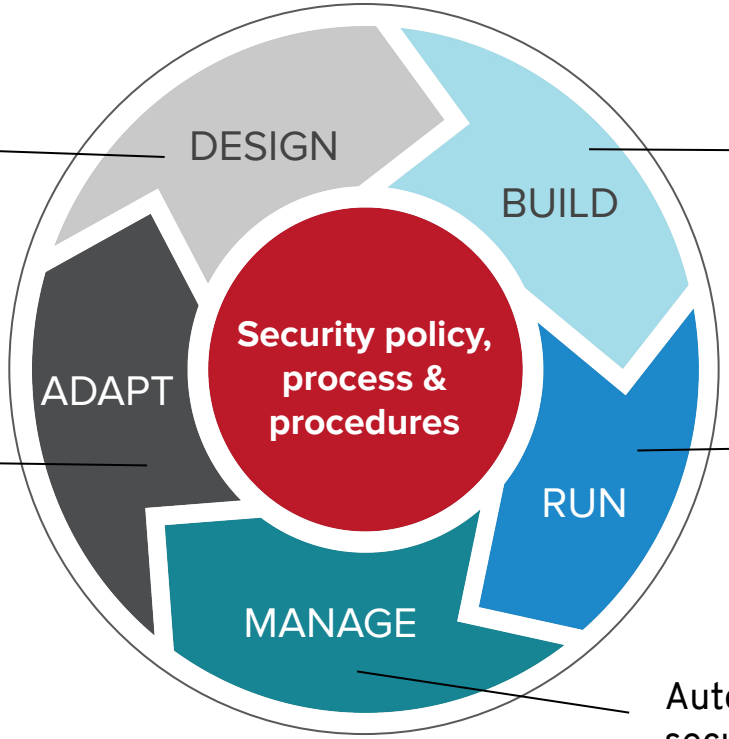
SECURING CONTAINERS WITH OPENSHIFT

Red Hat

SECURITY MUST BE CONTINUOUS

And integrated throughout the IT lifecycle



Identify security requirements & governance models

Built-in from the start; not bolted-on

Deploy to trusted platforms with enhanced security capabilities

Automate systems for security & compliance

Revise, update, remediate as the landscape changes

Red Hat

COMPREHENSIVE CONTAINER 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

HARDENING TOOLS & APPLICABILITY GUIDES

Product Applicability Guides

- FISMA Moderate & FISMA (NIST)
- ISO 27001
- PCI-DSS
- PCI-DSS Reference Architecture

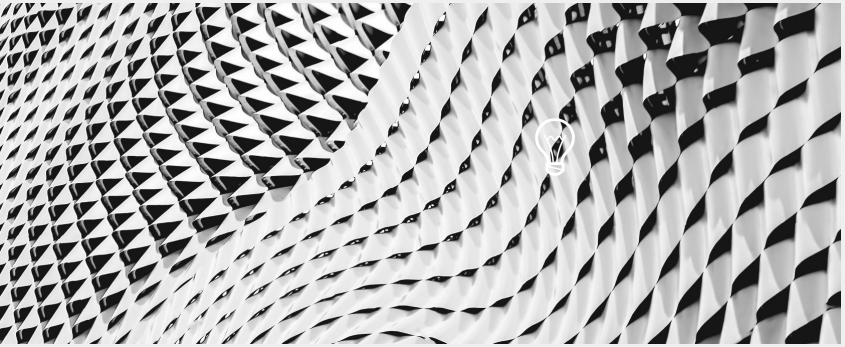
OpenShift Hardening Guide for 3.10 & 3.11 - OpenShift 4 Guide planned for Fall 2019

Upstream, 3rd party tools

- docker-bench supports versions 1.13 and 17.06
- kube-bench → WIP, support for OCP 3.9 & 3.10

https://orocktech.com/company/news/2019-07-23/

CONTROL APPLICATION SECURITY



Red Hat

DEVSECOPS

THROUGH THE ADOPTION OF CONTAINERS

We created Dev and Ops and Security user stories and tackled them together.

DEVELOPER

I can break builds if security and compliance rules aren't followed…

SECURITY

We're empowering the developers and ideally empowering them straight to production.

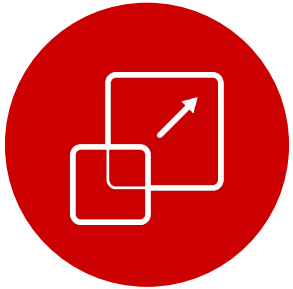
OPERATIONS

[DevNation Federal - The Journey to DevSecOps]

