Red Hat OpenShift

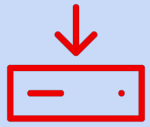
What's New in OpenShift 4.13

OpenShift Product Management

Red Hat

OpenShift 4.13

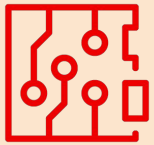
OPERATIONAL



3 Node Cluster Support in AWS, Azure, GCP and vSphere

Single Click Scale of Control Plane (Azure, GCP)

CORE



Custom Metric Auto Scaler

Cgroups v2

Kubernetes 1.26

SECURITY

Cert-manager operator is GA

Deploy OpenShift on encrypted VMs and encrypted storage in vSphere

User managed key to encrypt storage on AWS, Azure, and GCP

EDGE

Single Node OpenShift on AWS and Arm bare metal

LVM Storage resource optimization

crun is GA

Red Hat

Kubernetes 1.26

Major Themes and Features

- CSI migration
- Azure file in-tree to CSI driver migration
- Kubernetes metrics improvements
- Pod scheduling improvements
- Non-Graceful Node Shutdown for StatefulSet Pods [Beta]
- Signing Release Artifacts [Beta]
- Reduction of Secret-Based Service Account Tokens [Beta]

Significant list of other graduations to stable:

- CSI migration for Azure File and vSphere
- Delegate FSGroup to CSI Driver
- Service Internal Traffic Policy
- Reserve Service IP Ranges for Dynamic and Static IP Allocation
- Mixed Protocols in Services with Type LoadBalancer
- kubelet Credential Provider

CRI-O 1.26  Kubernetes 1.26 

OpenShift 4.13 

Release Announcement: https://kubernetes.io/blog/2022/12/09/kubernetes-v1-26-release/

Red Hat

Notable Top RFE's and Components

Top Requests for Enhancement (RFEs)

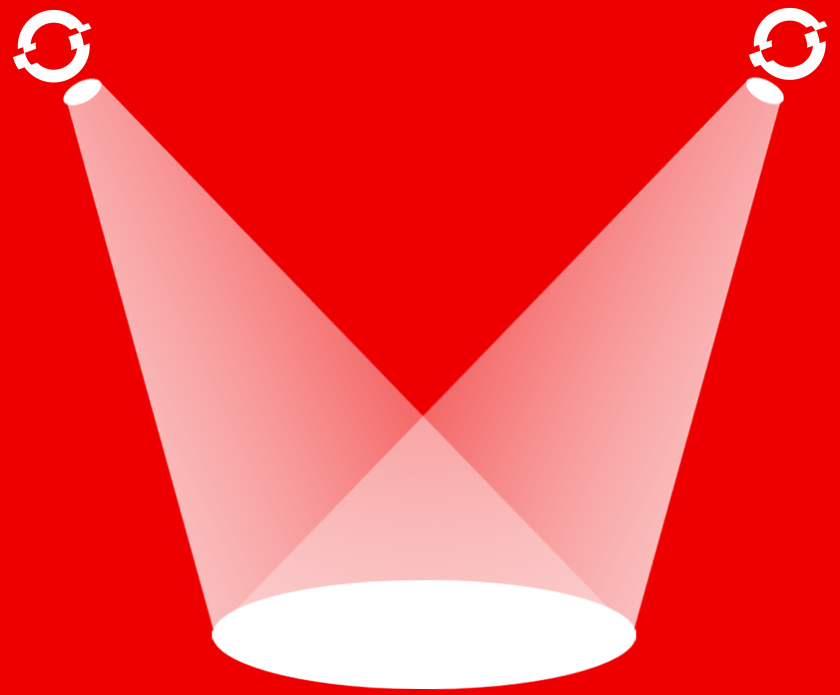
- Ability to deploy OpenShift in vSphere on different zones
  - Delivered for new clusters. Upgraded clusters can opt into this feature
- Allow expanding ClusterNetworks
  - Reduces the risk of clusters running out of pod or service IP space
- Add ability to log into node through RHCOS system console
  - Ability to login as a local account through the node console in the event the kubelet is down which removes the ability to use oc debug mode.
- Apply user defined tags to all resources created by OpenShift - Azure [TP]
  - Tags can only be configured during cluster creation. Along with user-defined tags, OpenShift adds tags required for its internal use to all the resources.
- Enable OpenShift IPI Installer to deploy OCP to a shared VPC in GCP [GA]
  - Ability to deploy cluster(s) into service project(s) on network(s) shared from a host project.

33 RFEs

shipped in **OpenShift 4.13** for customers

Red Hat

OpenShift 4.13 Spotlight Features



Red Hat

OpenShift 4.13 + RHEL 9

RHEL CoreOS is now based on RHEL 9.2

RHEL where you are

The latest generation of RHEL is designed to meet the needs of the hybrid cloud environment, from the edge to the cloud

9.2 kernel

The latest in hardware support & performance

Cgroups v2 enhancements

Security & innovation

Industry-leading security response & upstream engineering leadership

Red Hat

Red Hat Advanced Cluster Security Cloud Service

Going Live (LA)

Get more value from your cloud investment with Red Hat ACS cloud services.

Faster time to value

Quickly deploy ACS in minutes and scale as needed across clouds and geographies. Focus on securing your applications, not managing infrastructure

Reduce complexity

Fully-Managed ACS throughout the stack, 24x7 expert SRE support and an industry leading 99.0% SLA

Hybrid Cloud Flexibility

Delivering a consistent ACS experience on cloud giving you the choice and ease of use to choose the offering that best fits your needs

Red Hat

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
- (in addition to Vertical control plane scaling on AWS)

More at Control plane machine management and 1-click scaling and About the Control Plane Machine Set Operator

```yaml
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>
```


Red Hat

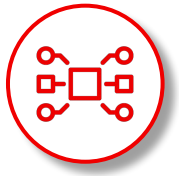
Systems Enablement

OpenShift on Arm

- Run OpenShift on highly efficient, high performance per watt architectures

o----------o

- Support for Arm on Azure (UPI)
- Single Node OpenShift on Arm (bare metal)
- Assisted Installer on Arm



Multi-architecture Cluster

- Allow more flexibility in a cluster, use different cloud platforms

o----------o

- Multi-architecture compute platforms:
  - AWS Arm support (GA)
  - Azure Arm support (GA)
  - Bare Metal Arm (TP)
- Multi-architecture compute migration and upgrade support
- Hosted Control Plane:
  - AWS Arm control plane

IBM Power and zSystems

- Run OpenShift on highly available, highly secure, scalable hardware

o----------o

- FIPS Mode supported
- Cluster Resource Override Operator
- Network Bound Disk Encryption
- Metal LB support
- Egress IP support

Customizable RHEL CoreOS

GA in 4.13

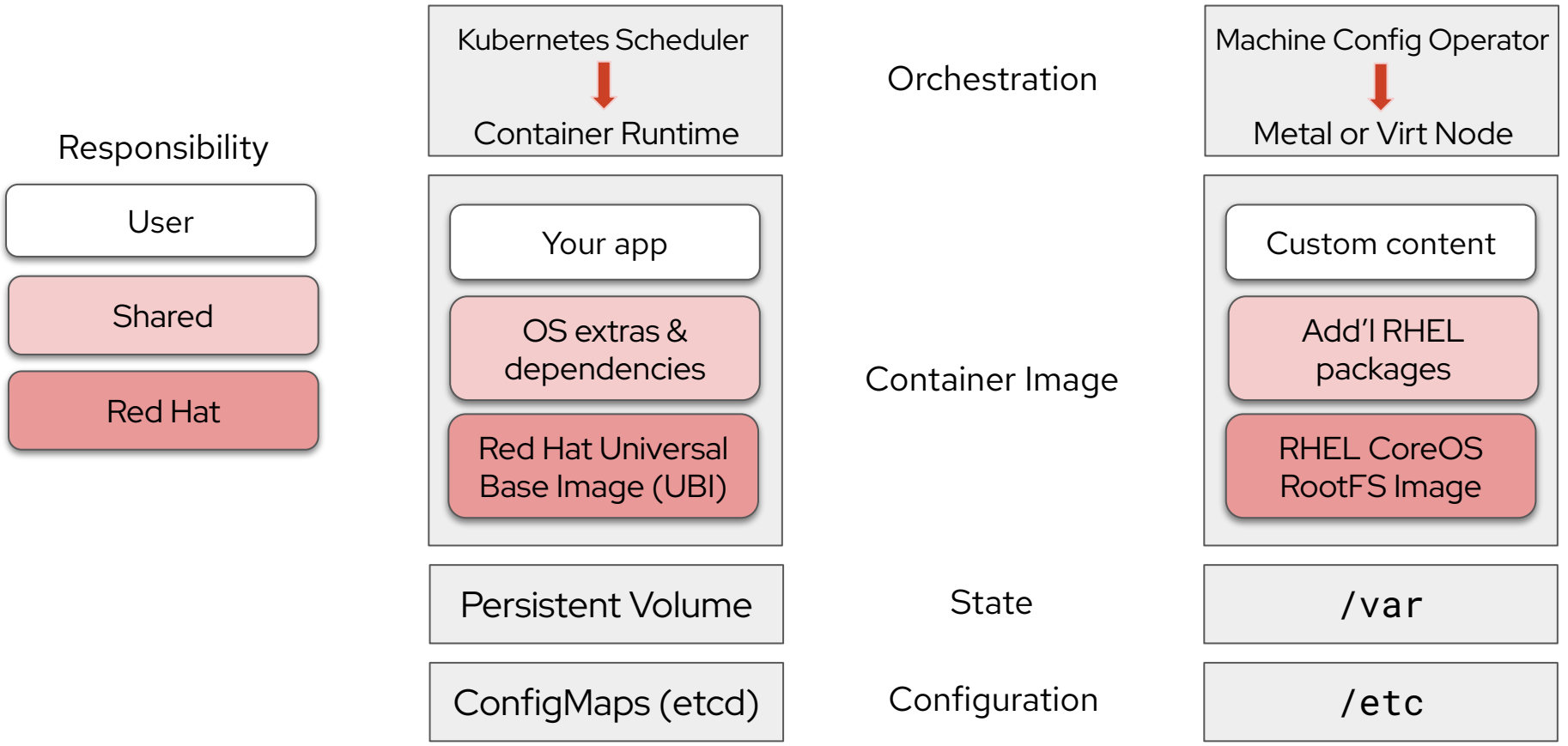
RHEL CoreOS images can now be customized using industry-standard OCI container building tools

- Add 3rd party content to the RHCOS base image
- Manage configuration files with a simpler UX
- You define the image, the Machine Config Operator rolls it out

More info:
RHCOS Image Layering examples and FCOS Layering examples
https://coreos.github.io/rpm-ostree/container/
https://github.com/containers/bootc

Red Hat

A common model for apps and OS



Red Hat

Tech Preview 4.13

Utilizing OpenShift Virtualization to Consolidate OpenShift Clusters

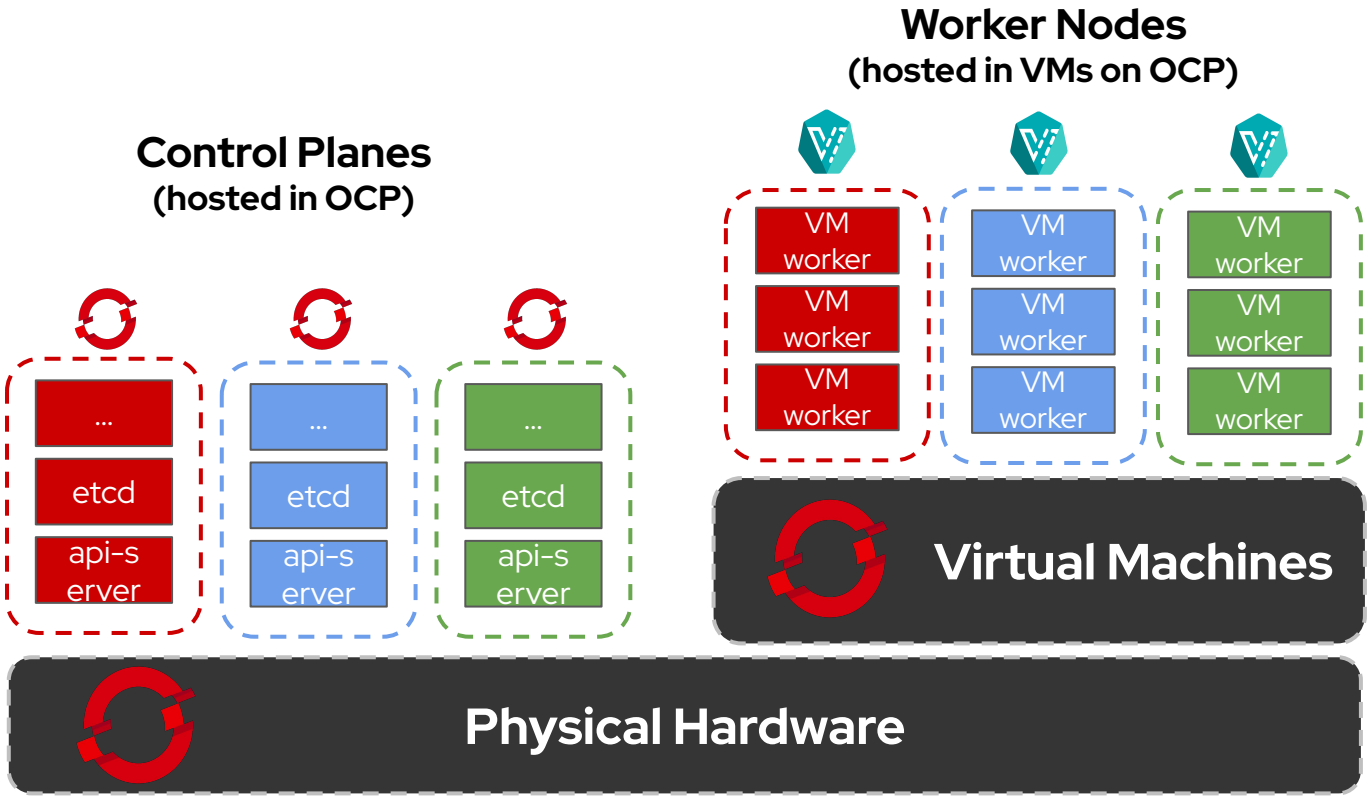
Hosted Control Planes with KubeVirt provider

Increase Utilization of Infrastructure

- Reduce unused and underutilized infrastructure
- Increase bare metal node utilization by deploying multiple hosted clusters.

Reduce Dependency on Legacy Virtualization

- Eliminate legacy hypervisor hosting your container platform.
- Underlying virtualization layer is included with hosted OpenShift cluster entitlements (no separate licensing needed)



Red Hat

Developer Tools Update

Red Hat

Developer Tools Update

Video & slides provide a deep dive

HIGHLIGHTS

- The **Developer Perspective** in **OpenShift Console** includes so many new features and improvements ... from RFEs including the ability for admins to define pre-pinned resources on Dev navigation, improved Helm user experience, users can easily identify which pods are receiving traffic in Topology as well as the Pods list view and more!.
- **Podman Desktop** adds new capabilities to help developers to go from containers, to pods and to OpenShift. Air Gapped installation is becoming available.
- **Odo 3.9.0 is now available** , Integration with OpenShift Toolkit IDE extension on VSCode and IntelliJ.
- **Janus/Backstage** What's happening and which plug-ins are available in project Janus.

