RED HAT SUMMIT

BEST PRACTICES FOR SECURING THE CONTAINER LIFECYCLE

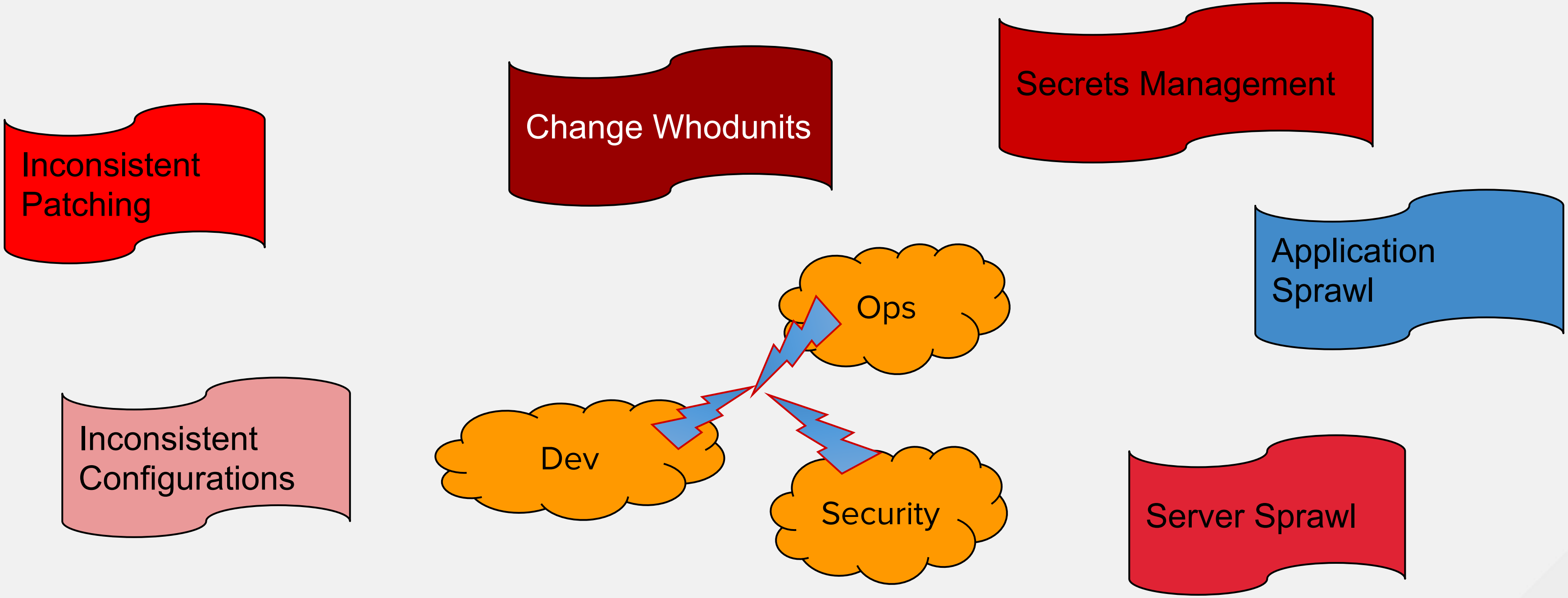
Improving Security with Containers

Laurent Domb, Principal Cloud Solutions Architect
Kirsten Newcomer, OpenShift Product Management

May 2018

NOTHING IS TRULY SECURE BY DEFAULT

COMMON SECURITY CHALLENGES



Inconsistent Patching

Change Whodunits

Secrets Management

Application Sprawl

Ops

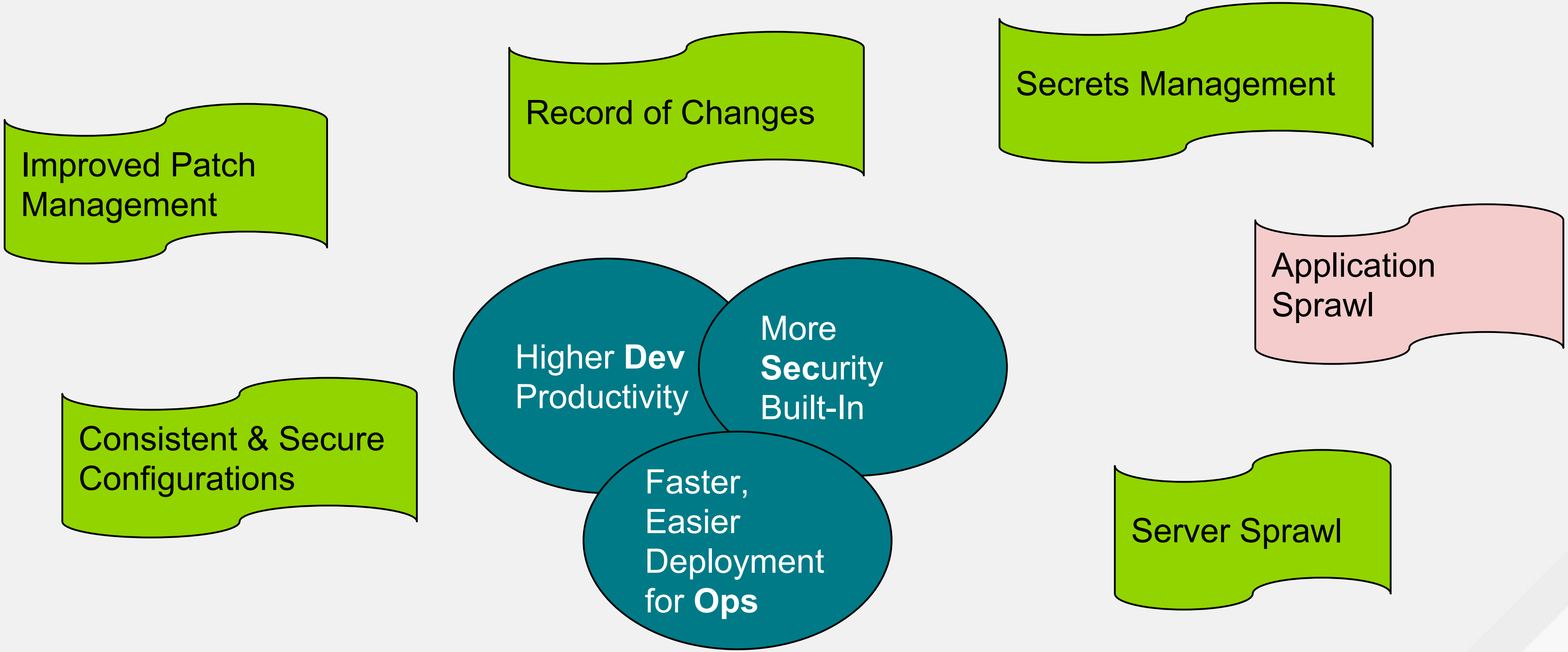
Dev

Security

Inconsistent Configurations

Server Sprawl

IMPROVED SECURITY WITH CONTAINERS



Improved Patch Management

Record of Changes

Secrets Management

Application Sprawl

Higher **Dev** Productivity

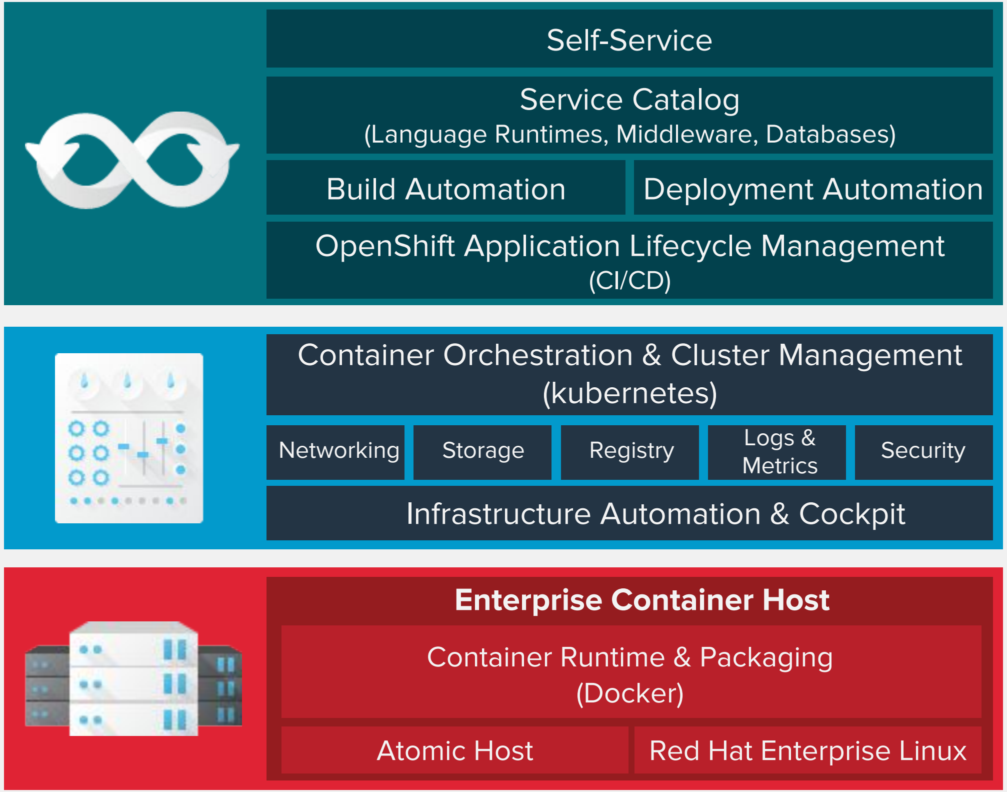
More **Security** Built-In

Faster, Easier Deployment for **Ops**

Consistent & Secure Configurations

Server Sprawl

ELEMENTS OF AN ENTERPRISE CONTAINER SOLUTION



Self-Service

Service Catalog
(Language Runtimes, Middleware, Databases)

Build Automation | Deployment Automation

OpenShift Application Lifecycle Management
(CI/CD)

Container Orchestration & Cluster Management
(kubernetes)

Networking | Storage | Registry | Logs & Metrics | Security

Infrastructure Automation & Cockpit

Enterprise Container Host

Container Runtime & Packaging
(Docker)

Atomic Host | Red Hat Enterprise Linux

AUTOMATED & INTEGRATED SECURITY

CONTROL

Application Security

- Container Content
- CI/CD Pipeline
- Container Registry
- Deployment Policies

DEFEND

Infrastructure

- Container Platform
- Container Host Multi-tenancy
- Network Isolation
- Storage
- Audit & Logging
- API Management

