Red Hat Security Day
We start at 9:30 / 8:30 UK Time

Please write your name here :
http://etherpad-etherpad.apps.shift.rhepds.com/p/
(the link is also in the chat !!)

Alfred Bach
Technical Partner Enablement Manager
abach@redhat.com

Red Hat

OpenShift from a security perspective

Alfred Bach
Technical Partner Enablement Manager
abach@redhat.com

Red Hat

About me ..

Alfred Bach
Technical Partner Enablement Manager

Living in Austria near Vienna

4 Years with Red Hat
Coming from CA and SUSE/NOVELL

abach@redhat.com

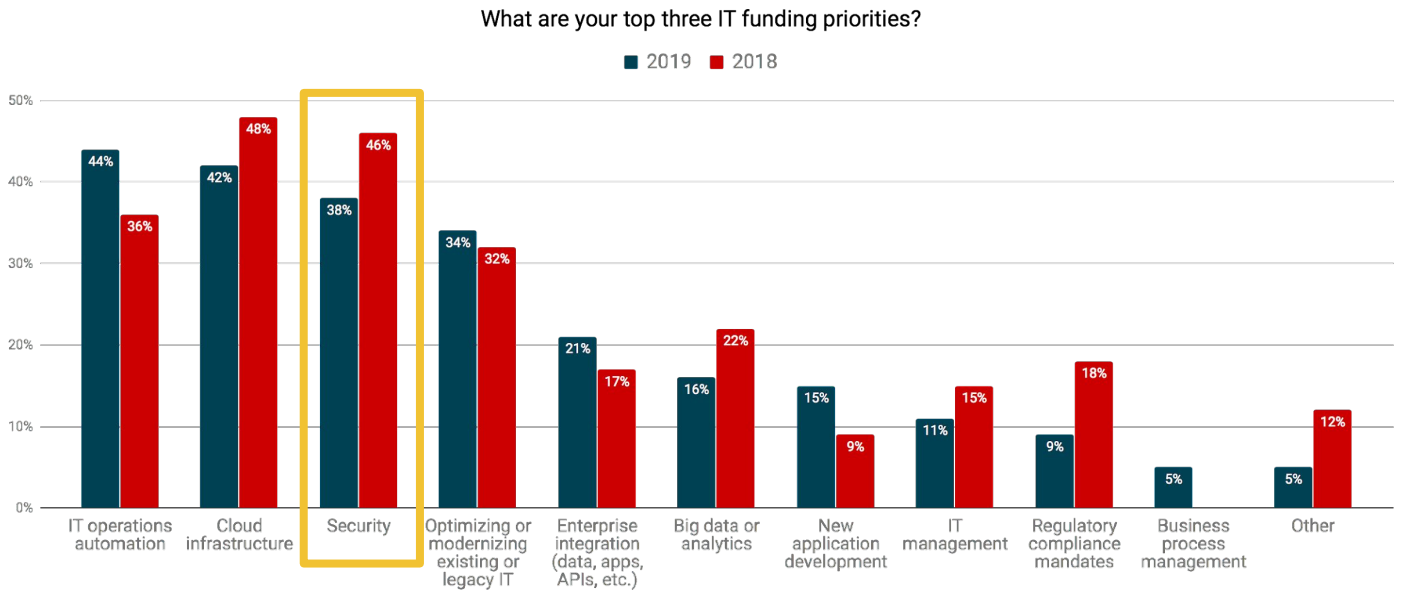
Red Hat

About you ?

https://www.menti.com/e1tqzb6n8b

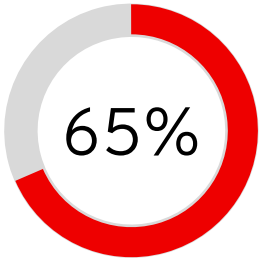
Red Hat

Top Funding Priorities for 2019: Automation, Cloud, & Security

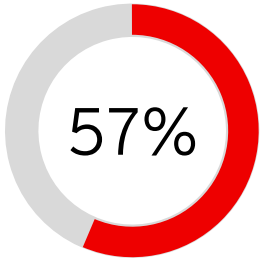


Source: Global IT Trends & Priorities Research, November 2018, Qualtrics and Red Hat

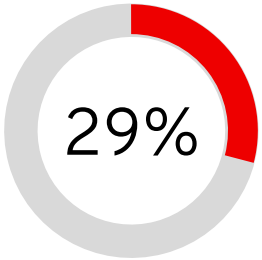
The Cyber Security Challenge is not Getting Easier



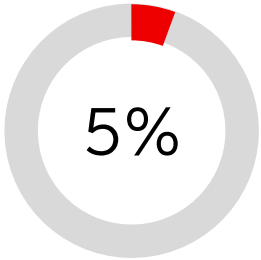
Reported increased Severity of attacks



Said the time to resolve an incident has grown



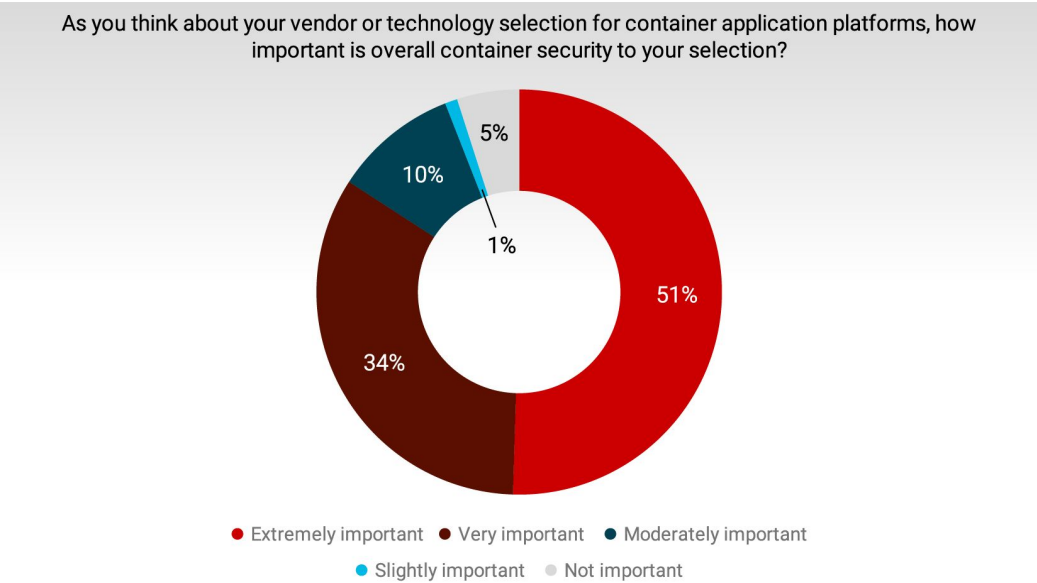
Have their ideal security-skilled staffing level, making it the #2 barrier to Cyber resilience



Portio of alerts coming in that the average security team examines every day

[1] The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute, 2018 (Sponsored by IBM)
[2] https://venturebeat.com/2017/12/16/the-lesson-behind-2017s-biggest-enterprise-security-story/

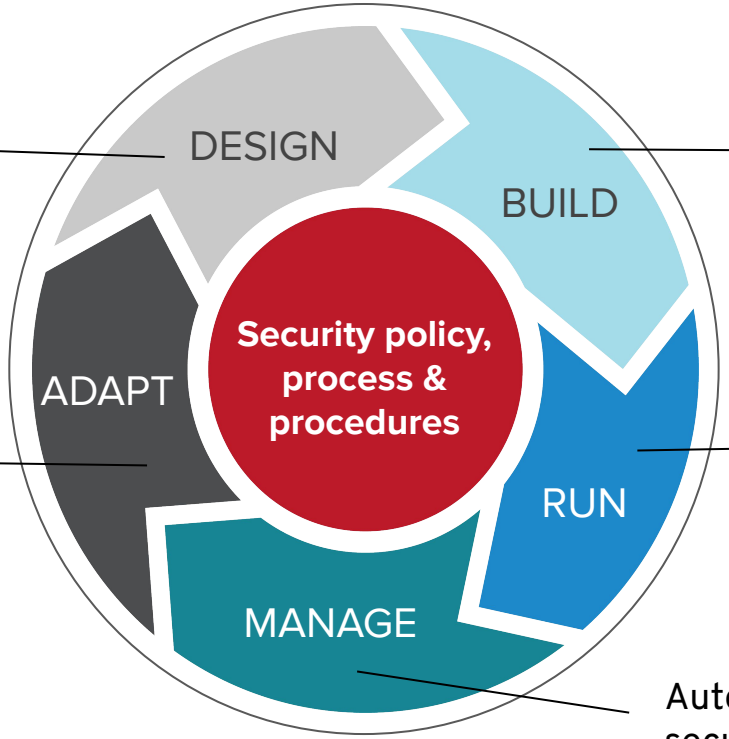
Choosing a Container Platform Vendor? Security is Critical



Source: Global IT Trends & Priorities Research, November 2018, Qualtrics and 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

OpenShift 3

- NIST National Checklist for Red Hat OpenShift Container Platform 3
- FISMA Moderate
- ISO 27001
- PCI-DSS Reference Architecture

OpenShift Hardening Guide for 3.11

- Inspired by CIS Kubernetes benchmark v1.2

Targeted for 1H CY 2020

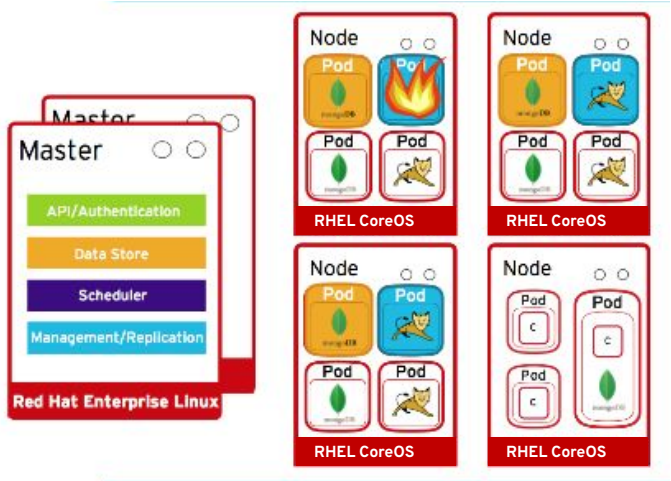
OpenShift 4

- Target Q1 CY 2020
  - HIPAA
  - HITRUST
  - OCP Hardening Guide for 4.3
- Target Q2 CY 2020
  - FISMA
  - ISO 27001
  - PCI-DSS

What Does It Take To Secure the Infrastructure?

