Red Hat OpenShift

What's New in OpenShift 4.6

OpenShift Product Management

Red Hat

OpenShift 4.6

NEW INSTALLER PLATFORMS

Bare Metal IPI

AWS and Azure Gov Clouds

Disconnected Update Intelligence

CORE PLATFORM

Remote Worker Nodes

Real Time and Low Latency

OVN (GA)

Compliance Operator (GA)

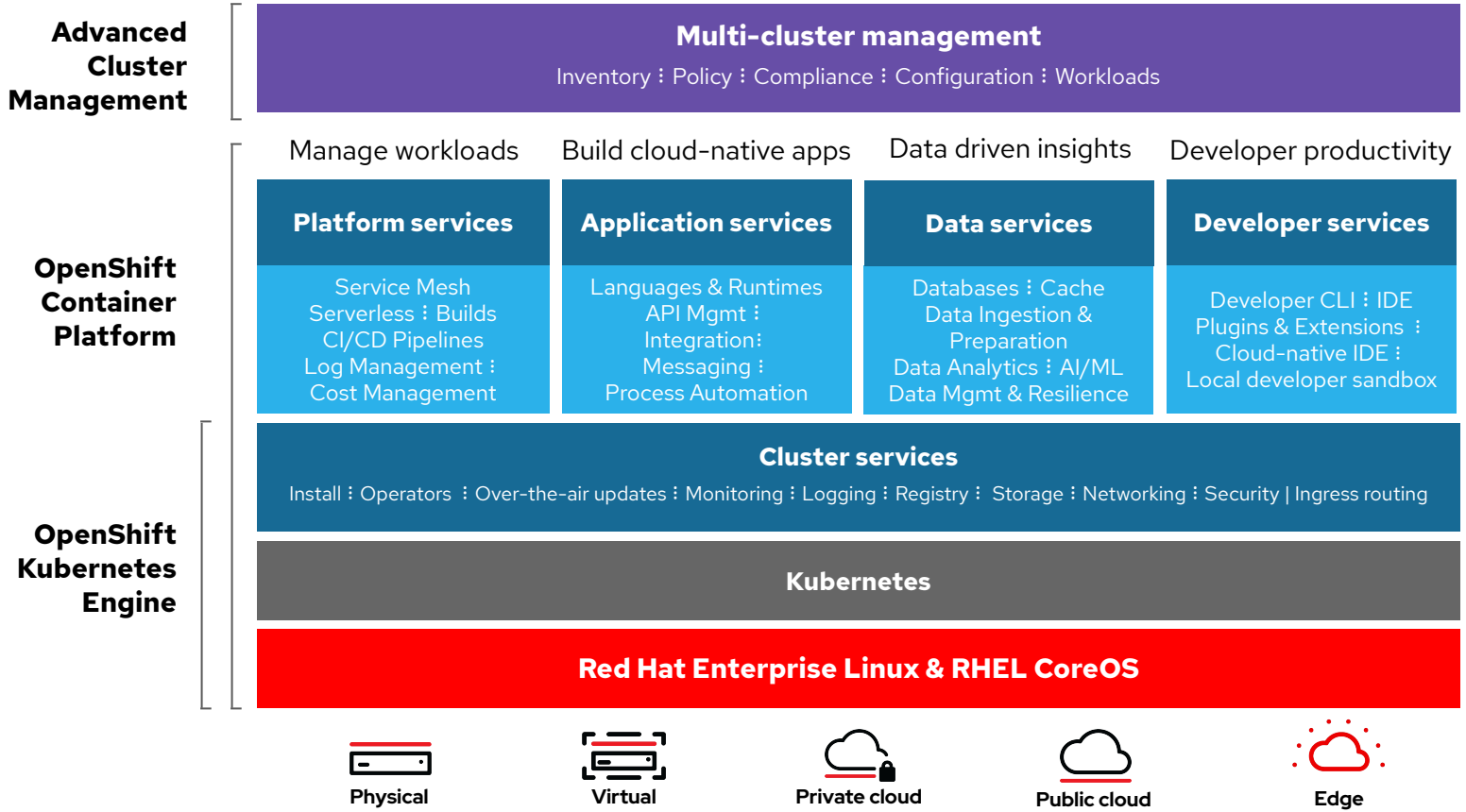
WORKLOAD STABILITY

User Workload Monitoring (GA)

Log Forwarding API (GA)

Serverless Eventing (GA)

OpenShift Container Platform



Red Hat

OpenShift Roadmap

Q4 2020
OpenShift 4.6

DEV
- Improved getting started experience for devs
- OpenShift Serverless Eventing GA
- OpenShift Pipelines (Tekton) TP
- Jenkins Operator TP

APP
- Monitor application workloads (GA)
- Operator dependency tools v2
- OpenShift Builds (v2) DP

PLATFORM
- OVN GA, OVN Egress Firewall/Router/IP
- Bare metal (IPI) GA
- Remote worker nodes for Edge
- Realtime kernel (TP, RAN use-cases only)
- AWS GovCloud support
- Microsoft Azure Government (MAG) support
- VMware vSphere 7.0 support
- Improved cloud credential handling
- Disconnected OpenShift Update Service
- GCP & Azure spot instances
- CSI resize/snapshot GA
- Windows containers GA
- OAuth secure storage & inactivity timeout
- Enhanced RHCOS static networking UX
- Compliance Operator
- RHV UPI support

MANAGED
- Amazon Red Hat OpenShift
- ARO Government (MAG) support
- OSD / AMRO Upgrade Scheduling
- OSD / AMRO Machine Pools
- AMRO Auto Scaling, BYO VPC
- BYOK disk encryption (AWS, Azure)

H1 2021
OpenShift 4.7/4.8

DEV
- OpenShift Pipelines (Tekton) GA
- OpenShift Builds (v2) TP
- Jenkins Operator TP
- Argo CD GA
- Schema based forms for Event Sources

APP
- Improvements to GitOps experience
- Cluster Update Compatibility Checks
- Hybrid Operators with Operator-SDK
- Simplify Operator Lifecycle interactions

PLATFORM
- IPv6 (single/dual stack on control plane)
- Enable user space pod int & API Library
- Utilize cgroups v2
- Azure Stack Hub support
- AWS C2S and China support
- Equinox Packet support
- IBM Cloud support
- Assisted Installer
- Network Enhancements derived from OVN
- Local storage support in OCS
- OpenShift Service Mesh Federation
- GPU Sharing

MANAGED
- OSD GCP CCS & private clusters
- OSD CCS on-demand Marketplace billing
- OSD cluster autoscaling
- OSD custom domains, log forwarding
- ACM integration
- OSD / AMRO PCI Certification

H2 2021
OpenShift 4.Next

DEV
- Console integration with Tekton Hub
- Pipelines Notifications
- OpenShift Builds (v2) GA
- Jenkins Operator GA

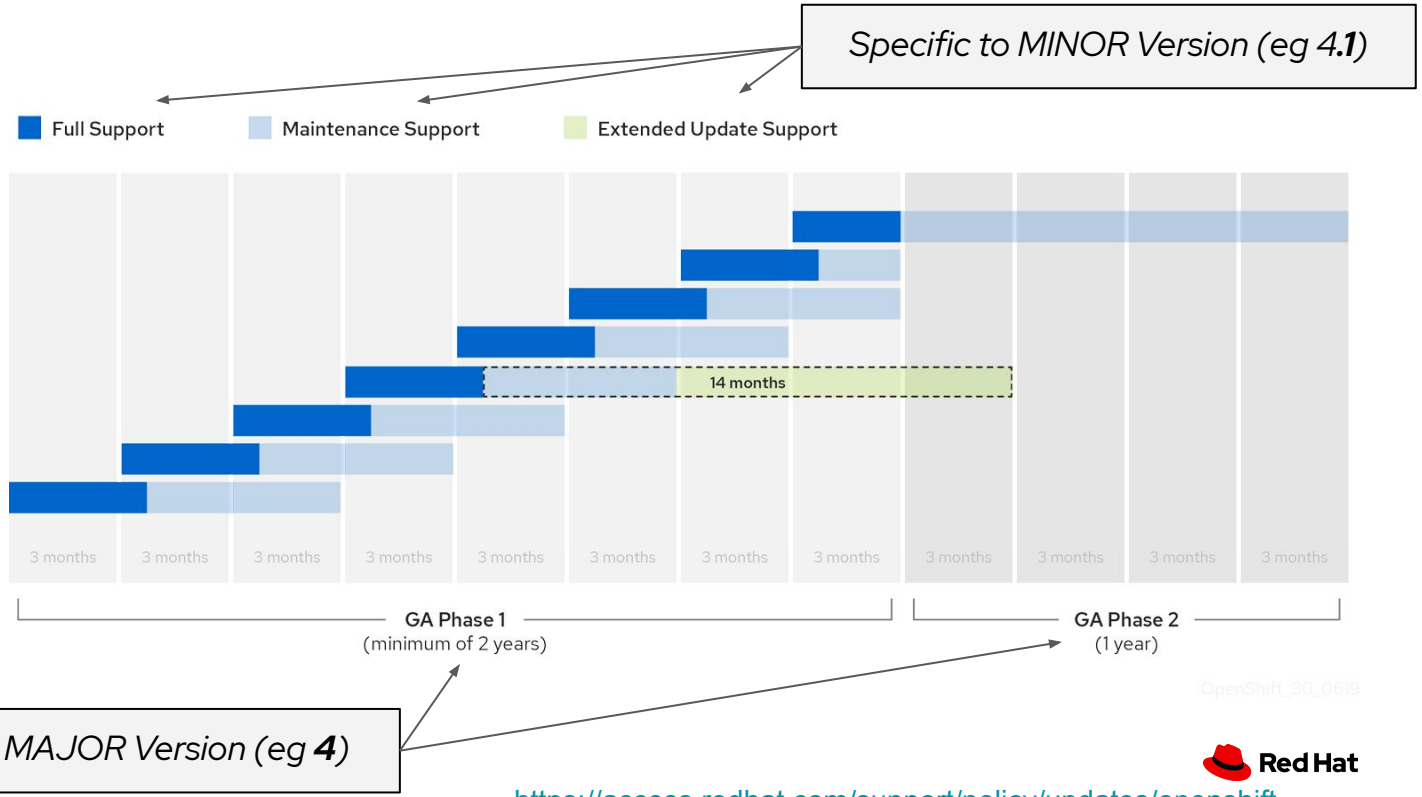
APP
- Workload Metrics Visualization
- Operator SDK: Python and Java Support
- Operators install/upgrade as a group
- Serverless Streaming

PLATFORM
- OpenShift Single node
- Utilize cgroups v2
- Microsoft Hyper-V (UPI) support
- Alibaba Cloud support
- Network Enhancements derived from OVN
- Local storage support in OCS
- OpenShift Service Mesh Multi-Cluster
- Next gen SmartNic architecture

MANAGED
- OSD / AMRO FedRAMP Certification
- Build, Operate, Transfer operational model
- Windows containers
- GPU optimized VMs

OpenShift Life Cycle Reminder

- Release Driven - function of the next release
- 3 Minor Releases are in play at any given time. *(4 if you count the EUS release)*
- OCP 4.6 will bump OCP 4.3 out of support.
- OCP 4.2 = 10 months of support
- OCP 4.3 = 10 months of support



https://access.redhat.com/support/policy/updates/openshift

Red Hat

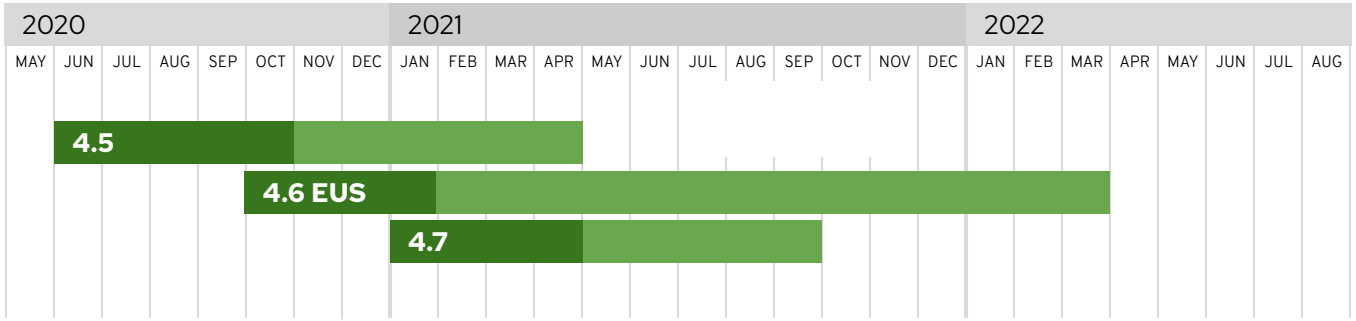
OpenShift 4.6 EUS

What is Extended Update Support (EUS) ?

- OCP with an extended timeframe for critical security and bug fixes
- Available to premium support customers
- Not available as an add-on for standard support

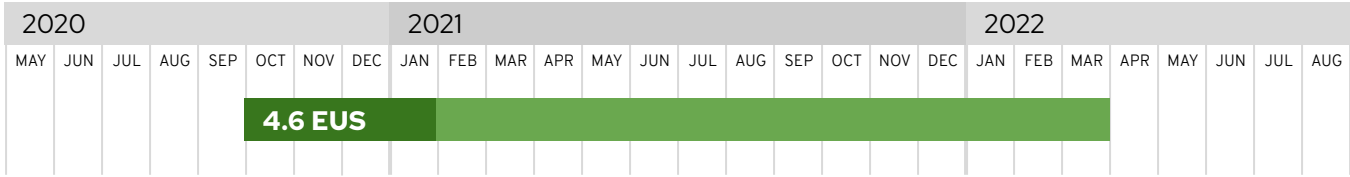
Goals for the 4.6 EUS

- Work within a customer's release management philosophies
- Provide an over-the-air pathway to update between EUS releases (currently serially)
  - Customer might align more to CAM or ACM
- Aligned with RHEL 8.2 EUS



Red Hat

OpenShift EUS and Layered Product and Add-ons



Duration of the Platform EUS

Add-ons have a version that is guaranteed to work for Platform EUS

OpenShift Serverless
OpenShift Pipelines
OpenShift Service Mesh

OpenShift Logging
OpenShift Container Storage
Advanced Cluster Manager

Red Hat

Kubernetes 1.19

Control Plane & Security

- Automatically track and act on the features not making Stable
- Warning mechanism for use of deprecated APIs
- AppProtocol to Services and Endpoints
- Kubelet Client TLS Certificate bootstrap and rotation
- NodeRestriction admission controller

Misc

- Structured Logging proposal

Scheduling

- Customize the behavior of the Kube-scheduler
- Scheduler Profiles
- Pod Topology Spread constraints

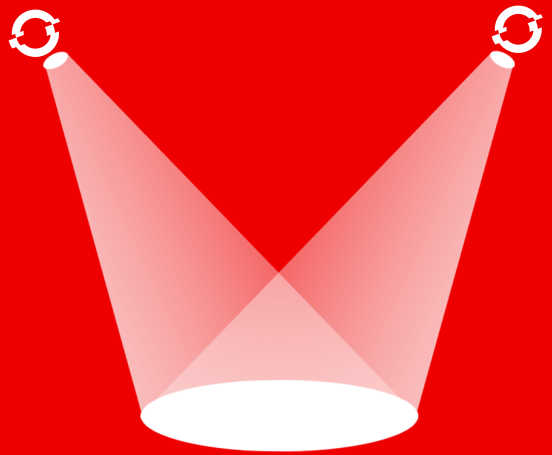
Storage

- Immutable Secrets and ConfigMaps
- CSI Storage Capacity management (alpha)

CRI-O 1.19  Kubernetes 1.19  OpenShift 4.6 

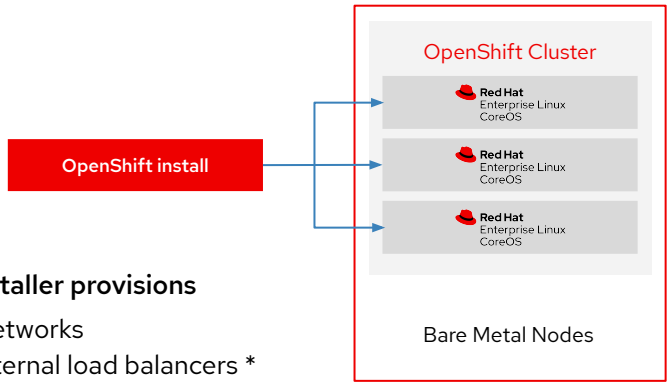
Blog: https://www.openshift.com/blog/kubernetes-1.19-arrives

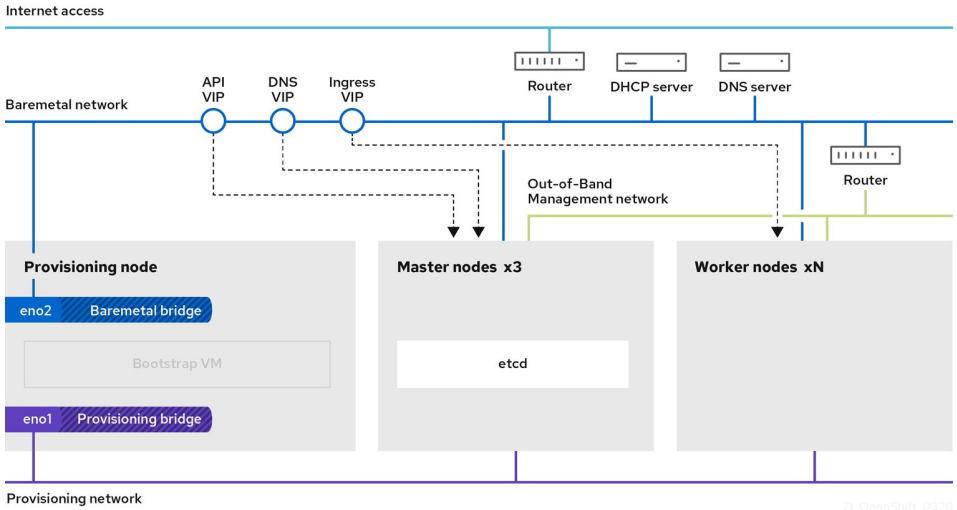
OpenShift 4.6 Spotlight Features



Full stack automation (IPI) installation on Bare Metal

Deploying Red Hat OpenShift on Bare Metal on Installer-Provisioned Infrastructure (IPI)





- **Installer provisions**
  - Networks
  - Internal load balancers *
  - Internal DNS *
  - Red Hat CoreOS installation
  - CoreOS ignition configs
  - OpenShift nodes
  - OpenShift cluster resources

*External Load Balancers (routing) and external DNS servers are provided by the user

Full stack automation (IPI) installation on Bare Metal

Deploying Red Hat OpenShift on Bare Metal on Installer-Provisioned Infrastructure (IPI)

Bare Metal Management
Powered by Metal^3 and OpenStack Ironic under the hood

Host Power Management
Redfish, IPMI, iDrac, iLo.

Provisioning over the network
Installation over DHCP/PXE or Virtual Media

Disconnected Installations
RHCOS image cache and disconnected registry

Metal^3


OpenStack Ironic

```
apiVersion: v1
basedomain: <domain>
metadata:
  name: <cluster-name>
networking:
  machineCIDR: <public-cidr>
  networkType: OVNKubernetes
compute:
- name: worker
  replicas: 2
controlPlane:
  name: master
  replicas: 3
  platform:
    baremetal: {}
```

```
platform:
  baremetal:
    apiVIP: <api-ip>
    ingressVIP: <wildcard-ip>
    provisioningNetworkInterface: <NIC1>
    provisioningNetworkCIDR: <CIDR>
    hosts:
      - name: openshift-master-0
        role: master
        bmc:
          address: ipmi://<out-of-band-ip>
          username: <user>
          password: <password>
        bootMACAddress: <NIC1-mac-address>
        hardwareProfile: default
      - name: openshift-master-1
        role: master
        bmc:
          address: ipmi://<out-of-band-ip>
          username: <user>
          password: <password>
        bootMACAddress: <NIC1-mac-address>
        hardwareProfile: default
```

AWS GovCloud

Deploy OpenShift to AWS GovCloud regions

- Government customers and their Partners can now deploy OpenShift to the AWS GovCloud 'US-East' & 'US-West' regions.
- AWS GovCloud (US) is specifically designed for US government agencies at the federal, state, and local level, as well as contractors, educational institutions, and other U.S. customers that need to run sensitive workloads in the cloud.
- RHEL CoreOS AMI publishing is not available in the GovCloud regions, so users must upload their own prior to installing OpenShift via:
  - 'aws ec2 import-snapshot' & 'aws ec2 register-image'
- Installation of OpenShift on AWS GovCloud is similar to existing deployment methods for other AWS regions, but the AWS region and RHEL CoreOS AMI ID must be manually configured in install-config.yaml.

```
% aws ec2 describe-regions --output text
REGIONS    ec2.us-gov-west-1.amazonaws.com    opt-in-not-required    us-gov-west-1
REGIONS    ec2.us-gov-east-1.amazonaws.com    opt-in-not-required    us-gov-east-1

% grep -B 1 -A 2 "aws:" mycluster/install-config.yaml
platform:
  aws:
         region: us-gov-west-1
         amiID: ami-9dbf86fc

% ./openshift-install create cluster --dir mycluster
INFO Credentials loaded from default AWS environment variables
INFO Consuming Common Manifests from target directory
INFO Consuming Worker Machines from target directory
INFO Consuming Openshift Manifests from target directory
INFO Consuming OpenShift Install (Manifests) from target directory
INFO Consuming Master Machines from target directory
INFO Creating infrastructure resources…
INFO Waiting up to 20m0s for the Kubernetes API at
https://api.mycluster.example.com:6443...
INFO API v1.19.0+f5121a6 up
INFO Waiting up to 30m0s for bootstrapping to complete...
INFO Destroying the bootstrap resources...
INFO Waiting up to 40m0s for the cluster at https://api.mycluster.example.com:6443
to initialize...
INFO Waiting up to 10m0s for the openshift-console route to be created...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/Users/userid/openshift-install/mycluster/auth/kubeconfig'
INFO Access the OpenShift web-console here:
https://console-openshift-console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password:
"5char-5char-5char-5char"
INFO Time elapsed: 40m10s
```


Generally Available

Product Manager: Katherine Dubé

Microsoft Azure Government (MAG)

Microsoft Azure

Deploy OpenShift to Microsoft Azure Government

- Government customers and their Partners can now deploy OpenShift to the Microsoft Azure Government (MAG) dedicated instance.
- MAG is comprised of six government-only datacenter regions, all granted an Impacted Level 5 Provisional Authorization.
- Installation of OpenShift to MAG is similar to existing deployment methods for other Azure regions, but the 'cloudName' field must be set to 'AzureUSGovernmentCloud' in the install-config.

```
% az cloud set --name AzureUSGovernment
Switched active cloud to 'AzureUSGovernment'.
Active subscription switched to 'Production (291bba3f-e0a5-47bc-a099-3bdcb2a50a05)'.

% az account list-locations -o table
DisplayName     Name             RegionalDisplayName
--------------  -------------  --------------------
Global          global           Global
USDoD Central   usdodcentral   (US) USDoD Central
USDoD East      usdodeast        (US) USDoD East
USGov Arizona   usgovarizona   (US) USGov Arizona
USGov Iowa      usgoviowa        (US) USGov Iowa
USGov Texas     usgovtexas       (US) USGov Texas
USGov Virginia  usgovvirginia  (US) USGov Virginia

% ./openshift-install explain installconfig.platform.azure.cloudName
RESOURCE: <string>
  cloudName is the name of the Azure cloud environment which can be used to configure the Azure SDK
with the appropriate Azure API endpoints. If empty, the value is equal to "AzurePublicCloud".

% export AZURE_AUTH_LOCATION=/Users/userid/.azure/osServicePrincipal-mag.json ; ./openshift-install
create cluster --dir mycluster
INFO Credentials loaded from file "/Users/userid/.azure/osServicePrincipal-mag.json"
INFO Consuming Common Manifests from target directory
INFO Consuming Worker Machines from target directory
INFO Consuming Openshift Manifests from target directory
INFO Consuming OpenShift Install (Manifests) from target directory
INFO Consuming Master Machines from target directory
INFO Creating infrastructure resources…
INFO Waiting up to 20m0s for the Kubernetes API at https://api.mycluster.example.com:6443...
INFO API v1.19.0+f5121a6 up
INFO Waiting up to 30m0s for bootstrapping to complete...
INFO Destroying the bootstrap resources...
INFO Waiting up to 40m0s for the cluster at https://api.mycluster.example.com:6443 to initialize...
INFO Waiting up to 10m0s for the openshift-console route to be created...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/Users/userid/openshift-install/mycluster/auth/kubeconfig'
INFO Access the OpenShift web-console here:
https://console-openshift-console.apps.mycluster.example.com
INFO Login to the console with user: "kubeadmin", and password: "5char-5char-5char-5char"
INFO Time elapsed: 40m10s
```


