



What's New in OpenShift?

Emre Özkan
Senior Solution Architect

OpenShift Enhancements

- Core Platforms
- Application & Platform Services
- Developer Experience
- Security
- Management
- Observability
- Sustainability

Core Platform

Kubernetes 1.27

Major Themes and Features

- ▶ SeccompDefault graduates to stable
- ▶ Mutable scheduling directives for Jobs graduates to GA
- ▶ DownwardAPIHugePages graduates to stable
- ▶ Pod Scheduling Readiness goes to beta
- ▶ Node log access via Kubernetes API
- ▶ ReadWriteOncePod PersistentVolume access mode to beta
- ▶ Respect PodTopologySpread after rolling upgrades
- ▶ Faster SELinux volume relabeling using mounts
- ▶ Robust VolumeManager reconstruction to beta
- ▶ Mutable Pod Scheduling Directives to beta

Significant list of other graduations to stable:

- ▶ Default container annotation to be used by kubectl
- ▶ TimeZone support in Cronjob
- ▶ Expose metrics about resource requests and limits that represent the pod model
- ▶ Server side unknown field validation
- ▶ Node topology manager
- ▶ Add gRPC probe to Pod.Spec.Container.{Liveness,Readiness,Startup} probe
- ▶ Add configurable grace period to probes
- ▶ OpenAPI v3
- ▶ Stay on supported Go versions

CRI-O
1.27



Kubernetes
1.27

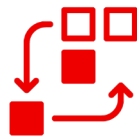


OpenShift
4.14



OpenShift 4.14 Supported Providers

Installation Experiences



Automated

Installer Provisioned Infrastructure

- Auto-provisions infrastructure
- *KS like
- Enables self-service



Full Control

User Provisioned Infrastructure

- Bring your own hosts
- You choose infrastructure automation
- Full flexibility
- Integrate ISV solutions



Interactive - Connected

Assisted Installer

- Hosted web-based guided experience
- Agnostic, bare metal, vSphere and Nutanix
- ISO driven



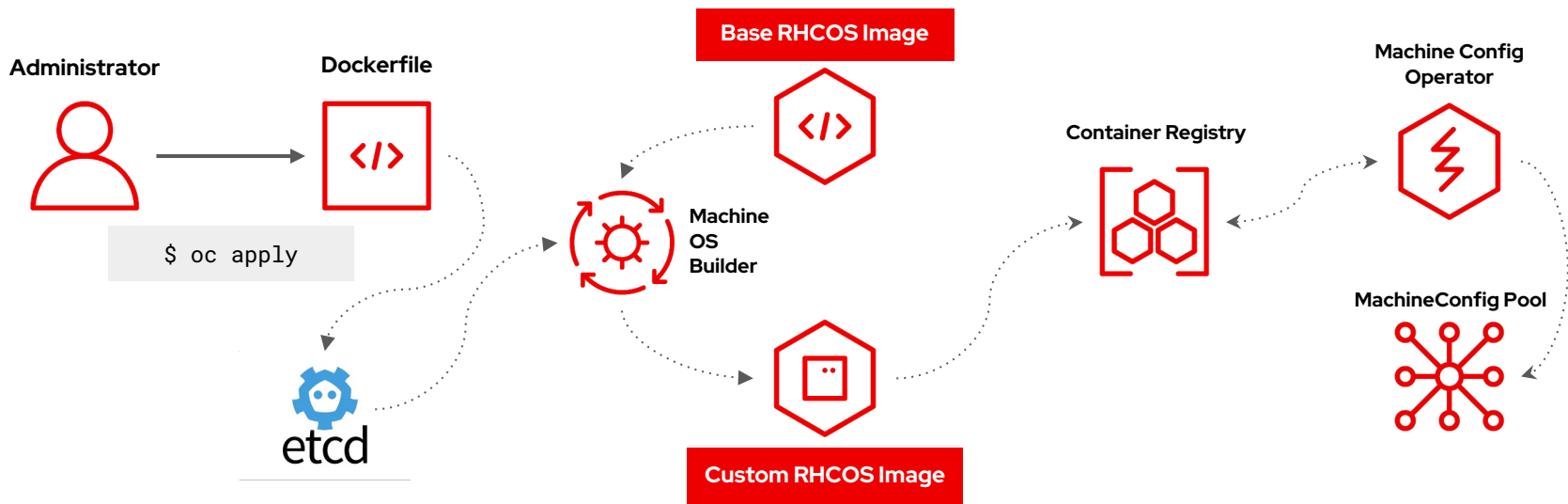
Local - Disconnected

Agent-based Installer

- Disconnected / air -gapped
- Automatable installations via CLI
- Bare metal, vSphere, SNO
- ISO driven

CoreOS Layering on-cluster builds

Make it so!



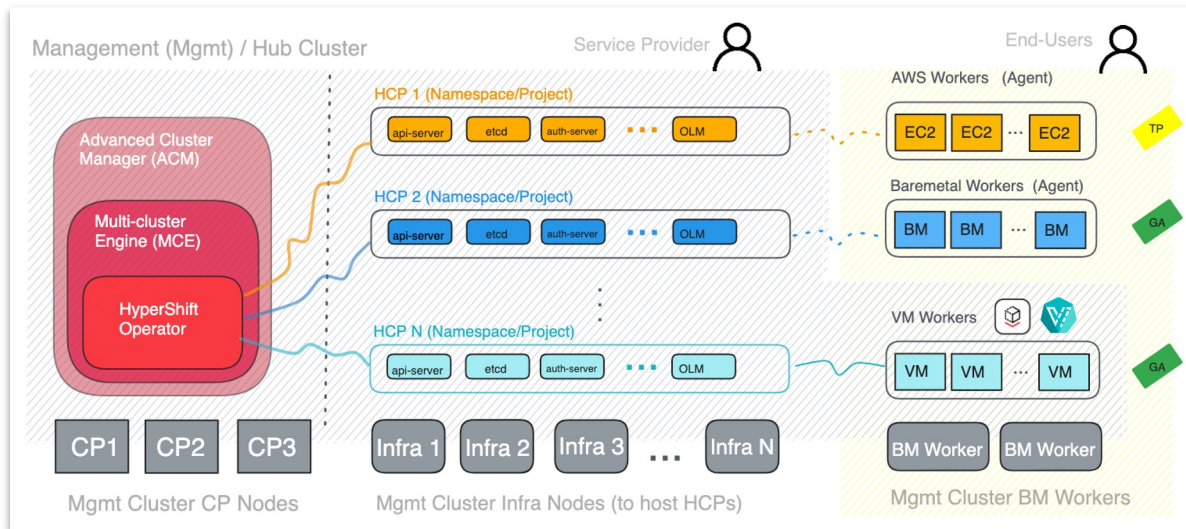
Hosted Control Planes for Red Hat OpenShift

What's new (w/ MCE 2.4)

- Baremetal with the Agent Provider (GA)
- OpenShift Virtualization Provider (GA)

