SECURING CONTAINERS WITH OPENSHIFT

Alfred Bach
Principal Solution Architect Cloud /Infra
EMEA Partner Enablement

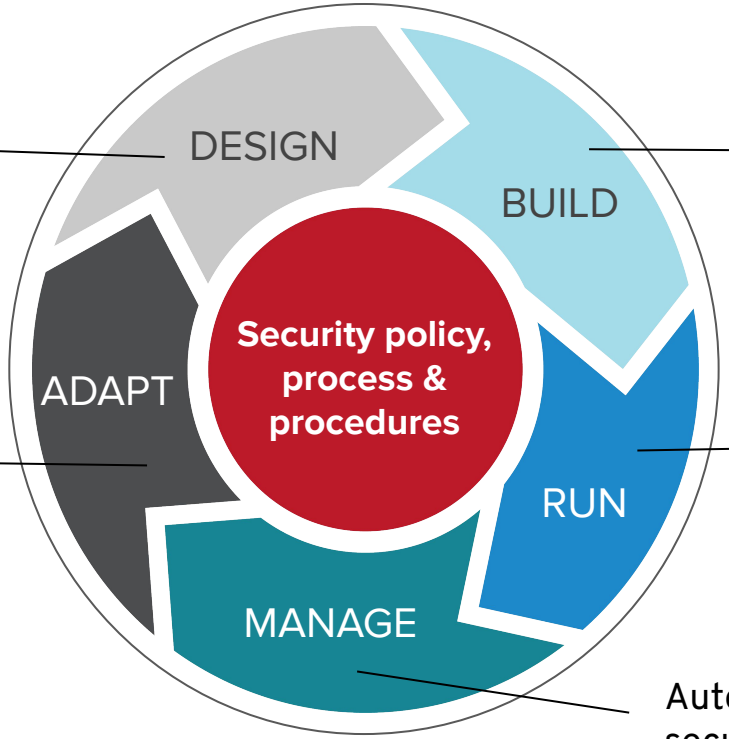
Red Hat

Security must be continuous

And integrated throughout the IT lifecycle

Identify security requirements & governance models

Built-in from the start; not bolted-on



Revise, update, remediate as the landscape changes

Deploy to trusted platforms with enhanced security capabilities

Automate systems for security & compliance

Red Hat

A Comprehensive Approach to Securing Containers

CONTROL
Application Security

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

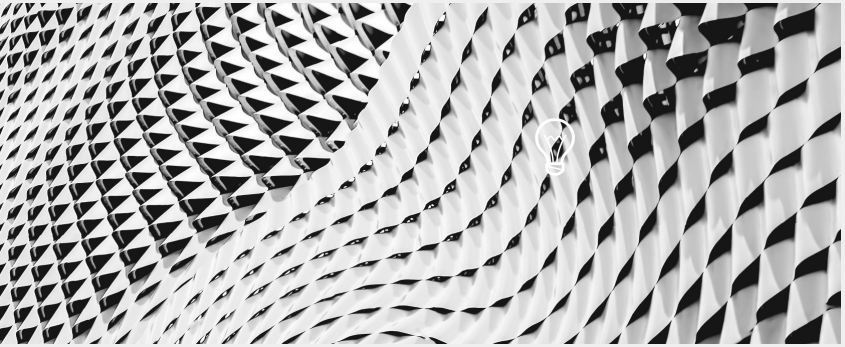
DEFEND
Infrastructure

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

EXTEND

- Security Ecosystem

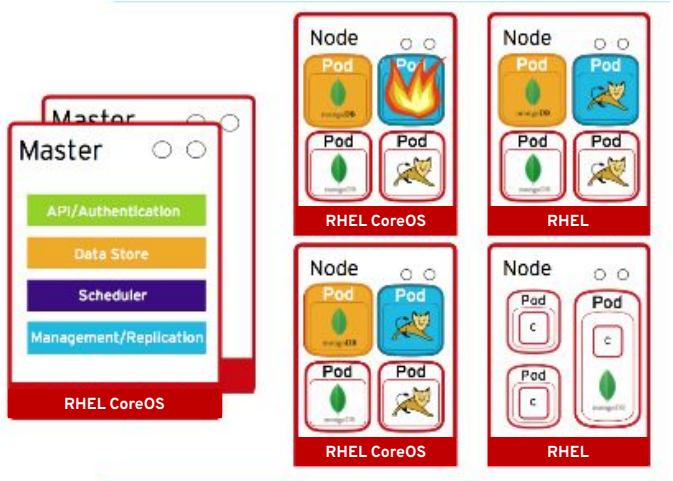
DEFEND INFRASTRUCTURE



Red Hat

Securing the container platform

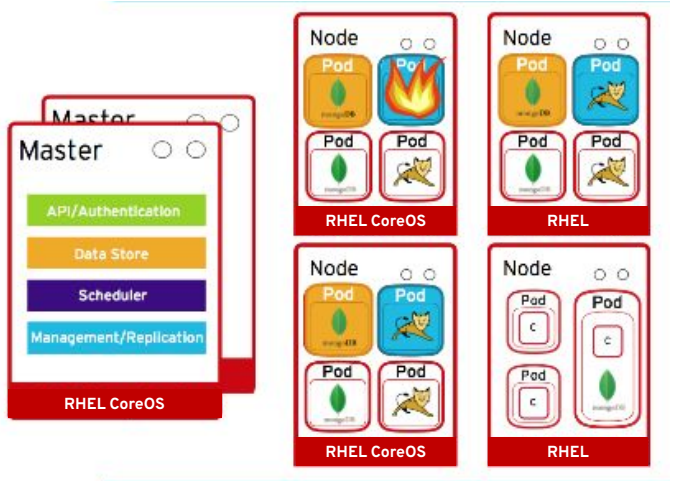
- Configuration and lifecycle management
- Host & runtime security
- Identity and Access Management
- Data at rest, data in transit
- Logging, Monitoring, Metrics
- Audit and Compliance



Red Hat

Securing the container platform

- **Configuration and lifecycle management**
- Host & runtime security
- Identity and Access Management
- Data at rest, data in transit
- Logging, Monitoring, Metrics
- Audit and Compliance



Red Hat

Automated Configuration and Lifecycle Management

Dramatically simplified for the Hybrid Cloud

Machines

Machines are complex for ops

Make machines easy
(like containers)