Generally Available

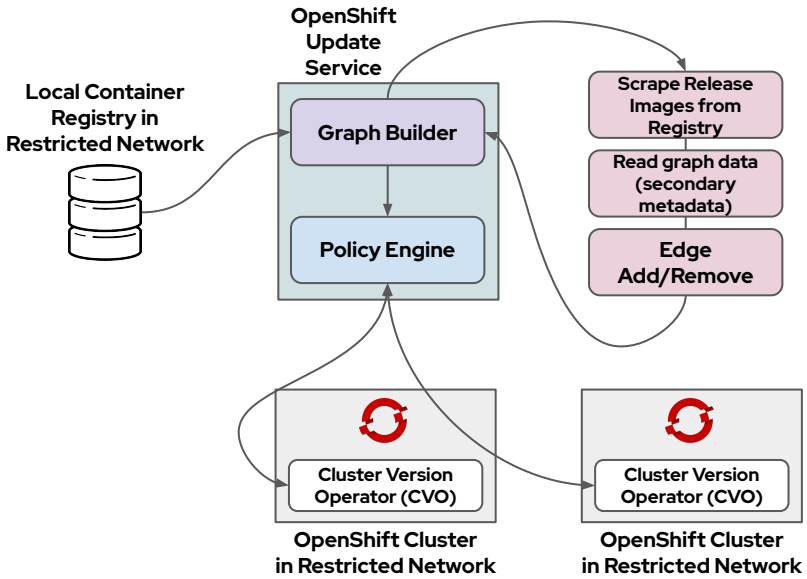
Red Hat

Product Manager: Katherine Dubé

OpenShift Update Service

Update manager for your clusters in restricted or disconnected networks

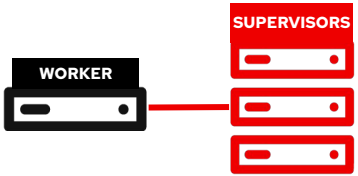
- OpenShift Update Service (OSUS) is the on-premise release of Red Hat's hosted update service
- Supports the publishing of upgrade graph information to clusters in restricted networks
- Provides clusters with a list of next recommended update versions based on the current version installed on the cluster
- Comprised of two services:
  - **Graph Builder:** Fetches OpenShift release payload information (primary metadata) from any container registry (compatible with Docker registry V2 API) and builds a directed acyclic graph (DAG) representing valid upgrade edges
  - **Policy Engine:** Responsible for selectively serving updates to every cluster by altering a client's view of the graph with a set of filters
- GA release planned for post-4.6 and will be distributed on Operator Hub as an optional add-on operator
- Blog post announcing OpenShift Update Service Generally Available



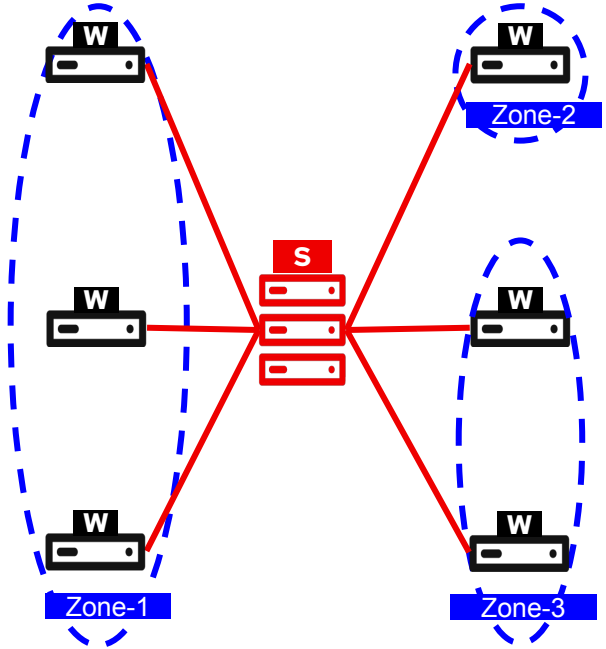
Product Manager: Katherine Dubé

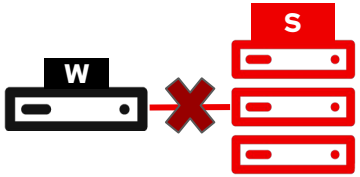
Red Hat

Specifications for Remote Worker Nodes



Red Hat OpenShift Supervisors reside in a central location, with reliably-connected workers distributed at edge sites sharing a control plane.





Tolerant of disruption

- Admin can configure status update frequency
- Zones with disruption budget
- Tolerations
- DaemonSet & Static Pods stay running

Product Manager: Tushar Katarki

Red Hat

Open Virtual Network (OVN)

Goal: Develop and support a modern, maintainable, community-based, open-source Kubernetes CNI network plugin for OpenShift that complements the existing capabilities of OVS to add native support for virtual network abstractions.

- Next-gen Kubernetes CNI plugin (ovn-kubernetes)
- OCP 4.6 GA (non-default, default TBD)
- Install-time option or post-install (bare metal only) migration

Why?

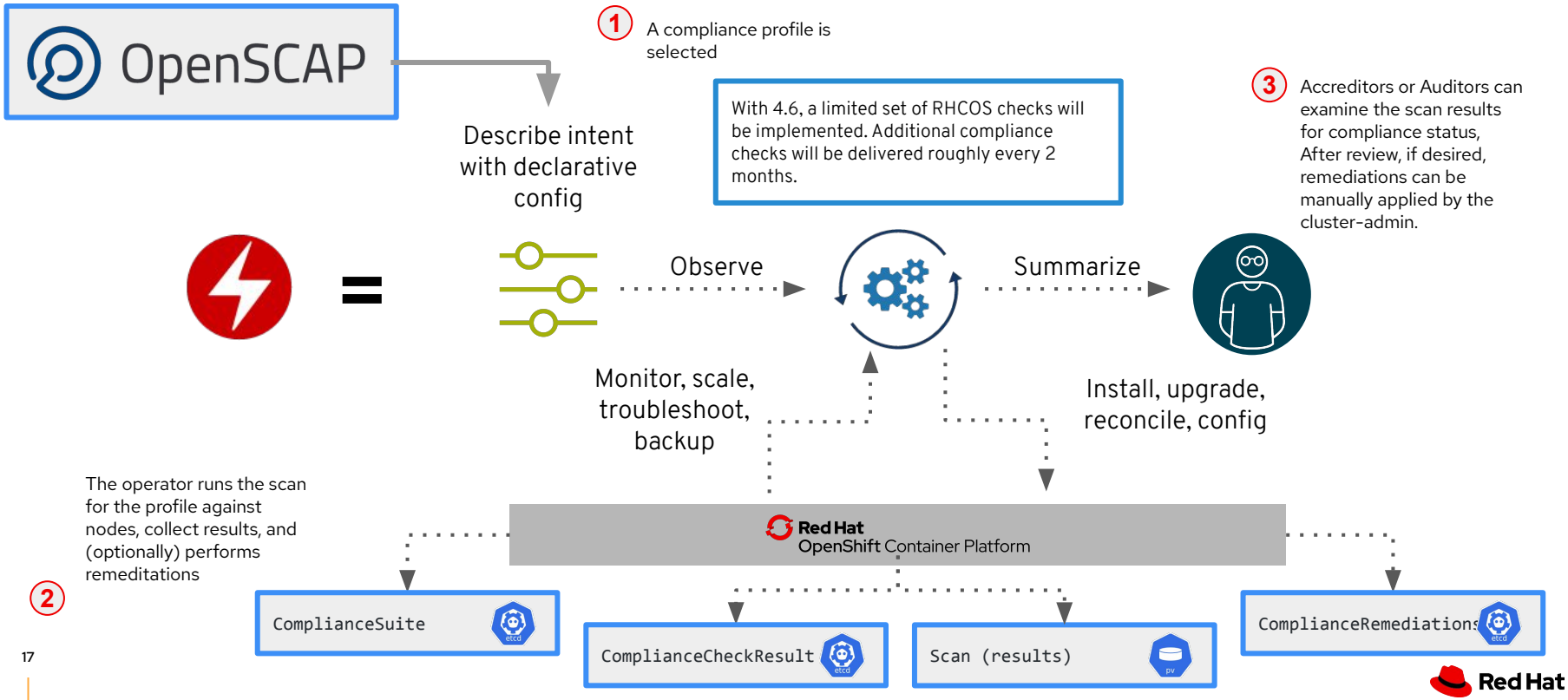
- Consolidates Red Hat SDN efforts across products
- Advanced Telco and enterprise-grade features
- Flexible SDN architecture for faster feature development
- Large upstream community (Linux Foundation project)
- Red Hat leadership in upstream OVS & OVN communities
- Manages overlays and physical network connectivity
- Flexible security policies via ACLs and security groups
- Distributed L3 routing, L2/L3 Gateways to other networks
- IPv4 and IPv6 capability
- Integration with TOR and other "physical" gateways
- Native support for NAT, load balancing and IPAM
- Windows “Hybrid Overlay” service for pod-to-pod traffic between Windows and Linux cluster nodes.

Technology Highlights Comparison

OpenShift SDN	OVN Kubernetes
veth pairs	veth pairs
OVS bridge	OVS bridge
Central controller / host-ipam	Central controller / host-ipam
VXLAN tunnels	Geneve tunnels
OVS flows for NetworkPolicy	OVS flows for NetworkPolicy
IPTables for services	OVN LBs for services
IPTables for NAT	OVS for NAT

Product Manager: Marc Curry

OpenShift Compliance Operator: Declarative Security Compliance



Product Manager: Kirsten Newcomer

Monitor your own services

Generally Available

Leverage our existing Monitoring infrastructure to monitor your own workloads.

- Enable a dedicated monitoring stack managed by us.
- Configure monitoring for your custom services or infrastructure services not covered by the out-of-the-box cluster monitoring stack.
- Access metrics and alert information through a single, multi-tenant interface.
    - **Note:** You can explore and manage both from the developer perspective inside the OpenShift Console.
- Not in scope for this release are things like adding your own dashboards to the console, creating new rules inside platform-specific namespaces (e.g. openshift-*), tenant-based routing configuration for Alertmanager, and a few more.
- *Monitoring your sample application* **Quick Start** available to show users how to access basic monitoring features