Red Hat

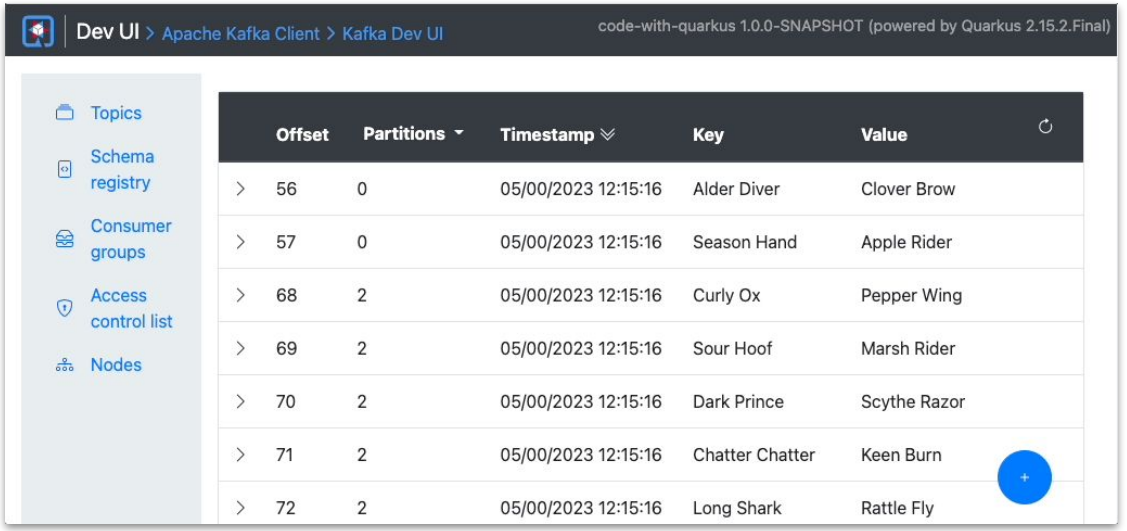
Runtimes

Red Hat

Kube Native Java with Quarkus

Key Features & Updates (Quarkus 2.13)

- **Java 17** support for JVM apps *and* native executables (GA)
- **Apache Kafka Dev UI**
  - Very useful when developing Kafka apps
  - List and create Topics, visualize and publish records
  - Inspect consumer groups and their consumption logs
- Improved **Dev Services**
  - New: **ElasticSearch**
    - No longer need to setup local ElasticSearch service
    - Integrated with Hibernate Search extension (automatic schema initialization)
  - Enhanced: **Infinispan** (upstream of **Red Hat Data Grid**)
    - Initialize cache from clients, generate cache keys
- **OpenID Connect** preconfigured providers
  - Simplified integration with Apple, Facebook, GitHub, Google, Microsoft, Spotify, and Twitter authentication.
- **Kubernetes Service Binding** support for Reactive SQL Clients
  - Workload projection for MariaDB, MySQL, SQL Server, Postgres, Mongo (TP), Kafka, reactive clients



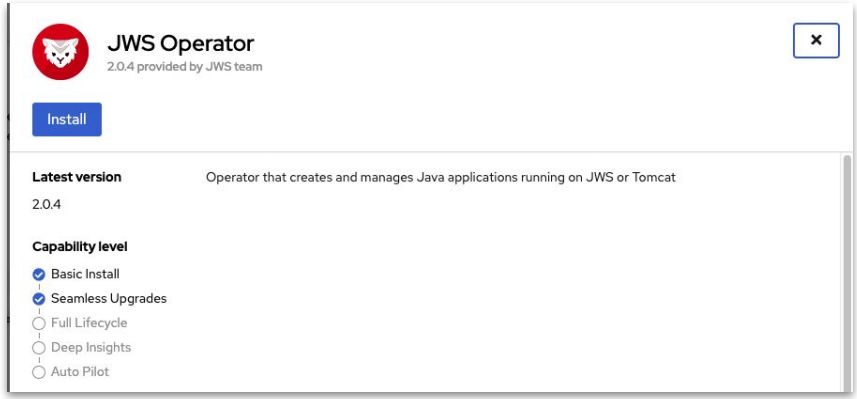
Kafka in the Dev UI

Red Hat

JBoss Web Server

Key Features & Updates (JWS 5.7)

- Upgrades to Tomcat 9.0.62, Tomcat-Native 1.2.31, Apache HTTPD 2.4.51
- **RHEL 9** full support
- Also includes minor updates to:
  - **tomcat-vault**: an extension used for securely storing passwords and other sensitive information used by JBoss Web Server.
  - **mod_cluster** - enables communication between JBoss Web Server and the Apache HTTP Server for load balancing
  - **Apache portable runtime** - enables access to advanced IO functionality; functionality at the operating system level; and native process handling such as shared memory, Unix sockets.
  - **OpenSSL** = a software library that implements SSL/TLS protocols and includes a basic cryptographic library.
- **JWS Operator** - Support for JWS 5.7 and enables seamless upgrades (Level II)



JWS Operator as seen in in OperatorHub

Red Hat

OpenJDK on OpenShift with Eclipse Adoptium

Key Features & Updates

- Adoptium is a community project to protect availability of free and open source Java SE distributions across multiple platforms
- Adoptium's *Temurin* distribution of OpenJDK has 400M+ downloads (200k/day)
- **Temurin is fully supported on OpenShift** for Java 8, 11, 17 applications
- Also includes:
  - **Production** support for Linux x64, win32, win64
  - **Developer** support for macOS x64 & aarch64, installation via zip, rpm, sdkman, homebrew, winget
  - **Container images** - published on DockerHub as official Docker images
  - **GitHub Actions** support

```yaml
steps:
- uses: actions/checkout@v3
- uses: actions/setup-java@v3
  with:
    distribution: 'temurin' # See 'Supported distributions' for available options
    java-version: '17'
- run: java HelloWorldApp.java
```

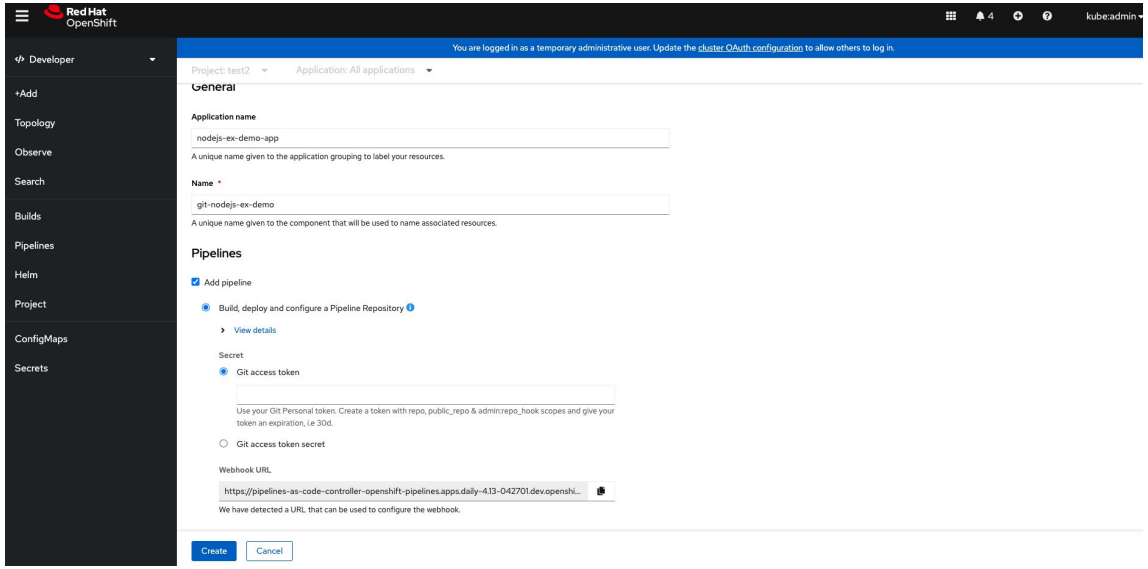

Red Hat

Platform Services

Red Hat

OpenShift Pipelines

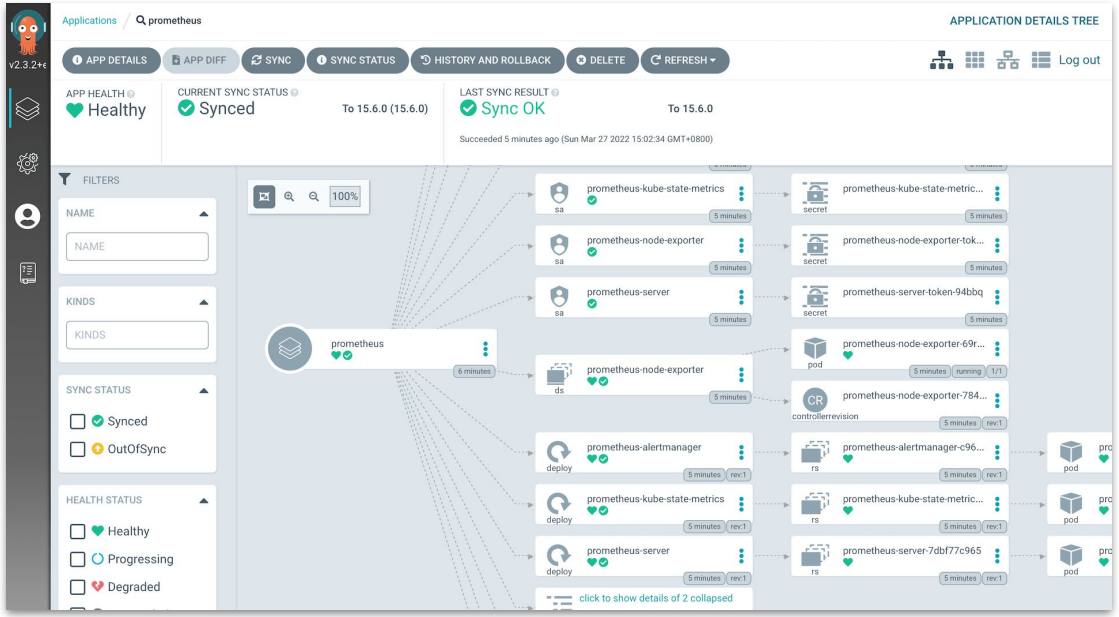
- **OpenShift Pipelines 1.10 (Tekton Pipelines 0.44)**
- Support of v1 API along with v1beta1
- Specify environment variables in a PipelineRun or TaskRun pod template to override or append the variables that are configured in a task or step
- **Custom tasks** in pipelines are enabled
- Owners file configuration in GitHub Interceptor
- **FIPS support** of Openshift Pipelines
- **Pipelines as code**
  - Support for custom console dashboards in addition to configuring a console for OpenShift and Tekton dashboards for k8s.
  - Better error logging
- Dev Console UX improvements :
  - Configure Pipelines As Code automatically if .tekton folder exists in repo while importing application from Git in dev console



Red Hat

OpenShift GitOps

- OpenShift GitOps 1.8
- Includes Argo CD 2.6
- Support for running on ARM
- Progressive sync for ApplicationSets (TP)
- Multiple sources for Applications (TP)