Configuration

Config change is risky

Make config management
and config change
easy and safe

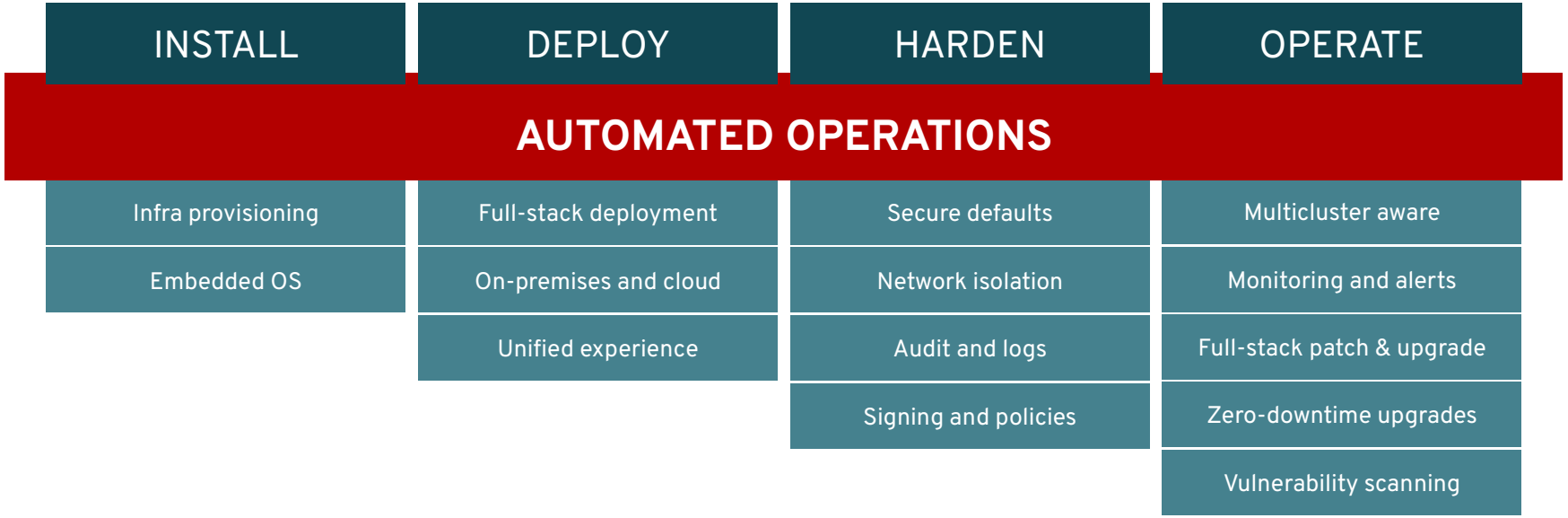
Lifecycle

Software lifecycle is hard

Automate software
lifecycle on Kube

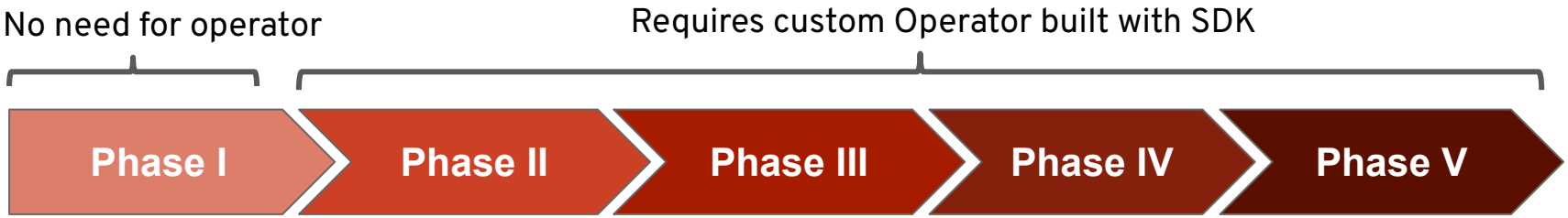
Automated Container Operations

FULLY AUTOMATED DAY-1 AND DAY-2 OPERATIONS



Red Hat

The Value Of Kubernetes Operators



Installation
Automated application provisioning and configuration management

Upgrades
Patch and minor version upgrades supported

Lifecycle
App lifecycle, storage lifecycle (backup, failure recovery)

Deep Insights
Metrics, alerts, log processing and workload analysis

Auto-pilot
Horizontal/vertical scaling, auto config tuning, abnormal detection, scheduling tuning...

Day 1 Installation

OPENSHIFT CONTAINER PLATFORM

Full Stack Automation

Simplified opinionated "Best Practices" for cluster provisioning

Fully automated installation and updates including host container OS.

Red Hat Enterprise Linux CoreOS

Pre-existing Infrastructure

Customer managed resources & infrastructure provisioning

Plug into existing DNS and security boundaries

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux

HOSTED OPENSHIFT

Azure Red Hat OpenShift

Deploy directly from the Azure console. Jointly managed by Red Hat and Microsoft Azure engineers.

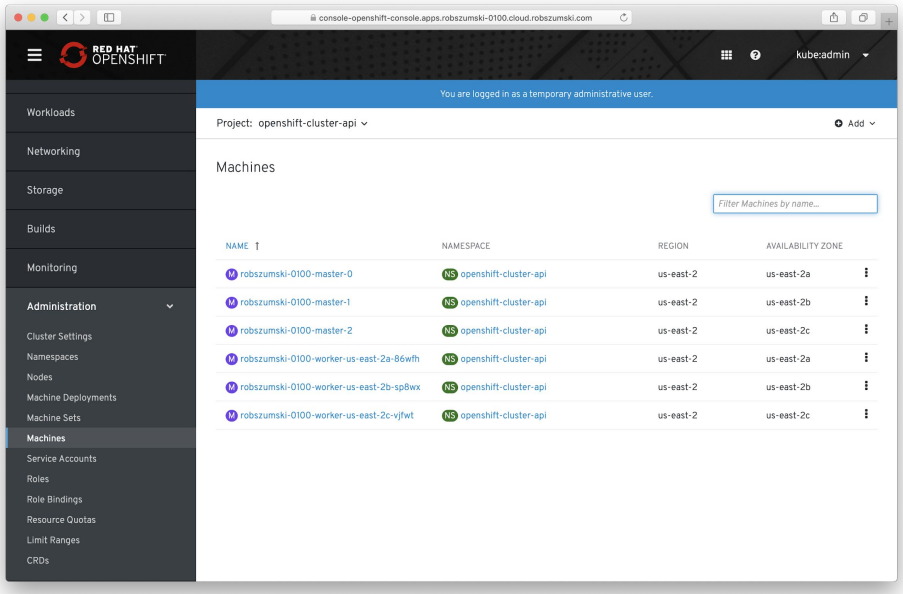
OpenShift Dedicated

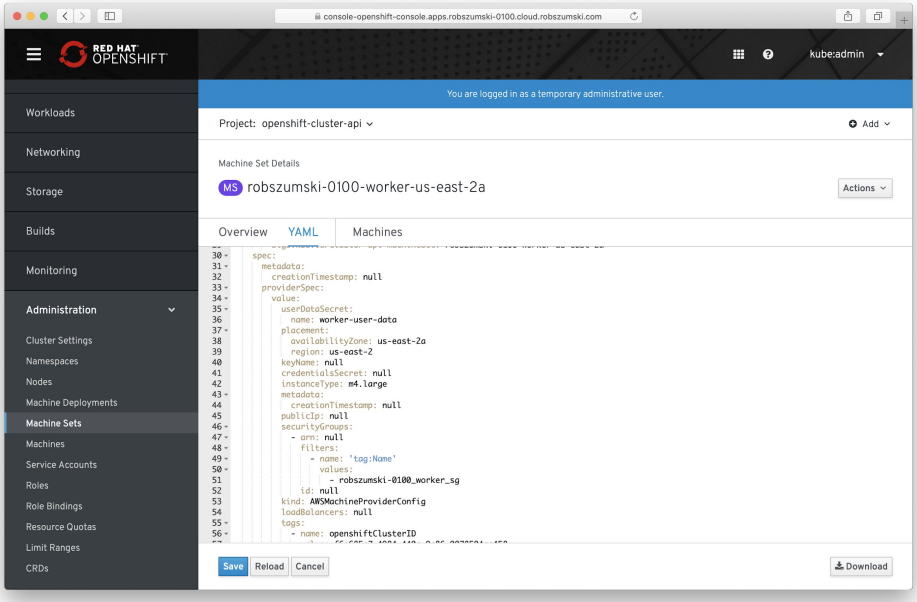
Get a powerful cluster, fully Managed by Red Hat engineers and support.

