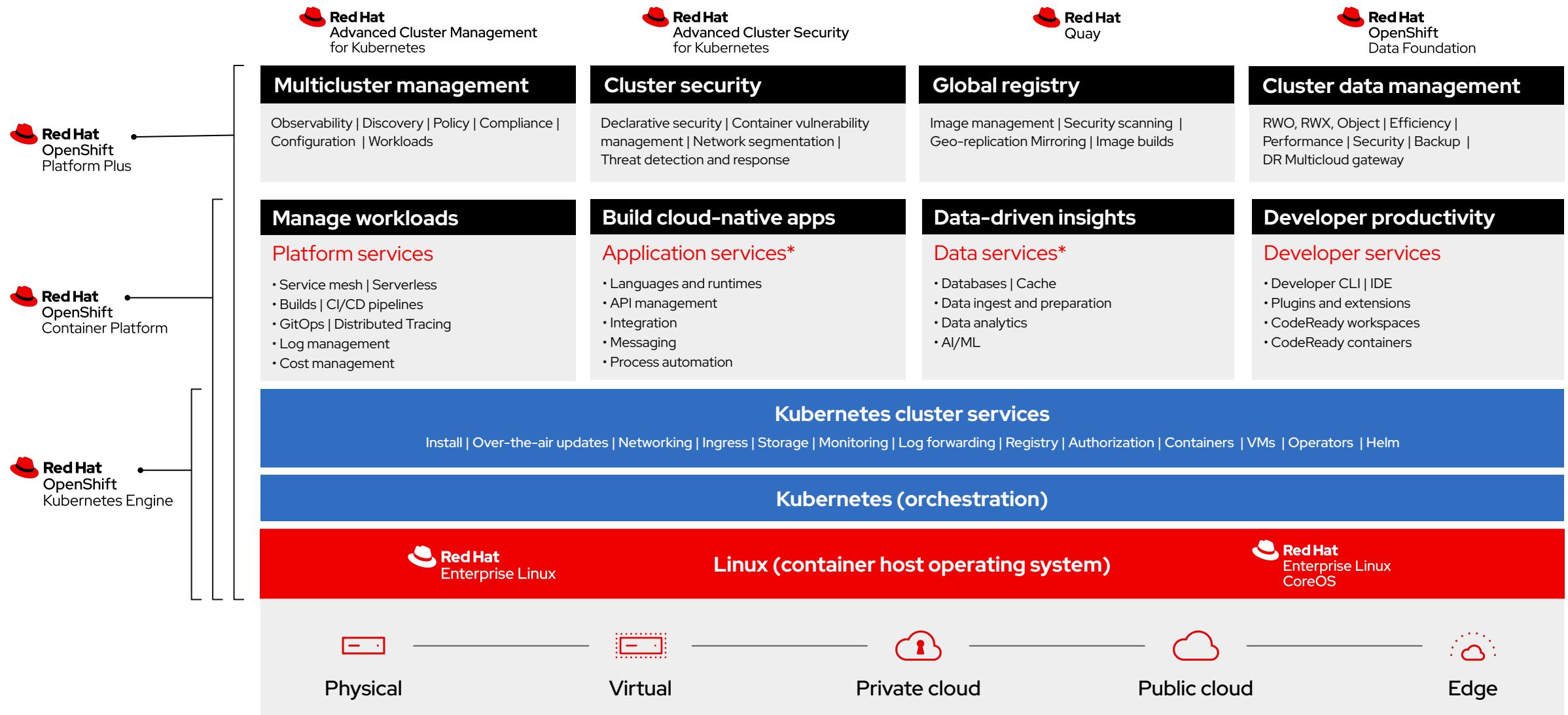


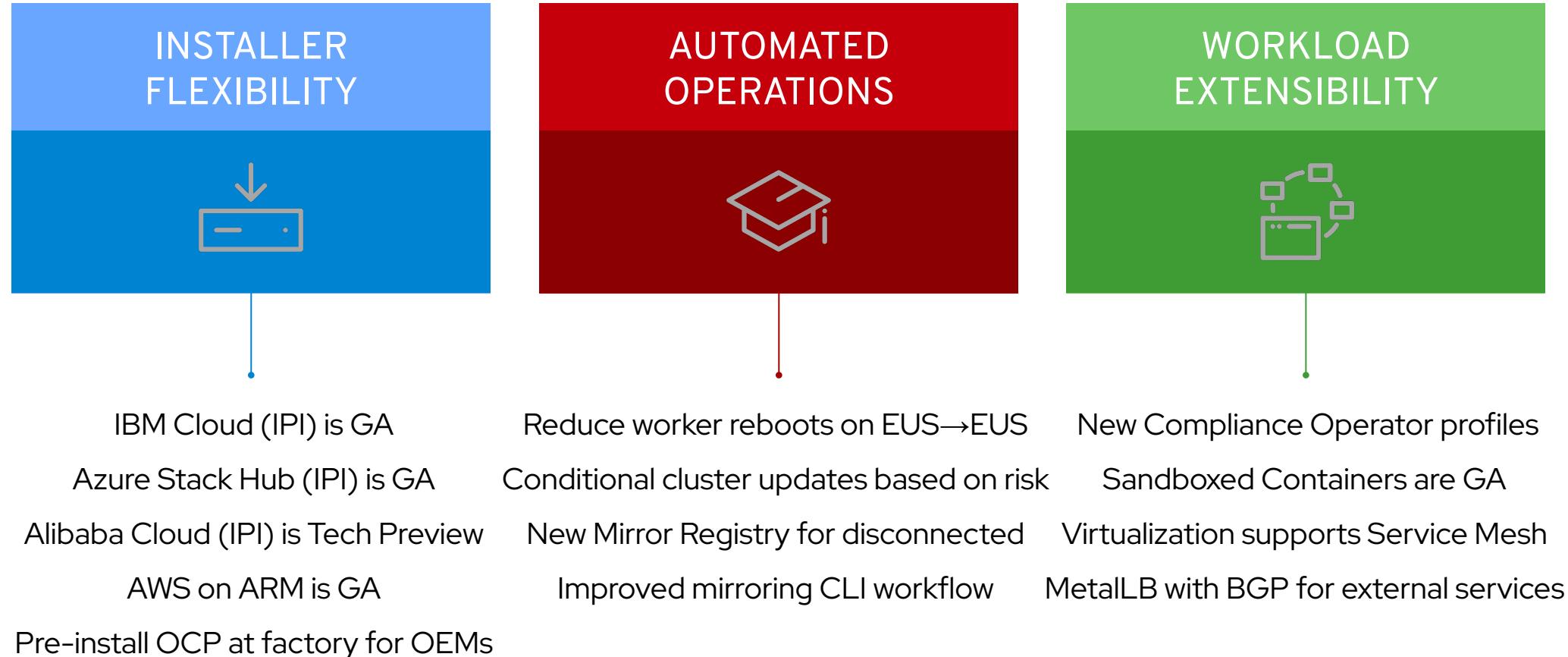


# What's New in OpenShift 4.10

# Red Hat open hybrid cloud platform



# OpenShift 4.10



# Kubernetes 1.23

## Major Themes and Features

- ▶ Clusters default to Dual Stack networking
  - ▶ Feature gate is removed, meaning IPv4 and IPv6 is default
  - ▶ In OpenShift, dual-stack has been GA since 4.8
- ▶ PodSecurity graduates to Beta
  - ▶ Red Hat is making upstream contributions here
  - ▶ OpenShift will support pod security admission and continue to support SCCs side by side
- ▶ CSI Migration
  - ▶ Replacement of existing in-tree storage plugins with a corresponding CSI driver
  - ▶ OpenShift will seamlessly migrate in the future
- ▶ Software Supply Chain
  - ▶ SLSA Level 1 Compliance in the Kubernetes Release Process



# OpenShift Roadmap

## Q1 2022

<b>HOSTED</b>	<ul style="list-style-type: none"> <li>• ROSA: Cluster manager UI for ROSA provisioning</li> <li>• ROSA/OSD: Cluster hibernation</li> <li>• OCM: Updated OSD cluster creation UI</li> <li>• OSD: PrivateLink</li> <li>• ROSA: Cluster-wide proxy</li> </ul>
<b>PLATFORM</b>	<ul style="list-style-type: none"> <li>• Alibaba Cloud (IPI) technology preview</li> <li>• IBM Cloud &amp; Azure Stack Hub (IPI)</li> <li>• OpenShift on ARM (AWS and Bare Metal)</li> <li>• Zero Touch Provisioning and Central infrastructure Management in ACM is GA</li> <li>• External Control Planes with HyperShift in ACM TP</li> <li>• MetalLB BGP support</li> <li>• ExternalDNS technology preview</li> <li>• Disconnected mirroring simplification</li> <li>• Service Mesh on VMs</li> </ul>
<b>APP</b>	<ul style="list-style-type: none"> <li>• Dynamic Plugins TP</li> <li>• Unified Console(ACM +OCP) TP</li> <li>• Serverless:Knative Kafka Broker and Sink TP</li> <li>• Operator SDK: Hybrid Helm Operator plugin TP</li> <li>• Operator SDK: Digest-based bundle (disconn.)</li> </ul>
<b>DEV</b>	<ul style="list-style-type: none"> <li>• Unprivileged builds in OpenShift Pipelines</li> <li>• Custom Tekton Hub on OpenShift</li> <li>• Automatic pull of RHEL entitlements GA</li> <li>• BuildConfig CSI volume mounts</li> <li>• Tekton Chains (sigstore) TP</li> <li>• OpenShift sandboxed containers GA</li> </ul>

## Q2 2022

<b>HOSTED</b>	<ul style="list-style-type: none"> <li>• ROSA/OSD: FedRAMP High on AWS GovCloud</li> <li>• ROSA/OSD/ARO: GPU Support</li> <li>• ROSA/OSD: ISO27017+ISO27018</li> <li>• ROSA/OSD: Additional instance types</li> <li>• ARO: Upgrades through cluster manager</li> <li>• Cost management understands IBM Cloud IaaS</li> </ul>
<b>PLATFORM</b>	<ul style="list-style-type: none"> <li>• Nutanix (UPI/IPI)</li> <li>• SRO manages third party special devices</li> <li>• Additional capabilities for Windows containers: health management, 3rd party CNI (like Calico)</li> <li>• NetFlow/sFlow/IPFIX Collector</li> <li>• Introduce Gateway API</li> </ul>
<b>APP</b>	<ul style="list-style-type: none"> <li>• OpenShift Serverless Functions GA</li> <li>• Encryption pf inflight data natively in Serverless</li> <li>• Serverless:workflow orchestration TP</li> <li>• Serverless: Knative Kafka Broker and Sink GA</li> <li>• Operator Maturity increase via SDK</li> <li>• OLM operator update retries</li> </ul>
<b>DEV</b>	<ul style="list-style-type: none"> <li>• Private Preview of App Studio, a hosted dev exp</li> <li>• OpenShift Serverless Functions IDE Experience</li> <li>• OpenShift Dev CLI (odo onboarding &amp; more)</li> <li>• GitOps ApplicationSets GA</li> <li>• OpenShift Pipelines on Arm</li> <li>• Extended pipeline history</li> <li>• Custom Argo CD plugins support</li> </ul>

## H2 2022+

<b>HOSTED</b>	<ul style="list-style-type: none"> <li>• ROSA/OSD: Terraform provider</li> <li>• ROSA/OSD: AWS Dedicated instances</li> <li>• ROSA/OSD: Detailed Quota Usage in cluster manager</li> <li>• Cost mgmt integration to Subs Watch, ACM</li> <li>• Network Policy v2 &amp; OVN no-overlay option</li> <li>• SmartNIC Integrations</li> <li>• eBPF Support</li> <li>• Network Topology and Analysis Tooling</li> <li>• Utilize cgroups v2</li> <li>• Enable user namespaces</li> <li>• Windows Containers: CSI proxy, improved monitoring/logging &amp; more platforms supported</li> <li>• Network Policy v2 &amp; OVN no-overlay option</li> <li>• BGP Advertised Services (FRR)</li> <li>• SigStore style image signature verification</li> <li>• Cost mgmt integration to Subs Watch, ACM</li> <li>• Detailed Quota Usage in cluster manager</li> <li>• ROSA/OSD: AWS Dedicated instances</li> <li>• ROSA/OSD: Terraform provider</li> </ul>
<b>PLATFORM</b>	<ul style="list-style-type: none"> <li>• Azure China</li> <li>• File-based operator catalog management</li> <li>• Operator SDK for Java/Quarkus TP</li> <li>• Integration of Knative(Serverless) with KEDA</li> <li>• Multi Tenancy for Serverless</li> <li>• Serverless Cost Management</li> </ul>
<b>APP</b>	<ul style="list-style-type: none"> <li>• Operator Maturity increase via SDK</li> <li>• OLM operator update retries</li> <li>• Nutanix (UPI/IPI)</li> <li>• SRO manages third party special devices</li> <li>• Additional capabilities for Windows containers: health management, 3rd party CNI (like Calico)</li> <li>• NetFlow/sFlow/IPFIX Collector</li> <li>• Introduce Gateway API</li> </ul>
<b>DEV</b>	<ul style="list-style-type: none"> <li>• Private Preview of App Studio, a hosted dev exp</li> <li>• OpenShift Serverless Functions IDE Experience</li> <li>• OpenShift Dev CLI (odo onboarding &amp; more)</li> <li>• GitOps ApplicationSets GA</li> <li>• OpenShift Pipelines on Arm</li> <li>• Extended pipeline history</li> <li>• Custom Argo CD plugins support</li> </ul>

# Notable Top RFE's and Components

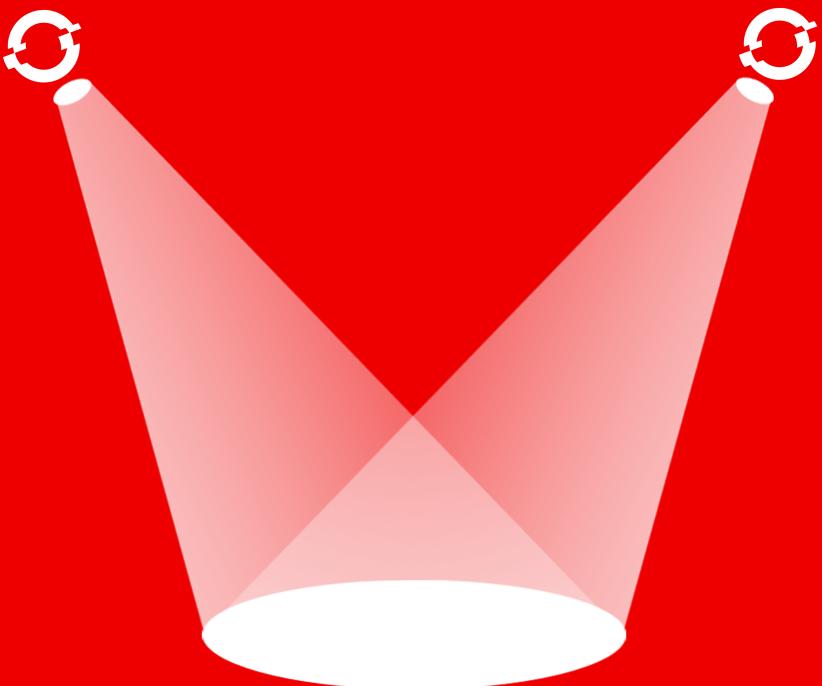
## Top Requests for Enhancement (RFEs)

- ▶ Support for Day-2 changes in static network configuration
  - ▶ Static network configuration can become obsolete and need to be updated after cluster deployment.
- ▶ Capture MachineConfigDaemon Events in the Operator Events
  - ▶ Provides a way to check configuration regularly so admins know about potential problems sooner.
- ▶ Force write MachineConfig to Node
  - ▶ A way to align nodes configurations back to the rendered one in case the files monitored by MCO become misconfigured on UPI installations.
- ▶ Support for AvailabilitySets in MachineSets for Azure
  - ▶ Some Azure Regions do not support multiple zones, high availability can be achieved to some extent by using AvailabilitySets.
- ▶ Ability to change MTU of openshift-sdn post installation
  - ▶ Gives a way to adapt cluster setting to the environment on Day-2.