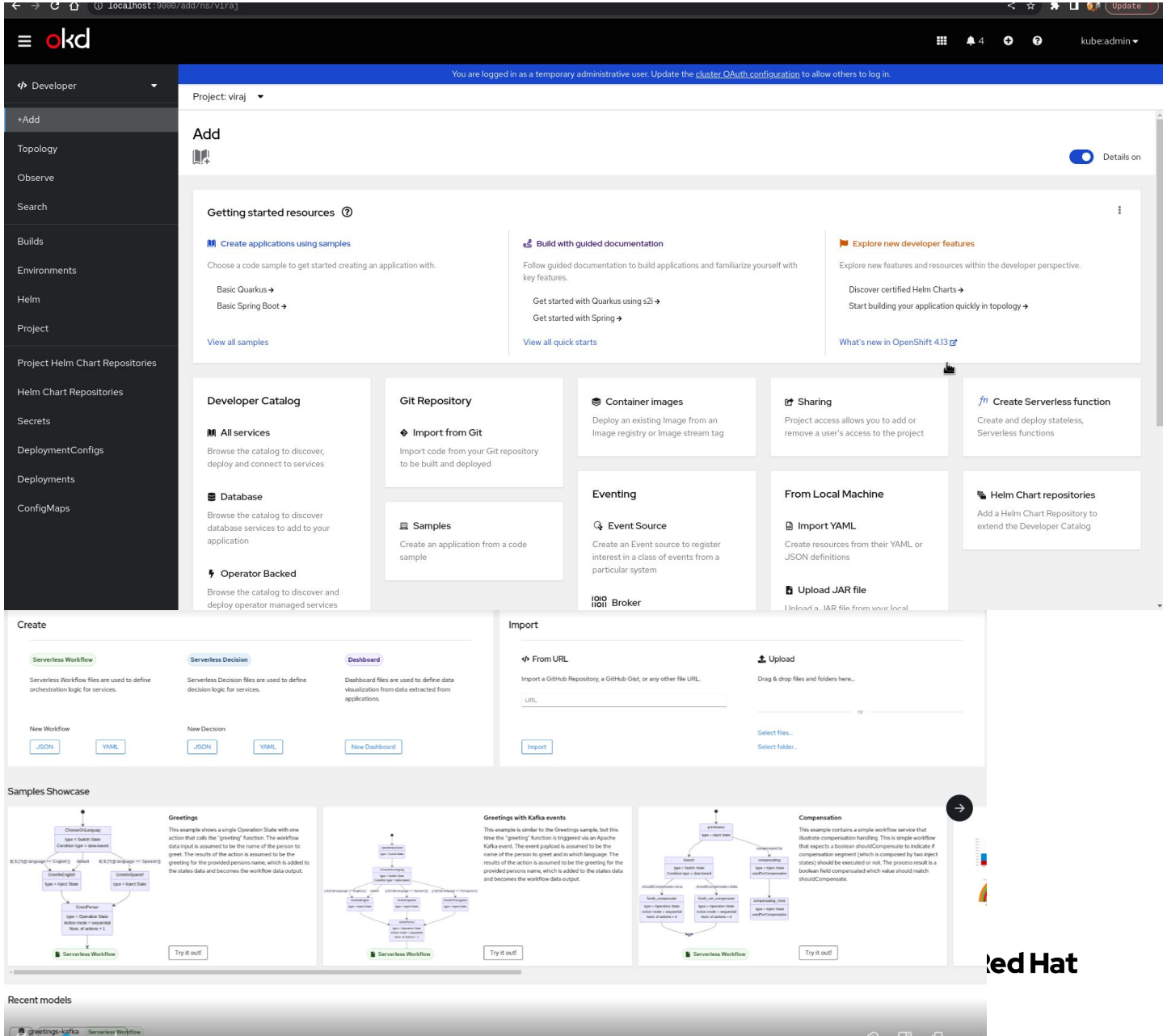


Red Hat

OpenShift Serverless

Key Features & Updates

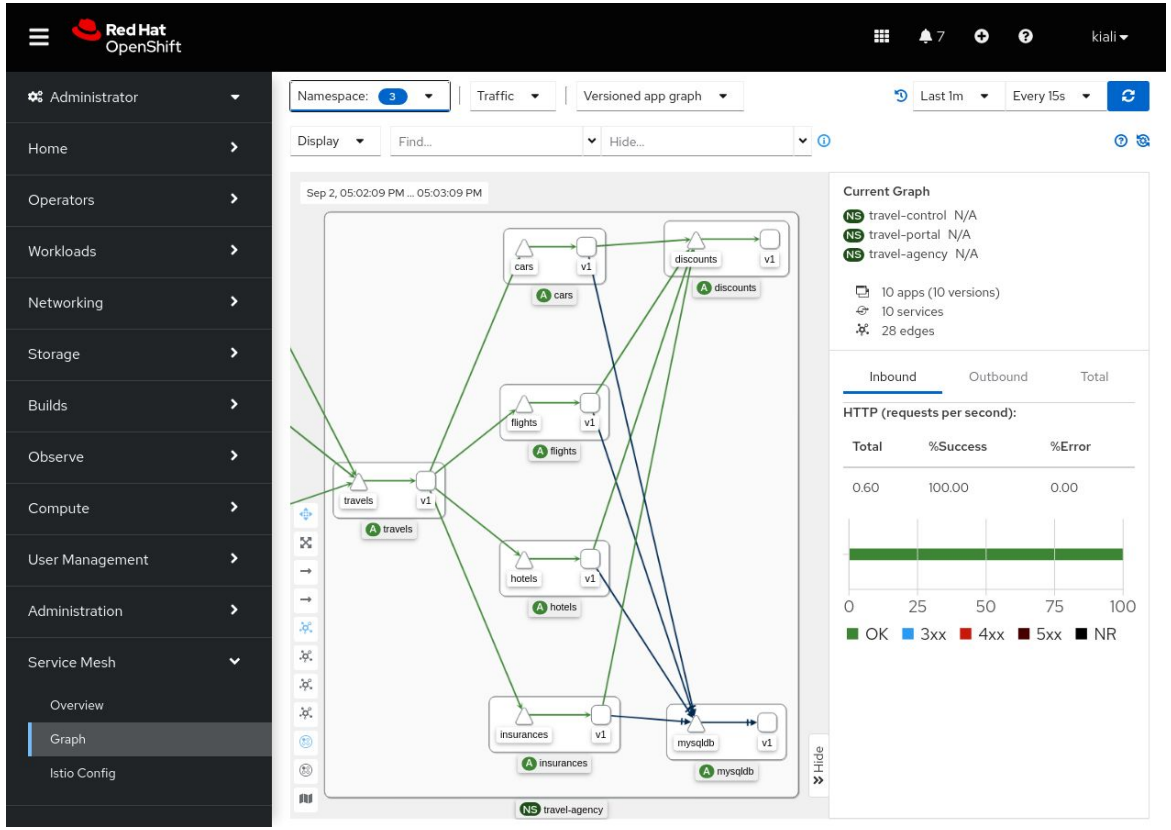
- Serverless 1.29 : Update to Knative 1.8
- Serverless functions
  - **New runtimes** : Node.js, TypeScript
  - In Cluster build using OpenShift Pipelines
  - Local experience with CLI and IDE (VScode and IntelliJ)
    Docker and Podman
  - Create Serverless functions from Dev Console
- Multi-Container support (Tech Preview)
  - Multi-container pod using a single Knative service
- Upgraded Serverless Logic (Dev Preview)
  - Orchestration for Functions and Services
  - CLI and Workflow Editor(UX)
- New Landing page for Serverless Documentation



ed Hat

OpenShift Service Mesh

- OpenShift Service Mesh 2.4 is coming soon!
- Based on **Istio 1.16** and **Kiali 1.65**
- New GA features:
  - **cluster-wide** installation option
  - Integration with **cert-manager**
  - **External Authorization** for Auth Policies
  - **Prometheus provider** for integrating with OpenShift user monitoring.
  - Documented support for control plane on OpenShift **infrastructure nodes**
- **Single Stack IPv6** is now Developer Preview
- Updated **Gateway API** is Technology Preview



Red Hat

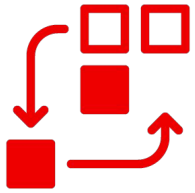
Installer Flexibility

Red Hat

OpenShift 4.13 Supported Providers

Installation Experiences

aws Outposts
AWS Local Zones
Azure
Azure Stack Hub
Alibaba Cloud
Bare Metal
Google Cloud
vmware vSphere
IBM Cloud
IBM Power Systems
IBM Z and IBM LinuxONE
NUTANIX
RED HAT OPENSTACK PLATFORM
RED HAT VIRTUALIZATION



Automated

Installer Provisioned Infrastructure

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

Full Control

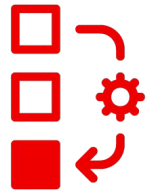
User Provisioned Infrastructure

- 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

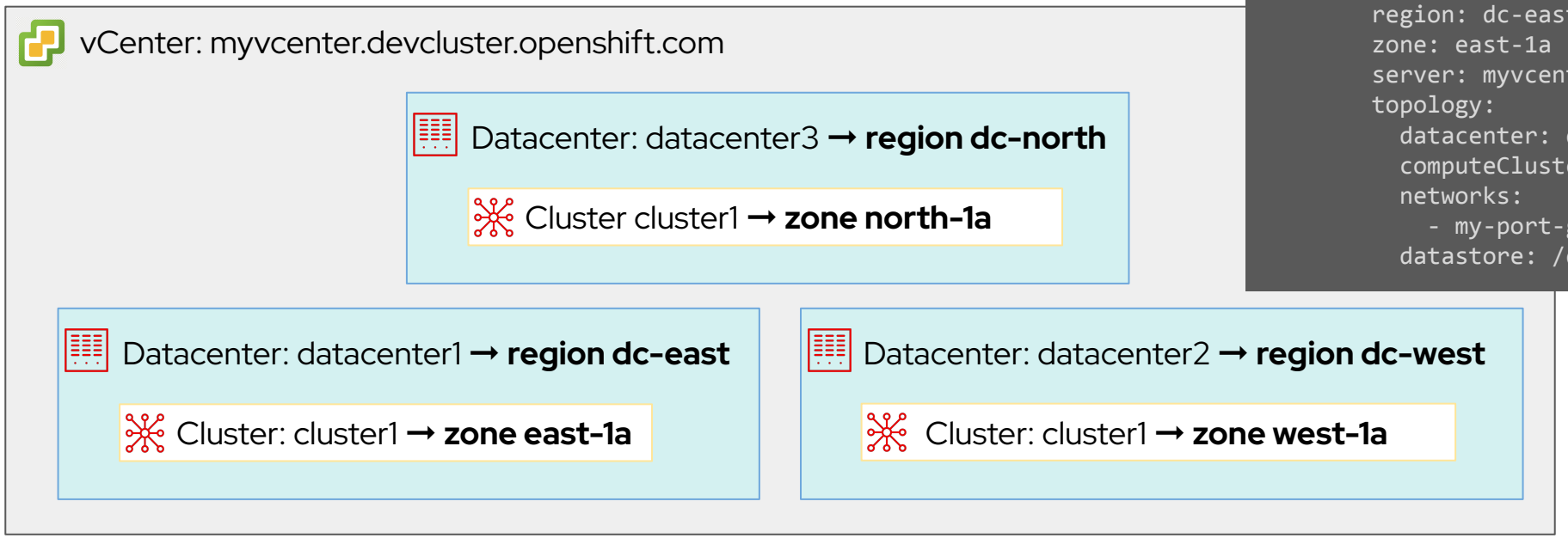
Red Hat

OpenShift in VMware vSphere is Zone Aware (GA)

- Eliminate single points of failure distributing OpenShift clusters in **Regions and Zones**
- Map vSphere Data Centers and Clusters to Regions and Zones
- Available for new installations in OpenShift 4.13

```
controlPlane:
  name: master
  replicas: 3
  platform:
    vsphere:
      zones:
      - "dc-east-1"
      - "dc-west-1"
      - "dc-north-1"
```

```
   failureDomains:
      - name: dc-east-1
        region: dc-east
        zone: east-1a
        server: myvcenter.devcluster.openshift.com
        topology:
          datacenter: datacenter1
          computeCluster: /datacenter1/cluster1
          networks:
            - my-port-group-in-dc1
          datastore: /datacenter1/datastore/share1
```



Red Hat

VMware vSphere Notable Changes OpenShift 4.13

Feature	OpenShift 4.13	Guidance
VMware vSphere 7.0 Update 1 or earlier*	Removed	Use VMware vSphere 7.0 Update 2 or later
VMware vSphere 8.0	GA	vSphere 8 is now supported with OpenShift 4.12 and OpenShift 4.13
Three-node clusters	GA	Three-node clusters are now supported
Dual stack VIPs	GA	On installer-provisioned vSphere clusters, you can use dual-stack networking

Additional details and guidance at OpenShift 4.13 Release Notes.

*Before upgrading OpenShift 4.12 to OpenShift 4.13, you must upgrade to **vSphere to v 7.0 Update 2 or later**; otherwise, the cluster will be **marked unupgradable**.

Red Hat

Additional VMware vSphere Enhancements

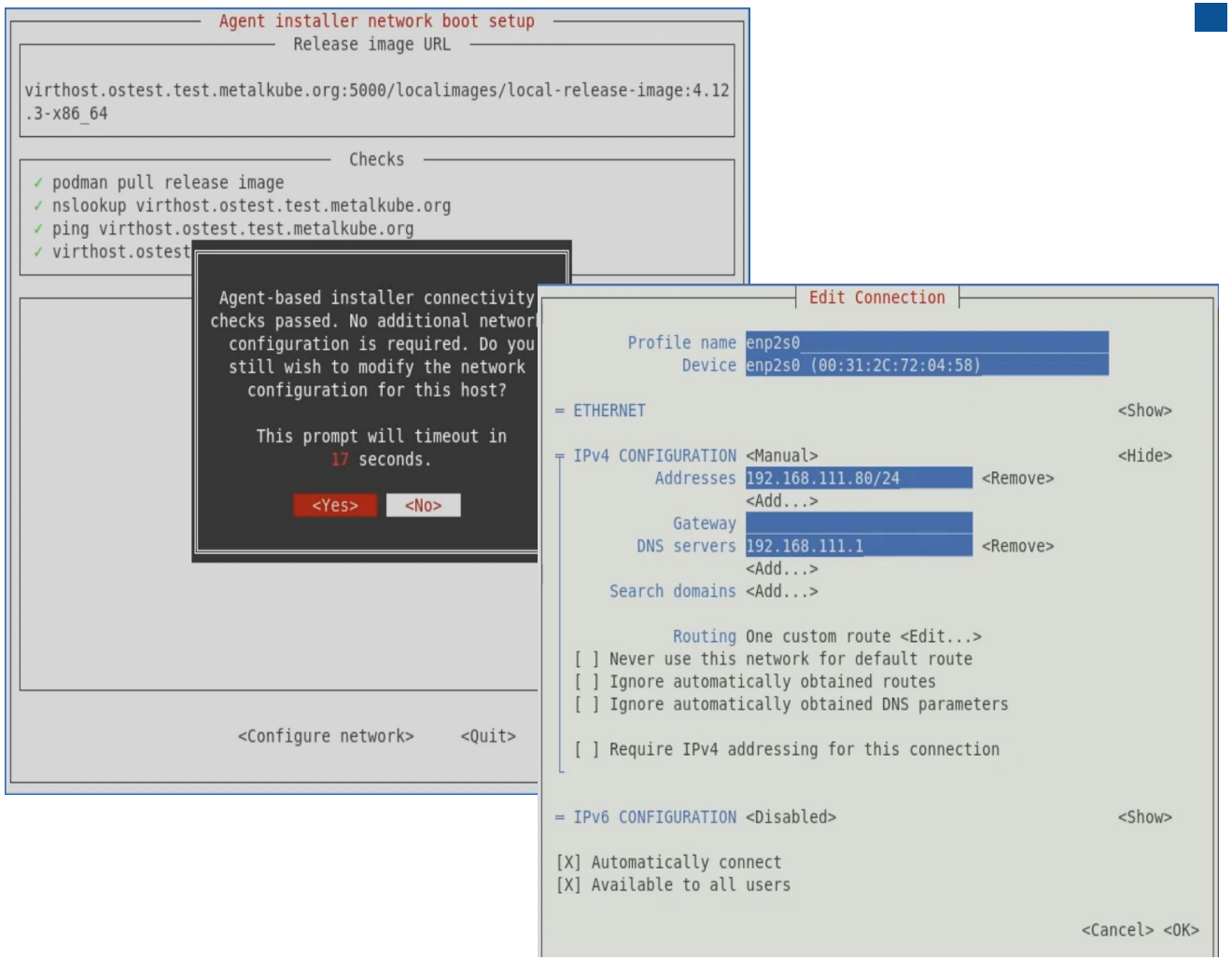
- vSphere encryption
  - Deploy OpenShift on encrypted vSphere VMs and encrypt PVs provisioned by the vSphere CSI driver to comply with corporate security policies or regulatory mandates
- vSphere CSI migration
  - New OpenShift 4.13 clusters have CSI by default
  - Existing clusters will migrate to CSI in OpenShift 4.14
  - Automatic migration to CSI not in OpenShift 4.13 due to an unresolved vSphere issue*
  - Opt-in option for CSI migration available in OpenShift 4.13
- OpenShift on VMware Cloud Verified clouds
  - Host OpenShift on a VMware vSphere infrastructure on-premises or on VMware Cloud Verified providers that meets VMware vSphere infrastructure requirements

* https://github.com/kubernetes-sigs/vsphere-csi-driver/issues/2165 | https://kb.vmware.com/s/article/91752 | https://issues.redhat.com/browse/OCPBUGS-5817

Red Hat

Agent Installer Network Setup at Boot Time

- Configure the host network via a new Text User Interface
  - Installer will allow users to configure the host network during the installation interactively.
  - Config still set before booting installer.
  - If checks fail the installer will ask to reconfigure the network



Red Hat

Scale UPI Clusters with the Bare Metal Operator

- Automate the provisioning of new bare metal nodes using their BMC
- Scale using Redfish Virtual Media (not iPXE)

```
# bmh.yaml
---
apiVersion: v1
kind: Secret
metadata:
  name: worker1-bmc
  namespace: openshift-machine-api
type: Opaque
data:
  username: <base64_of_uid>
  password: <base64_of_pwd>

---
apiVersion: metal3.io/v1alpha1
kind: BareMetalHost
metadata:
  name: worker1
  namespace: openshift-machine-api
spec:
  bmc:
    address: <protocol>://<bmc_url>
    credentialsName: "worker1-bmc"
  bootMACAddress: <nic1_mac_address>
  externallyProvisioned: false
  customDeploy:
    method: install_coreos
  online: true
  userData:
    name: worker-user-data-managed
    namespace: openshift-machine-api
```

```
$ oc create -f bmh.yaml
```


Red Hat

Flexible OpenShift Installation

Disable/enable operators from installation

- Exclude one or more optional operators during installation
- Option to enable a previously excluded operator after cluster is installed
- Optional operators you can exclude:
  - Node tuning operator
  - (in addition to baremetal operator, console operator, csi-snapshot-controller operator, Insights operator, marketplace operator, storage operator, and openshift-samples operator)
- Disable by setting **baselineCapabilitySet** and **additionalEnabledCapabilities** parameters in the **install-config.yaml** configuration file prior to installation

More at Customize your Kubernetes - OpenShift gets composable and Optional Capability Product Documentation

OpenShift on cloud providers

- Shared VPC (XPN) deployment support with installer-provisioned infrastructure (GA)
  - Deploy OpenShift in GCP Service Project while networks defined in GCP Host Project moved to GA
- Confidential computing in GCP (TP)
  - Take advantage of the “Isolation” feature to ensure data is secure and encrypted while in use
- Shielded VMs in GCP
  - Protect workloads running on these hardened VMs from threats like remote attacks, privilege escalation, and malicious insiders
- Single click control plane scaling in Azure and GCP
  - Leverages control plane machine sets to manage the cluster’s control plane machines and adds additional automation on existing Machine API concepts
- Compact 3-node clusters support in AWS, Azure and GCP
  - Take advantage of new form factor with 3 control plane nodes with no workers, wherein the control plane and cluster workloads run on the same nodes
- New GCP and AWS regions
  - **GCP**: Santiago (Chile), Milan (Italy), Madrid (Spain), Paris (France), Columbus (Ohio), Dallas (Texas), Tel Aviv (Israel), Turin (Italy)
  - **AWS**: UAE, Spain, Zurich, Hyderabad and Melbourne
- AWS Local Zones extended integration
  - Enhance the installation experience for a user to be able to deploy “edge” Machines on AWS Local Zones into an existing VPC from day-0

Red Hat

Azure User Tags (TechPreview)

New field .platform.azure.userTags

- Tags can only be configured during cluster creation
- Tags required for internal use added to all resources
- Supported for resources created on AzurePublicCloud alone.