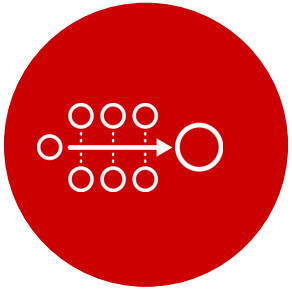
OPENSHIFT LOVES CI/CD

DevOps Excellence Awards 2017

JENKINS-AS-A SERVICE ON OPENSHIFT



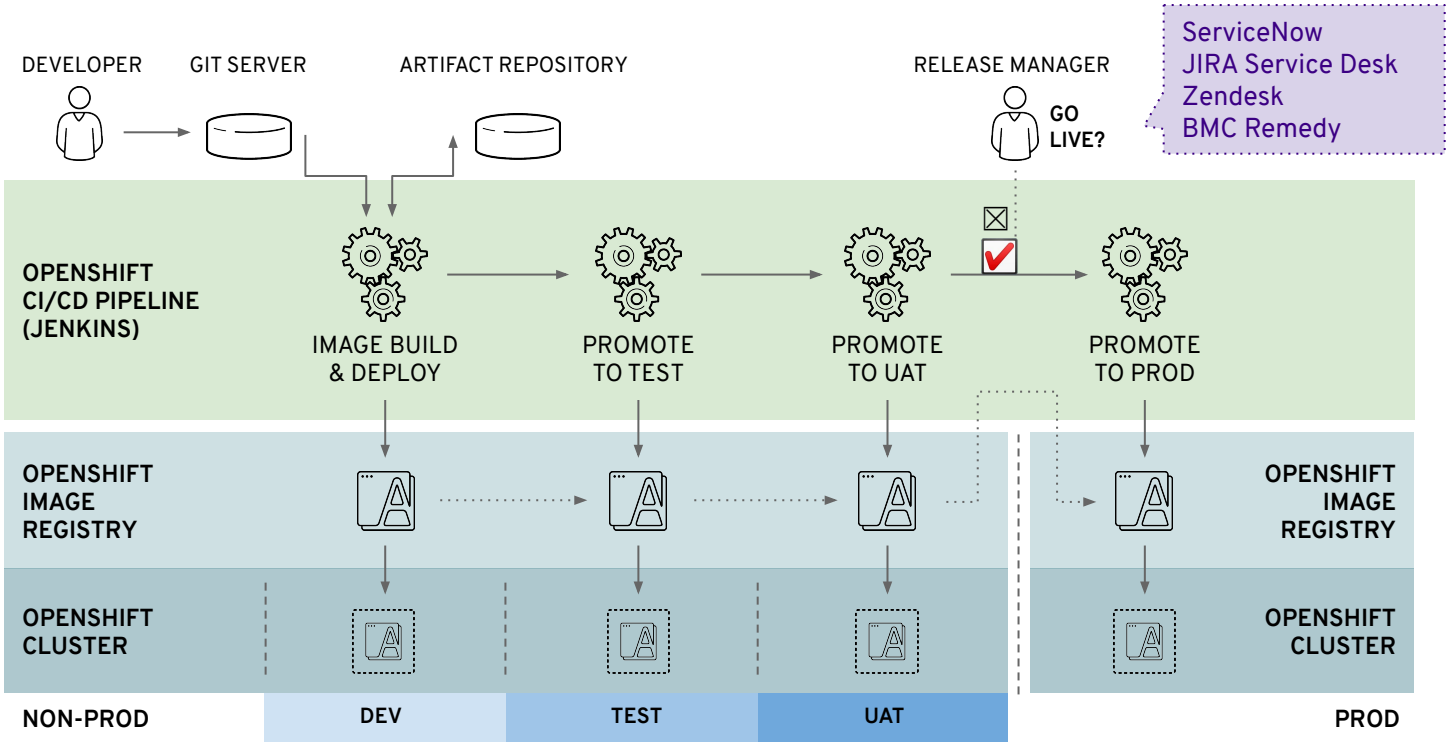
HYBRID JENKINS INFRA WITH OPENSHIFT



EXISTING CI/CD DEPLOY TO OPENSHIFT

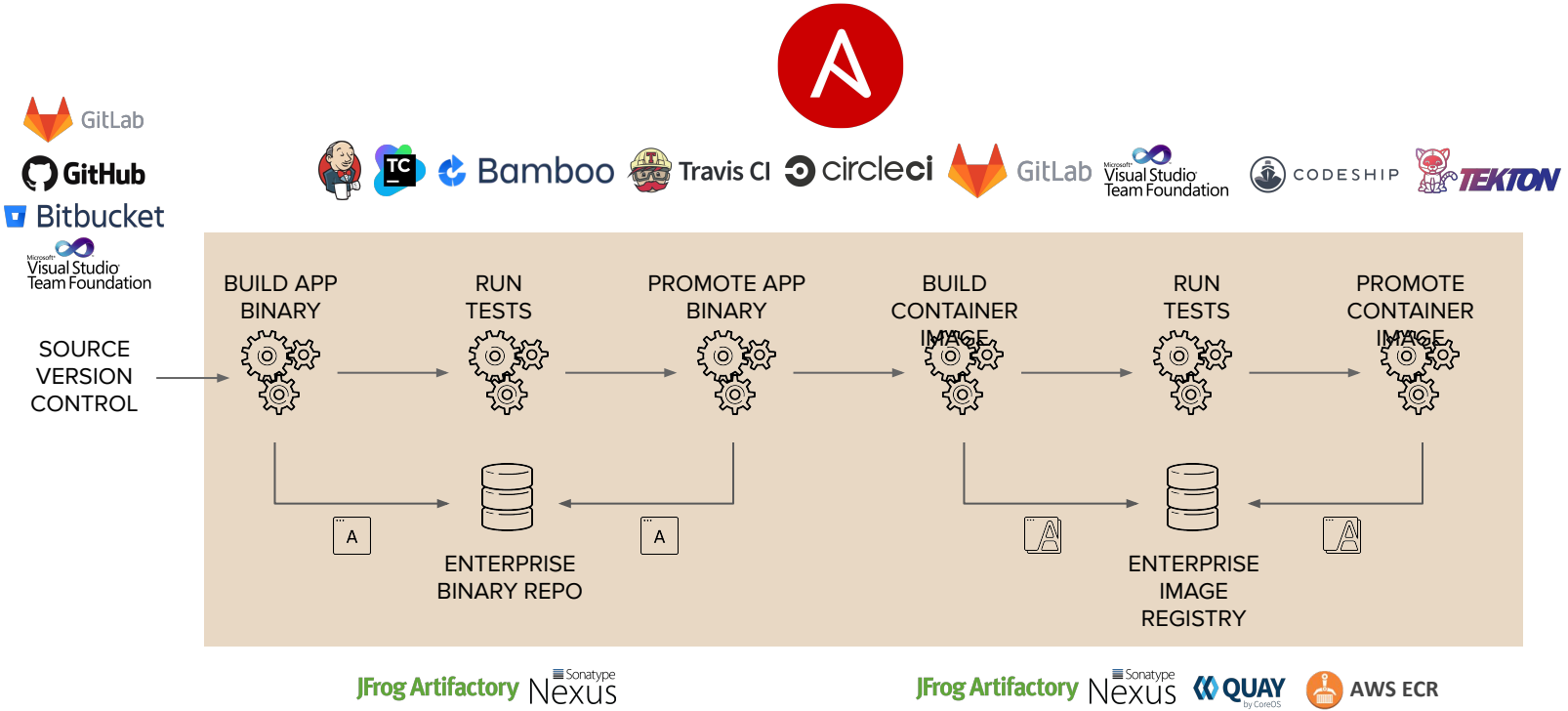
Red Hat

USE THE OPENSHIFT PIPELINE



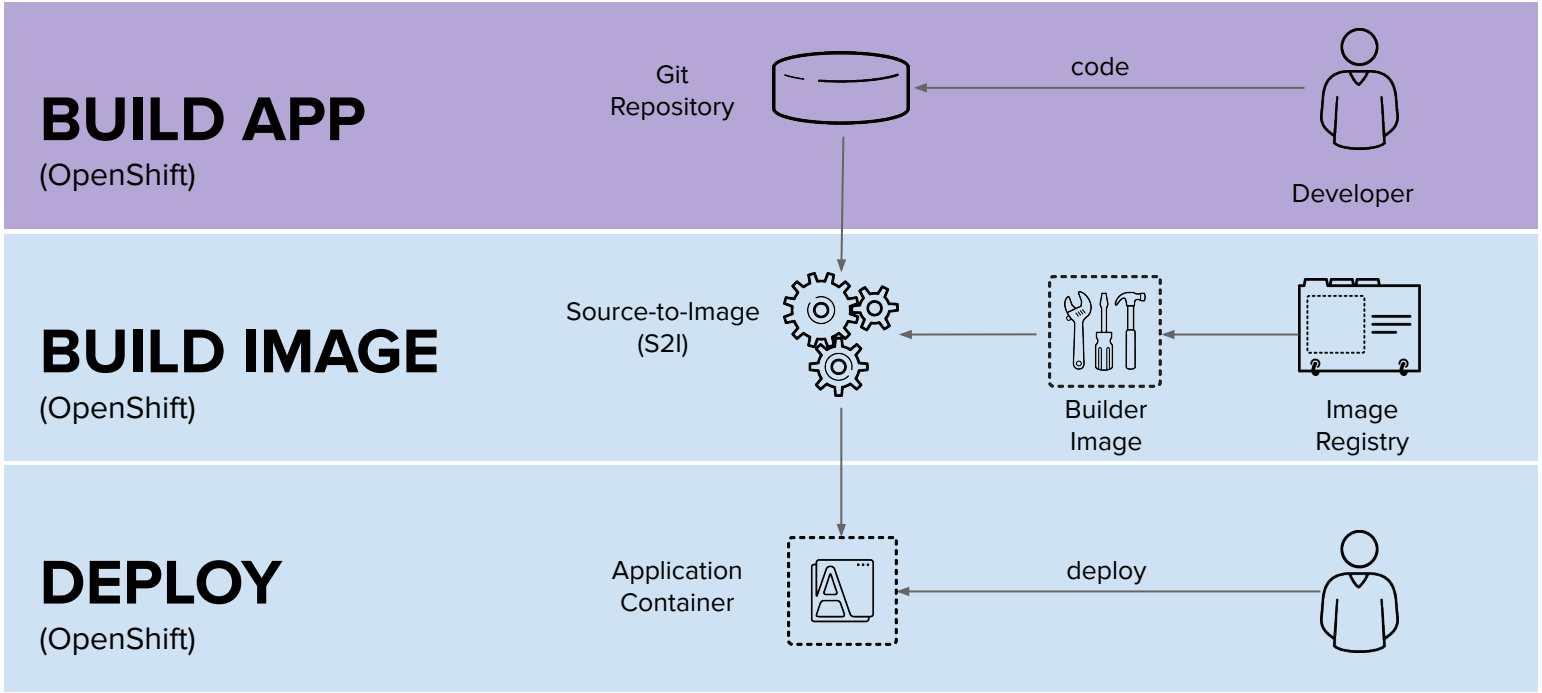
Red Hat

OR USE EXISTING DELIVERY PROCESSES



Red Hat

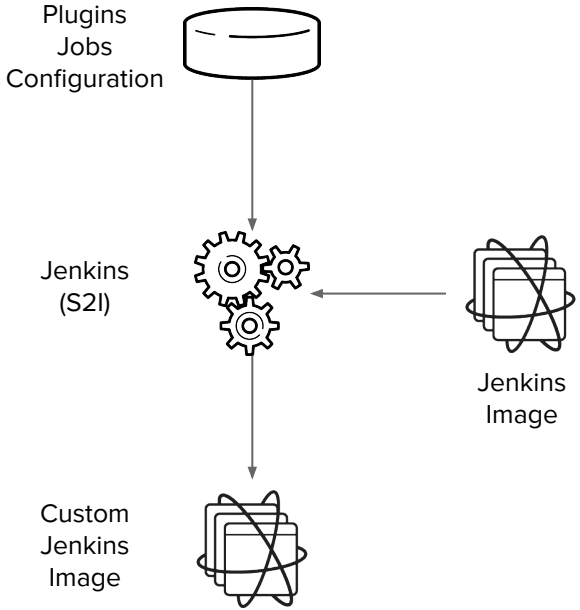
DEPLOY IMAGES, APPLICATION BINARIES OR SOURCE CODE WITH OPENSHIFT



Red Hat

JENKINS-AS-A-SERVICE ON OPENSHIFT

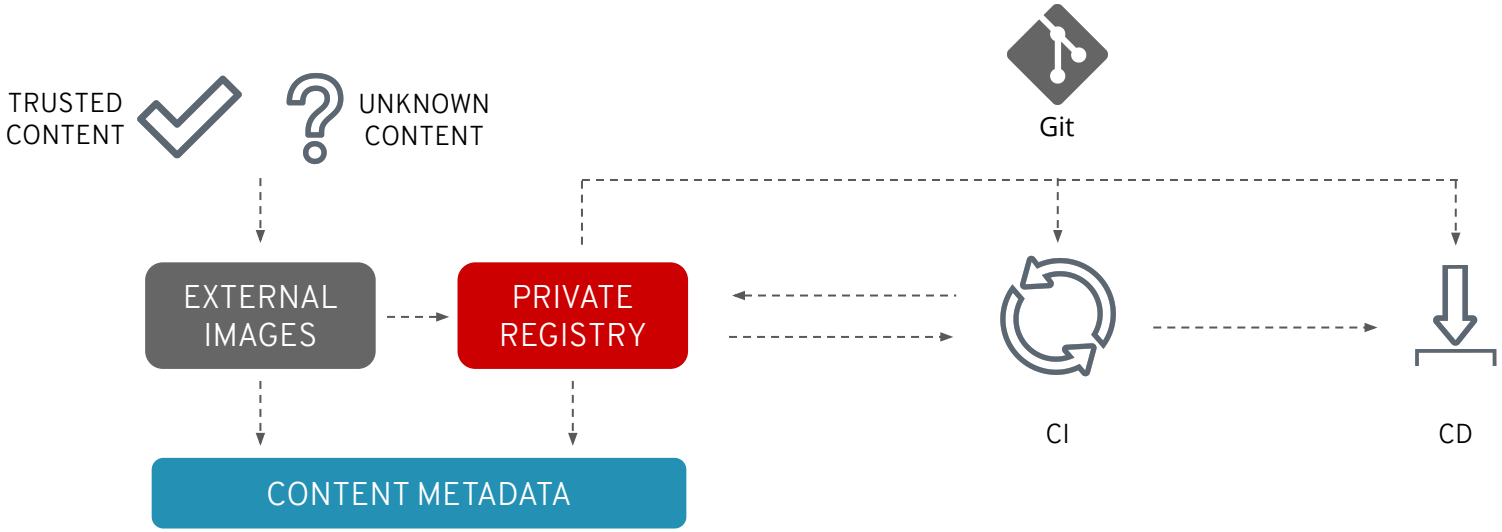
- Certified Jenkins images with pre-configured plugins
  - Provided out-of-the-box
  - Follows Jenkins 1.x and 2.x LTS versions
- Jenkins S2I Builder for customizing the image
  - Install Plugins
  - Configure Jenkins
  - Configure Build Jobs
- OpenShift plugins to integrate authentication with OpenShift and also CI/CD pipelines
- Dynamically deploys Jenkins slave containers