EXTEND

- Security Ecosystem

CONTROL

Secure the Pipeline & the Applications

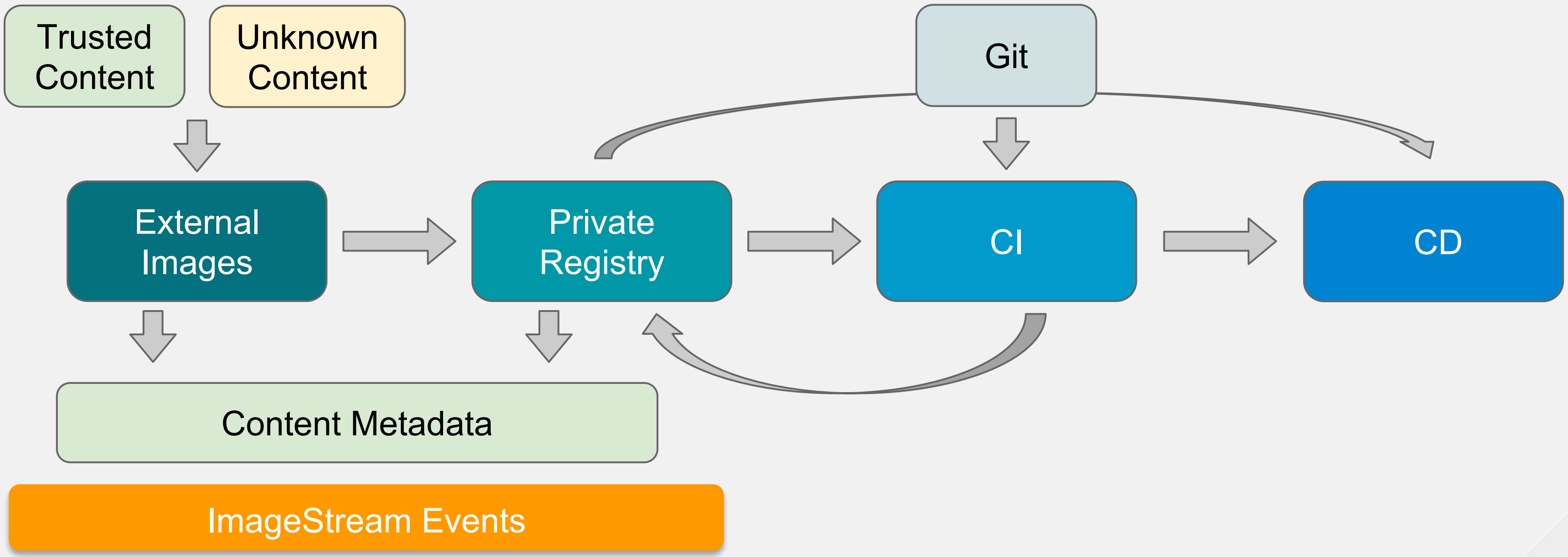
Container Content

CI/CD Pipeline

Container Registry

Deployment Policies

SECURE THE CONTAINER LIFECYCLE



Trusted Content

Unknown Content

Git

External Images

Private Registry

CI

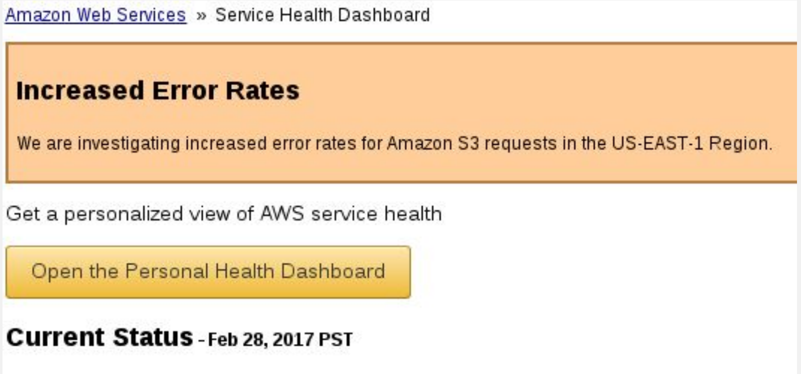
CD

Content Metadata

ImageStream Events

External Images

IS YOUR REGISTRY SECURE & AVAILABLE?

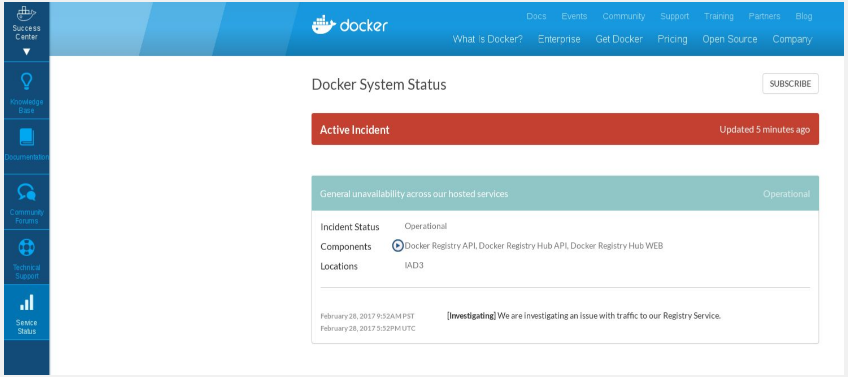

Amazon Web Services » Service Health Dashboard

Increased Error Rates

We are investigating increased error rates for Amazon S3 requests in the US-EAST-1 Region.

Get a personalized view of AWS service health

Current Status - Feb 28, 2017 PST



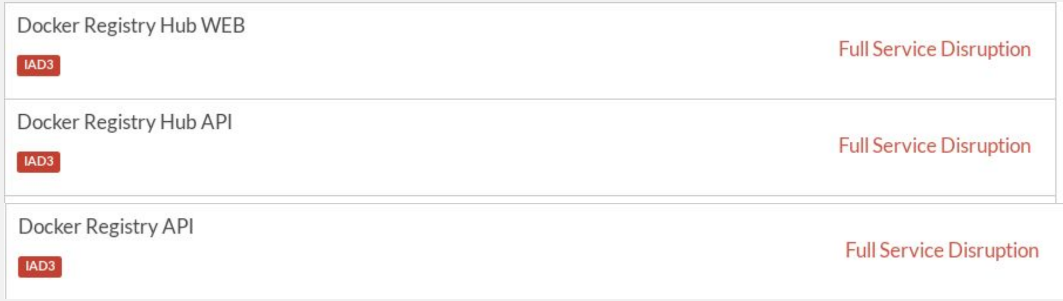
Docker System Status

Active Incident — Updated 5 minutes ago

General unavailability across our hosted services — Operational

Incident Status	Operational
Components	Docker Registry API, Docker Registry Hub API, Docker Registry Hub WEB
Locations	IAD3

February 28, 2017 9:52AM PST
February 28, 2017 5:52PM UTC
[Investigating] We are investigating an issue with traffic to our Registry Service.

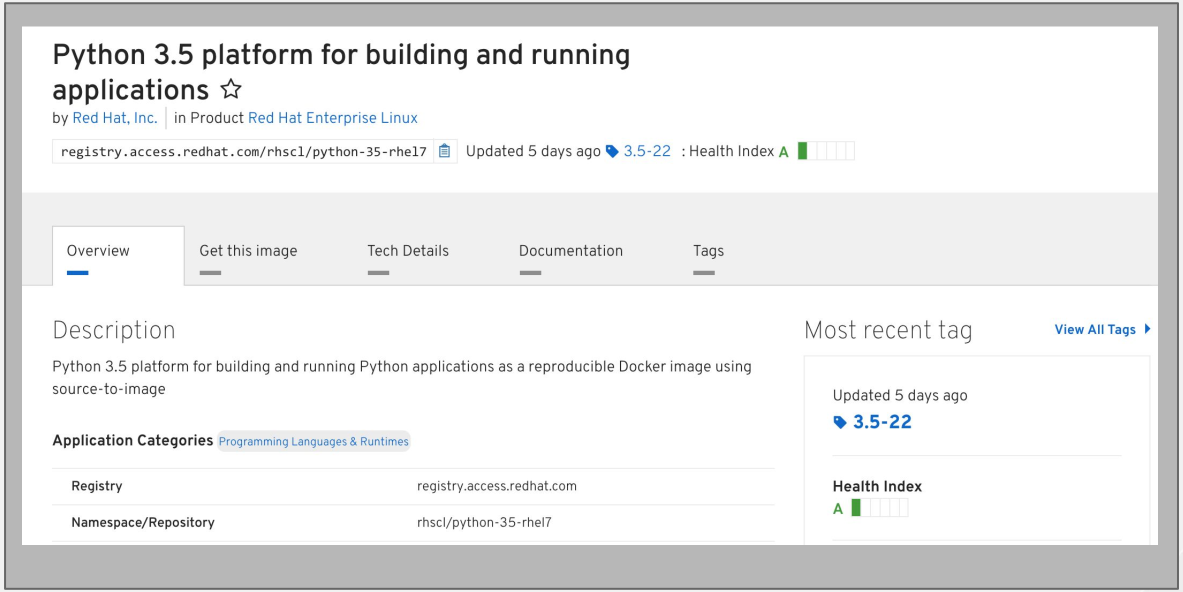


Docker Registry Hub WEB IAD3	Full Service Disruption
Docker Registry Hub API IAD3	Full Service Disruption
Docker Registry API IAD3	Full Service Disruption

External Images

CONTENT: USE TRUSTED SOURCES

- Are the container images signed?
- Are the runtime and OS layers up to date?
- How frequently will the container be updated and how will I know when it's updated?



Python 3.5 platform for building and running applications ☆

by Red Hat, Inc. | in Product Red Hat Enterprise Linux

`registry.access.redhat.com/rhscl/python-35-rhel7` Updated 5 days ago 3.5-22 : Health Index A

Description

Python 3.5 platform for building and running Python applications as a reproducible Docker image using source-to-image

Application Categories Programming Languages & Runtimes

Registry	registry.access.redhat.com
Namespace/Repository	rhscl/python-35-rhel7

Most recent tag

Updated 5 days ago

3.5-22

Health Index

A

Red Hat rebuilds container images when security fixes are released

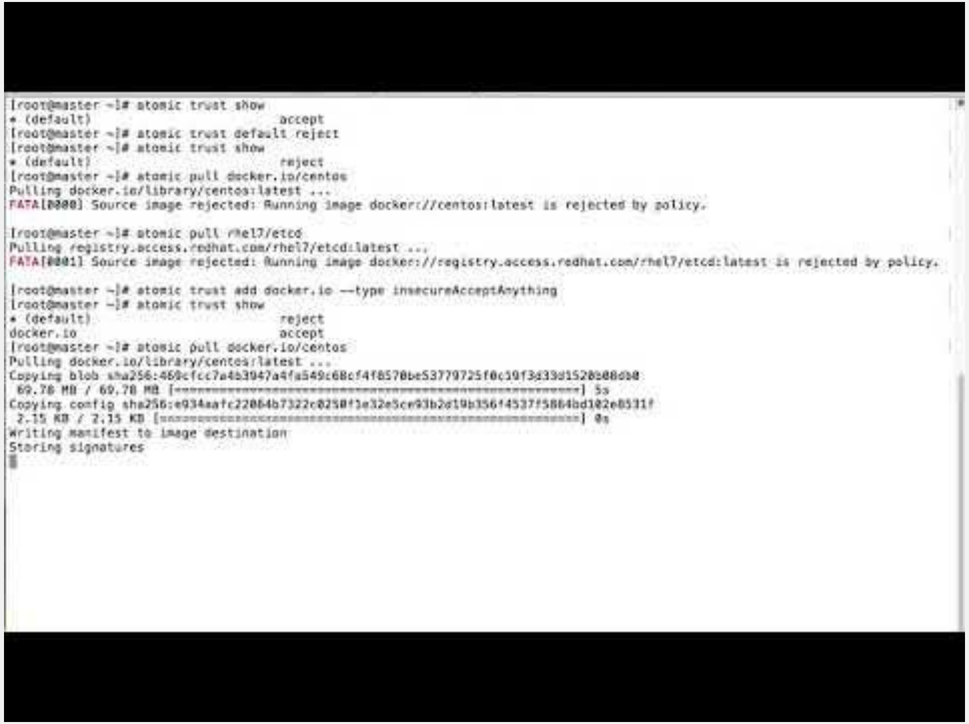
External Images

CONTENT: SIGNED IMAGES FROM TRUSTED SOURCES / RED HAT

- Cryptographically verifying that images have come from Red Hat
  - Assure authorship and integrity
  - Enable non-repudiation
  - Red Hat images are signed using Hardware Security Modules (HSMs)