1. Enable dedicated monitoring by setting ‘enableUserWorkload’ to ‘true’ inside the cluster-monitoring-config ConfigMap.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml: |
    enableUserWorkload: true
```

2. Configure a ServiceMonitor CR inside a user-defined namespace where app is running that exposes a /metrics endpoint.

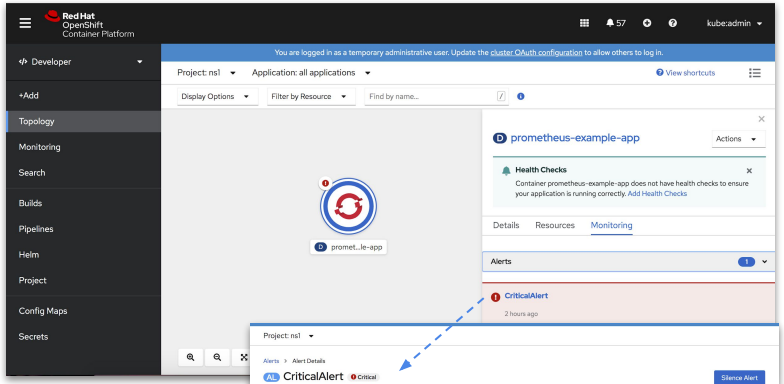
3. Go to the Developer Perspective, switch to your namespace and look for your metrics (it can take a bit time to have our infra picking up everything)

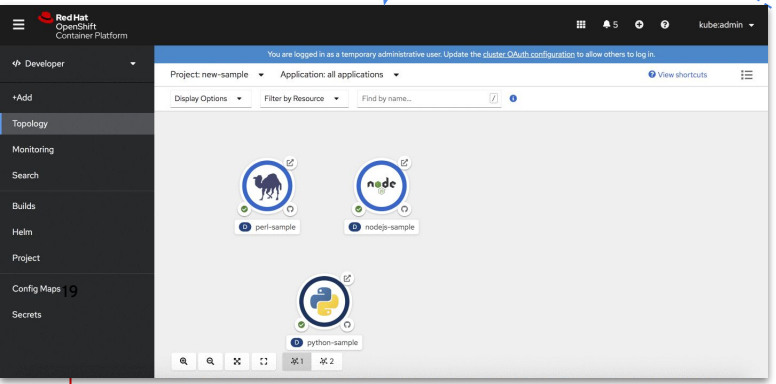
Application Monitoring & Troubleshooting

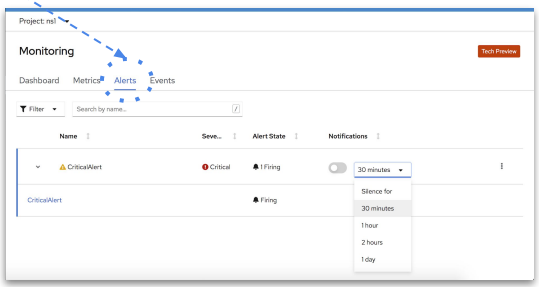
Generally Available

Monitor your applications with ease!

- Improved discoverability of alerts in topology and Monitoring
- Easy access to **Alert Details**
- **Alerts** tab allows users to view application alerts & silence them as as needed
- *Monitoring your sample application* **Quick Start** available to show users how to access basic monitoring features







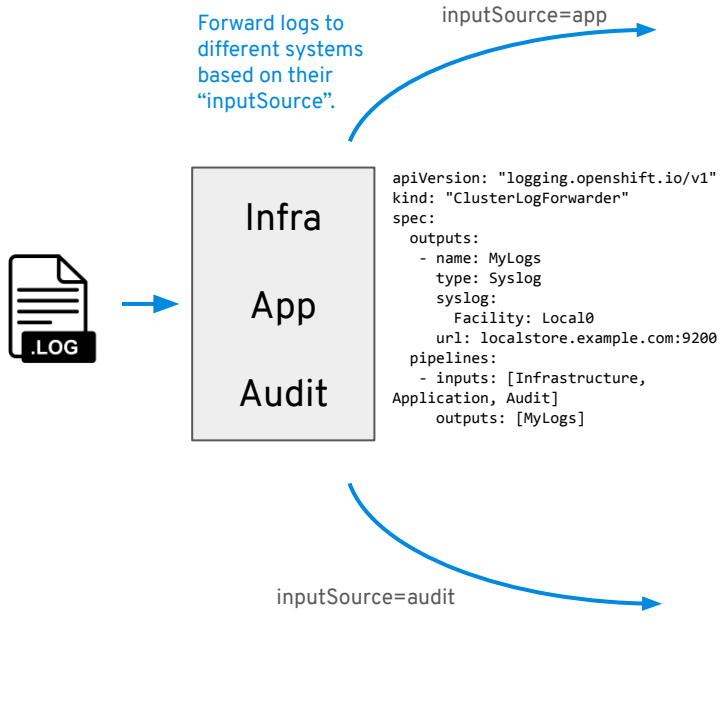
Red Hat

Introduce new log forwarding API

Generally Available

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

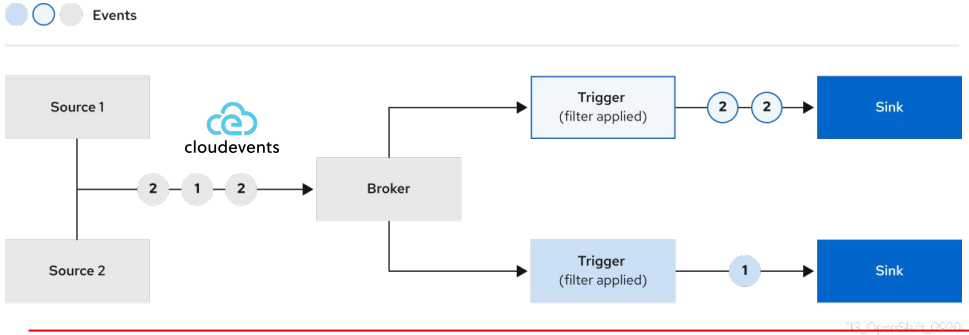
- Introduce a new, cluster-wide *ClusterLogForwarder* CRD (API) that replaces needs to configure log forwarding via Fluentd ConfigMap.
- The API helps to reduce probability to misconfigure Fluentd and helps bringing in more stability into the Logging stack.
- Features include: Audit log collection and forwarding, Kafka support, namespace- and source-based routing, tagging, as well as improvements to the existing log forwarding features (e.g. syslog RFC5424 support).
- **WARNING:** We will not automagically migrate old Tech Preview CRs into a GA CR.



Generally Available

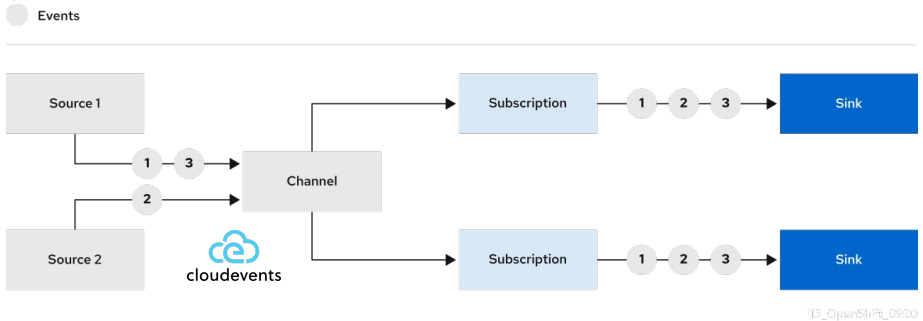
Coming with OpenShift Serverless 1.11

Eventing



- **Brokers**
  - ✓ Built-in Event Filtering
  - ✓ Routing based on event types or attributes
  - ✓ Multiple event types
  - ✓ Multi-tenant

- **Channels**
  - ✓ Event Fanout to multiple subscribers
  - ✓ *Same event type*
  - ✓ *Single-tenant*



Product Manager: William Markito & Naina Singh

Red Hat

Generally Available

Coming with OpenShift Serverless 1.11

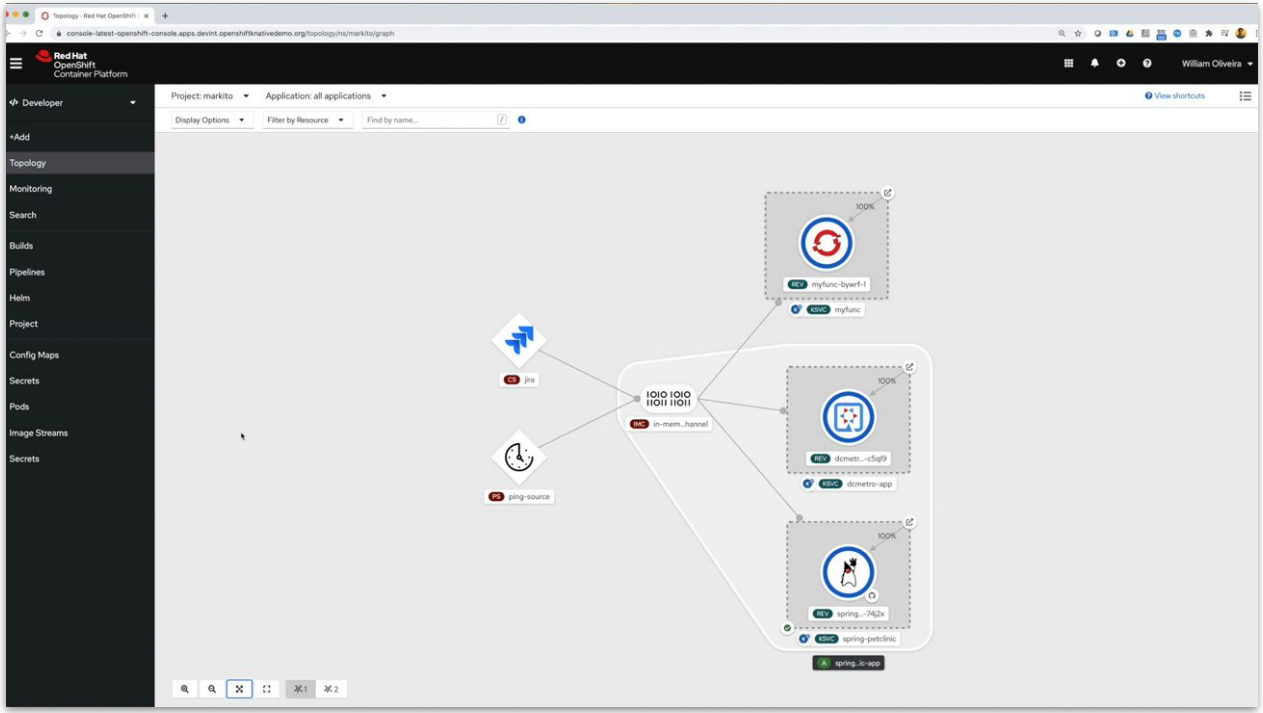
Eventing User Experience

Camel-K Connectors

- Connect your applications with AWS Kinesis, AWS SQS, Slack, JIRA, Telegram, SalesForce and more...

Red Hat AMQ Streams

- Integration with Apache Kafka for reliable event delivery with Channels and Broker support.



Product Manager: William Markito & Naina Singh

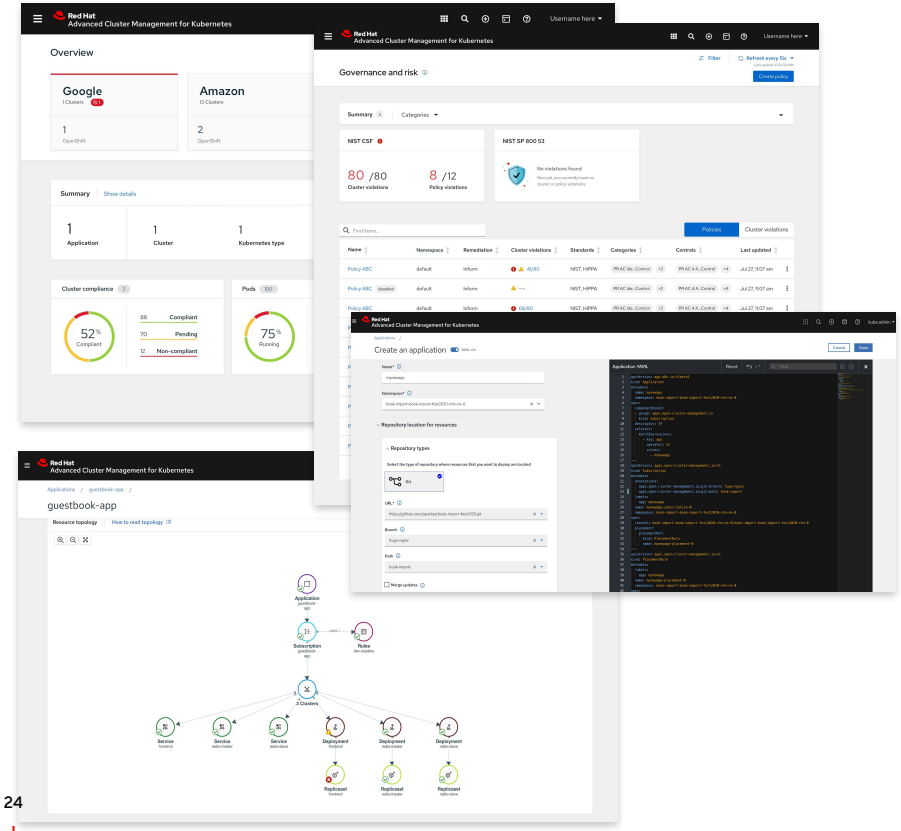
Red Hat

Red Hat Advanced Cluster Management for Kubernetes

Robust. Proven. Award-winning.

Red Hat Advanced Cluster Management for Kubernetes

What's new with 2.1



Multi-cluster lifecycle management

- GA provisioning of OpenShift on vSphere
- GA provisioning of OpenShift on Bare Metal

Policy driven governance, risk, and compliance

- Open Source Policy Repository
- Enhanced OPA integration

Advanced application lifecycle management

- Simplified Application Experience
- Portfolio Integration with Ansible Automation Platform - Tech Preview

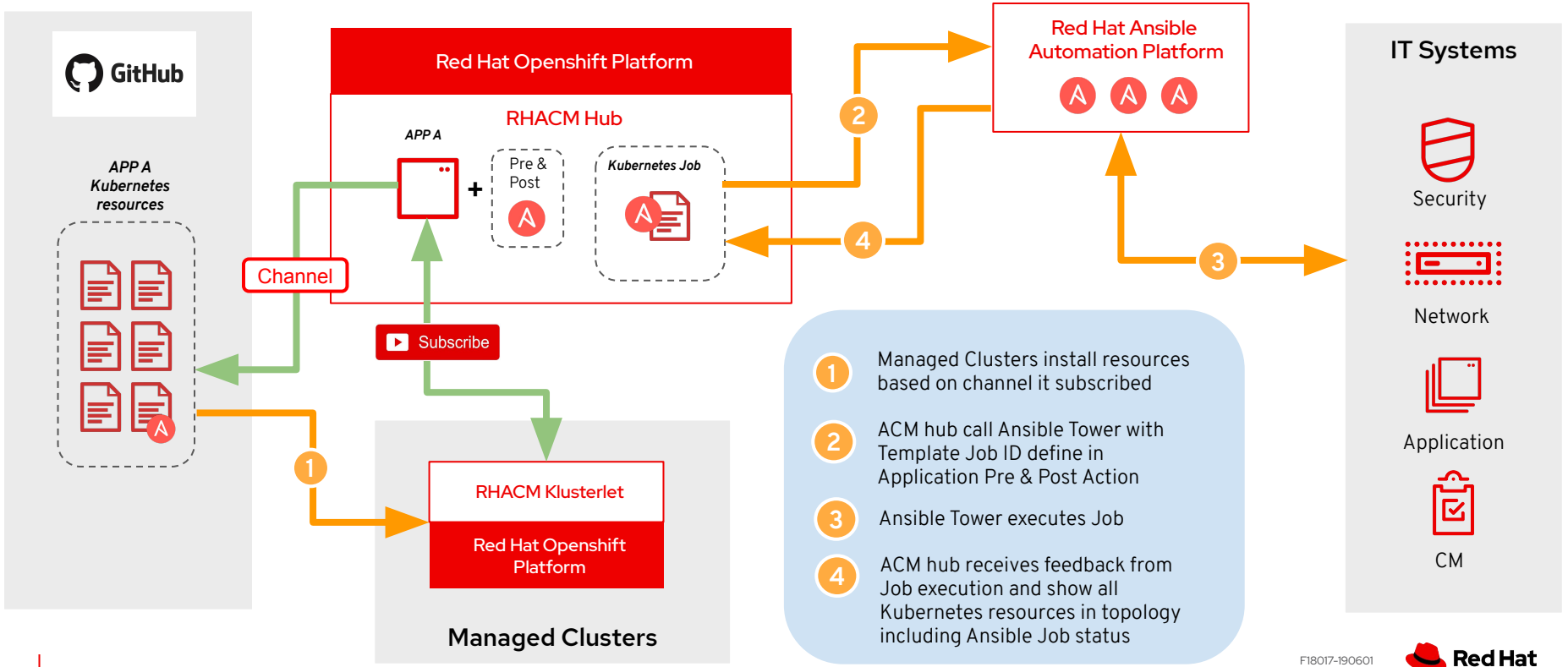
Observability for your Clusters and Apps

- Cluster Health monitoring with Thanos
- Multi-cluster health optimization with Grafana

Red Hat

Tech Preview

Integration Architecture Overview for Application Life Cycle



F18017-190601

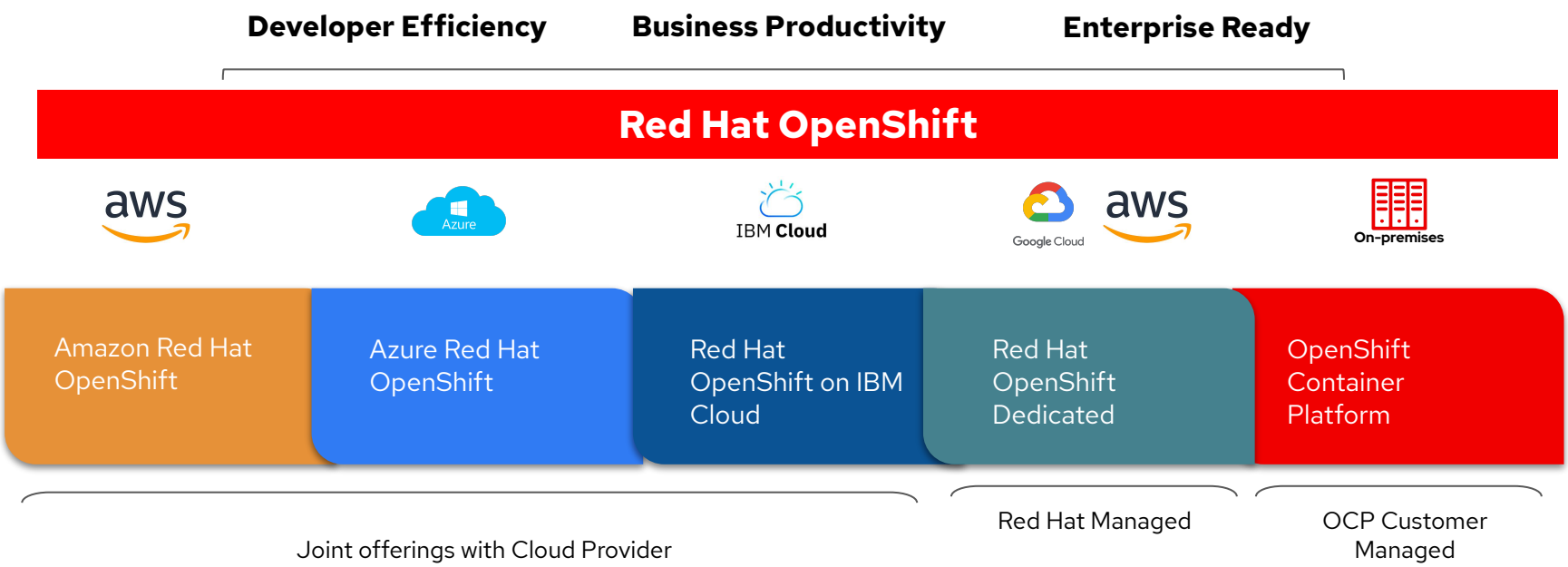
Red Hat

Managed OpenShift

Get the best of OpenShift without being on call

Red Hat

OpenShift offers the broadest set of hybrid cloud services



Offered as a Native Console offering on equal parity with cloud provider Kubernetes service

or

OCP Customer Managed

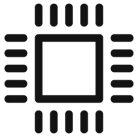
Red Hat

New Managed OpenShift Pricing

Cluster Fee

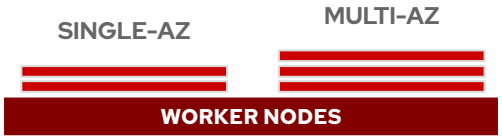
$0.03 per hour

vCPU Based Pricing



4 vCPU
24x7 Premium Support
99.95% Uptime SLA

New Minimum Cluster Size (OSD)



4 vCPU SUBSCRIPTION	PRICE
On-demand (hourly)	$0.171
1 Year	$1,000
3 Year	$2,000

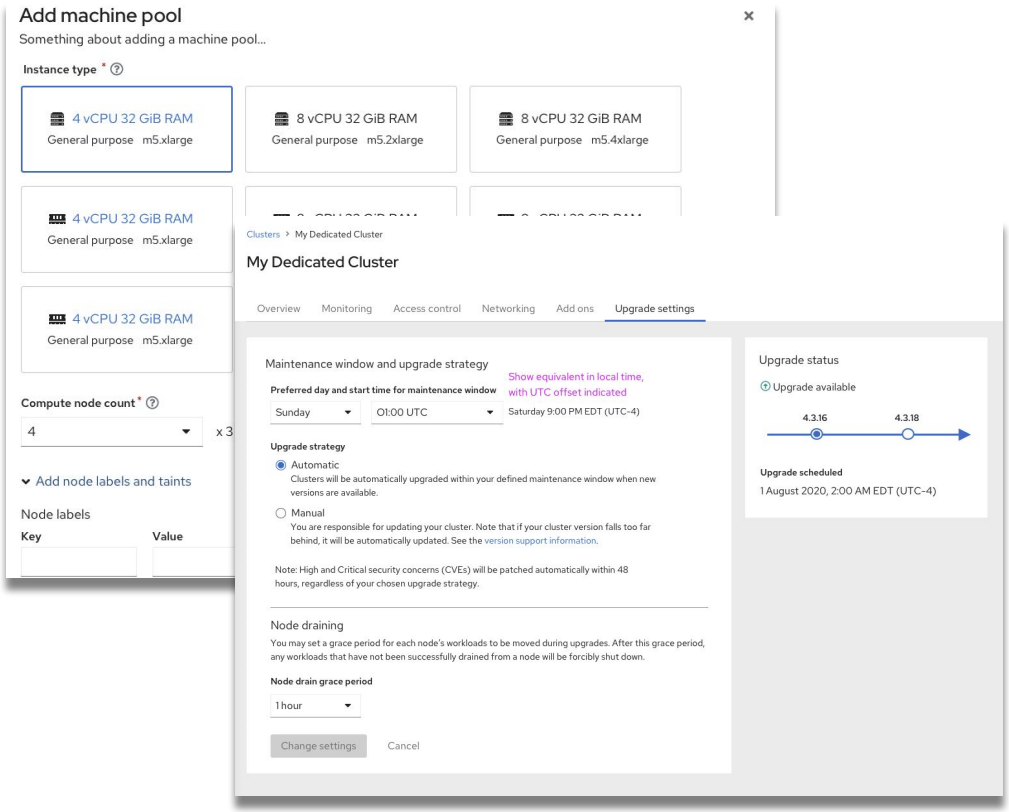
https://www.openshift.com/pricing/

Product Managers: Patrick Strick, Jacob Lucky, Andrew Cathrow

OpenShift Dedicated & Amazon Red Hat OpenShift

New Feature Highlights

- UI for cluster upgrade scheduling
- Custom Machine Pools (AZ aware Machine Sets)
- Customer notifications tied to Cluster History Log
- BYOK Disk Encryption on AWS CCS



Azure Red Hat OpenShift

Microsoft Azure Government (MAG)

- Deploy managed OpenShift clusters on Azure's government cloud

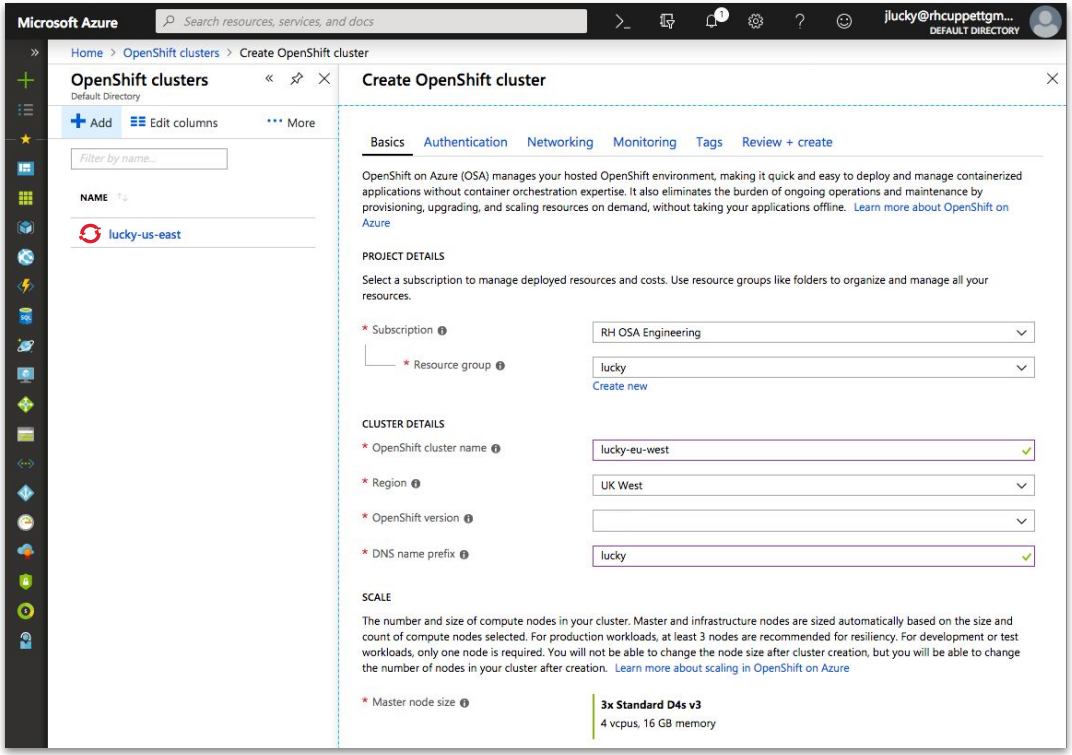
Egress lockdown

- Documented outbound IP/DNS requirements to secure outbound traffic via firewall

BYOK disk encryption for PV's and OS disk

Larger VM sizes, including dedicated instances

Cluster create GUI in Azure Portal

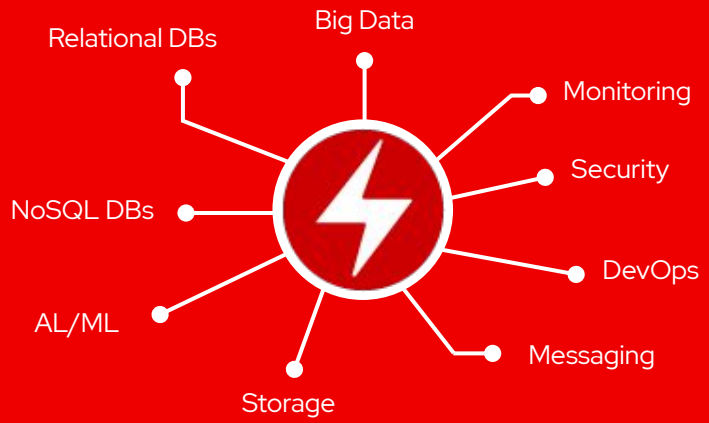


Product Manager: Jacob Lucky

Red Hat

A broad ecosystem of workloads

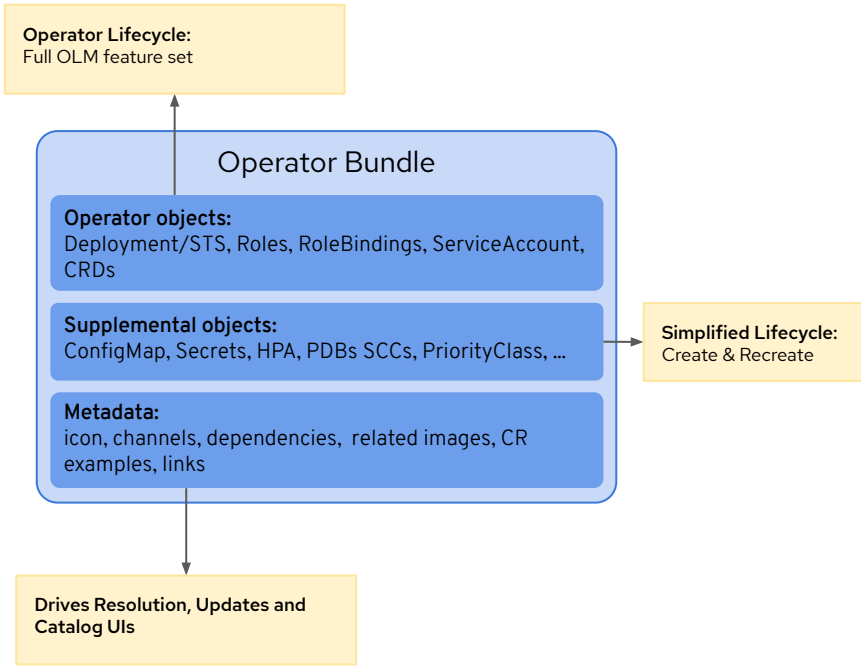
Services allow for a
SaaS experience on your own infrastructure



Red Hat

New Operator Bundle Format

The Bundle format uses standard container technology for shipping the metadata and allows developers to publish their own Operator update streams in catalogs. This is very similar to how OCI artifact spec plans to ship non-runnable image artifacts through registries.



Changes to building custom catalogs

- Using opm was optional, now it is mandatory
- Much easier UX to add/remove/update catalog content

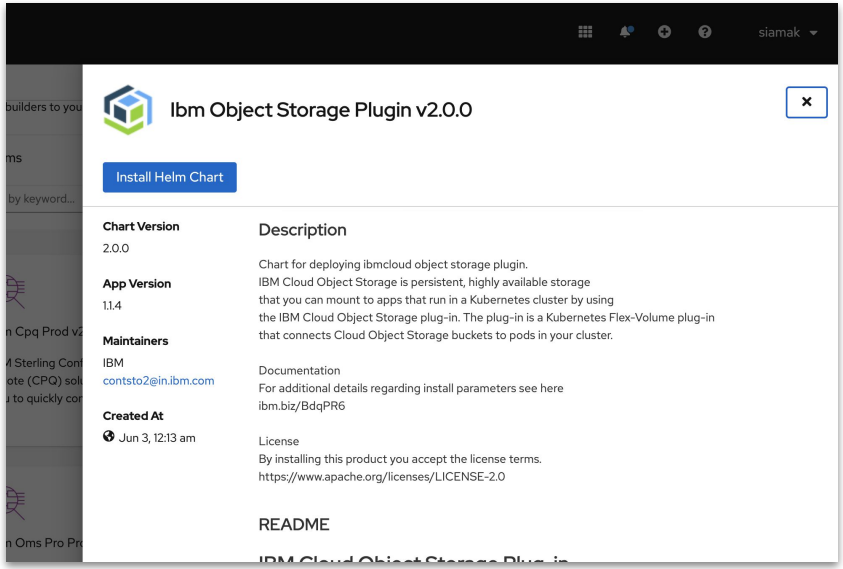
```
opm index add
  --bundles quay.io/username/my-bundle:0.0.1 # add this bundle
  --tag quay.io/username/my-index:1.0.0      # to this catalog
```

OpenShift now has per-version Operator catalogs

- Teams can ship to very intentional ranges of OCP versions
- 4.1 to 4.5 will continue to share a single catalog

Helm 3 on OpenShift 4.6

- Helm 3.3 GA
- Support for multiple Helm repositories in Developer Catalog
- Select chart version on install
- Form-based `values.yaml`
- Displays charts compatible with OpenShift version (`kubeVersion`)

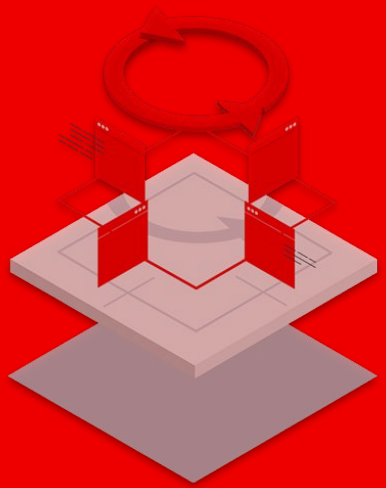


Product Manager: Karena Angell

Red Hat

Cloud Native Development

OpenShift has all of the latest **tools** and **services**
to make your devs more productive

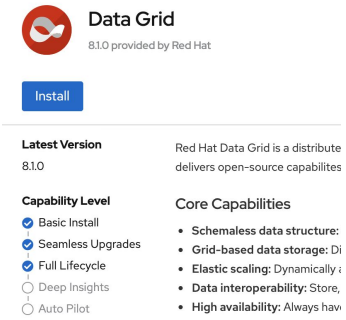


Code	**CI/CD**
Serverless	**Service Mesh**
RED HAT® MIDDLEWARE	IBM *Cloud Paks*

Red Hat Application Services

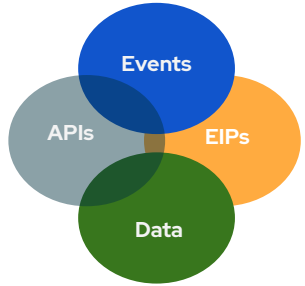
Red Hat Runtimes

- **Quarkus** - GA of Native Compilation Support, OpenShift Extension GA and new Spring compatibilities
- **Data Grid 8.1** - Cross-site cluster support and auto-scaling on OpenShift