OpenShift security features include

- Host & Runtime security
- Identity and Access Management
- Role-based Access Controls
- Project namespaces
- Network isolation
- Integrated & extensible secrets management
- Logging, Monitoring, Metrics, Audit



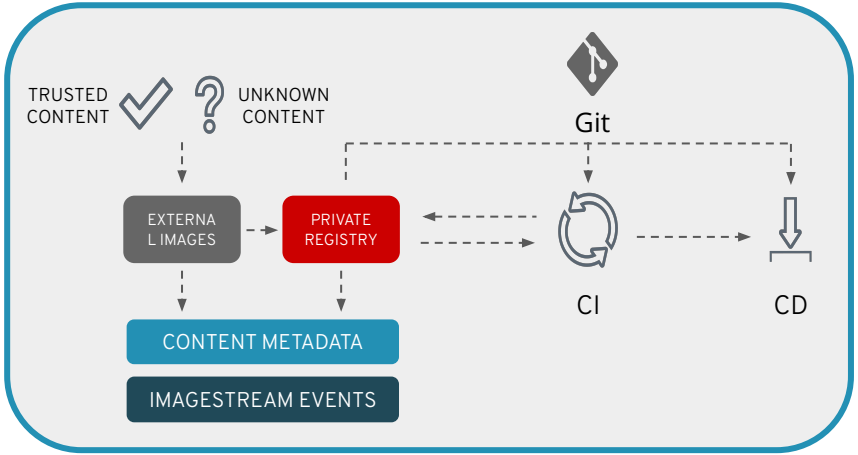
Red Hat

Securing Containerized Applications

An opportunity to shift security left

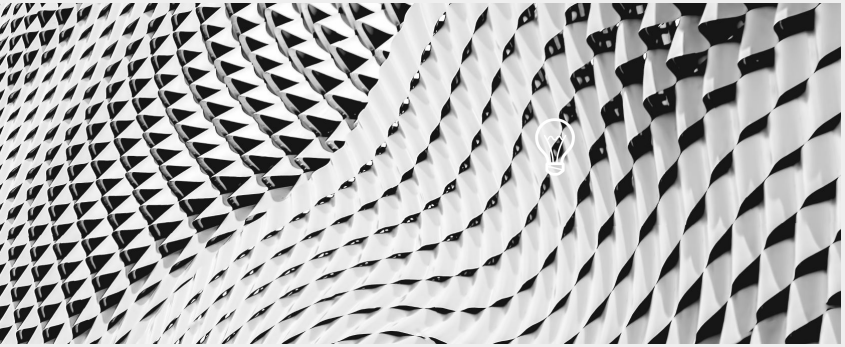
Best practices

- Use trusted sources for external content
- Use a private registry to manage images
- CI/CD must have security gates
- Application secrets management
- Apply runtime security policies
- Rebuild and redeploy - never patch a running container
- Ensure application logging, monitoring



Red Hat

DEFEND INFRASTRUCTURE

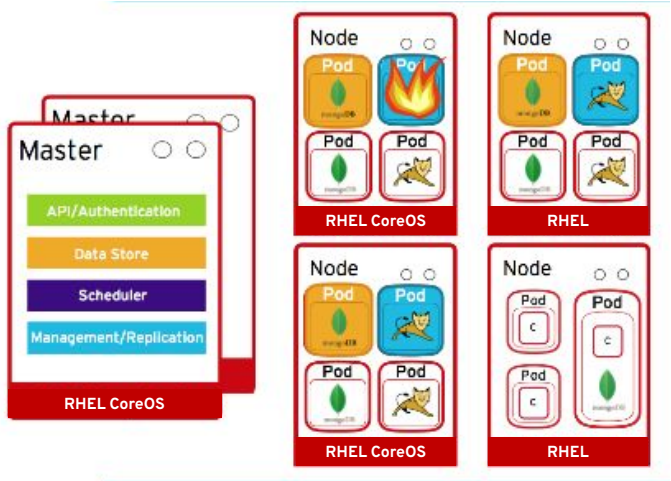


Red Hat

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

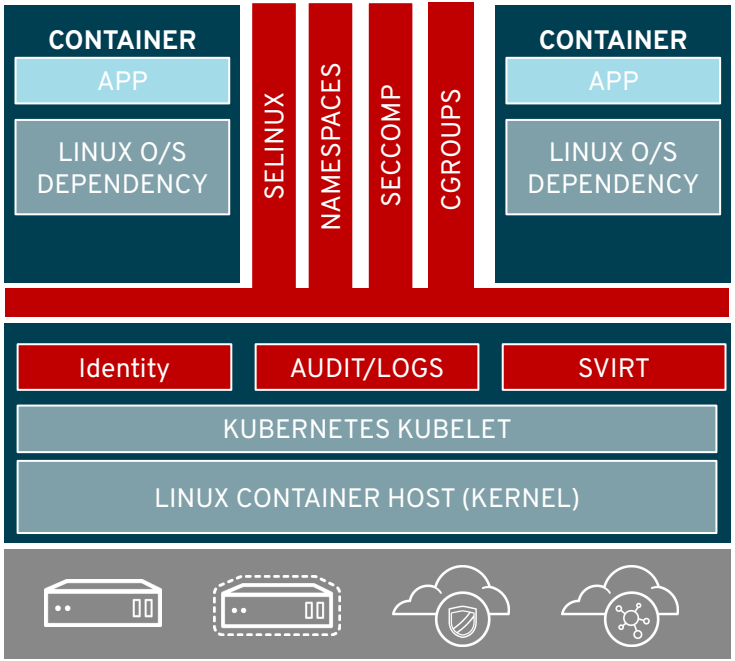


Red Hat

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



Red Hat

SELINUX MITIGATES CONTAINER RUNTIME VULNERABILITIES

SELinux Mitigates container Vulnerability

January 13, 2017 | Joe Brockmeier

< Back to all posts Tags

A new CVE, (CVE-2016-9962), for the docker container runtime and runc were rec
released. Fixed packages are being prepared and shipped for RHEL as well as Fedo
CentOS. This CVE reports that if you `exec` d into a running container, the processe
the container could attack the process that just entered the container.

https://www.redhat.com/en/blog/selinux-mitigates-container-vulnerability

Latest container exploit (runc) can be blocked by SELinux

February 28, 2019 | Dan Walsh

< Back to all posts Tags: *Security*, *Containers*

A flaw in runc (CVE-2019-5736), announced last week, allows container processes to "escape" their containment and execute programs on the host operating system. The good news is that well-configured SELinux can stop it.

https://www.redhat.com/en/blog/latest-container-exploit-runc-can-be-blocked-selinux

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

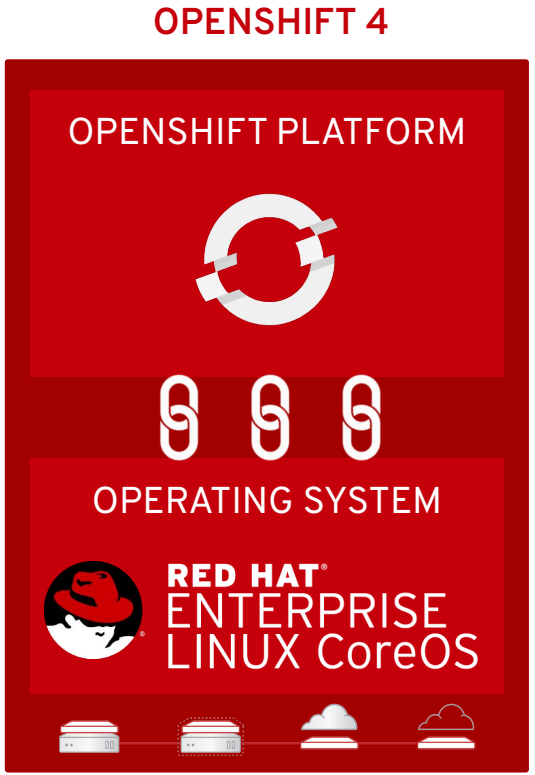
Red Hat Enterprise Linux CoreOS is versioned with OpenShift

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

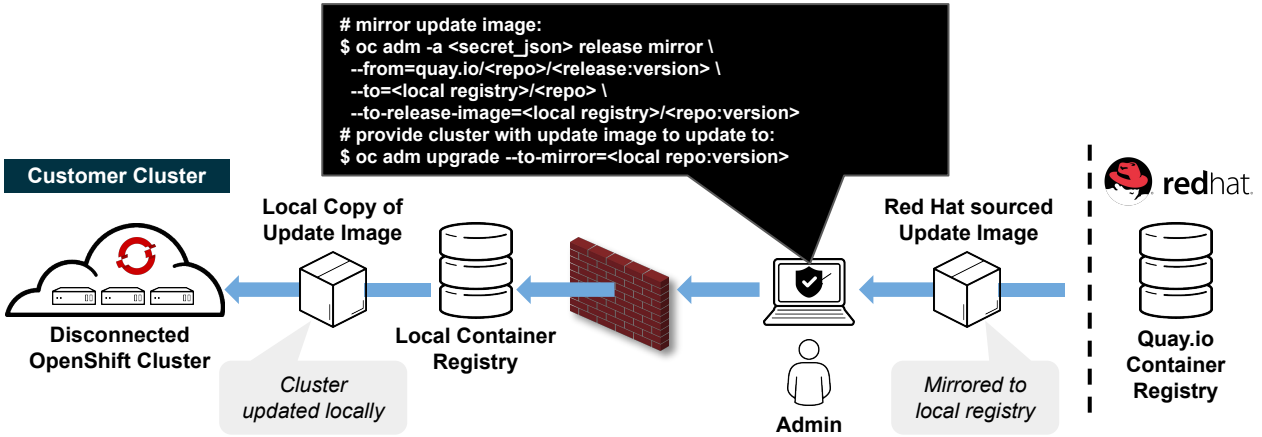
The Operating system is operated as part of the cluster, with the config for components managed by Machine Config Operator:

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



Red Hat

DISCONNECTED “AIR-GAPPED” INSTALL & UPGRADE



Overview

- 4.2 introduces support for installing and updating OpenShift clusters in disconnected environments
- Requires local Docker 2.2 spec compliant container registry to host OpenShift content
- Designed to work with the user provisioned infrastructure deployment method
  - *Note: Will not work with Installer provisioned infrastructure deployments*

Installation Procedure

- Mirror OpenShift content to local container registry in the disconnected environment
- Generate install-config.yaml: $ ./openshift-install create install-config --dir <dir>
  - Edit and add pull secret (PullSecret), CA certificate (AdditionalTrustBundle), and image content sources (ImageContentSources) to install-config.yaml
- Set the OPENSHIFT_INSTALL_RELEASE_IMAGE_OVERRIDE environment variable during the creation of the ignition configs
- Generate the ignition configuration: $ ./openshift-install create ignition-configs --dir <dir>
- Use the resulting ignition files to bootstrap the cluster deployment