External Images

DEMO: RESTRICT REGISTRY ACCESS



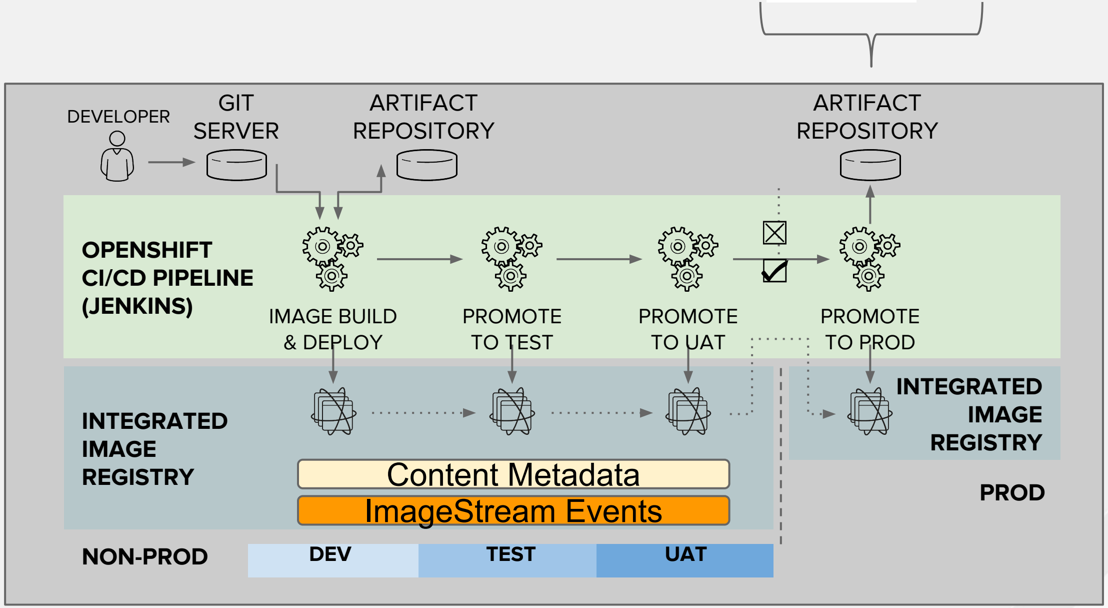
```
[root@master ~]# atomic trust show
* (default)                             accept
[root@master ~]# atomic trust default reject
[root@master ~]# atomic trust show
* (default)                             reject
[root@master ~]# atomic pull docker.io/centos
Pulling docker.io/library/centos:latest ...
FATA[0000] Source image rejected: Running image docker://centos:latest is rejected by policy.

[root@master ~]# atomic pull rhel7/etcd
Pulling registry.access.redhat.com/rhel7/etcd:latest ...
FATA[0001] Source image rejected: Running image docker://registry.access.redhat.com/rhel7/etcd:latest is rejected by policy.

[root@master ~]# atomic trust add docker.io --type insecureAcceptAnything
[root@master ~]# atomic trust show
* (default)                             reject
docker.io                               accept
[root@master ~]# atomic pull docker.io/centos
Pulling docker.io/library/centos:latest ...
Copying blob sha256:469cfcc7a4b3947a4fa549c68cf4f8570be53779725f0c19f3d33d1528b88db8
 69.78 MB / 69.78 MB [=======================================================] 5s
Copying config sha256:e934aafc22064b7322c0250f1e32e5ce93b2d19b356f4537f5864bd102e8531f
 2.15 KB / 2.15 KB [=========================================================] 0s
Writing manifest to image destination
Storing signatures
```

Private Registry

PRIVATE REGISTRIES: SECURE ACCESS TO IMAGES

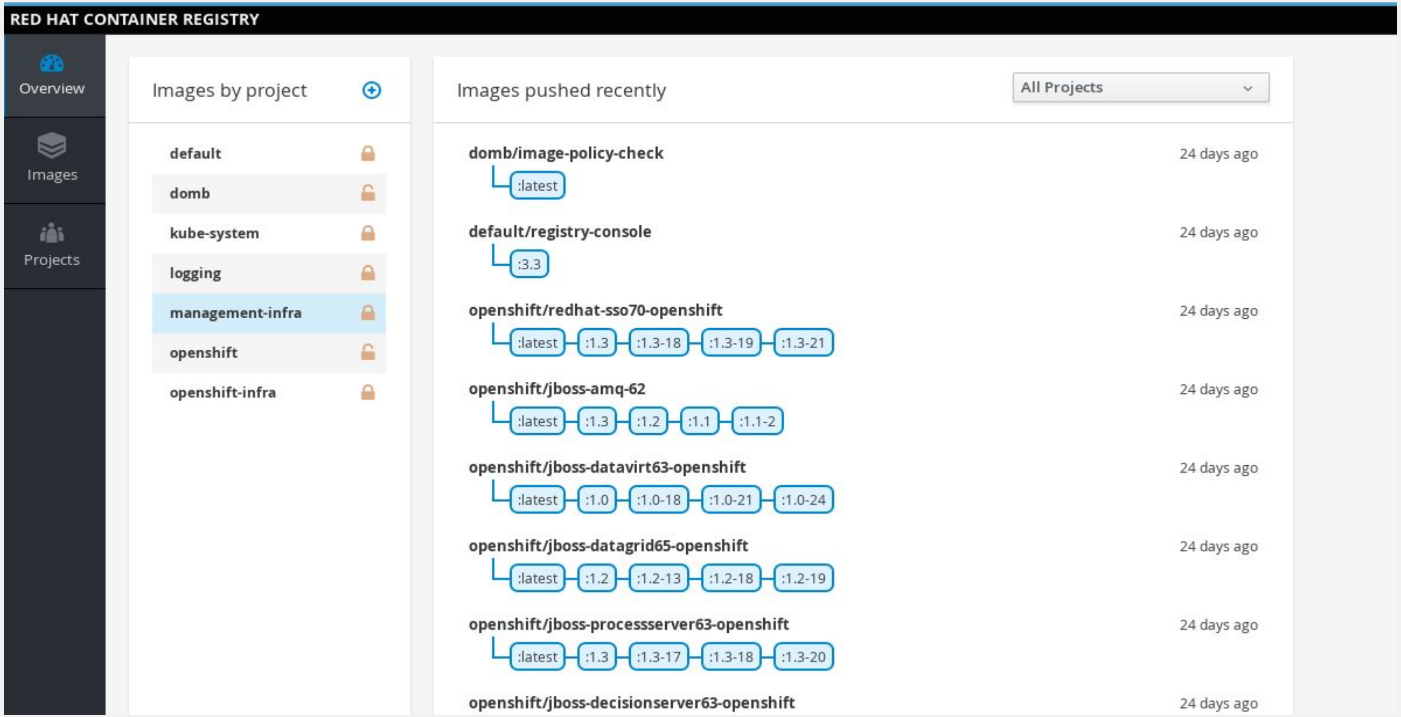
QUAY
Sonatype
JFrog Artifactory
archiva

- Manage access to and promotion of images
- Metadata to automate policies for approved use (e.g. dev, test, UAT, production)
- Monitor changes to external sources
- Manage image signatures for your custom containers



Private Registry

OPENSHIFT INTEGRATED CONTAINER REGISTRY: LOCAL AND SECURE



RED HAT CONTAINER REGISTRY

Images by project

- default
- domb
- kube-system
- logging
- management-infra
- openshift
- openshift-infra

Images pushed recently

All Projects

domb/image-policy-check :latest	24 days ago
default/registry-console :3.3	24 days ago
openshift/redhat-sso70-openshift :latest :1.3 :1.3-18 :1.3-19 :1.3-21	24 days ago
openshift/jboss-amq-62 :latest :1.3 :1.2 :1.1 :1.1-2	24 days ago
openshift/jboss-datavirt63-openshift :latest :1.0 :1.0-18 :1.0-21 :1.0-24	24 days ago
openshift/jboss-datagrid65-openshift :latest :1.2 :1.2-13 :1.2-18 :1.2-19	24 days ago
openshift/jboss-processserver63-openshift :latest :1.3 :1.3-17 :1.3-18 :1.3-20	24 days ago
openshift/jboss-decisionserver63-openshift	24 days ago

Private Registry

RED HAT QUAY.io & QUAY ENTERPRISE

Securely store your containers

Easily build and deploy new containers

Automatically scan and secure containers

Private Registry

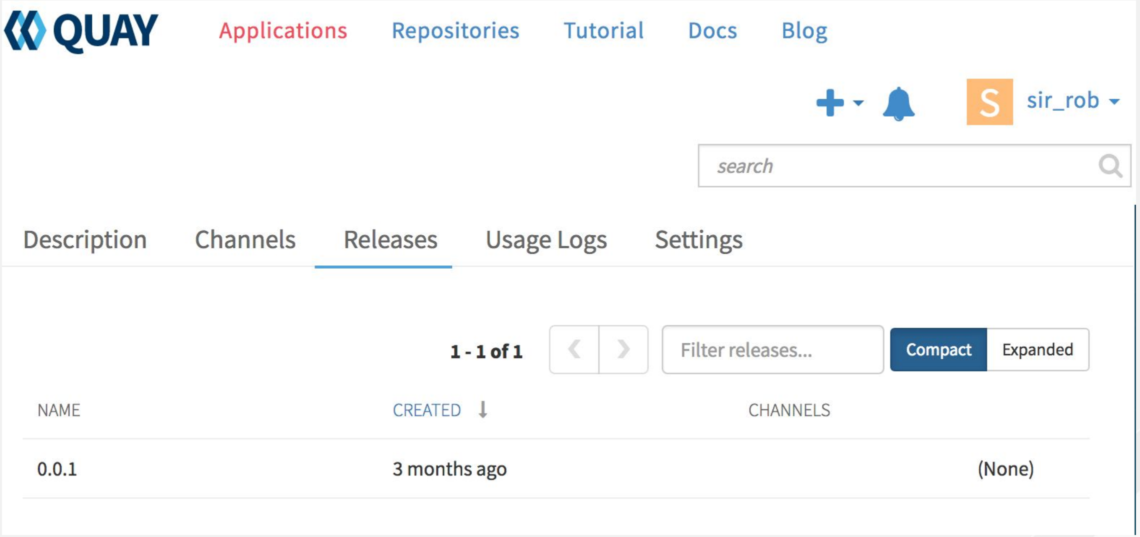
QUAY APPLICATION REGISTRY

Quay Applications Let you Automate Kubernetes Deployments

Push, pull & discover Kubernetes applications.