- **Red Hat Build of OpenJDK** Support for the Java Flight Recorder - OpenJDK 8
- **Spring Boot 2.2** - New AMQ Starters, GA of Reactive support and Kubernetes Java annotations.



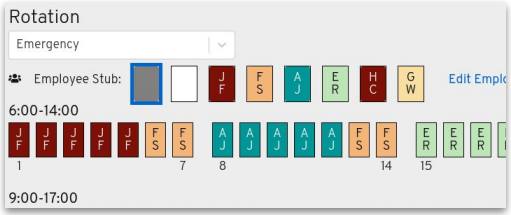
Red Hat Integration

- **3scale API Management -** Improved manageability with operator for Air-Gapped deployment, Monitoring & backup/restore. Accelerated API performance with content caching, and new policies for API Gateway.
- **Fuse -** Air-Gapped deployment, OpenShift AuthN/AuthZ for Console, and Spring Boot 2 support for Fuse on OpenShift.
- **Camel K for Serverless (TP) -** now integrated to OpenShift Developer Console to leverage the huge Camel connector catalog for apps based on Camel K and Knative Eventing.



Red Hat Process Automation

- **OptaPlanner -** Support for new rotation screen in Optaweb Employee Rostering
- **Dashboard Builder -** Stand alone Dashbuilder: Support for multiple dashboards, Runtime REST api, React components



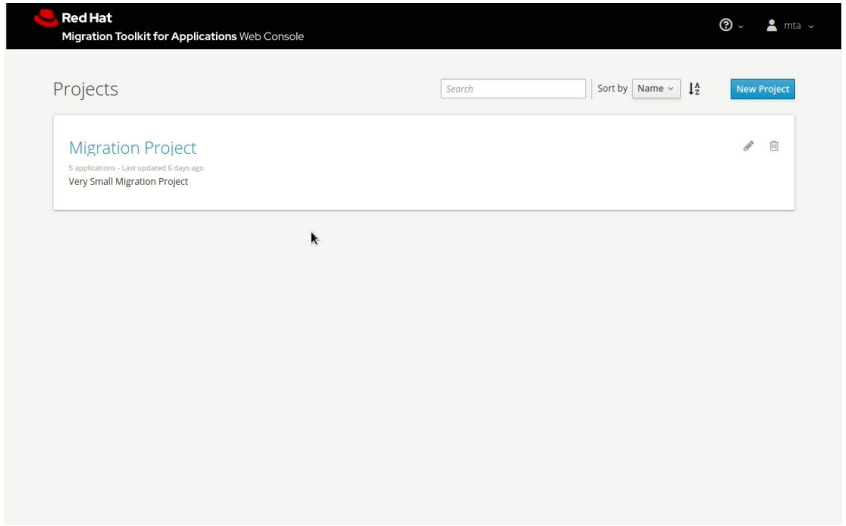
Product Manager: Karena Angell (on behalf of the Red Hat Application Services team)

Red Hat

Migration Toolkit for Applications

MTA 5.0 Launched

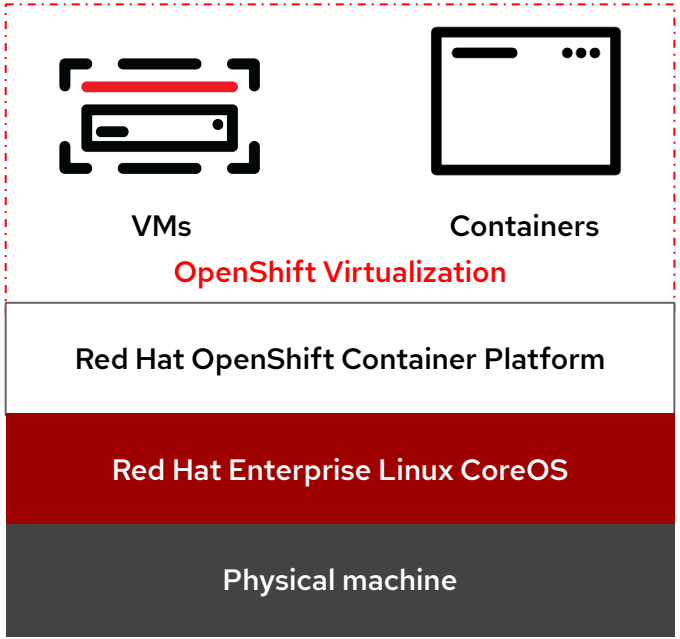
- **Review Java Apps -** review source code or decompile binaries and find ways to make them more JEE compliant, and container friendly.
- **OpenJDK, Container and Linux rules -** discover fixes to be applied to your app to increase its mobility
- **Camel 2 to 3 Rules -** review your Camel 2 rules and find out how to convert them to Camel 3 (more container friendly).
- **Web,CLI, Maven and IDE -** use the tool in any your preferred context, from CI/CD pipelines , to maven builds and in within your development environment. Easy to deploy on OpenShift.



red.ht/mta

What's new in OpenShift Virtualization (2.5)

Modernized workloads, support mixed applications consisting of VMs, containers, and serverless



Core

- Deploy operator on a subset of cluster nodes
- Import from VMware - cold or offline migration
- Robust VM baseline performance

Network

- Support of bonding modes 2 (balance-xor) and 4 (802.3ad)
- Added CNI certification test suite for VMs

Storage

- Improved dev workflow with default OS images & templates
- Fast DataVolume CDI cloning via CSI Snapshots
- Offline VM Snapshots
- Import ContainerDisks to persistent storage more efficiently

Product Manager: Peter Lauterbach, Rob Young

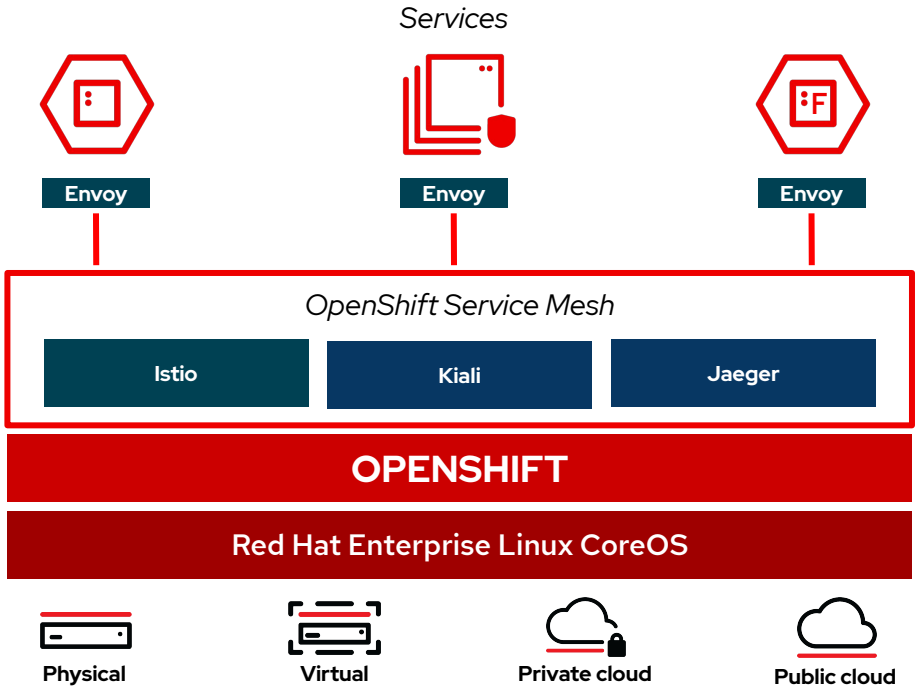
Service Mesh

OpenShift Service Mesh

Connect, Secure, Control and Observe Services on OpenShift

- Connect services securely with zero-trust network policies.
- Automatically secure your services with managed authentication, authorization and encryption.
- Control traffic to safely manage deployments, A/B testing, chaos engineering and more.
- See what's happening with out of the box distributed tracing, metrics and logging.
- Manage OpenShift Service Mesh with the **Kiali** web console.

[Product briefing deck]



Product Manager: Jamie Longmuir and Mauricio "Maltron" Leal

* Eventing is currently in Technology Preview

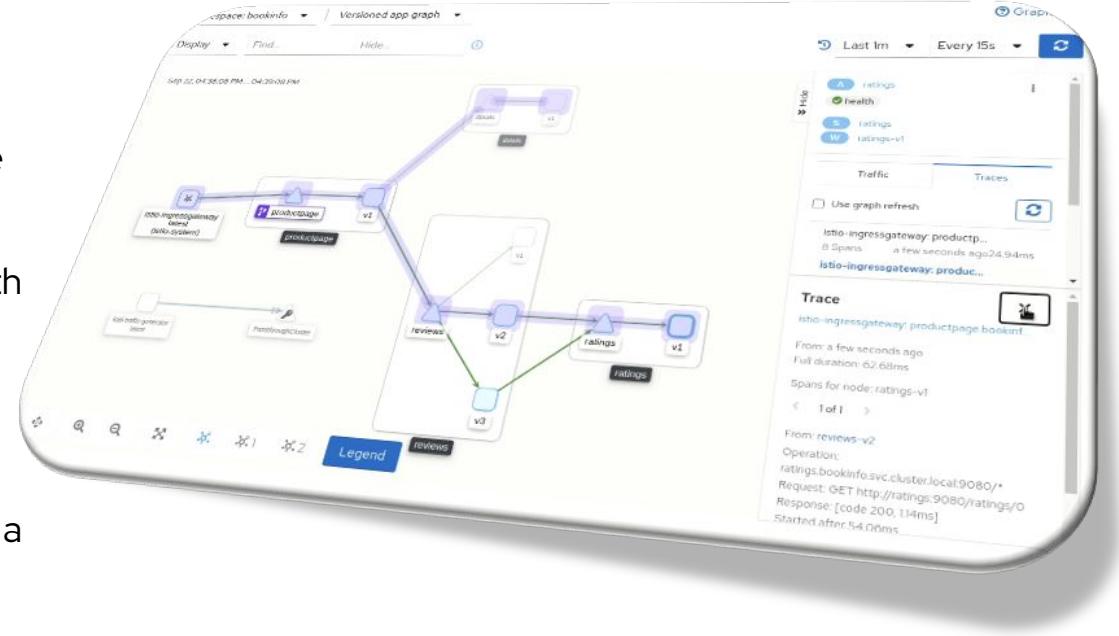
** Functions are currently a work in progress initiative

Red Hat

OpenShift Service Mesh 2.0

Key Features & Updates

- Version 2.0 to GA in November 2020
- Upgrades Istio to version 1.6
- Simplifies architecture based on a single Istio daemon (“Istiod”)
- Improves key and certificate rotation with Secret Discovery Service
- Improves metrics collection with Telemetry V2 architecture.
- Introduces WebAssembly extensions as a “Tech Preview” feature.



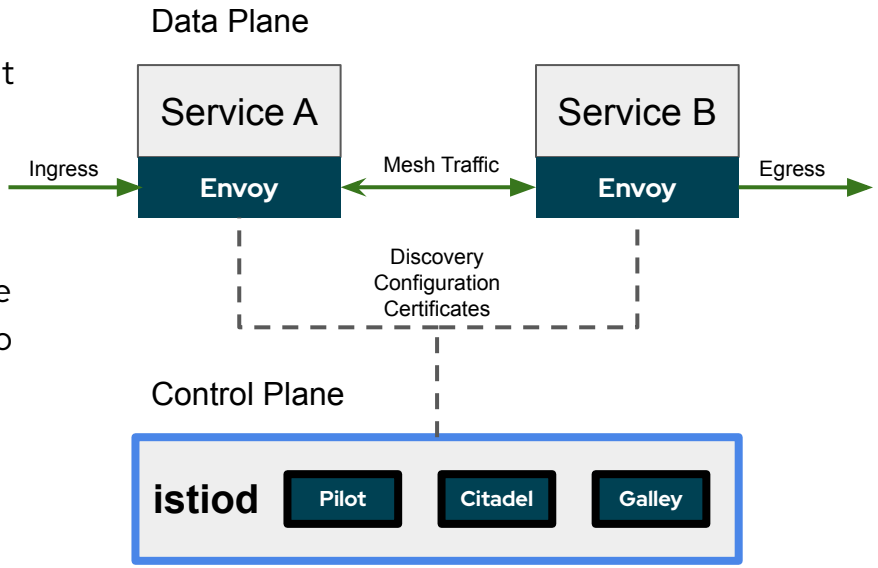
Product Manager: Jamie Longmuir and Mauricio "Maltron" Leal

Red Hat

OpenShift Service Mesh 2.0

Istio 1.6 - Architectural Changes

- Consolidates the Istio control plane components (Pilot, Galley, Citadel) into a single binary known as **istiod**.
  - Simplifies installation, upgrades and management of the Control Plane.
  - Reduces the Control Plane's resource usage, startup time and improves performance.
- Secret Discovery Service (**SDS**) provides a more secure and performant mechanism for delivering certificates to Envoy side car proxies.
  - Removes the use of Kubernetes Secrets.
  - Enables 3rd party cert manager integrations.
- New **Telemetry V2** architecture substantially reduces metrics collection latency.



OpenShift Service Mesh 2.0

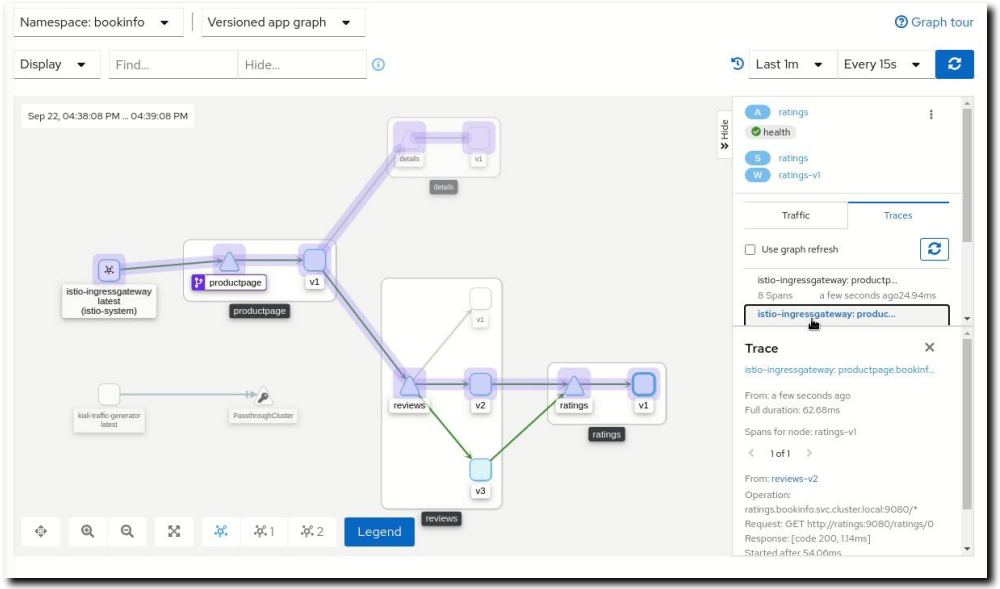
Secret Discovery Service

- Secret Discovery Service (**SDS**) is a more secure and performant mechanism for delivering secrets to Envoy side car proxies.
  - Removes the need to use Kubernetes Secrets, which have well known security risks.
  - Improves performance during certificate rotation, as proxies no longer require a restart.
  - Enables integration with 3rd party certificate managers, such as Vault.

OpenShift Service Mesh 2.0

User Experience Enhancements

- New **ServiceMeshControlPlane** resource (v2) to simplify configuration.
- **Kiali**:
  - Distributed traces are visualized and accessible in the service graph.
  - New wizards make it easier to configure timeouts, retries and fault injection scenarios.
- **Jaeger**:
  - Support for external ElasticSearch clusters.
  - OpenTelemetry collector in Tech Preview enabling vendor-neutral instrumentation.



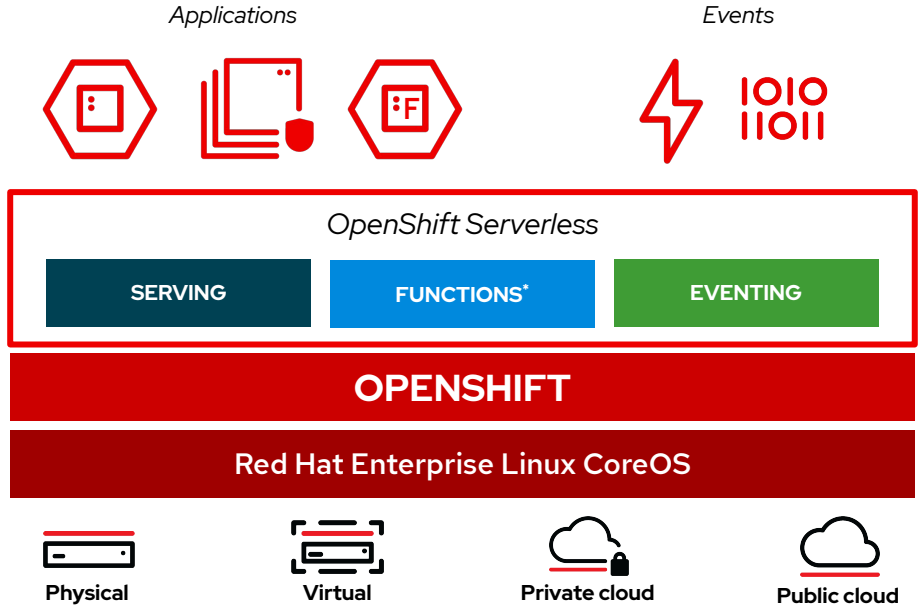
Product Manager: Jamie Longmuir and Mauricio "Maltron" Leal

Serverless

OpenShift Serverless

Event-driven serverless containers and functions

Packages and Extends ***Knative*** *with* ***Functions*** *and is installed and managed by an* ***Operator***



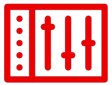
* Developer Preview

Product briefing deck

Product Manager: William Markito

Red Hat

Serverless Themes



Day 2

Powerful monitoring capabilities with configuration and automation for GitOps and modern CI/CD practices.

Integrations and Ecosystem

Eventing capabilities enabling a rich ecosystem Event Sources from Red Hat and Partner products.

Developer Experience

Intuitive developer experience through the Developer Console and CLI/IDE with Functions support.

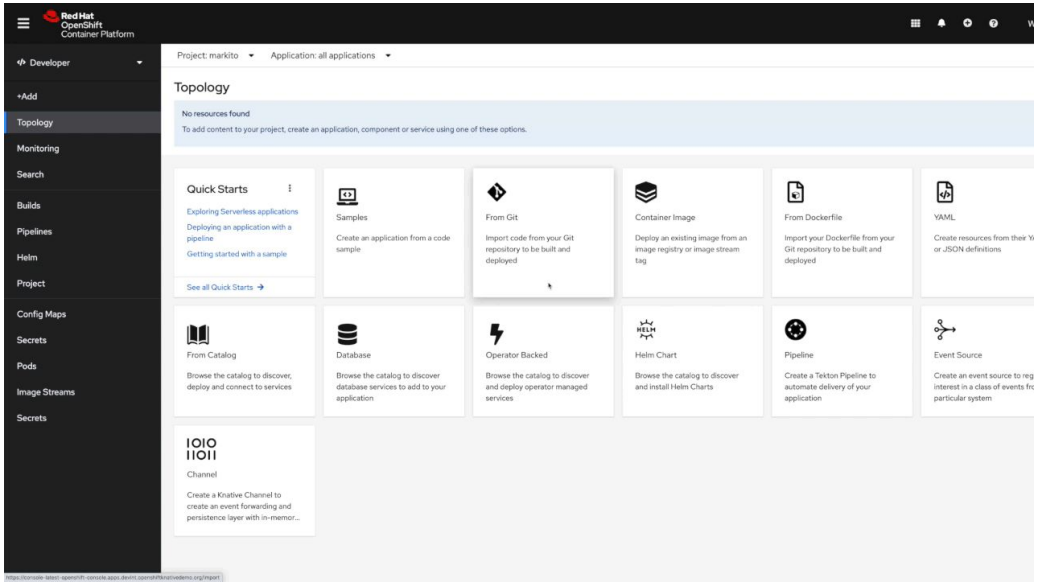
Serverless & the Portfolio

- ✓ OpenShift Service Mesh Support [doc]
  - Support for JWT Auth [doc]
  - Custom Domains for Knative Services [doc]
- ✓ OpenShift Pipelines Templates and Tasks
- ✓ CLI Commands for Eventing

Service Mesh

Serverless

Pipelines



Serverless & Pipelines Experience

Developer Preview

Coming with OpenShift Serverless 1.11

Functions

Powerful CLI experience

- ✓ Local Developer Experience
- ✓ Based on Buildpacks
- ✓ Deploy as Knative Service
- ✓ Project templates
- ✓ Support for Cloud Events/HTTP
- ✓ **Runtimes:**