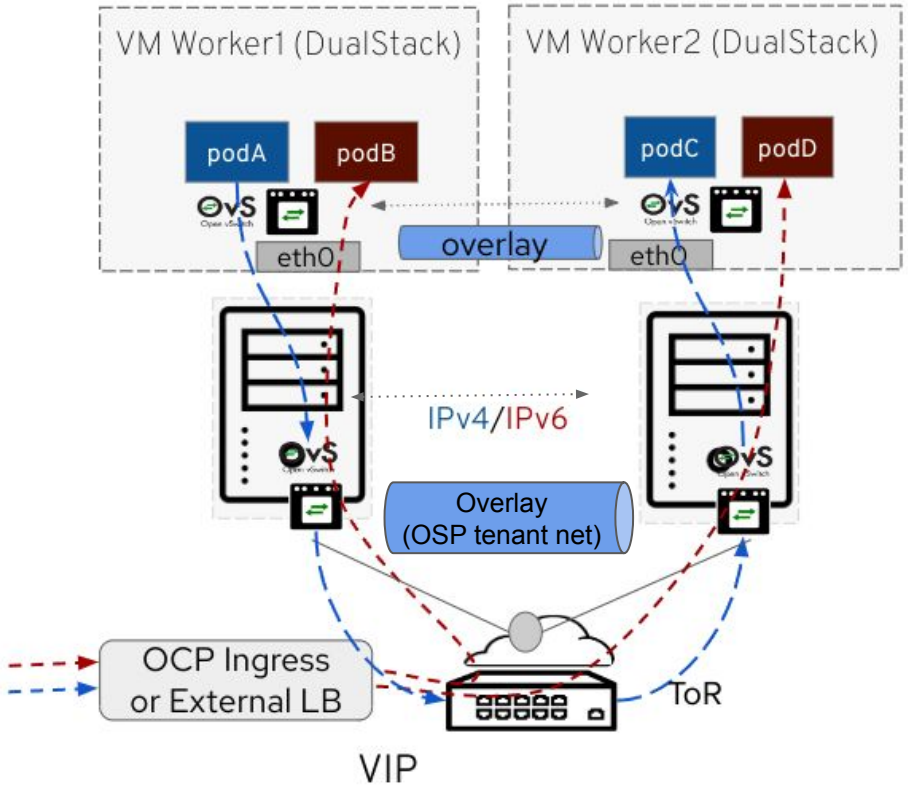
```
Unset
apiVersion: v1
featureSet: TechPreviewNoUpgrade
platform:
  azure:
    cloudName: AzurePublicCloud
    userTags:
      environment: demo
      .
      .
      <key>: <value>
```

```
Unset
apiVersion: config.openshift.io/v1
kind: Infrastructure
metadata:
  name: cluster
spec:
  platformSpec:
    type: Azure
status:
  infrastructureName: azure-tags-demo
  platform: Azure
  platformStatus:
    azure:
      resourceTags:
      - key: environment
        value: demo
    type: Azure
```


Red Hat

OpenShift On OpenStack 4.13 Update

- Dual Stack in Dev Preview
  - Driven by several Telco customers as 5G Workloads expand
  - Ctlplne and dataplane running dual stack
  - Added to the dual stack functionality already supported on the 2ndary interfaces
  - Support Openstack Provider Networks and ML2/OVN tenant networks with OVNKubernetes double encapsulation
- Kuryr to OVNKubernetes migration in Tech Preview (GA in 4.14)
  - Following Kuryr deprecation notice in 4.12
  - Targeting removal in 4.15



Red Hat

Control Plane Updates

Red Hat

Crun and Cgroup V2

(GA as non default)

Crun

- An OCI-runtime written in C.
- Faster and lower memory footprint than runc.

Cgroup V2

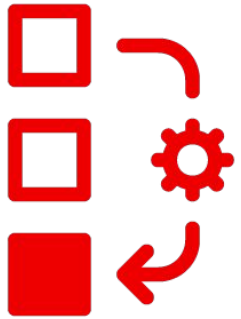
- Next generation of cgroups in the kernel. All new development happens in v2.
- Better node stability under OOM pressure scenarios.
- Better page cache write-back accounting.
- Current implementation is a 1:1 with v1 but it opens the door to start consuming new v2 specific features.

Red Hat

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



Red Hat

Run once duration override Operator

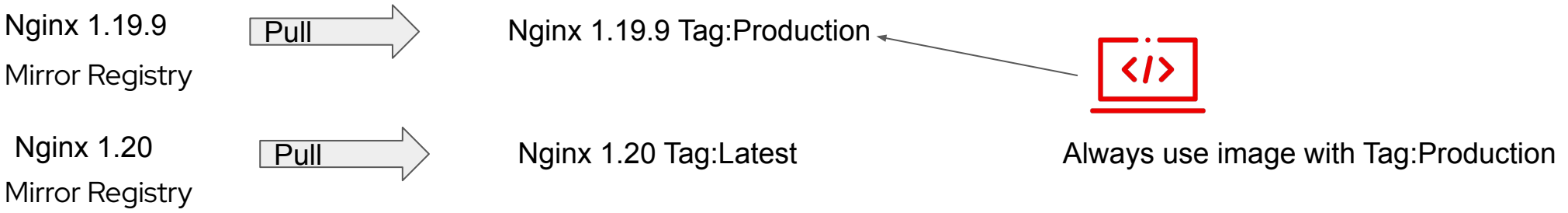
GA

- Customers will be able to configuring a default value for activeDeadlineSeconds for all "run once" pods like the builder, deployer, and jobs
- The duration is counted from the time when a first pod gets scheduled in the system, and defines how long a job can be active.
- Install RunOnceDuration operator from Operator hub

Red Hat

Allow mirroring Image by Tag

GA



Customer now has ability to tag mirrored images. This allows you to reference images by tag, which can be used consistently across deployments, even if the image is updated in the upstream registry.

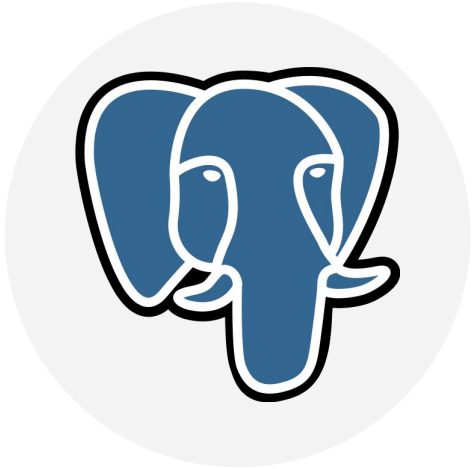
Red Hat

Security

Red Hat

4.0 Major Release

Central's DB moves to PostgreSQL



Performance & scale
Database queries are now faster. Better scalability

Easy upgrade
Seamless migration from 3.74 with Operator

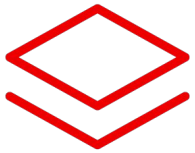
ACSCS proven
ACS Cloud Service has been running on Amazon RDS since 3.73

BYODB (Bring Your Own DB) - **Tech Preview in 4.0**

- Leverage existing investment in PostgreSQL
- Utilize cloud PostgreSQL database service.

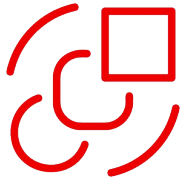
Red Hat

Vulnerability Management



Red Hat Enterprise Linux CoreOS (RHCOS) Host Node Vulnerability Scanning

- RHACS 4.0 release introduces **RHCOS node host scanning** for security vulnerabilities
- **The scope:** RHCOS RPMs installed on the node host as part of the RHCOS installation for any known vulnerabilities



Clair Scanner Consolidation Major Milestone: Clair version 4 Integration

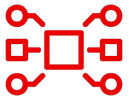
- RHACS 3.74 introduces integration option with **upstream Clair v4** to get image vulnerability scan data.

Red Hat

General Product Improvements (3.74, 4.0)

Validation on FIPS Compliant Red Hat OpenShift

RHACS functionality has been validated on OpenShift 4.12 running in FIPS mode



Processes Listening on endpoints API

- Assess security posture by looking which deployments and associated processes have open ports.
- This is a planned enabler for a larger feature set (real-time NW graph, new policies/alerts, historic data of connections,...)

IBM Power, IBM zSystems, and IBM® LinuxONE support for secured clusters

Secure clusters with RHACS where Red Hat OpenShift cluster nodes are running on IBM servers:

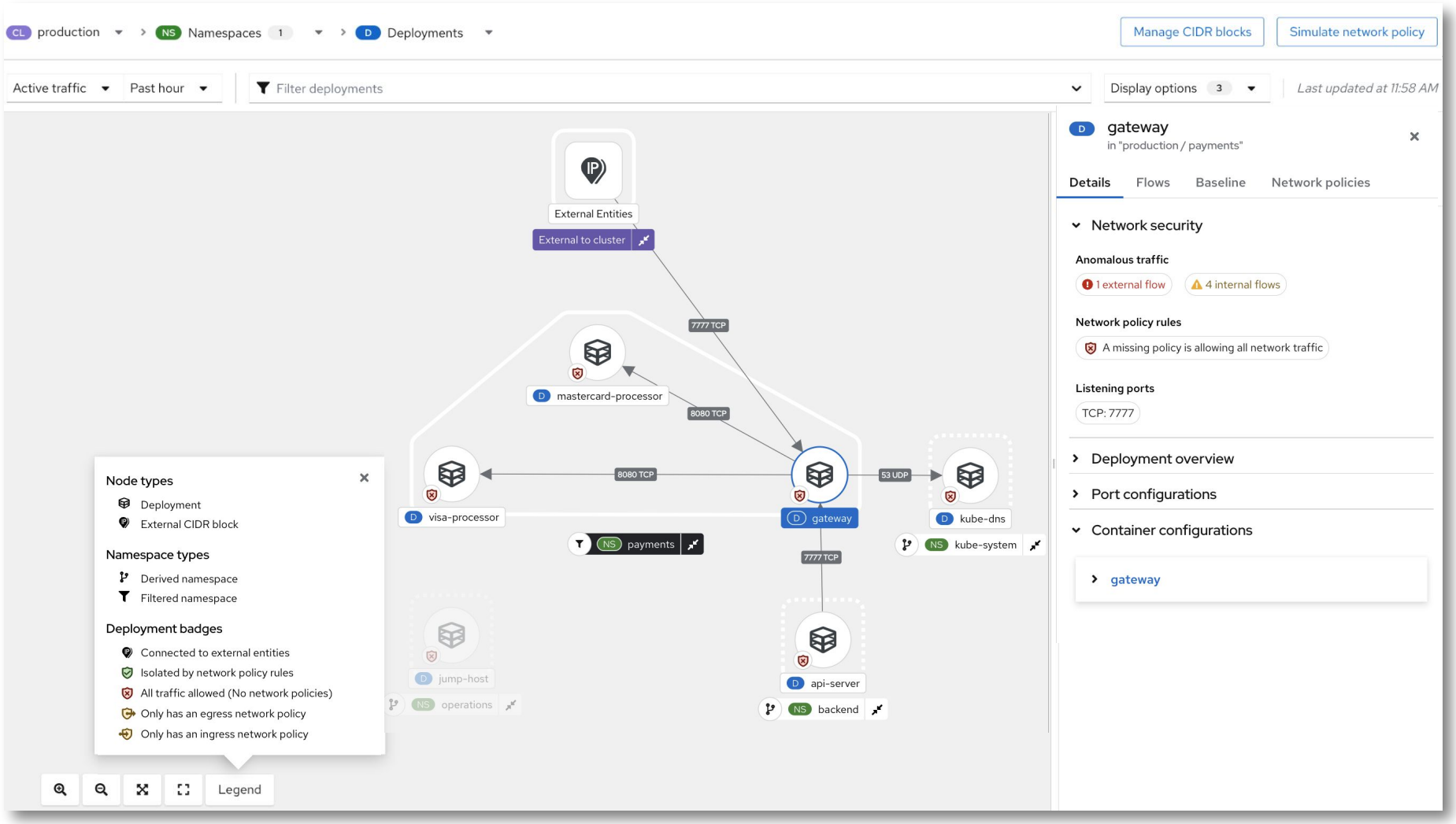
- Red Hat OpenShift 4.12 on IBM Power (ppc64le)
- Red Hat OpenShift 4.10 and 4.12 on IBM zSystems (s390x) and IBM® LinuxONE (s390x)

Red Hat

Network Graph 2.0

- Crisp display
- Easier to use side panel
- Deployment Badges
- Display Options to control level of detail

NWG 1.0 is deprecated and will disappear in RHACS 4.1



Red Hat

Kubernetes Network Policy Generation

Automated in Build time

Pod isolation can reduce risk of

- Data leakage / exfiltration
- Unauthorized access
- Lateral movement by attackers
- Denial of Service attacks

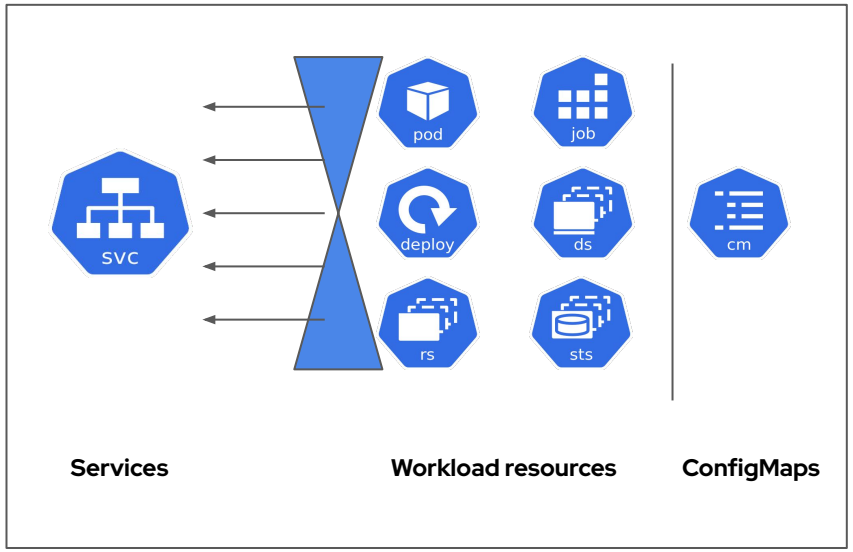
ACS Build Time tool (tech preview)

```
% roxctl generate netpol
```

Input : folder with manifest YAMLs

output: network policies

- Tight ingress/egress per flow
- Default deny namespaces
- Allow DNS only if we detect it is required.
  - Prevent DNS Data Exfiltration.