Interact with Helm charts like you do with container images.

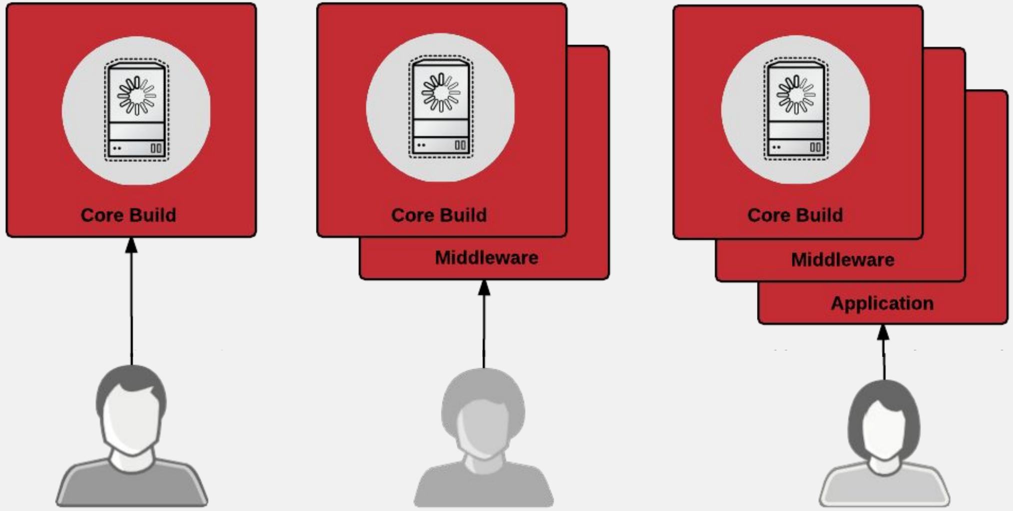
```
$ helm registry install
quay.io/jzelinskie/nginx
```



NAME	CREATED ↓	CHANNELS
0.0.1	3 months ago	(None)

CI

DESIGN FOR SEPARATION OF CONCERNS



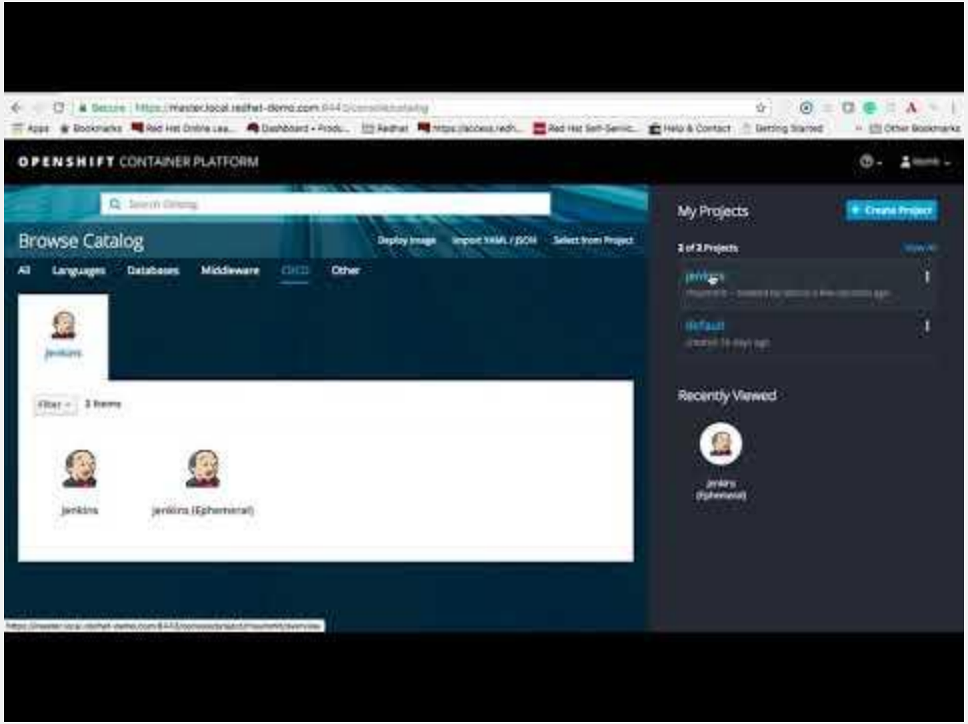
Operations

Architects

Application developers

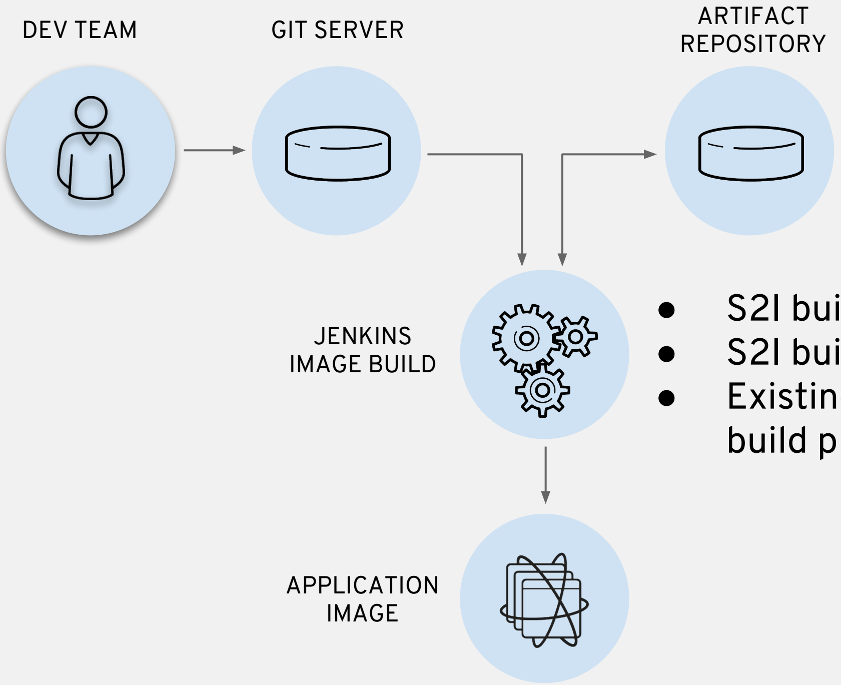
CI

JENKINS-AS-A-SERVICE ON OPENSHIFT



CI

CONTINUOUS INTEGRATION PIPELINE

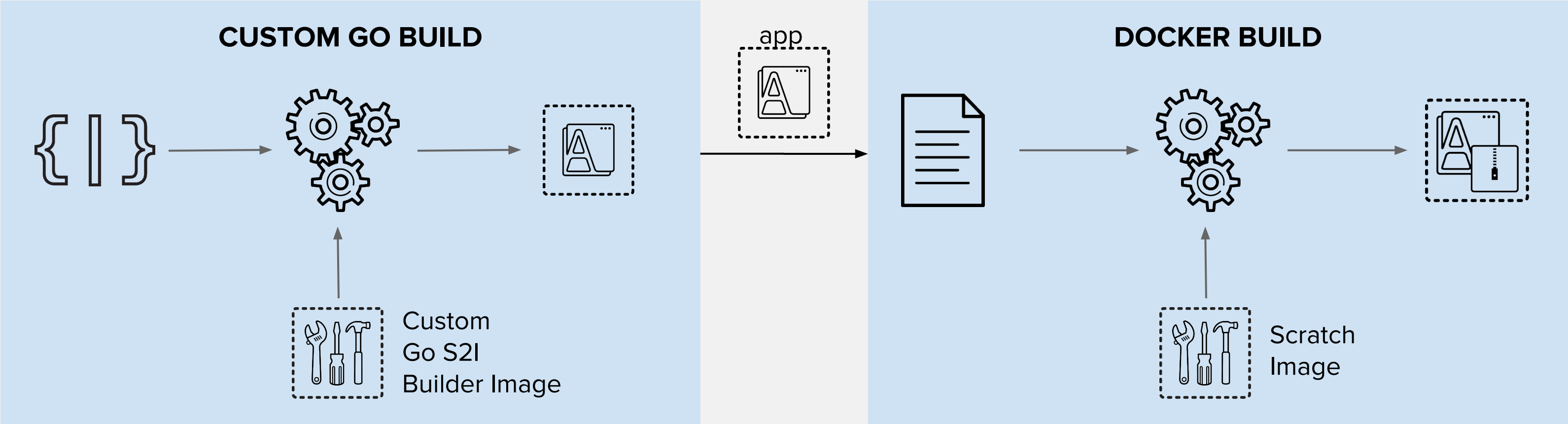


- S2I build from source code
- S2I build from app binary
- Existing docker container image build process

CI

EXAMPLE: SMALL LEAN RUNTIMES

Build the app binary and deploy on small scratch images



read more on https://blog.openshift.com/chaining-builds/

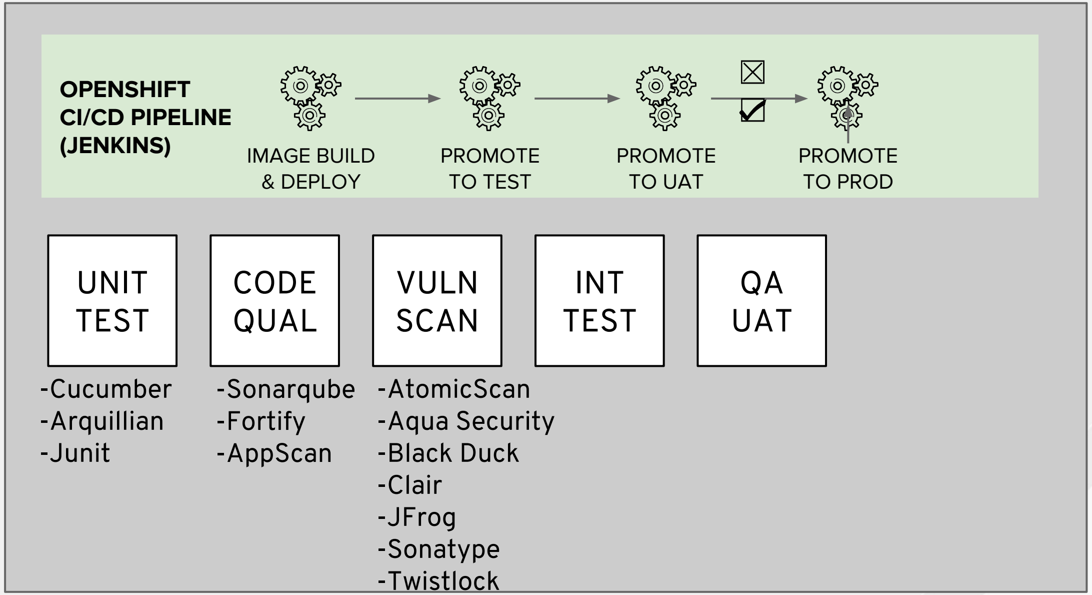
How to use a non-builderimage for the final application image