Red Hat

SECURE & AUTOMATE THE CONTENT LIFECYCLE

Elements of the Openshift container pipeline

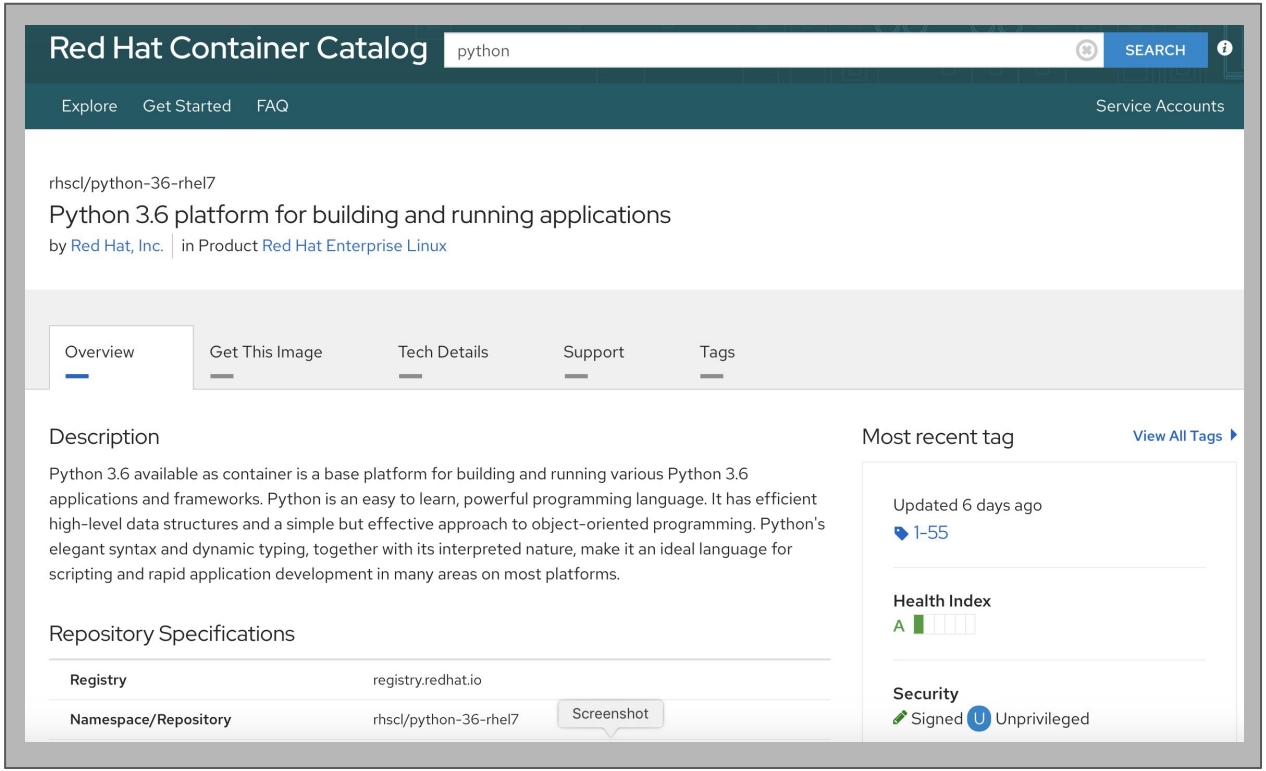


Red Hat

EXTERNAL CONTENT: USE TRUSTED SOURCES

Red Hat Container Images

- Signed Images
- Health Index
  (A to F grade)*
- Security advisories &
  errata (patches)

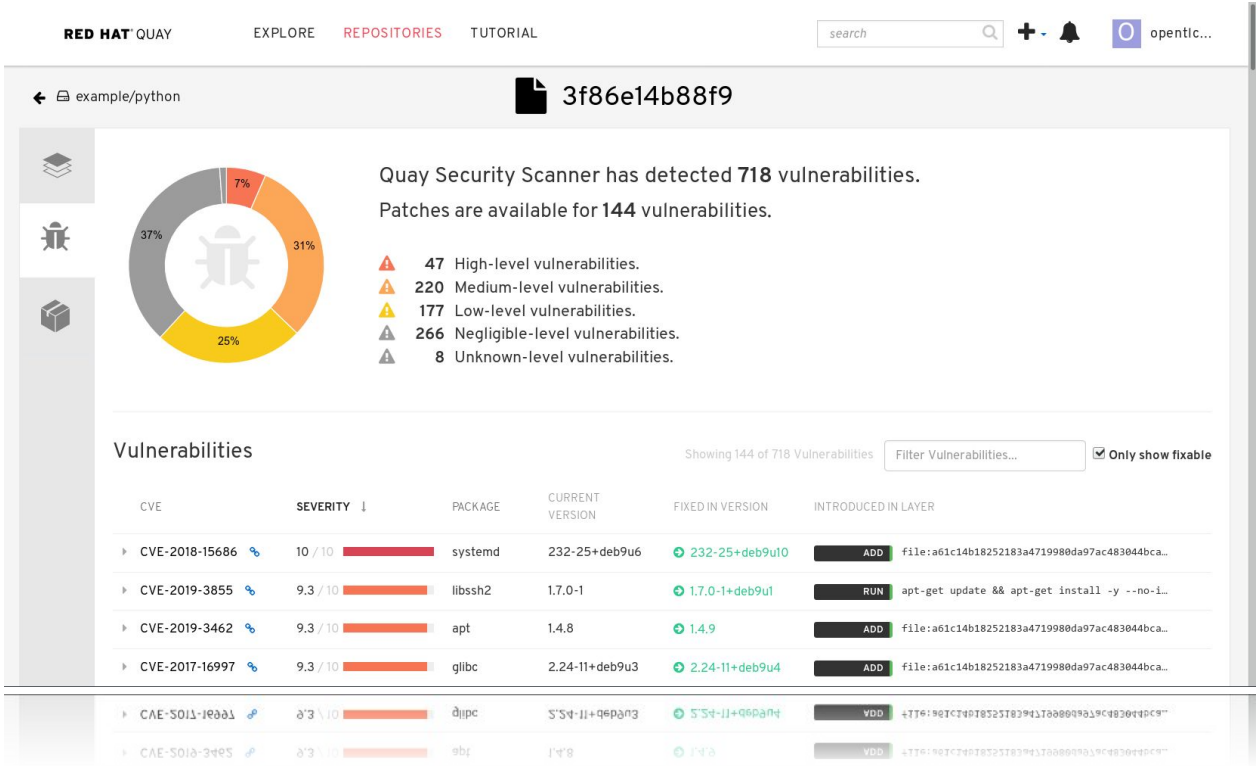


*More about the Health Index

Red Hat

RED HAT QUAY
ENTERPRISE CONTAINER REGISTRY

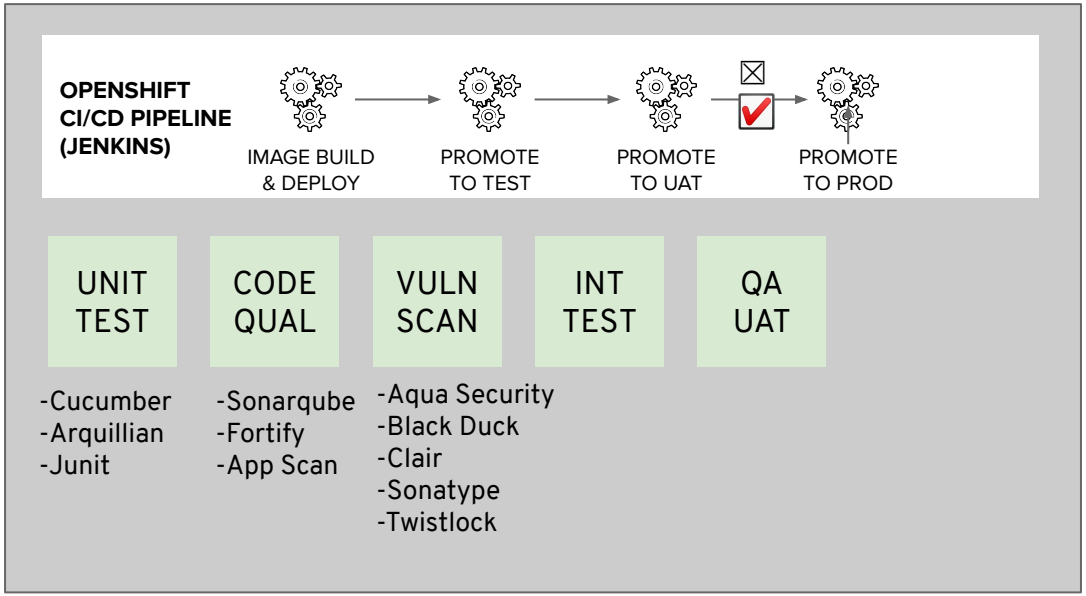
- Offered as self-managed and as-a-service
- Vulnerability Scanning (Clair)
- Geographic Replication
- Build Image Triggers
- Image Rollback with Time Machine



Red Hat

CI/CD MUST INCLUDE SECURITY GATES

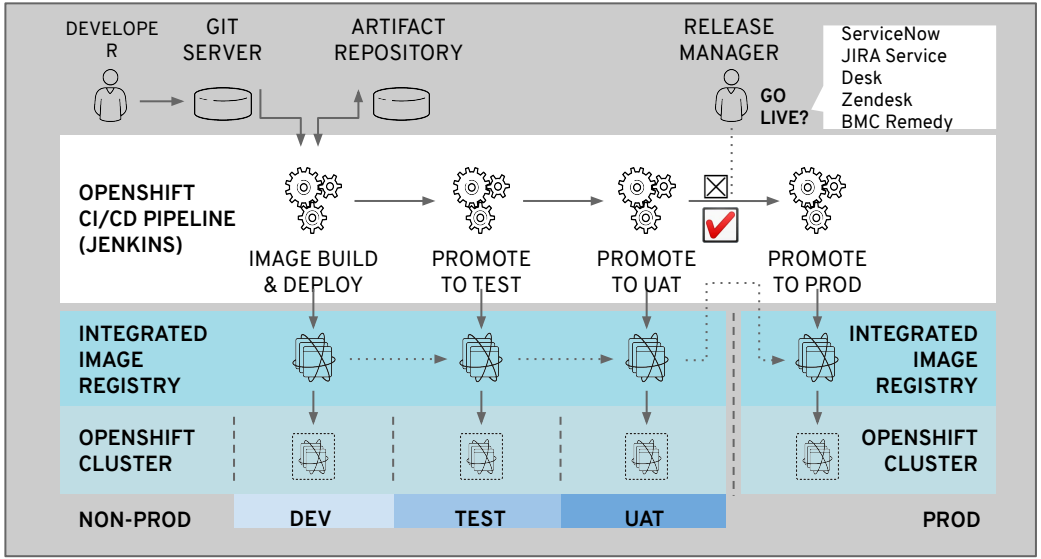
- Integrate security testing into your build / CI process
- Use automated policies to flag builds with issues
- Sign your custom container images