Generally Available

Kubernetes Machine Api Operator

Using Kubernetes To Provision And Scale Clusters





Red Hat

Day 2 Configuration

Global Configuration

You complete most of the cluster configuration and customization after you deploy your OpenShift Container Platform cluster.

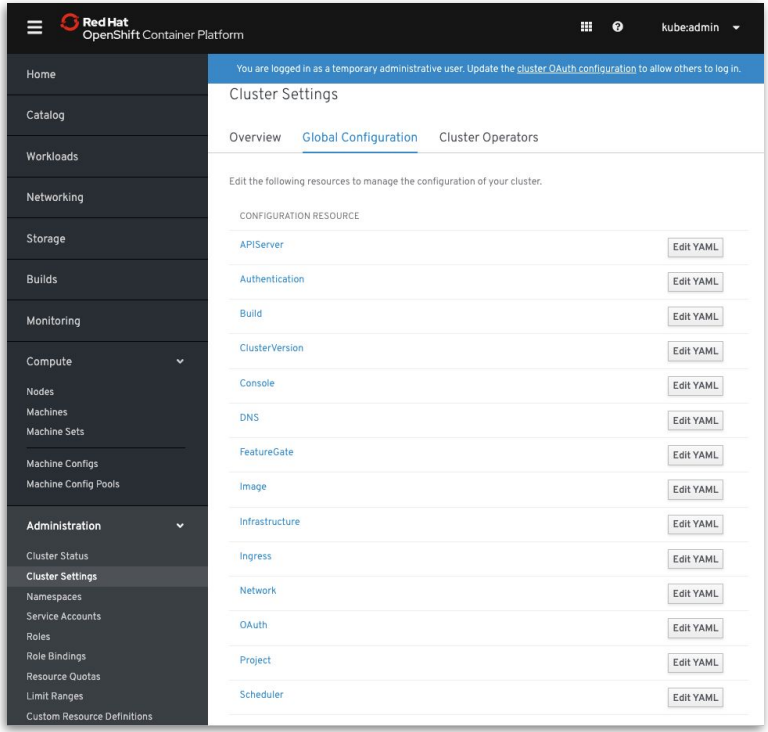
Change via Cluster Settings screen

Once you have discovered your desired settings (prev. slide), changes can be made via Console or CLI.

Operators apply these updates

One or more Operators are responsible for propagating these settings through the infrastructure

- Identity Provider
- Ingress Controller
- Logging, Metrics



Smarter Software Updates

No downtime for well behaving apps

Applications with multiple replicas, using liveness probes, health checks and taints/tolerations

Node Pools with more than one worker and slack resources

Maintenance window for entire cluster

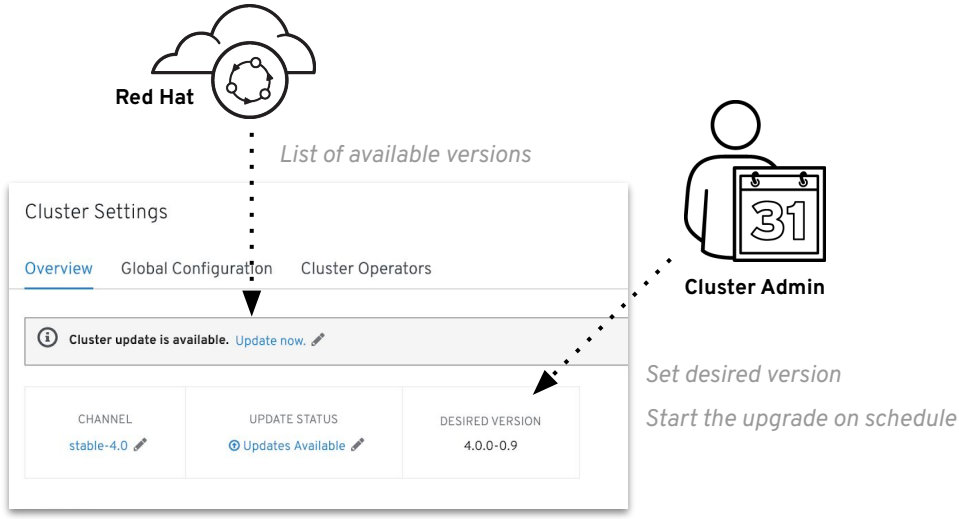
No need for separate windows for each component

Upgrade runs completely on the cluster

No more long running processes on a workstation

Constant health checking from each Operator

Operators are constantly looking for incompatibilities and issues that might arise

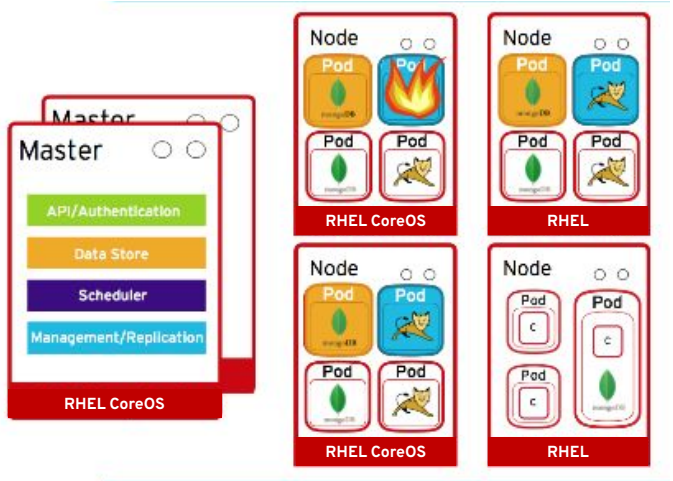


[NEW: OpenShift Update Service for restricted networks]