```
$ kn faas help
Usage:
  faas [command]

Available Commands:
  build       Build an existing Function project as an OCI image
  completion  Generate bash/zsh completion scripts
  create      Create a new Function, including initialization of
local files and deployment
  delete      Delete a Function deployment
  deploy      Deploy an existing Function project to a cluster
  describe    Describes the Function
  help        Help about any command
  init        Initialize a new Function project
  list        Lists deployed Functions
  run         Runs the Function locally
  update      Update a deployed Function
  version     Print version.  With --verbose the build date stamp
and commit hash are included if available.
```

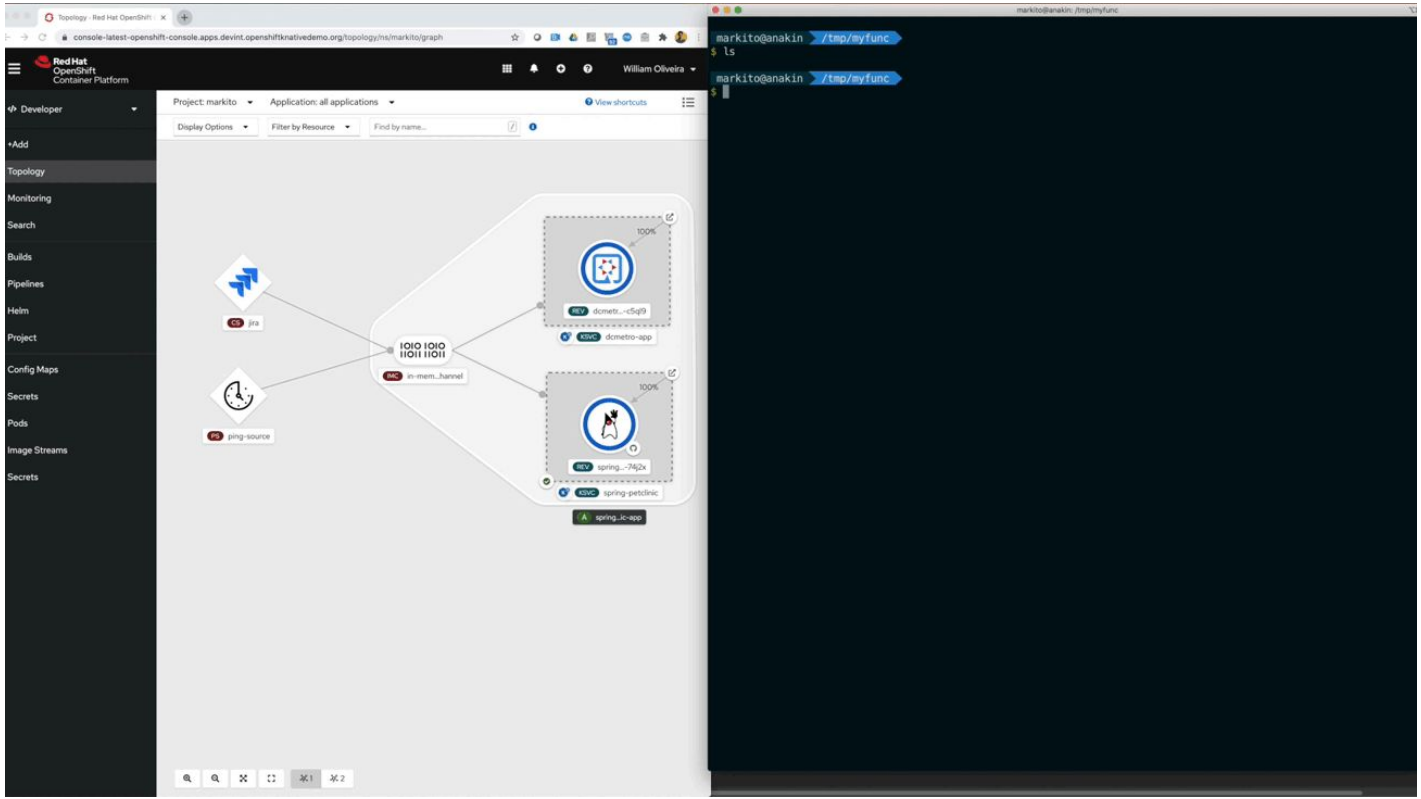

Product Manager: William Markito & Naina Singh

Red Hat

Developer Preview

Coming with OpenShift Serverless 1.11

Functions



Product Manager: William Markito & Naina Singh

Red Hat

Red Hat's OpenShift Serverless for hybrid, legacy and greenfield

FEBRUARY 21 2020

By William Fellows

Kubernetes is complex and difficult to deploy – it autoscales based on available resources, not on requests themselves. OpenShift Serverless is designed to resolve this complexity to deliver the benefits 'as advertised' of quicker time to market and faster recovery.

Read the analyst report

451 Research®

Red Hat

Product Manager: William Markito & Naina Singh

CI/CD & GitOps

OpenShift Pipelines

Tech Preview

Kubernetes-native declarative Pipelines with Tekton

Serverless CI/CD with no single server to share and maintain

Run pipelines in isolated containers with all required dependencies

Standard and portable to any Kubernetes platform

Web, CLI, and Visual Studio Code and IDE plugins

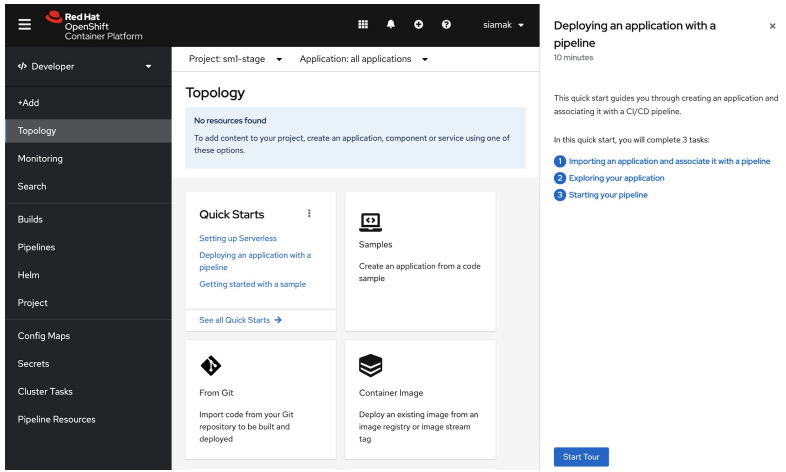
Red Hat

OpenShift Pipelines 1.2*

Tech Preview

TEKTON

- Pipeline templates for serverless when importing application (+Add)
- Pipeline templates use workspaces instead of PipelineResources
- Default workspace per PipelineRun or globally
- Expanded Task library
  - Helm tasks
  - Skopeo tasks
  - Trigger Jenkins jobs from Tekton
- Support for disconnected clusters
- Pipeline metrics in cluster monitoring
- Pipeline Quick Start tours in Dev Console
- Enhancements in Tekton CLI: workspaces, results, ...



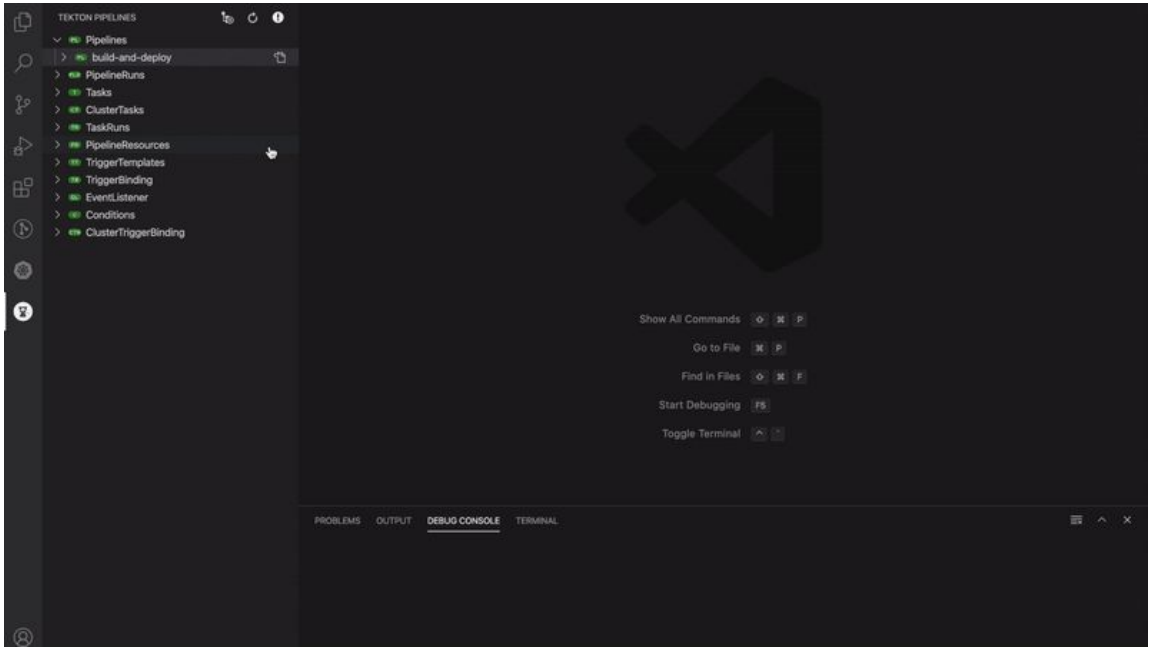
Product Manager: Siamak Sadeghianfar

* Available through the OpenShift Pipelines operator “preview” channel

Red Hat

Tekton Pipelines in IntelliJ & Visual Studio Code

- Start pipeline wizard
- Add trigger wizard
- Open Tekton docs from YAML
- Restart pipeline action



Product Manager: Siamak Sadeghianfar

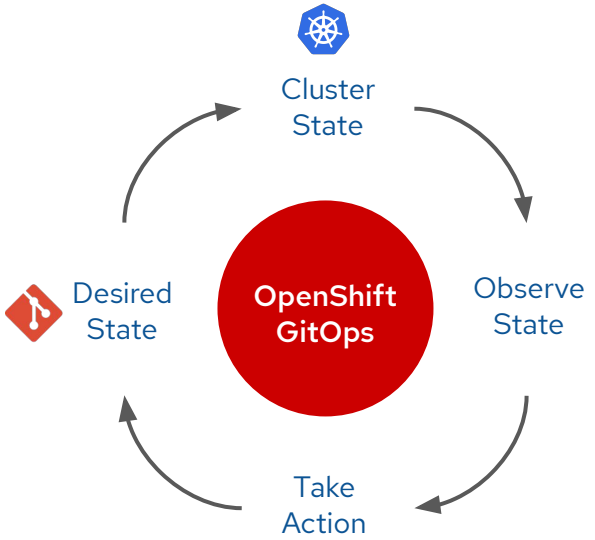
Red Hat

Tech Preview Q4CY20

OpenShift GitOps

(new add-on)

- Enable teams to adopt a declarative GitOps approach to multi-cluster configuration and continuous delivery
- OpenShift GitOps is complementary to OpenShift Pipelines and includes
  - Argo CD
  - GitOps Application Manager CLI
  - Integrated into Dev Console (App Stages)
- Included in OpenShift SKUs



Product Manager: Siamak Sadeghianfar

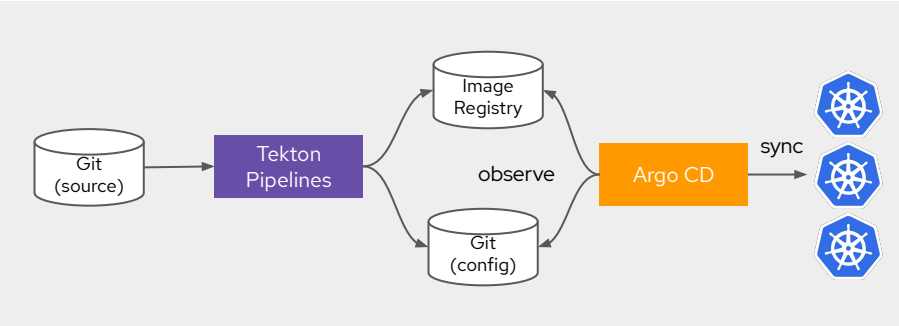
Red Hat

Dev Preview

GitOps Application Manager CLI

- Enable teams to adopt GitOps for app delivery
- Scaffolds Git repos and CI/CD for services
  - Git as the single source of truth
  - Application Stages (environments)
  - Tekton pipelines for CI
  - Argo CD for multi-cluster CD
  - Kustomize for cluster-specific configs
  - Sealed secrets
- Download GitOps Application Manager CLI
  github.com/redhat-developer/kam/releases
- Application Stages in Dev Console

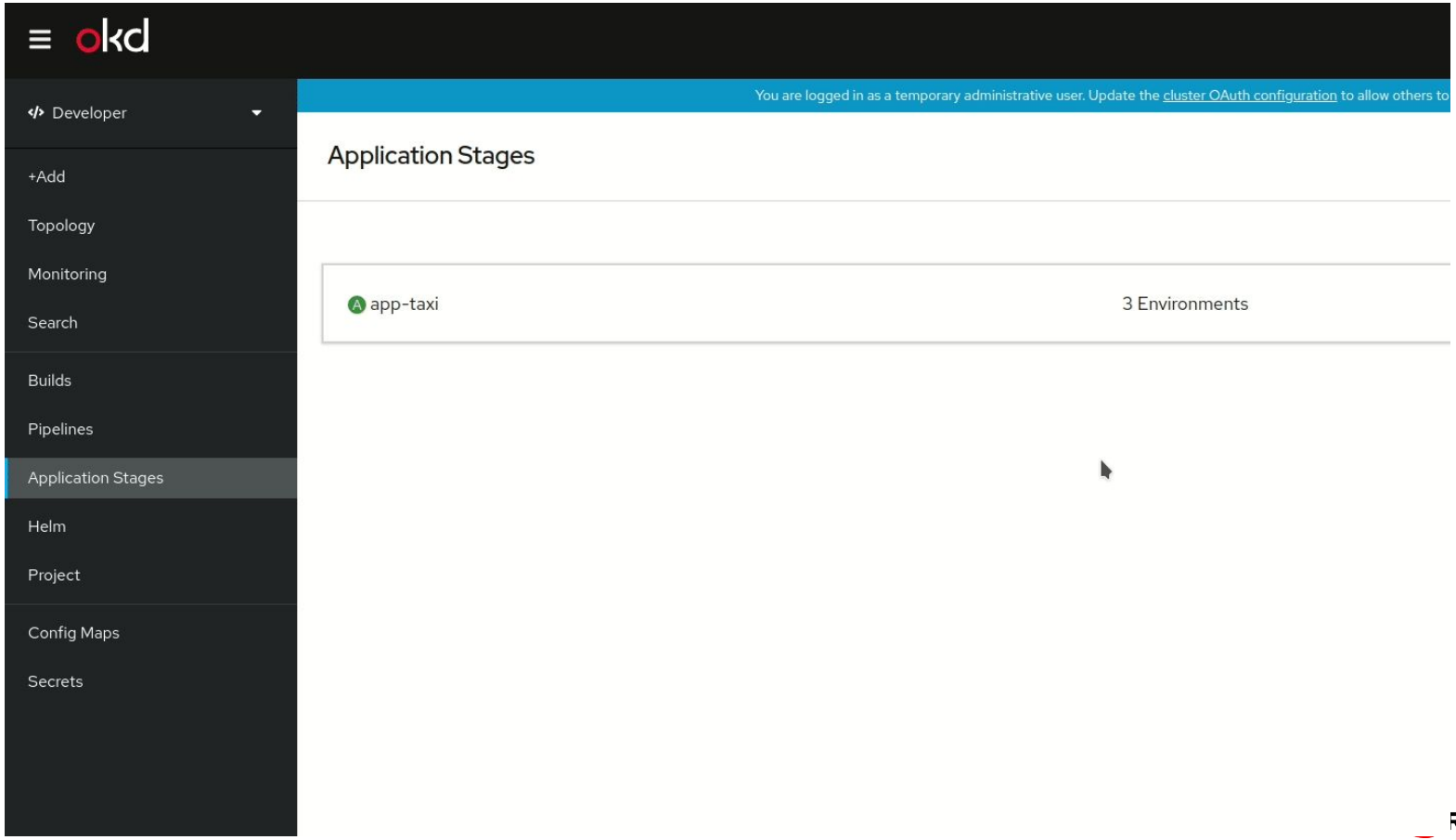
```
$ kam bootstrap
$ kam environment add
```



demo

Red Hat

Application Stages in Dev Console



A Comprehensive DevOps Platform for Hybrid Cloud

Build container images from source code using Kubernetes tools

Traditional and Kubernetes-native CI/CD

Declarative GitOps for multi-cluster continuous delivery

OpenShift Builds | **OpenShift Pipelines** | **OpenShift GitOps**

OpenShift

CodeReady / Dev Tools

Tech Preview

Service Binding Operator

- Automate configuring applications to find the coordinates of the backing service (database, mq, etc)
  - Operator services
  - Helm Charts
  - Any k8s resource
- Injects service coordinates into `Deployments`, `DeploymentConfig`, `Knative Service` and more
- Requires services to advertise injectable configuration via annotation present on k8s resources

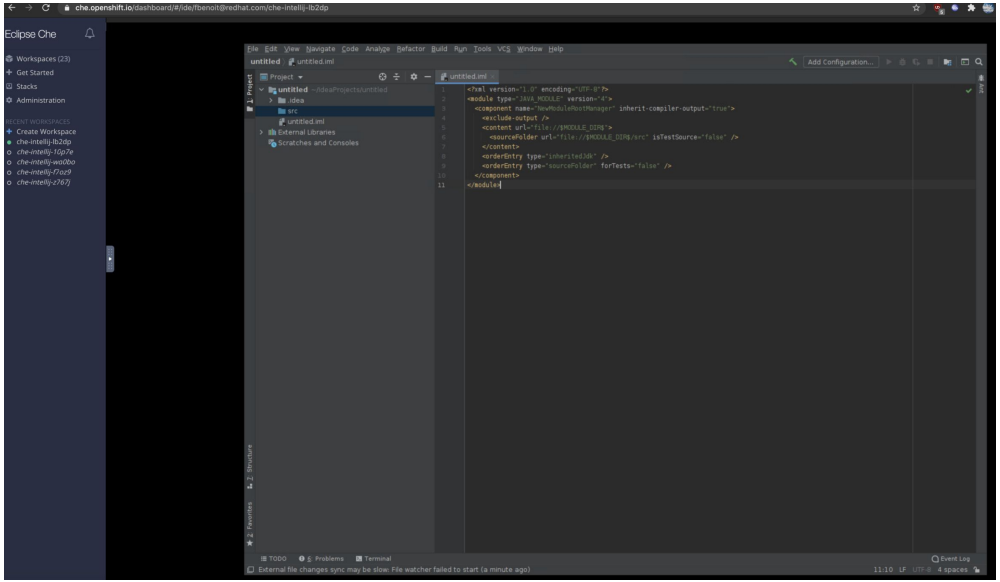

```yaml
kind: ServiceBinding
metadata:
  name: binding-request
spec:
  application:
    name: cool-app
    resource: deployments
    group: apps
    version: v1
  services:
  - group: postgresql.baiju.dev
    version: v1alpha1
    kind: Database
    name: cool-db
```


Red Hat

CodeReady Workspaces 2.5

Targeted for Nov 4

- **Support for IBM Z (v2.4)**- run on OpenShift on IBM Z
- **Single host proxy** - route ingress to all components from single host
- **Support OpenShift-trusted CA bundle (v2.4)**
- **Experimental support for IntelliJ as IDE** - community edition with steps to use customer's licensed version



Red Hat

odo 2.0 - OpenShift's Dev-Focused CLI

Released September 24th!

Core language support via a common/shared model with Eclipse Che with **devfile** stack definitions

```
$ odo catalog list components

Odo Devfile Components:
NAME                DESCRIPTION                          REGISTRY
java-maven          Upstream Maven and OpenJDK 11        DefaultDevfileRegistry
java-openliberty    Open Liberty microservice in Java    DefaultDevfileRegistry
java-quarkus        Upstream Quarkus with Java+GraalVM   DefaultDevfileRegistry
java-springboot     Spring Boot® using Java              DefaultDevfileRegistry
nodejs              Stack with NodeJS 12                 DefaultDevfileRegistry
```

Start quickly using linked samples

```
$ odo create nodejs --starter
```

Works with core Kubernetes!
- Creation of operands
- Binding of services

```
$ odo catalog list services
Operators available in the cluster
NAME                          CRDs
etcdoperator.v0.9.4           EtcdCluster, EtcdBackup, EtcdRestore