Generally Available

Red Hat

OpenShift 4 and Fips 140-2

FIPS ready Services

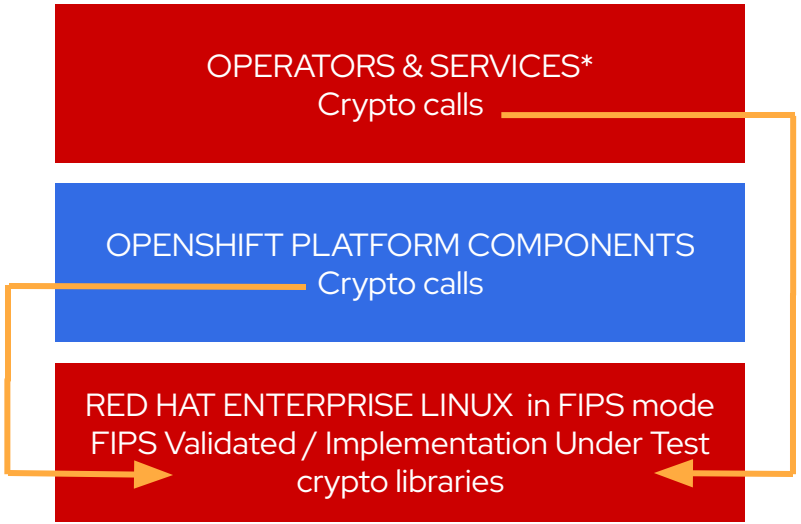
- When built with RHEL 7 base image

OpenShift calls FIPS validated crypto

- When running on RHEL 7.6 in FIPS mode, OpenShift components bypass go cryptographic routines and call into a RHEL FIPS 140-2 validated cryptographic library
- This feature is specific to binaries built with the RHEL go compiler and running on RHEL

RHEL CoreOS FIPS mode

- Configure at install to enforce use of FIPS Implementation Under Test* modules



*When built with RHEL base images

More about RHEL go and FIPS 140-2

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)

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

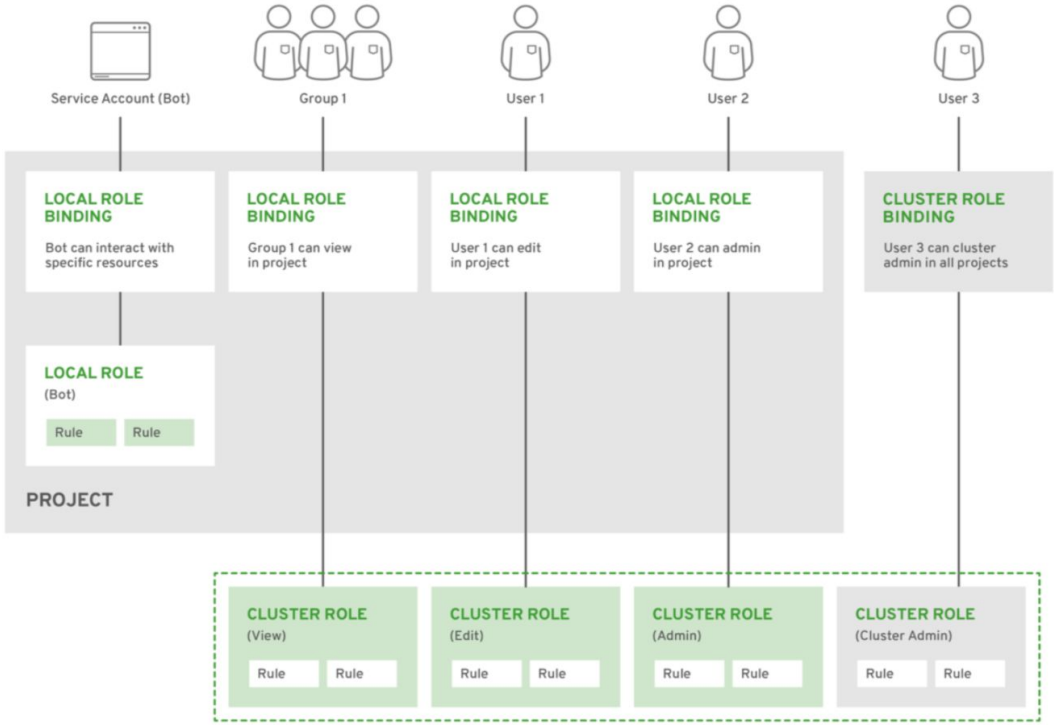


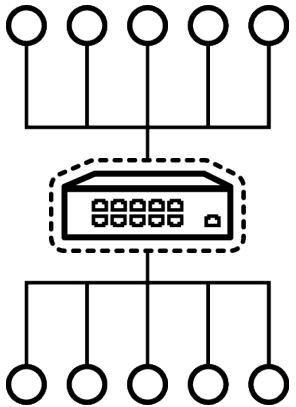
Figure 12 - Authorization Relationships

For more information see: [Managing RBAC in OpenShift]

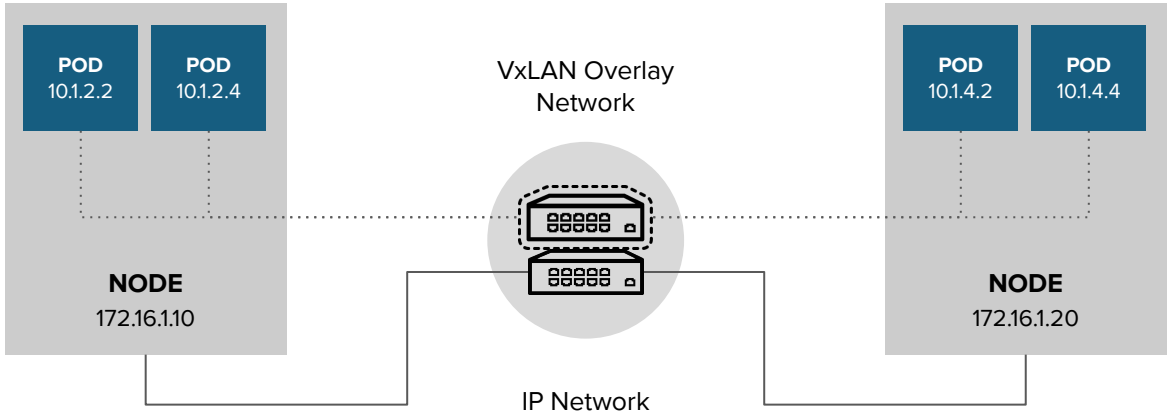
Network security

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

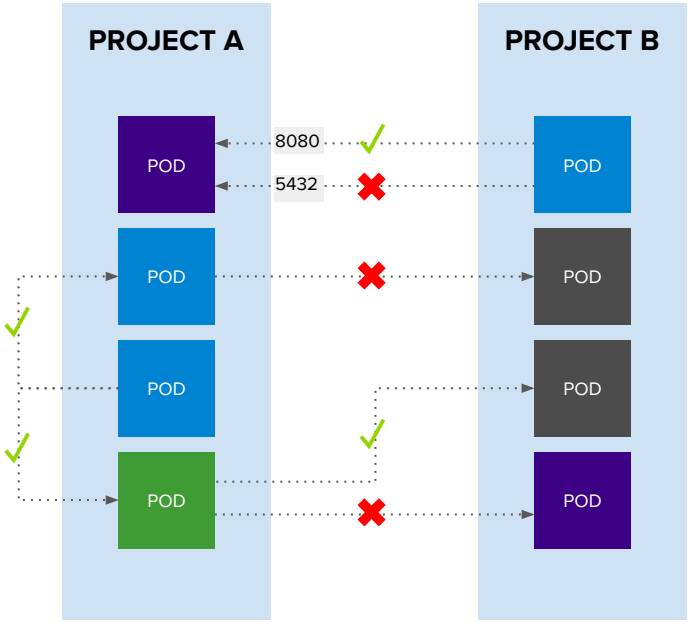


OPENSHIFT POD to POD NETWORKING



OPENSHIFT SDN

Network Policy enabled by default in OpenShift 4



Example Policies

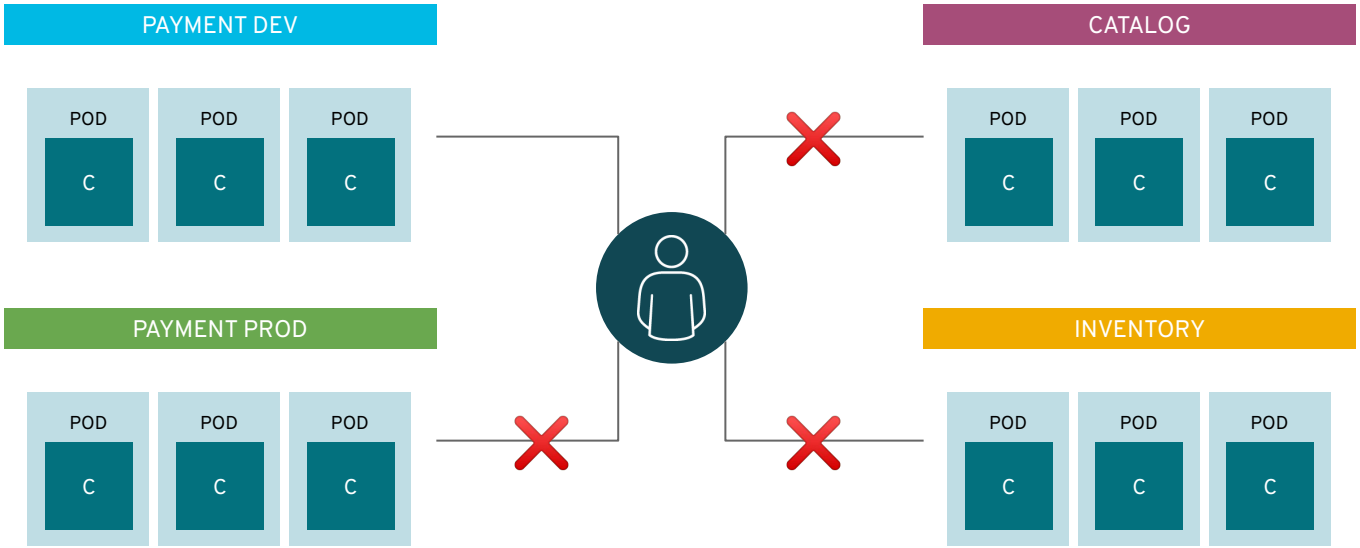
- Allow all traffic inside the project
- Allow traffic from green to gray
- Allow traffic to purple on 8080