CI

CONTINUOUS INTEGRATION MUST INCLUDE SECURITY GATES

- Integrate security testing into your build / CI process

- Use automated policies to flag builds with issues



OPENSHIFT CI/CD PIPELINE (JENKINS)

IMAGE BUILD & DEPLOY → PROMOTE TO TEST → PROMOTE TO UAT ☒ ☑ → PROMOTE TO PROD

UNIT TEST
-Cucumber
-Arquillian
-Junit

CODE QUAL
-Sonarqube
-Fortify
-AppScan

VULN SCAN
-AtomicScan
-Aqua Security
-Black Duck
-Clair
-JFrog
-Sonatype
-Twistlock

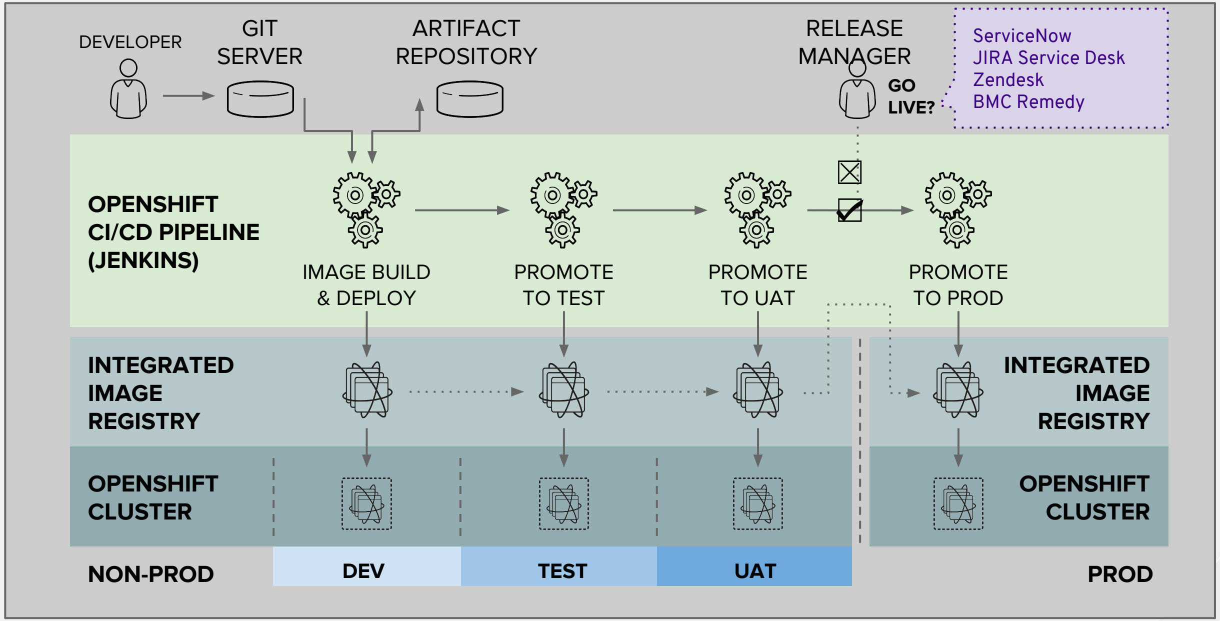
INT TEST

QA UAT

CD

MANAGING CONTAINER DEPLOYMENT

- Secrets
- Deployment policies
- Image signing
- Monitor for new vulnerabilities



CD

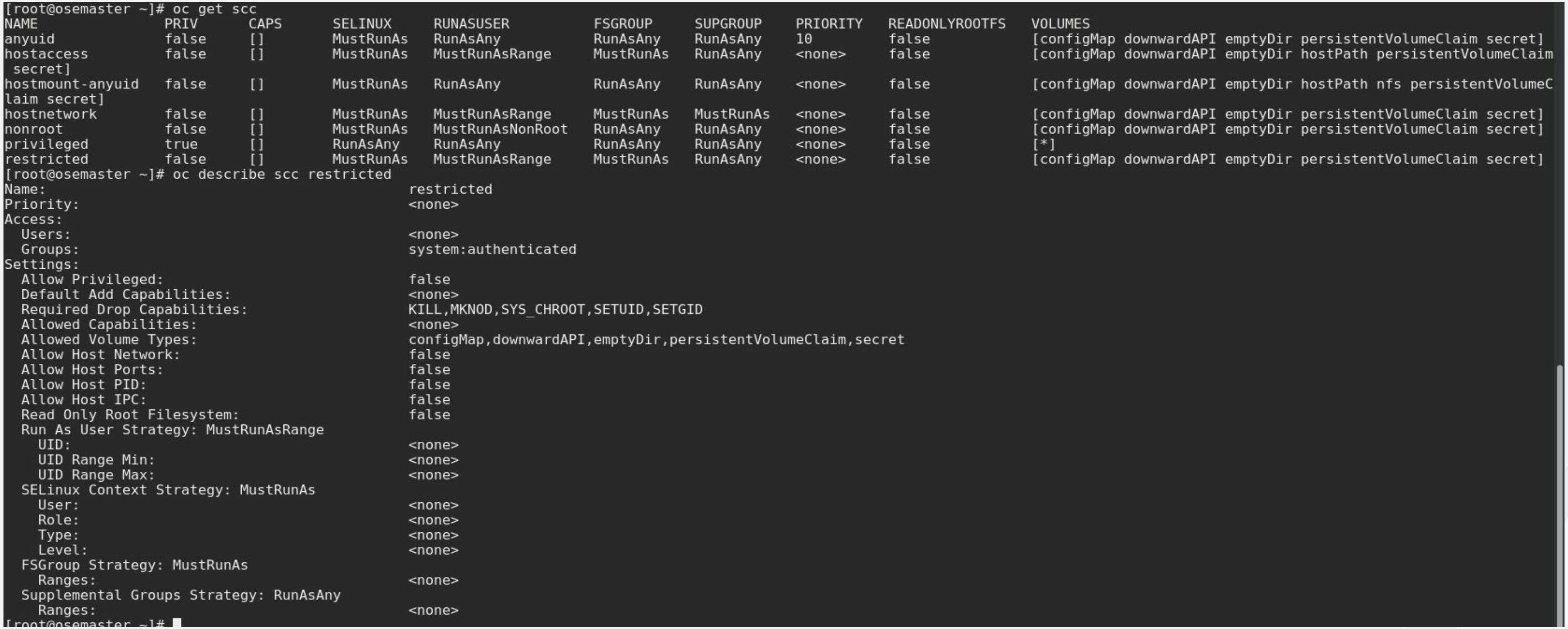
SECRETS MANAGEMENT

- Etcd secrets encrypted by default
- Flexvolume API supported for easier integration with 3rd party vault solutions
- Use Node Authorizer & Node Restriction Admission to prevent Pods from gaining access to secrets, configMaps, PV, PVC or API objects from other nodes

```
# oadm policy remove-cluster-role-from-group system:node system:nodes
```

CD

CONTAINER DEPLOYMENT PERMISSIONS: Security Context Constraints



```
[root@osemaster ~]# oc get scc
NAME               PRIV      CAPS      SELINUX     RUNASUSER          FSGROUP     SUPGROUP    PRIORITY    READONLYROOTFS    VOLUMES
anyuid             false     []        MustRunAs   RunAsAny           RunAsAny    RunAsAny    10          false             [configMap downwardAPI emptyDir persistentVolumeClaim secret]
hostaccess         false     []        MustRunAs   MustRunAsRange     MustRunAs   RunAsAny    <none>      false             [configMap downwardAPI emptyDir hostPath persistentVolumeClaim
 secret]
hostmount-anyuid   false     []        MustRunAs   RunAsAny           RunAsAny    RunAsAny    <none>      false             [configMap downwardAPI emptyDir hostPath nfs persistentVolumeC
laim secret]
hostnetwork        false     []        MustRunAs   MustRunAsRange     MustRunAs   MustRunAs   <none>      false             [configMap downwardAPI emptyDir persistentVolumeClaim secret]
nonroot            false     []        MustRunAs   MustRunAsNonRoot   RunAsAny    RunAsAny    <none>      false             [configMap downwardAPI emptyDir persistentVolumeClaim secret]
privileged         true      []        RunAsAny    RunAsAny           RunAsAny    RunAsAny    <none>      false             [*]
restricted         false     []        MustRunAs   MustRunAsRange     MustRunAs   RunAsAny    <none>      false             [configMap downwardAPI emptyDir persistentVolumeClaim secret]
[root@osemaster ~]# oc describe scc restricted
Name:                                           restricted
Priority:                                       <none>
Access:
  Users:                                        <none>
  Groups:                                       system:authenticated
Settings:
  Allow Privileged:                             false
  Default Add Capabilities:                     <none>
  Required Drop Capabilities:                   KILL,MKNOD,SYS_CHROOT,SETUID,SETGID
  Allowed Capabilities:                         <none>
  Allowed Volume Types:                         configMap,downwardAPI,emptyDir,persistentVolumeClaim,secret
  Allow Host Network:                           false
  Allow Host Ports:                             false
  Allow Host PID:                               false
  Allow Host IPC:                               false
  Read Only Root Filesystem:                    false
  Run As User Strategy: MustRunAsRange
    UID:                                        <none>
    UID Range Min:                              <none>
    UID Range Max:                              <none>
  SELinux Context Strategy: MustRunAs
    User:                                       <none>
    Role:                                       <none>
    Type:                                       <none>
    Level:                                      <none>
  FSGroup Strategy: MustRunAs
    Ranges:                                     <none>
  Supplemental Groups Strategy: RunAsAny
    Ranges:                                     <none>
[root@osemaster ~]#
```