NP-Guard Red Hat

ACS Collections[1]

Describe the organization's view of their deployments

A new type of **named reference** object in ACS

Create a logical grouping using selection rules:

- Static identifiers: Cluster ID, Namespace name, Deployment name
- Dynamic identifiers: Cluster label , NS Label , Deployment label

Reusable

Named References

Recursive

May include other collections

Dynamic

- Resolved in run time
- Include identifiers that may not exist at the time of definition

[1] *Initially (4.0) used in Vulnerability Reporting. Use in Policy Management on the roadmap*

Red Hat

Red Hat Advanced Cluster Security

What's New Summary

RHACS 3.73

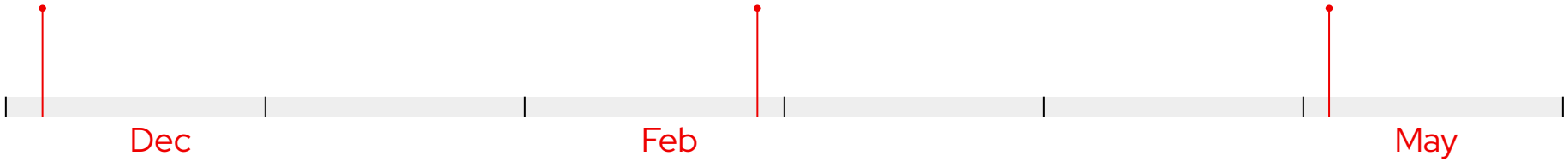
ACSCS Field Trial
PostgreSQL TP,
Build Time Network Policy Generation

RHACS 3.74

IBM Power, Z, LinuxOne
Clair Scanner V4 support
Network Graph 2.0
Vuln Reporting with Collections (1)
Policy Categories (1)

RHACS 4.0

ACSCS Limited Availability
PostgreSQL GA
RHCOS Scanning



(1) *Requires PostgreSQL*

Red Hat

Enable etcd encryption with AES-GCM ciphers

- AES-GCM is a secure cipher suite for encrypting etcd data at rest.
- AES-GCM is considered a stronger cipher than AES-CBC.
- Configuration enables using AES-GCM ciphers with a random nonce and a 32 byte key to perform the encryption.
- Encryption keys are automatically rotated weekly.

Adding aesgcm to APIServer configuration

```
spec:
  encryption:
      type: aesgcm
```

PSa enforcement (Tech Preview)

PSa Default config 4.13

```
{
 "configuration": {
  "apiVersion":
"pod-security.admission.config.k8s.io/v1beta
a1",
  "defaults": {
   "audit": "restricted",
   "audit-version": "latest",
   "enforce": "privileged",
   "enforce-version": "latest",
   "warn": "restricted",
   "warn-version": "latest"
  },
  "exemptions": {
   "usernames": [

"system:serviceaccount:openshift-infra:build
-controller"
   ]
  },
  "kind": "PodSecurityConfiguration"
 }
}
```

Test PSa enforcement for workloads with FeatureGate

```
oc patch featuregate cluster -p '{"spec":
{"featureSet":
"TechPreviewNoUpgrade"}}' --type
merge
```

PSa enforced config

```
 "configuration": {
  "apiVersion":
"pod-security.admission.config.k8s.io/v1beta
a1",
  "defaults": {
   "audit": "restricted",
   "audit-version": "latest",
   "enforce": "restricted",
   "enforce-version": "latest",
   "warn": "restricted",
   "warn-version": "latest"
  },
  "exemptions": {
   "usernames": [

"system:serviceaccount:openshift-infra:build
-controller"
   ]
  },
  "kind": "PodSecurityConfiguration"
 }
}
```

Red Hat

Management

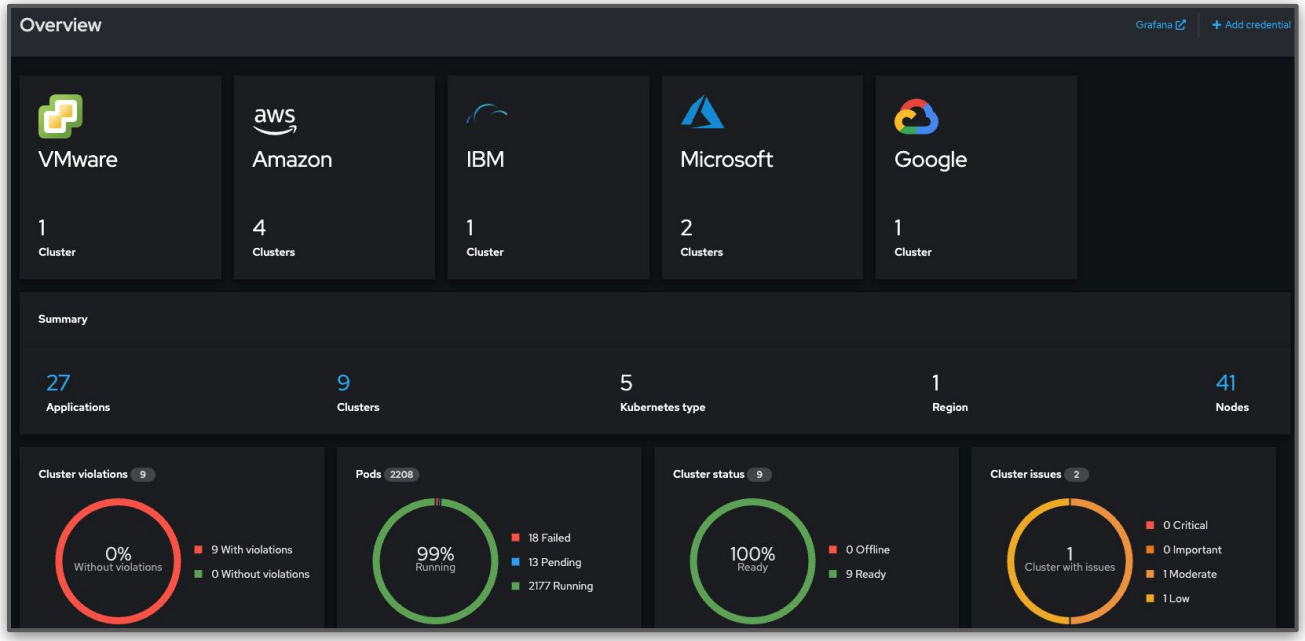
Red Hat

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.8

Delivering Value

We are listening to your feedback, iterating with intention, and we are focused on delivering unique value to our customers.



- Deploy and manage Hosted Control Planes (HyperShift)
  - TP - BareMetal agent, BareMetal KubeVirt, AWS
- Fine grained RBAC for RHACM Observability (DP)
- Right-size recommendations for namespaces (DP)
- Observability support for GCP WIF token
- OpenShift GitOps ApplicationSet pull model (TP)

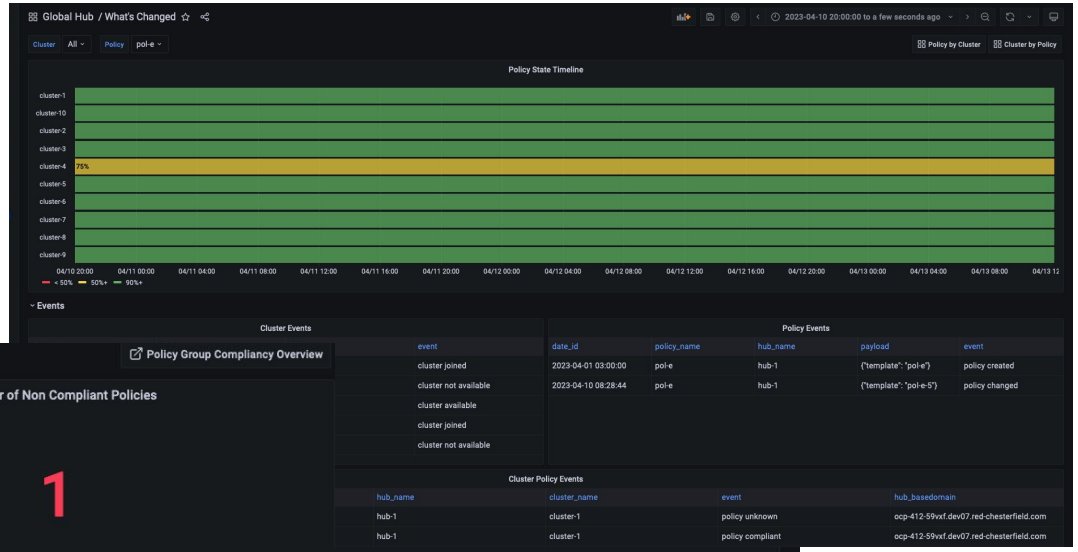
Red Hat

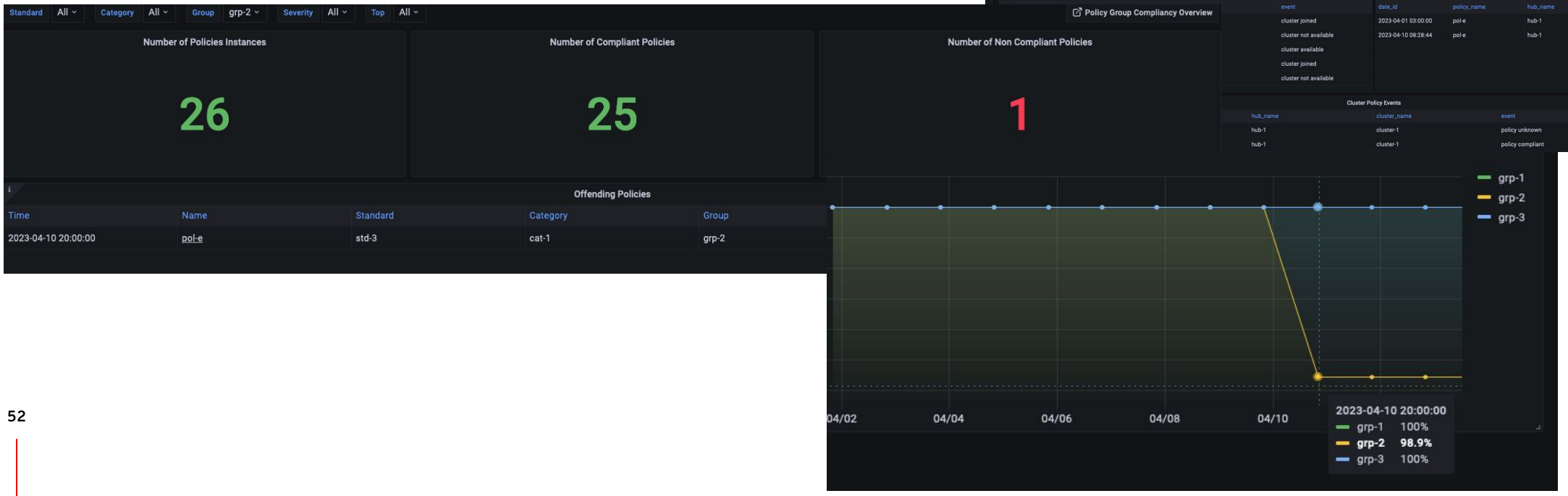
Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.8

Global Hub 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 (TP)**
  - **Policy Compliance Status and Trend (TP)**
  - Policy compliance state and policy trends across multiple RHACM Hubs
  - **Quickly Assess and Audit (TP)**
  - Report the count of compliance states across the last 30 days
  - Show the compliance for production clusters for the last 30 days





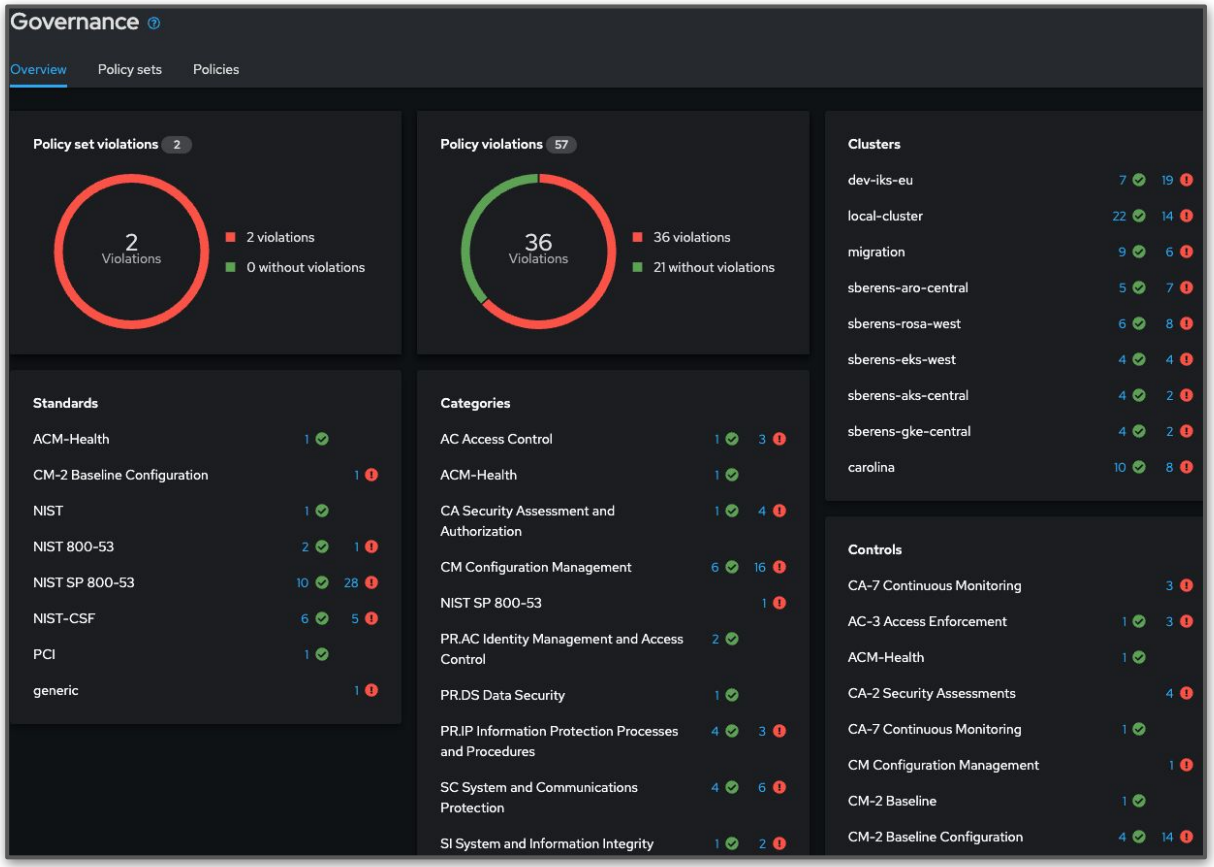
Red Hat

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.8

Governance

Red Hat Advanced Cluster Management's Governance framework is continuously evolving to keep up with the growing Kubernetes policy landscape.