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


Red Hat

PROJECTS ISOLATE APPLICATIONS

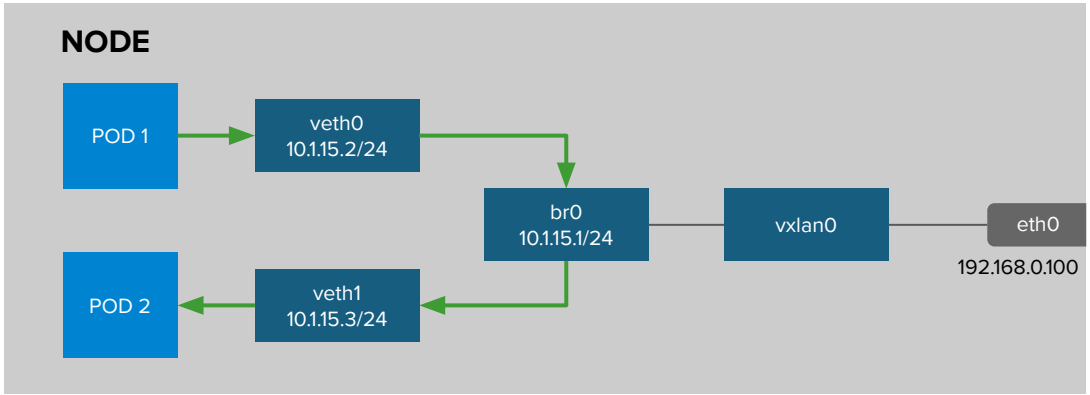
across teams, groups and departments



Red Hat

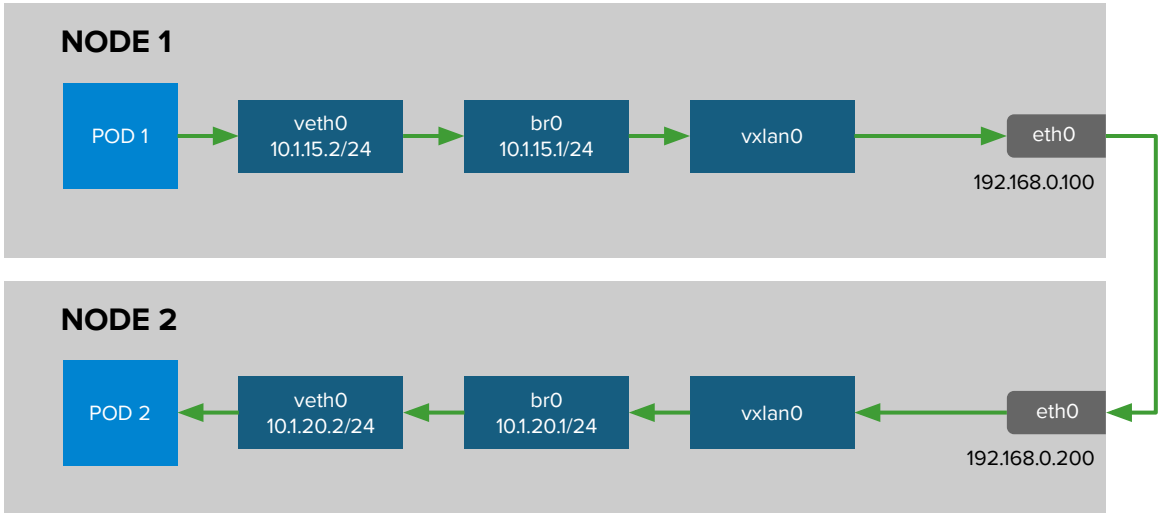
OPENSHIFT SDN - OVS PACKET FLOW

Container to Container on the Same Host



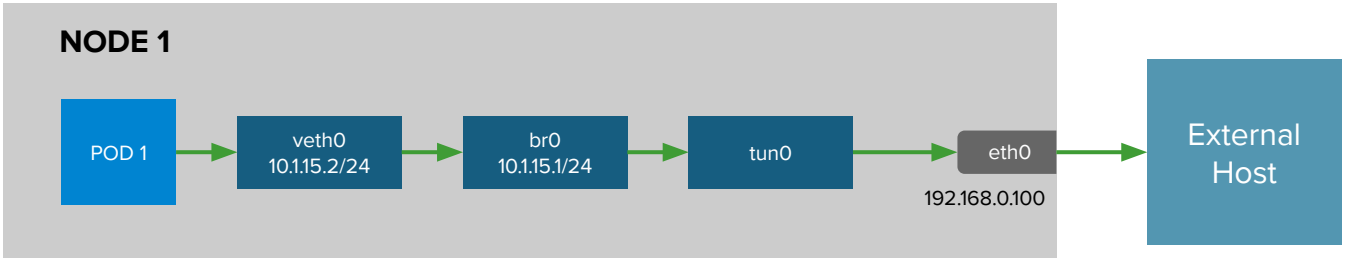
OPENSHIFT SDN - OVS PACKET FLOW

Container to Container on the Different Hosts



OPENSHIFT SDN - OVS PACKET FLOW

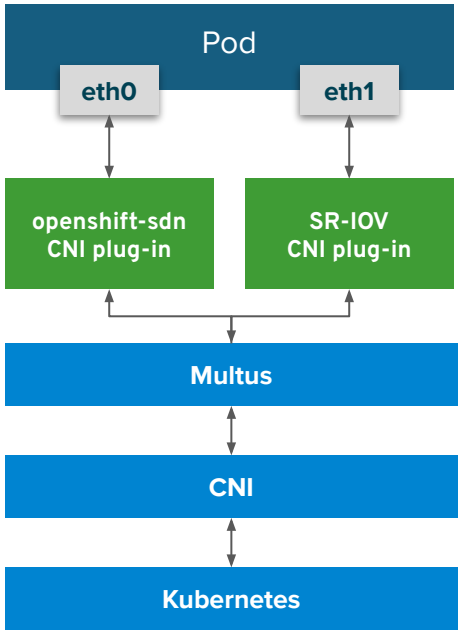
Container Connects to External Host



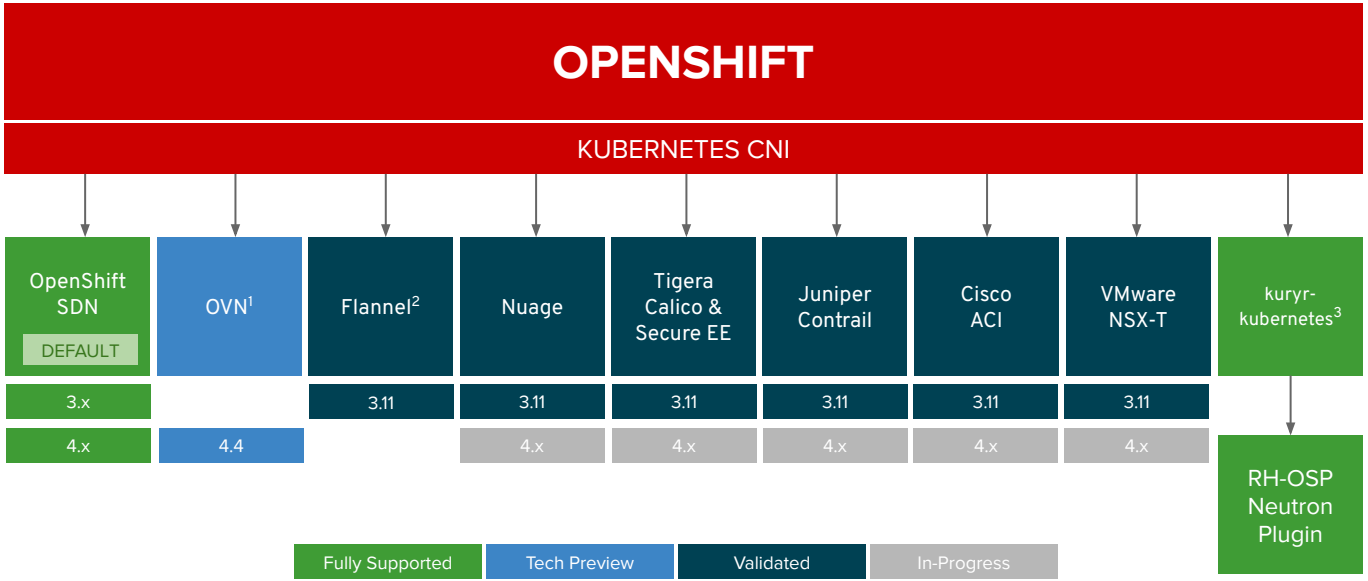
Multus

- Problem: Kubernetes only supports one network interface, “eth0”, but we need:
  - Functional separation of control/data planes
  - Link aggregation for network redundancy
  - Different network protocol stacks, capabilities, SLAs
  - Traffic isolation / Network segregation and security
  - QoS
- Solution: Multus “meta plug-in” for Kubernetes CNI
- Enables multiple network interfaces per pod, each assigned a different CNI plug-in defined in pod spec
  - Each with its configuration defined in CRD objects
- SR-IOV enablement

Pod with Multus



OPENSHIFT NETWORK PLUGINS

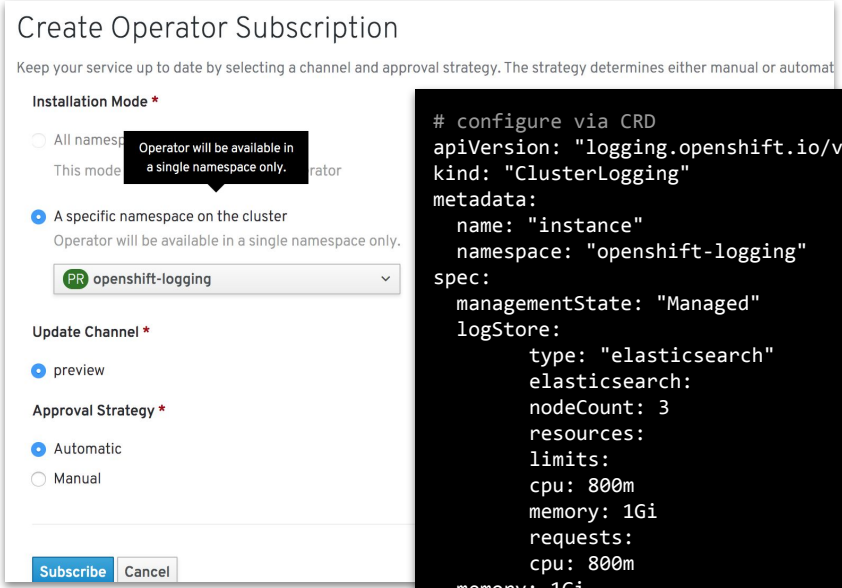


[1]Targeting GA at OCP 4.3 (not default SDN)
[2]Flannel is minimally verified and is supported only and exactly as deployed in the OpenShift on OpenStack reference architecture
[3]Available as an install-time option at 3.11.119 and 4.2.z (targeting 4.2.2)