**45 RFEs**

shipped in  
**OpenShift 4.10**  
for customers

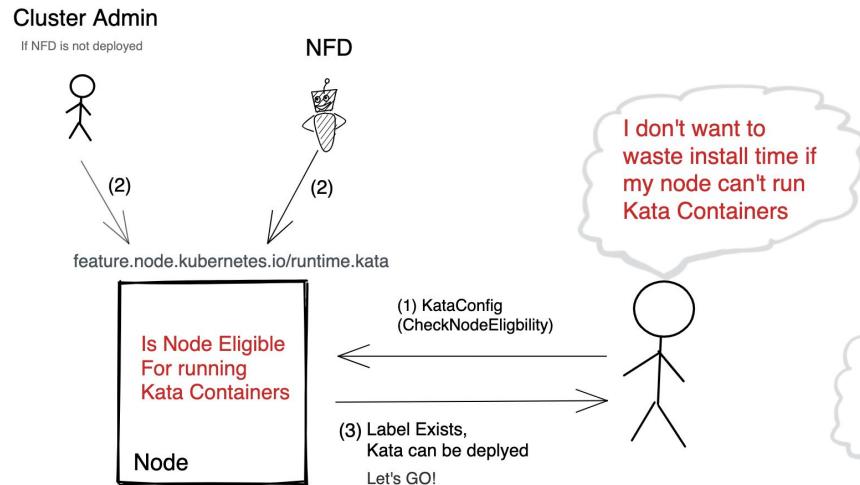
# OpenShift 4.10 Spotlight Features



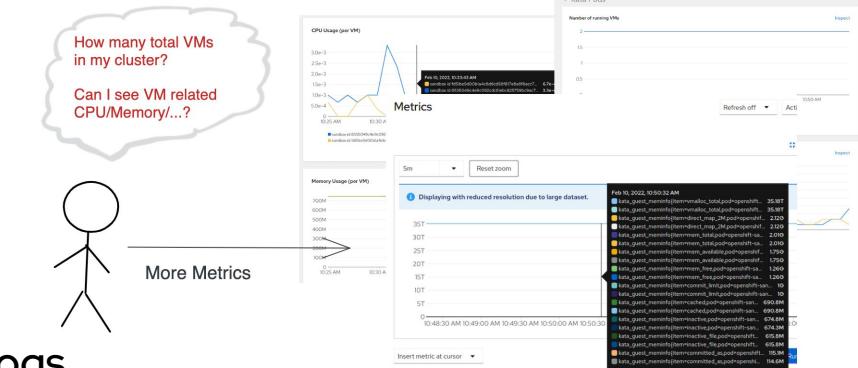
# OpenShift sandboxed containers

Graduated from *Tech Preview* to **GA**

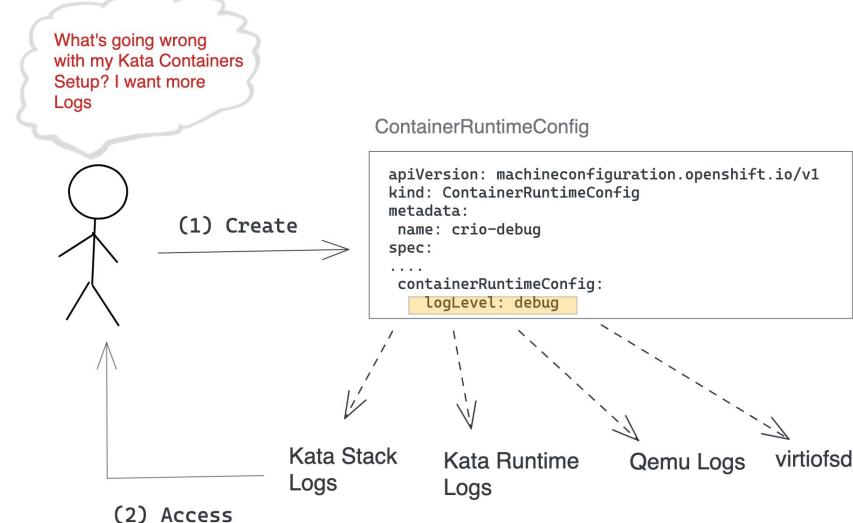
## 1. Pre-install checks for Node eligibility to run sandboxed containers



## 2. Added additional metrics



## 3. Increased debugability -> more logs



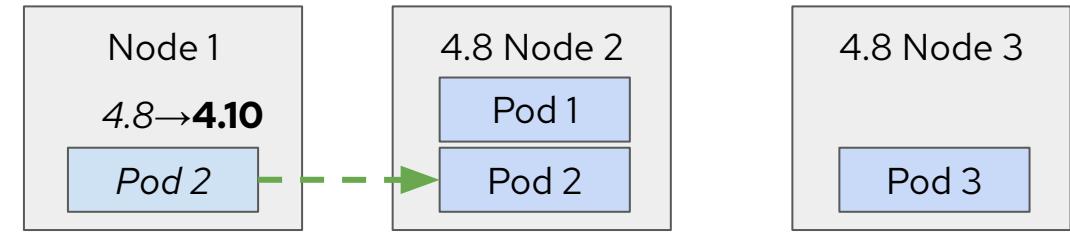
# EUS to EUS Upgrade Experience

Quicker, Safer upgrades and less disruptions to workloads

## EUS-aware Scheduler

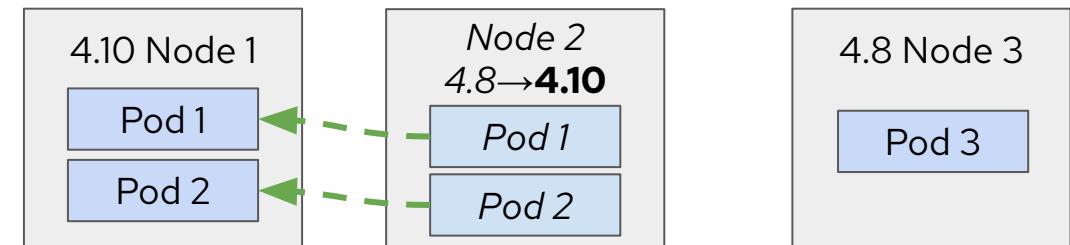
- ▶ EUS-to-EUS upgrade from 4.8.14+ to 4.10 incurs **single reboot** of non-master nodes
- ▶ **Upgrade-aware** scheduler steers rescheduled Pods to updated Nodes
- ▶ Pods restart **less frequently**

Upgrade drains Node1. Pod 1 moves from Node 1 to Node 2.



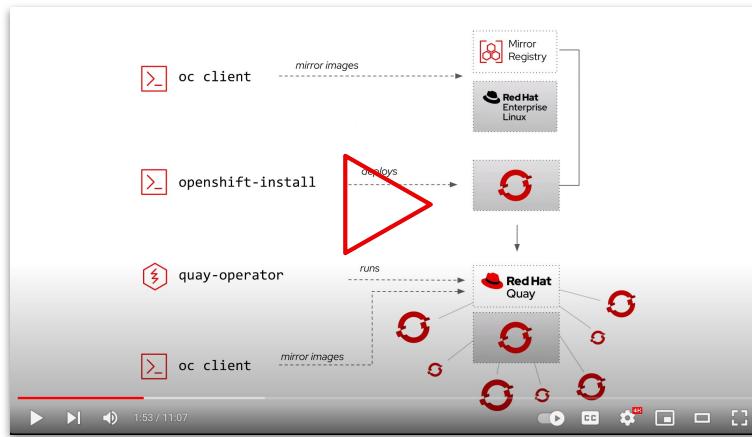
Pods relocate from Node 2 to Node 1.

Node 3 is ready to upgrade and will get new workloads afterwards.



# OpenShift Disconnected

New: Single command to get a registry



- ▶ Local all-in-one Quay instance on RHEL 8 to get customers a supported mirror registry at no additional cost for their first cluster
- ▶ More details: [Technical Enablement Deck](#)
- ▶ Next up (past 4.10 GA): Update support

New: Single command to mirror content



- ▶ A single CLI tool to mirror all OCP content (images, operators, helm charts): `oc mirror`
- ▶ Smart: maintains update paths of OCP & operators
- ▶ Declarative: config to filter for particular OCP & operator catalogs / releases / channels
- ▶ Fast: Incremental mirroring

# Three new Compliance Operator profiles

Customers will be able to Scan,  
Report and Remediate  
Compliance issues using the  
following profiles



## PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.



## FedRAMP Moderate

FedRAMP moderate impact level is the standard for cloud computing security for controlled unclassified information across federal government agencies. The moderate impact level is appropriate for CSPs that will handle government data that is not publicly available.



## NERC CIP

NERC Critical Infrastructure Protection (NERC CIP) is a set of requirements designed to secure the assets required for operating North America's bulk electric system to protect critical cyber assets and minimize risk and manipulation by bad actors seeking to cause damage.

# OpenShift on Arm

- ▶ Announcing **GA** of support for OpenShift on Arm platforms
  - ▶ AWS Full Stack Automation (IPI)
  - ▶ Bare Metal Pre-existing Infrastructure(UPI)
- ▶ It's about choice, run on the architectures that best suit your workloads
- ▶ OpenShift "core" parts for this release
  - ▶ Logging
  - ▶ ACM
  - ▶ Storage: EBS, NFS only
- ▶ Hardware support
  - ▶ What RHEL supports
  - ▶ Certified systems on HCL for best experience but ...
  - ▶ Also systems that meet Arm SystemReady/ServerReady specification\*

Fully Automated Installers (IPI)	✓
Customizable Installers (UPI)	✓
RHEL or CoreOS entitlement	✓
CRIO Runtime	✓
Over the Air Smart Upgrades	✓
Operating System (CoreOS) Management	✓
Enterprise Secured Kubernetes	✓
Kubectl and oc automated command line	✓
Auth Integrations	✓
Operator Lifecycle Manager (OLM)	✓
Administrator Web console	✓
Node Feature Discovery	✓
Embedded OperatorHub	✓
Embedded Marketplace	✓
Embedded Registry	✓
Helm	✓
Cluster Monitoring	✓
Log Forwarding	✓
Telemeter and Insights	✓
OVS and OVN SDN	✓
HAProxy Ingress Controller	✓
Ingress Cluster Wide Firewall	✓
Egress Pod	✓
Ingress Non-Standard Ports	✓
Network Policies	✓
IPv6 Single and Dual Stack	✓
CNI Plugin ISV Compatibility	✓
CSI Plugin ISV Compatibility	✓
Service Binding Operator	✓
Platform Logging	✓
OpenShift Elasticsearch Operator	✓
Developer Web Console	✓



# MetalLB BGP Support

- ▶ MetalLB has two modes to announce reachability information for load balancer IP addresses:
  - ▶ Layer 2 ([4.9](#))
  - ▶ BGP ([4.10](#))
- ▶ BGP (FRR) mode: Traffic can target multiple nodes – routers can perform load balancing across the cluster using ECMP
  - ▶ Active / Active configuration handled by the external routers
  - ▶ Extra configuration required to establish BGP sessions
  - ▶ BFD Support
  - ▶ Refusing incoming routes
  - ▶ BGP Peer node selector
  - ▶ iBGP and eBGP, single and multihop

```
apiVersion: metallb.io/v1beta1
kind: AddressPool
metadata:
  name: addresspool-sample1
  namespace: metallb-system
spec:
  protocol: bgp
  addresses:
    - 172.18.0.100-172.18.0.255
```

```
apiVersion: metallb.io/v1beta1
kind: BGPPeer
metadata:
  name: peer-sample1
  namespace: metallb-system
spec:
  peerAddress: 10.0.0.1
  peerASN: 64501
  myASN: 64500
  peerPort: 179
  holdTime: "180s"
  keepaliveTime: "180s"
  password: "test"
```

# RHEL entitlement management for image builds

## Pull entitlements

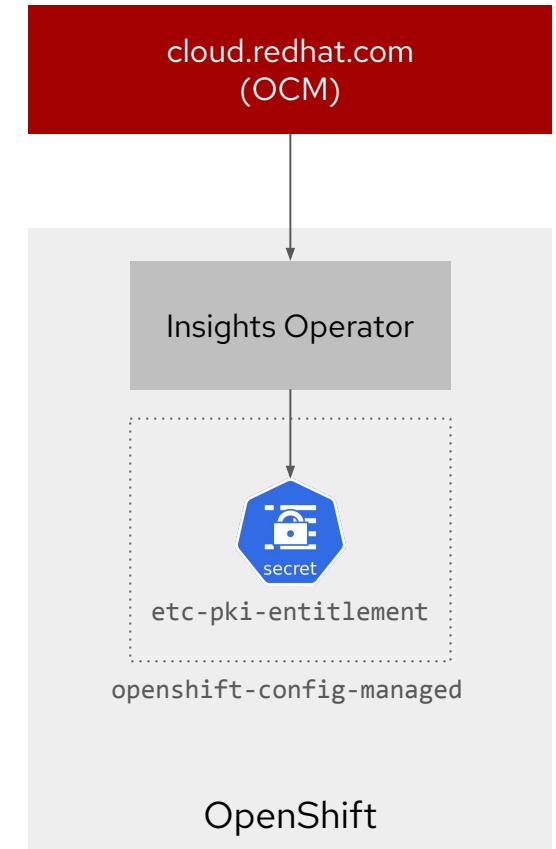
- ▶ Insights Operator manages and refreshes cluster entitlements (**GA**)
- ▶ Simple Content Access (SCA) must be enabled on customer's account
- ▶ NOT available for OSD/ROSA/ARO

## Manage access

- ▶ Shared Resource CSI Driver (**Tech Preview**)
- ▶ Provide tenants access to entitlements without sharing certificates

## Use entitlements

- ▶ Mount shared entitlements in BuildConfigs (**Tech Preview**)
- ▶ Mount entitlement secret in BuildConfigs, Pipelines, Pods, etc (**GA**)