- **ACM Templatized Policies: add support for ranges for policy simplification**
  - As a policy user, I would like to use ranges in my policy templates to avoid duplication in my object-templates definition.
  - As a policy user, I would like to use conditionals around arrays and objects so that I can avoid duplicating policies for different environments.
- **Improve the RHACM policy experience with Gatekeeper constraints**
  - Support Gatekeeper constraints natively in RHACM policies.
  - Make adoption of Gatekeeper easier
- **Out of the box PolicySet for installing and managing OpenShift Platform Plus**

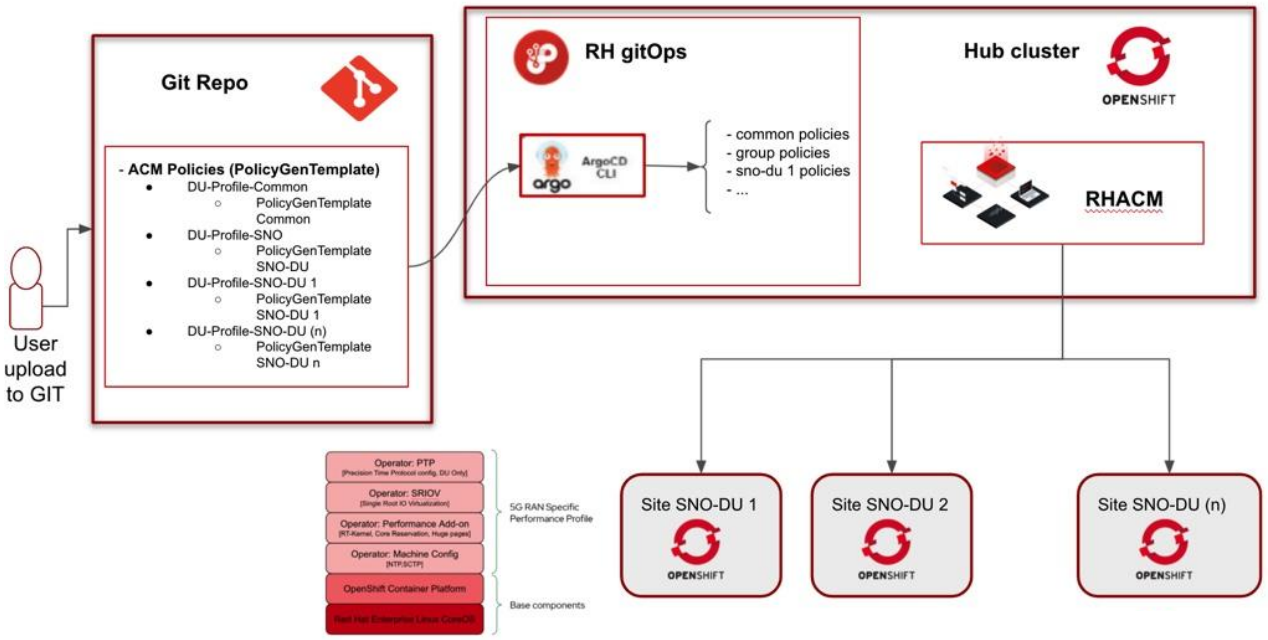
Red Hat

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.8

Manage At Scale

Consistency at scale for edge use cases across many industries including Telco, Industrial and Commercial. RHACM helps by providing a single api, cli and user interface to standardize regardless of where your application runs.

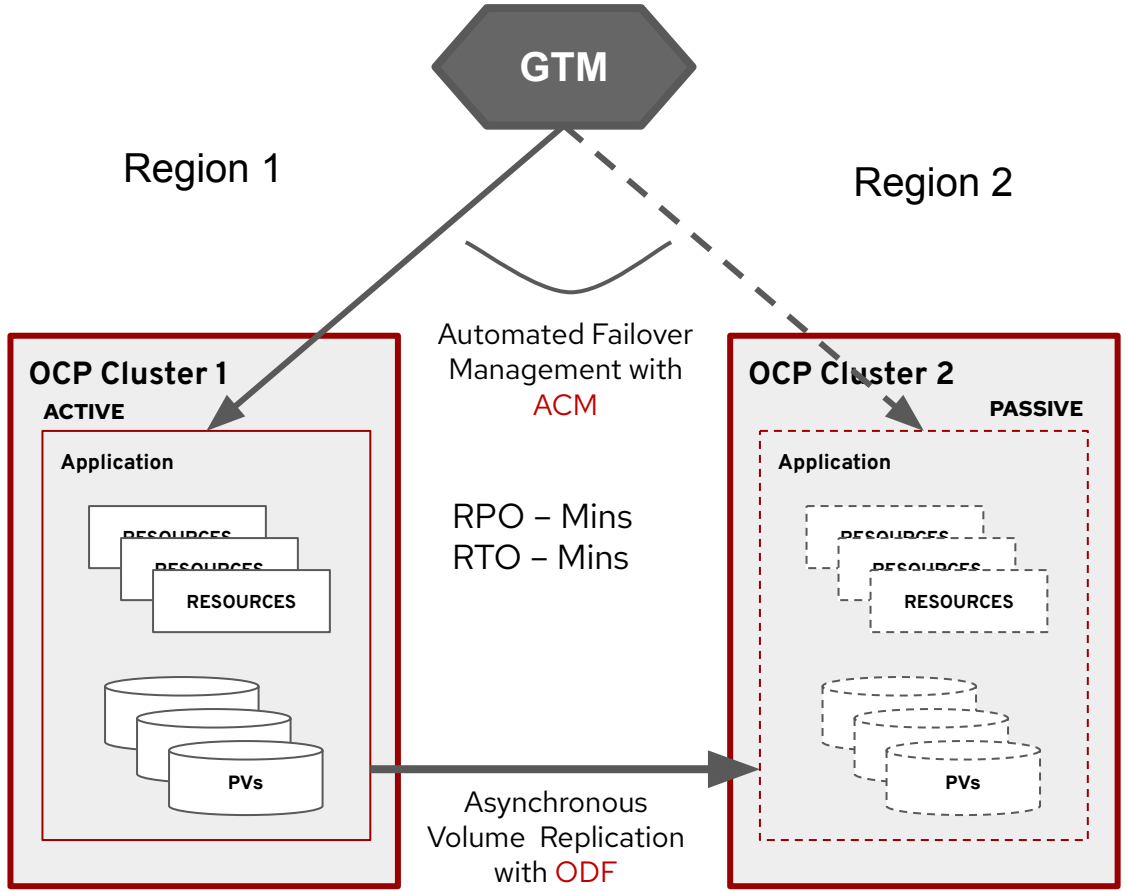


- **Extend scale** in a mixed fleet of OpenShift clusters
  - ACM create & manage 3500 SNO with the DU Profile
  - Mixed - 857 SNOs, 200 3 Node, 200 Standard Clusters deployed, across 91 hypervisors with the DU Profile
  - 3 Node - 432 Compact Clusters deployed, across 48 hypervisors with the DU Profile
  - Standard - 207 Standard (3 control-plane, 3 workers) Clusters deployed, across 48 hypervisors with the DU Profile

Red Hat

Red Hat Advanced Cluster Management for Kubernetes and OpenShift Data Foundation

Business Continuity

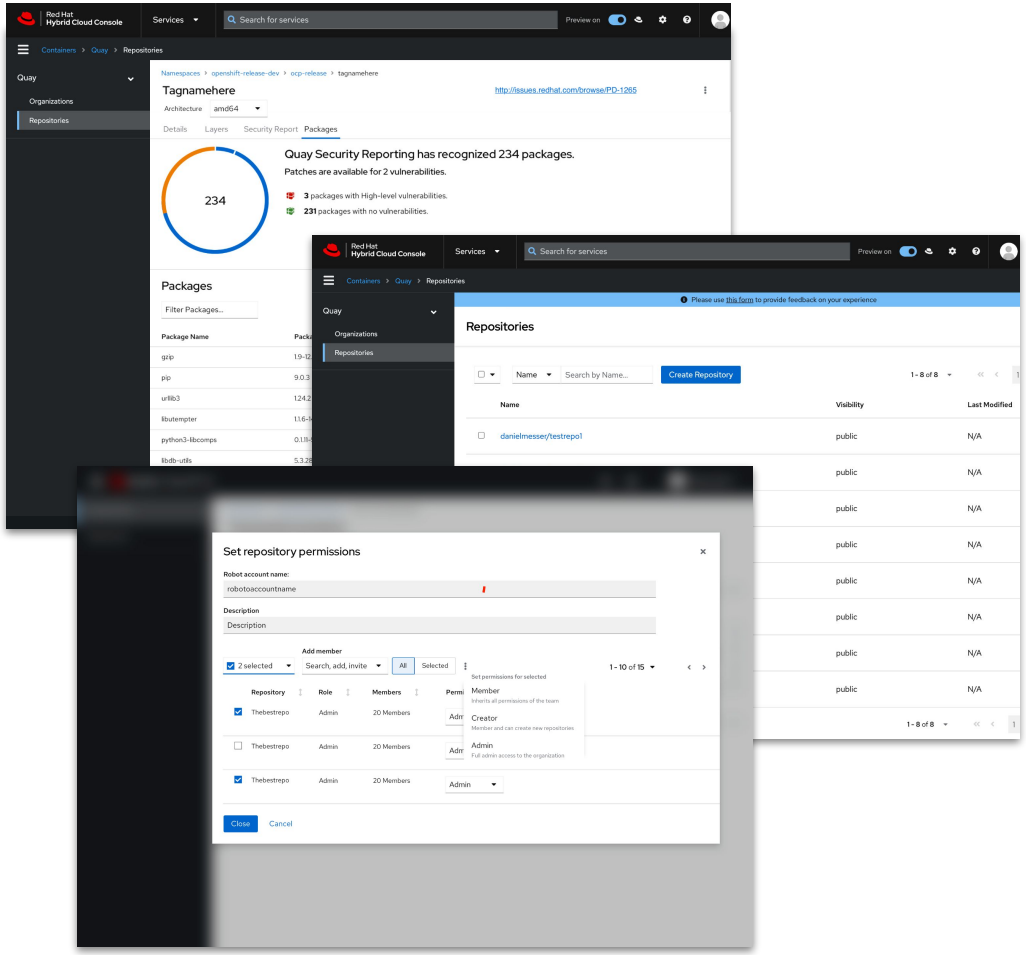


- **Regional stateful app replication with ODF 4.13 (GA)**
- **Asynchronous Volume Replication => low RPO**
  - OpenShift Data Foundation (ODF) enables cross cluster replication of data volumes with low replication intervals
  - ODF Storage operators synchronizes both volume persistent data and kubernetes metadata for PVs
  - *No distance limitations between peer clusters*
- **Automated Failover Management => low RTO**
  - ACM Multi-Cluster manager and ODF DR operators enables failover and failback automation at application granularity
  - Both clusters remain active with Apps distributed and protected by the alternate cluster

** Regional DR provided in conjunction with OpenShift Data Foundation Advanced 4.13. Please review the ODF-Advanced release schedule for specific details.

Red Hat

Red Hat Quay & Quay.io



Quay.io moving into console.redhat.com

Quay.io will be integrating with the Red Hat Hybrid Cloud Console. Billing via AWS Marketplace and POs will be possible.

Completely new User Interface

Effectively manage your central source of truth for all containerized content in an effective, yet familiar way.

Enterprise Logging Integration

Increased registry event logging coverage and Splunk log forwarding to keep an audit trail of all user actions in Quay 3.9.

Improved Storage Consumption Tracking

Faster and more accurate accounting for storage consumption by images with the ability to delete immediately.

Red Hat

Observability

Red Hat

OpenShift Observability: Five Pillars

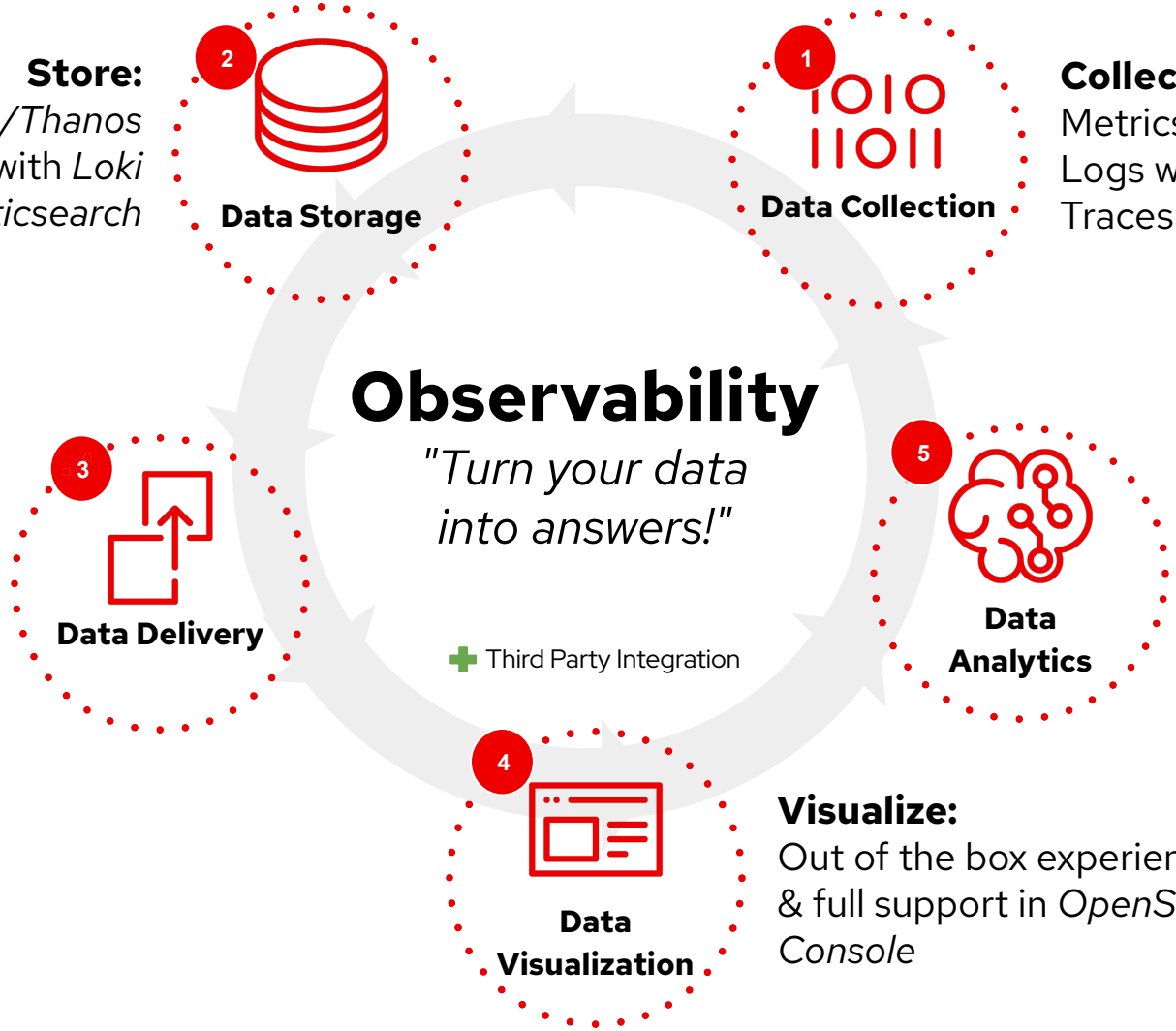
Store:
Metrics with *Prometheus/Thanos*
Logs with *Loki*
Traces with *Jaeger/Elasticsearch*

Collect:
Metrics with *Prometheus*
Logs with *Vector*
Traces with *OpenTelemetry*

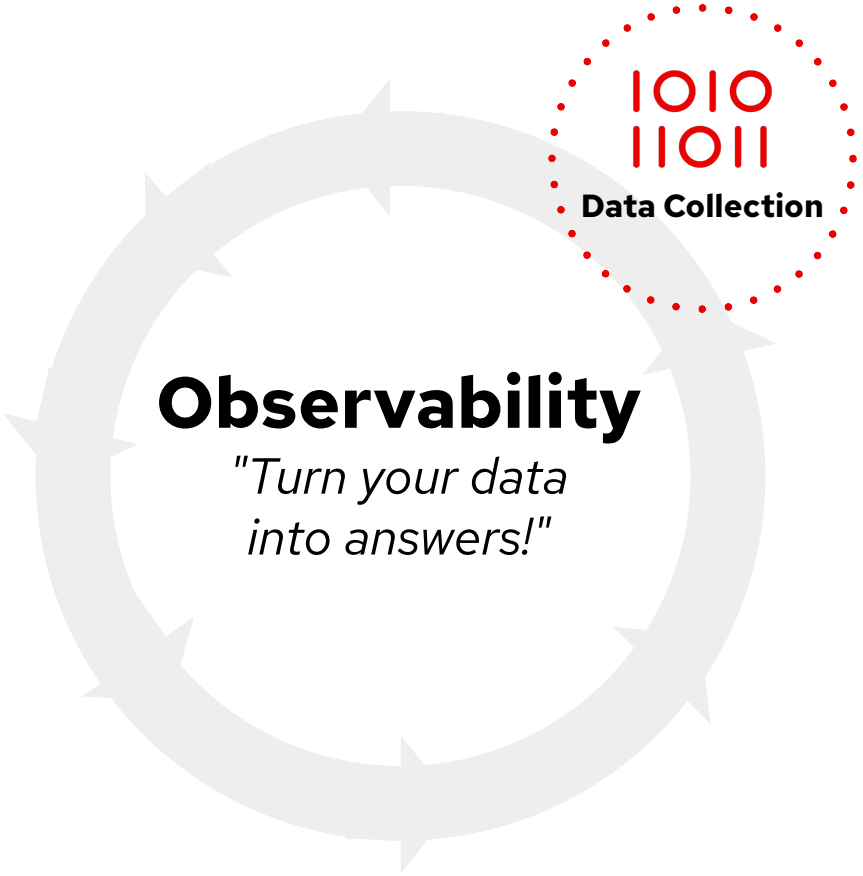
Deliver:
Aggregate & Normalize data
Transport it with *Observability Operator*

Visualize:
Out of the box experience
& full support in *OpenShift Web Console*

Analyze:
Query metrics
Search metrics targets
Filter logs by severity



Red Hat



OpenShift 4.13 Monitoring

- Customizations for node-exporter collectors tcpstat, netclass, netdev, cpufreq
- Design scrape profiles in CMO
- VPA metrics

Logging 5.7

- Vector - Multiline exception traces are forwarded as single log entries

Distributed Tracing 2.8

- Tech Preview: Multi-cluster tracing data collection

Observability

"Turn your data into answers!"