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

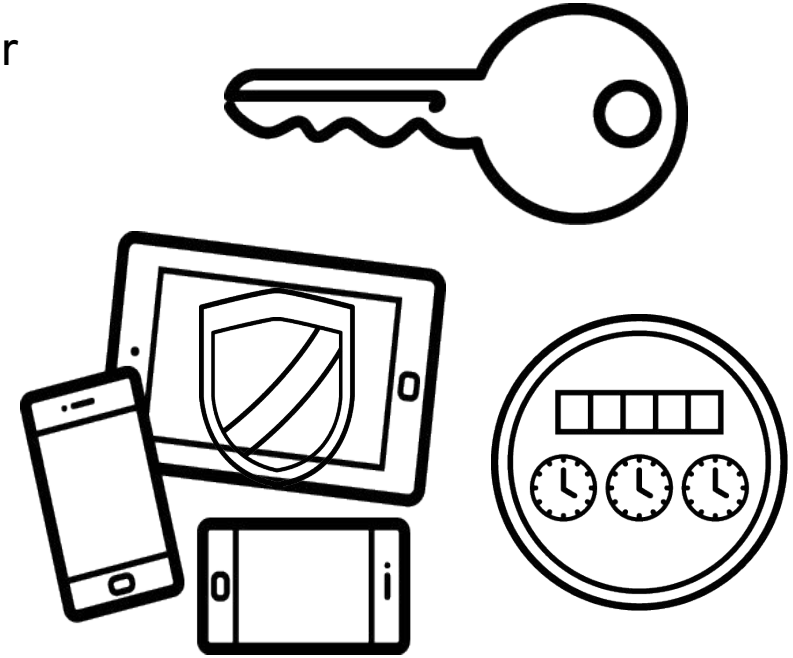



```
# configure via CRD
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"
  namespace: "openshift-logging"
spec:
  managementState: "Managed"
  logStore:
        type: "elasticsearch"
        elasticsearch:
        nodeCount: 3
        resources:
        limits: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

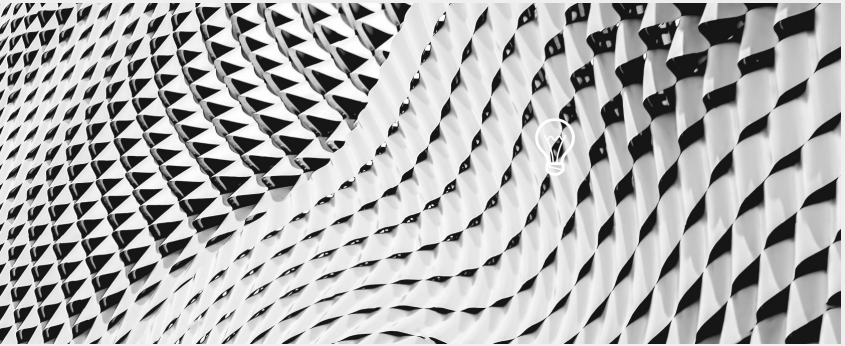
APPLICATION API MANAGEMENT

Consider configuring an API gateway for container platform & application APIs

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



CONTROL APPLICATION SECURITY



Red Hat

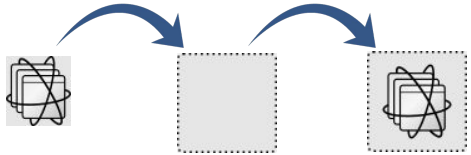
NEXT-GEN CONTAINER TOOLS

Providing stability, flexibility and performance with containers and images

Container-tools - OCI tooling to create, run, and manage, Linux Containers with an enterprise life cycle.

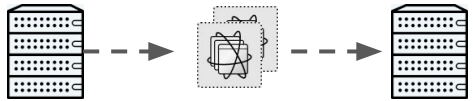
- Conform to the OCI image and runtime specifications
- Daemon-less, OS-native container tooling
- Separation of concerns

buildah



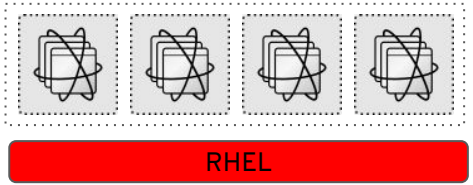
Build OCI/docker Images

skopeo



Inspect, copy, & sign Images

podman



run, manage, debug containers

Red Hat

cri-o

A lightweight, OCI-compliant container runtime

Optimized for Kubernetes

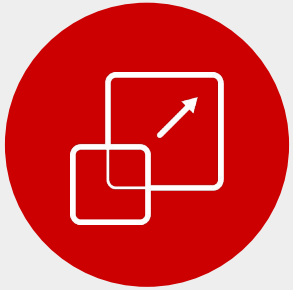