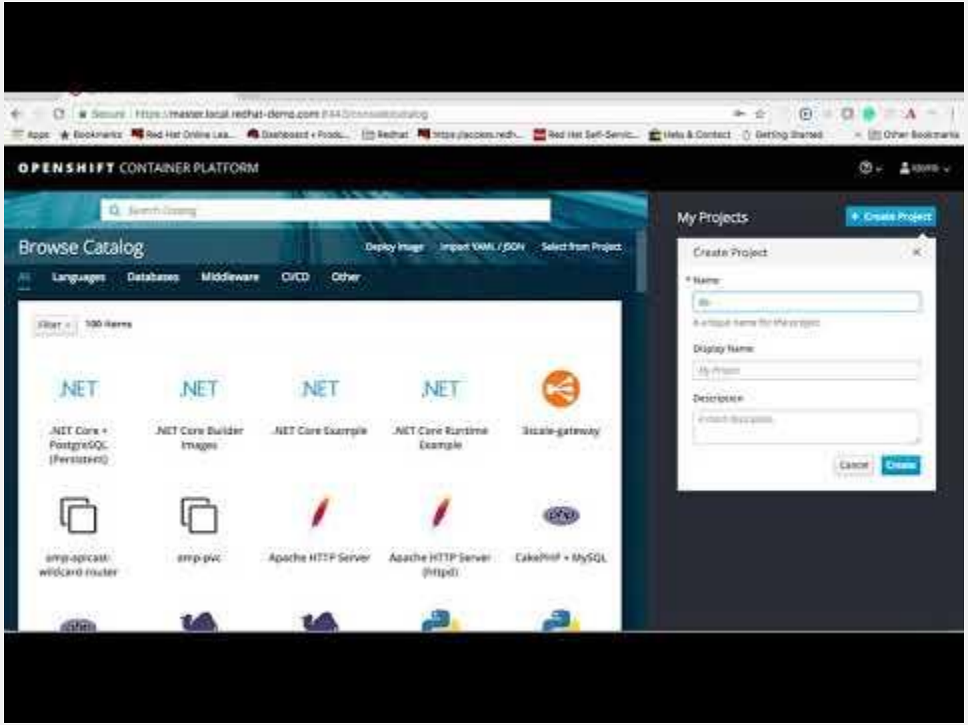
CI / CD

RESTRICT WHERE YOU CAN PULL FROM

```
imagePolicyConfig:
  allowedRegistriesForImport:
    - domainName: registry.access.redhat.com
    - domainName: registry.connect.redhat.com
    - domainName: quay.io
```

CI / CD

DEMO: Deny Docker.io



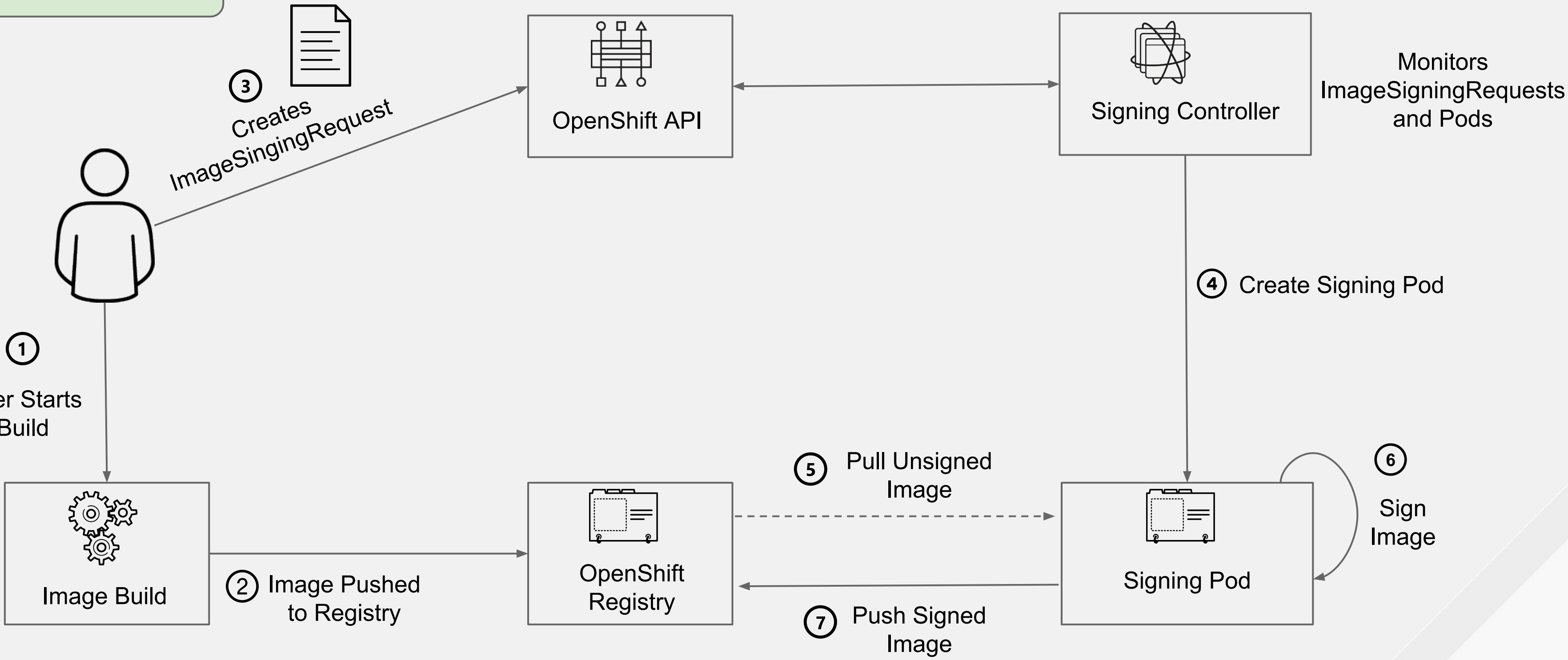
#redhat #rhsummit

redhat.

CI / CD

Demo Flow Image Signing Request

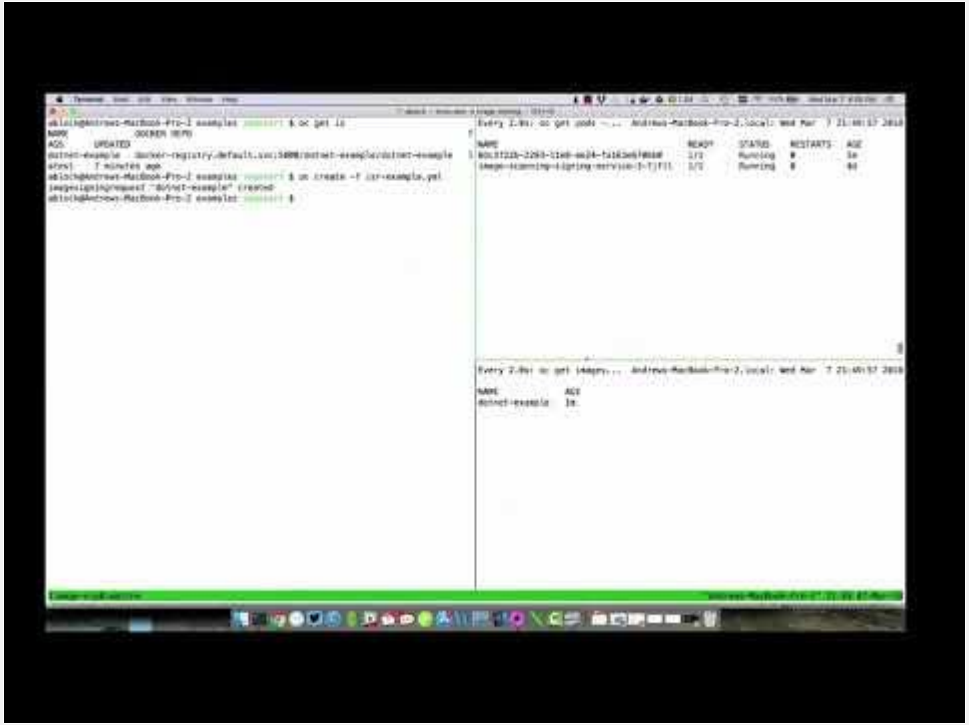
Content Metadata



CI / CD

Demo Image Signing Request

Content Metadata



```
ablock@Andrews-MacBook-Pro-2 examples [illegible] $ oc get is
NAME              DOCKER REPO
AGE      UPDATED
dotnet-example    docker-registry.default.svc:5000/dotnet-example/dotnet-example
[illegible]       7 minutes ago
ablock@Andrews-MacBook-Pro-2 examples [illegible] $ oc create -f isr-example.yml
imagesigningrequest "dotnet-example" created
ablock@Andrews-MacBook-Pro-2 examples [illegible] $
```

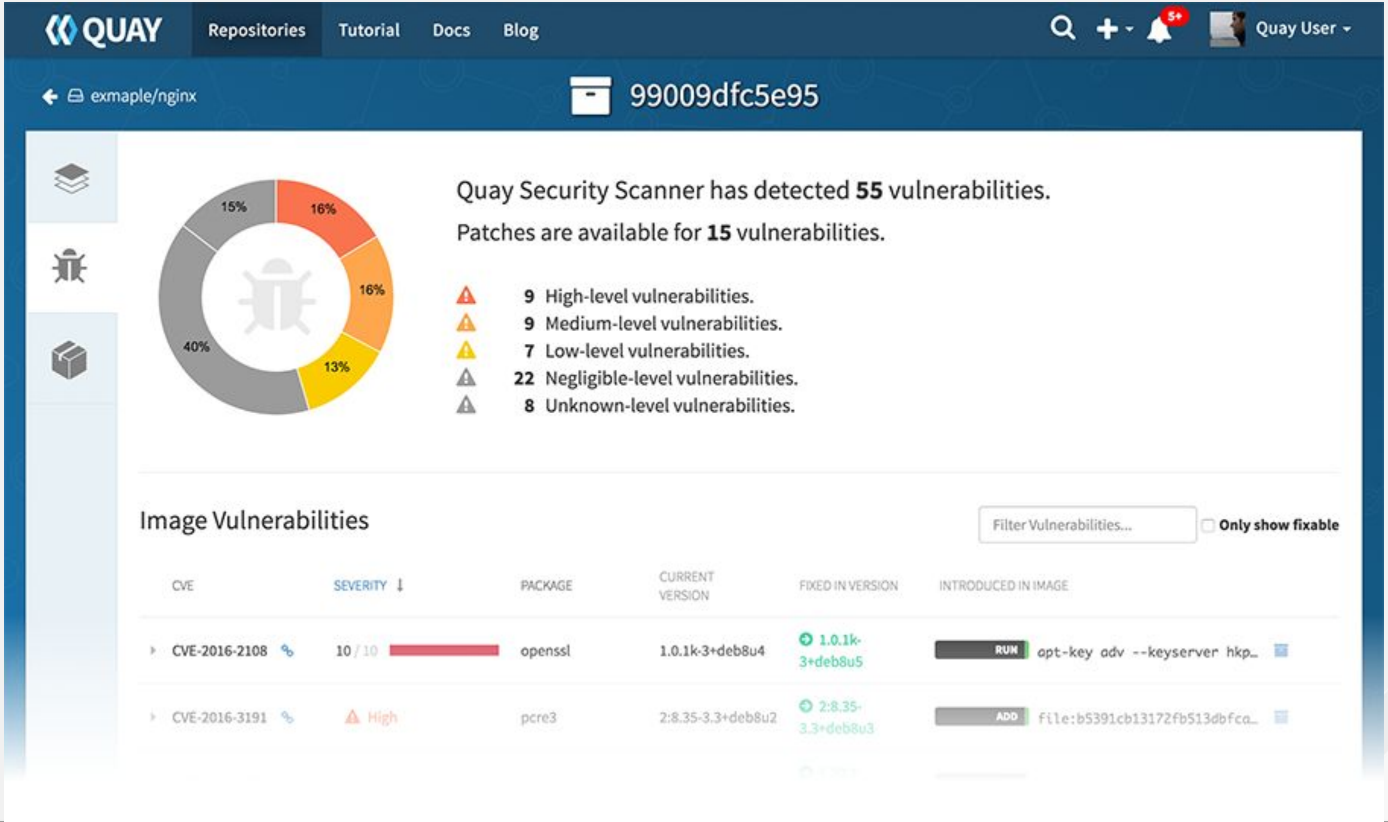
```
Every 2.0s: oc get pods -...  Andrews-MacBook-Pro-2.local: Wed Mar  7 21:40:17 2018

NAME                                    READY   STATUS    RESTARTS   AGE
[illegible]                             1/1     Running   0          1m
image-scanning-signing-service-3-[illegible]   1/1     Running   0          4d
```

```
Every 2.0s: oc get images...  Andrews-MacBook-Pro-2.local: Wed Mar  7 21:40:17 2018

NAME             AGE
dotnet-example   1m
```

