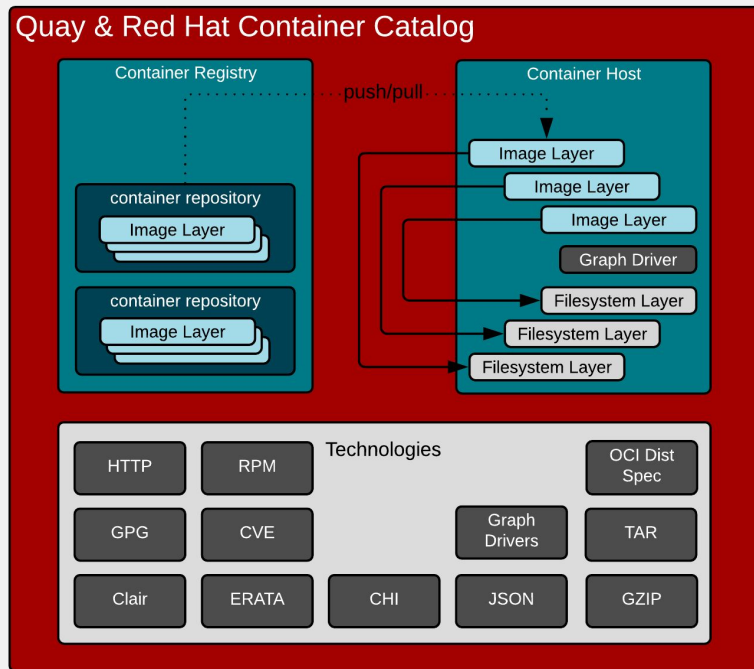
tag

GRAPH DRIVERS

Mapping layers uses file system technology

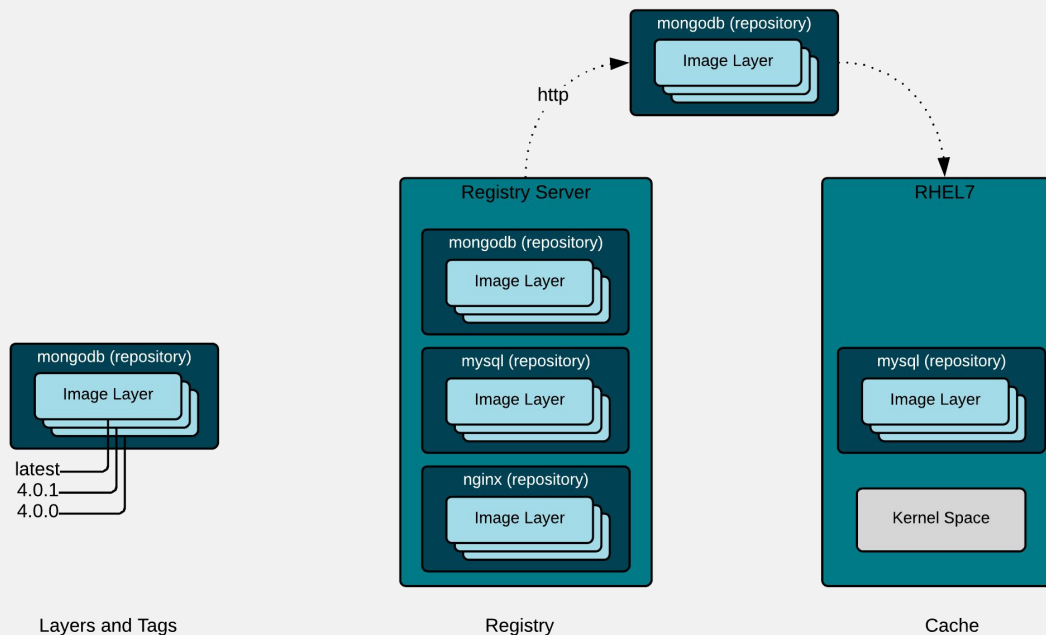
Local cache maps each layer to volume or filesystem layer:

- Overlay2 file system and container engine driver
- Device Mapper volumes and container engine driver



PUSH, PULL & SIGNING

Mapping image layers



CONTAINER REGISTRY & STORAGE

Mapping image layers

Covering push, pull, and registry:

- Rest API (blobs, manifest, tags)
- Image Scanning (clair)
- CVE Tracking (errata)
- Scoring (Container Health Index)
- Graph Drivers (overlay2, dm)
- Responsible for maintaining chain of custody for secure images from registry to container host