Why it matters

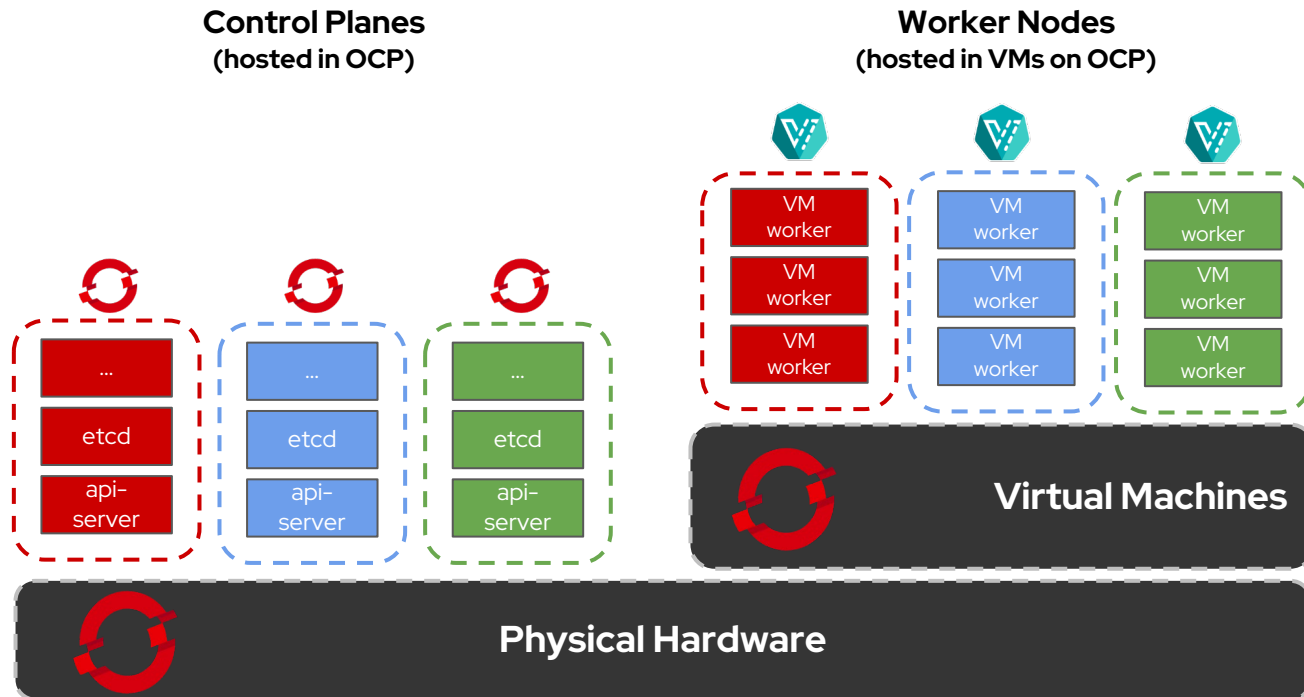
- ~30% infra savings, ~65% for SREs/Operations savings.
- ~60% time-saving for devs (↑ Productivity), ~50% reductions in power & facility costs.
- Solve for Multi-cluster, build on a efficient grounds.
- Build your Cluster-as-a-Service on top for speed and efficiency



Generally Available in OCP 4.14 + ACM 2.9

Consolidate OpenShift Clusters with OpenShift Virtualization

Hosted Control Planes with KubeVirt provider



Standardized operator lifecycle

Starting with 4.14, all Red Hat operators now fall into one of three tiers

Platform Aligned

- ▶ Multiple version lines supported in parallel
- ▶ Release dates aligned OCP
- ▶ Lifecycle length aligned with OCP
- ▶ Channel names aligned with OCP
- ▶ No update required during the lifecycle of a given OCP release to stay supported

Platform Agnostic

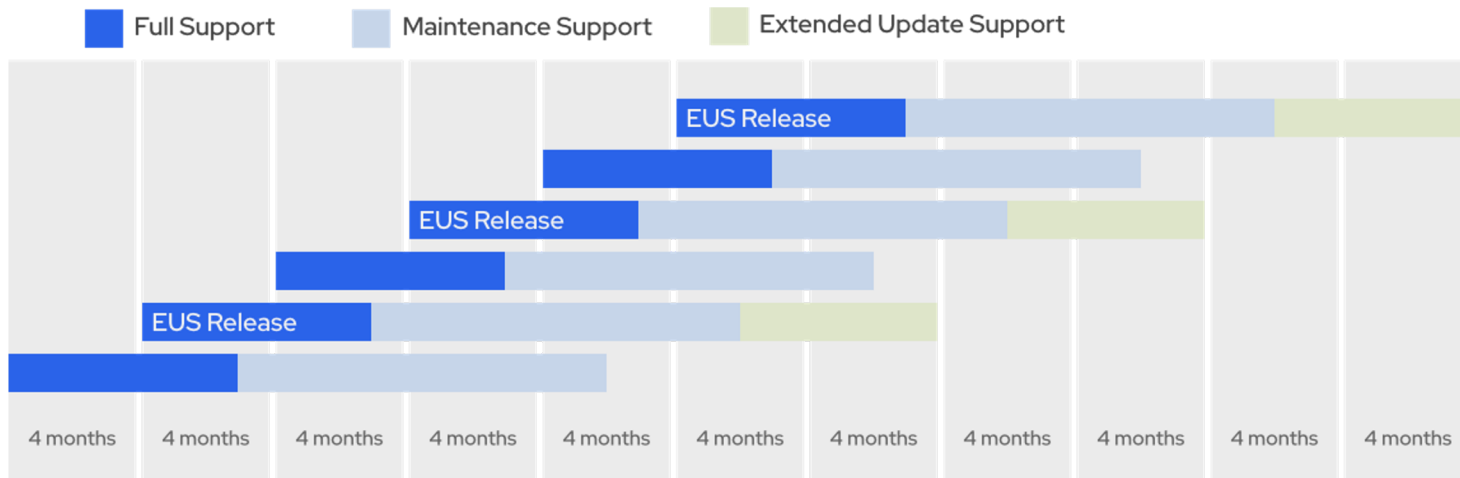
- ▶ Multiple version lines supported in parallel
- ▶ Custom Release dates
- ▶ Shorter Lifecycle length
- ▶ Minor-version based channel names
- ▶ Updates may be required during the lifecycle of a given OCP release to stay supported

Rolling Stream

- ▶ Only a single, latest version is supported at a given time
- ▶ Frequent releases
- ▶ Every release supports all OCP versions
- ▶ Only a single channel
- ▶ Updates are mandatory to stay supported

For every supported OpenShift release, there is at least one version of every Red Hat operator in support

Extended Update Support





Secrets Store CSI Driver Operator (TechPreview)

Mount secrets from external secret storage solutions



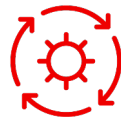
**Mount Secrets
directly for
Application usage**

SSCSI driver mounts secrets in tmpfs, so **Secrets are deleted when pod is deleted**



**Integrates with
Secret Store CSI
Driver Providers**

Upstream Azure, GCP, AWS and Vault



Secret Auto-rotation
Operator is

configured to sync with external secret storage every 2 minutes and auto-rotate if secret content has changed



**Sync as Kubernetes
Secrets**

Operator can sync secrets and create Kubernetes secrets.



**Available in
OperatorHub**

Flexible OpenShift Installation

Disable/enable capabilities from installation

- ▶ Include / exclude one or more optional capabilities (includes operators) during installation
- ▶ Option to enable a previously excluded capabilities after cluster is installed
- ▶ Optional capabilities you can exclude:
 - Machine API operator, cluster autoscaler operator, cluster control plane machine set operator, Build capability (affects Build and BuildConfig)
 - (in addition to baremetal operator, console operator, csi-snapshot-controller operator, Insights operator, marketplace operator, node tuning operator, storage operator, and openshift-samples operator)

```
capabilities:  
  baselineCapabilitySet: vCurrent  
  additionalEnabledCapabilities:  
  - CSISnapshot  
  - Console  
  - Storage
```

Excerpt from Install-config.yaml

Tackle scaling, node failure in control plane

- ▶ Vertical control plane scaling automatically on Azure and Google Cloud Platform
- ▶ Leverages ControlPlaneMachineSet to manage the cluster's control plane machines and adds additional automation on existing Machine API concepts

```
apiVersion: machine.openshift.io/v1
kind: ControlPlaneMachineSet
metadata:
  name: cluster
  namespace: openshift-machine-api
spec:
  ...
  state: Active
  replicas: 3
  strategy:
    type: RollingUpdate [2]
  template:
    machineType: machines_v1beta1_machine_openshift_io
    machines_v1beta1_machine_openshift_io:
      failureDomains: [3]
      ...
    metadata:
      ...
    spec:
      providerSpec: [1]
      value:
        <platform specific provider spec>
```

Cgroup V2 as Default

Making Openshift more stable

Features

- ▶ Next generation of cgroups in the kernel.
All new development happens in v2.
- ▶ Better node stability under OOM pressure scenarios.