Red Hat

MANAGING CONTAINER DEPLOYMENT

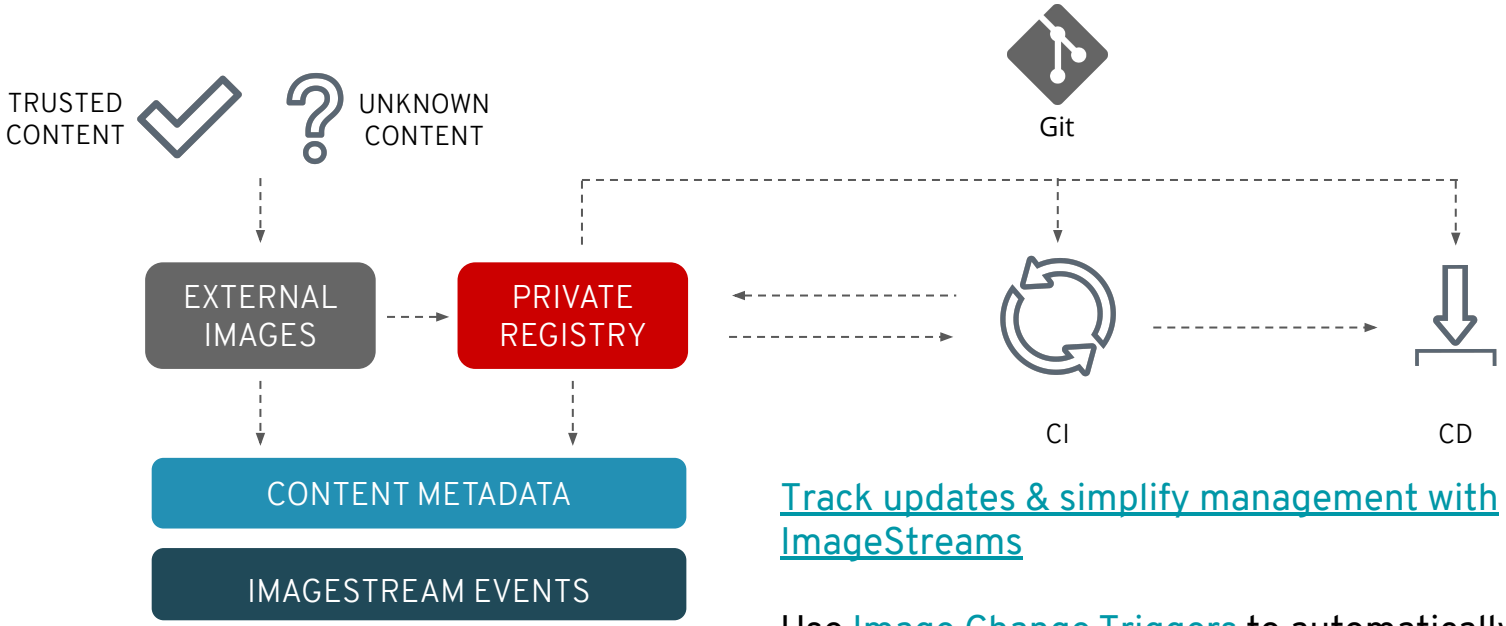
- Deployments: Containerized App Configuration as Code
- Whitelist / Blacklist external repos
- Apply runtime security policies
- Validate image signatures
- Monitor for new vulnerabilities
- Trust is temporal:
  rebuild & redeploy as needed



Red Hat

SECURE & AUTOMATE THE CONTENT LIFECYCLE

Trust is temporal; rebuild and redeploy as needed

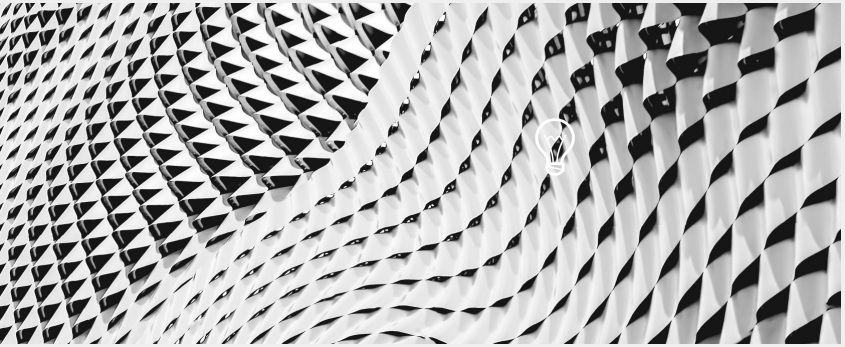


Track updates & simplify management with ImageStreams

Use Image Change Triggers to automatically rebuild custom images with updated (patched) external images

Red Hat

DEFEND INFRASTRUCTURE

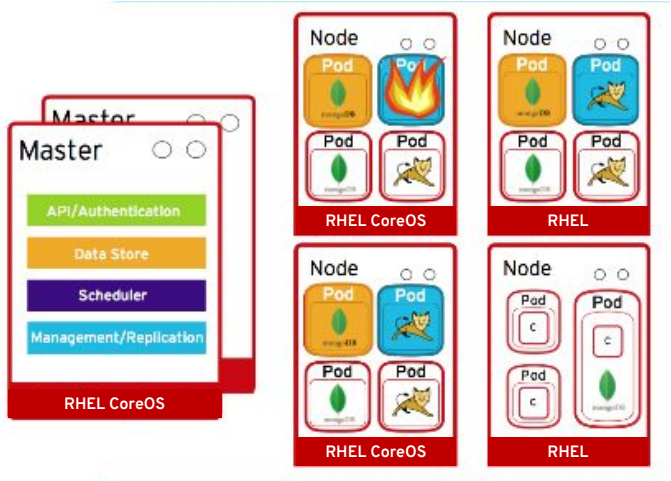


Red Hat

SECURING THE CONTAINER PLATFORM

Security Features Include

- Host & Runtime security
- Identity and Access Management
- Role-based Access Controls
- Project namespaces
- Integrated SDN - Network Policies is default
- Integrated & extensible secrets management
- Logging, Monitoring, Metrics

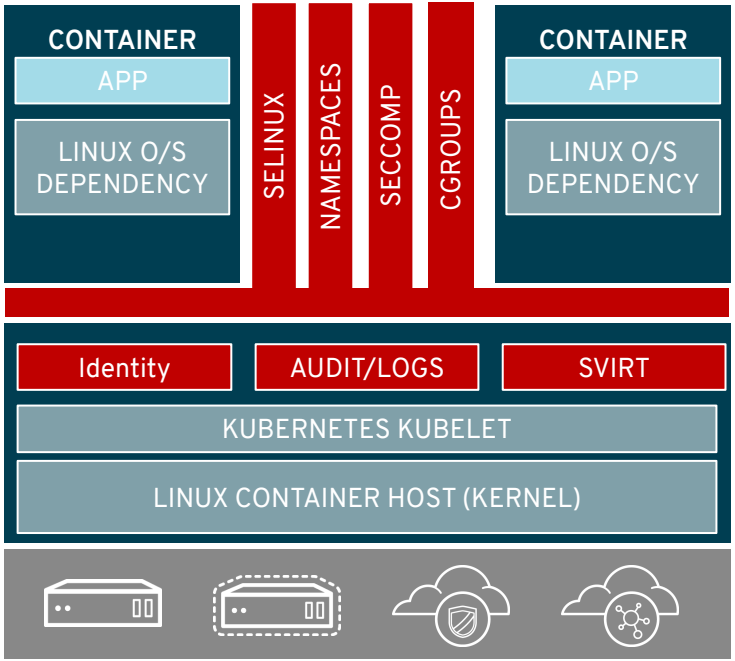


Red Hat

HOST OS CONTAINER MULTI-TENANCY

Container Security starts with Linux Security

- Security in the RHEL host applies to the container
- SELINUX and Kernel Namespaces are the one-two punch no one can beat
- Protects not only the host, but containers from each other
- RHEL CoreOS provides minimized attack surface
- Common Criteria certification



Red Hat

Container Host Vision

An Ideal Container Host would be	RHEL CoreOS
Minimal	Only what's needed to run containers
Secure	Read-only & locked down
Immutable	Immutable image-based deployments & updates
Always up-to-date	OS updates are automated and transparent
Updates never break my apps	Isolates all applications as containers
Updates never break my cluster	OS components are compatible with the cluster
Supported on my infra of choice	Inherits majority of the RHEL ecosystem
Simple to configure	Installer generated configuration
Effortless to manage	Managed by Kubernetes Operators

IMMUTABLE OPERATING SYSTEM

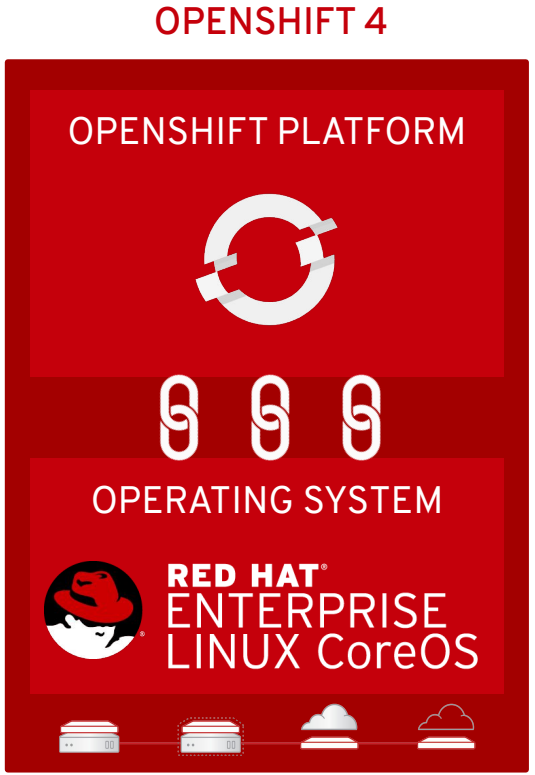
Red Hat Enterprise Linux CoreOS is versioned with OpenShift

CoreOS is tested and shipped in conjunction with the platform. Red Hat runs thousands of tests against these configurations.

Red Hat Enterprise Linux CoreOS is managed by the cluster

The Operating system is operated as part of the cluster, with the config for components managed by Machine Config Operator:

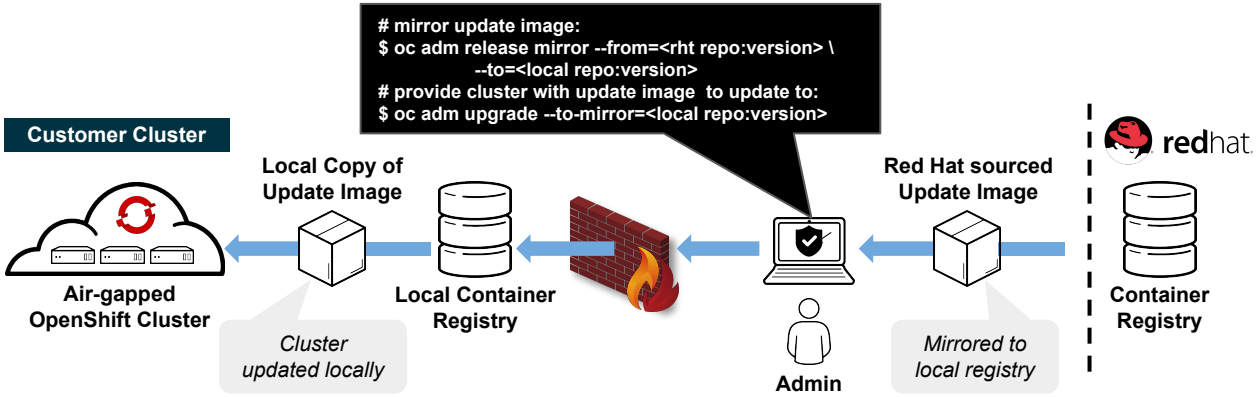
- CRI-O config
- Kubelet config
- Authorized registries
- SSH config