# Console

# Multi-Cluster Focused

## Selectable Cluster Inventory

Tech Preview

### What is this console integration?

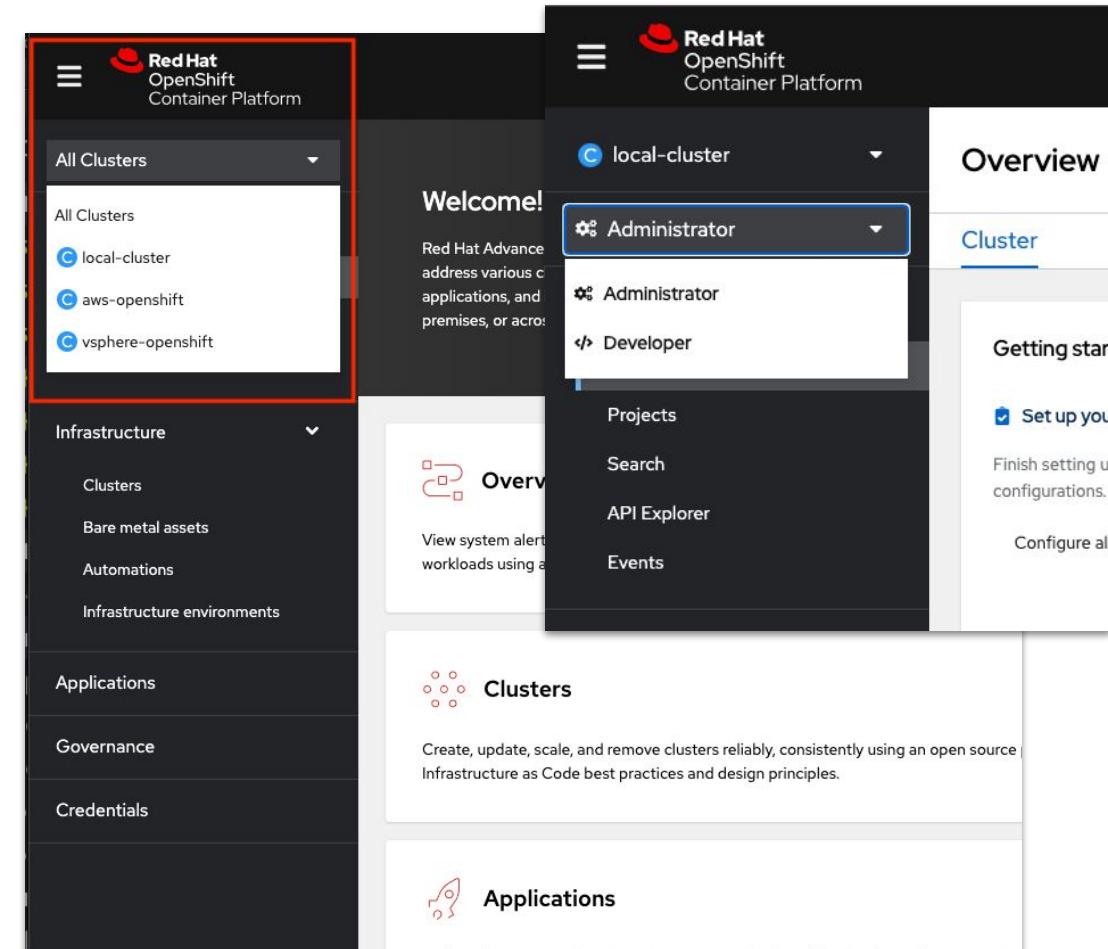
Experience allows users to select clusters across their company as they enter the hub cluster's OCP console! Bringing together 3 tools into one UX:

- ▶ OpenShift Console (OCP) - main user experience for all individual clusters
- ▶ Multicloud Engine (MCE) - offers basic cluster inventory/create/update/destroy
- ▶ Advanced Cluster Management (ACM) - full multi-cluster management

### Moving from single cluster to a fleet of OpenShift:

1. Start deploying apps on a single OpenShift cluster
2. Use the Multicloud Engine to create more clusters and enable RBAC controlled multi-cluster views
3. Upgrade with Advanced Cluster Management to simplify multi-cluster configuration, application deployment, observability, networking, and more.

All OCP customers get MCE included in their subscription



# Console Extensibility

## Dynamic Plugins

Tech Preview

### What is a dynamic plugin?

- ▶ Dynamic Plugin enables partners & customers to build high quality, unique user experiences **natively** in the OCP Console !
- ▶ Update existing perspectives
  - ▶ Add new flows, pages, actions, .... to either the Admin or Dev perspectives
- ▶ Add new perspectives
  - ▶ Create persona or task based perspectives based on your needs

## Dynamic Plugin Technical Details

### How does it work?

- ▶ Based on [webpack 5 module federation](#)
- ▶ Built with [PatternFly 4](#) components
- ▶ Plugins are dynamically loaded at runtime & dis/enabled via Console UI
- ▶ Plugins can be updated independently of the host application
- ▶ Plugins provide extension points or whole perspectives
- ▶ ACM is built with Dynamic Plugins and will give us the ability to extend the Multi Cluster view.

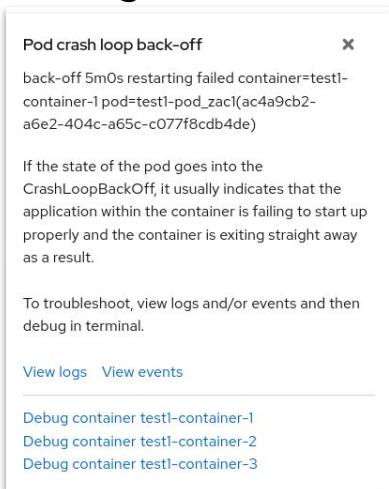
Name	Version	Description	Status	Last Updated
container-storage	4.6.3	OpenShi	Disabled	Jul 21, 9:23 am
virtualization-4.7	4.7.0	OSV plugin	Disabled	Jul 18, 2:47 am
new_extension	1.0.1	Adds more elements to console	Dependency not met	Mar 3, 10:04 am

# Common Console Updates

## Pod Debug Mode

**How do I debug a application that fails on startup?**

- ▶ Quickly troubleshoot mis behaving pods from the UI 
- ▶ Same as running `oc debug pod`
- ▶ Starts each container in a interactive shell
  - ▶ Stops the pod from CrashLooping
  - ▶ Check environment variables, config files, ...
- ▶ Access to logs & events



## User Preferences updates

**How do I hide user workload notifications?**

User Preferences

Set your individual preferences for the console experience. Any changes will be autosaved.

General      User workload notifications

Language       Hide user workload notifications

Notifications      Do not display notifications created by users for specific projects on the cluster overview page or in the drawer.

Applications

**Change your defaults for route creation in creation flows!**

User Preferences

Set your individual preferences for the console experience. Any changes will be autosaved.

The defaults below will only apply to the Import from Git and Deploy Image forms when creating Deployments or Deployment Configs.

General       Secure route

Language      Routes can be secured using several TLS termination types for serving certificates.

Notifications      TLS termination

Applications      Edge

Insecure traffic      Redirect

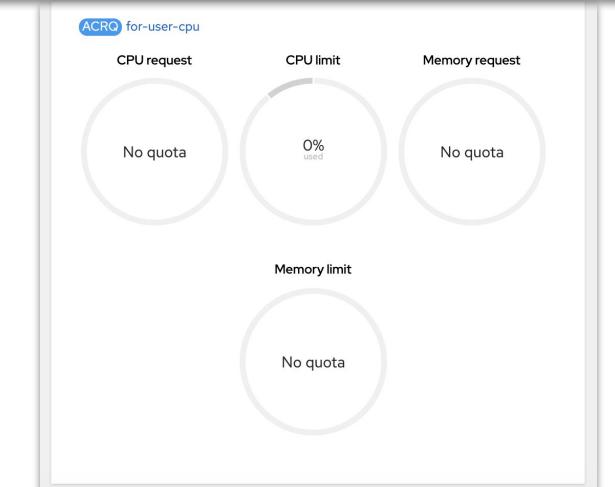
Policy for traffic on insecure schemes like HTTP.

## Improved Quota Visibility

**How do I see how much quota is left?**

- ▶ Non admin users can now see their usage of the [AppliedClusterResourceQuota](#)

Resource type	Capacity	Used	Total used	Max
pods	0	1	2	10
secrets	0	8	20	20



# Platform Services

# OpenShift Builds

## Classic Builds

- ▶ Shared Resource CSI Driver ([Tech Preview](#))
  - ▶ Share secrets/configmaps (e.g. entitlement certs, git credentials, and registry credentials) across namespaces for use by tenants
  - ▶ Control access to shared secrets (e.g. tenants can consume but not see content)
- ▶ Mount CSI volumes in BuildConfigs ([Tech Preview](#))
  - ▶ Mount a shared secret/configmap in BuildConfig for use during image build

## Shipwright Builds

- ▶ Build images from source code in local directory
- `myapp$> shp build upload myapp-build`
- ▶ Custom annotations on output images
  - ▶ Volume support

# OpenShift Pipelines

- ▶ OpenShift Pipelines 1.7
- ▶ Pipeline as code (**Tech Preview**)
- ▶ TaskRun and image signing with Tekton Chains (**Tech Preview**)
- ▶ In-cluster Tekton Hub for custom Task curations (**Tech Preview**)
- ▶ Run Tasks in kernel user namespace  
(root in container, non-root on host)
- ▶ Unprivileged Dockerfile and S2I image builds
- ▶ Triggers emit events in the user namespace to simply debugging
- ▶ OpenShift sandboxed containers verified runtime for pipelines
- ▶ Pipeline UI enhancements in Dev Console
  - ▶ Support for multiple pipeline templates per runtime
  - ▶ Webhooks created when importing apps from Git
  - ▶ Tasks in Tasks selector within pipeline builder link to docs in Tekton Hub

Pipelines

Add pipeline

s2i-nodejs-deployment-advanced

s2i-nodejs-deployment

s2i-nodejs-deployment-advanced

```

graph LR
    A[fetch-repository] --> B[build]
    B --> C[static-analysis]
    C --> D[cve-scan]
    D --> E[deploy]
  
```

Tasks

Pods

nodejs-ex-7d59646b8-mc54z

ImagePull BackOff

View logs

PipelineRuns

PL nodejs-ex

Start last run

nodejs-ex-hvuw8

Running

View logs

(1 minute ago)

Triggers

trigger-template-nodejs-ex-53pac4

http://el-event-listener-9enbj6-demo.apps.ci-in-hbipit-72292.origin-ci-int-gce.dev.rhcloud.com

```

apiVersion: tekton.dev/v1beta1
kind: PipelineRun
metadata:
  generateName: build-deploy-run-
spec:
  pipelineRef:
    name: build-deploy
  podTemplate:
    runtimeClassName: kata
  
```

# OpenShift GitOps

- ▶ OpenShift GitOps 1.5
- ▶ Provides Argo CD 2.3
- ▶ Now generates in ApplicationSets
  - ▶ Generate Application for pull requests
  - ▶ Merge result of multiple generators
- ▶ Support for ignoring managed fields by specific managers
- ▶ Respects “ignore differences” setup during sync for objects and fields owned or mutated by operators
- ▶ [Dev Console] Health status for resources added

The screenshot shows the Red Hat OpenShift Container Platform Dev Console interface. The left sidebar has a 'Developer' tab selected, with options like '+Add', 'Topology', 'Observe', 'Search', 'Builds', 'Pipelines', 'Environments' (which is highlighted), 'Helm', 'Project', 'ConfigMaps', and 'Secrets'. The main content area shows an environment named 'app-taxi' from 'https://github.com/ciay/gitops.git'. It displays a namespace named 'dev' with the URL 'https://kubernetes.default.svc'. A warning message says 'make syncPolicy to manual for testing' and lists a commit by 'ciay' with hash '6ca7c83'. It also shows the last deployment date as 'Oct 7, 2021, 2:01 PM'. Below this, the 'Resources' section provides a summary of the current state of various Kubernetes resources:

Resource Type	Status
Deployments	1 D
Secrets	0 S
Services	1 S
Routes	1 RT
Role Bindings	0 RB
Cluster Roles	0 CR
Cluster Role Bindings	0 CRB

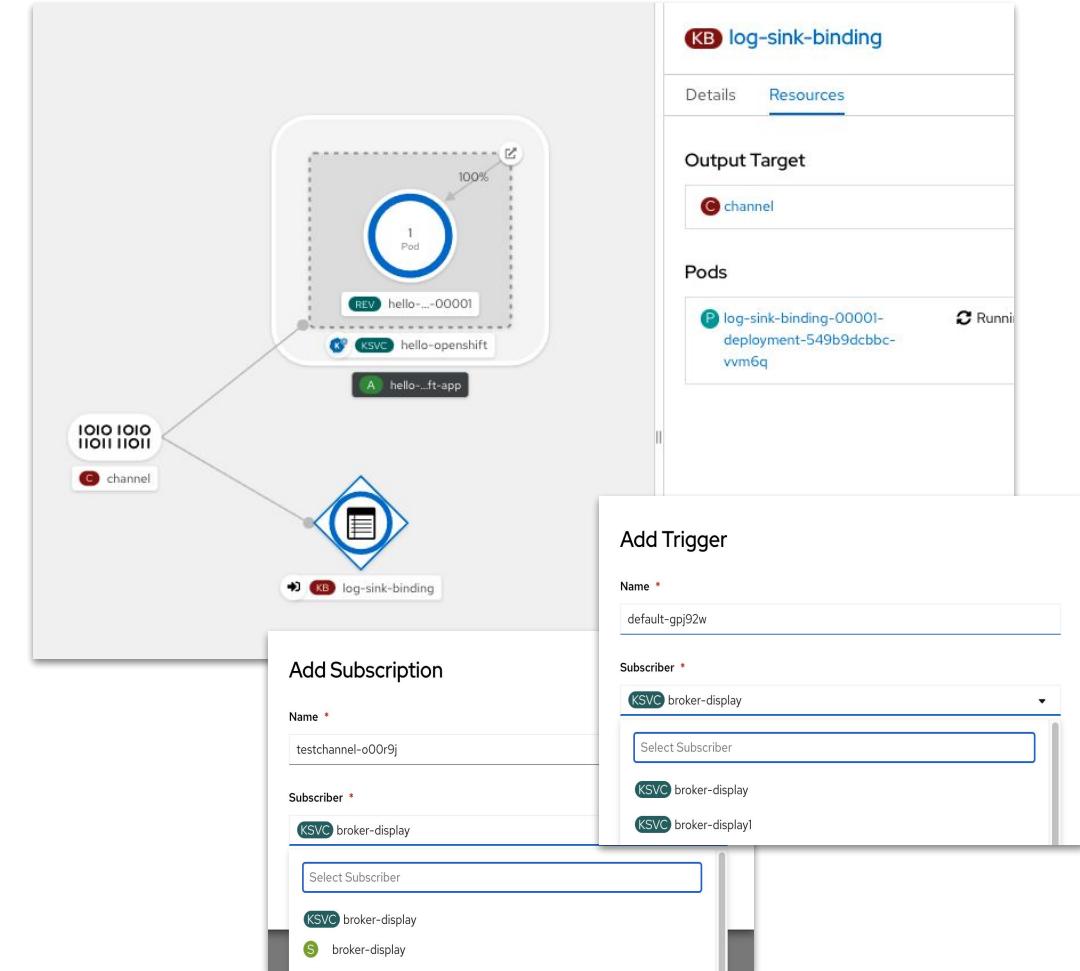
A tooltip over the 'Resources' section indicates '1 of 1 OutOfSync'.