Implementation details

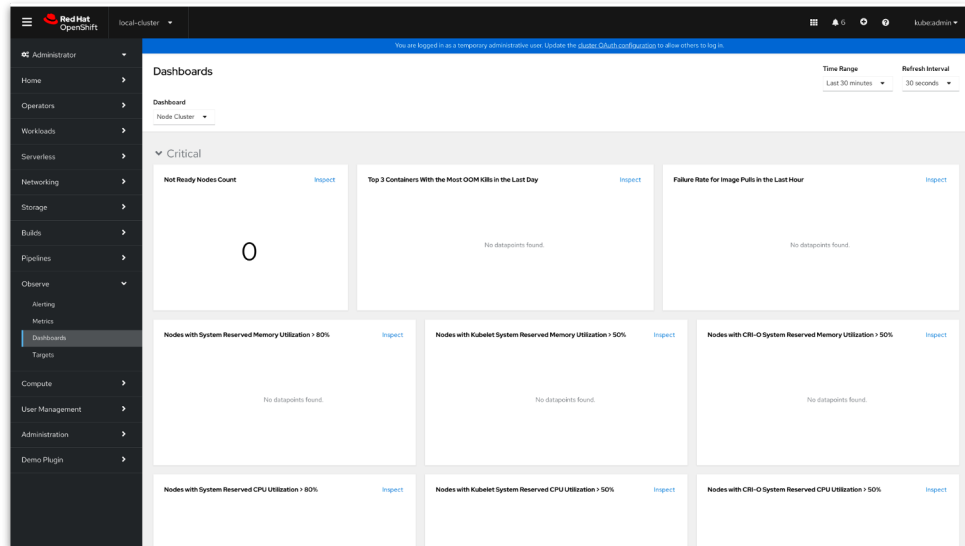
- ▶ Customer to check their java version compatibility with CgroupV2 (Please see release notes for more details)
- ▶ Cgroup V1 is available as non default
- ▶ All new cluster will be on CgroupV2
- ▶ All upgrading cluster will be on CgroupV1 with option to move to CgroupV2 as Day 2

Node Dashboard for monitoring pod density per node

Define your own green zone/red zone

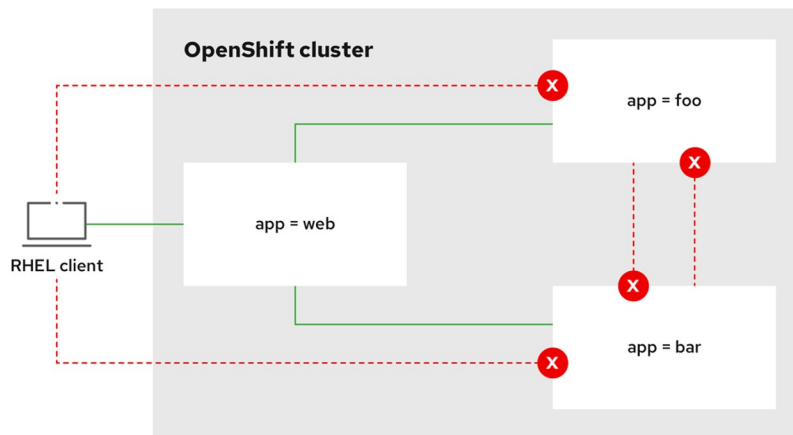
Feature

- ▶ Pre loaded dashboard with predefined metrics .
- ▶ Sometimes even though there is lot of CPU/Mem left in the server but scheduler cannot schedule pod.
- ▶ This dashboard will help in understanding why my scheduler cannot schedule pod in that node



Admin Network Policy

- OpenShift will support Admin Network Policy to enhance overall cluster security by providing cluster-admin-only policies that cannot be overridden by project admins or individual developers
- Tech Preview of East-West pod-to-pod enablement at OpenShift 4.14



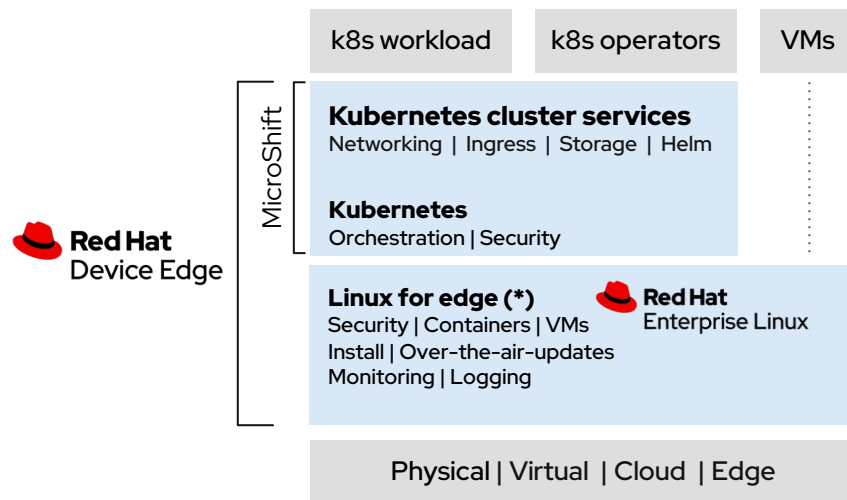
Red Hat Device Edge and MicroShift

What is it?

Red Hat Device Edge with MicroShift is a Kubernetes distribution derived from OpenShift Container Platform that is designed for optimizing small form factor devices and edge computing.

New Features:

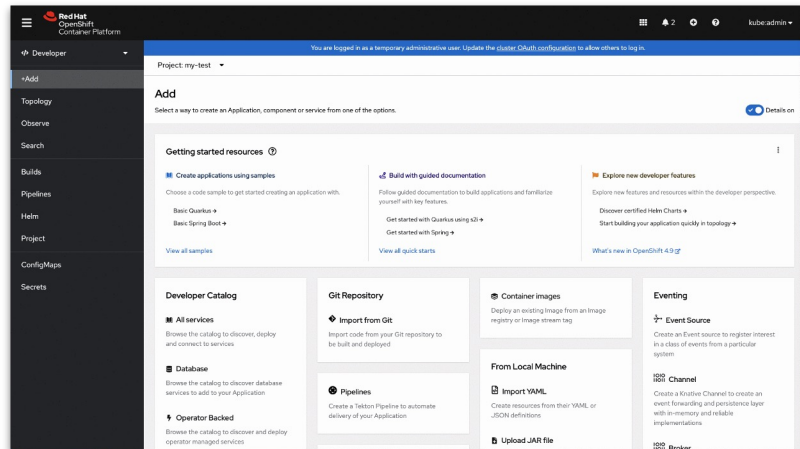
- General availability
- Updateability
- Automatic rollback with rpm-ostree
- Manual backup and restore
- CSI Snapshots
- CNCF certification
- Networking enhancements (full offline)