Red Hat

Securing the container platform

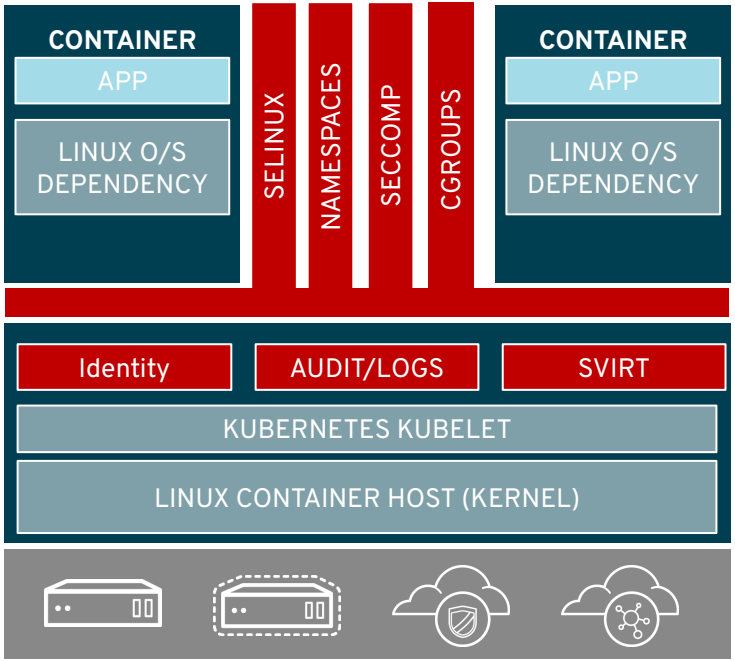
- Configuration and lifecycle management
- **Host & runtime security**
- Identity and Access Management
- Data at rest, data in transit
- Logging, Monitoring, Metrics
- Audit and Compliance



Red Hat

Container security starts with Linux security

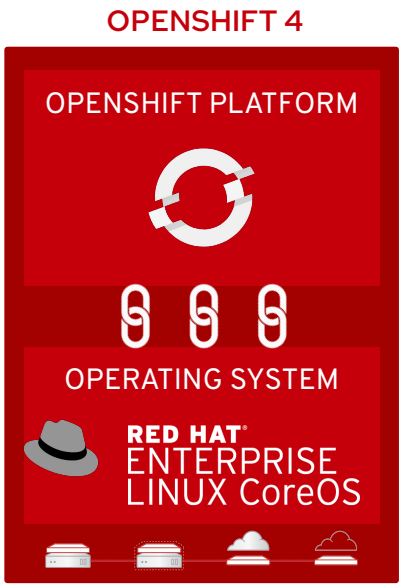
- Security in the RHEL host applies to the container
- RHEL enables container multitenancy
- SELINUX and Kernel Namespaces are the one-two punch no one can beat
- Protects not only the host, but containers from each other
- RHEL CoreOS provides minimized attack surface



Red Hat

Red Hat Enterprise Linux CoreOS

The Immutable Container Optimized Operating System



Role in OpenShift Ecosystem

- Versioned and validated for specific OpenShift version
- Required for masters. RHEL option for workers
- User space read-only

Managed by the OpenShift Cluster

- Considered a member of an OpenShift Deployment
- Configuration managed by the Machine Config Operator
  - Container runtime
  - Kubelet configuration
  - Authorized container registries
  - SSH Configuration

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

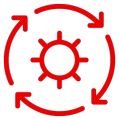
[CRI - the Container Runtime Interface]
[OpenShift 4 defaults to CRI-O]
[Red Hat contributes CRI-O to the Cloud Native Computing Foundation]

New

Security Profile Operator

Helps admins use **SELinux** and **seccomp effectively**

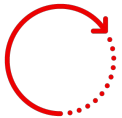
Easy seccomp and SElinux profile creation by recording what your application needs and creates a profile from it



Manages profiles across nodes and namespaces

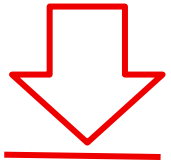
It also validates if node supports seccomp and doesn't synchronize it if not

Validate your profile



Reuse profiles

across namespaces



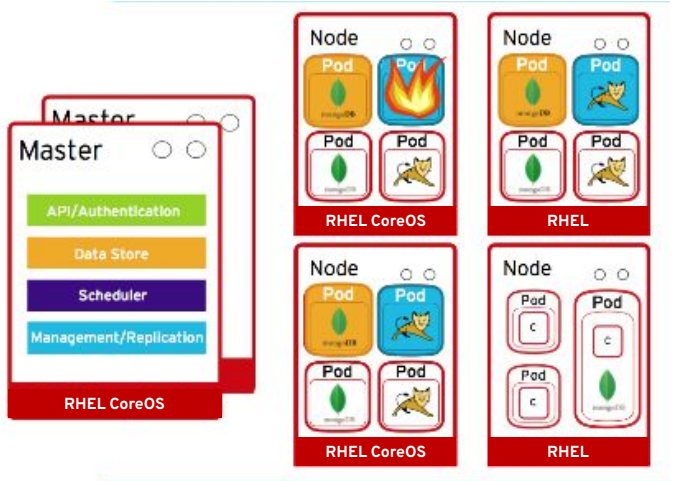
Available in OperatorHub

Product Managers: Maria Simon

Red Hat

Securing the container platform

- Configuration and lifecycle management
- Host & runtime security
- **Identity and Access Management**
- Data at rest, data in transit
- Logging, Monitoring, Metrics
- Audit and Compliance