OpenShift 4.13 Monitoring

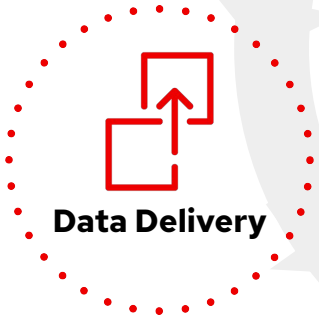
- Allow to specify secrets in alertmanager component
- Version updates to Monitoring stack components & dependencies
- Alertmanager proxy environment

Logging 5.7

- Loki - OpenShift Administrators and Application Owners can create alerting rules based on logs

Distributed Tracing 2.8

- Tech Preview: Ability to store tracing data in Tempo using S3 compatible storage
- Tech Preview: Multitenancy



Observability

"Turn your data into answers!"

OpenShift 4.13 Monitoring

- Cluster Monitoring Operator available without ingress controller
- Allow node related filters
- Telemeter remote write

Logging 5.7

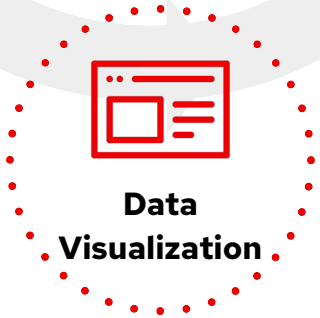
- Vector support for forwarding logs to both Syslog and HTTP targets

Distributed Tracing 2.8

- Tech Preview: Tempo integration provides same data access mechanisms as Elasticsearch.

Observability

"Turn your data into answers!"



OpenShift 4.13 Monitoring

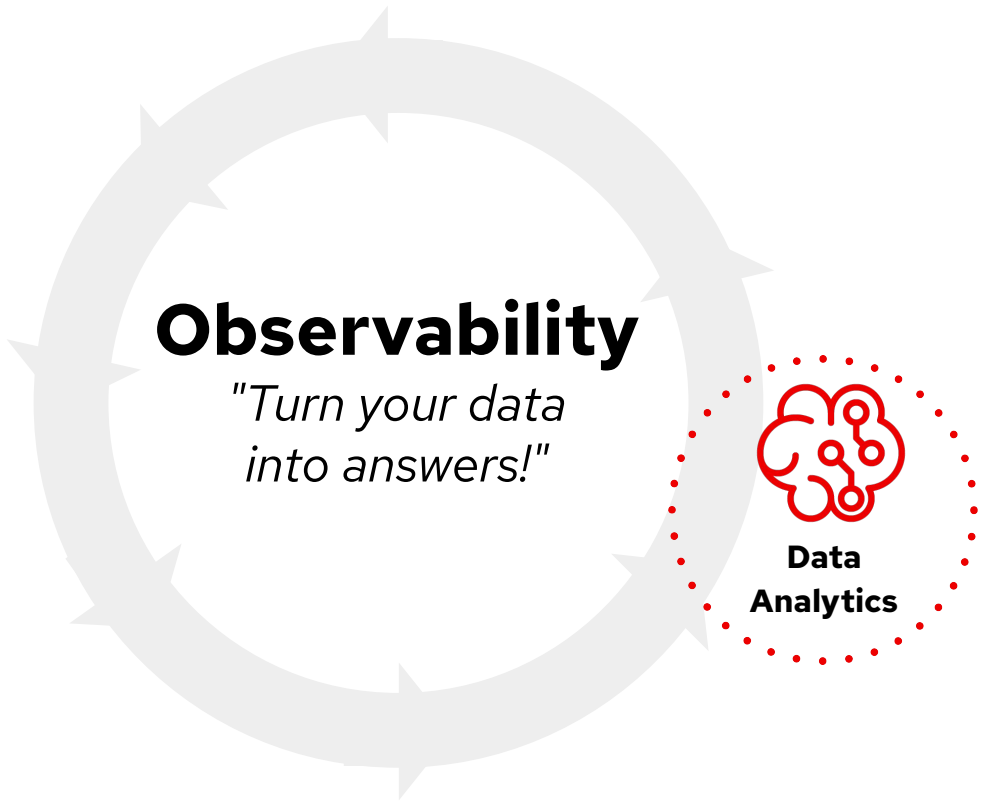
- Improved UX experience in OpenShift Web Console: *Metrics UI* > improved navigation when querying metrics

Logging 5.7

- Support for Logs-based Alerts (Loki) in the OpenShift Web Console > Admin Perspective > *Alerting UI*
- Improved UX experience in OpenShift Web Console: *Logs UI* > added Plugin Text Translation and enabled users to configure the front-end query limit

Distributed Tracing 2.8

- Tech Preview: Tempo trace visualization using Jaeger UI



OpenShift 4.13 Monitoring

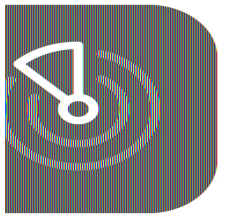
- Now possible to filter data by node attributes in Monitoring Dashboards

Logging 5.7

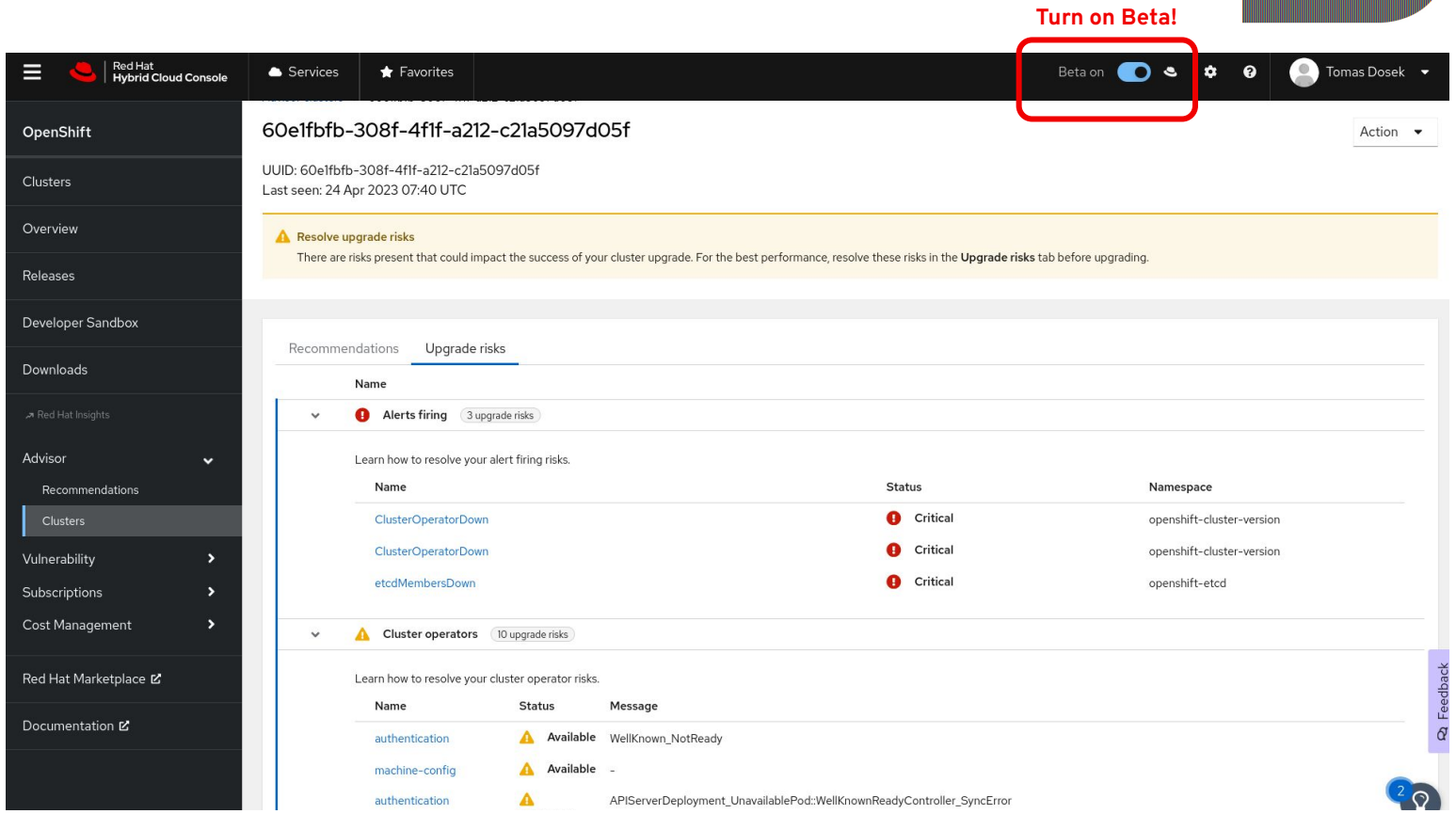
- Debug information on Loki error messages now added to support users in their troubleshooting process

Red Hat

Insights Advisor for OpenShift



- **Free service leveraging Red Hat experience with supporting and operating OpenShift**
- Insights Advisor UI adds **Upgrade risks (Preview)** - ML powered technology to identify potential blockers that could interrupt OCP upgrade flow
- **New Insights recommendations** focusing on preventing issues with OpenShift Data Foundation (ODF), OpenShift Cluster Version Operator (CVO) and OpenShift Cluster Autoscaler Operator (CAO)
- Insights recommendations available in Hybrid Cloud Console -> **Cluster History** page

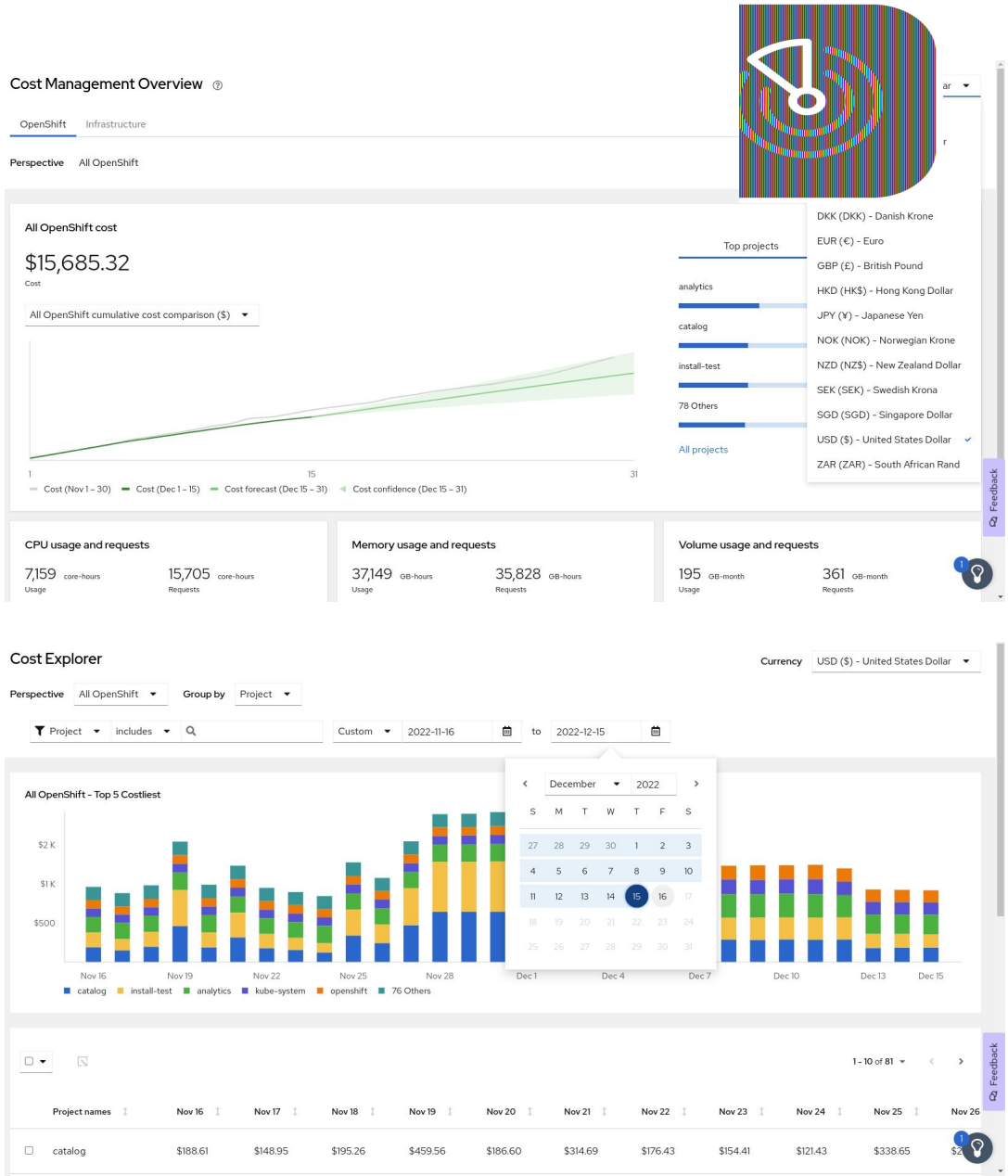


https://console.redhat.com/openshift/advisor
https://console.redhat.com/settings/notifications/openshift