# OpenShift Serverless

## Key Features & Updates

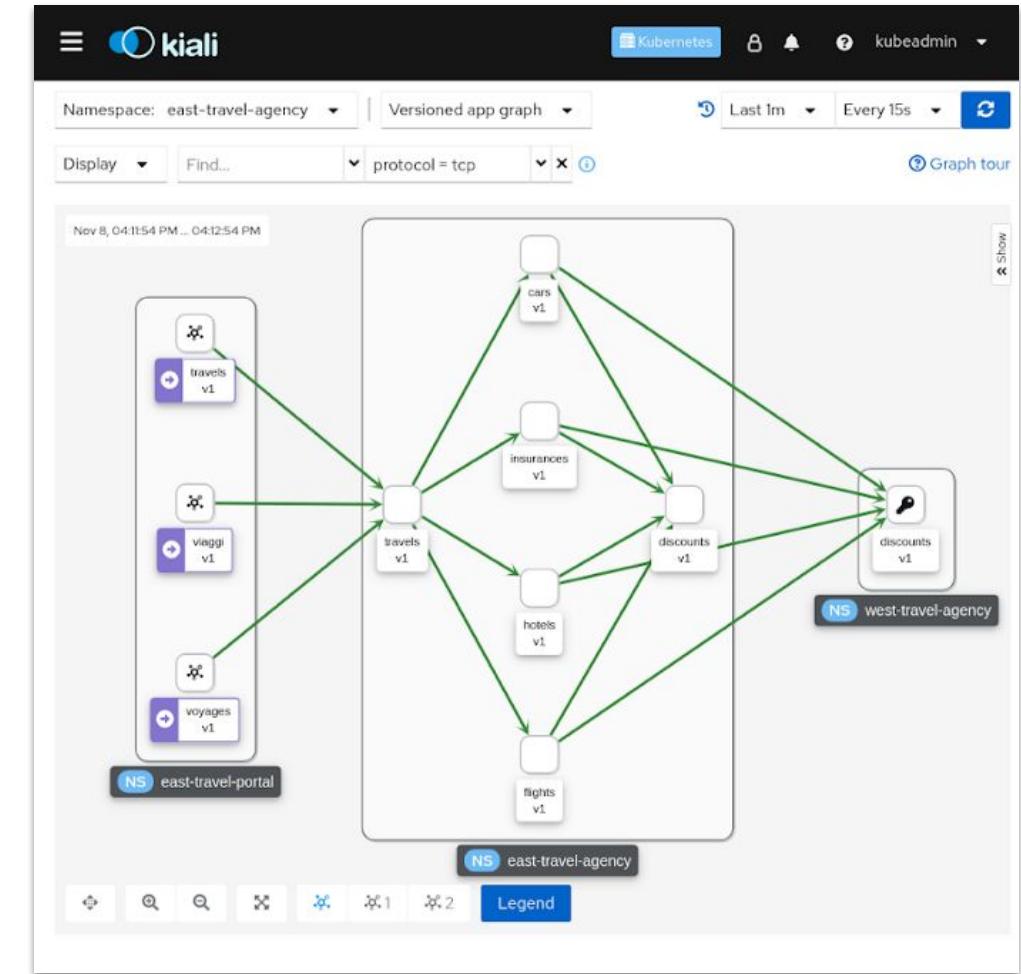
- ▶ Update to Knative 1.0
- ▶ Apache Kafka based Knative Broker (**Tech Preview**)
  - ▶ Maximises Kafka performance and avoids events duplications
  - ▶ Prevents tight coupling with Kafka and eliminated the use of Kafka client by event producers
- ▶ Knative Kafka Sink (**Tech Preview**)
  - ▶ Store CloudEvents from Source/Subscription/Trigger on a Kafka topic, without writing custom code
- ▶ Developer Experience:
  - ▶ Support for developing, debugging and testing EDA applications by sending CloudEvents via the kn CLI (**Tech Preview**)
  - ▶ Visualization of Event Sink on Dev Console
- ▶ Functions (**Tech Preview**)
  - ▶ Node.js, TypeScript, Quarkus, Python, Rust, Go & Spring Boot
  - ▶ Available on MacOS, RHEL, Windows with Docker and/or Podman
  - ▶ Local Development and Testing for quick iteration

## Event Sink & Event Source visualization



# OpenShift Service Mesh

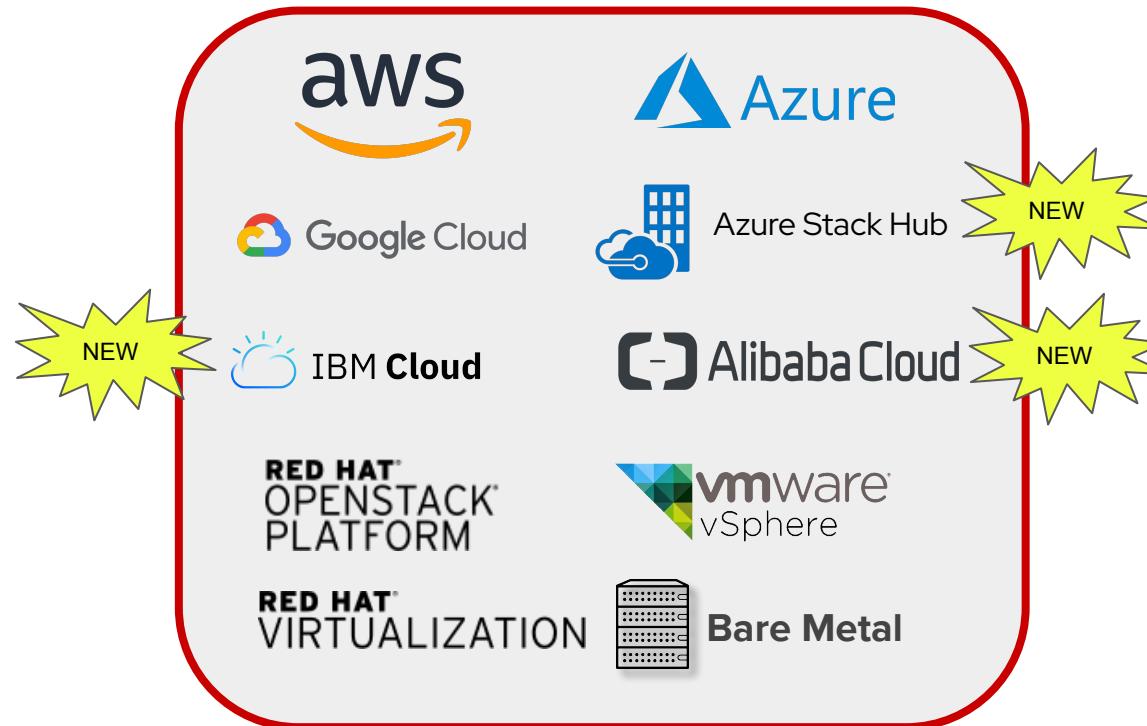
- ▶ OpenShift Service Mesh 2.2 (ETA: April 2022) will be based on **Istio 1.12** and **Kiali 1.47+**.
- ▶ Istio 1.12 introduces **WasmPlugin** API which will deprecate the ServiceMeshExtensions API introduced in 2.0.
- ▶ Service Mesh 2.1.1+ and 2.2 allows users to override and **customize Kubernetes NetworkPolicy creation**.
- ▶ Kiali updates in Service Mesh 2.2:
  - ▶ Enhancements to improve viewing and navigating large service meshes
  - ▶ View internal certificate information
  - ▶ Set Envoy proxy log levels
  - ▶ New [Service Mesh Federation](#) demo



# Installer Flexibility

# 4.10 Supported Providers

Full Stack Automation (IPI)



Pre-existing Infrastructure (UPI)



Generally Available



# Deploy OpenShift on IBM Cloud



## Installing a cluster using installer-provisioned infrastructure (IPI) on IBM Cloud

- ▶ Allows an OpenShift cluster to be deployed using **installer-provisioned infrastructure** on IBM Cloud VPC infrastructure
- ▶ Support to public clusters only with CIS (Cloud Internet Services DNS)
- ▶ **Private and disconnected** deployments available once IBM Cloud DNS Services are integrated in **future releases**

```
apiVersion: v1
baseDomain: example.com
controlPlane:
  hyperthreading: Enabled
  name: master
  platform:
    ibm-cloud: {}
    replicas: 3
  compute:
    - hyperthreading: Enabled
      name: worker
      platform:
        ibmcloud: {}
        replicas: 3
  metadata:
    name: test-cluster
  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:
    ibmcloud:
      region: us-south
  credentialsMode: Manual
  publish: External
  pullSecret: '{"auths": ...}'
  fips: false
  sshKey: ssh-ed25519 AAAA...
```

# Deploy OpenShift on Azure Stack Hub



## Installing a cluster using installer-provisioned infrastructure (IPI) on Azure Stack Hub

- ▶ Azure's solution to run applications in an **on-premises** environment and deliver **Azure services** in your data center
- ▶ Allows an OpenShift cluster to be deployed using **installer-provisioned infrastructure** on Azure Stack Hub
- ▶ Document enhancements to support deployments using **custom CAs**

```
apiVersion: v1
baseDomain: example.com
controlPlane:
  name: master
  replicas: 3
compute:
- name: worker
  platform: {}
  replicas: 0
metadata:
  name: ash-cluster
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:
    armEndpoint: azurestack_arm_endpoint
    baseDomainResourceGroupName: resource_group
    region: azure_stack_local_region
    resourceGroupName: existing_resource_group
    outboundType: Loadbalancer
    cloudName: AzureStackCloud
  pullSecret: '{"auths": ...}'
  fips: false
  sshKey: ssh-ed25519 AAAA...
```

# Deploy OpenShift on Alibaba Cloud



## Installing a cluster using installer-provisioned infrastructure (IPI) on Alibaba Cloud

- ▶ International portal includes world and china mainland
  - ▶ IPI does not support cn-nanjing (China (Nanjing) and UAE (Dubai))
- ▶ Fully connected installation with new and existing VPC

```

apiVersion: v1
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    alibabacloud:
      instanceType: ecs.g6.xlarge
      replicas: 3
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    alibabacloud:
      instanceType: ecs.g6.large
      replicas: 3
metadata:
  name: openshift-on-alibaba
platform:
  alibabacloud:
    region: us-east-1
    resourceGroupID: rg-aeck2wky7lxk4f5y
    vpcID: vpc-0xi6h9s2713tmqc5bpyhc
    vswitchIDs:
    - vsw-0xi183q0g3xqdmkhpgc93
    - vsw-0xi3nk4nu9366f623vtb9
pullSecret: HIDDEN
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  serviceNetwork:
  - 172.30.0.0/16
  machineNetwork:
  - cidr: 10.0.0.0/16
    networkType: OpenShiftSDN
  publish: Internal

```

# Thin provisioning support on VMware

Support for thin provisioned OS disks for OCP VMs in VMware vSphere IPI deployments

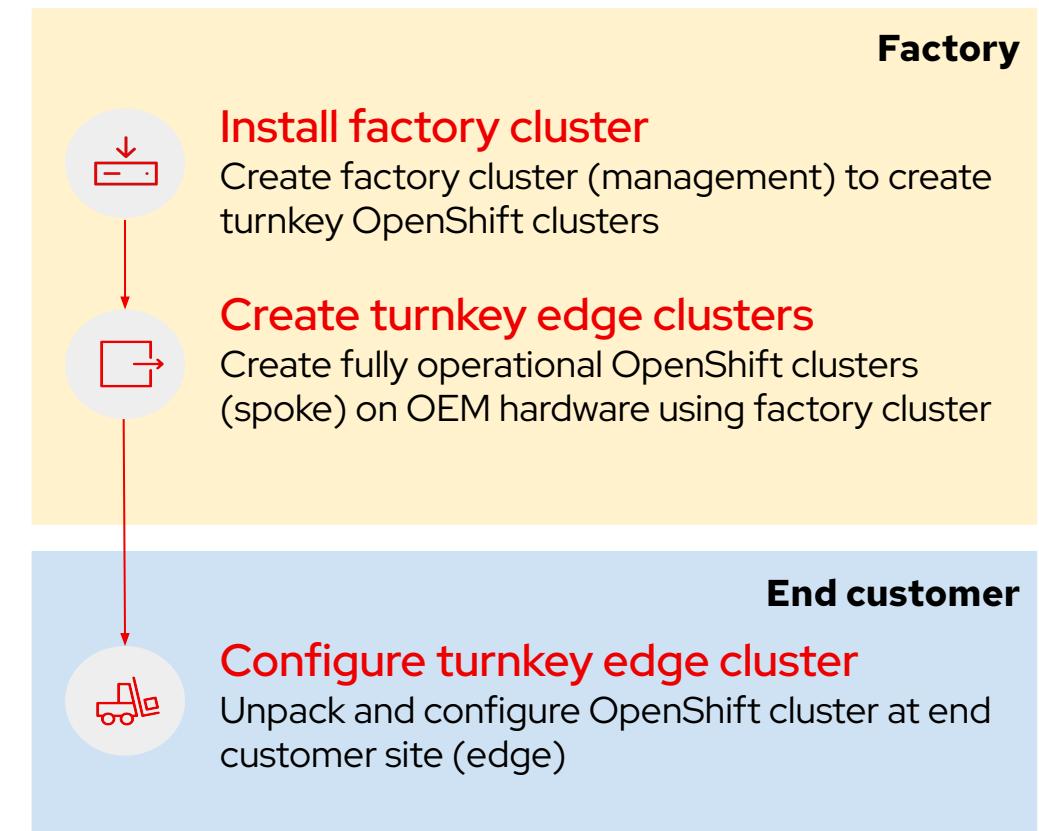
- ▶ Disk provisioning method for primary disks now includes '**thin**' in addition to 'thick' or 'eagerZeroedThick' using **installer-provisioned infrastructure (IPI)** on vSphere
- ▶ Thin provisioning only consumes space needed and grows over time based on demand
- ▶ NFS datastore is always thin

```
...  
...  
  
metadata:  
  name: cluster  
platform:  
  vsphere:  
    vcenter: your.vcenter.server  
    username: username  
    password: password  
    datacenter: datacenter  
    defaultDatastore: datastore  
    folder: folder  
    diskType: thin  
    network: VM_Network  
    cluster: vsphere_cluster_name  
    apiVIP: api_vip  
    ingressVIP: ingress_vip  
    fips: false  
    pullSecret: '{"auths": ...}'  
    sshKey: 'ssh-ed25519 AAAA...'
```

# Pre-install OpenShift at the Factory for OEMs

Build turnkey solutions with OpenShift

- ▶ Build **turnkey edge** solutions with OpenShift **pre-installed** on OEM hardware
- ▶ Leverages Zero Touch Provisioning (ZTP) to build a **factory pipeline** to deploy self-contained OpenShift clusters that can be **relocated** for edge deployments
- ▶ Document enhancements on how to deploy factory cluster (management cluster) and turnkey edge clusters



# Bare Metal Configuration

## Advanced Host Network Configuration at Install with IPI

- ▶ Insert config in install-config.yaml
- ▶ Per host “networkConfig” field,
- ▶ Configure static IP addresses, Bonds, VLANs
- ▶ DHCP not required

```
[...]
  hosts:
    - name: openshift-master-0
      networkConfig:
        routes:
          config:
            - destination: 0.0.0.0/0
              next-hop-address: 192.168.123.1
              next-hop-interface: enp0s4
        dns-resolver:
          config:
            server:
              - 192.168.123.1
        interfaces:
          - name: enp0s4
            type: ethernet
```

Both use NMState syntax: [nmstate.io/examples.html](https://nmstate.io/examples.html)

## Kubernetes NMState Operator is promoted to GA for bare metal

- ▶ Supported with OpenShift 4.10 for the bare metal platform
- ▶ Apply network changes on nodes on Day 2

```
apiVersion: nmstate.io/v1beta1
kind: NodeNetworkConfigurationPolicy
metadata:
  name: enp0s3-dns-policy
spec:
  nodeSelector:
    kubernetes.io/hostname: worker-0
  desiredState:
    dns-resolver:
      config:
        search:
          - example.com
        server:
          - 8.8.8.8
    interfaces:
      - name: enp0s3
```

## Update your hosts BIOS Settings

- ▶ New “hardware firmware settings” (hfs) and “firmwareschema” CRDs
- ▶ Retrieve available BIOS attributes from your bare metal hosts (bmh)
- ▶ Update BIOS attributes on Day 2

```
$ oc edit hfs/ostest-worker-0 -n
openshift-machine-api -o yaml
apiVersion: metal3.io/v1alpha1
kind: HostFirmwareSettings
[...]
spec:
  settings: {}
    EmbeddedSata: Ata
    ProcTurboMode: Enabled
[...]
```