Red Hat

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

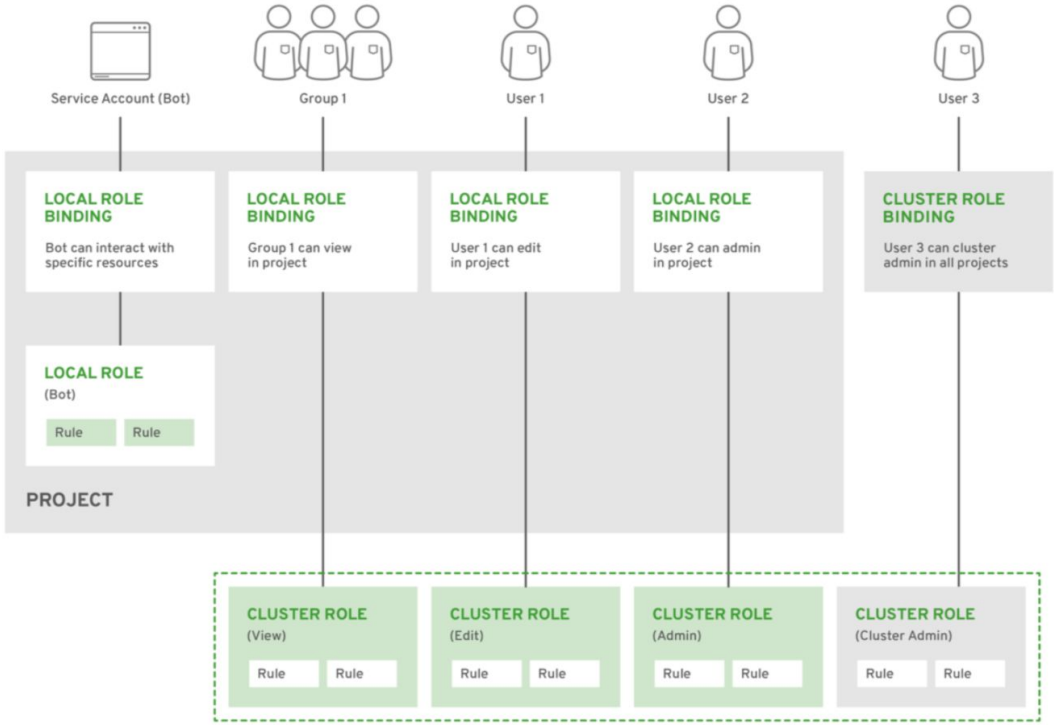
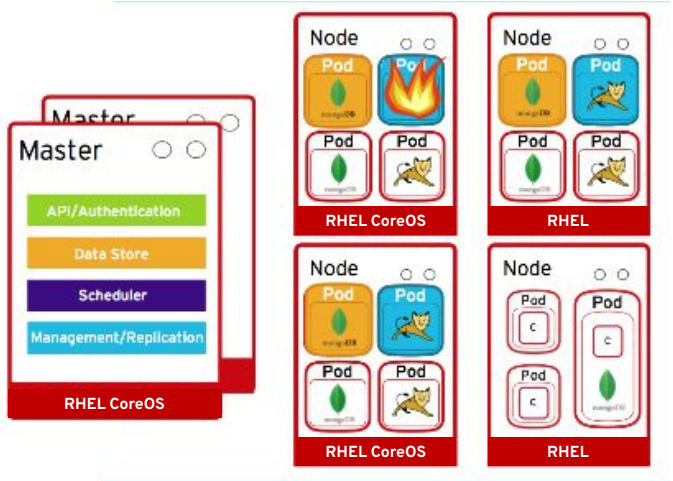


Figure 12 - Authorization Relationships

For more information see: [Managing RBAC in OpenShift]

Securing the container platform

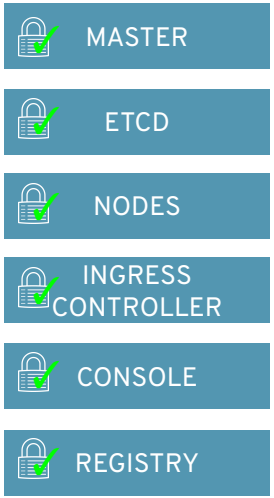
- Configuration and lifecycle management
- Host & runtime security
- Identity and Access Management
- **Data at rest, data in transit**
- Logging, Monitoring, Metrics
- Audit and Compliance



Red Hat

Certificate management

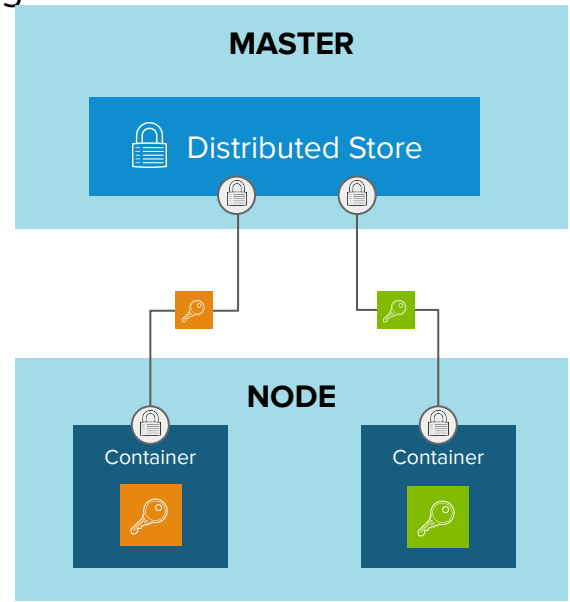
- Certificates are used to provide secure connections to
  - master and nodes
  - Ingress controller and registry
  - etcd
- Certificate rotation is automated
- Optionally configure external endpoints to use custom certificates
- For example:
  [Requesting and Installing Let's Encrypt Certificates for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



Red Hat

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
  - Encrypt the etcd datastore
  - Encrypt RHCOS volumes
- Never rest on the nodes



Volume Encryption

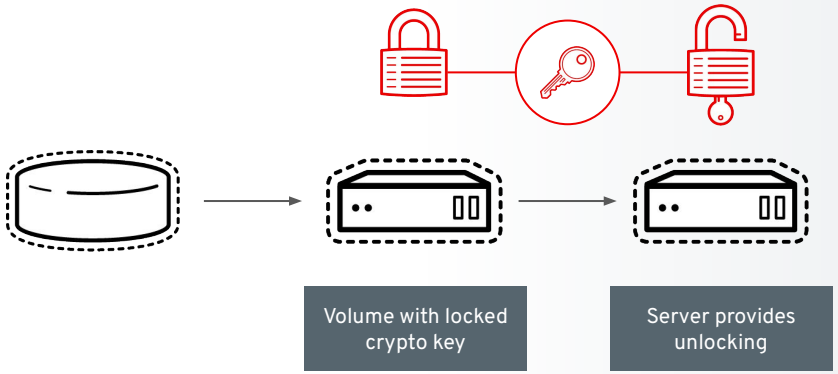
Network Bound Disk Encryption

- Provides encryption for local storage
- Addresses disk/image theft
- Platform/cloud agnostic implementation
- TPM/vTPM (v2) and Tang endpoints for automatic decryption

Attached storage

Secure storage by using

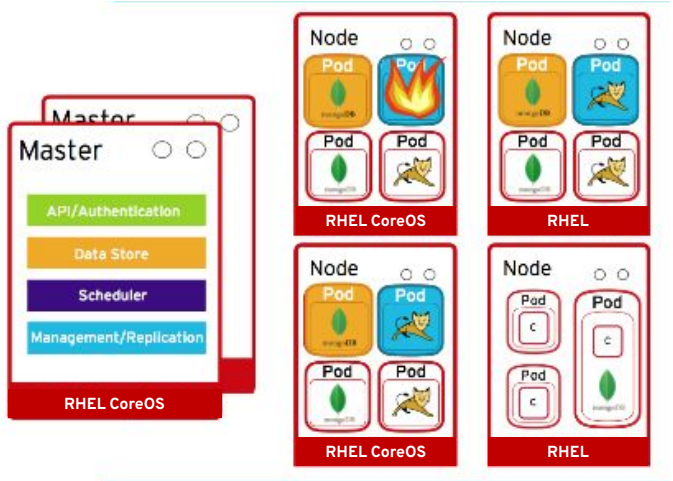
- SELinux access controls
- Secure mounts
- Supplemental group IDs for shared storage
- Network bound disk encryption



Red Hat

Securing the container platform

- Configuration and lifecycle management
- Host & runtime security
- Identity and Access Management
- Data at rest, data in transit
- **Logging, Monitoring, Metrics**
- Audit and Compliance