Red Hat

Insights Cost Management

- **Free service to monitor per-resource (namespace, cluster, node, tag) usage and spending on-prem and major clouds**
- **Cost of running Openshift**, i. e. reporting and distributing cost of control plane and unallocated capacity
- Lots of enhancements for **more accurate cost reporting** and including additional AWS costs
- **Upload past data** and fill data gaps (improve continuity of reports)
- **Customer-side filtering** of billing data. Users no longer need to share all their cloud data.
- Initial support of **Oracle Cloud Infrastructure**



https://console.redhat.com/openshift/cost-management
https://console.redhat.com/settings/notifications/openshift
https://listman.redhat.com/mailman/listinfo/costmanagement

Red Hat

Networking & Routing

Red Hat

Red Hat OpenShift Networking Enhancements

Network Edge Enhancements

Support for AWS Application Load Balancer

The ability to manage the AWS ALB with Openshift is now GA

- Full ROSA support:
  - AWS STS support
  - Support the cluster-wide egress proxy
  - Support clusters without Cloud Credentials Operator
- New stable API

Hardware Enablement Updates

Hardware enablement

- GA Support for switching the BlueField-2 network device from data processing unit (DPU) mode to network interface controller (NIC) mode
- Hardware offload for the MT2892 Family [ConnectX-6 Dx] of network cards is GA
- Technology Preview of NIC partitioning for SR-IOV devices/Supporting OpenShift Container Platform installation on nodes with dual-port NICs

Red Hat OpenShift Networking Enhancements

Networking Enhancements

IPv6 Improvements

- IPv6 as the primary IP address family on bare metal dual-stack clusters
- Dual stack IPv4/IPv6 on vSphere platform

Expanding cluster Networks post installation

```
$ oc patch Network.config.openshift.io cluster
--type='merge' --patch \
  '{
    "spec":{
      "clusterNetwork": [
{"cidr":"<network>/<cidr>","hostPrefix":<prefix>} ],
      "networkType": "OVNKubernetes"
    }
  }'
```

Enhanced ovn-kubernetes health monitoring and observability

Network Observability Operator v1.2 GA

Networking Enhancements

Tech Preview: ovn-kubernetes CNI plug-in as secondary network

- For customers requiring feature-rich capabilities on a secondary pod network interface
- Control/Data-plane separation
- Define isolated tenant networks
- Ability to define a single flat (L2) network for virtual instances

Optional NodePort for LoadBalancer Services

- Useful for VIP-based LoadBalancer Service where the node port is not needed, e.g. MetalLB
- Not limited by the # of available node ports
- Unnecessarily exposed ports can fail regulatory/compliance requirements

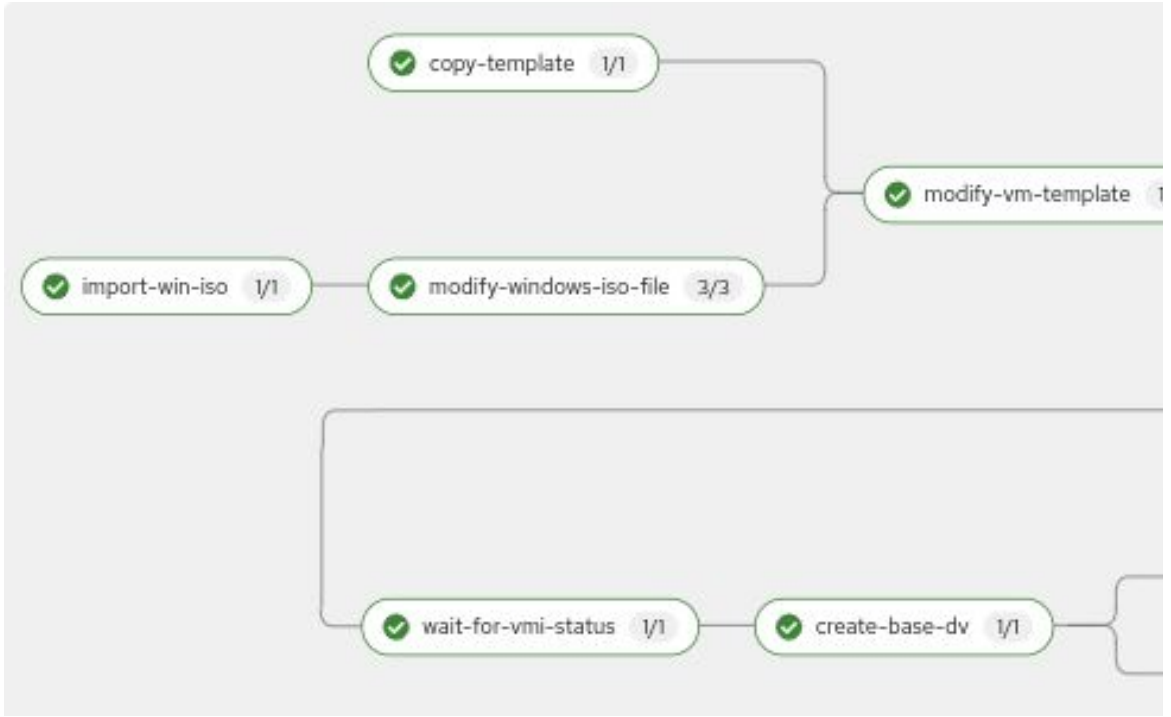
Virtualization

Red Hat

OpenShift Virtualization

Modernize workloads, bring VMs to Kubernetes

- Administrator workflow improvements
  - Cloud like instance types - Dev Preview
- Support high performance network workload with DPDK (Tech Preview)
- Observability
  - Identify under pressure nodes on CPU, memory or storage
  - Identify VM state and underutilized VMs
  - Optimize VM migrations
  - Snapshot storage consumption Migration
- Infrastructure High Availability
  - Compact Clusters running VMs can avail of Self Node Remediation
- Tekton Reference Pipeline for VMs (Tech Preview)



Red Hat

OpenShift sandboxed containers

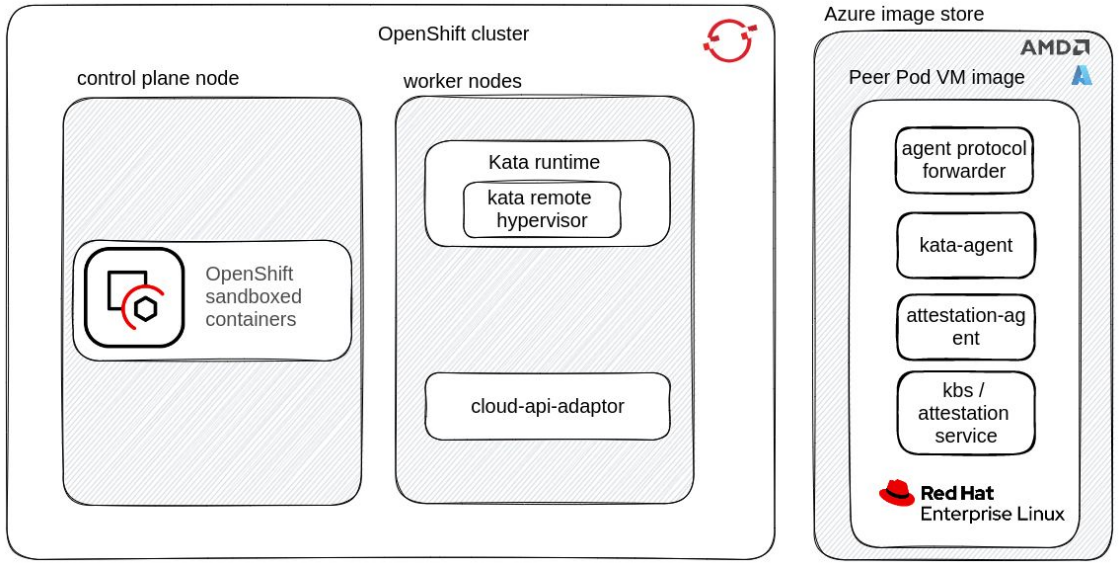
Kernel Isolation for containerized workloads

Cloud Support

- Peer Pods to Run AWS and Azure Natively (Tech Preview)
  - Install OpenShift sandboxed containers on public cloud without bare metal (AWS and Azure)
- Isolated CI/CD Pipelines key use case
  - Isolate CI/CD elevated privilege workloads with Openshift sandboxed containers

Confidential Containers

- Confidential containers on Azure dev-preview
- Based on the CNCF upstream project
- Big data analytics with Apache Spark key use case
- Joint demo with Microsoft Azure available on YouTube



Red Hat

Operator Framework

Red Hat

See version history of operators

Users can now introspect all available versions in all release channels of a particular operator

```
$ oc describe packagemanifest quay-operator

Name:         quay-operator
...
Channels:
  Name: stable-3.7
  Entries:
    Name:       quay-operator.v3.7.11
    Version:    3.7.11
    Name:       quay-operator.v3.7.10
    Version:    3.7.10
    Name:       quay-operator.v3.7.9
    Version:    3.7.9
  ...
  Name: stable-3.8
  Entries:
    Name:       quay-operator.v3.8.5
    Version:    3.8.5
  ...
```

- ✔ Install an older release to replicate a staging env
- ✔ Verify content of a mirrored offline catalog
- ✔ Find the channel of a desired release
- \+ Older versions no longer disappear from catalogs
- ↗ Console UI support aimed at 4.14

Red Hat

Storage

Red Hat

OpenShift Storage - Journey to CSI

- CSI Migration
  - Azure File GA
  - vSphere GA
    - Enabled by default on new clusters
    - Disabled on upgraded clusters
      - Option to opt-in
- vSphere CSI
  - RWO PVs encryption
  - Zones configuration via the installer & day 2
- AWS EFS CSI
  - Cross account mount support
- LVM Storage CSI
  - Multiple Storage Classes (e.g. for NVMe and HDD)
  - Disconnected installations
  - IPv6 dual stack support
  - Reduce resource usage of LVMs

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

Red Hat

OpenShift Storage – Storage class management

- Define how OCP storage operators manage their storage classes
- Set storageClassState in the ClusterCSIDriver object
  - **Managed(Default):** Operator actively manages and reconciles the storage class
  - **Unmanaged:** The operator does not actively reconcile the storage class.
  - **Removed:** The operator deletes the storage class.
- Supported all operators deployed by the CSO
  - Alicloud Disk, AWS EBS, Azure Disk & File, GCP PD, IBM VPC Block, OSP Cinder, RHV, vSphere.

```
$ oc edit clustercsidriver csi.driver.company.com

apiVersion: operator.openshift.io/v1
kind: ClusterCSIDriver
metadata:
    name: csi.driver.company.com
(...)
spec:
(...)
  storageClassState: <State>   # Add here
```

Red Hat

OpenShift Storage – CSI In-line volumes GA

- CSI Ephemeral In-line volumes are fully supported
  - Allow PVCs to be defined in the pod specs
  - Volumes have the same lifecycle as the pod
- The CSI driver needs to support in-line volumes.
- Comes with a security admission plugin
  - Define which namespaces can consume in-line volumes
    - privileged (default if not set)
    - baseline
    - restricted

```
kind: CSIDriver
metadata:
  name: csi.driver.company.org
  labels:
    security.openshift.io/csi-ephemeral-volume-profile:
baseline
```

```
kind: Pod
metadata:
  name: csi-pod-inline
spec:
  containers:
(...)
      volumeMounts:
      - name: volume-inline
        mountPath: "/mnt/volume-inline"
(...)
  volumes:
    - name: volume-inline
      csi:
        driver: csi.driver.company.org
        volumeAttributes:
(...)
```

Red Hat

OpenShift Storage – Non Graceful node shutdown

(Technology Preview)

- **Release CSI volume attachments** when the node's shutdown is not detected by Kubernetes.
- **Volumes can be reattached** on other nodes
- Taint the node with
  - out-of-service=nodeshutdown:NoExecute
- Remove the taint once the node is back online

```
# Ensure the node is down

# Taint the node
$ oc adm taint node <node-name> \
node.kubernetes.io/out-of-service=nodeshutdown:NoExecute


# Start the node and ensure it is online


# Untain the node
$ oc adm taint node <node-name> \
node.kubernetes.io/out-of-service=nodeshutdown:NoExecute-
```

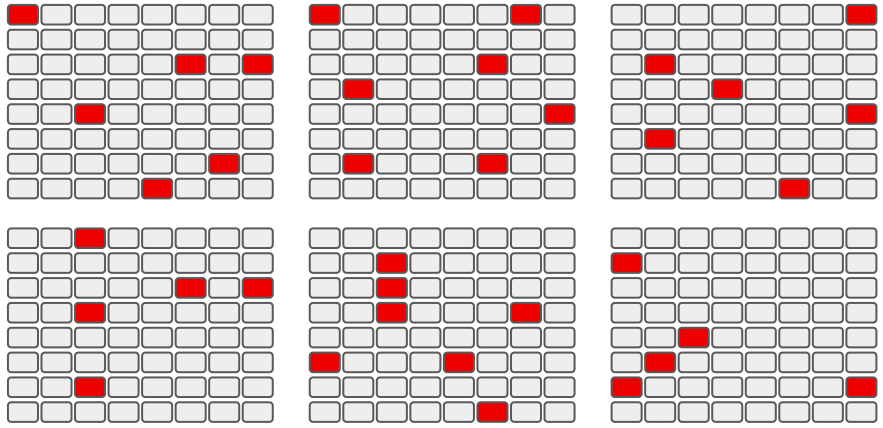
Red Hat

Telco 5G

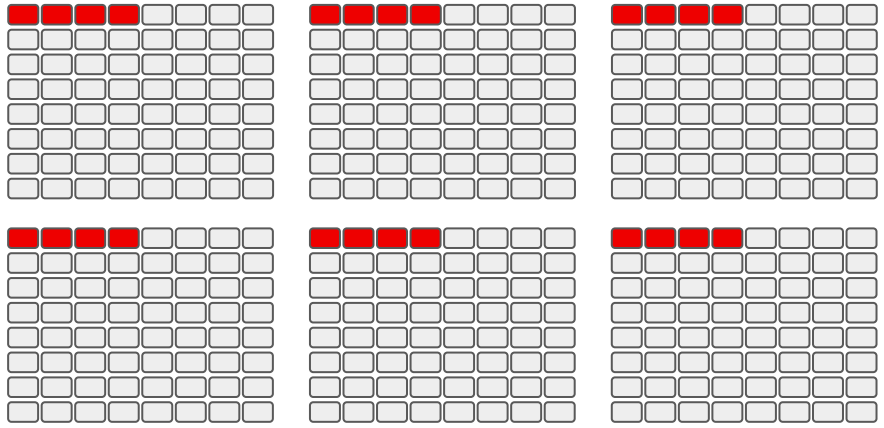
Red Hat

Multi Node Cluster CaaS CPU Isolation

Multi-Node Cluster with no Optimizations



Multi-Node Cluster with Reserved and Isolated CPUs with Workload Partitioning



- Previously only available on Single Node OpenShift clusters
- Now available on all deployment types, specifically multi-node clusters
- Caveats Apply
  - Must be configured at installation time
  - No backing out, the cluster is configured this way for its life
  - Nodes added to the cluster at a later date must be configured similarly
  - Platform CPU requirements are governed by use case , the size of the cluster and the CNF's dimensions

CPU with CaaS processes running on it

CPU with no CaaS processes running on it

Red Hat

Telco Operational Enhancements

Feature	Benefit
crun is GA	More efficient runtime reduces CaaS compute needs
LVM Storage resource optimization	Reduce CaaS compute needs when using local logical volumes
Replace AMQP event bus with HTTP implementation	One less dependency and fewer processes running on Single Node OpenShift cluster
Utilize Composable OpenShift	Filter out unnecessary components when installing on a Single Node OpenShift cluster
TALM Upgrade preCaching Optimization	Reduce the amount of data downloaded when using TALM preCaching by filtering out unnecessary content

Red Hat

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

Red Hat