Application & Platform Services

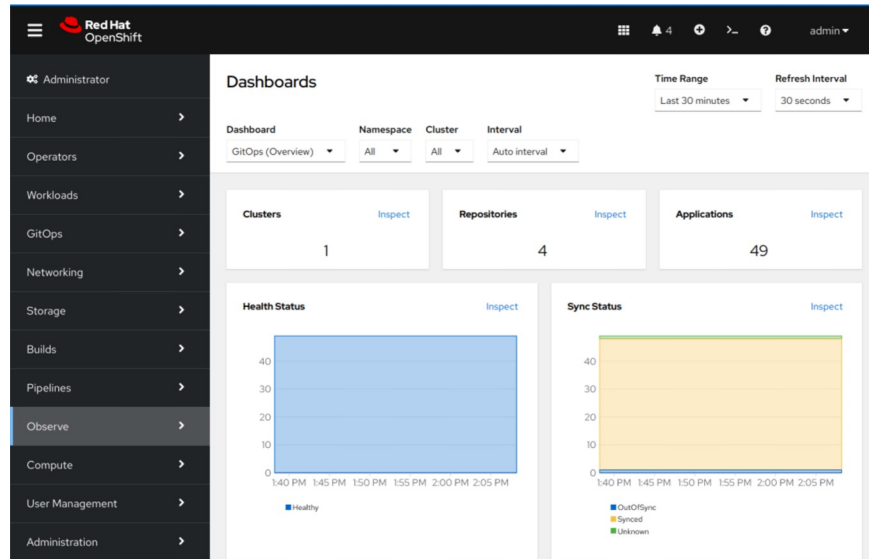
OpenShift Pipelines

- ▶ **OpenShift Pipelines 1.12 (Tekton Pipelines 0.50)**
- ▶ **Tekton Chains** is now GA
- ▶ **Tekton Results** for extended pipeline history retention (Tech Preview)
 - ▶ Support for Google Storage Bucket, S3, etc as external log storage



OpenShift GitOps

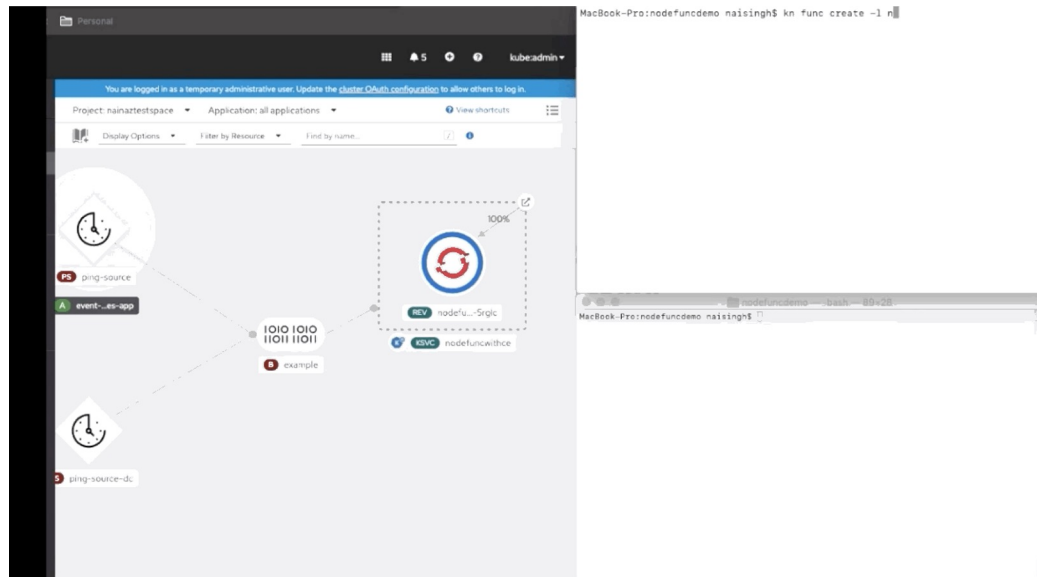
- ▶ **OpenShift GitOps 1.10**
- ▶ Includes **Argo CD 2.8**
- ▶ Three monitoring dashboards in the OpenShift Admin console
- ▶ **Dynamic scaling** for the Application controller



OpenShift Serverless

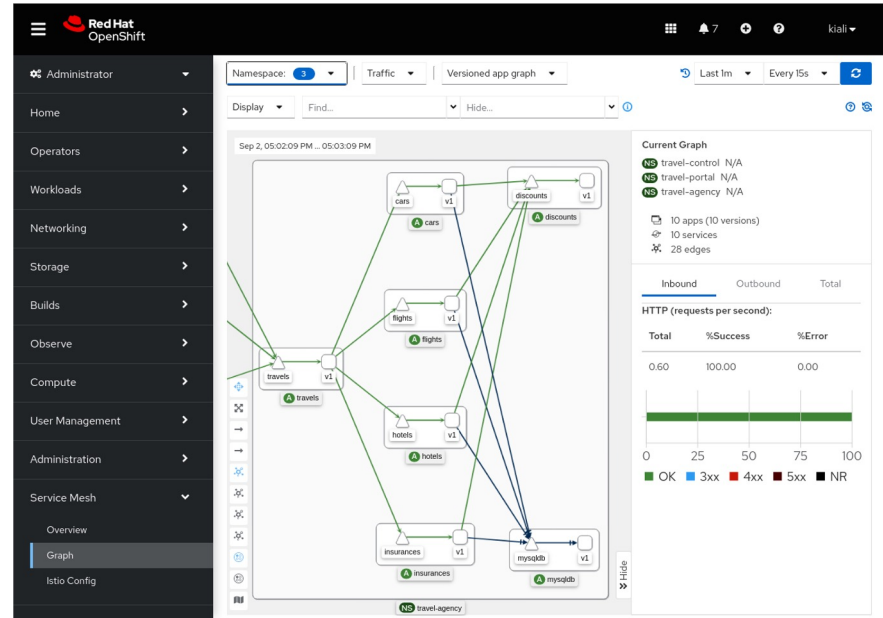
Key Features & Updates

- ▶ Serverless 1.30 : Update to Knative 1.9
- ▶ Serverless functions on IBM zSystems and Power
 - ▶ s2i builder
- ▶ Hosted Control Planes support