Any OCI-compliant container from any OCI registry
(including docker)

Improve Security and Performance at scale

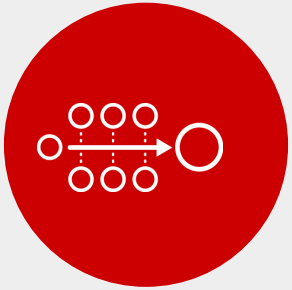
[CRI - the Container Runtime Interface]
[OpenShift 4 defaults to CRI-O]
[Red Hat contributes CRI-O to the Cloud Native Computing Foundation]

OPENSHIFT LOVES CI/CD

JENKINS-AS-A SERVICE
ON OPENSHIFT



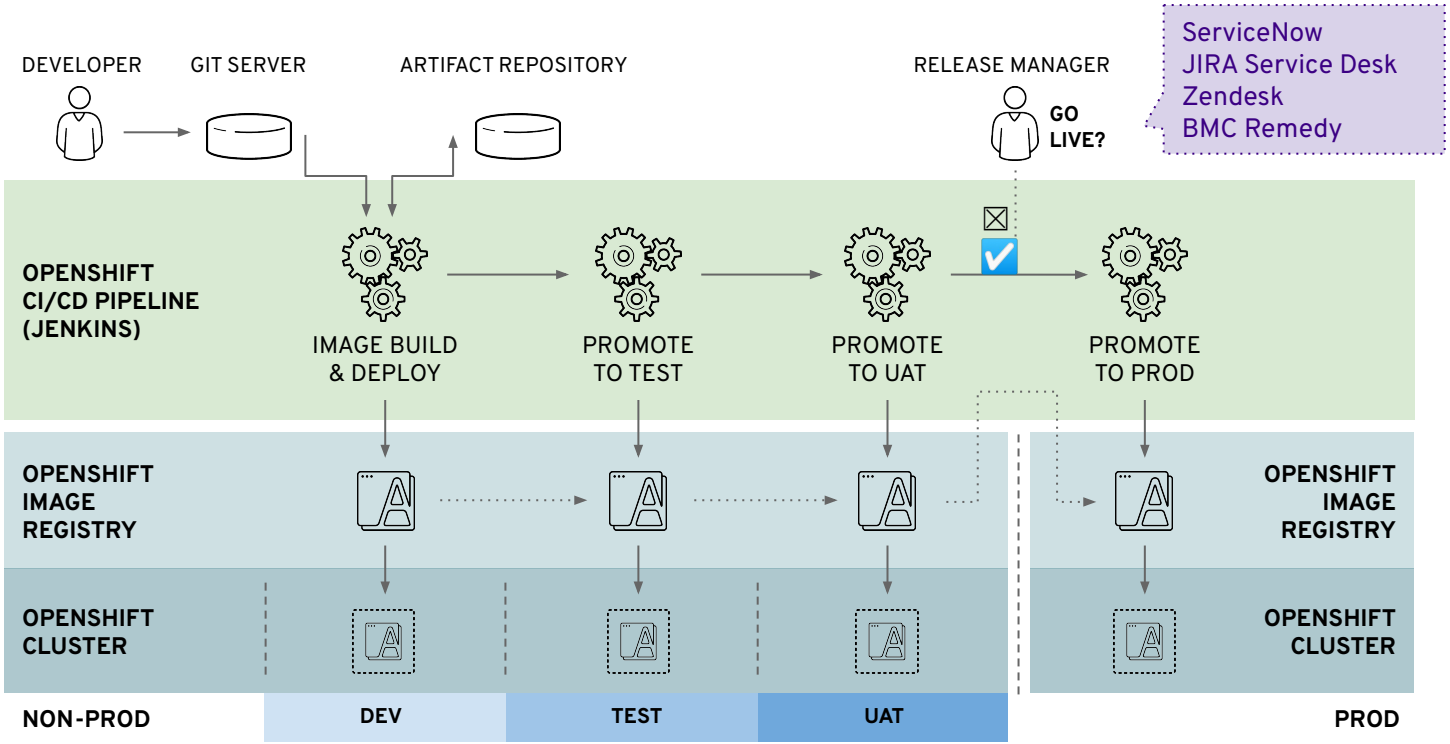
HYBRID JENKINS INFRA
WITH OPENSHIFT



EXISTING CI/CD
DEPLOY TO OPENSHIFT

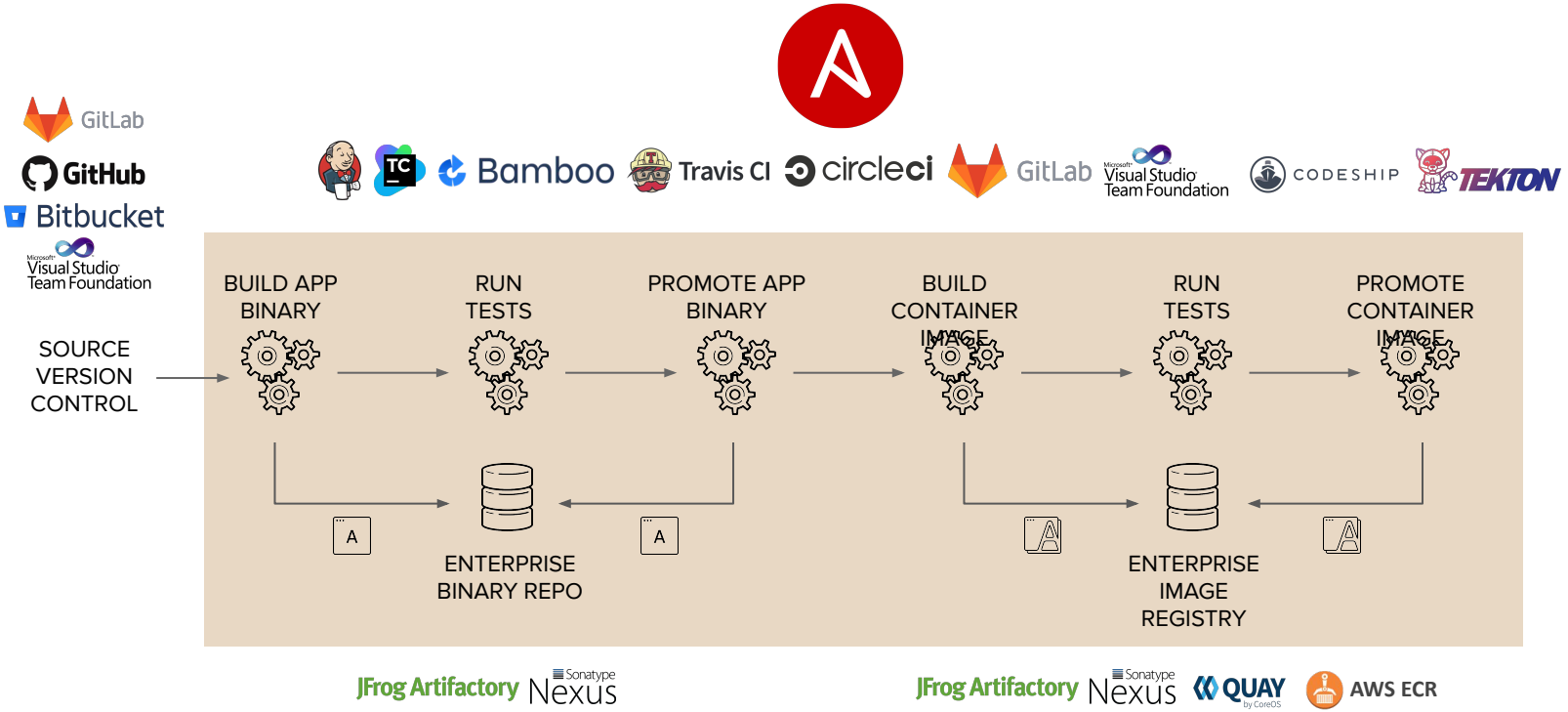
Red Hat

USE THE OPENSHIFT PIPELINE



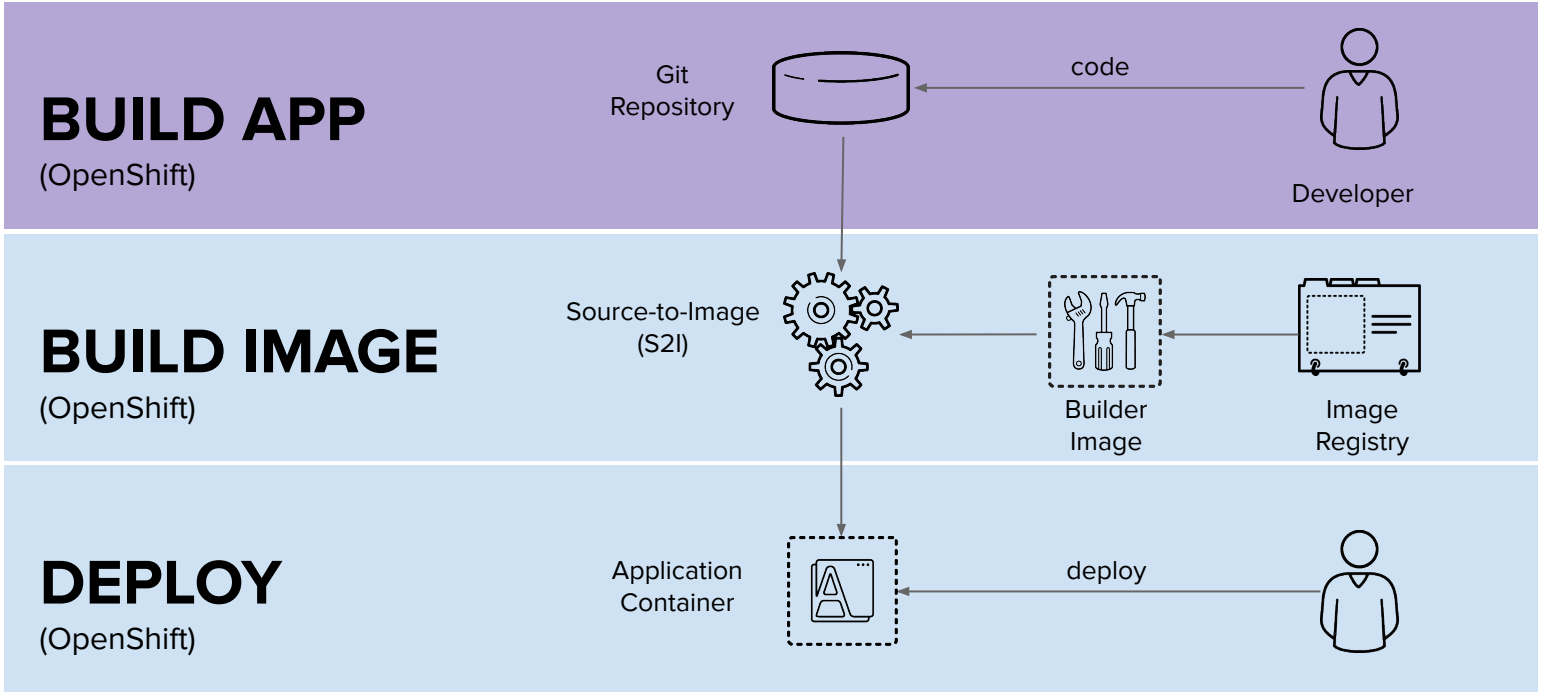
Red Hat

OR USE EXISTING DELIVERY PROCESSES



Red Hat

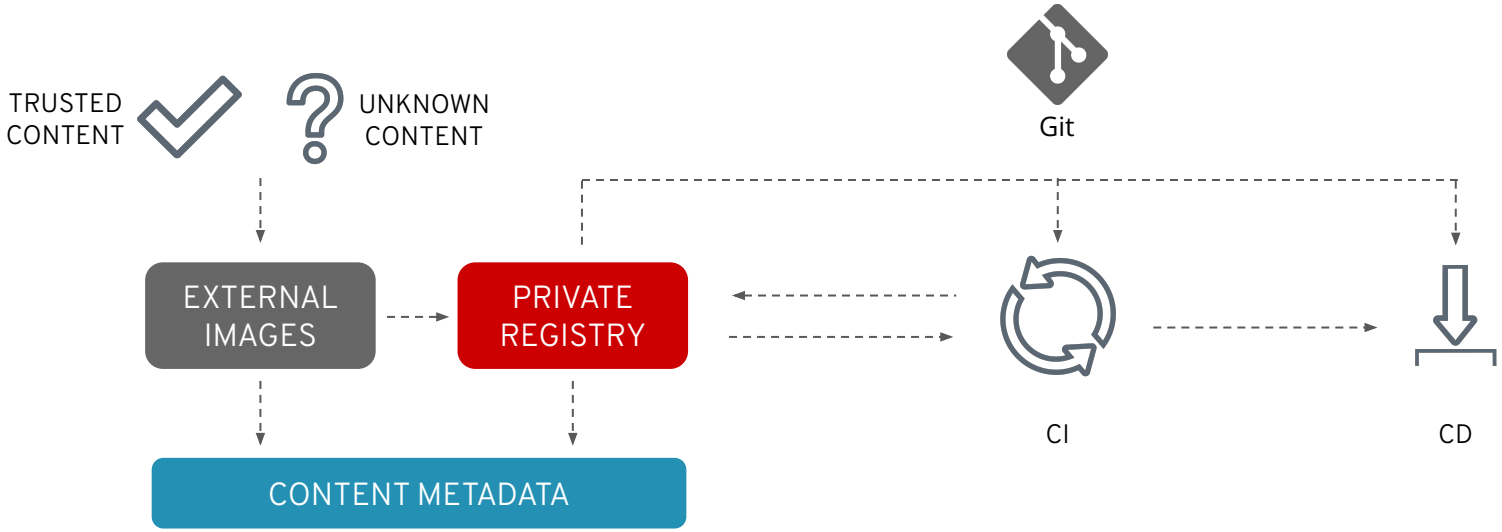
DEPLOY IMAGES, APPLICATION BINARIES OR SOURCE CODE WITH OPENSHIFT



Red Hat

SECURE & AUTOMATE THE CONTENT LIFECYCLE

Elements of the Openshift container pipeline

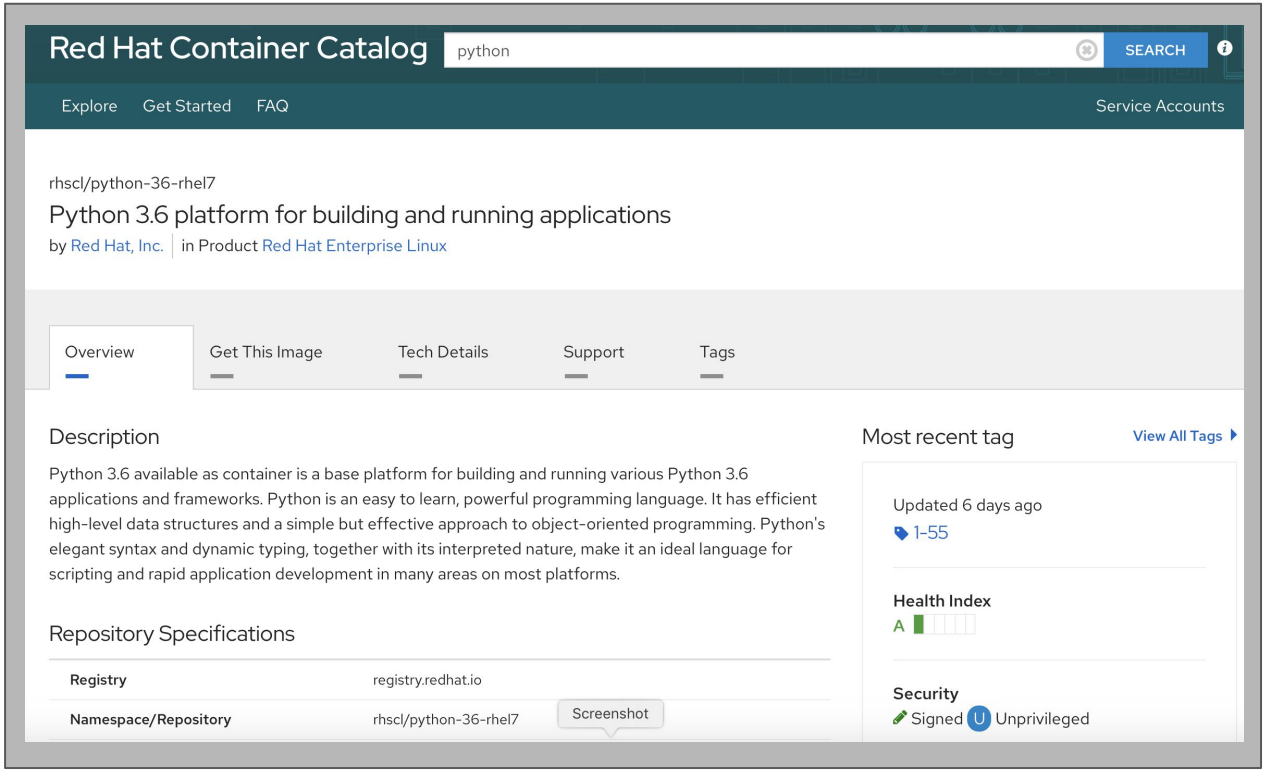


Red Hat

EXTERNAL CONTENT: USE TRUSTED SOURCES

Red Hat Container Images

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

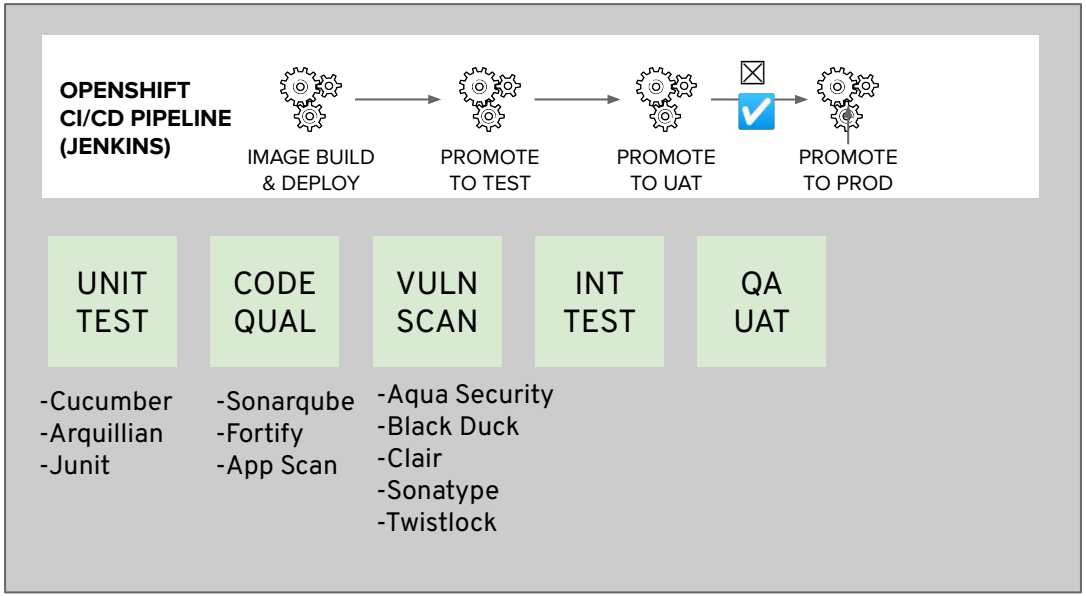


*More about the Health Index

Red Hat

CI/CD MUST INCLUDE SECURITY GATES

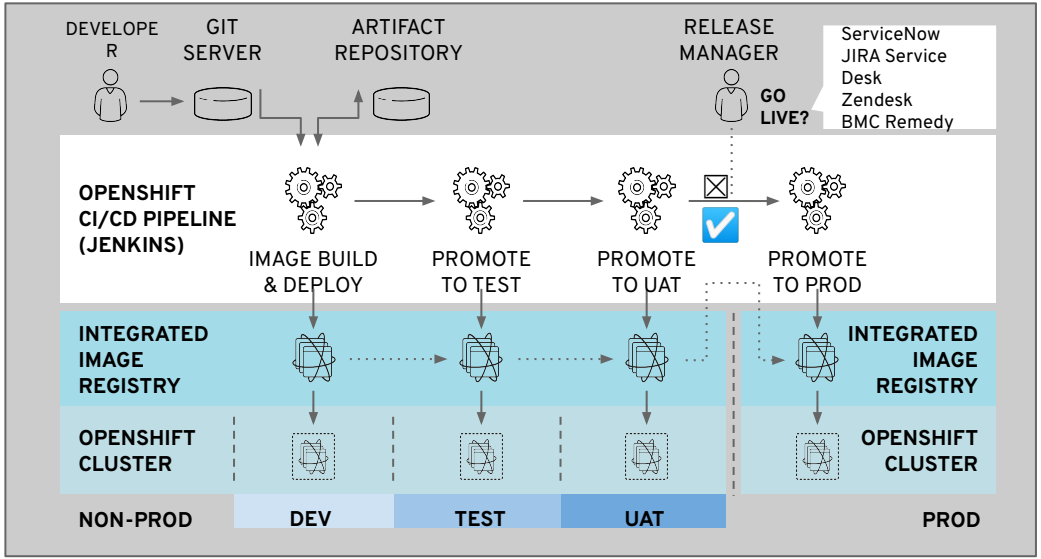
- Integrate security testing into your build / CI process
- Use automated policies to flag builds with issues
- Sign your custom container images



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