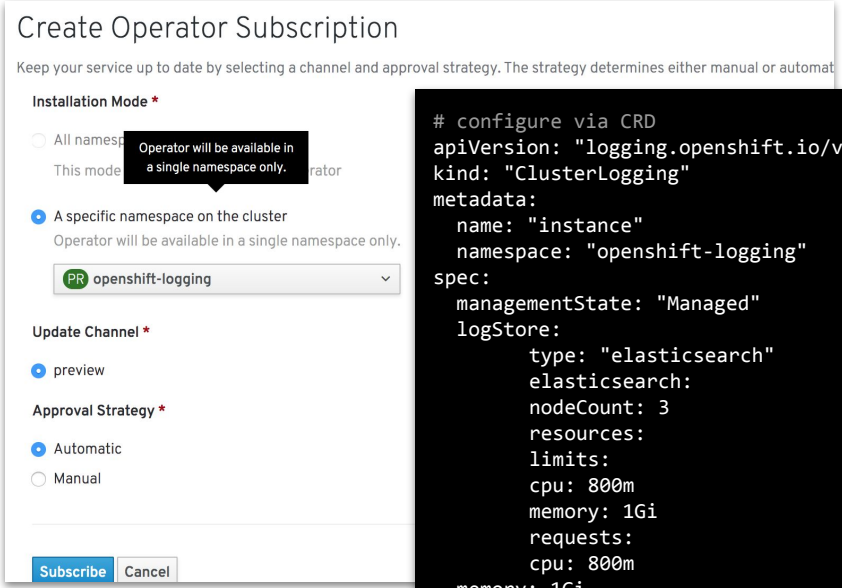


Red Hat

Cluster log and audit management

Install the Elasticsearch and Cluster Logging Operators

- 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
- API server events are automatically audited
- Logging pipelines collect API server and host audit logs as well as cluster and application logs for forwarding to the SIEM of your choice