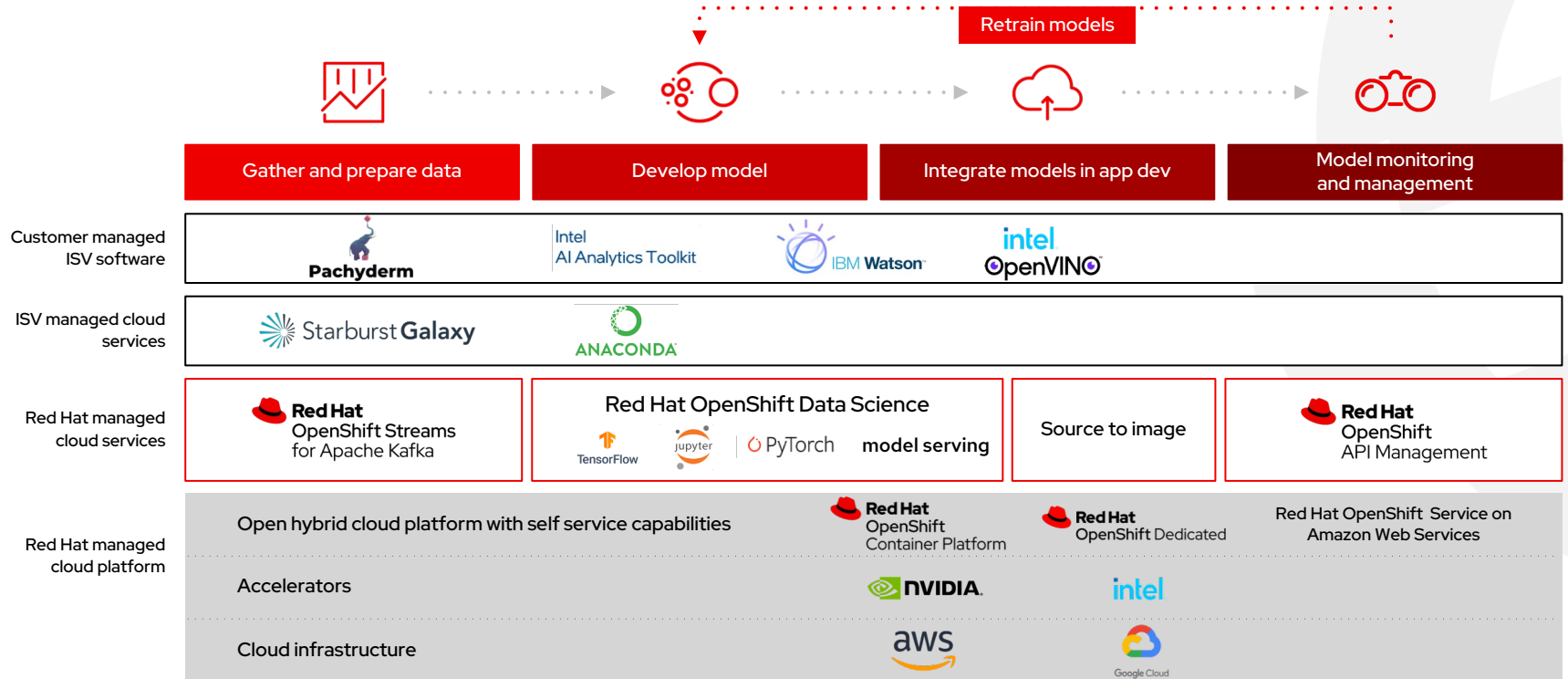


OpenShift Service Mesh

- ▶ OpenShift **Service Mesh 2.4.3** introduced:
 - ▶ Technology Preview on **ARM64** clusters
 - ▶ gRPC extension for external authorization
- ▶ OpenShift **Service Mesh 2.5** is coming soon:
 - ▶ Based on **Istio 1.18** and **Kiali 1.7.3**
 - ▶ Support for Service Mesh on ARM64
- ▶ “Sail Operator” – Developer Preview of OpenShift **Service Mesh 3** is now available:
 - ▶ Based directly on upstream Istio



OpenShift Data Science



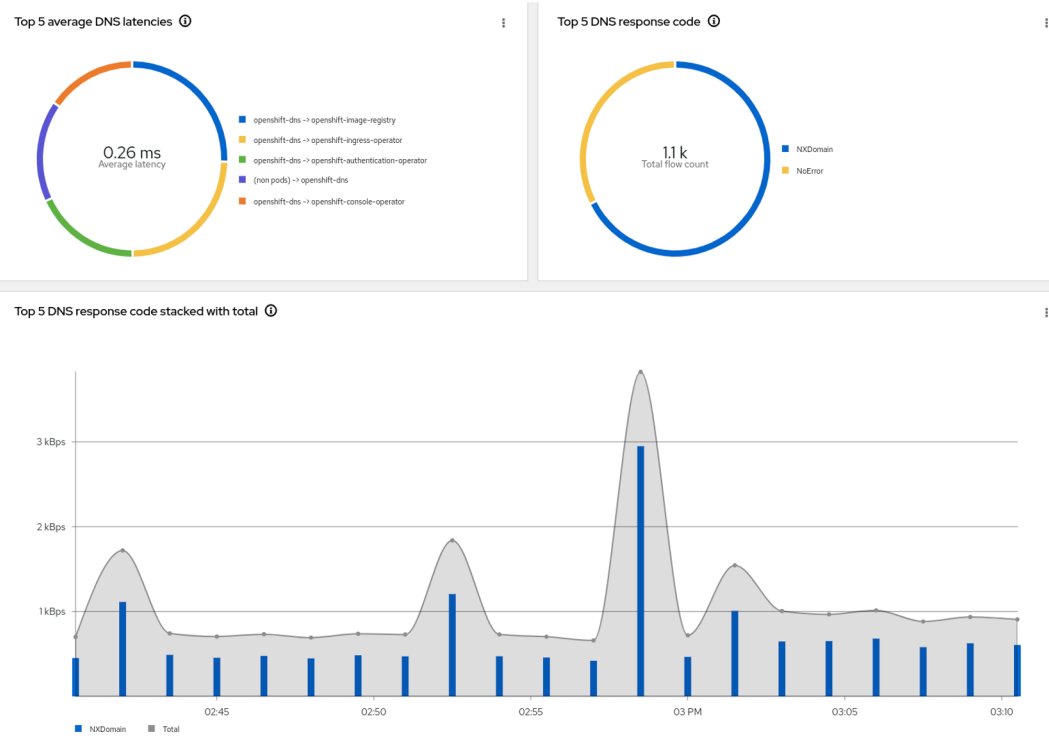
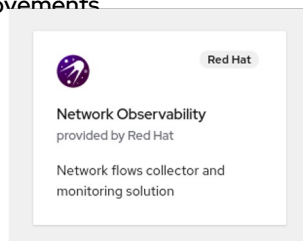
Network Observability Operator

Network Observability Operator

v1.4

What's new:

- Identify source of packet drops
- DNS analysis
- No longer requires Loki
- Network Observability for secondary interfaces with Multus and SR-IOV plugins
- Support for IBM Z architectures
- User Interface improvements
- Flow-based dashboard and health dashboard improvements



Developer Experience



Dynamic Plugins Updates for the OCP Console

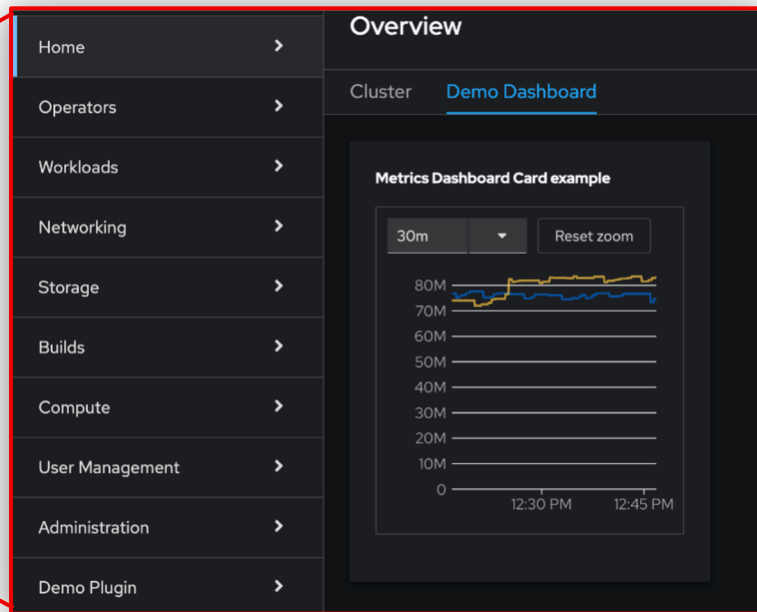
New Extension Points with Updated Examples

Examples

- ▶ [Dynamic Demo Plugin](#)
- ▶ [CronTab Plugin](#)
- ▶ [Plugin Template](#)