Red Hat

Air-gapped Environments

Disconnected Installation & Updating



- Support for installing and updating of OpenShift clusters in air-gapped environments is targeted for 4.2
- Admins first need to mirror installation and update payload images to a local container registry, then openshift-install and ‘oc adm upgrade’ can be configured to leverage the offline content
  - RH CoreOS images for AWS will also need to be copied to a local S3 bucket and AMI ID defined in install-config

cri-o

A lightweight, OCI-compliant container runtime

Optimized for Kubernetes	Any OCI-compliant container from any OCI registry (including docker)	Improve Security and Performance at scale

[CRI - the Container Runtime Interface]
[OpenShift 4 defaults to CRI-O]
[Red Hat contributes CRI-O to the Cloud Native Computing Foundation]

RUNTIME SECURITY POLICIES

SCC (Security Context Constraints)

Allow administrators to control permissions for pods

Restricted SCC is granted to all users

By default, no containers can run as root

Admin can grant access to privileged SCC

Custom SCCs can be created

```
$ 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 Seccomp Profiles:             <none>
  Allowed Volume Types:                 configMap,downwardAPI,emptyDir,persistentVolumeClaim,projected,
  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
```

IDENTITY AND ACCESS MANAGEMENT

OpenShift includes an OAuth server, which does three things:

- Identifies the person requesting a token, using a configured identity provider
- Determines a mapping from that identity to an OpenShift user
- Issues an OAuth access token which authenticates that user to the API

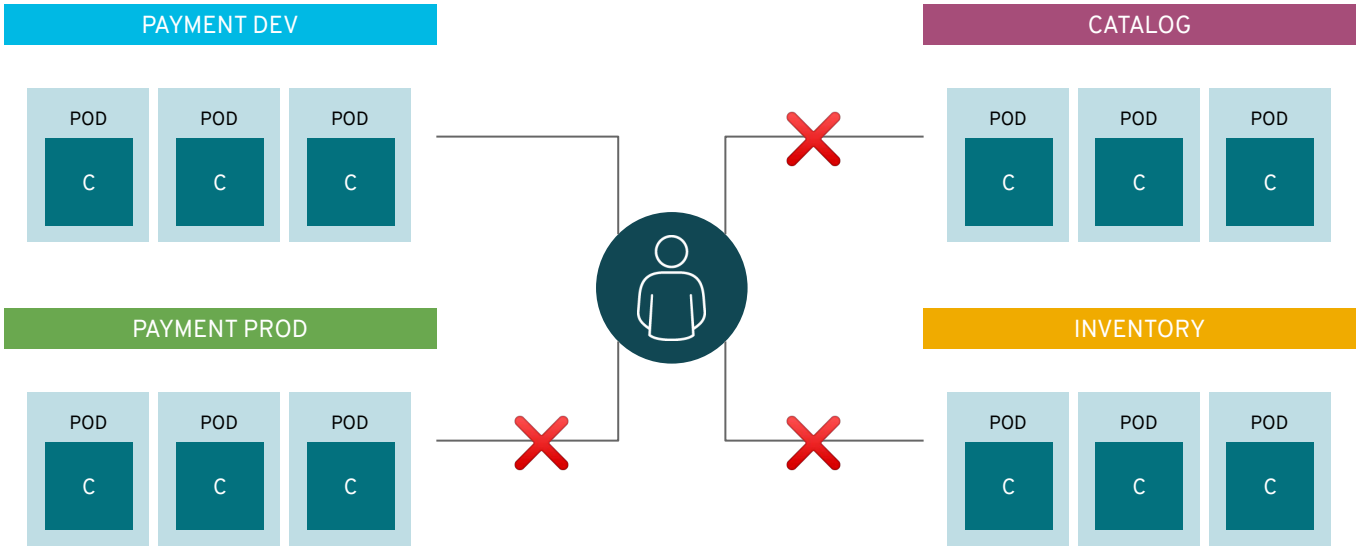
Managing Users and Groups in OpenShift
Configuring Identity Providers

Supported Identity Providers include

- Keystone
- LDAP
- GitHub
- GitLab
- GitHub Enterprise (new with 3.11)
- Google
- OpenID Connect
- Security Support Provider Interface (SSPI) to support SSO flows on Windows (Kerberos)

PROJECTS ISOLATE APPLICATIONS

across teams, groups and departments



Red Hat

RESTRICT ACCESS BY NEED TO KNOW

Role based authorization

- Project scope & cluster scope available
- Matches request attributes (verb,object,etc)
- If no roles match, request is denied (deny by default)
- Operator- and user-level roles are defined by default
- Custom roles are supported

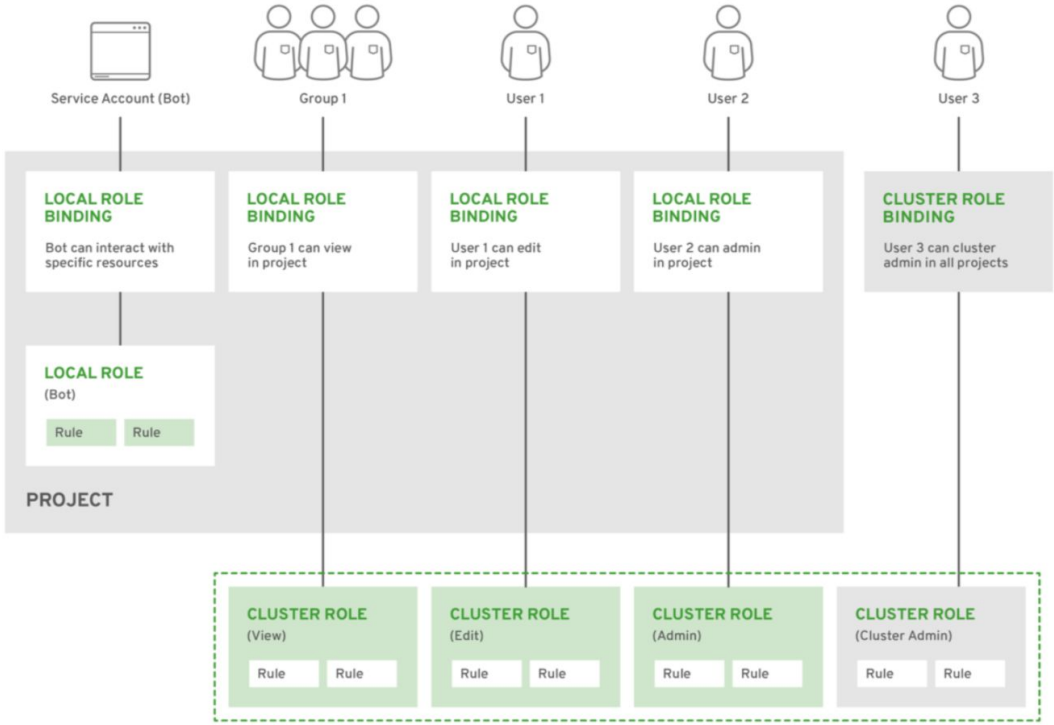
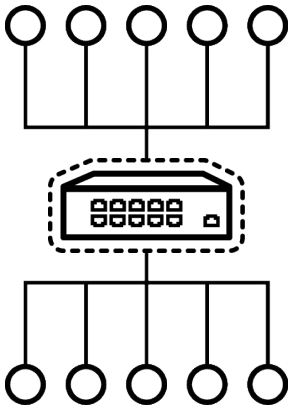


Figure 12 - Authorization Relationships

For more information see: [Managing RBAC in OpenShift]

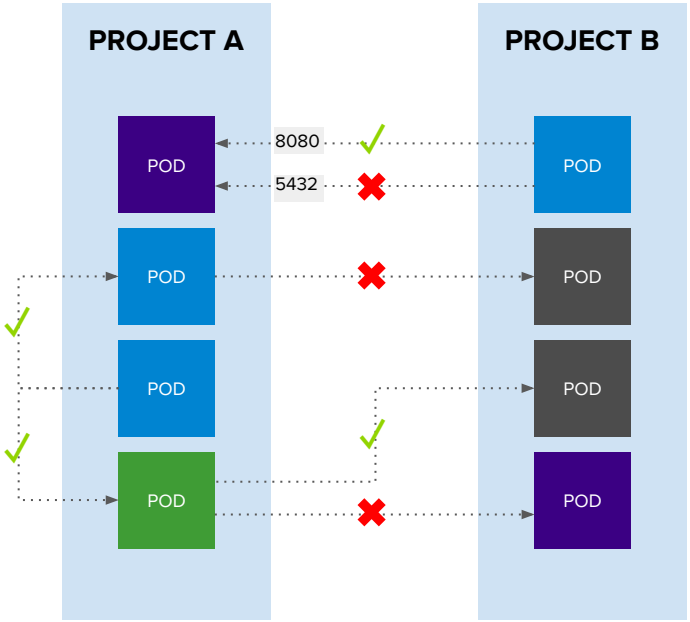
OPENSHIFT NETWORKING

- Built-in internal DNS to reach services by name
- Software Defined Networking (SDN) for a unified cluster network to enable pod-to-pod communication
- OpenShift follows the Kubernetes Container Networking Interface (CNI) plug-in model
- Isolate applications from other applications within a cluster
- Isolate environments (Dev / Test / Prod) from other environments within a cluster



OPENSHIFT SDN

Network Policy enabled by default in OpenShift 4



Example Policies

- Allow all traffic inside the project
- Allow traffic from green to gray
- Allow traffic to purple on 8080