# Control Plane Updates

# Conditional Updates

Evaluate risk before updating

- ▶ Update Service declares **conditionally recommended updates** associated with known risks
- ▶ Cluster Version Operator (CVO) **continually evaluates known risks** associated with updates
- ▶ Update recommended when no risks found

```
# View description of the update when it is not recommended because a risk might apply.  
$ oc adm upgrade --include-not-recommended  
  
# Evaluate for potential known risks and decide if acceptable for current cluster, then waive safety guards and proceed the update.  
# <version> is the supported but not recommended update version you obtained from the output of the previous command.  
$ oc adm upgrade --allow-not-recommended --to <version>
```

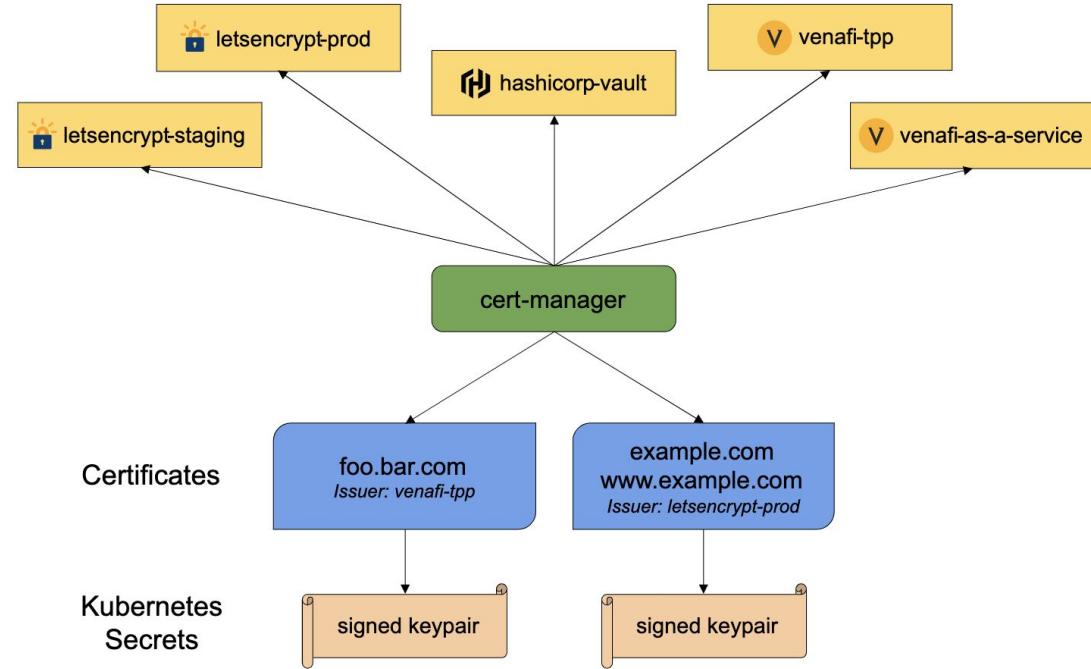
# cert-manager (Tech Preview)

## Automate certificate management in cloud native environments

[cert-manager](#) builds on top of Kubernetes, introducing certificate issuers authorities and certificates as first-class resource types in the Kubernetes API. This makes it possible to provide 'certificates as a service' to developers working within your Kubernetes cluster.

### Use Cases

- ▶ Provide easy to use tools to manage certificates.
- ▶ A standardised API for interacting with multiple certificate authorities (CAs).
- ▶ Gives security teams the confidence to allow developers to self-serve certificates.
- ▶ Support for ACME (Let's Encrypt), HashiCorp Vault, Venafi, self signed and internal certificate authorities.
- ▶ Extensible to support custom, internal or otherwise unsupported CAs.



### Latest Release (v1.7.1):

<https://github.com/cert-manager/cert-manager/releases/tag/v1.7.1>

# Syncing group membership from identity providers

## Connect Groups to RBAC

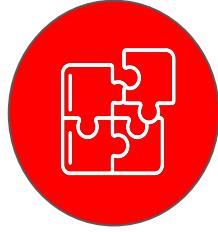
- ▶ 4.10 release introduces support for synchronizing group membership from an OpenID Connect provider to OpenShift Container Platform upon user login.
- ▶ You can enable this by configuring the groups claim in the OpenShift Container Platform OpenID Connect identity provider configuration.

```
apiVersion: config.openshift.io/v1
kind: OAuth
metadata:
  name: cluster
spec:
  identityProviders:
    - name: oidcidp
      mappingMethod: claim
      type: OpenID
      openID:
        clientID: ...
        clientSecret:
          name: idp-secret
      claims:
        preferredUsername:
          - preferred_username
        name:
          - name
        groups:
          - groups
      issuer: https://www.idp-issuer.com
```

# Management & Security

# Red Hat streamlines Kubernetes Security programs

## Red Hat Advanced Cluster Security



Developer workflows



Security Notifications



<sup>38</sup> Enhanced Administration

1

**Enable developers to streamline risk management** by marking vulnerabilities as false positives or accept risk with an in product request and approval workflow.

2

**Simplified issue prioritization and remediation in CI** with additional vulnerability output and summaries of policies responsible for breaking builds.

3

**Shorten feedback loops** with automated, scheduled reporting of vulnerabilities to the remediation stakeholders.

4

**Runtime notification enhancements** send additional details to system notifiers and SIEMs about the timelines of runtime policy violations and risks.

5

**Simplify administration of OpenShift Platform Plus** by allowing the re-use of OpenShift OAuth authentication for ACS users.

6

**Enable scalable registry integration** with Amazon Elastic Container Registry by leveraging IAM AssumeRole for authorization at scale.

# Red Hat Advanced Cluster Management for Kubernetes

## What's new in RHACM 2.5

**Better Together**

Red Hat Advanced Cluster Management brings together Ansible and OpenShift Platform Plus, including OpenShift GitOps, Red Hat Advanced Cluster Security, Red Hat OpenShift Data Foundation across cloud vendors all from a single-pane of glass.

- ▶ **RHACM cluster inventory available in Ansible Automation Platform (Dev Preview)**: Access ACM functionality, such as cluster creation, directly from Ansible Automation Platform using the Ansible collections.
- ▶ **Support for OpenShift GitOps ApplicationSets**: Easily create ArgoCD ApplicationSets directly from RHACM.
- ▶ **Stronger security**: Gatekeeper Mutating Webhooks can change resources upon admission, while variable templating provides improved secrets management integration.
- ▶ **RHACS Integration**: Provide PolicySets for ACS and OpenShift+ Integration



# Red Hat Advanced Cluster Management for Kubernetes

## What's new in RHACM 2.5

### Manage OpenShift Everywhere

Meeting the needs of customers across all sectors, whether on premise with Red Hat Virtualization, bare metal, or in the cloud with AWS GovCloud (US).

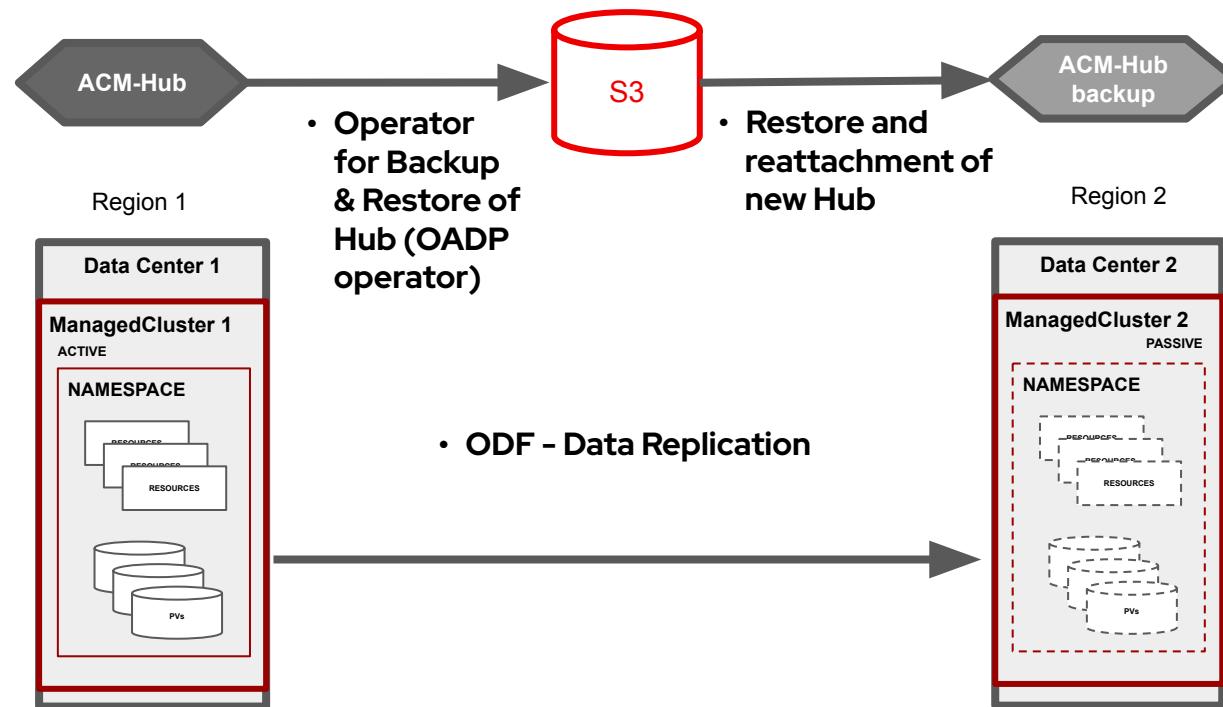
The screenshot shows the 'Create cluster' wizard in the Red Hat Advanced Cluster Management interface. The left sidebar includes sections for Cluster Management, Home, Infrastructure (Clusters, Bare metal assets, Automation, Infrastructure environments), Applications, Governance, and Credentials. The main area shows the 'Clusters > Create cluster' path. The 'Create cluster' step is selected, with a 'YAML: On' toggle. The 'Installation type' section lists infrastructure providers: aws, Google Cloud, Microsoft Azure, VMware vSphere, Bare metal, and Red Hat OpenStack Platform. The 'Red Hat Virtualization' option under 'Assisted installation' is highlighted with a red box.

- ▶ **Cluster lifecycle:** New provider support for OCP on Red Hat Virtualization and AWS GovCloud (US).
- ▶ **Arm architecture (Tech Preview):** Deploy an ACM hub on Arm, as well as import and manage OpenShift clusters leveraging Arm for low power consumption.
- ▶ **HyperShift (Tech Preview):** Host and provision containerized OpenShift control planes at scale, reducing cost, hardware footprint, and time to provision.
- ▶ **Central Infrastructure Management (GA):** Provides a self-service model that easily allows infrastructure owners to enable developers access to bare metal hosts for OCP cluster provisioning.

# Red Hat Advanced Cluster Management for Kubernetes

## What's new in RHACM 2.5

### Business Continuity



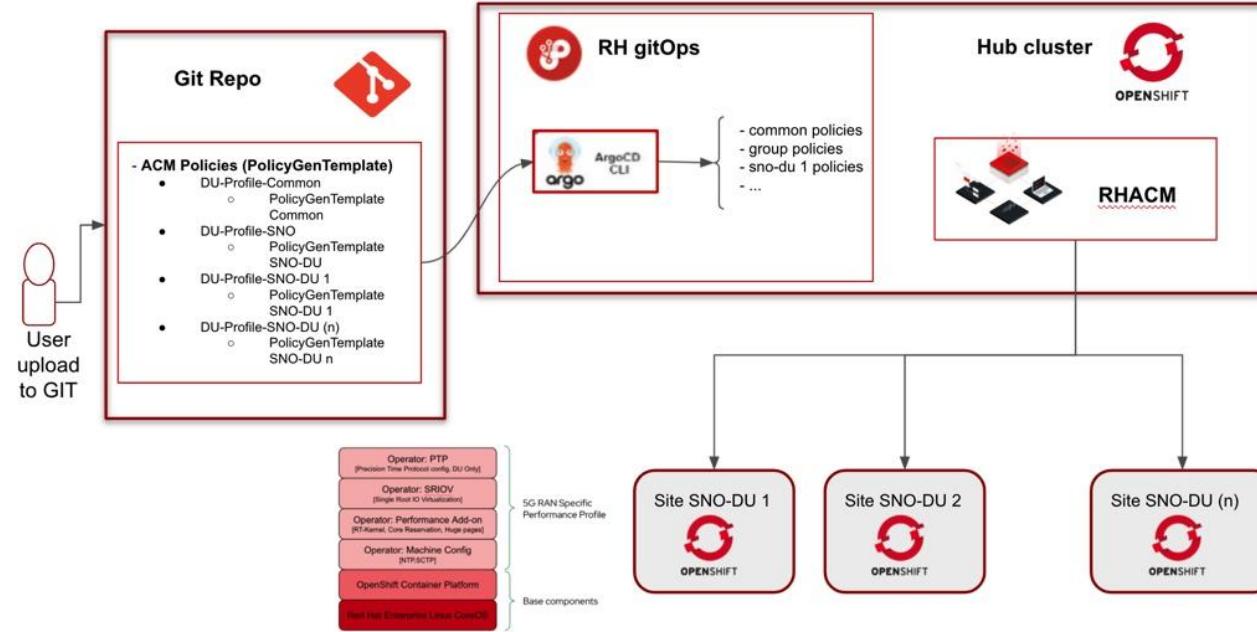
Users expect centralized management to provide support for disaster recovery scenarios, without the need for additional tooling.

- ▶ **Hub backup and restore (GA):** Using OpenShift API for Data Protection (OADP operator), managed cluster configurations can be backed up and restored to a different hub cluster.
- ▶ **Application DR (Tech Preview):** Application Disaster Recovery capabilities using Red Hat OpenShift Data Foundation (ODF) across two distinct OCP clusters separated by distance.

# Red Hat Advanced Cluster Management for Kubernetes

## What's new in RHACM 2.5

### Manage At the Edge



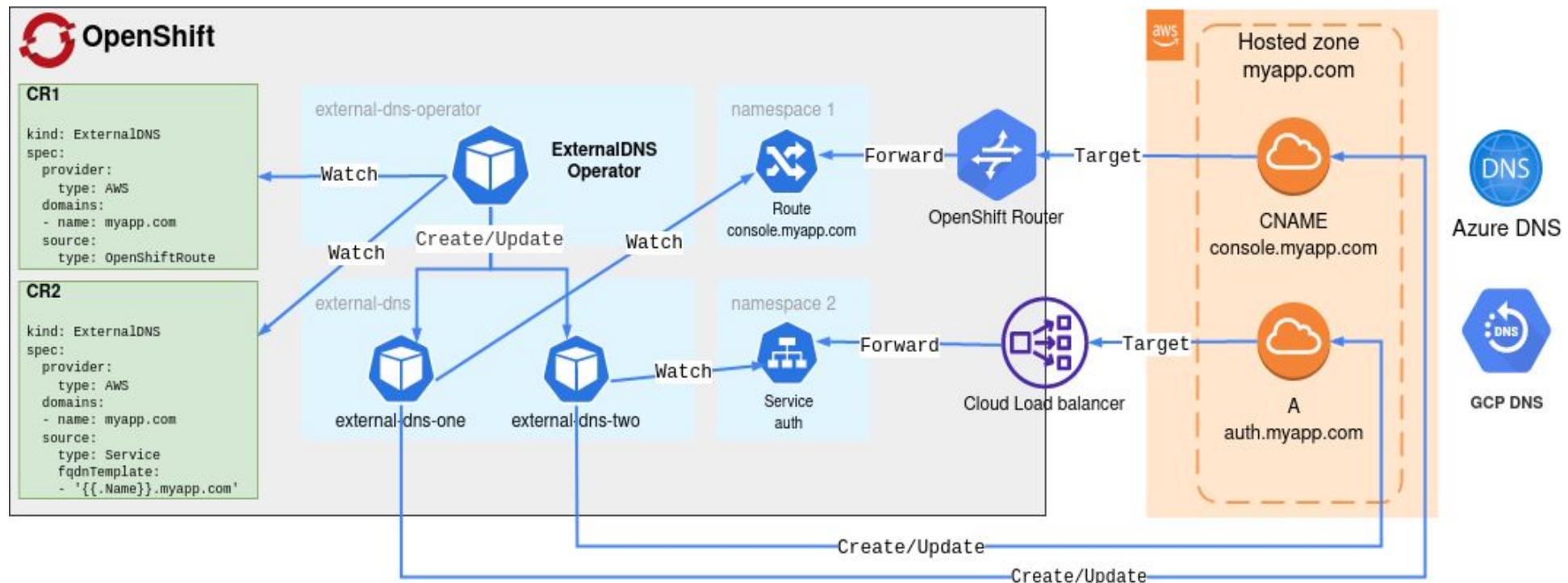
At Red Hat, we see edge computing as an opportunity to extend the open hybrid cloud all the way to the data sources and end users. Edge is a strategy to deliver insights and experiences at the moment they're needed.