$ odo service create
etcdoperator.v0.9.4/EtcdCluster
```

Easily connect for debugging

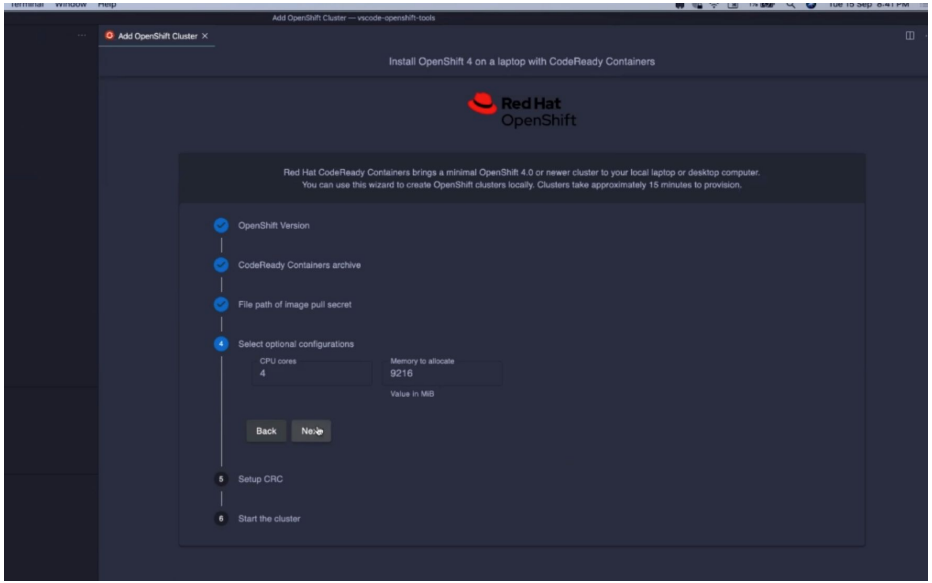
```
$ odo debug
```


Product Manager: Serena Nichols

CodeReady Containers: OpenShift on your Laptop

OCP 4.6 update - Oct 22

- Regular releases to pick up 4.5 z-streams and fresh certs
- **Resource requirements** - no changes for 4.6, worked on future improvements
- **VS Code** OpenShift Connector extended to work with starting and using CodeReady Containers

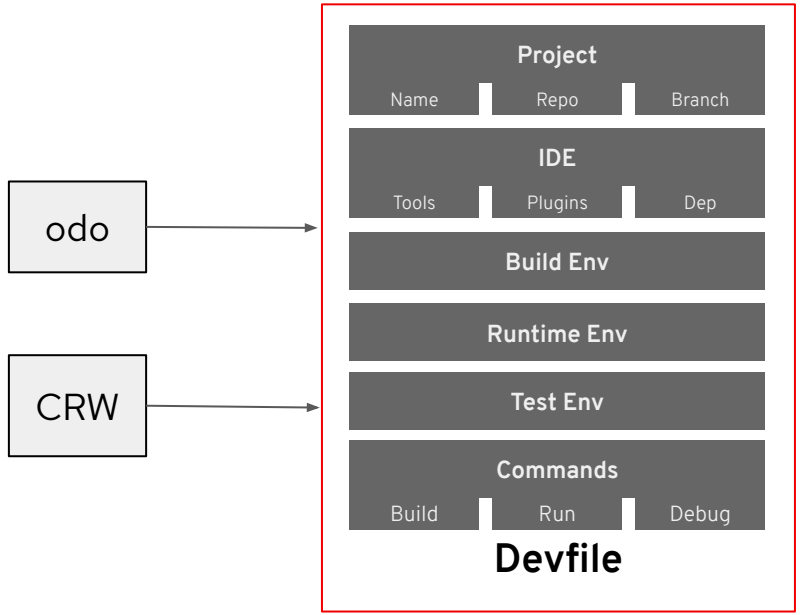


Red Hat

odo 2.0 - OpenShift's Dev-Focused CLI

Released September 24th!

- **Open runtime/platform model** - shared devfiles with CodeReady Workspaces
- **Core language support** - OpenJDK, Quarkus, NodeJS, Python
- `odo debug` graduated from TP
- Creation of operands
- Works with core Kubernetes!
- Binding of services



OpenShift Console

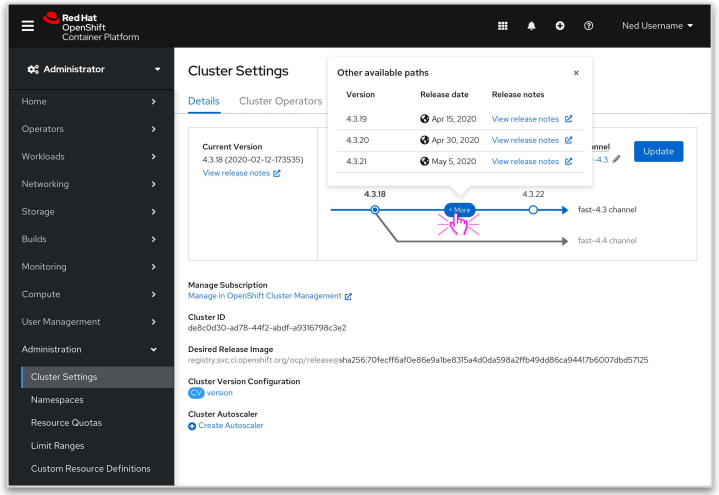
OpenShift = Kubernetes

Developing on Kubernetes | **Learning Kubernetes** | **Extending Kubernetes** | **Managing Kubernetes**

Over the air goodness!

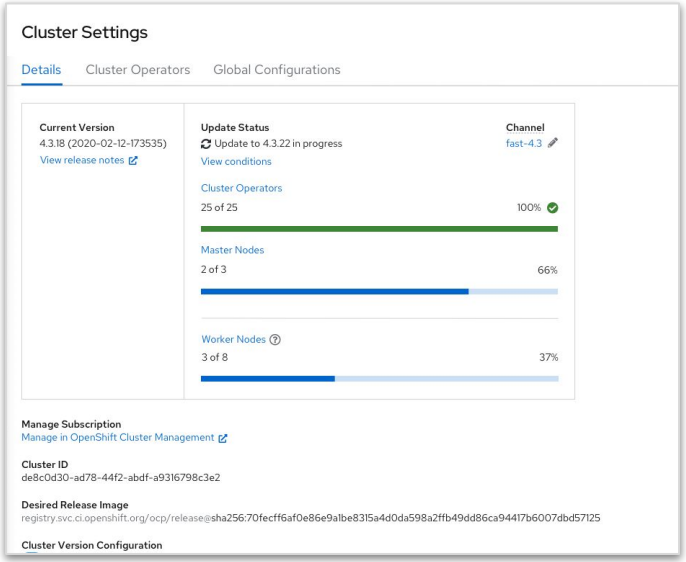
Guide users to recommended update paths and available channels.

- Make it easier to find information on channels and versions
- Provide recommended update paths



Provide transparency into the update process with an in progress checklist

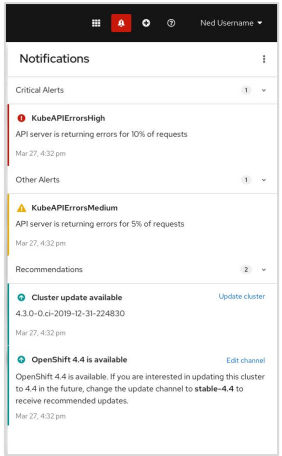
- Inform on Operator and Node Progress
- Surface conditions



Generally Available

Recommendation Alerts

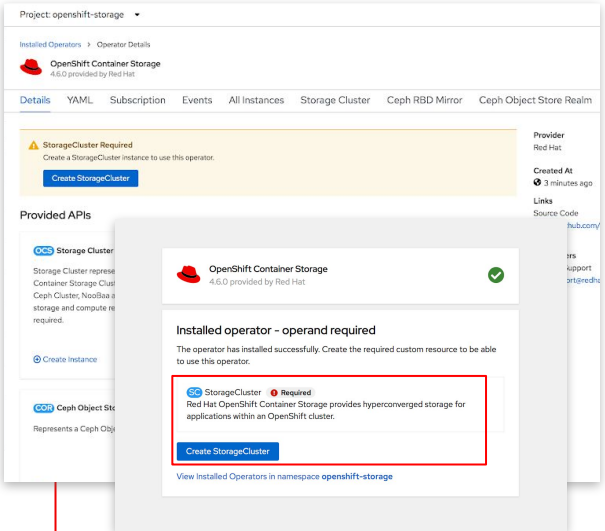
- Three new recommendation alerts were added to inform users when:
  - a new patch becomes available
  - a new minor release becomes available
  - new channels become available



Managing Operators at ease

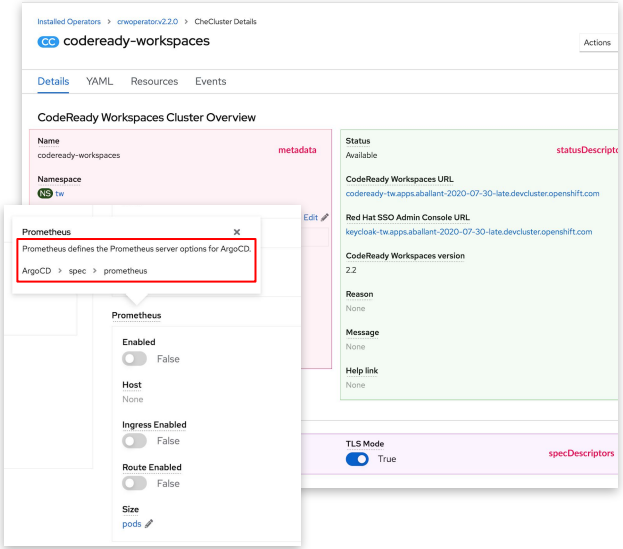
Combine an “init custom resource” creation with Operator installation flow

- Easily see the **installation status** with a new "**Installing...**" Operator screen.
- A **custom resource** contains **initialization setups** to be created during the Operator installation.



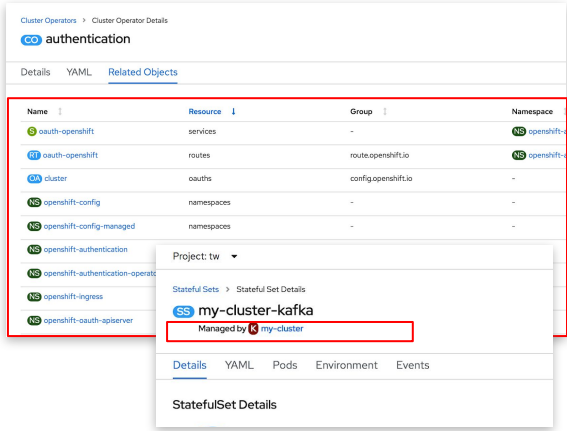
Group Operand’s properties per CRD’s schema structure

- Easily understand and see the **spec/status** properties of the CR instance.
- Easily learn **schema info** on **property’s popover** directly on this UI.



Show when a k8s resource “owned by” or “related to” an Operator / Operand

- **OLM managed Operator:** Easily see if the resource is **managed by** the Operator or an Operand instance.
- **Cluster Operator:** A list of resources **associate with** the Operator.

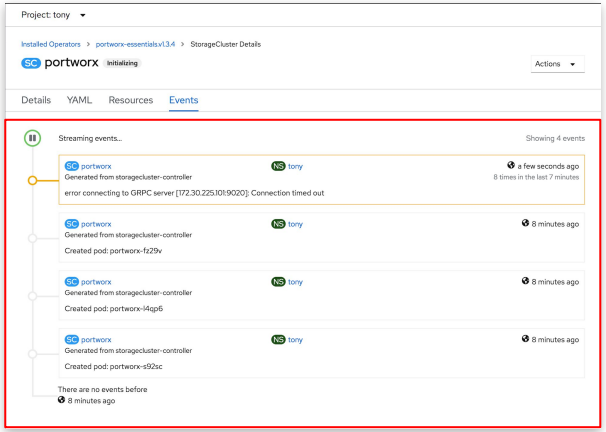


Product Manager: Ali Mobrem, Tony Wu

Managing Operators at ease

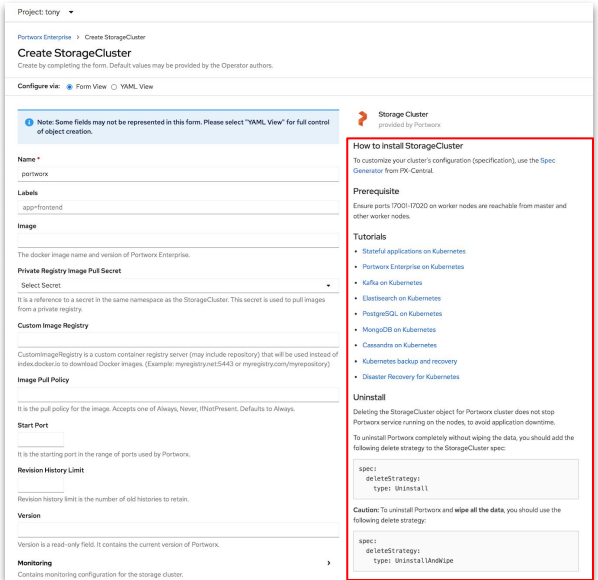
Surface Operand's Event stream on Operand's Details page

- Easier see the ***Operand's Events*** stream directly on the details page under "Operators" nav section for troubleshooting.



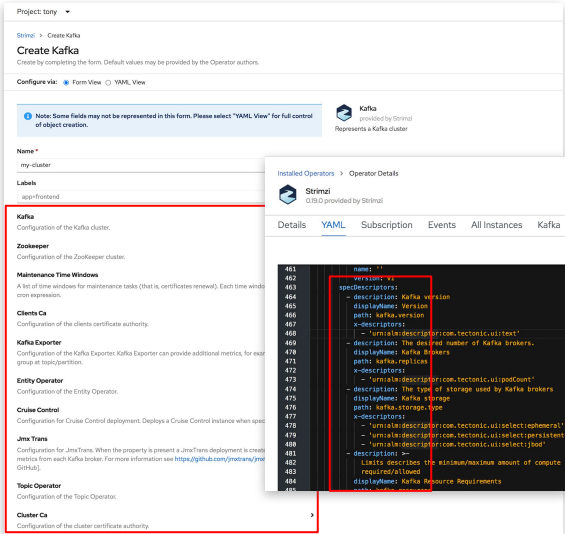
Console supports markdown for CRD description stored in Operator's CSV

- Provides ***instructions***, ***prerequisites***, or ***tutorials*** with ***external links*** to guide users how to ***create*** and ***manage*** an Operand / custom resource instance.



Customize the order of form fields with OLM descriptors in Operator's CSV

- The creation form fields are ordered by the ***specDescriptors array order*** in CSV file.
- Renders CRD ***schema description*** as the ***help text*** for each property field if no specDescriptors assigned.

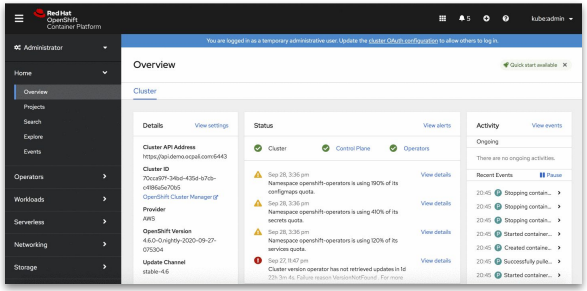


Product Manager: Ali Mobrem, Tony Wu

Getting started experience

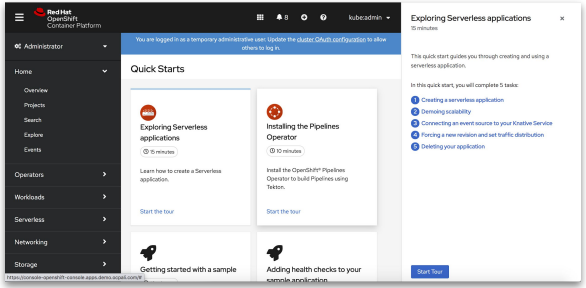
Default Perspective --and-- Guided Tour

- Non privileged users are brought to Developer perspective by default upon initial login
- A Guided Tour has been added to the Developer Perspective to help with discoverability



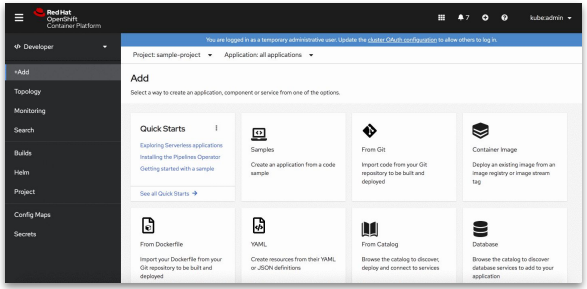
Quick Starts

- Guides customers with interactive documentation tours
- Helps customers to discover and enable value added services
- Reduces the time it takes to get customers up and running
- Educates users on how to maximize usage of the UI
- Accessible on both the Administrator and Developer perspectives



Getting started with samples

- Developer get started quickly with samples

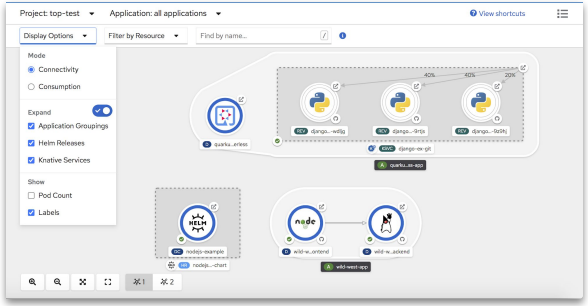


Product Manager: Ali Mobrem, Serena Nichols

Application topology

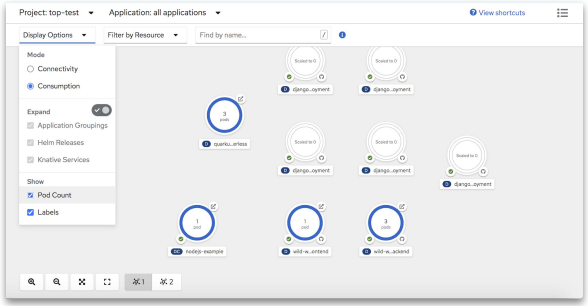
Connectivity mode

- Allows developers to focus on the composition of their application, both on how it's managed as well as how things are connected.



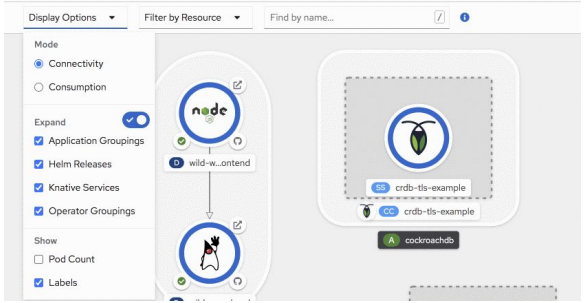
Consumption mode

- Allows developers to focus solely on components consuming resources.
- Thus, no connectors are shown (Service Binding, Visual, Traffic, Triggers, etc), nor groupings. Pod count is shown by default.

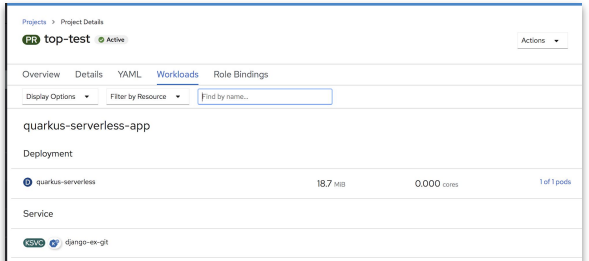


Parity between List & Graphical

- Display Options
- Filters
- Find



Admin's Project-> Workload tab has an increased feature set

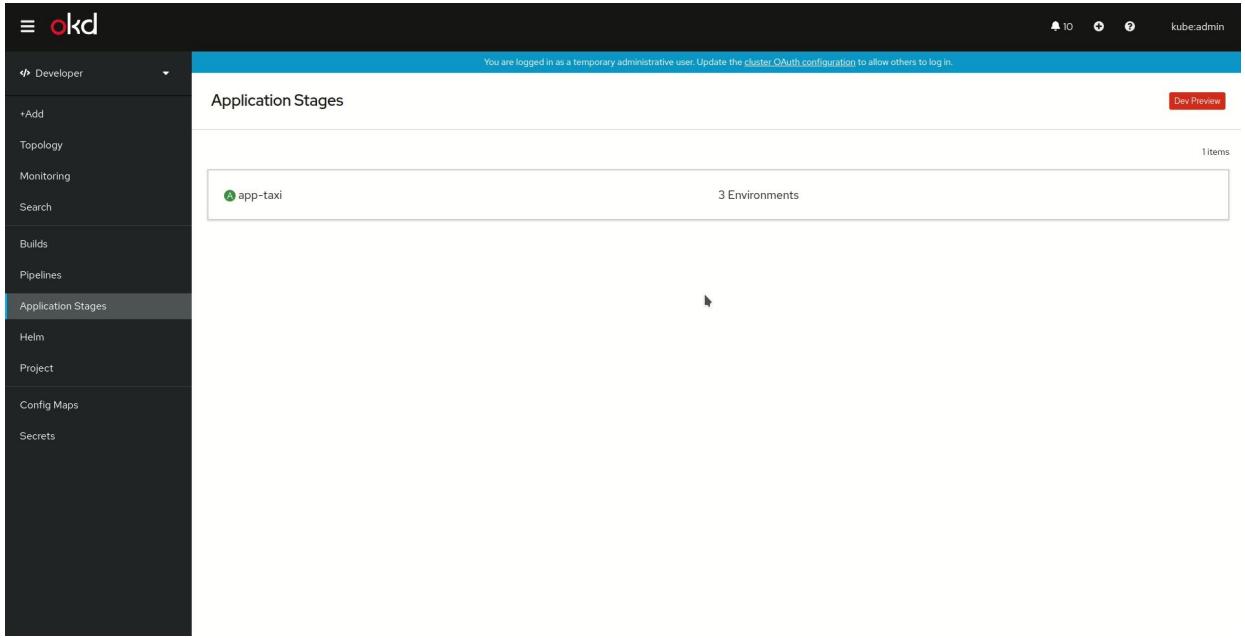


Visibility of apps across environments

Dev Preview

Empower developers with visibility of their application across all environments

- Dedicated **Application Stages** view
- View all app groupings
- Drill into app grouping details to get visibility into the composition and status of the applications/workloads deployed across environments



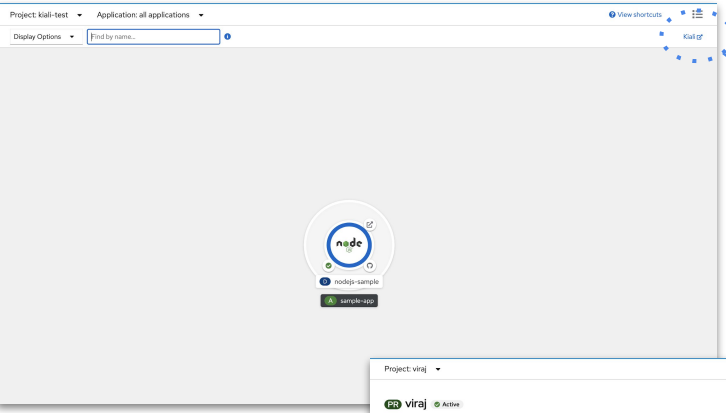
Red Hat

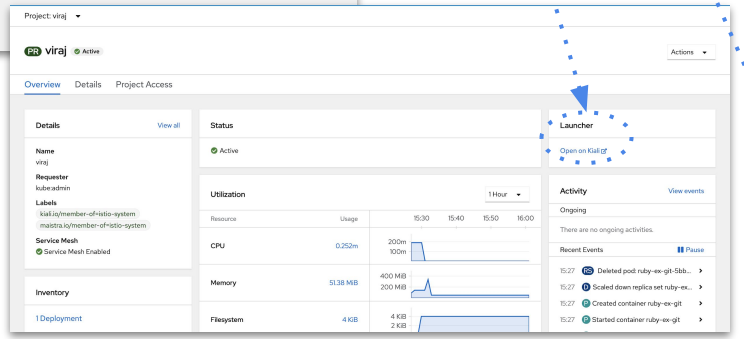
Easy access to Kiali

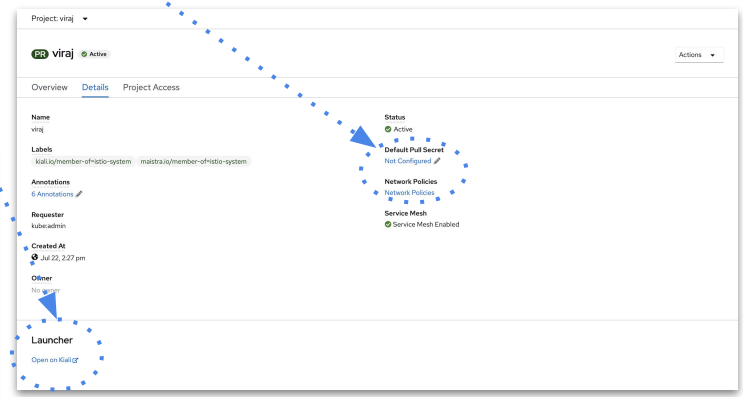
Easy access to the Kiali UI from the OpenShift Developer perspective

When OpenShift Service Mesh is enabled on the cluster:

- Developers can easily **navigate to the Kiali dashboard** from
  - Topology view
  - Project Overview
  - Project Details page
- Developers can easily see if **Service mesh is enabled** for the project in context







Observability

“Tune” Fluentd

Expose selected Fluentd performance optimization parameters in the ClusterLogging API.

- Not relevant to most users, default settings should give good general performance.
- Ultimately we want great performance "out of the box" with no user intervention. However, today we can't always predict/detect the best settings; customers have had to adjust fluentd parameters to get good performance.
- All possible settings relate to optimizing the forwarding process, meaning when logs leave Fluentd to either our internal storage or a configured 3rd party system.
- Settings include retries, memory usage and the flushing output behaviour.

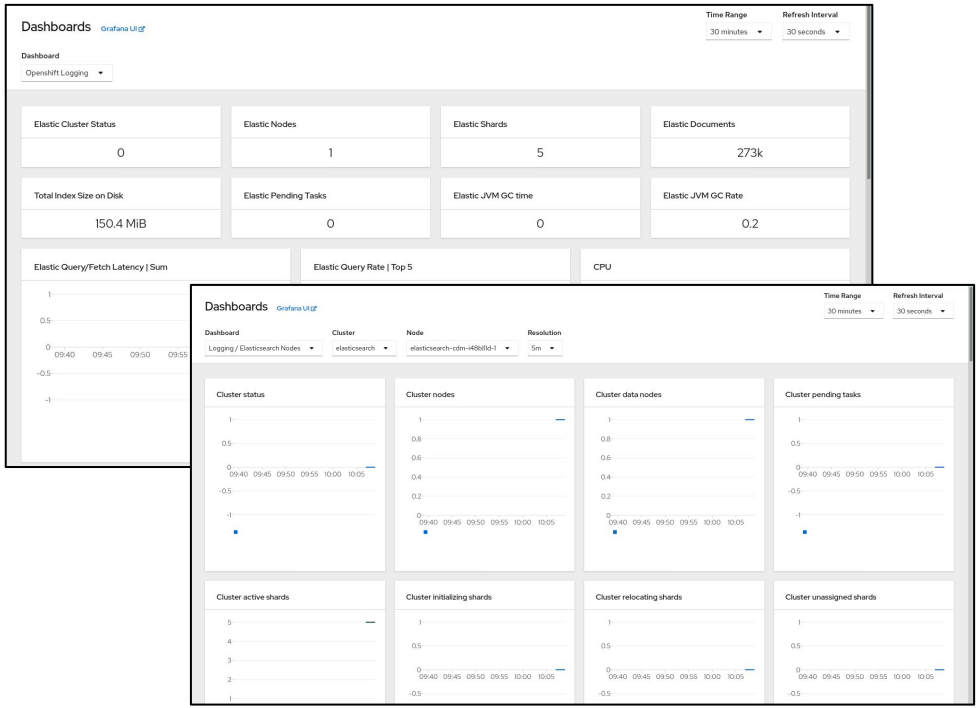
1. After installing OpenShift Logging, apply the following YAML.

```
apiVersion: logging.openshift.io/v1
kind: ClusterLogging
metadata:
  name: instance
  namespace: openshift-logging
spec:
  forwarder:
    fluentd:
      buffer:
        chunkLimitSize: 8m
        flushInterval: 5s
        flushMode: interval
        flushThreadCount: 3
        overflowAction: throw_exception
        retryMaxInterval: "300s"
        retryType: periodic
        retryWait: 1s
        totalLimitSize: 32m
```

Logging “Observability”

Improve our current Monitoring capabilities to better help admins to gain insights into OpenShift Logging.

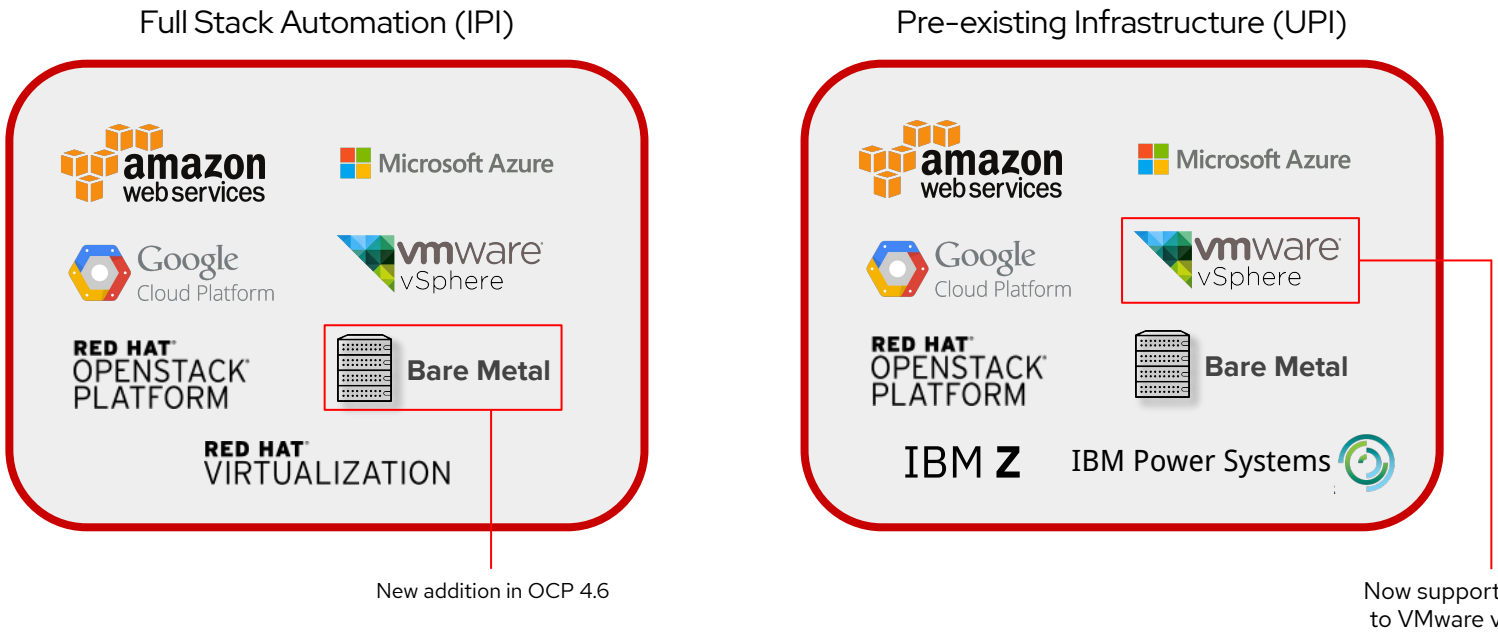
- Introduce dashboards into the OpenShift Console (admin perspective) that shows the most critical data points for admins to proactively research problems.
  - Two new dashboards: OpenShift Logging (central overview look) and Elasticsearch.
  - Access from *Monitoring -> Dashboards* and select either from the dropdown list.
- Enrich and/or improve current alerting rules to cover "you must page me at 3am" scenarios.
- Overhaul metrics where necessary.
  - **Note:** Removed all index level metrics since they introduced an abnormal amount of metrics which ended up exploding our Monitoring solution. We will reintroduce some + improvements in a future release.



Red Hat

Install & Upgrades

4.6 Supported Providers



Generally Available

Product Manager(s): Katherine Dubé (AWS, Azure, GCP), Maria Bracho (VMware), Peter Lauterbach (RHV & OCP Virtualization), Ramon Acedo Rodriguez (OSP, BM), & Duncan Hardie (IBM Z & Power)

OpenShift on OpenStack

Supported OSP releases with OCP 4.6

Red Hat OpenStack Platform 13
Red Hat OpenStack Platform 16.1

New with OCP 4.6 on OSP

- OpenStack Bare Metal (Ironic) integration
- Installer support for specifying OpenStack Availability Zones
- Floating IPs no longer required

Product Manager: Ramon Acedo Rodriguez

Enhancements to RHV full stack installer

What's new in OCP 4.6

- Dynamically provision storage to OCP cluster with RHV CSI operator
- Improved control of workloads and resources by auto-scaling workers nodes
- Support for Disconnected / restricted installs
- OCP on RHV User Provisioned Infrastructure

Supported RHV releases with OCP 4.6

- RHV 4.4.2+
- Customers running OCP 4.5 on RHV 4.3 must upgrade to RHV 4.4.2+ **before** upgrading to OCP 4.6

```
$ ./openshift-install create cluster --dir ./demo
? SSH Public Key /home/user_id/.ssh/id_rsa.pub
? Platform ovirt
? Enter oVirt's api endpoint URL admin:pw123
https://rhv-env.virtlab.example.com/ovirt-engine/api
? Is the installed oVirt certificate trusted? Yes
? Enter oVirt's CA bundle xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
? Enter ovirt-engine username admin@internal
? Enter passsword xxxxxxxxxxxx
? Select oVirt cluster Default
? Select oVirt storage domain hosted_storage
? Select oVirt network ovirtmgmt
? Enter the internal API virtual IP 10.35.1.19
? Enter the internal DNS virtual IP 10.35.1.21
? Enter the ingress IP 10.35.1.20
? Base Domain example.com
? Cluster Name demo
? Pull Secret [? for help] xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
INFO Creating infrastructure resources...
INFO API v1.17.1 up
INFO Install complete!
INFO Access the OpenShift web-console here:
https://console-openshift-console.apps.demo.example.com
INFO Login to the console with user: kubeadmin, password: xxxxx-xxxxx-xxxxx-xxxxx
```

		Name	Host	Cluster	Memory	CPU	Network	Status	Uptime
▲ !		orv-67prb-master-0	rhv01.work.lan	Cluster2	48%	20%	0%	Up	29 min
▲ !		orv-67prb-master-1	rhv02.work.lan	Cluster2	49%	22%	0%	Up	29 min
▲ !		orv-67prb-master-2	rhv01.work.lan	Cluster2	62%	22%	0%	Up	29 min
▲ !		orv-67prb-worker-0-5fw4w	rhv01.work.lan	Cluster2	12%	8%	0%	Up	18 min
▲ !		orv-67prb-worker-0-fq7vt	rhv02.work.lan	Cluster2	15%	9%	0%	Up	17 min
▲ !		orv-67prb-worker-0-pn5vp	rhv02.work.lan	Cluster2	16%	10%	0%	Up	19 min

Generally Available

Red Hat

New Credential Modes for OpenShift Installation

Specify how *CredentialsRequests* are satisfied

- Allows users to define how *CredentialsRequest* are handled on behalf of OpenShift components requiring cloud API access.
- Three new modes can now be specified for deployments on AWS, Azure, and GCP:
  - **Mint:** Creates new credentials with a subset of the overall permissions as specified by the *CredentialsRequest*.
  - **Passthrough:** Uses the provided credentials "as is" for each OpenShift component's *CredentialsRequest*.
  - **Manual:** *CredentialsRequests* must be manually handled by the user (*useful for cases where access to the IAM endpoint has been restricted.)*
- If the field is set to any of the above values, then the installer will not attempt to check the credential permissions prior to installing OpenShift.
  - Important for situations where the credential policy checking can't adequately validate the user credentials *(when using SCP on AWS.)*

```
% ./openshift-install explain installconfig.credentialsMode
KIND:     InstallConfig
VERSION:  v1

RESOURCE: <string>
  CredentialsMode is used to explicitly set the mode with which CredentialRequests are
satisfied.
 If this field is set, then the installer will not attempt to query the cloud
permissions before attempting installation. If the field is not set or empty, then the
installer will perform its normal verification that the credentials provided are
sufficient to perform an installation.
 There are three possible values for this field, but the valid values are dependent upon
the platform being used. "Mint": create new credentials with a subset of the overall
permissions for each CredentialsRequest "Passthrough": copy the credentials with all of
the overall permissions for each CredentialsRequest "Manual": CredentialsRequests must
be handled manually by the user
 For each of the following platforms, the field can set to the specified values. For all
other platforms, the field must not be set.
```


Generally Available

Red Hat

Product Manager: Maria Bracho / Katherine Dubé

AWS Custom Endpoint Support

Define custom API endpoints for private AWS regions

- Adds a new field 'serviceEndpoints' in install-config.yaml, which contains a list of custom endpoints for overriding the default service endpoints of AWS services.
- Custom API endpoints can be specified for EC2, S3, IAM, Elastic Load Balancing, Tagging, Route 53, and STS AWS services.
- Only required for cases were alternative AWS endpoints (like FIPS) need to be used.
  - *Note: Not needed for deploying to known regions (which are found in the AWS SDK.)*
- List of AWS service endpoints can be found here: https://docs.aws.amazon.com/general/latest/gr/aws-service-information.html