CI/CD

Vulnerability Scanning - Clair

Content Metadata



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

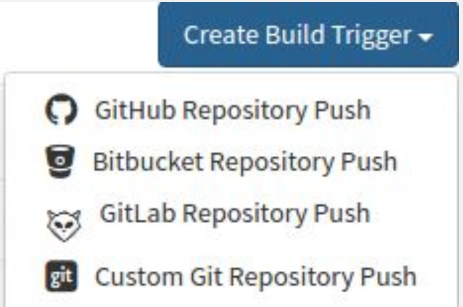
Filter Vulnerabilities... □ **Only show fixable**

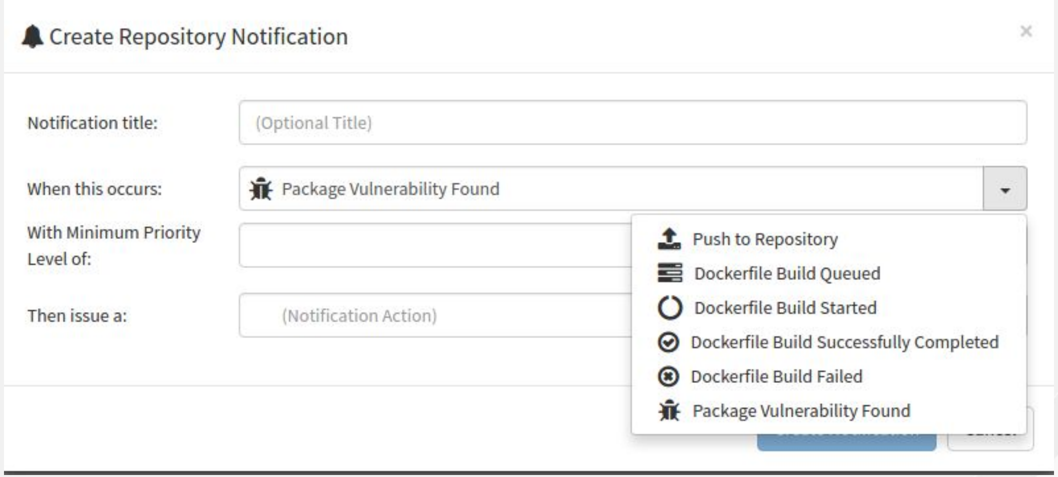
CVE	SEVERITY ↓	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN IMAGE
CVE-2016-2108	10 / 10	openssl	1.0.1k-3+deb8u4	1.0.1k-3+deb8u5	RUN `apt-key adv --keyserver hkp...`
CVE-2016-3191	High	pcre3	2:8.35-3.3+deb8u2	2:8.35-3.3+deb8u3	ADD `file:b5391cb13172fb513dbfca...`

CI/CD

Content Metadata

QUAY: BUILD TRIGGERS & NOTIFICATIONS




Create Repository Notification
×

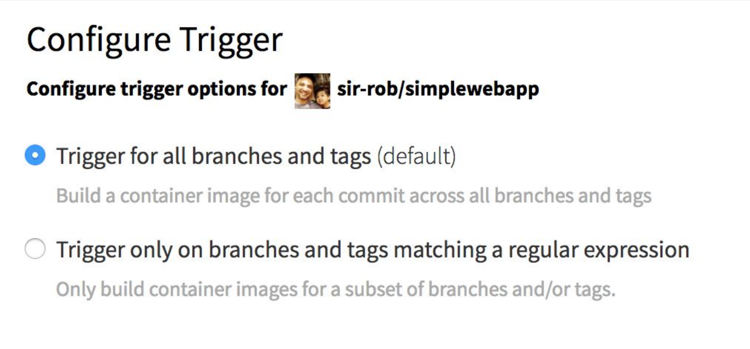
Notification title: (Optional Title)

When this occurs: Package Vulnerability Found

With Minimum Priority Level of:

Then issue a: (Notification Action)

Push to Repository
Dockerfile Build Queued
Dockerfile Build Started
Dockerfile Build Successfully Completed
Dockerfile Build Failed
Package Vulnerability Found



Configure Trigger

Configure trigger options for sir-rob/simplewebapp

● Trigger for all branches and tags (default)

Build a container image for each commit across all branches and tags

○ Trigger only on branches and tags matching a regular expression

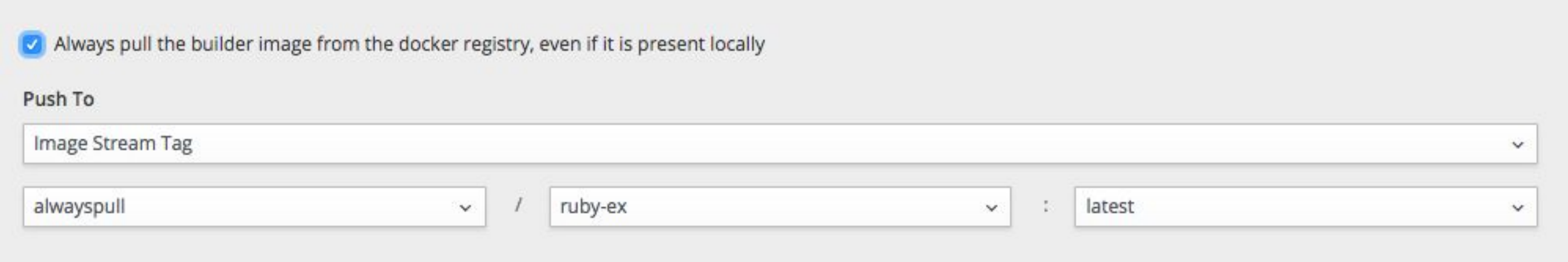
Only build container images for a subset of branches and/or tags.

CI / CD

Content Metadata

ImageStream Events

ALWAYS PULL BUILDER IMAGE



☑ Always pull the builder image from the docker registry, even if it is present locally

Push To

Image Stream Tag

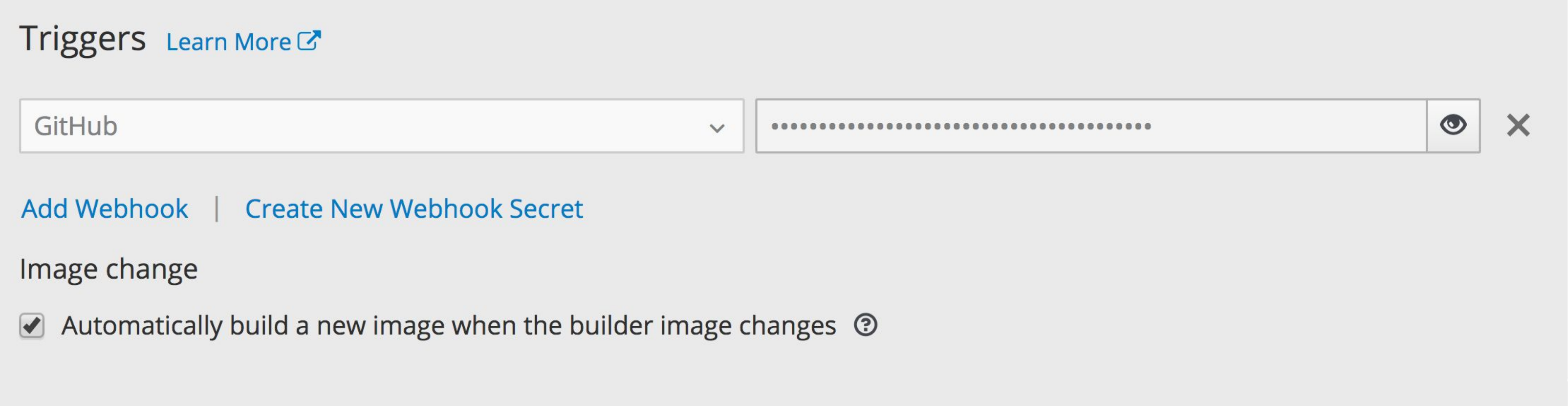
alwayspull / ruby-ex : latest

CI / CD

Content Metadata

ImageStream Events

GET UPDATED BASE IMAGE



Triggers Learn More

GitHub ●● ✕

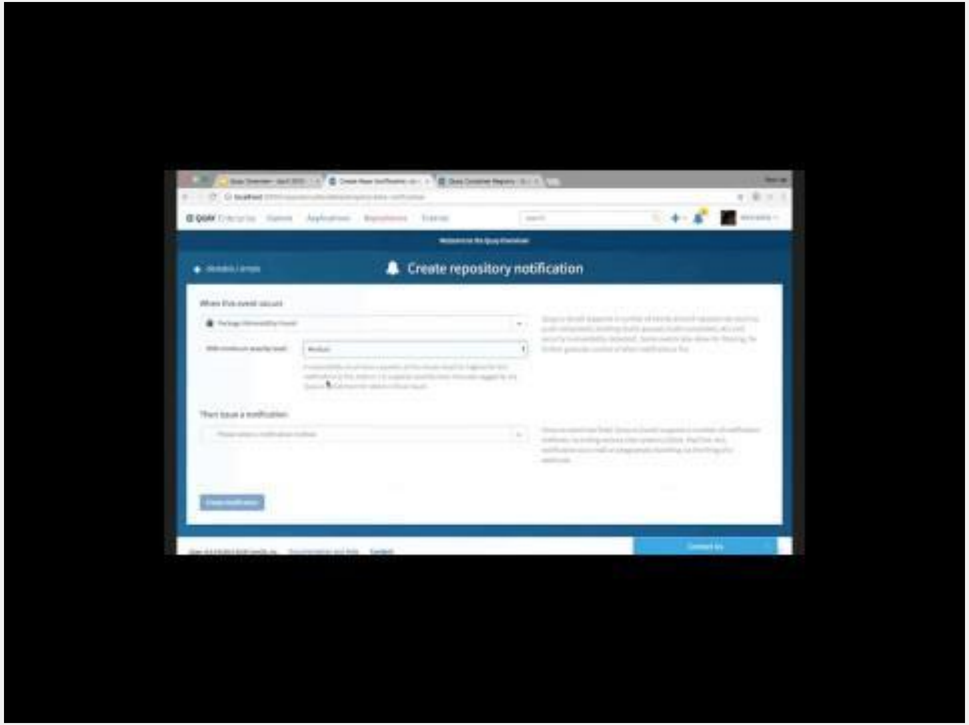
Add Webhook | Create New Webhook Secret

Image change

☑ Automatically build a new image when the builder image changes

CI / CD

Content Metadata



QUAY Enterprise
Create repository notification
When this event occurs
Package Vulnerability Found
With minimum severity level
Medium
Then issue a notification
Create Notification
Contact Us

CD

VULNERABLE? OPENSHIFT TAKES ACTION!