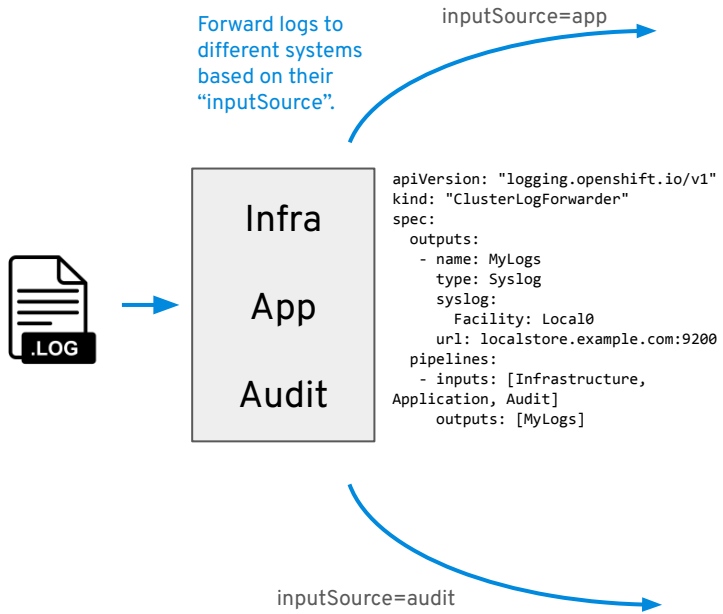



```
# configure via CRD
apiVersion: "logging.openshift.io/v1"
kind: "ClusterLogging"
metadata:
  name: "instance"
  namespace: "openshift-logging"
spec:
  managementState: "Managed"
  logStore:
        type: "elasticsearch"
        elasticsearch:
        nodeCount: 3
        resources:
        limits: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

Introduce new log forwarding API

Abstract Fluentd configuration by introduce new log forwarding API to improve support and experience for customers.

- Introduce a new, cluster-wide *ClusterLogForwarder* CRD (API) that replaces needs to configure log forwarding via Fluentd ConfigMap.
- The API helps to reduce probability to misconfigure Fluentd and helps bringing in more stability into the Logging stack.
- Route logs based on their source type (infra, app or audit logs) and filter them further by namespaces.
- Collecting and forwarding audit logs
- With the API, we also introduce the following endpoint improvements to bring more value on to the table:
    - Improved syslog support adding TLS for secure communication + support for the newest standard (RFC5424).
    - Kafka support.

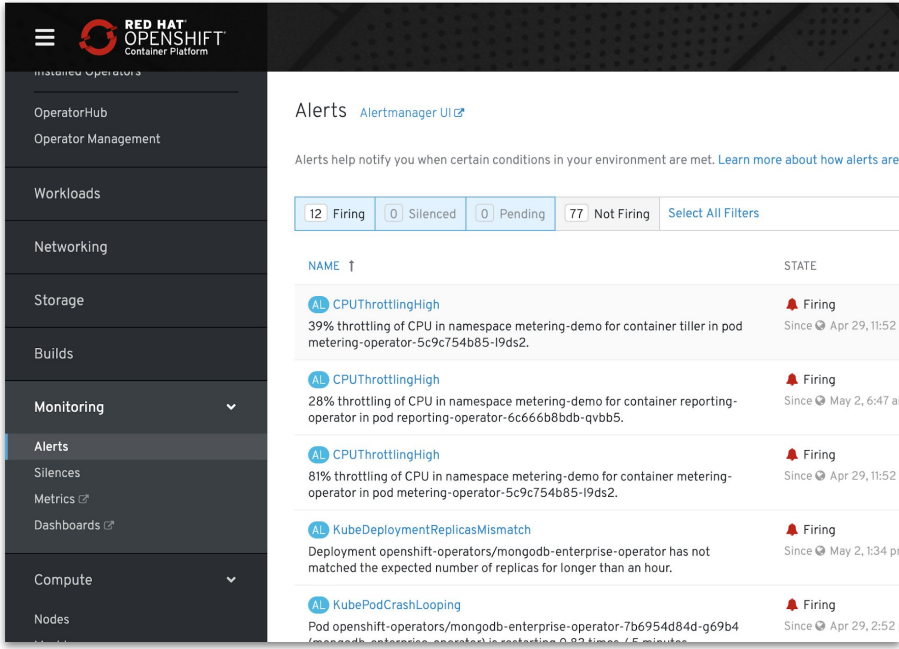


Red Hat

Cluster monitoring

Cluster monitoring is installed by default

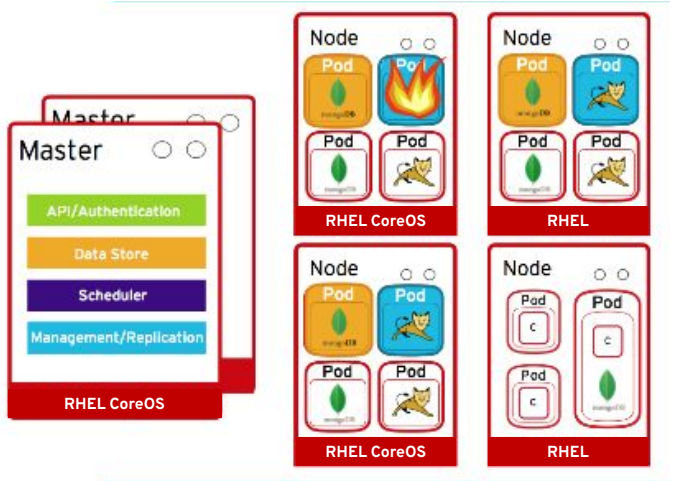
- Exposes resource metrics for Horizontal Pod Autoscaling (HPA) by default
  - HPA based on custom metric is tech preview
- No manual etcd monitoring configuration anymore
- New screens for managing Alerts & Silences
- More metrics available for troubleshooting purposes (e.g. HAproxy)
- Configuration via ConfigMaps and Secrets



Red Hat

Securing the container platform

- Configuration and lifecycle management
- Host & runtime security