```
apiVersion: v1
baseDomain: example.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  Platform: {}
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform: {}
  replicas: 3
metadata:
  creationTimestamp: null
  name: mycluster
networking:
  clusterNetwork:
  - cidr: 10.18.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OpenShiftSDN
  serviceNetwork:
  - 172.30.0.0/16
platform:
  aws:
    Region: us-east-2
    amiID: ami-0f4ecf819275850dd
    serviceEndpoints:
    - service: ec2
      url: https://ec2-fips.us-east-2.amazonaws.com
    - service: s3
      url: https://<account-id>.s3-control.us-east-2.amazonaws.com
publish: External
```

Generally Available

Product Manager: Katherine Dubé

User Defined Routing on Azure

Microsoft Azure

Define custom API endpoints for private Azure regions

- Today, internal clusters on Azure always use Public Standard Load Balancers for Internet egress. This means public IPs and public load balancers are required, which many customers don't want to use for internal clusters.
- User Defined Routing allows the users to choose their own outbound routing for Internet access enabling them to leverage pre-existing setups instead of defaulting to the per-cluster OpenShift recommended way.
- Users are only allowed to change the outbound type when using pre-existing networking since outbound routing needs to be setup by user prior to installing the cluster.
- Adds a new egress strategy 'UserDefinedRouting' to the 'outboundType' field in the install-config

```
apiVersion: v1
baseDomain: example.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform: {}
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform: {}
  replicas: 3
metadata:
  creationTimestamp: null
  name: mycluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
          hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OpenShiftSDN
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
          baseDomainResourceGroupName: os4-common
          cloudName: AzurePublicCloud
          outboundType: UserDefinedRouting
          region: eastus
publish: External
pullSecret: <secret>
```


Generally Available

Red Hat

Product Manager: Katherine Dubé

Specify Disk Type & Size for Control Plane & Compute Nodes on Azure & GCP

Microsoft Azure Google Cloud Platform

Configure both disk type and size based on node requirements

- Support for configuring disk type and size on control plane and compute nodes has been extended to Azure & GCP.
- Introduces two new fields 'osDisk.diskSizeGB' & 'osDisk.diskType' in the install-config
- For Azure, supported disk types include: "Standard_LRS","Premium_LRS", & "StandardSSD_LRS"
  - *Note: For control plane nodes only "Premium_LRS" & "StandardSSD_LR" can be configured.*
- For GCP, supported disk types include: "pd-ssd" & "pd-standard"
  - *Note: For control plane nodes only "pd-ssd" can be configured.*

```
apiVersion: v1
baseDomain: example.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
  - osDisk:
          DiskSizeGB: 120
          DiskType: pd-standard
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
  - osDisk:
          DiskSizeGB: 120
          DiskType: pd-ssd
  replicas: 3
metadata:
  creationTimestamp: null
  name: mycluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
         hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OpenShiftSDN
  serviceNetwork:
  - 172.30.0.0/16
platform:
  gcp:
    projectID: openshift-production
    region: us-central1
publish: External
```


Generally Available

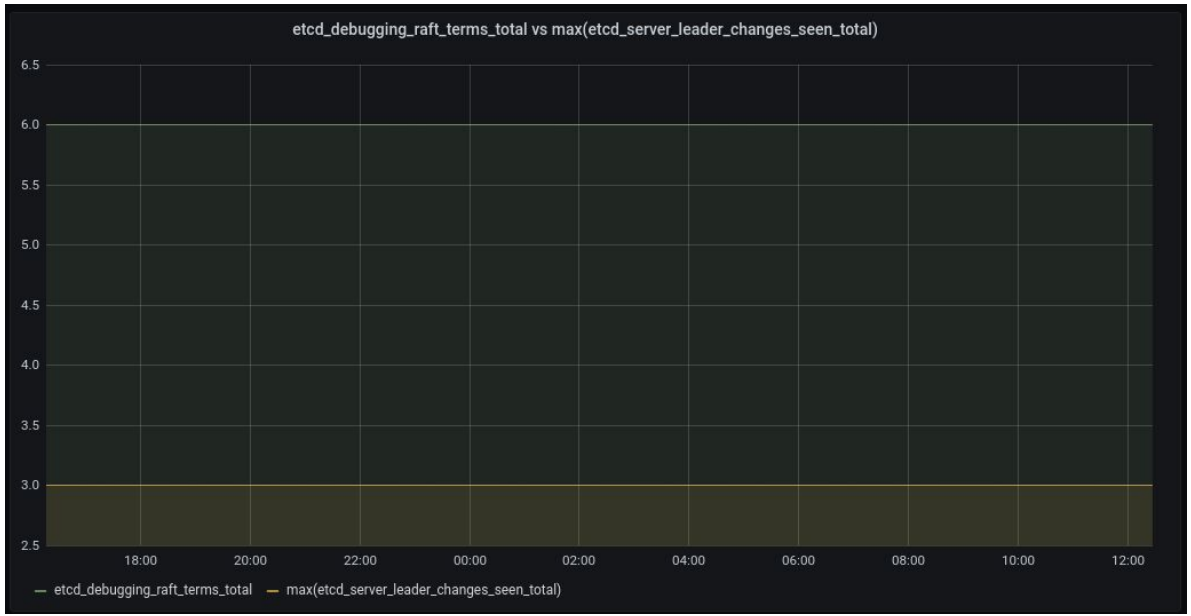
Red Hat

Product Manager: Katherine Dubé

Control Plane

etcd Improvements

- Support for etcd's golang pprof endpoint by default. This will allow for easier profiling of etcd resource utilization.
- Use `ionice -c2 -n0` for etcd process which improves I/O priority scheduling.
- New metric `etcd_debugging_raft_terms_total` this metric is used to expose actual raft terms through Prometheus metrics. This experimental metric can assist in triage of etcd performance issues.



Product Manager: Anand Chandramohan

Improved Recovery Time After Hard Shutdown of Master Node

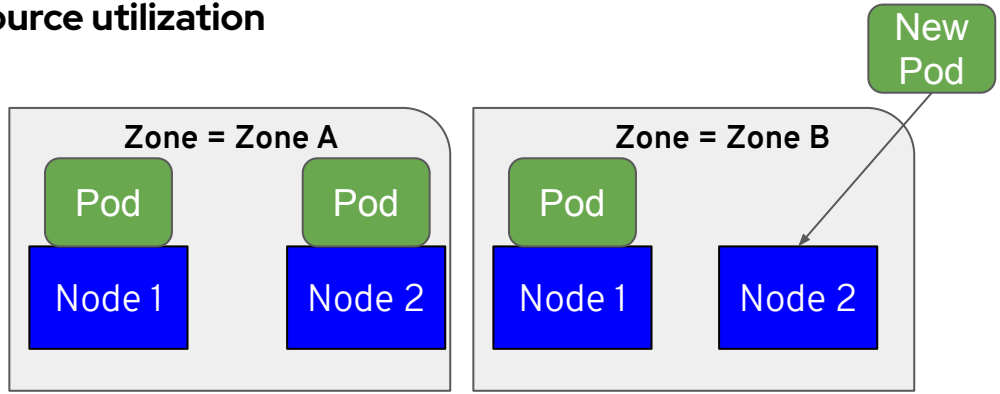
After a hard shutdown of a master node, the result of a failure or not, the OpenShift APIs would become unavailable for a lengthy period of time (15min+) while the endpoints were reconciled and the cluster detected and adapted to the loss of the node.

For OpenShift 4.6, the recovery time of the control plane was dramatically improved, in most cases, to ~90s.

Pod Topology Spread Constraints

Control how **Pods are spread** across the cluster among **failure-domains** such as regions, zones, nodes, and other user-defined topology domains.

Help to achieve **high availability** as well as **efficient resource utilization**




```
kind: Pod
apiVersion: v1
metadata:
  name: mypod
  labels:
    foo: bar
spec:
  topologySpreadConstraints:
  - maxSkew: 1
    topologyKey: zone
    whenUnsatisfiable: DoNotSchedule
    labelSelector:
      matchLabels:
        foo: bar
```

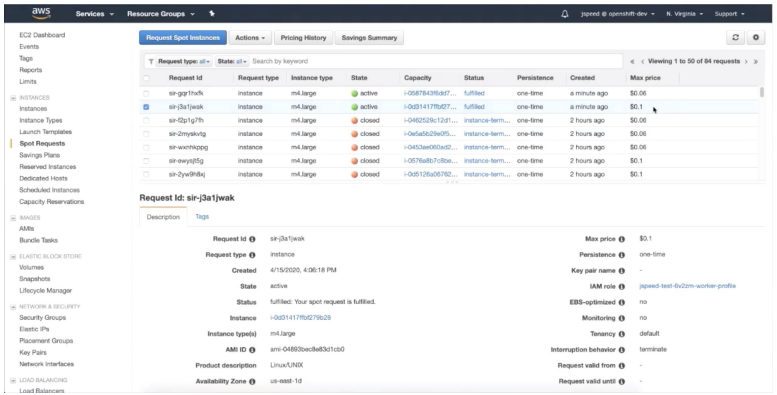

Product Manager: Tushar Katarki

Cluster Infrastructure updates

- Expanding Spot Instance support
  - Azure: machine API support for spot instances
  - GCP: machine API support for Preemptible VM instances
- Security and Compliance
  - AWS: Support for custom endpoints and air-gapped regions
  - Azure: Support for GovCloud
- Usability
  - AWS Machine API Support of more than one block device
  - Get validation/defaulting for providerSpec APIs

MachineSet

```
apiVersion: machine.openshift.io/v1beta1
spec:
  metadata:
    creationTimestamp: null
  providerSpec:
     spotMarketOptions:
      maxPrice: "0.06"
```



Generally Available

Product Manager: Duncan Hardie

RHEL CoreOS

Red Hat Enterprise Linux CoreOS

RHCOS 4.6 EUS

- Aligned for full life cycle with RHEL 8.2.z EUS stream
- Stable 4.18 kernel ABI allowlist
- Deploy /var on a separate disk
- Extension system with usbguard

Product Manager: Mark Russell

Updated CoreOS Image & Installer

Key Features

- Hardware and interface name discovery
- Preserve existing data partitions option
- Automatic 4K-sector drive detection
- Easily embed custom ignition configuration into custom ISOs for installation in environments with restricted networking
- Live PXE and Live ISO environment

```
Red Hat Enterprise Linux CoreOS 46.82.20200928174-0 (Ootpa) 4.6
SSH host key: SHA256:mmPpxnYfcrXsMng0c72dEm6GqoM5Bx/eOP3bm1DsuV4 (ECDSA)
SSH host key: SHA256:Nb30rUtSbanzeLyT4quS1tnH1116aFFZGZrmNWJMidQ (ED25519)
SSH host key: SHA256:u1wL1agK+UIGNLn5iBU8+bHBryk3QWGgNpZ8KfofZFa (RSA)
enp1s0: 192.168.122.51 fw80::5054::ff:fe6a:add7
enp6s0: 192.168.122.145 fe80::5054::ff:fe78:befe
localhost login: core (automatic login)

################################################################################
Welcome to the CoreOS live environment. This system is running completely
from memory, making it a good candidate for hardware discovery and
installing persistently to disk. Here is an example of running an install
to disk via coreos-installer:

sudo coreos-installer install /dev/sda \
    -- ignition-url https://example.com/example.ign

You may configure networking via 'sudo nmcli' or 'sudo nmtui' and have
that configuration persist into the installed system by passing the
'--copy-network' argument to 'coreos-installer install'. Please run
'coreos-installer install --help' for more information on the possible
install options.
################################################################################

[core@localhost ~]$
```

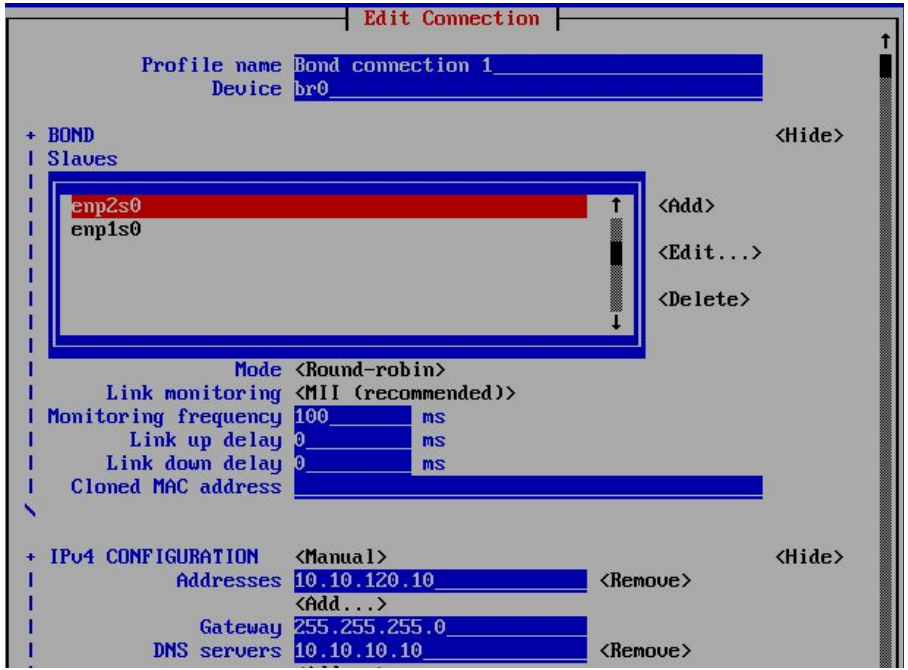
Improved Networking UX

For Bare Metal

- Use `nmtui` or `nmcli` from the Live Installer environment
- Pass your live config by invoking the RHCOS installer with the `--copy-network` argument

For VMware

- The new RHCOS VMware OVA file accepts static networking in the guestinfo fields
- Pass dracut `ip=` syntax to configure static networking through the vSphere web console or API



Networking and Routing

SR-IOV Enhancements

Infiniband Support

- High-throughput low-latency communication standard for high-perf internode message passing
- Configured via SR-IOV Operator and is enabled on Mellanox CX-4/5/6 cards

IPAM Plug-in: whereabouts

- A CNI plug-in providing IPAM for other (Multus) CNI plugins, e.g. DHCP
- Assigns IP addresses dynamically across the cluster, and without DHCP, and allows overlapping IP ranges
- Stores IP address allocations via Kubernetes API

```
{
  "ipam": {
    "type": "whereabouts",
    "range": "<range>",
    "exclude": ["<exclude_part>, ..."],
  }
}
```

Infiniband Configuration Overview

1. Install SR-IOV operator
2. Create a SriovNetworkNodePolicy CR

```
apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: policy-ib-net-1
  namespace: openshift-sriov-network-operator
spec:
  resourceName: ibnic1
  nodeSelector:
    feature.node.kubernetes.io/network-sriov.capable:
"true"
  numVfs: 4
  nicSelector:
    vendor: "15b3"
    deviceID: "101b"
    rootDevices: ['0000:19:00.0']
  linkType: ib
  isRdma: true
```

3. Create an SR-IOV network
4. Create a pod with the Infiniband device and network

Additional Networking Enhancements

Switch to System OVS

- OVS previously ran in a cluster pod, resulting in existing network flow disruption upon cluster upgrades/restarts
- OVS now runs on the RHCOS host, and remains active during cluster upgrades/restarts
- Requires node reboot to update the OVS version

Extended serviceNodePortRange (UPI only)

Allows expansion of the default service node port range (30000-32767) for services of type NodePort for customers that implement a large number of node ports, if the corresponding ports are opened at the infrastructure layer..

```
oc patch network cluster -p '{"spec":{"serviceNodePortRange": "30000-33000"}}' --type=merge
```

Increased Maximum Number of Rules per EgressFirewall Policy

The number of rules in a single EgressFirewall policy was insufficient for some deployments, and was raised from a maximum of 50 to 1000.

HAPROXY Configuration Enhancements

HTTP `Forwarded` Header Policy

Use Case: A developer that configures an application-specific proxy that injects X-Forwarded-For and wants an IngressController to pass the header through unmodified for the application's Route.

Ingress TLS Termination Policy

Ingresses can now specify reencrypt or passthrough policy:

- "reencrypt" decrypts and re-encrypts HTTP traffic when forwarding it.
- "passthrough" passes traffic through without terminating TLS.

HTTP Cookie Capture

Configure OpenShift to log specific, named HTTP cookies, to ensure security compliance and enable business analytics.

HTTP Header Capture

Configure OpenShift to log specific HTTP request and response headers for Routes, to ensure security compliance and increase observability.

HTTP Unique-Id Header

Configure an IngressController to inject an HTTP header with a unique request id into each HTTP request before forwarding the request to the application, so that I can trace HTTP requests and increase observability.

HTTP Path Rewriting

Support for a Route annotation to configure path rewriting. On incoming requests, the Route's spec.path is replaced with the rewrite target before forwarding.

Configure IngressController to Use AWS NLB

By default, an IngressController resource will use an AWS Classic Load Balancer when the endpoint publishing strategy is "`type: LoadBalancerService`" and the Infrastructure resource platform status is "`type: AWS`".

Simply by specifying the AWS provider parameter "`type: NLB`" the IngressController resource will instead use an AWS Network Load Balancer (NLB).