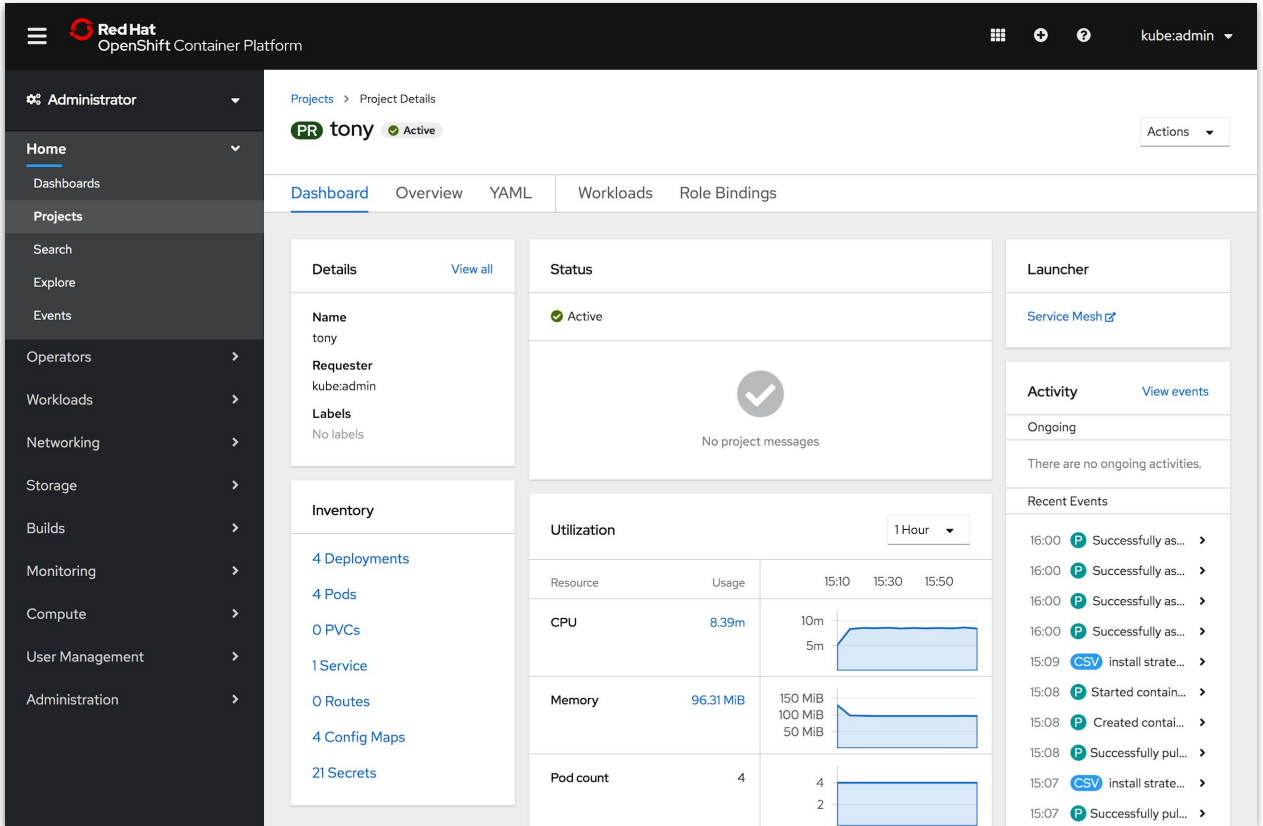
Red Hat

Enhanced Visibility with the New Project Dashboard

Project-scope Dashboard gives Developer Clear Insights

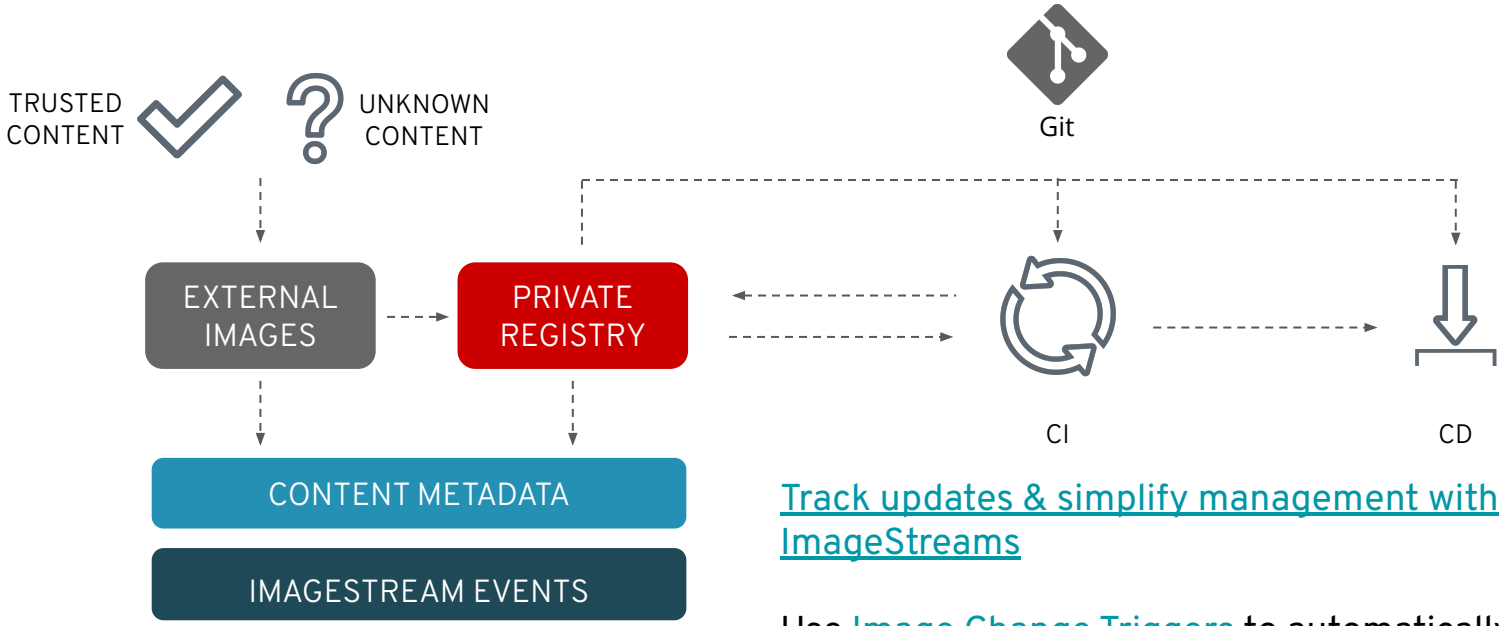
Drill down in context from the new project dashboard widgets:

- Project Details
- Project Status/Health
- Project External Links (Launcher)
- Project Inventory
- Project Utilization
- Project Resource Quota
- Project Activity (Top consumers)



SECURE & AUTOMATE THE CONTENT LIFECYCLE

Trust is temporal; rebuild and redeploy as needed



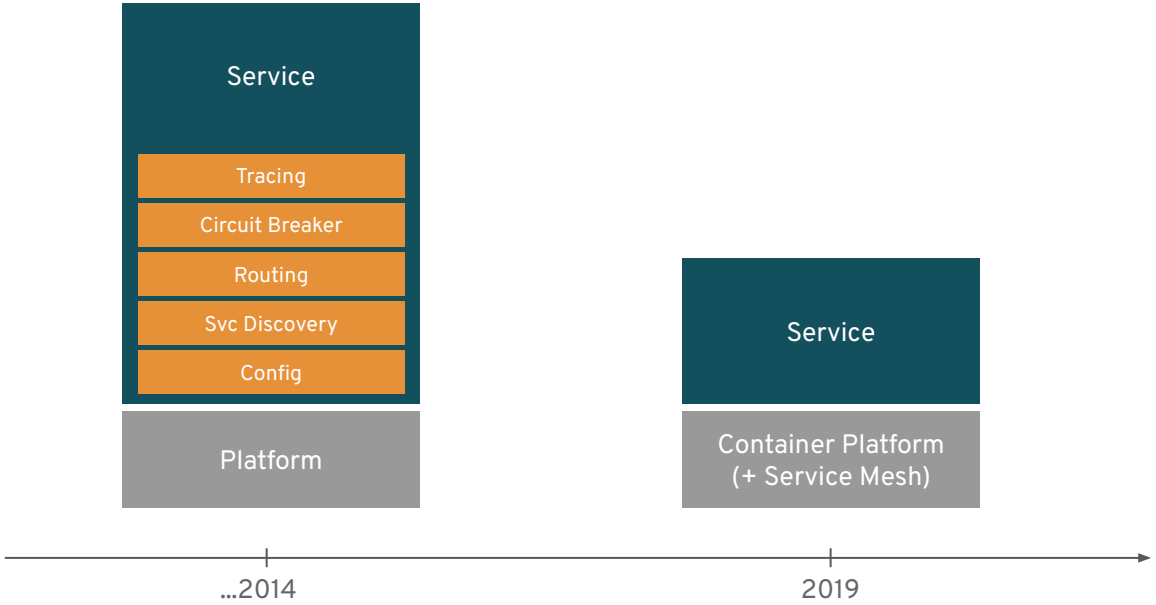
[Track updates & simplify management with ImageStreams]

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

Red Hat

Red Hat Service Mesh

MICROSERVICES EVOLUTION



Red Hat

RED HAT SERVICE MESH

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

Jaeger

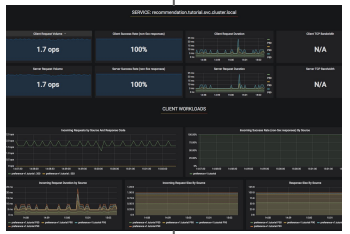
Secure

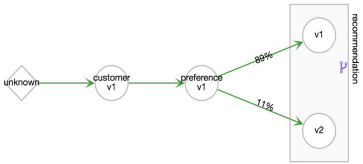
Istio

Observe

Observe

Prometheus





kiali

Kiali

Connect

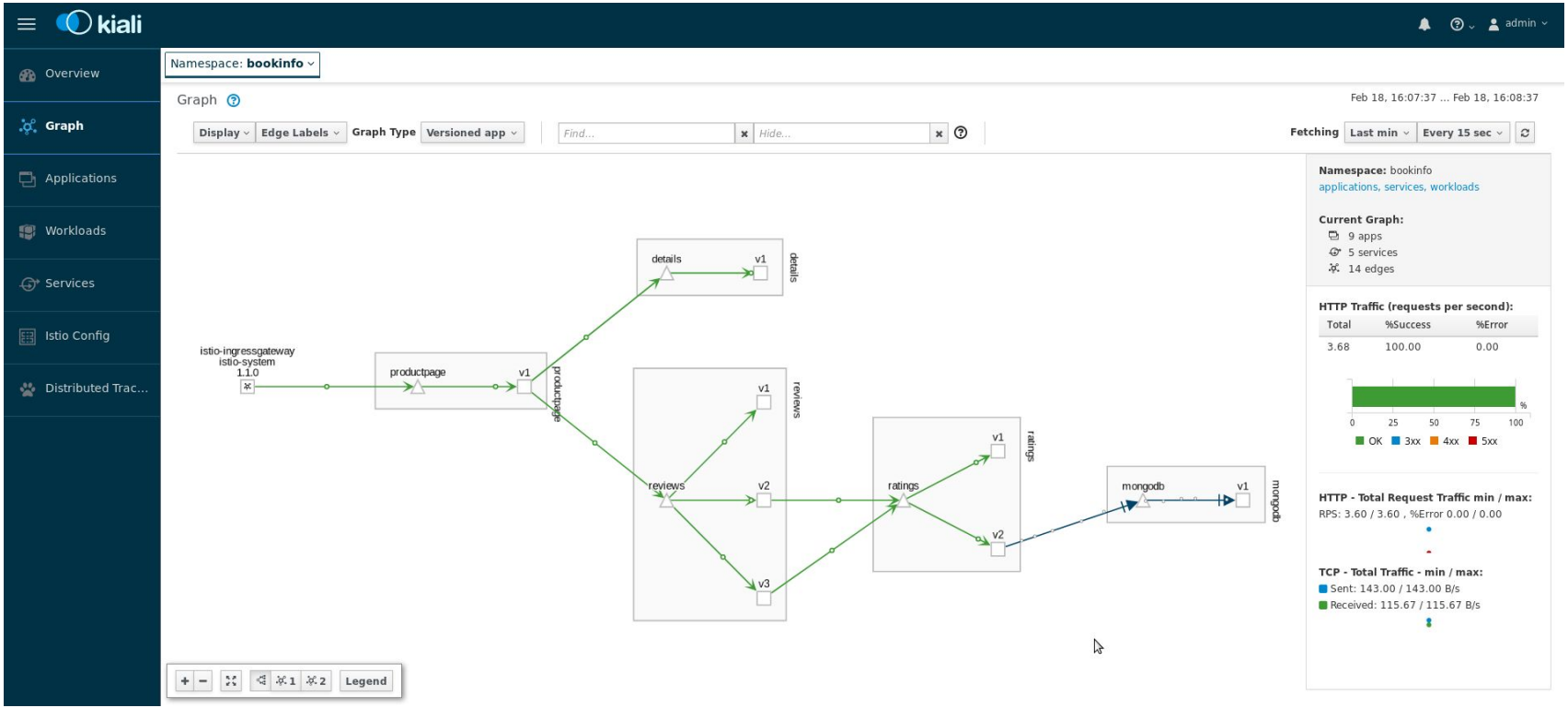
Control

Grafana

Generally Available in July

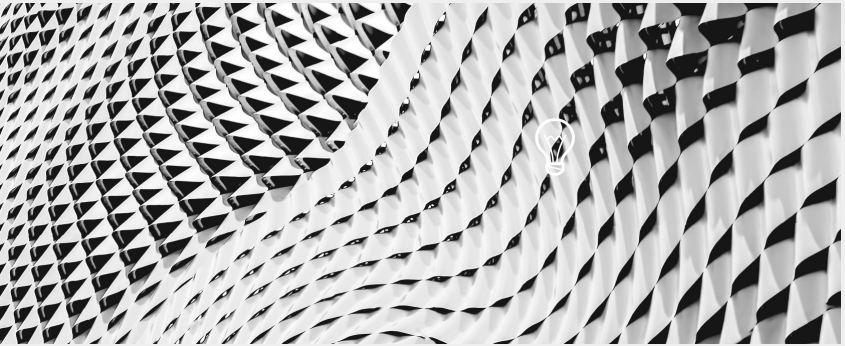
Red Hat

OBSERVABILITY WITH KIALI



Red Hat

EXTEND SECURITY



Red Hat

THE SECURITY ECOSYSTEM

For enhanced security, or to meet existing policies, you may choose to integrate with enterprise security tools, such as