- ▶ **Deploy & manage 2000 SNO (GA):** Support DU profile delivery with ACM in IPv6 connected and disconnected scenarios.
- ▶ **Export hub collected metrics to external tools:** Operations teams can integrate metrics collected from their Kubernetes clusters with metrics collected from other IT sources for a holistic view in their preferred tooling.
- ▶ **Policy Enhancements:** The PolicyGenerator simplifies distribution of Kubernetes resource objects to managed clusters, while improvements in the policy user experience help users perform fleet compliance.

# Networking & Routing

# External DNS Operator (Tech Preview)

- ▶ Provide the ability to dynamically control DNS records of an external DNS server via Kubernetes resources in a DNS provider-agnostic way.
- ▶ The feature makes use of an operator that will be deployed via the OperatorHub to manage the upstream external-dns functionality
- ▶ Supported cloud providers include AWS, GCP and Azure (Tech Preview)



# General Networking Enhancements

## Egress traffic steering

### Egress IP address support for clusters installed on public clouds

- ▶ For OVN-K and OpenShift SDN cluster network providers on
  - ▶ Amazon Web services
  - ▶ Google Cloud Platform
  - ▶ Microsoft Azure

```
IP capacity = public cloud default capacity -  
sum(current IP assignments)
```

## MTU

### Modify Cluster Network MTU post installation

```
oc patch Network.operator.openshift.io cluster  
--type=merge --patch \  
'{"spec": { "migration": null, "defaultNetwork":{  
"ovnKubernetesConfig": { "mtu": <mtu> }}}}'
```

## Hardware Enablement

### SR-IOV support for

- ▶ Intel Columbiaville E810
  - ▶ E810-CQDA2
  - ▶ E810-2CQDA2
  - ▶ E810-XXVDA2
  - ▶ E810-XXVDA4
- ▶ Broadcom
  - ▶ BCM57414 & BCM57508

# Virtualization

# OpenShift Virtualization

Modernized workloads, support composite applications with VMs, containers, and serverless

## Enhanced Data Protection

- ▶ VM backup and restore built into OADP
- ▶ Disaster recovery workflows coordinated through ACM

## Additional Deployment Options

- ▶ Small footprint in resource constrained deployments e.g. SNO
- ▶ IBM Public Cloud Bare Metal ([Tech Preview](#))

## Operational Enhancements

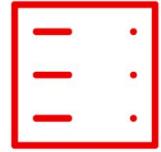
- ▶ Composite applications (container & VM) in same Service Mesh
- ▶ Enhanced Virtual Machine Workflow Management

## Workload Acceleration

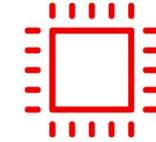
- ▶ Accelerate compute and 3D apps with shared vGPU resources



Telco  
a path to k8s



Modernize with  
composite apps



Accelerate  
compute workloads



Compact clusters  
at the edge



cloud-native VMs

"Red Hat technology stands out from the competition in terms of its ability to run virtualized workloads and container workloads in a streamlined and well-integrated manner. Red Hat allows us to deliver value to our users more quickly, minimizing time to market and accelerating the software development lifecycle."

Gökhan Ergül  
CTO,  
[sahibinden.com](http://sahibinden.com)

**sahibinden.com**

# VM lift-and-shift to OpenShift

## Migration Toolkit for Virtualization 2.3

MTV 2.3 is adding **warm migration** capabilities for both VMware and RHV to OpenShift Virtualization

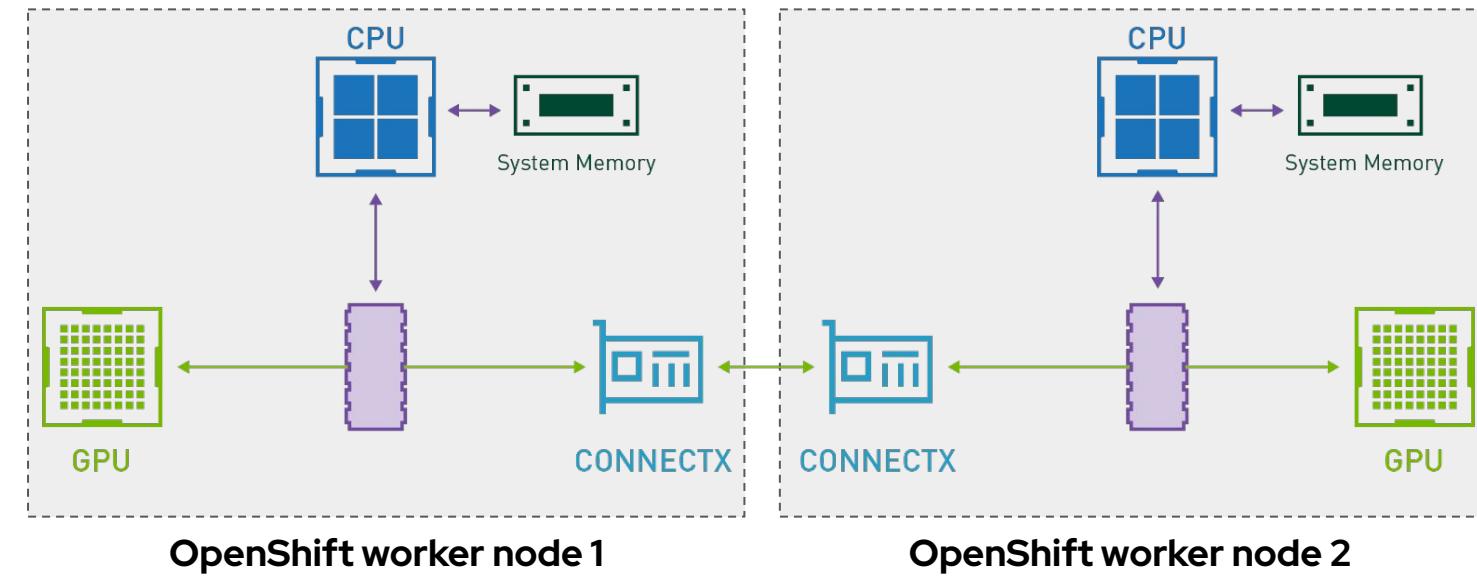
*Warm migration reduced the amount of downtime by pre-copying the data from disks before the final shutdown and reboot of your VM on the destination platform.*

Name	Source provider	Target provider	VMs	Plan status
planteast-1 my first plan	vcenter-1	ocpv-1	2	Running 0 of 2 VMs migrated
planteast-2 my 2nd plan	vcenter-1	ocpv-1	1	Ready

# Specialized Workloads

# Distributed deep learning training with GPUs

- ▶ NVIDIA DGX A100 server: OpenShift deployment and NVIDIA GPU operator enablement
- ▶ GPU utilization in the OpenShift Console
- ▶ vGPUs simplified enablement with the Driver Toolkit
- ▶ Distributed deep learning training enabled by the NVIDIA Network Operator and GPUDirect RDMA (**Tech Preview**)
- ▶ OpenShift NVIDIA GPU Operator on ARM systems (**Tech Preview**)
- ▶ OpenShift Virtualization vGPU enablement (**Tech Preview**)

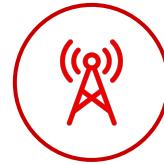


# Multi-architecture: IBM Power and IBM Z



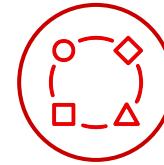
## Security

- ▶ Enhance data security from email communications to website access, transparently, with no changes to your applications
- ▶ Describe compliance state and provide an overview of gaps and remediation
- ▶ OVNKube IPSec support
- ▶ Compliance Operator



## Networking

- ▶ More tools/options in your networking stack so you can meet your user and workflow needs
- ▶ Multus Plugins
  - IPVLAN
  - Host Device
  - Bridge
  - Static IPAM



## Flexibility

- ▶ Respond to rise and fall in demand automatically, be agile and improve end user experience
- ▶ Vertical Pod Autoscaler
- ▶ Horizontal Pod Memory Autoscaling ([Tech Preview](#))

# Operator Framework

# Operator SDK Enhancements

Operator Maturity increased via custom Helm reconciler, exposing metrics, and advanced capabilities



## Hybrid Helm Operator SDK plugin (Tech Preview)

- ▶ Jump start an Operator with **Helm Chart** and add advanced / event-based Ops logics to Helm reconciler in **Go**.
- ▶ Continue adding new APIs/CRDs in the same project in **Go**.

```
$ operator-sdk init --plugins hybrid.helm.sdk.operatorframework.io \
--project-version="3" --repo github.com/example/memcached-operator

$ operator-sdk create api --plugins helm.sdk.operatorframework.io/v1 \
--group cache --version v1alpha1 --kind Memcached

$ operator-sdk create api --plugins=go/v3 \
--group cache --version v1 --kind MemcachedBackup --resource --controller
```



## Digest-based bundle (for disconnected env)

- ▶ Easily package Operator project into an Operator bundle that works in the **disconnected environment** with the OLM.

```
$ make bundle USE_IMAGE_DIGESTS=true
```



## Resource pruning for Operator created objects

- ▶ A common library that helps enable Operators to prune/delete cluster objects in GVK per customized strategies or hooks.

```
cfg = Config {
    log:          logf.Log.WithName("prune"),
    DryRun:       false,
    Clientset:   client,
    LabelSelector: "app=churro",
    Resources: []schema.GroupVersionKind {
        {Group: "", Version: "", Kind: JobKind},
    },
    Namespaces: []string {"churro-namespace"},
    Strategy: StrategyConfig {
        Mode:           MaxCountStrategy,
        MaxCountSetting: 10,
    },
    PreDeleteHook: myhook,
}
```

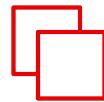


## Enable Ansible Operator insight (capability level IV)

- ▶ Ansible Operator SDK supports exposing custom metrics, emitting k8s events, and better logging.



# Operator Lifecycle Management Enhancements



## Support for Hypershift

OLM components including the catalogs run entirely on the Hypershift-managed control plane and doesn't incur any cost to tenants on worker nodes.



## Support for extremely dense clusters

Operator availability projection (CSV copying) can become resource intensive on clusters with large number of namespaces (>1000). There is now a switch to disable that.



## Fine-grained dependencies

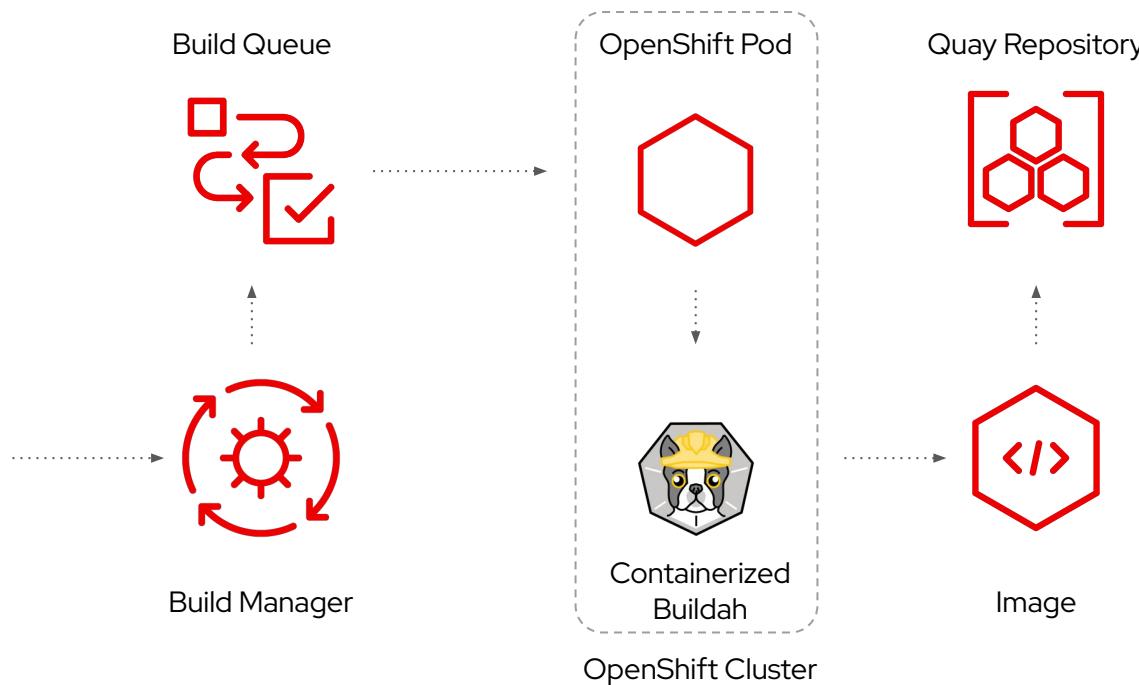
Operators with very specific dependency needs can now use complex constraints / requirements expressions

```
schema: olm.bundle
name: baz.v1.0.0
properties:
- type: olm.constraint
  value:
    failureMessage: All are required for Baz because...
  all:
    constraints:
      - failureMessage: Package bar is needed for...
        package:
          name: bar
          versionRange: '>=1.0.0'
      - failureMessage: GVK Buf/v1 is needed for...
        gvk:
          group: bufs.example.com
          version: v1
          kind: Buf
```