```
apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  name: $MY_INGRESS_CONTROLLER
  namespace: openshift-ingress-operator
spec:
  replicas: 1
  domain: $MY_UNIQUE_INGRESS_DOMAIN
  endpointPublishingStrategy:
    type: LoadBalancerService
    loadBalancer:
      scope: External
      providerParameters:
        type: AWS
        aws:
          type: NLB
```

Storage

Storage updates

- No change on support for intree drivers
- CSI Operators
  - CSI Operator Library
  - Move to CSO managing CSI Operators
  - Indicate support of fsGroup
- CSI Capabilities
  - Crash Consistent Snapshots (Tech preview)
    - Fully supported when used with OCS or OpenShift Virtualization
- Enabling OCS via Local Storage Operator
  - Auto-provision of PVs
  - Continuous inventory of local disks

OCP Supported	
AWS EBS	Fibre Channel
Azure File & Disk	HostPath
GCE PD	Local Volume
VMware vSphere Disk	Raw Block
NFS	iSCSI
Supported via OCS	
File , Block, Raw Block, Object	
Supported via OSP	
Cinder	

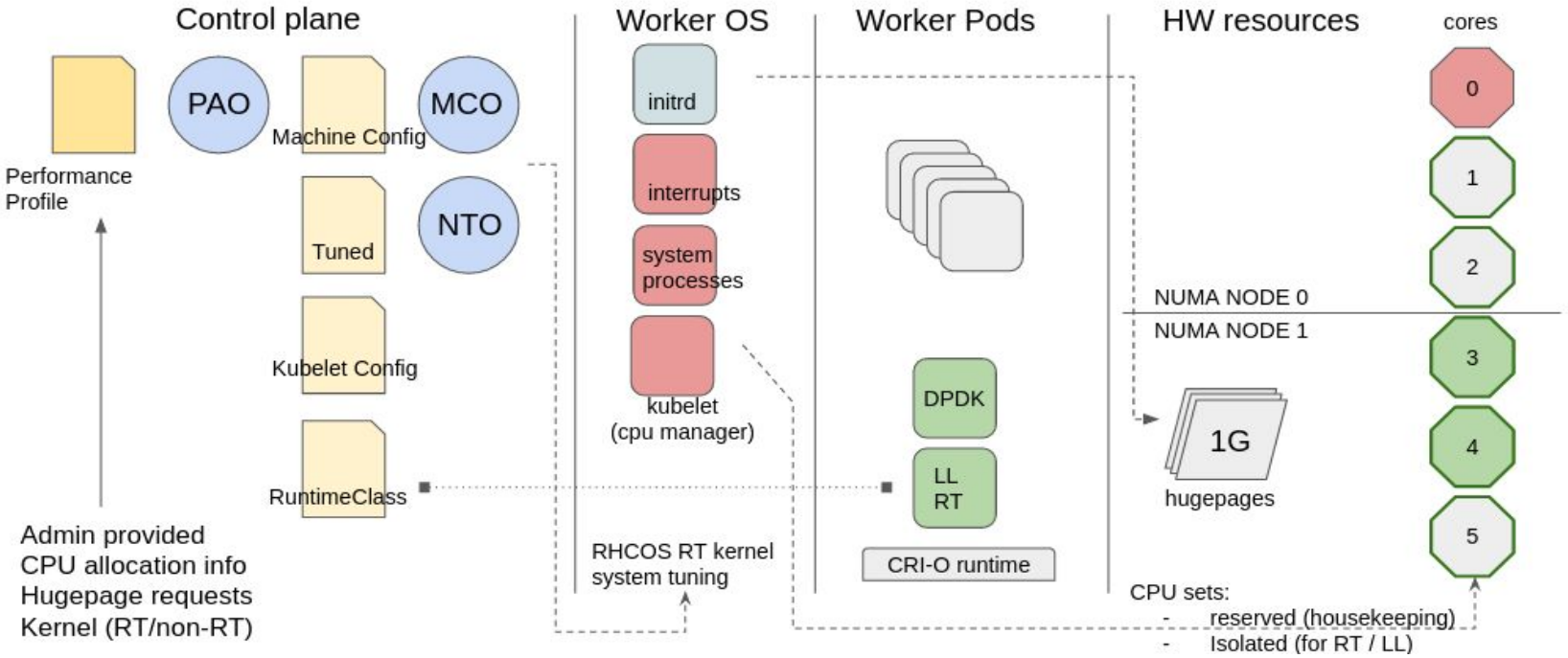
OpenShift Container Storage updates

- Encryption support for the entire cluster
- Crash Consistent Snapshots, Clones
- Compression and Replica 2 for block storage
- Object namespaces - single view for multiple object storage buckets.
- Improved bare metal deployment with LSO
  - Auto-provision of PVs
  - Continuous inventory of local disks
  - Easy local drive filtering
- Additional platforms - IBM Z/Power (by IBM)

Out of the box support	
Block, File, Object	
Platforms	
AWS	Azure (Tech Preview)
Bare metal	Google Cloud (Tech Preview)
VMWare	Azure (Tech Preview)
IBM Z/Power (by IBM)	Oct 2020 - RHV (Tech Preview) Nov 2020 - OSP (Tech Preview)
Deployment modes	
Disconnected environment and Proxied environments	

Telco/Edge

Real Time and Low Latency Workloads (for RAN) with the Performance Addon Operator (PAO)

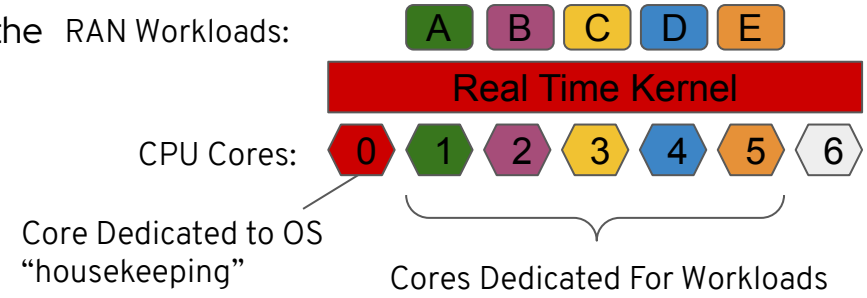


Real Time Kernel and Low Latency Workloads for RAN

A Real Time Kernel is a Red Hat Enterprise Linux kernel that is modified to maintain **low latency**, **consistent response time** and **workload determinism**.

This feature allows workloads to run uninterrupted by the Operating System.

- Allow the installation of the Real Time Kernel on RHEL CoreOS nodes.
- Allow the cluster administrator to provide a PerformanceProfile that defines:
  - A number of CPU cores dedicated to “housekeeping” tasks.
  - A number of CPU cores dedicated for workloads (CPU Pinning).
- NUMA alignment for devices, memory and cores used by Low Latency Workloads.



Cloud-native Network Functions Tests (CNF Tests)

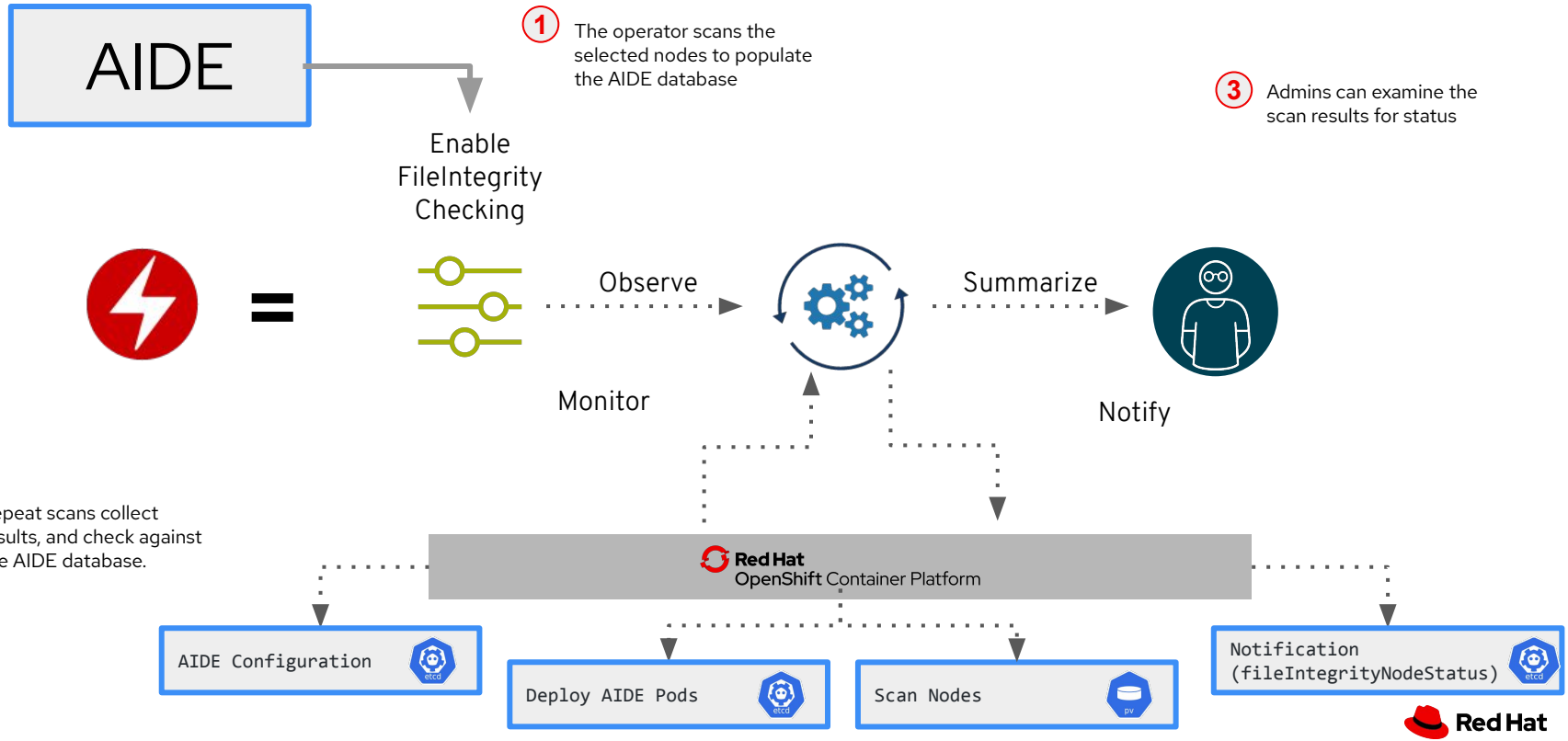
The CNF Tests container image allows service providers to validate that their cluster has been provisioned and configured correctly ready to run CNFs. The documentation resides here.

It validates the following additional performance-related functionality is configured and available on the cluster:

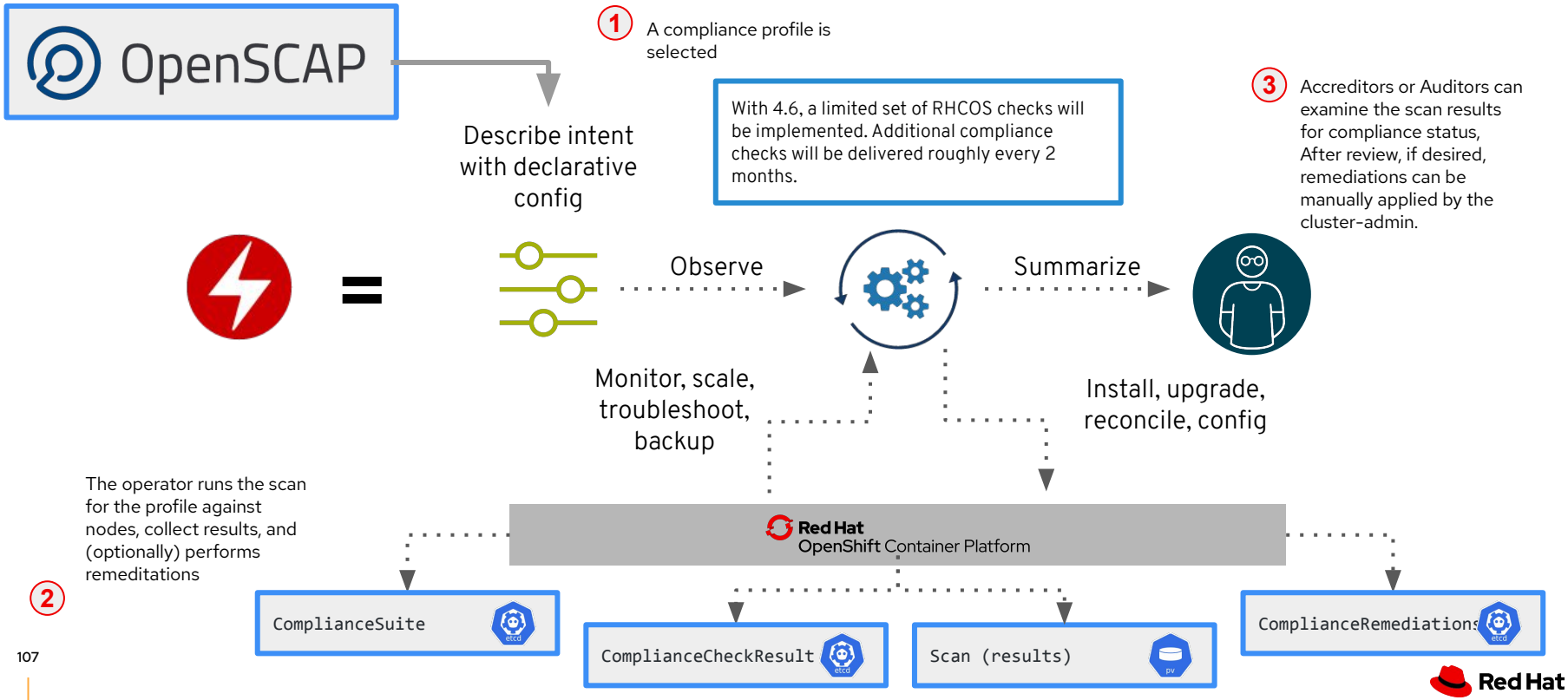
- Precision Time Protocol (PTP)
- Single-root input/output virtualization (SR-IOV)
- Stream Control Transmission Protocol (SCTP)
- Data Plane Development Kit (DPDK)
- Performance AddOn Operator (PAO)

Security and Compliance

Openshift File Integrity Operator



OpenShift Compliance Operator: Declarative Security Compliance



Product Manager: Kirsten Newcomer

Declarative Security Compliance

The compliance operator runs in the OpenShift cluster to scan the cluster nodes and the OpenShift platform itself

Builds on existing and proven technologies that are accepted by the industry and used in the RHEL world.

The operator itself

The operator lets the administrator describe the desired compliance state of a cluster and provides them with an overview of gaps and ways to remediate the gaps.

OpenSCAP

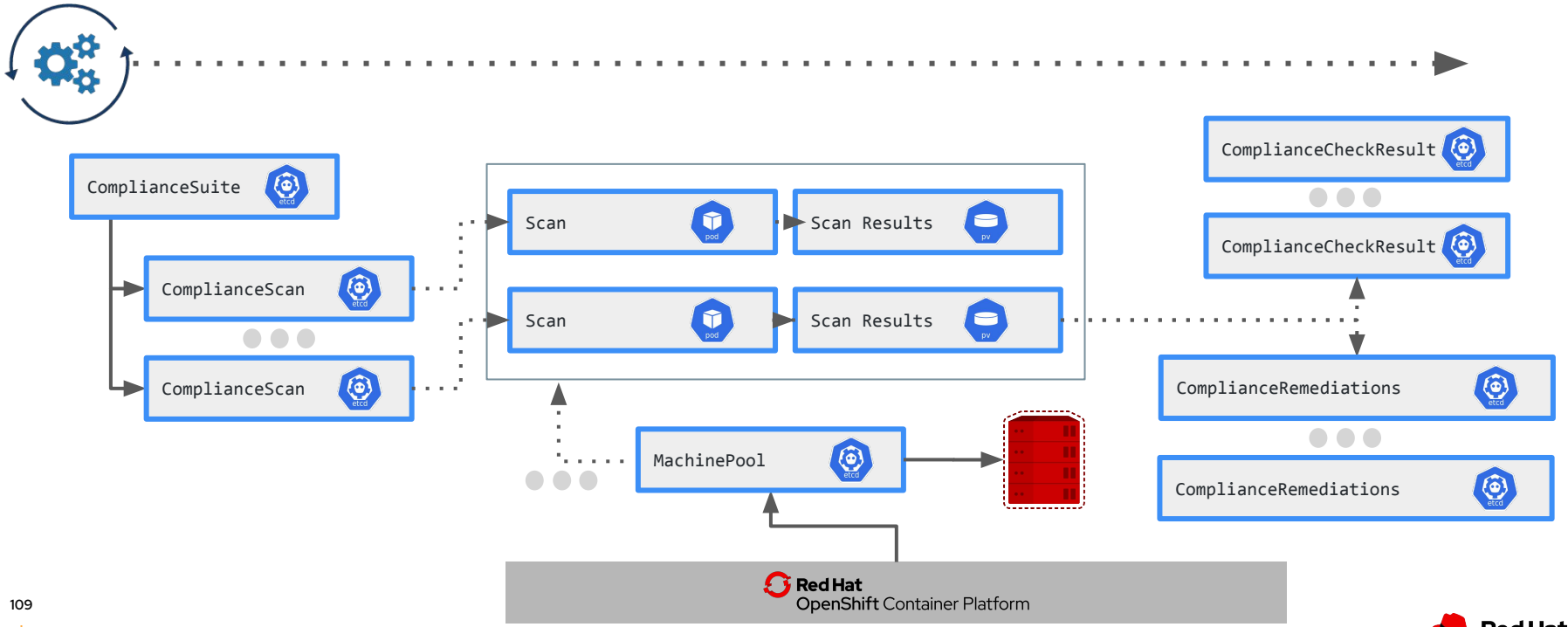
NIST-certified tool to scan and enforce security policies provided by the content.

Compliance Profile Content

The compliance checks themselves are delivered through SCAP content, with a lifecycle independent from the operator or the OpenSCAP scanner

Under the hood

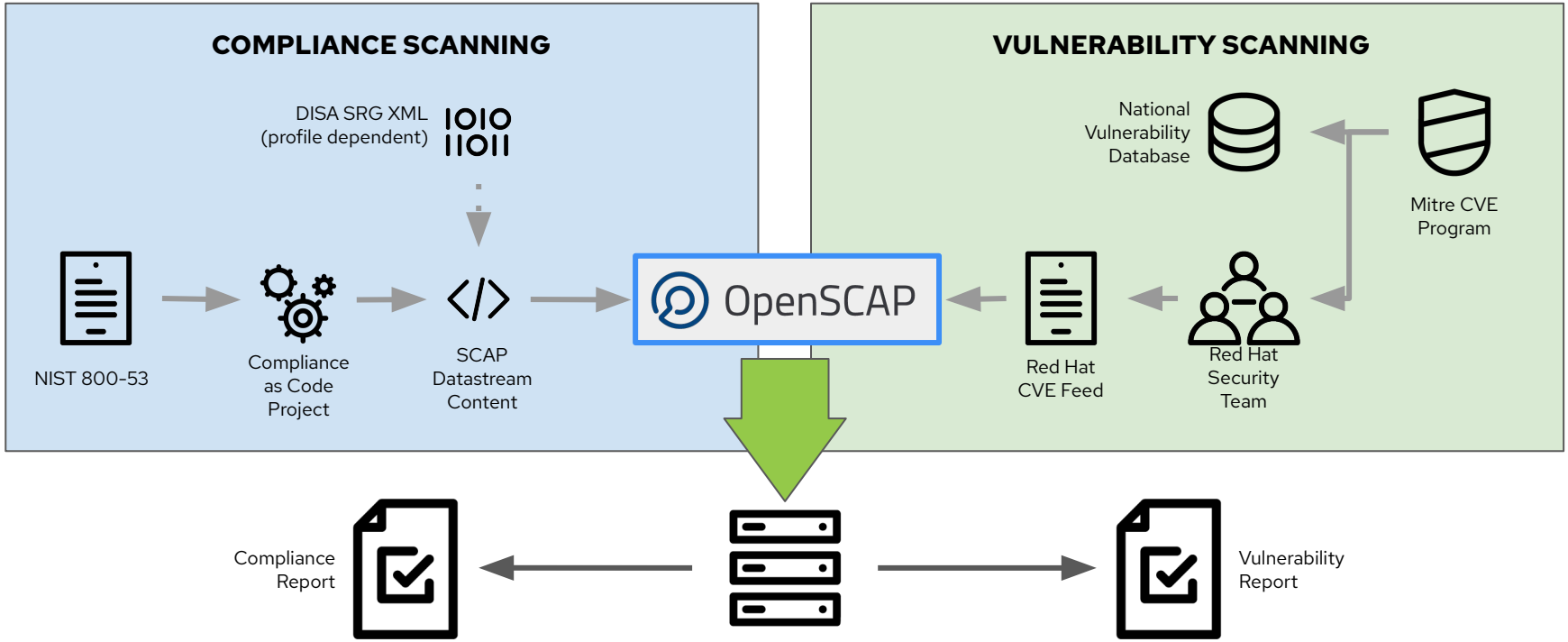
How the Compliance Operator does its work



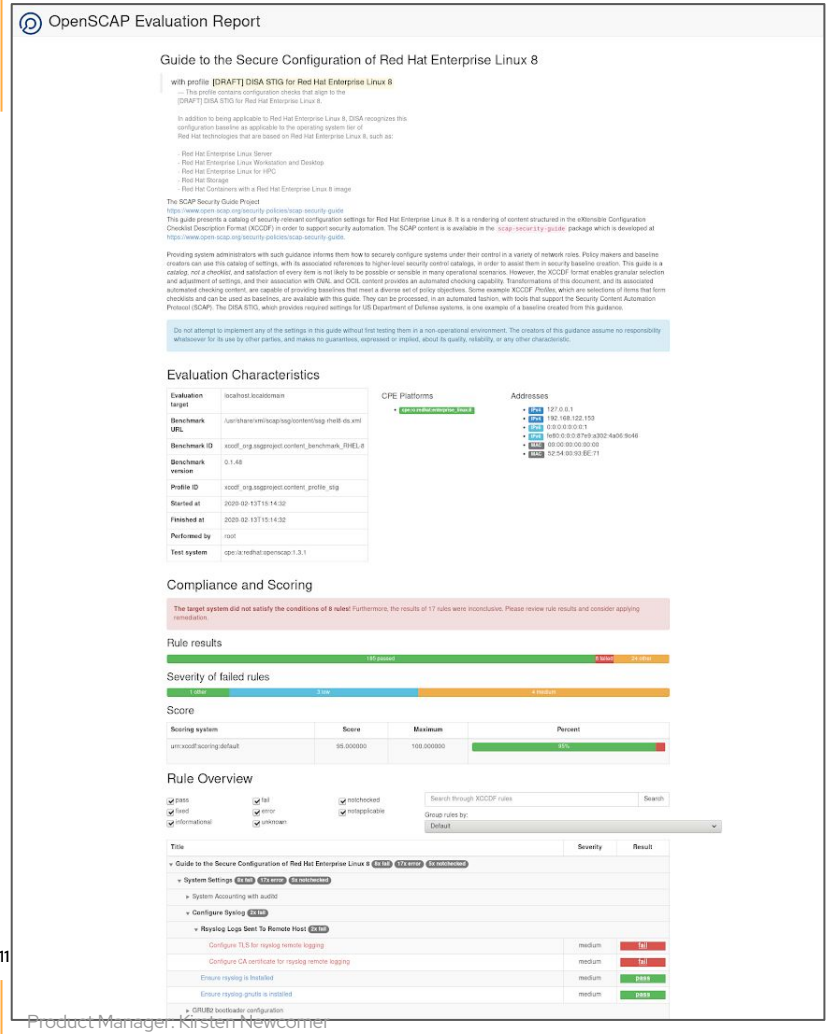
Product Manager: Kirsten Newcomer

Red Hat

How OpenSCAP Works



110




```
$ sudo oscap info /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
Document type: Source Data Stream
Imported: 2020-02-06T09:36:38
...
Checklists:
...
                Generated: 2020-02-06
                Resolved: true
                Profiles:
                        Title: [DRAFT] DISA STIG for Red Hat Enterprise
Linux 8
                                Id:
xccdf_org.ssgproject.content_profile_stig
...
Dictionaries:
        Ref-Id: scap_org.open-scap_cref_ssg-rhel8-cpe-dictionary.xml

## PERFORM AN INITIAL SCAN AND SAVE THE REPORT AS scan.html
$ oscap xccdf eval --report scan.html \
--profile xccdf_org.ssgproject.content_profile_stig \
/usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
...
Title   Uninstall nfs-utils Package
Rule    xccdf_org.ssgproject.content_rule_package_nfs-utils_removed
Ident   CCE-82932-5
Result  fail

Title   Enable the Hardware RNG Entropy Gatherer Service
Rule    xccdf_org.ssgproject.content_rule_service_rngd_enabled
Ident   CCE-82831-9
Result  pass

## SCAN WITH THE REMEDIATE OPTION AND SAVE A REPORT AS remediated.html
$ oscap xccdf eval --report remediated.html --remediate \
--profile xccdf_org.ssgproject.content_profile_stig \
/usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
...
Title   Uninstall nfs-utils Package
Rule    xccdf_org.ssgproject.content_rule_package_nfs-utils_removed
Ident   CCE-82932-5
```

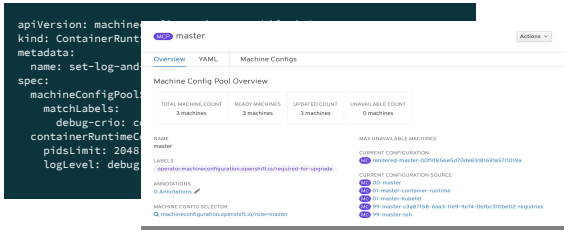
111

111

RH ACM and Compliance

1 A user requests a new cluster

Red Hat Advanced Cluster Management for Kubernetes



2 *Red Hat curates cluster configs, including RHCOS configs to meet security profiles, like CIS or NIST-800-53*

Red Hat OpenShift Container Platform

Red Hat Enterprise Linux CoreOS

Describe intent with declarative config

=

Observe

Maintain

4 Metrics are sent to Red Hat Insights for analysis via secured HTTPS.

3 *OpenShift operators apply updates; he Machine Config Operator applies the selected secure machine config for RHCOS updates*

Monitor, scale, troubleshoot, backup

Install, upgrade, *reconcile*, config

Red Hat OpenShift Container Platform

Product Manager: Kirsten Newcomer

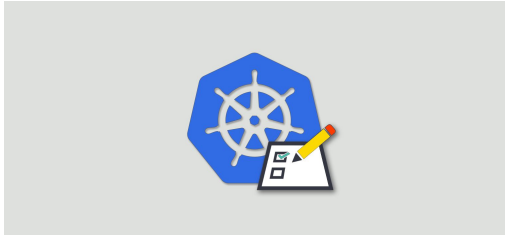
Red Hat

Security/Auth Improvements: Customize Audit Config

Control the amount of information that is logged to the node audit logs by choosing the audit log policy profile to use.

- **Default**: Logs only metadata for read and write requests; does not log request bodies. This is the default policy.
- **WriteRequestBodies**: In addition to logging metadata for all requests, logs request bodies for every write request to the API servers (create, update, patch). This profile has more resource overhead than the Default profile.
- **AllRequestBodies**: In addition to logging metadata for all requests, logs request bodies for every read and write request to the API servers (get, list, create, update, patch). This profile has the most resource overhead.

```
apiVersion: config.openshift.io/v1
 kind: APIServer
 metadata:
 ...
 spec:
   audit:
     profile: WriteRequestBodies
```



Security/Auth Improvements: Token inactivity timeout for OAuth Server

You can configure OAuth tokens to expire after a set period of inactivity. By default, no token inactivity timeout is set.

Add the `spec.tokenConfig.accessTokenInactivityTimeout` field and set your timeout value:

```
apiVersion: config.openshift.io/v1
kind: OAuth
metadata:
...
spec:
  tokenConfig:
    accessTokenInactivityTimeout: 400s
```

Example output

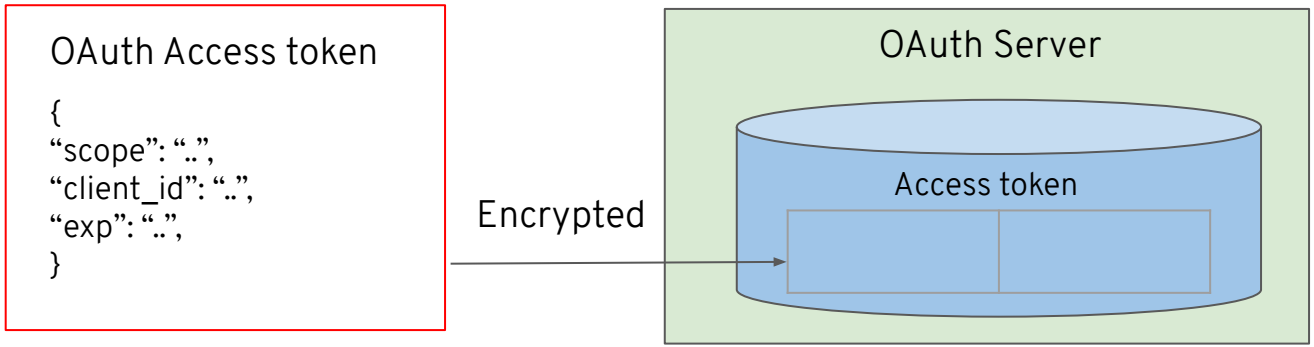
error: You must be logged in to the server (Unauthorized)

Security/Auth Improvements: Secure OAuth Resource Storage

OAuth access token and OAuth authorize token object names are now stored as non-sensitive object names.

Previously, secret information was used as the OAuth access token and OAuth authorize token object names. When etcd is encrypted, only the value is encrypted, so this sensitive information was not encrypted.

If you are upgrading your cluster to OpenShift Container Platform 4.6, old tokens from OpenShift Container Platform 4.5 will still have the secret information exposed in the object name. By default, the expiration for tokens is 24 hours, but this setting can be changed by administrators. Sensitive data can still be exposed until all old tokens have either expired or have been deleted by an administrator.



Red Hat

Multi-Arch & Windows

Windows Community Operator

- Community distribution of the Windows Machine Config Operator will be available in mid to late October
- The Windows Machine Config Operator is the entry point for OpenShift customers who want to run Windows workloads on their clusters.
- The intent of this feature is to allow a cluster administrator to add a Windows compute node as a day 2 operation with a prescribed configuration to an installer provisioned OpenShift 4.6 cluster and enable scheduling of Windows workloads.
- Prerequisite: OpenShift 4.6+ cluster configured with hybrid OVN Kubernetes networking.
- Tested on AWS and Azure. vSphere CI tests on-going
- Red Hat certified operator will be generally available in December

	Community Operator	**Red Hat Operator**
Location	In Cluster OperatorHub	Red Hat Marketplace
Available date	Mid Oct	Mid Dec
Platforms supported	AWS, Azure	AWS, Azure, vSphere (possibly)
Refresh cycle	Every 1-2 months	Every OCP Y stream

Windows Machine Config Operator (WMCO) workflow

Transfer binaries

This includes Windows Machine Config Bootstrapper

Configure kubelet

Remotely execute WMCB to configure kubelet

Run hybrid-overlay

Create OpenShift HNS network

Configure CNI

Configure kubelet for CNI plugin

Set up kube-proxy

Maintains network rules on nodes allowing outside communication

Multi-architecture updates

- Align IBM Power and IBM Z GA with x86
- Storage being expanded
  - Local Storage Operator
  - Fibre Channel
  - HostPath
  - Raw Block
  - iSCSI
  - 4k Disk support
- Logging now supported

Supported

- OpenShift Core (CVO Operators)
- UPI installer
- OVS/OVN (networking)
- RHEL7 Based container support
- RHEL CoreOS (host nodes)
- Ansible Engine
- Red Hat Software Collections
- AdoptOpenJDK with OpenJ9
- Single Sign-On (**Z only**)
- OpenShift Cluster Monitoring (Prometheus, Grafana)
- Node Tuning Operator
- OpenShift Jenkins
- OpenShift Logging (elasticSearch, kibana)
- Machine Configuration Operator (used in IPI installs)
- Node Feature Discovery Operator

Extra content ported

- Red Hat Runtimes (**Z only**)

Product Manager: Duncan Hardie

Thank you

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

Red Hat is here to help

Responding to COVID-19 requires collaboration, transparency, and the free exchange of expertise.

Ways to contact us

Red Hat