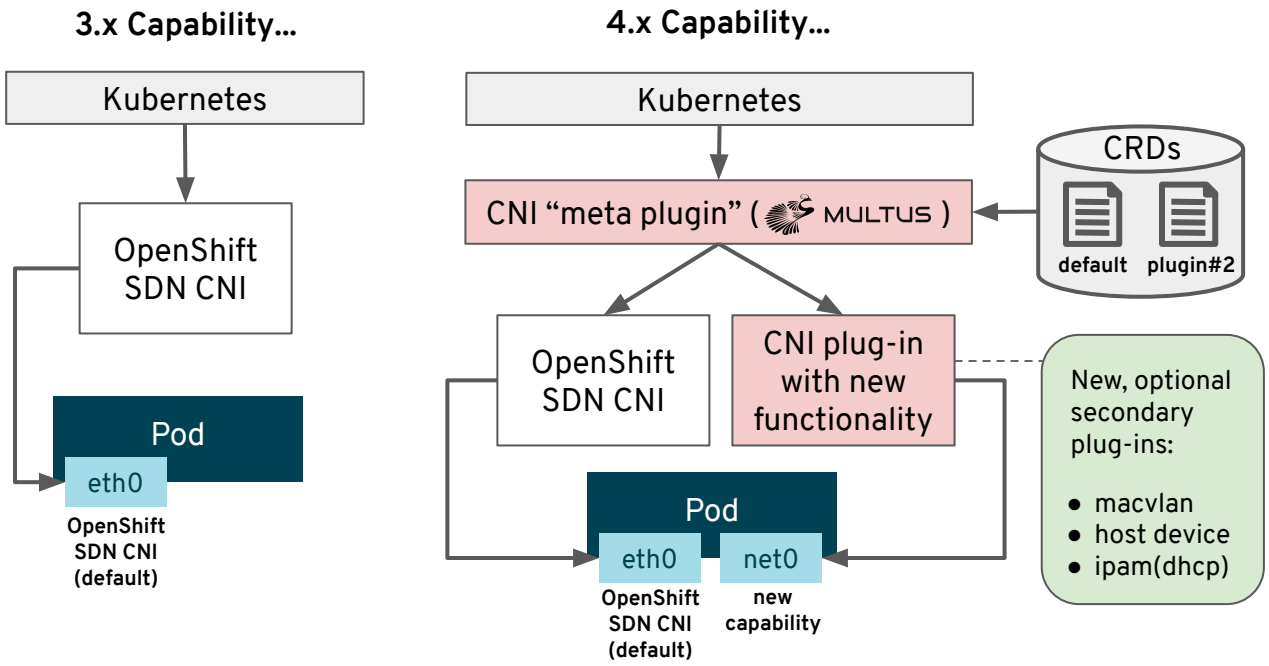
```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
  - ports:
    - protocol: tcp
      port: 8080
```

OPENSHIFT MULTUS

Multus Enables Multiple Networks & New Functionality to Existing Networking

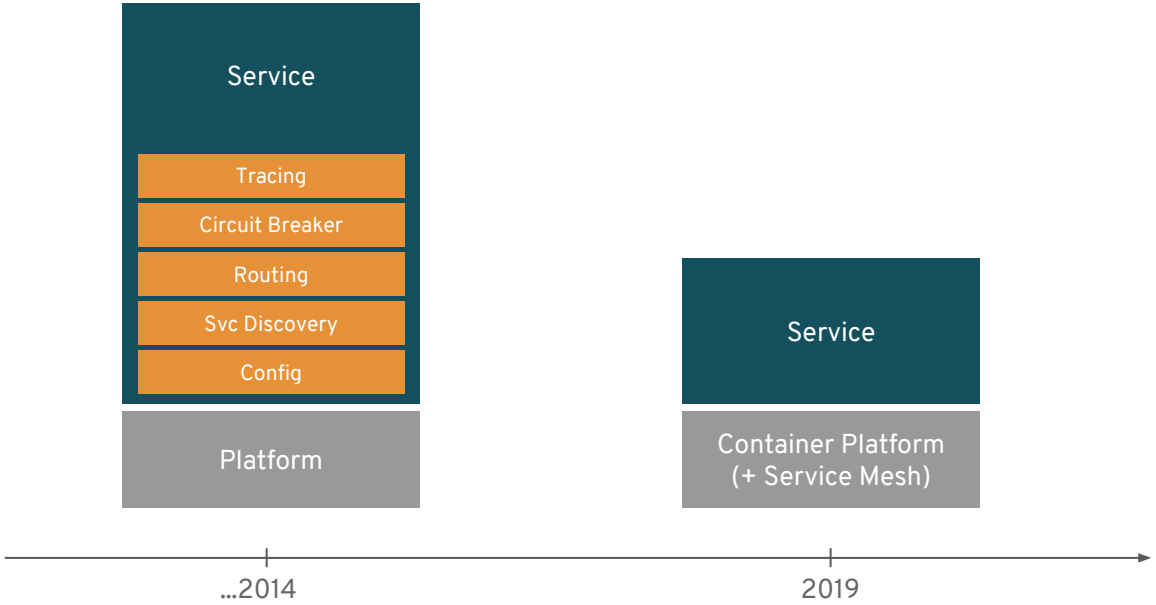
The Multus CNI “meta plugin” for Kubernetes enables one to create multiple network interfaces per pod, and assign a CNI plugin to each interface created.

1. Create pod annotation(s) to call out a list of intended network attachments…
2. …each pointing to CNI network configurations packed inside CRD objects



Red Hat

MICROSERVICES EVOLUTION



Red Hat

RED HAT SERVICE MESH

Applies security, route rules, policies and reports traffic telemetry at the pod level

Jaeger

Secure

Istio

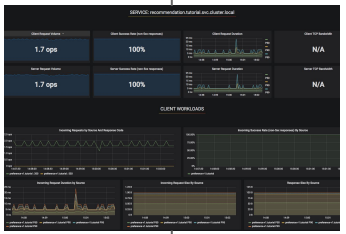
Observe

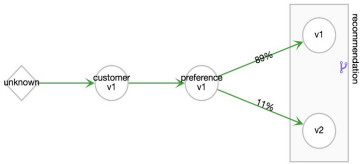
Connect

Control

Prometheus

Observe





kiali

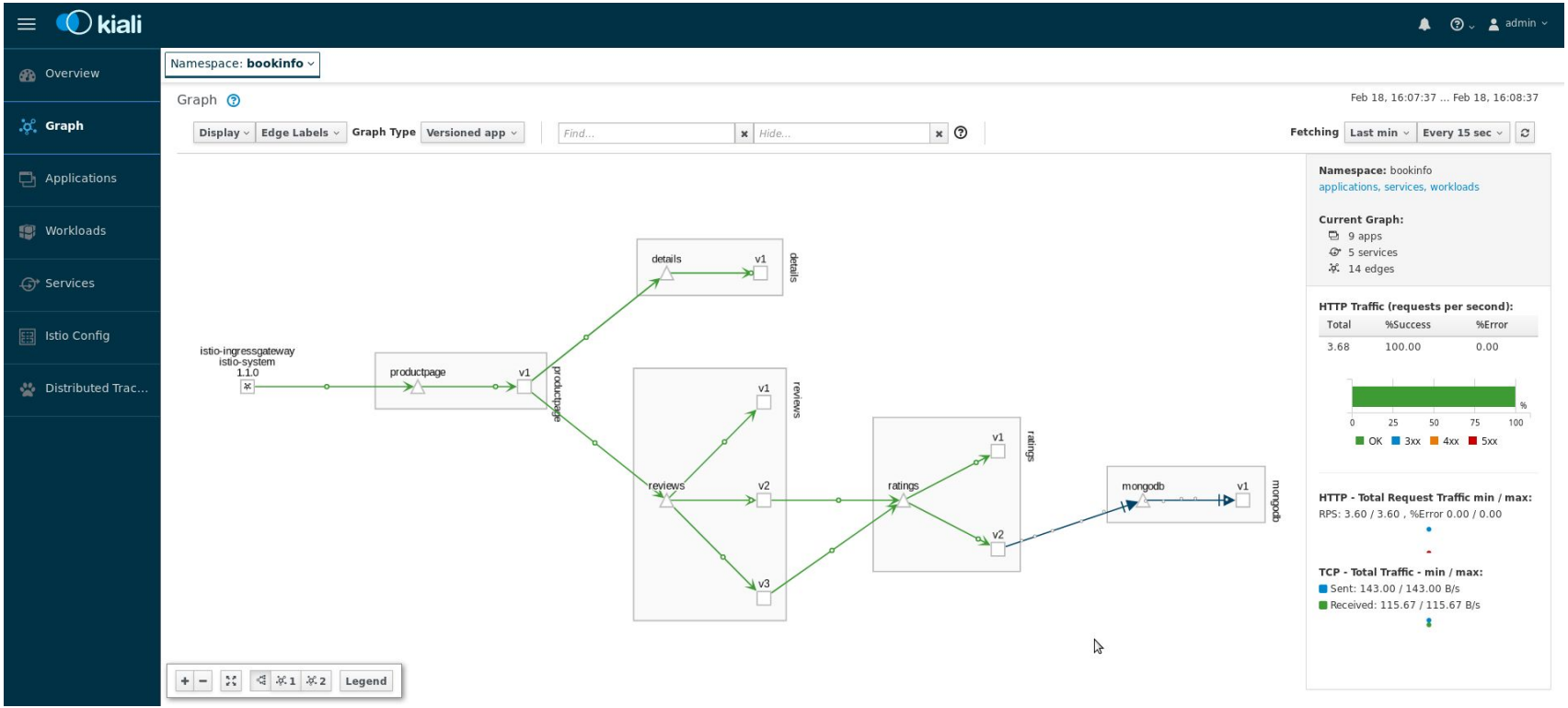
Kiali

Grafana

Generally Available in July

Red Hat

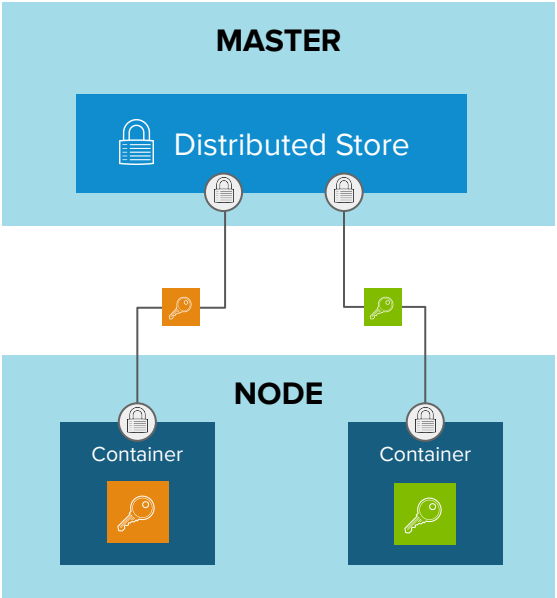
OBSERVABILITY WITH KIALI



Red Hat

SECRETS MANAGEMENT

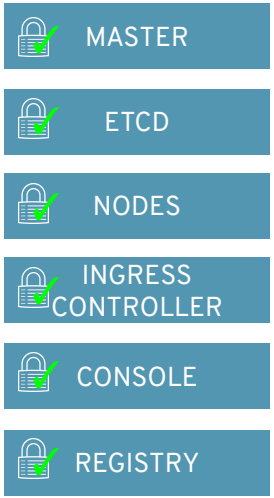
- Secure mechanism for holding sensitive data e.g.
  - Passwords and credentials
  - SSH Keys
  - Certificates
- Secrets are made available as
  - Environment variables
  - Volume mounts
  - Interaction with external systems (e.g. vaults)
- Encrypted in transit and at rest*
- Never rest on the nodes



* Full disk encryption is supported for AWS, VSphere. Encrypting the etcd datastore is not available in OCP 4.1. Targeted for OCP 4.3.