API

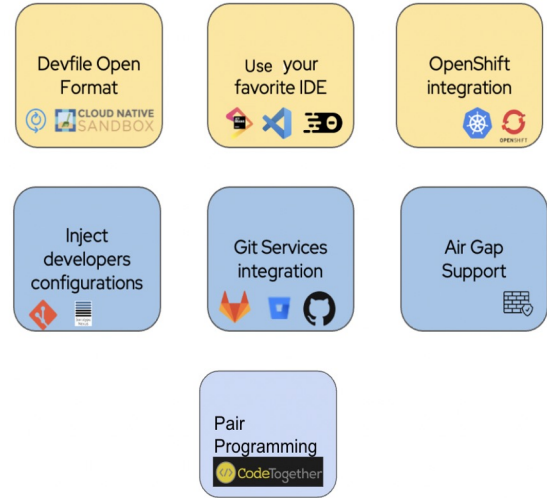
- ▶ [QueryBrowser](#)
- ▶ [useAnnotationsModal](#)
- ▶ [useDeleteModal](#)
- ▶ [useLabelsModal](#)
- ▶ [useActiveNamespace](#)
- ▶ [ErrorBoundaryFallbackPage](#)



Red Hat OpenShift Dev Spaces

What's New

- Microsoft Visual Studio Code - Open Source is the default editor
- Supported Github Enterprise Server
- Improved workspace startup time



| | |
|---------------|---|
| IDE Supported | VS Code, Eclipse Theia,(Tech Preview: JetBrains IntelliJ) |
| Languages | Languages that the above IDE Supports |
| Repositories | GitHub, Gitlab, Bitbucket |
| Browser | Chrome,Firefox |
| Platforms | OCP 4.10, 4.11 |

Custom Metric Autoscaler (GA)

Scale workloads horizontally based on custom metrics

- Custom Metric Autoscaler is built on CNCF project [KEDA](#)
- Installed from Operator hub
- GA with [Prometheus](#) scaler, Technical preview with [Apache Kafka](#) scaler
- Manages workloads to scale to 0
- Provides metrics for Horizontal Pod Autoscaler (HPA) to scale on



Deprecated deploymentconfig to deployment

Depreciation does not means "Removal"

Feature

- ▶ Customers are encouraged to use Deployment instead of Deploymentconfig

```
[knarra@knarra zap]$ oc create deploymentconfig registry-name1 --image=quay.io/openshifttest/registry@sha256:1106aedc1b2e386520bc2fb797d9a7af47d651db31d8e7ab472f2352da37d1b3
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.10000+
deploymentconfig.apps.openshift.io/registry-name1 created
[knarra@knarra zap]$
```

Security

Red Hat Advanced Cluster Security (RHACS) for Kubernetes

ACS Cloud Trial is Now Available

ACS Cloud is now available: <https://www.redhat.com/acstrial>

- Currently protecting:
 - 52 Centrals, 54 Clusters
 - Over 1000 nodes
 - Over 26k vCPU
- **Sign up online for 60 days free trial**
 - [redhat.com/acstrial](https://www.redhat.com/acstrial)
- Connect to your Openshift or any other kubernetes Cluster and start your evaluation in minutes
- Fully functional Trial with no limited on functionality of capacity
- Access to Red Hat's award-winning Customer Portal, including documentation, helpful videos, discussions, and more



A screenshot of the Red Hat ACS Cloud Trial sign-up page. At the top, there is a progress bar with three steps: 'Get started' (completed, red dot), 'Log in' (in progress, grey dot), and 'Trial success' (not started, white dot). Below the progress bar, the text reads 'Try Red Hat Advanced Cluster Security Cloud Service'. A prominent red button says 'Start your trial', with a link for 'Trial eligibility' below it. A section titled 'What you get with this product trial' lists two benefits: a 60-day subscription and access to the Customer Portal. At the bottom, a disclaimer states the trial is not for production use.

Vulnerability Management 2.0 (VM 2.0)

Workload CVEs and On-demand + Downloadable CVEs Report

(Technology Preview)



- Workload CVEs
- Create & Download an on-demand workload CVEs report in CSV format

The screenshot displays the Red Hat Advanced Cluster Security for Kubernetes interface. The left sidebar shows the navigation menu with 'Vulnerability Reporting (2.0)' highlighted. The main content area shows the 'Downloadable On-Demand Report' configuration page. The 'Report parameters' section includes fields for 'Report name' (Downloadable On-Demand Report), 'Description' (None), 'CVE severity' (Critical, Important), and 'CVE status' (Fixable). The 'Delivery destinations' section shows 'Email notifier' (None) and 'Distribution list' (None). The 'Schedule details' section shows 'No schedule set'. A red box highlights the 'Vulnerability Reporting' option in the sidebar and the 'Actions' dropdown menu on the right, which contains options: 'Edit report', 'Send report now', 'Generate download', 'Clone report', and 'Delete report'.

Built Time Network Policy Dev / DevOps Tools

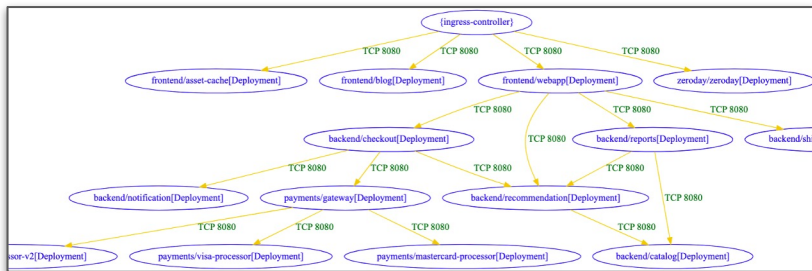
Two new options - Technology Preview



```
roxctl netpol connectivity map
```

Visualize impact of network policy

- Text: txt, json, md, csv
- Graph: dot



```
roxctl netpol generate
```



```
roxctl netpol connectivity diff
```

Compare between project branches

- Semantic diff

| diff-type | source | destination | dir1 | dir2 | workloads-diff-info |
|-----------|------------------------------|--|----------------|----------|---|
| added | payments/gateway[Deployment] | payments/visa-processor-v2[Deployment] | No Connections | TCP 8080 | workload payments/visa-processor-v2[Deployment] added |
| added | {ingress-controller} | frontend/blog[Deployment] | No Connections | TCP 8080 | workload frontend/blog[Deployment] added |
| added | {ingress-controller} | zeroday/zeroday[Deployment] | No Connections | TCP 8080 | workload zeroday/zeroday[Deployment] added |



Security Profile Operator

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



Easy seccomp and SELinux profile creation by

recording what your application needs and creates a profile from it



Manages profiles across nodes and namespaces

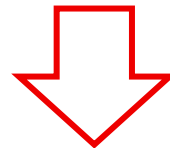
It also validates if node supports seccomp and doesn't synchronize it if not



Validate your profile



Reuse profiles across namespaces



Available in OperatorHub

Management

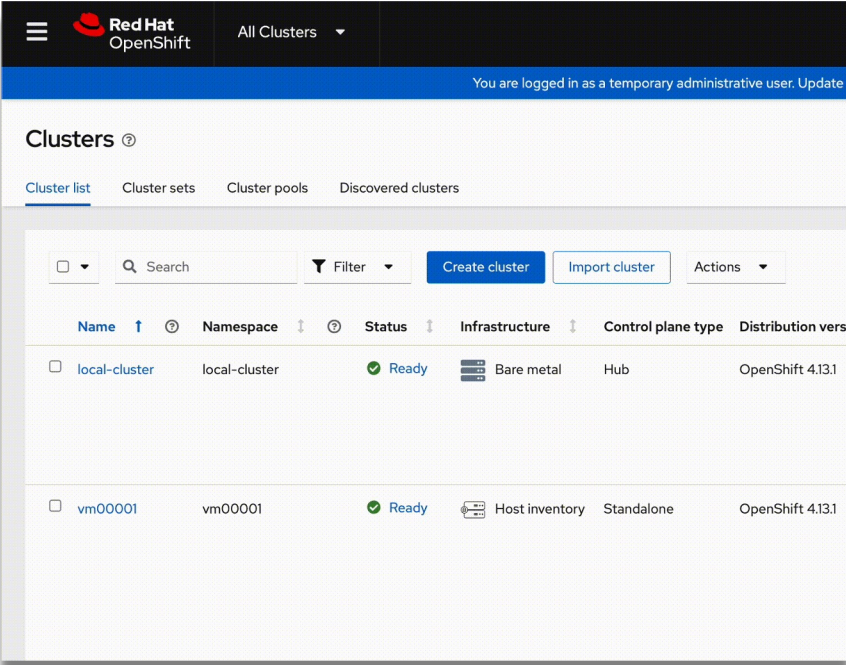
Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.9

OpenShift Everywhere

Providing platform engineers with a consistent approach for deploying OpenShift clusters, everywhere.