- Identity and Access management / Privileged Access Management
- External Certificate Authorities
- External Vaults / Key Management solutions
- Filesystem encryption tools
- Container content scanners & vulnerability management tools
- Container runtime analysis tools
- Security Information and Event Monitoring (SIEM)

THE BROADER SECURITY ECOSYSTEM







Red Hat

Linux Host Security
- RHCOS Immutable user space & automated updates
- SELinux+
- LUKS volume encryption
- FIPS mode

Authentication & Authorization
- Embedded OAuth Server
- Supports 9 Identity Providers including AD/LDAP
- Multi-Level Access Control (Users and Groups)
- Secrets and certificate management

Data Protection
- Encrypt secrets at rest (etcd datastore)
- All API server traffic is encrypted
- Configure cipher suites*
- Encrypt east / west traffic (Service Mesh)

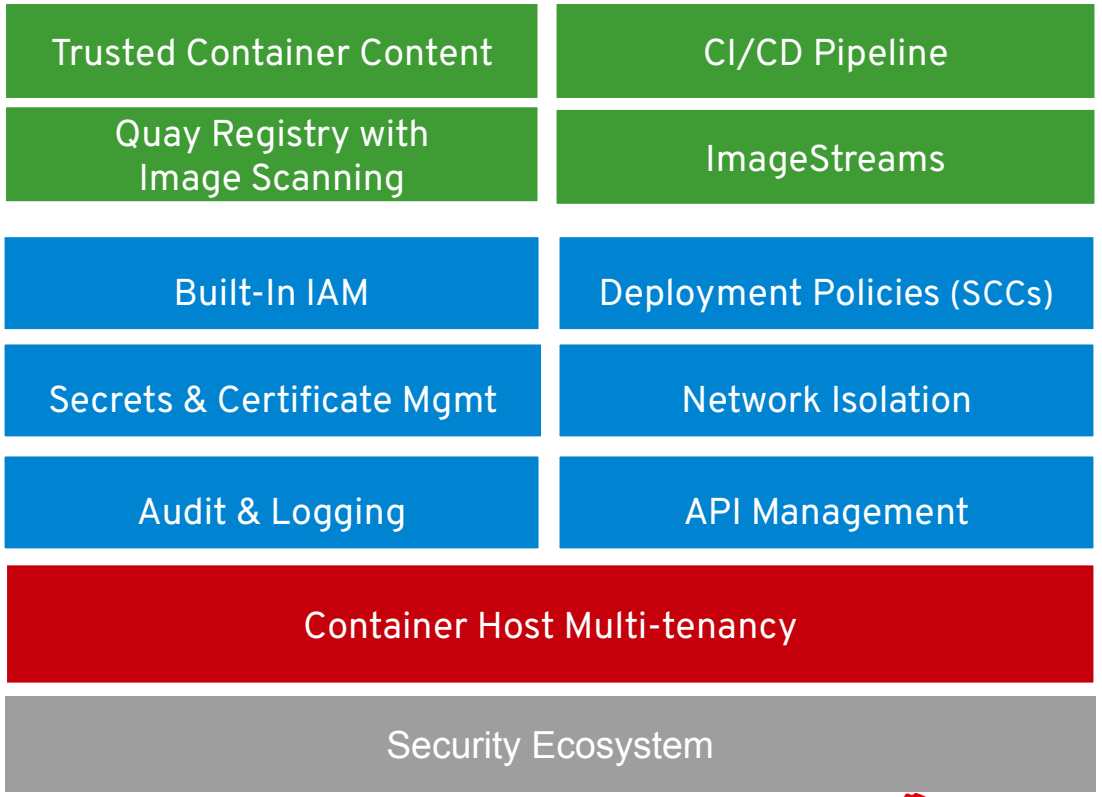
Image Security
- ImageStreams
- Scanning (Quay with Clair)
- Deployment policies (admission controllers)

Integrated Audit, Logging, Monitoring

Security Policies
- SCC (Security Context Controls)
- Non-Root Containers
- Controlled Access to Resources

Networking Isolation
- Ingress / Egress control
- Network microsegmentation

Defense in Depth with comprehensive security features



Ten Layers of Container Security

Red Hat

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