# Quay

# Quay Builds via podman

Builds on OCP clusters

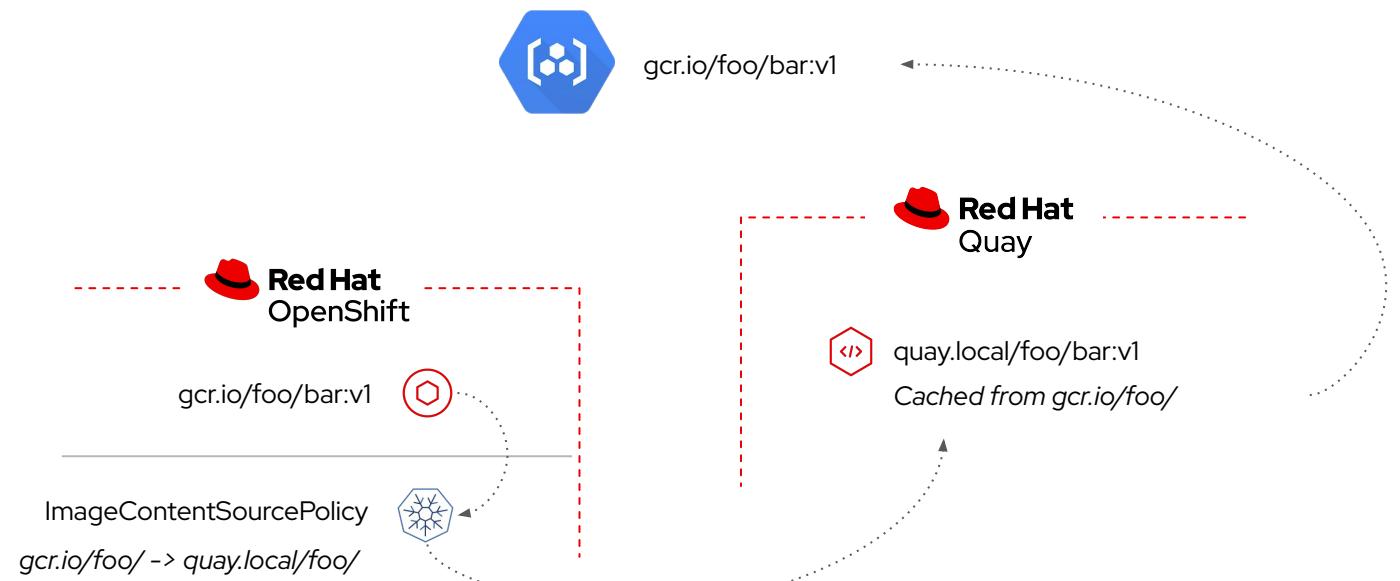


- ▶ Builds images triggered by code commits, avoid credential leakage in external CI
- ▶ Quay container builds trigger containerized build jobs, no qemu usage anymore (<= Quay 3.6)
- ▶ Builds execute on the same OCP cluster Quay is running on or a remote cluster, no external VMs or OCP on bare-metal required
- ▶ 3.7: configured via the Quay config file
- ▶ 3.8: managed by the Quay Operator
- ▶ *Future:*
  - multi-arch builds
  - Builds using OpenShift Pipelines

# Quay Pull-Through Cache Proxy

Serving multiple organizations and multiple cluster switch efficiency

- ▶ Transparent pull-thru caching for all registry clients
- ▶ Central Quay instance acts as a pull-cache for upstream registries
- ▶ Selectively enabled in Quay and OpenShift, allows to disable direct access to untrusted public registries
- ▶ Moderates and accelerates access to trusted upstream registries
- ▶ Cache size will be configurable



This workflow describes future state and depends on OpenShift support coming around 4.12 ([OCPNODE-521](#))

# Quay Quota Management

Manage storage consumption growth by setting limits

The screenshot shows the Quay interface. On the left is a sidebar with icons for Organization, Namespace, Avatar, Delete organization, Time Machine, Quota Management, and Settings. The main area has tabs for EXPLORE, REPOSITORIES (which is selected), and TUTORIAL. The REPOSITORIES tab shows a table of repositories with columns: REPOSITORY NAME, LAST MODIFIED, and QUOTA CONSUMED. Below the table is a section for Quota Management where an organization quota of 1000 bytes is set, with options for Warning and Reject thresholds.

REPOSITORY NAME	LAST MODIFIED	QUOTA CONSUMED
temporg / postgres	Today at 1:58 AM	132.5 MB
temporg / redis	Today at 2:44 AM	41.1 MB
temporg / alpine	Today at 3:42 AM	2.8 MB
temporg / keycloak	Today at 3:40 AM	407.6 MB
temporg / busybox	Today at 3:41 AM	2.6 MB
temporg / ubuntu	Today at 3:43 AM	28.6 MB
temporg / mysql	Today at 3:44 AM	154.0 MB
temporg / nginx	Today at 3:48 AM	67.9 MB
temporg / registry	Today at 3:48 AM	9.2 MB

**Quota Management:**

- Set Organization quota (bytes): 1000
- + Add Quota Limit
- Warning (selected)
- Reject
- Warning
- Save Quota Details

- ▶ Prevents unbound storage growth in multi-tenant registries
- ▶ Image Storage Quota for organizations in Quay
- ▶ Customizable threshold behavior
  - Soft quota: warning messages
  - Hard quota: pushes are rejected
- ▶ Cluster-wide default quota for all new organizations enforceable by administrators
- ▶ Organization-level consumption tracking by tenants
- ▶ Registry-level consumption tracking by administrators

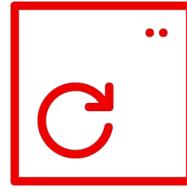
# Storage

# OpenShift Storage - Journey to CSI

- ▶ CSI Operators – pluggable, built-in upgrade, storage integration
  - ▶ vSphere (**GA**)
  - ▶ AWS EFS (**GA**)
  - ▶ IBM Cloud (**GA**)
  - ▶ AliCloud disk (**GA**)
  - ▶ Azure Disk (**GA**)
  - ▶ Azure File (**Tech Preview**)
- ▶ CSI Migration – allow easy move from using existing intree drivers to new CSI drivers
  - ▶ vSphere (**Tech Preview**)
  - ▶ Azure File (**Tech Preview**)
- ▶ Operator/CSI are automatically deployed at installation or after upgrades
- ▶ In-tree storage class remains **default** until CSI migration goes GA

CSI Operators		
Operator target	Migration	Driver
AliCloud Disk	n/a	GA (New in 4.10)
AWS EBS	Tech Preview	GA
AWS EFS	n/a	GA (New in 4.10)
Azure Disk	Tech Preview	GA (New in 4.10)
Azure File	Tech Preview	Tech Preview
Azure Stack Hub	n/a	GA
GCE Disk	Tech Preview	GA
IBM Cloud	n/a	GA (New in 4.10)
RH-OSP Cinder	Tech Preview	GA
vSphere	Tech Preview	GA (New in 4.10)

# OCP 4.10 vSphere CSI Journey

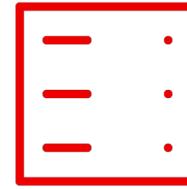


## VM Hardware version 15

vSphere CSI requires VMware

### Virtual Machine hardware version 15.

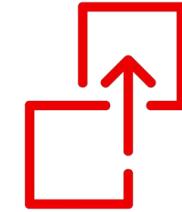
Make sure the OCP VMs are  
running HW version 15 or  
greater.



## vSphere >= v6.7U3

Virtual Machine Hardware v15  
depends on **vSphere v6.7U3 or  
greater.**

Make sure the cluster is running  
on a vSphere version that  
supports VM Hardware version  
15.



## Third Party CSI

OCP **can't run two versions of the  
CSI driver** at the same time.

If another vSphere CSI driver is  
present, remove it from the cluster  
after upgrading to 4.10.

(Red Hat vSphere CSI installation  
will automatically resume with no  
dataplane downtime nor dataloss)

OCP 4.10 clusters that don't meet these requirements **will be marked unupgradable.**  
Fix the issue to automatically resume the CSI driver deployment.

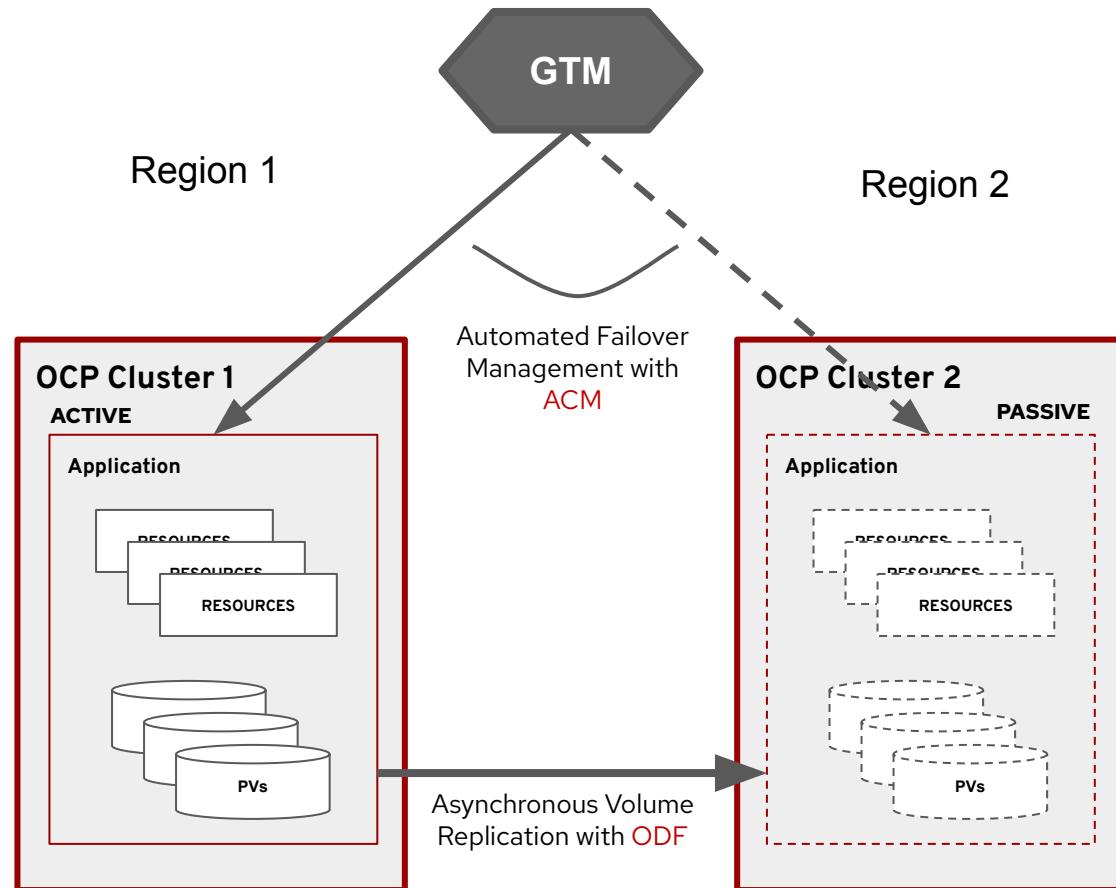
Regional-DR

RPO – Mins

RTO – Mins

# ODF 4.10 and ACM 2.5 – Regional-DR with Failover

Protection against Geographic Scale Disasters  
Automation



- ▶ Asynchronous Volume Replication => low RPO
  - ODF enables cross cluster replication of data volumes with replication intervals as low as 1 min
  - ODF Storage operators synchronizes both App data PVs and Cluster metadata
- ▶ Automated Failover Management => low RTO
  - ACM Multi-Cluster manager enables failover and fallback automation at application granularity
- ▶ Both clusters remain active with Apps distributed and protected among them

# Other OpenShift Data Foundation 4.10 updates

- Cluster wide encryption with Service Account
- AWS gp3/gp2 csi support as backing storage
- MCG support for namespace on top of filesystem
- Tech Preview
  - Dynamic storage for Single Node OpenShift, initial target is Telco RAN

Out of the box support	
Block, File, Object	
Platforms	
AWS/Azure	Google Cloud (Tech Preview)
ARO - Self managed OCS	IBM ROKS & Satellite - Managed ODF (GA)
RHV	OSP (Tech Preview)
Bare metal/IBM Z/Power	VMWare Thin/Thick IPI/UPI
Deployment modes	
Disconnected environment and Proxied environments	

# Observability

# Summary Enhancement for OpenShift 4.10 Monitoring

## Prometheus Audit Logging Enhancements

### Updated OpenShift Audit Logging for Metrics:

- ▶ New Support for enabling Audit Logging in Prometheus Adapter:
  - ▶ Ability to Observe which component are requesting calling the metrics API
  - ▶ Enables customers to monitor and troubleshoot performance problems via API audit capability
- ▶ Enable Query Logging in all Prometheus Instances:
  - ▶ Platform Monitoring & User Workload Monitoring
  - ▶ Use ThanosQuerier to see which query is frequently executed and the impact to operations

The following profiles are provided which corresponds to [Audit Log Levels](#)

- Request
- RequestResponse
- None
- *Metadata* (the default audit profile)

User can pick any of the profile by modifying the CMO configmap as follows

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml: |
    k8sPrometheusAdapter:
      audit:
        profile: Request
```

CMO picks up the change and (re)deploys `prometheus-adapter` with appropriate `--audit-` flags.

# Summary Enhancement for OpenShift 4.10 Monitoring

*Prometheus Logging & Certificate Capabilities - Improves the reliability of metrics collection*

- ▶ Client Certificate Authentication for Scraping Metrics: (Enable Prometheus to use Client Authentication)
  - ▶ For scraping metrics to reduce performance impacts on authentication APIs.
  - ▶ Provides consistency with Global OpenShift Security Configurations.
  - ▶ Prometheus is able to authenticate using TLS certificates instead of bearer tokens when scraping metrics.

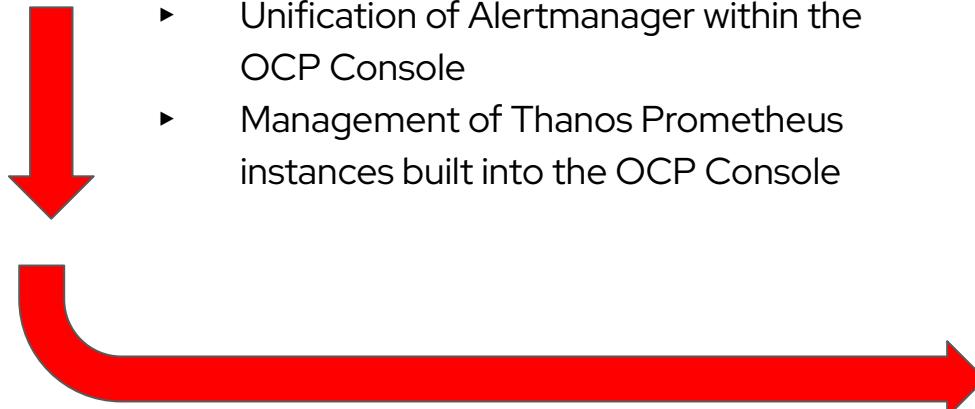
```
# token=`oc sa get-token prometheus-k8s -n openshift-monitoring`  
# oc -n openshift-monitoring exec -c prometheus prometheus-k8s-0 -- curl -k -H "Authorization: Bearer $token"  
Unauthorized  
  
# token=`oc -n openshift-user-workload-monitoring sa get-token prometheus-user-workload`  
# oc -n openshift-monitoring exec -c prometheus prometheus-k8s-0 -- curl -k -H "Authorization: Bearer $token"  
Unauthorized  
  