- Added Nutanix support
- Adjust RHACM hub capacity directly
- Allow node disk-wiping with ZTP
- Hosted Control Planes Generally Available



The screenshot displays the RHACM console interface. At the top, the Red Hat OpenShift logo is visible on the left, and 'All Clusters' is shown in the top right. A blue notification bar indicates the user is logged in as a temporary administrative user. Below this, the 'Clusters' section is active, with tabs for 'Cluster list', 'Cluster sets', 'Cluster pools', and 'Discovered clusters'. The 'Cluster list' tab is selected, showing a table of clusters with columns for Name, Namespace, Status, Infrastructure, Control plane type, and Distribution version. Two clusters are listed: 'local-cluster' (Bare metal, Hub) and 'vm00001' (Host inventory, Standalone).

| Name | Namespace | Status | Infrastructure | Control plane type | Distribution version |
|---------------|---------------|--------|----------------|--------------------|----------------------|
| local-cluster | local-cluster | Ready | Bare metal | Hub | OpenShift 4.13.1 |
| vm00001 | vm00001 | Ready | Host inventory | Standalone | OpenShift 4.13.1 |

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.9

Fleet Management

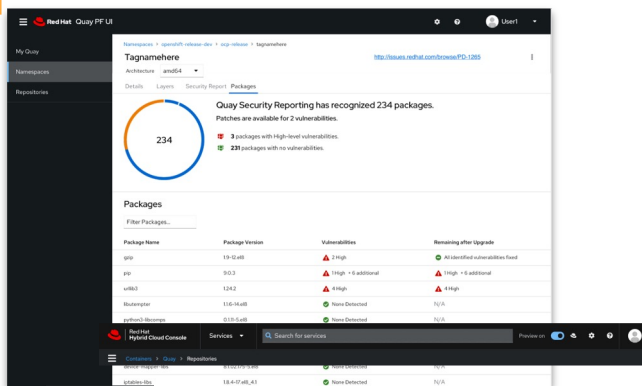
Expansion of management capabilities across the global fleet, providing solutions for data isolation boundaries and extremely high scale scenarios.

- **Global Hub phase 1: Policy compliance view (GA)**

- Policy compliance status and trend across all managed clusters
- Report compliance states for the past 30 days
- Inventory all managed hubs and managed clusters from overview
- Detect and alert on anomalous policy behavior
- Policy lifecycle changes ready for kafka event driven architecture



Red Hat Quay & Quay.io



Quay's new UI will default on console.rh

New Quay features will be live on & default in 2024. Red Hat Hybrid Cloud Console. Billing via AWS Marketplace and POs



Core UI Features & Functionality

Increase in intuitiveness and consistency across RH products with new features like Teams & Membership, Account settings, robot accounts, default permissions & Usage Logs and Builds by EOY



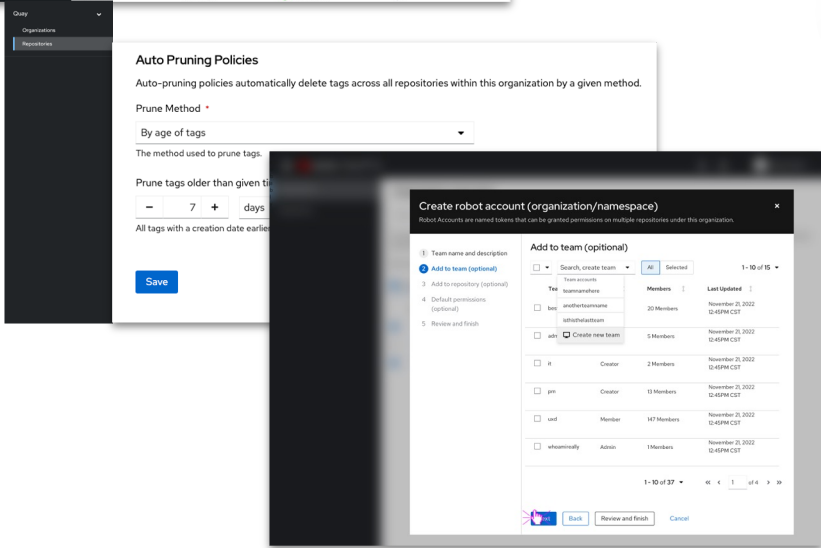
Auto-pruning Capabilities

Quay's intelligent auto-pruning policies will automatically remove unused artifacts to optimize storage constraints, improve performance, and enhance Quay user experience.