CERTIFICATE MANAGEMENT

- Certificates are used to provide secure connections to
  - master and nodes
  - Ingress controller and registry
  - etcd
- Certificate rotation is automated
- Optionally configure external endpoints to use custom certificates
- For example:
  [Requesting and Installing Let's Encrypt Certificates for OpenShift 4]

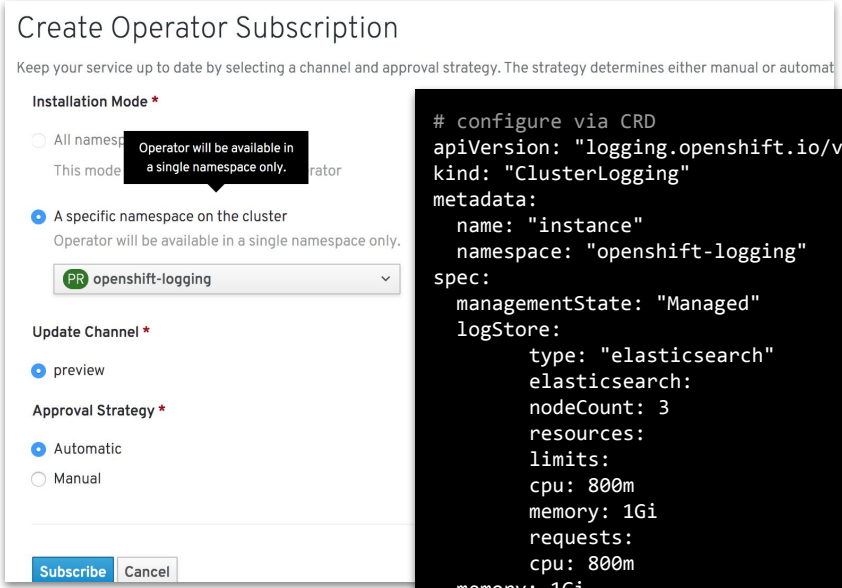


Red Hat

CLUSTER LOG MANAGEMENT

Install the Elasticsearch and Cluster Logging Operators from OperatorHub

- EFK stack aggregates logs for hosts and applications
  - Elasticsearch: a search and analytics engine to store logs
  - Fluentd: gathers logs and sends to Elasticsearch.
  - Kibana: A web UI for Elasticsearch.
- Access control
  - Cluster administrators can view all logs
  - Users can only view logs for their projects
  - Central Audit policy configuration
- Ability to send logs elsewhere
  - External elasticsearch, Splunk, etc

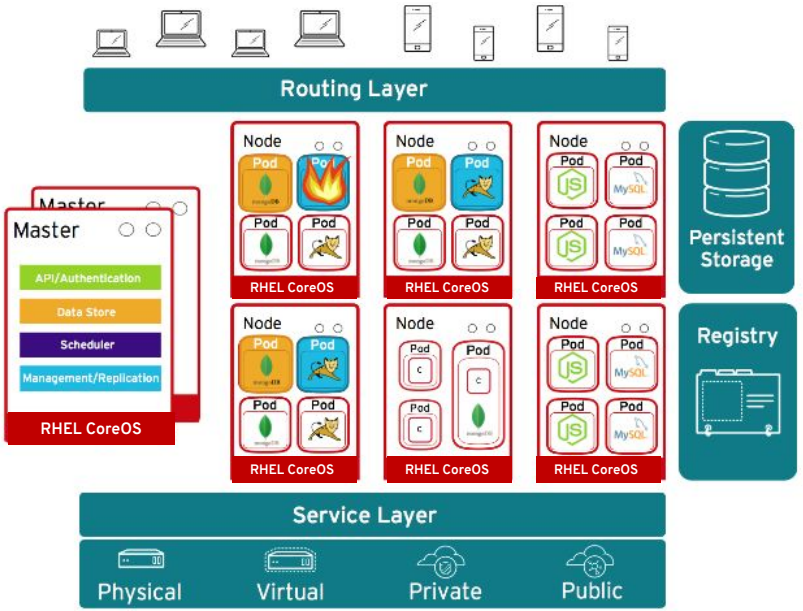



```
# configure via CRD
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"
  namespace: "openshift-logging"
spec:
  managementState: "Managed"
  logStore:
        type: "elasticsearch"
        elasticsearch:
        nodeCount: 3
        resources:
        limits:
        cpu: 800m
        memory: 1Gi
        requests:
        cpu: 800m
  memory: 1Gi
  storage:
        storageClassName: gp2
        size: 100G
        redundancyPolicy: "SingleRedunda
  visualization:
        type: "kibana"
        kibana:
        replicas: 1
  curation:
```

ATTACHED STORAGE

Secure storage by using

- SELinux access controls
- Secure mounts
- Supplemental group IDs for shared storage

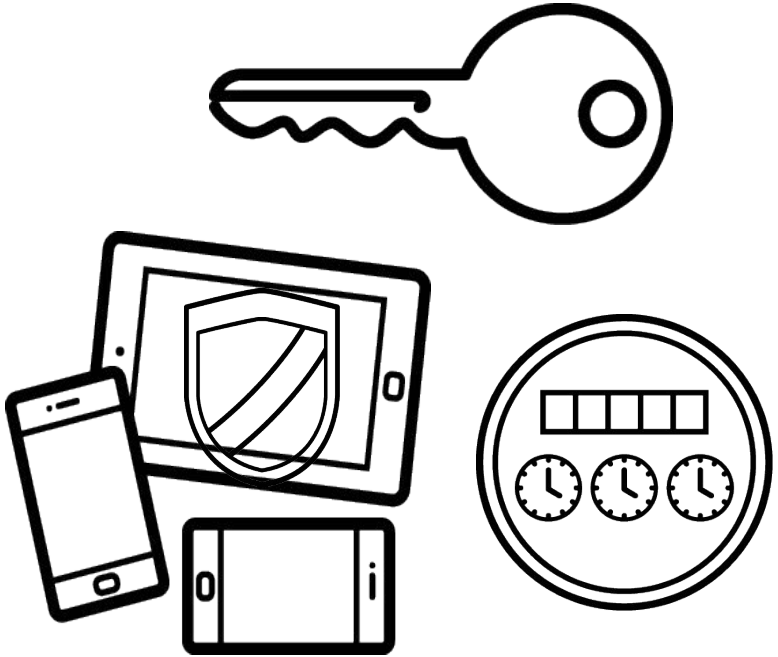


Red Hat

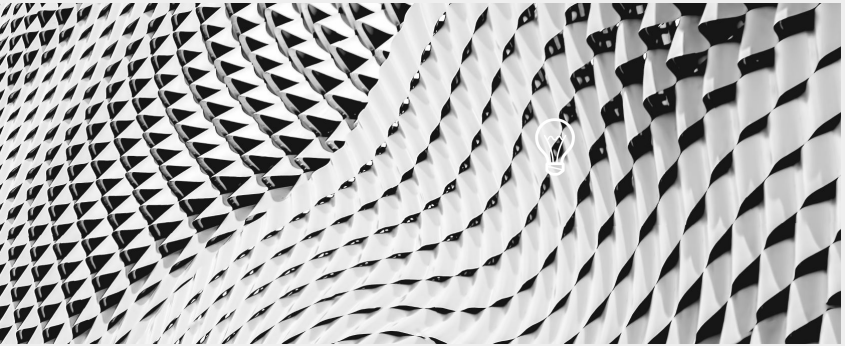
APPLICATION API MANAGEMENT

Container platform & application APIs

- Authentication and authorization
- LDAP integration
- End-point access controls
- Rate limiting

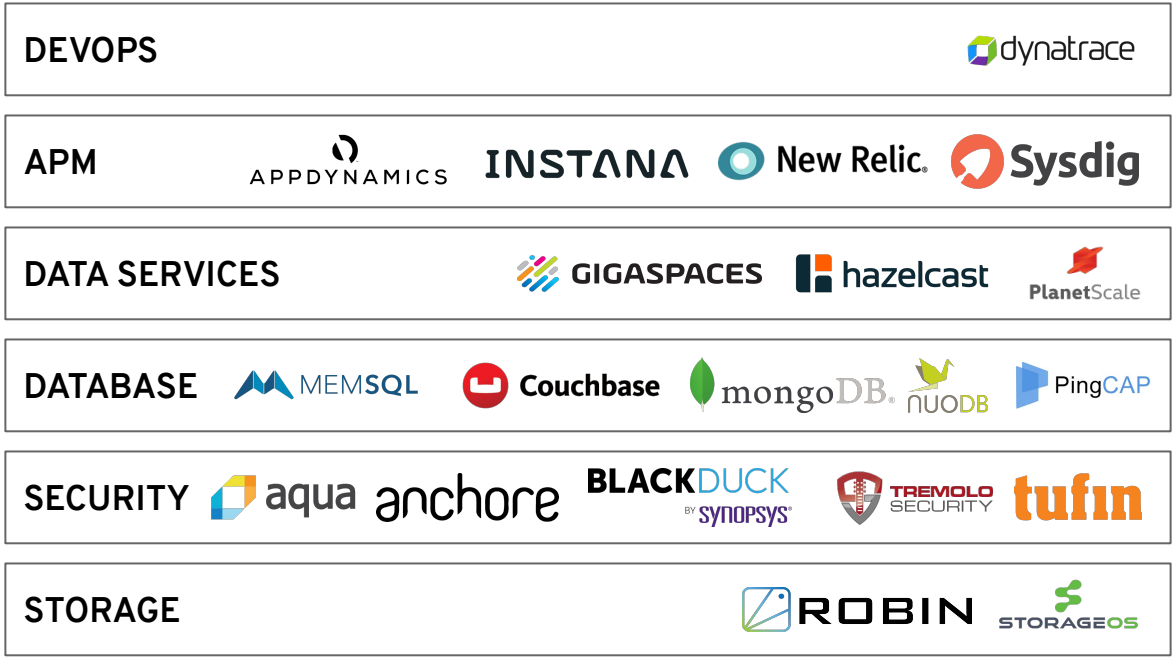


EXTEND SECURITY



Red Hat

RED HAT CERTIFIED OPERATORS



Red Hat

THE BROAD SECURITY ECOSYSTEM

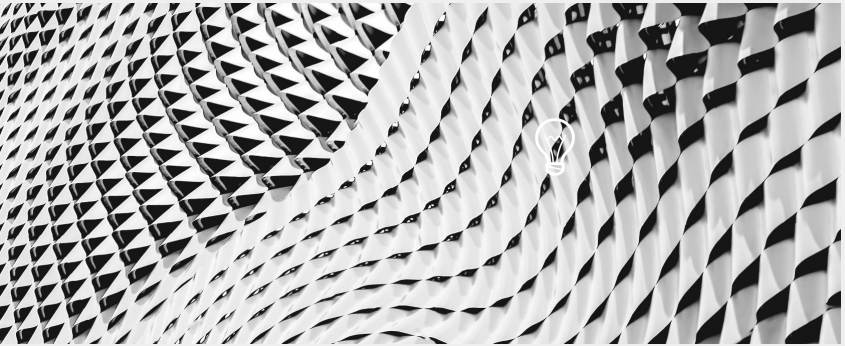







Red Hat

ROADMAP



Red Hat

SECURITY FEATURE ROADMAP

DEFENSE IN DEPTH - Control, Defend, Extend

Linux Host Security
- RHCOS FIPS mode
  RHCOS Auditd

Authentication & Authorization
- Integration with external Keycloak
- Use group membership from external IPs