Content Metadata

Default Policy

```
 openshift.io/ImagePolicy:
   configuration:
    apiVersion: v1
    executionRules:
    - matchImageAnnotations:
     - key:
images.openshift.io/deny-execution
      value: 'true'
     name: execution-denied
     onResources:
     - resource: pods
     - resource: builds
     reject: true
     skipOnResolutionFailure: true
    kind: ImagePolicyConfig
```

Image Annotation

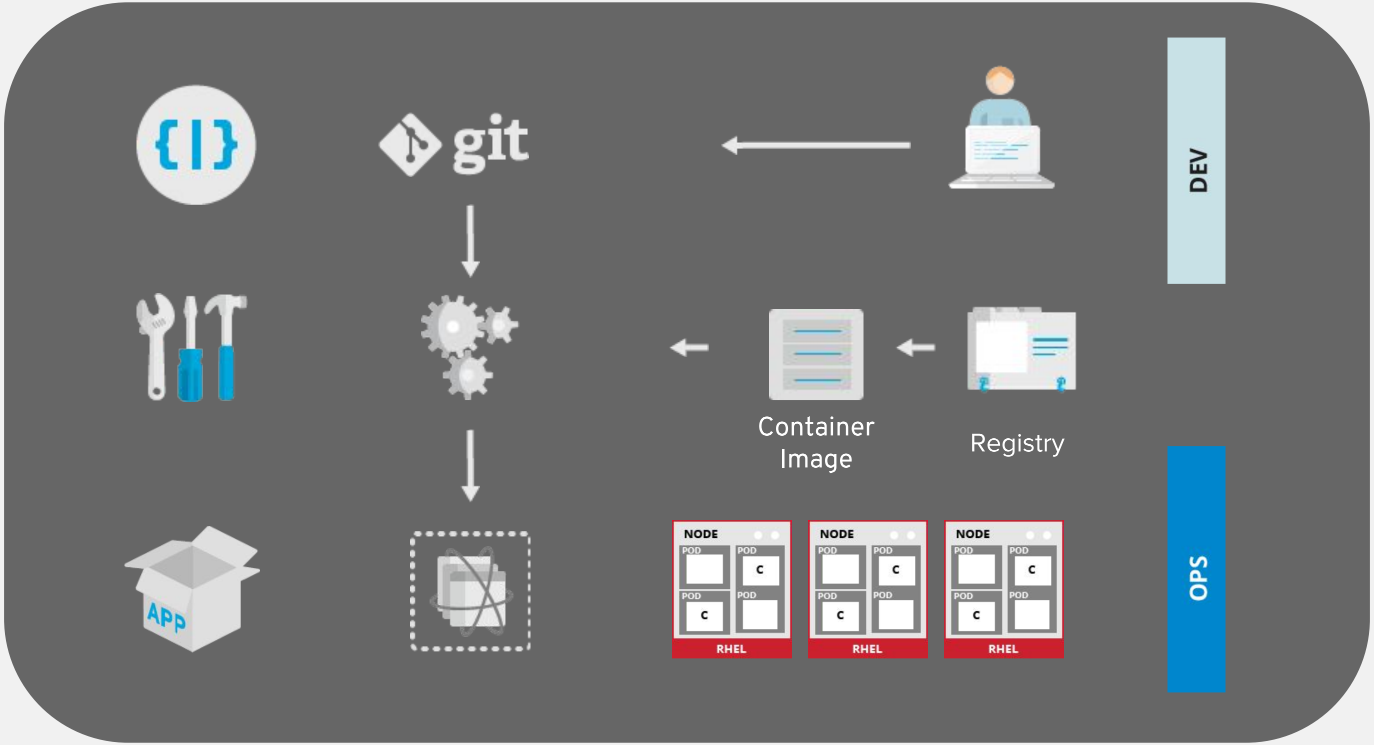
```
image.openshift.io/deny-execution: true
openshift.io/image.managed: true
security.manageiq.org/failed-policy:
openscap policy
```

CI

CD

CONTINUOUS SECURITY

Continuous Integration / Continuous Deployment / Continuous Security



Trust is temporal: rebuild and redeploy as needed

DEFEND

Secure the Infrastructure

- Container Platform
- Container Host Multi-tenancy
- Network Isolation
- Storage
- Audit & Logging
- API Management

CONTAINER HOST & MULTI-TENANCY
THE OS MATTERS

RED HAT ENTERPRISE LINUX

Atomic Host / RED HAT CoreOS

THE FOUNDATION FOR SECURE, SCALABLE CONTAINERS

A stable, reliable host environment with built-in security features that allow you to isolate containers from other containers and from the kernel.

Minimized host environment tuned for running Linux containers while maintaining the built-in security features of Red Hat Enterprise Linux..

SELinux

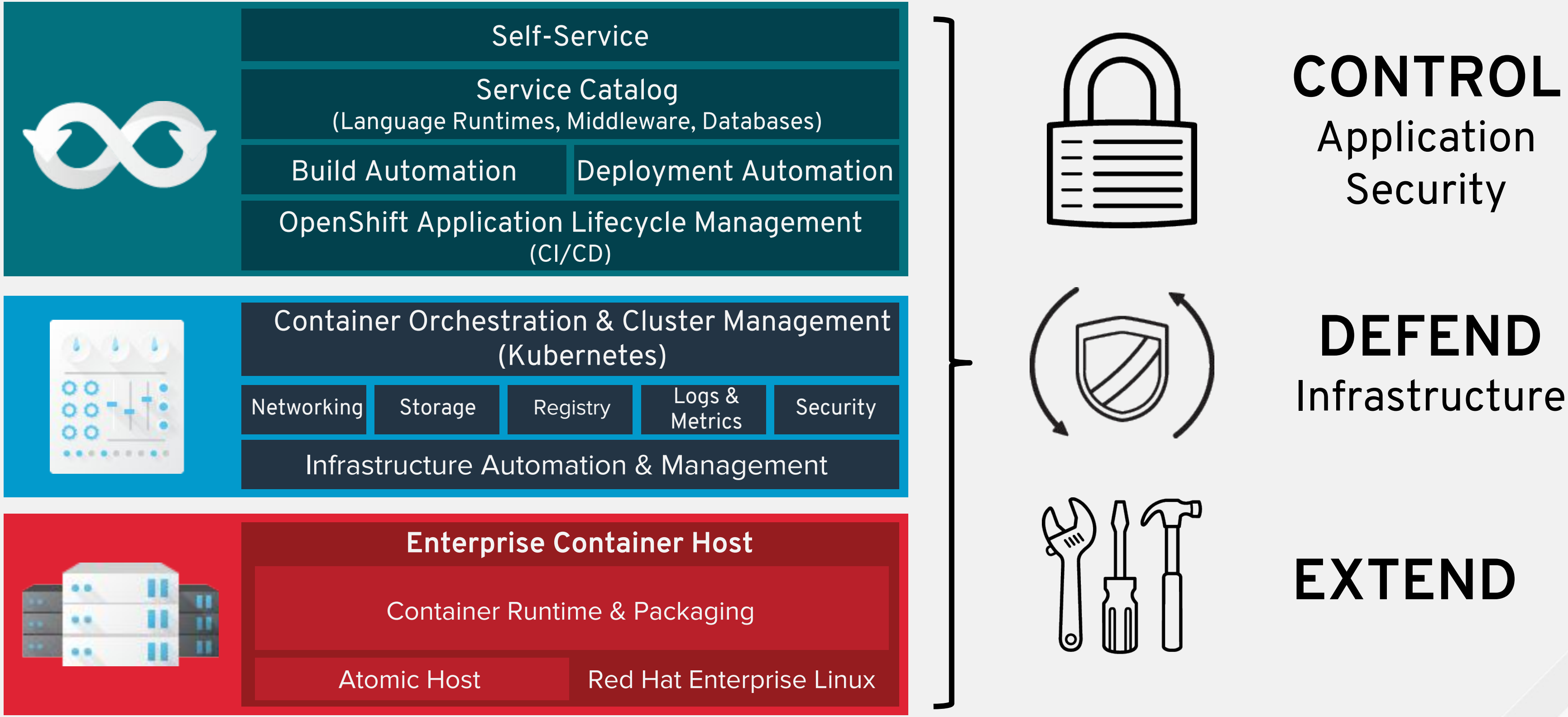
Kernel namespaces

Capabilities

Cgroups

Seccomp

BRINGING IT ALL TOGETHER



Self-Service

Service Catalog
(Language Runtimes, Middleware, Databases)

Build Automation | Deployment Automation

OpenShift Application Lifecycle Management
(CI/CD)

Container Orchestration & Cluster Management
(Kubernetes)

Networking | Storage | Registry | Logs & Metrics | Security

Infrastructure Automation & Management

Enterprise Container Host

Container Runtime & Packaging

Atomic Host | Red Hat Enterprise Linux

CONTROL
Application Security

DEFEND
Infrastructure

EXTEND

RELATED SESSIONS

Today

OpenShift for operations - S1225 (Thu, 1 pm, Moscone West 2003)

Building production-ready containers - S2105 (Thu, 3 pm, Moscone West 2002)

I’m a developer. What do I need to know about security? - B1046 (Thu, 3 pm, Moscone West 2103)

Previous - check for slides/recordings

Automating OpenShift Secure Container Deployment at Experian - S1689 (Tue)

Red Hat API management: overview, security models & roadmap - S1896 (Tue)

Network security for apps on OpenShift - S1220 (Wed)

Security-oriented OpenShift within regulated environments - S1778 (Wed)

ADDITIONAL RESOURCES

Ten Layers of Container Security

Openshift Security Guide

Container Image Signing Integration Guide

OpenShift and Network Security Zones: Co-existence Approaches

RED HAT SUMMIT

THANK YOU

- plus.google.com/+RedHat
- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHatNews

EXTEND

Leverage the Ecosystem

Aporeto

AquaSecurity

Avi Networks

big switch

Black Duck

Cisco Contiv

Contrail

dynatrace

f5

JFrog, Inc.

HashiCorp

NeuVector

NGINX

nuagenetworks

Portworx

Thales e-Security

Signal Sciences

Sonatype

Sysdig

Tigera

Treasure Data

Tremolo

Twistlock

OPENSHIFT PRIMED PARTNERS