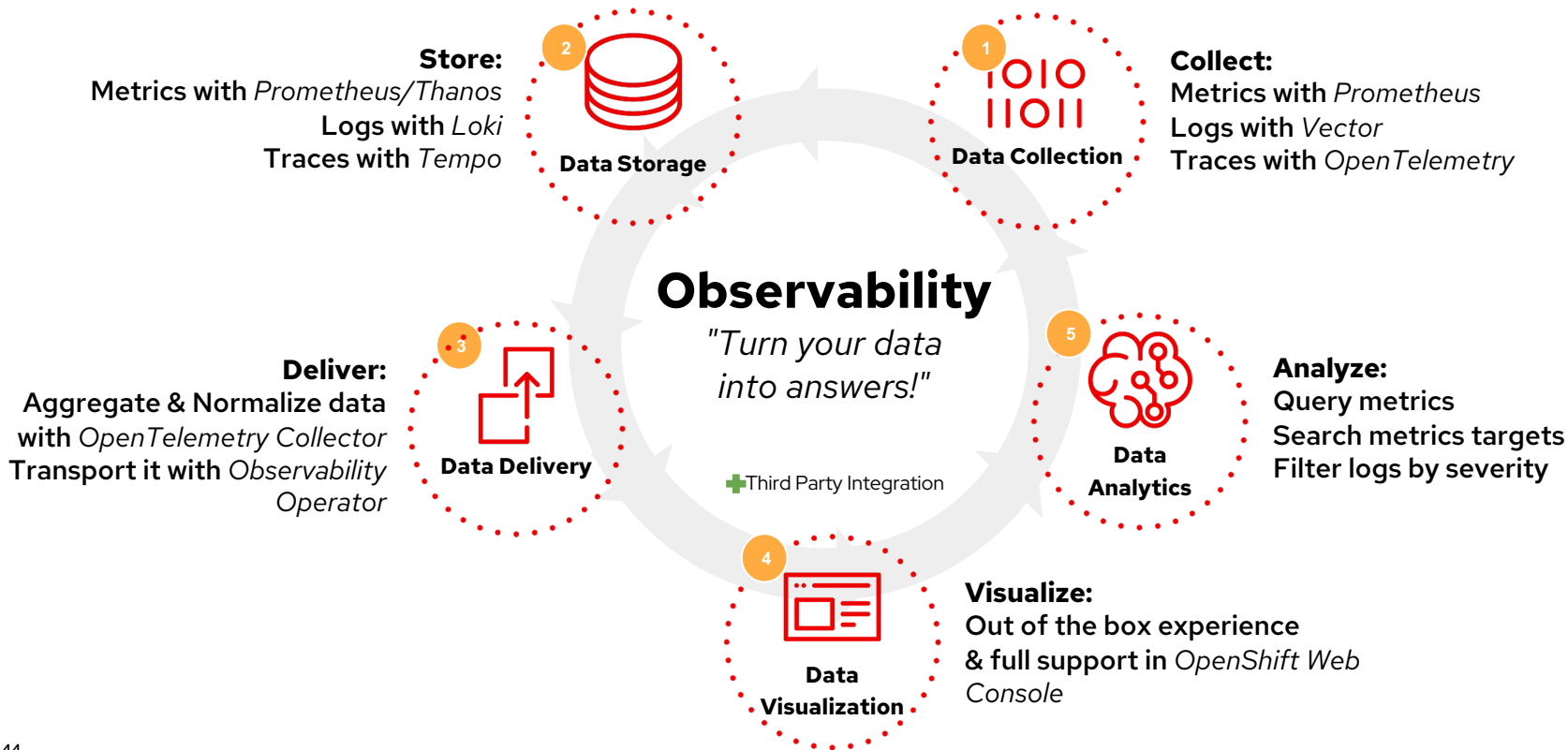


Improved Alignment with OpenShift

Future releases will align with OpenShift by 4 weeks will provide provide more reliable, efficient, and streamlined management of integrated Red Hat solutions.



Observability





Insights Advisor for OpenShift

- ▶ **Free service leveraging Red Hat experience with supporting and operating OpenShift**
- ▶ **Insights Update risk GA** – asses your cluster conditions and find the ones impacting safe cluster update!
- ▶ **New Insights recommendations** – Storage performance w/ CephFS and vSphere, obsolete conditions in openshift-network-operator, update blocking conditions

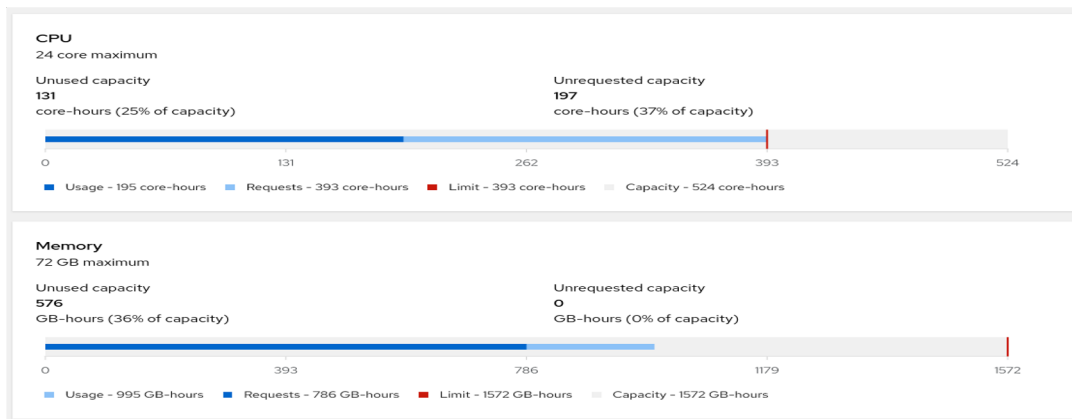
Advisor recommendations

| Name | Modified | Category | Total risk | Risk of change | Clusters |
|---|-------------|----------------------|------------|----------------|----------|
| False alert PodStartupStorageOperationsFailing generated in the cluster | 22 days ago | Service Availability | Low | Low | 32 |
| Cluster upgrades to 4.14.z are blocked due to a known bug in OpenShift | 24 days ago | Service Availability | Important | Low | 13 |



Insights Cost Management

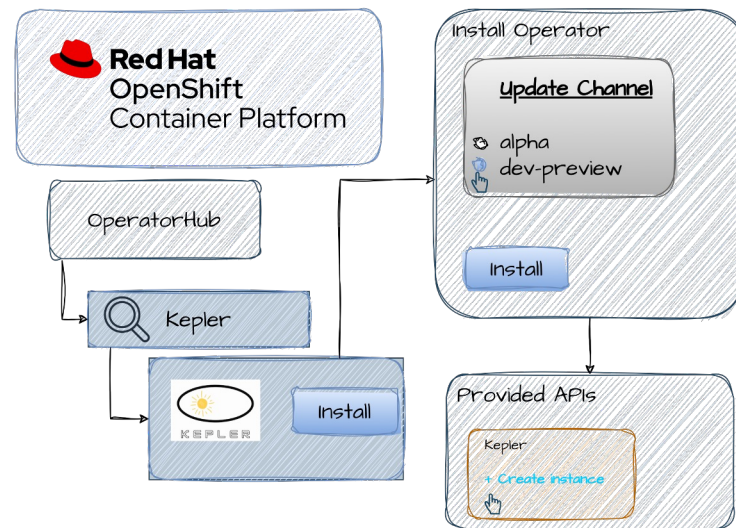
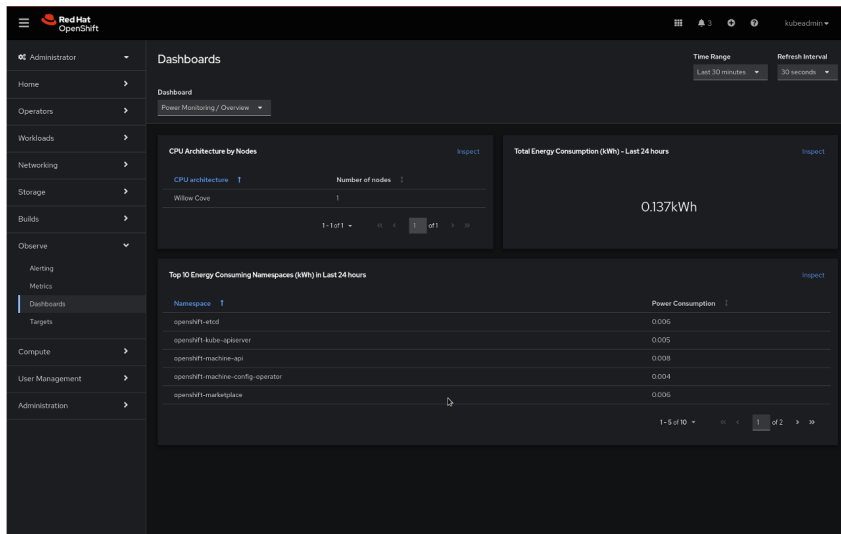
- ▶ **Free service to monitor per-resource (namespace, cluster, node, tag) usage and spending on-prem and major clouds**
- ▶ **Report vCPU count, RAM, and storage capacity**
 - ▶ Advanced cost model definition with distribution based on requested, used, or effective CPU or RAM usage, distributing the overhead costs of Kubernetes/OpenShift control plane.
- ▶ **Cost Management Metrics Operator 3.0.0**



Sustainability

Introducing **Power Monitoring for Red Hat OpenShift Developer-Preview**

- **Power monitoring for Red Hat OpenShift** is the downstream of Kepler project
- Embedded in the observability stack console, you can easily **experiment with Kepler** and **observe power consumption**



Thank you for joining!

Guided demos of
new features
on a real cluster

learn.openshift.com

OpenShift info,
documentation
and more

try.openshift.com

OpenShift Commons:
Where users,
partners, and
contributors come
together

commons.openshift.org