# token=`oc sa get-token prometheus-k8s -n openshift-monitoring`  
# oc -n openshift-monitoring exec -c prometheus prometheus-k8s-0 -- curl -k -H "Authorization: Bearer $token"  
# HELP go_gc_duration_seconds A summary of the pause duration of garbage collection cycles.  
# TYPE go_gc_duration_seconds summary  
go_gc_duration_seconds{quantile="0"} 2.4802e-05  
go_gc_duration_seconds{quantile="0.25"} 9.8683e-05  
go_gc_duration_seconds{quantile="0.5"} 0.000125406  
go_gc_duration_seconds{quantile="0.75"} 0.000145902  
go_gc_duration_seconds{quantile="1"} 0.004148246  
go_gc_duration_seconds_sum 0.035471605  
go_gc_duration_seconds_count 201
```

- ▶ **OpenShift Monitoring Component Updates:**
  - ▶ Alertmanager 0.23.0
  - ▶ Grafana 8.3.4
  - ▶ kube-state-metrics v2.3.0
  - ▶ node-exporter 1.3.1
  - ▶ prom-label-proxy 0.4.0
  - ▶ Prometheus 2.32.1
  - ▶ Prometheus adapter 0.9.1
  - ▶ Prometheus operator 0.53.1
  - ▶ Thanos 0.23.1

# Improved OpenShift Monitoring UI Experience

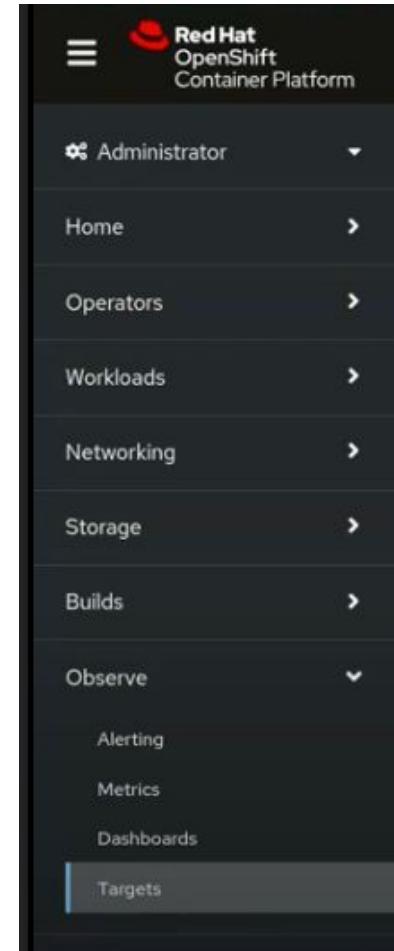
## New OpenShift Console Monitoring Experience:

- ▶ Console Monitoring User Interface Enhancements to Observe OpenShift:
  - ▶ Unification of Alertmanager within the OCP Console
  - ▶ Management of Thanos Prometheus instances built into the OCP Console

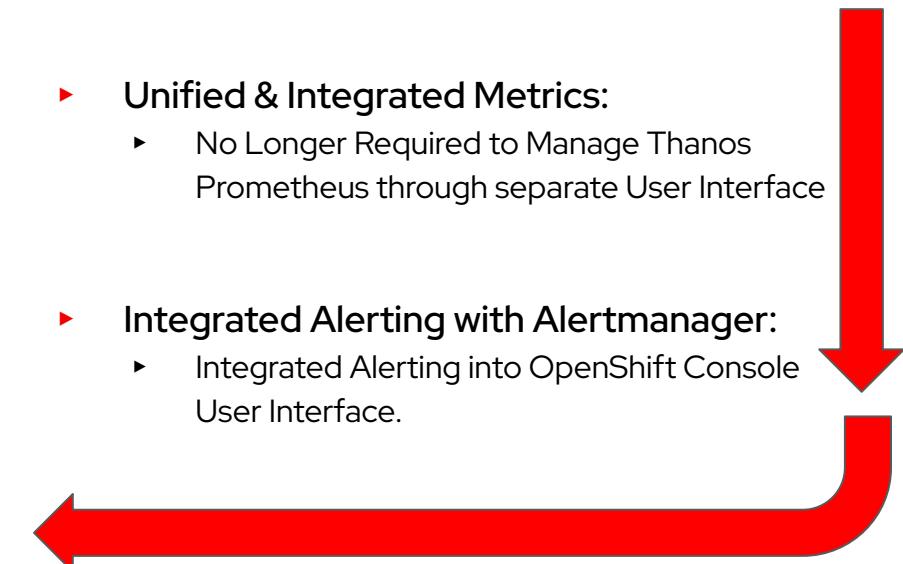


### Note:

Thanos and Alertmanager user interfaces previously used for external management have been deprecated in OpenShift 4.10



- ▶ Unified & Integrated Metrics:
  - ▶ No Longer Required to Manage Thanos Prometheus through separate User Interface
- ▶ Integrated Alerting with Alertmanager:
  - ▶ Integrated Alerting into OpenShift Console User Interface.
- ▶ Unified & Integrated Support:
  - ▶ Simplifying the End-to-End Monitoring Experience with Red Hat Support vs. 3rd Party



# Improved OpenShift Monitoring UI Experience

## New Prometheus Targets Endpoints Provided within the OpenShift Console:

- ▶ Ability to set “Target Endpoints” for monitoring and scraping metrics for infrastructure or services.
  - ▶ Single Administrative view and Management
  - ▶ Federated Targets API in Thanos + Allows both Platform and User Defined Workload Monitoring

**Observe Menu**

+  
Alerting, Metrics, Dashboards, &  
Targets

**Metrics Targets &  
Scrape Endpoints**

Red Hat OpenShift Container Platform

kube:admin ▾

Administrator

Home ▾

Operators ▾

Workloads ▾

Networking ▾

Storage ▾

Builds ▾

Observe ▾

Alerting

Metrics

Dashboards

Targets

You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.

Metrics Targets

Filter ▾ Text ▾ Search by endpoint or namespace... ▾

Endpoint	Monitor	Status	Namespace	Last Scrape	Scrape Durati...
http://10.0.0.3:9537/metrics	SM kubelet	Up	NS kube-system	Just now	3.9 ms
http://10.0.0.4:9537/metrics	SM kubelet	Up	NS kube-system	Just now	4.0 ms
http://10.0.0.5:9537/metrics	SM kubelet	Up	NS kube-system	Just now	3.7 ms
http://10.0.128.2:9537/metrics	SM kubelet	Up	NS kube-system	Just now	2.9 ms
http://10.0.128.3:9537/metrics	SM kubelet	Up	NS kube-system	Just now	3.3 ms
http://10.0.128.4:9537/metrics	SM kubelet	Up	NS kube-system	Just now	3.0 ms
http://10.128.2.25:8080/metrics	SM prometheus-example-monitor	Up	NS ns1	Just now	2.1 ms
http://10.128.2.25:8081/metrics	SM prometheus-example-monitor-wrong-port	Down	NS ns1	Just now	0.8 ms

# Logging 5.4 for OpenShift 4.10

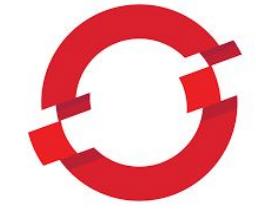
Tech Preview

## *Interoperable with Elasticsearch*

### *Loki & OpenShift (Day 1) Experience:*

- ▶ Ability to install, update, and manage a cluster with an alternative, scalable and performing log store
- ▶ Ability to deploy and manage Loki operator for OpenShift In-Cluster Log Configuration Management

## *On-Demand Queries In Milliseconds*



OPENSHIFT

## *Multi-Cloud Extensible Framework*

## *Multi-Tenancy Log Aggregation*

## *API Extensible Logging Architecture*

## *Log Exploration*

### *Loki & OpenShift (Day 2) Experience:*

- ▶ Substantial performance & scale over Elasticsearch Log Storage
- ▶ Loki is Highly Scalable and provides Multi-Tenancy Capability for evaluating OpenShift Multicloud Log Correlation & Exploration

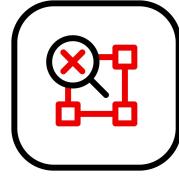
## *Supported Operator Framework*

## *High Scale & Performance (Loki + Vector)*

**Red Hat Multi-Cloud Scalable Logging Stack Evolution  
(Elasticsearch to Loki Tech Preview Journey)**

# Distributed Tracing

Saving costs and time with Distributed Scenarios

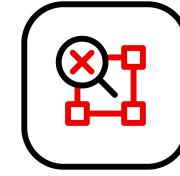


Red Hat OpenShift  
**distributed tracing**  
Platform

(based on Jaeger)

- ▶ Based on Jaeger 1.29
- ▶ Added in-memory storage support for adaptive sampling
- ▶ Added OpenTelemetry Protocol (OLTP) to the Query Service
- ▶ Includes rolling updates to the documentation to support the name change and new features

Tech Preview



Red Hat OpenShift  
**distributed tracing**  
Data Collection

(based on OpenTelemetry Collector)

- ▶ Based on OpenTelemetry Collector 0.41
- ▶ Available through Red Hat distributed tracing Data Collection Operator
- ▶ It can act as an agent to work side-by-side with the application for offloading
- ▶ It can act as Gateway to connect applications with legacy instrumentation to different backends
- ▶ Capability to export telemetry data leveraging OpenTelemetry Protocol (OLTP)

# Insights Advisor for OpenShift

- ▶ **New Insights Advisor!**
  - ▶ Account level view on all recommendations
  - ▶ Clusters affected by a recommendation
- ▶ **On-boarding tour** to walk you thru all new features (hit the *bulb* icon)
- ▶ **Advisor Recommendations** offered when opening a support case
- ▶ **Support Status**
  - ▶ Quickly identify the cluster support level
  - ▶ Eval Expiration Countdown
- ▶ **GA of Simple Content Access** (see other slides)

The screenshot shows the OpenShift Insights Advisor interface. On the left is a sidebar with links: Clusters, Overview, Releases, Downloads, Insights (highlighted), New service, Advisor (selected), Recommendations (highlighted with a red box), Clusters, Subscriptions, Cost Management, Support Cases, Cluster Manager Feedback, Red Hat Marketplace, and Documentation. The main area is titled "Advisor recommendations" and lists various issues with columns for Name, Last Seen, Impact, and Risk. A specific row is expanded to show more details. At the top right, there is a "Details" section for a cluster, which includes fields for Cluster API address, Cluster ID, Provider, OpenShift version, Service Level Agreement (SLA), and Update channel. A yellow box highlights the SLA section, which shows "Self-support, 60 day trial" and "15 days remaining". A red box highlights the "Recommendations" link in the sidebar.

Name	Last Seen	Impact	Risk
Cluster upgrade will fail when default SCC gets changed	2 years ago	<span>Service Availability</span>	<span>Important</span>
Workloads are still using the deprecated APIs which will be removed in the next release	5 months ago	<span>Service Availability</span>	<span>Important</span>
SystemMemoryExceedsReservation alerts when the system daemons memory usage on nodes exceeds 90% of the reservation for them	4 months ago	<span>Service Availability</span>	<span>Important</span>
Workloads are using the deprecated PodSecurityPolicy API	5 months ago	<span>Performance</span>	<span>Moderate</span>
CVE-2021-30465: runc vulnerable to privilege escalation	9 months ago	<span>Security</span>	<span>Moderate</span>
Nodes will become Not Ready due to a CRI-O PID leak in the running OpenShift Container Platform version	5 months ago	<span>Service Availability</span>	<span>Moderate</span>
The running OpenShift version has reached its End of Life	2 years ago	<span>Service Availability</span>	<span>Moderate</span>
Pods could fail to start if openshift-samples is degraded due to FailedImageImport which is caused by a hiccup while talking to the Red Hat registry	2 years ago	<span>Service Availability</span>	<span>Moderate</span>
Prometheus metrics data will be lost when the Prometheus pod is restarted or recreated	1 year ago	<span>Service Availability</span>	<span>Moderate</span>
The authentication operator is degraded when cluster is configured to use a cluster-wide proxy	2 years ago	<span>Security</span>   1 more	<span>Moderate</span>
An OCP node behaves unexpectedly when it doesn't meet the minimum resource requirements	2 years ago	<span>Performance</span>	<span>Moderate</span>

**Details**

Cluster API address: https://api.kdoberst.devcluster.ope  
443

Cluster ID: 2c987c4d-d4ff-4261

Provider: AWS

OpenShift version: 4.10.0-0.nightly-2021

Service Level Agreement (SLA): Self-support, 60 day trial  
**15 days remaining**  
Manage subscription settings

Update channel: stable-4.10

Service Level Agreement (SLA): None  
**Trial expired**  
Manage subscription settings

Update channel: stable-4.10

Total risk: 1 - 14 of 14

Clusters: 1

**Onboarding tour**

# Cost management for OpenShift

## AWS saving plans

- ▶ Customers with AWS saving plans now can select if they see amortized, blended and unblended costs.

## 90 days cost explorer

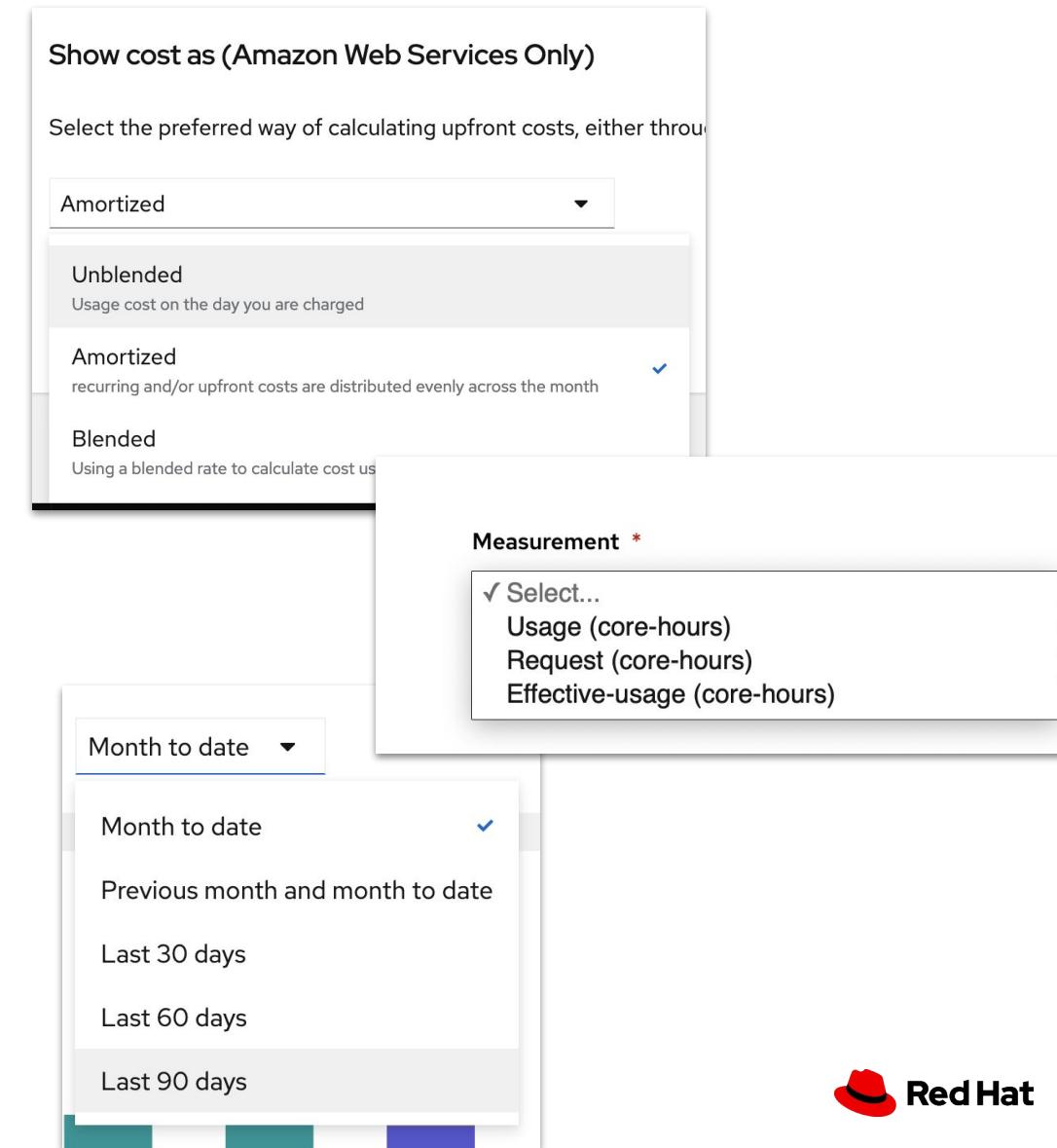
- ▶ We have updated the cost explorer and now you can select up to 90 days of data

## OCP on GCP

- ▶ OCP costs can now be automatically calculated when connected to the GCP underlying infrastructure, like previously with AWS and Azure

## Effective usage calculating costs

- ▶ A new rate policy has been added to take into account the maximum of requests and usage of each pod reflecting real reservation.



# Thank you!



[linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)



[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)



[facebook.com/redhatinc](https://facebook.com/redhatinc)



[twitter.com/RedHat](https://twitter.com/RedHat)