- Identity and Access Management
- Data at rest, data in transit
- Logging, Monitoring, Metrics
- **Audit and Compliance**



Red Hat

Openshift Compliance Operator: Declarative Security Compliance

OpenSCAP

1 A compliance profile is selected

Describe intent with declarative config

With 4.6, a limited set of RHCOS checks will be implemented. Additional compliance checks will be delivered roughly every 2 months.

3 Accreditors or Auditors can examine the scan results for compliance status, After review, if desired, remediations can be manually applied by the cluster-admin.

2 The operator runs the scan for the profile against nodes, collect results, and (optionally) performs remeditations

Red Hat OpenShift Container Platform

ComplianceSuite

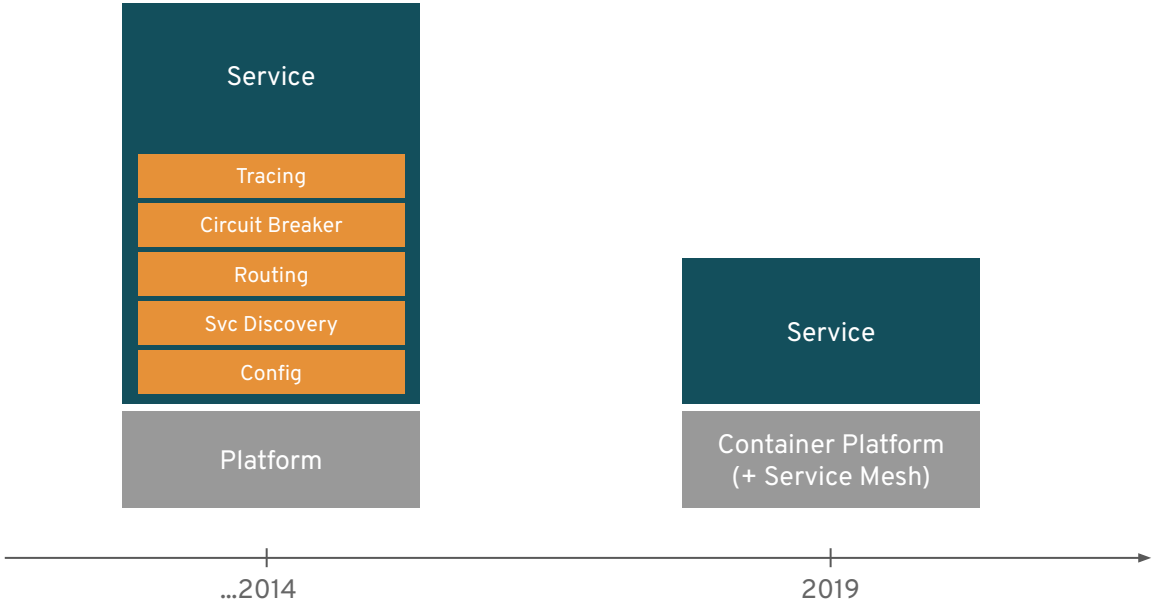
ComplianceCheckResult

Scan (results)

ComplianceRemediations

Red Hat

Microservices evolution

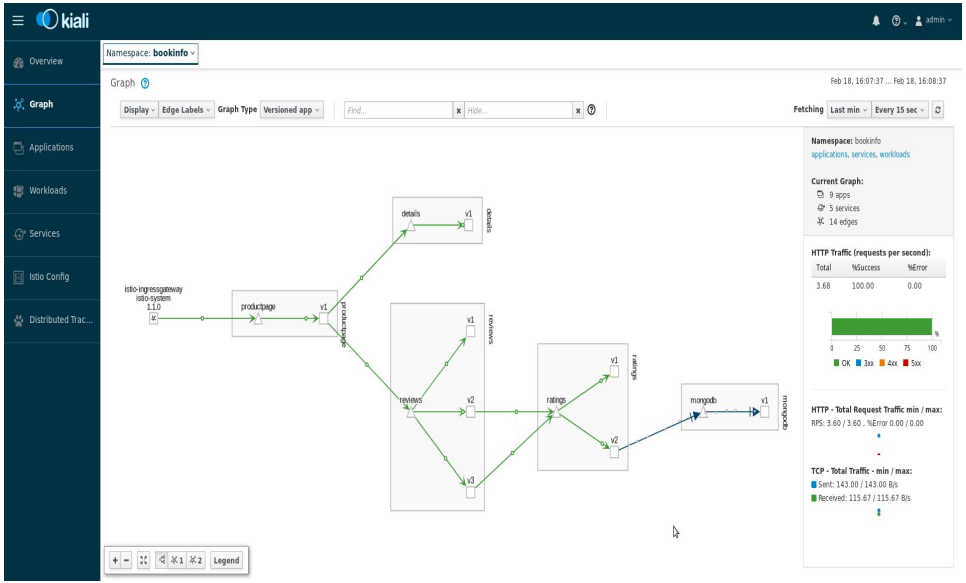


Red Hat

Secure microservices with Service Mesh

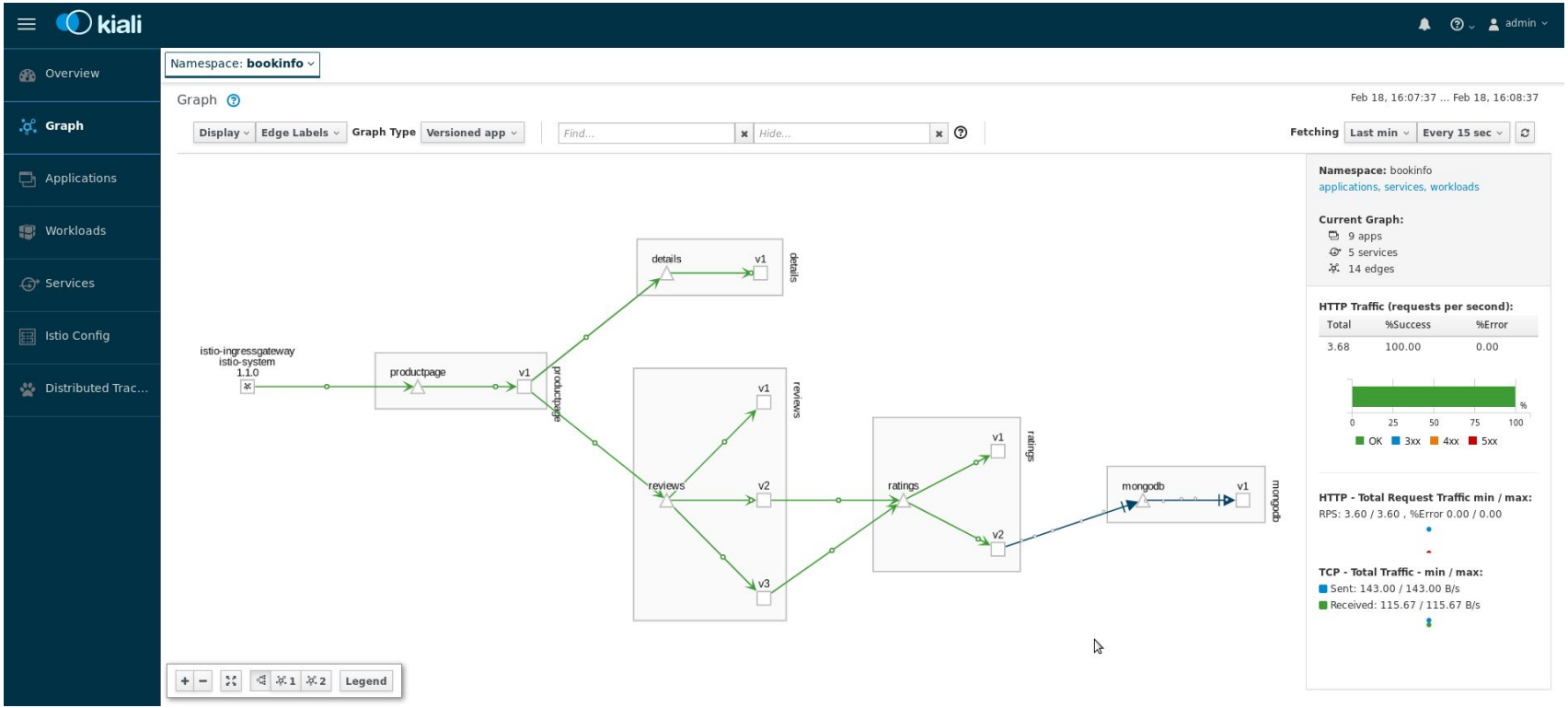
Key Features

- A dedicated network for service to service communications
- Observability and distributed tracing
- Policy-driven security
- Routing rules & chaos engineering
- Powerful visualization & monitoring
- Will be available via OperatorHub



Red Hat

Observability with Kiali

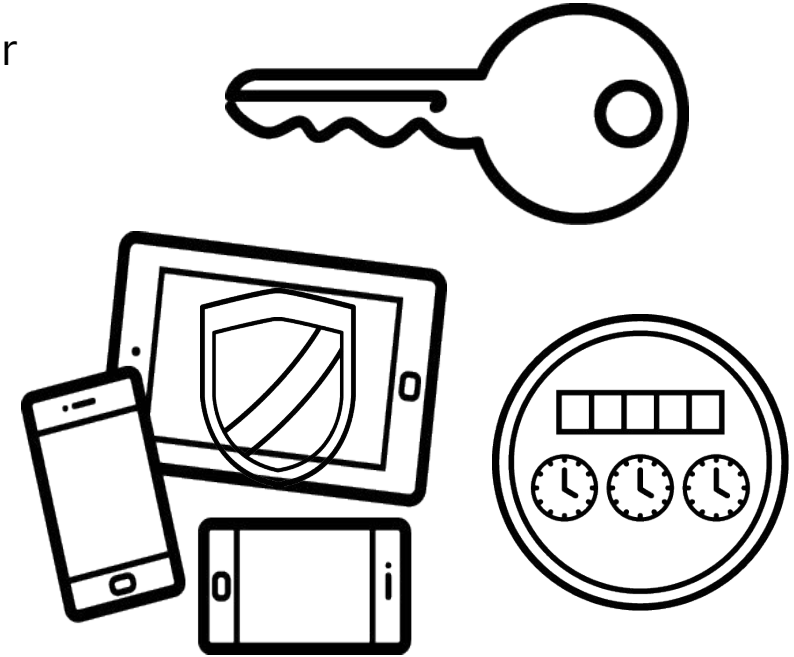


Red Hat

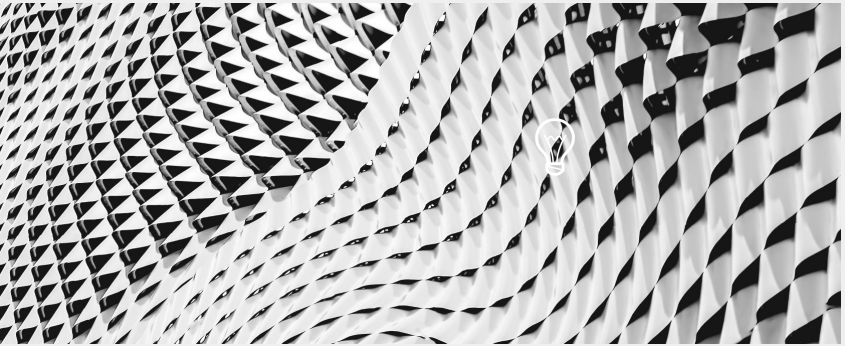
Application API management

Consider configuring an API gateway for container platform & application APIs

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



EXTEND SECURITY



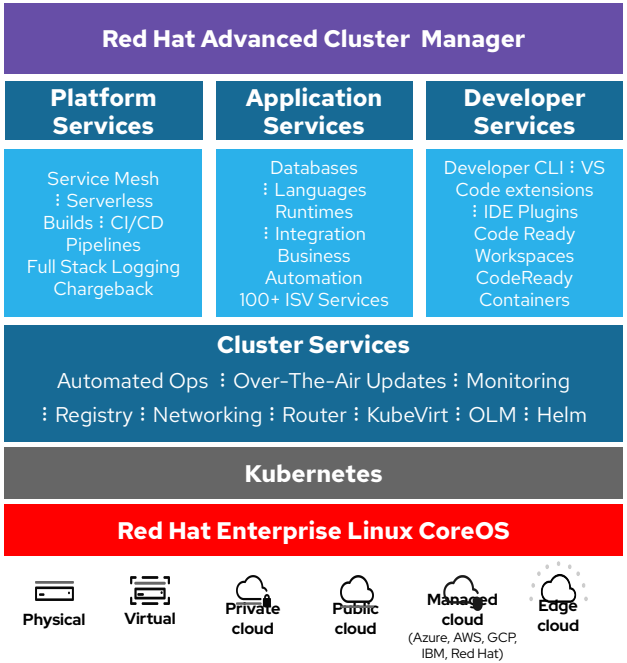
Red Hat

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)

Red Hat OpenShift certified operators - 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