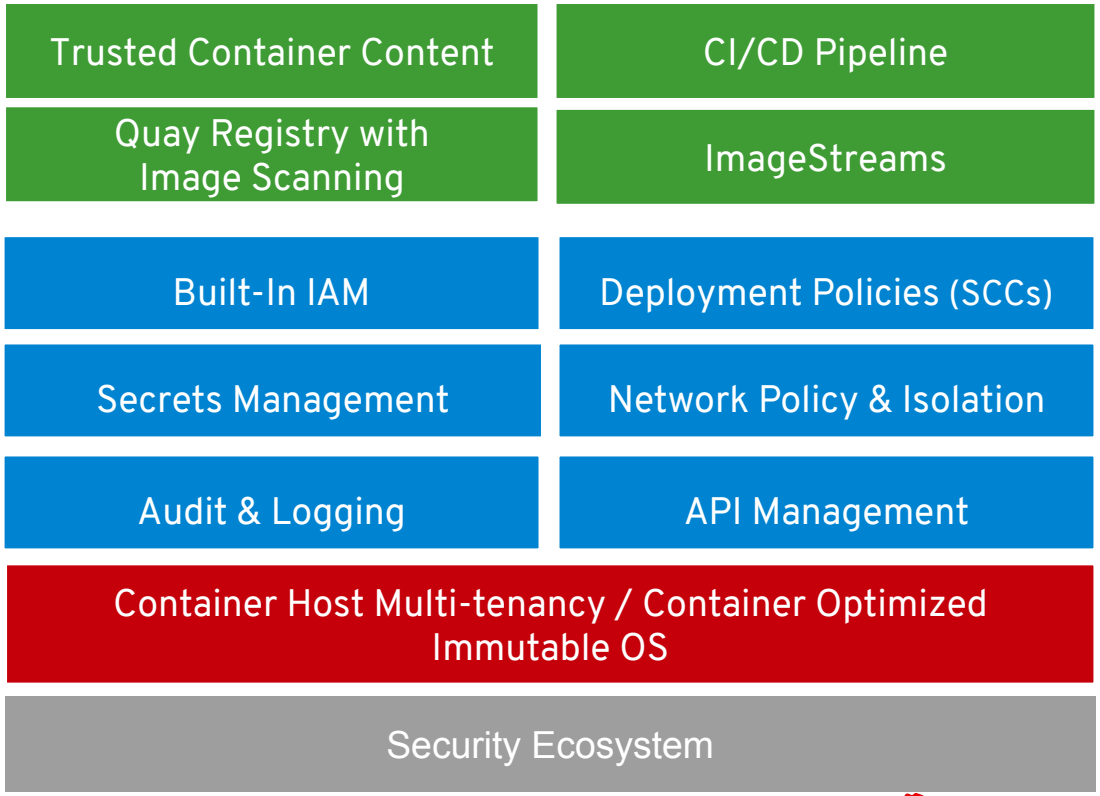
Secrets & Certificates
- Improved cert management and Integration with external CAs via ACME
- Integration with external Key Management Systems

Integrated Audit & Logging
- East / West traffic tracing with OpenShift Service Mesh (GA summer 2019)

Network Policies
- Control service access flow with OpenShift Service Mesh (GA summer 2019)

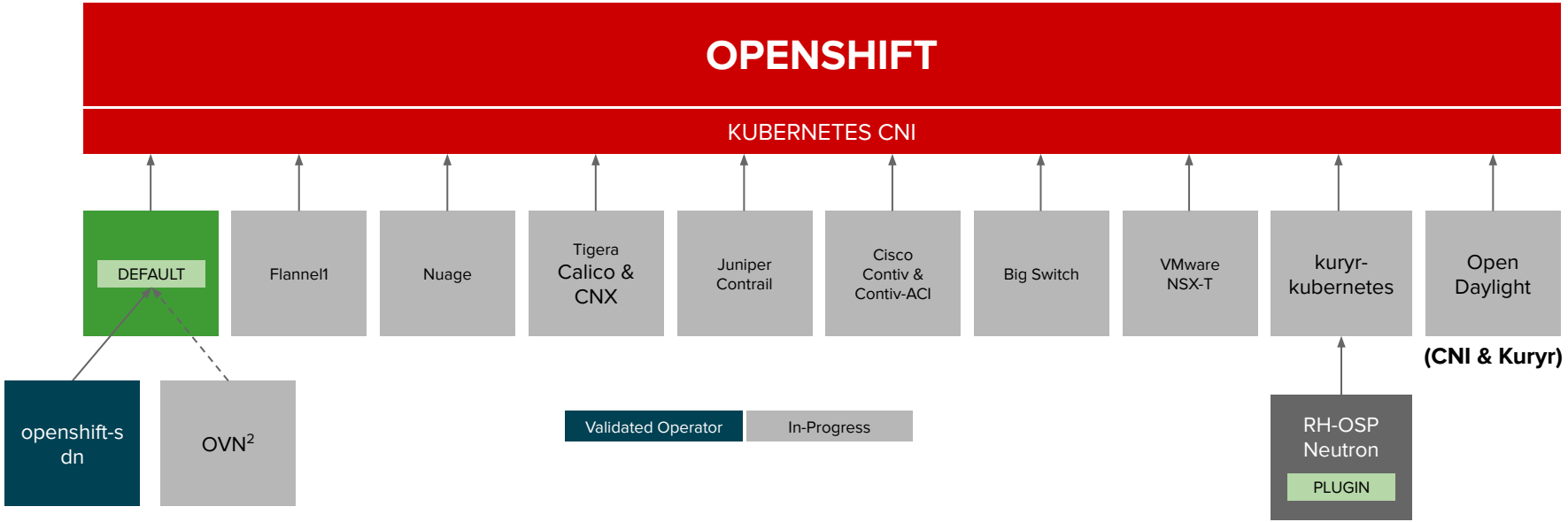
Networking Isolation
- East / West mutual TLS authentication with OpenShift Service Mesh (GA summer 2019)

Image Security
- Clair v3 covers more content



Red Hat

OPENSHIFT NETWORK PLUGINS

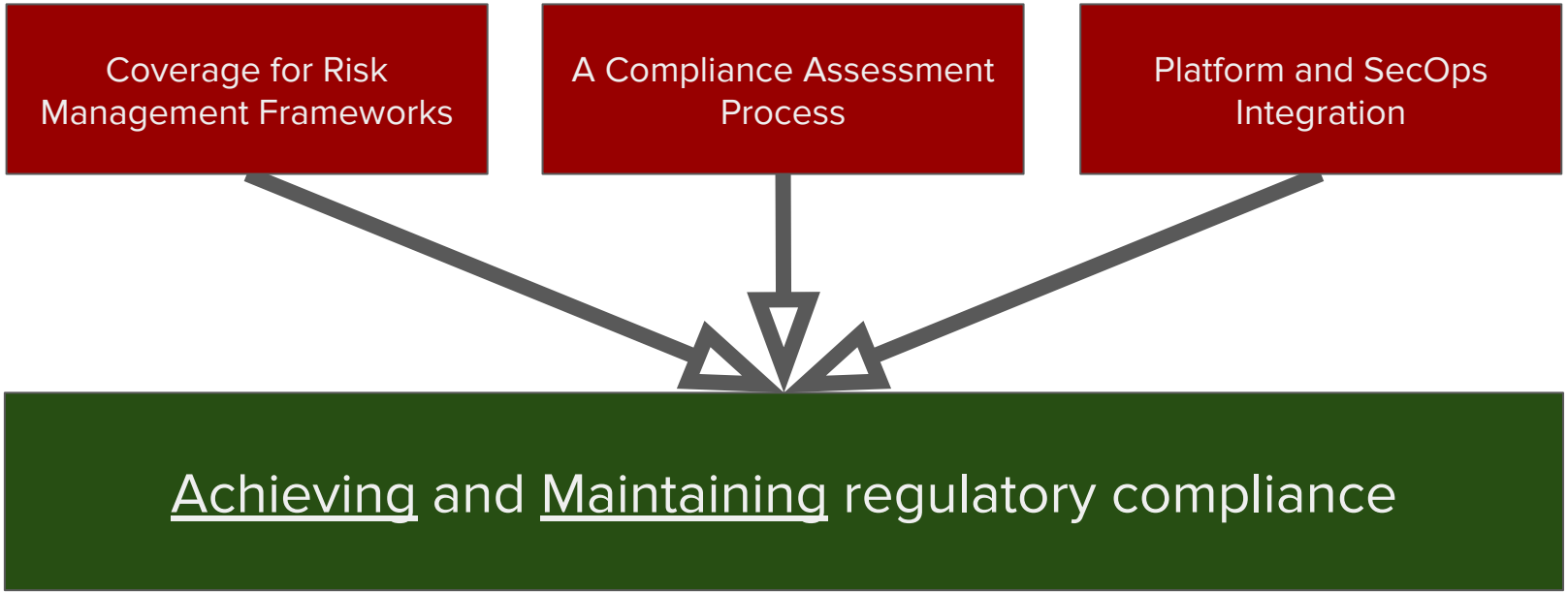


[1] Flannel is minimally verified and is supported only and exactly as deployed in the OpenShift on OpenStack reference architecture
[2] Targeting OCP 4.2 GA

Red Hat

RISK MANAGEMENT AND COMPLIANCE GOALS

Automate compliance audit and remediation



VIRT-BASED CONTAINERS

What is the future for KVM isolated containers?

- Lots of interest from customers in this area
- All of these solutions have limitations, compatibility issues, and are not mature enough to support
- Customers seem to get less excited as they learn about the gaps
- Not mature enough to be on our product roadmaps
- Kata seems to be the most promising solution and community
    - We are engaged upstream and currently bringing kata into Fedora

gVisor

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


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat