Red Hat OpenShift

What's New in OpenShift 4.14

OpenShift Product Management

Red Hat

What's new in Red Hat

OPENSHIFT 4.14

Red Hat OpenShift

ENHANCED SECURITY

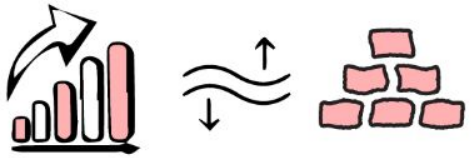
- SCC Preemption prevention
- ConfigMaps and Secrets sharing across namespaces (GA)
- Azure managed identity
- Secret Store CSI Driver Operator (Technology Preview)

OPTIMIZE TCO VIA HOSTED CONTROL PLANES (HCP)

- Self-managed HCP on baremetal (GA)
- Self-managed HCP on OpenShift Virtualization (GA)
- Heterogeneous clusters with HCP
- x86 control plane with Power data plane for HCP on bare metal (Technology Preview)

CORE AND FLEXIBILITY

- 24 months OpenShift lifecycle for ARM, Z, and Power
- CgroupV2 default
- OVN optimization
- VMware vSphere CSI migration
- External platform type for partner integration



red.ht/whatsnew

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

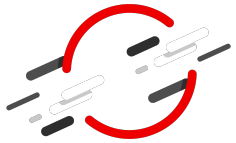
Significant list of other graduations to stable:

- 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



Release Announcement: https://kubernetes.io/blog/2023/04/11/kubernetes-v1-27-release/

Red Hat

Notable Top RFEs and Components

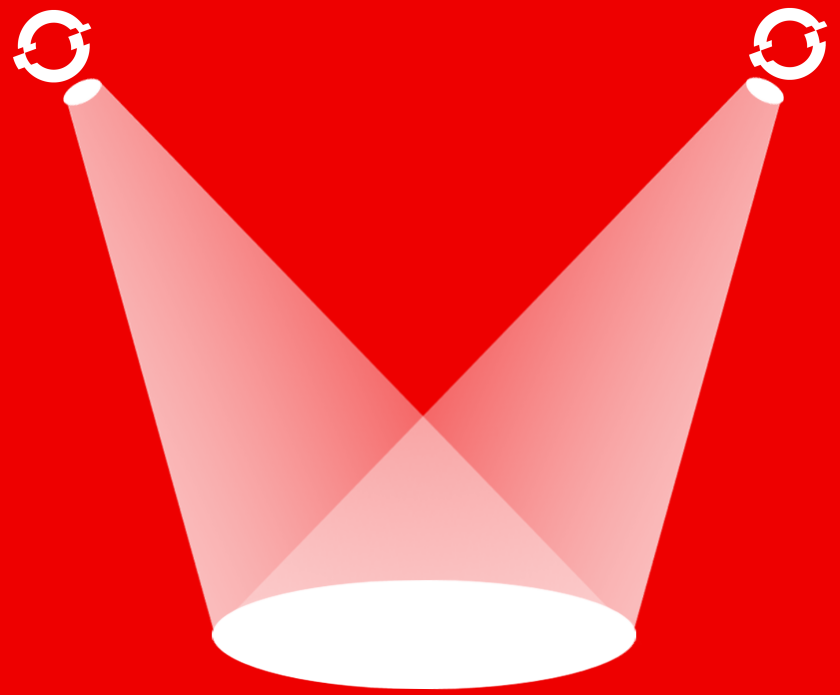
Top Requests for Enhancement (RFEs)

- Add additional HTTP header to HAProxy without customizing haproxy.conf
  - This allows for additional protection to be added to HTTP requests and prevent certain attack vectors from being exposed.
- Azure Managed/Workload Identity
  - Create and manage OpenShift clusters with temporary, limited privilege credentials on self-managed clusters
- GCP tags (Technology Preview)
  - Labels and tags can be used for categorizing, organizing and managing resources created for a particular cluster

26 RFEs

shipped in **OpenShift 4.14** for customers

OpenShift 4.14 Spotlight Features



Red Hat

Azure Managed/Workload Identity (MI/WI)

What	Azure managed/workload identities for customer-managed OpenShift clusters ▸ Create and manage OpenShift clusters with temporary, limited privileges
Who	Cluster administrators who deploy OpenShift clusters on Azure. Developers who run operators on Azure using access controls with temporary, limited privilege credentials. ▸ Operator Lifecycle Manager (OLM) managed operators to leverage MI/WI coming in next release (manual configuration for now)
Why	Minimize permissions needed to operate a cluster in Azure ▸ Identity and access management best practice ▸ Remove use of Azure service principal to install cluster
Availability	Supported in all Azure regions where Azure managed identity and Azure Active Directory workload identity is available
Limitations	Applies to new clusters from OpenShift 4.14+ only. ▸ You cannot migrate (or upgrade) an existing OpenShift cluster to use Azure MI/WI

External Platform for Onboarding Third Party Integrations

What	▸ "External" platform allows for partner integrations.
	▸ Builds on top of Installing a cluster on any platform with additional capabilities.
	`platform:`
	`  external:`
	`  platformName: "providerName"`

Who	▸ Provides partners a self-service approach to onboard their platform/provider to OpenShift and to add their own infrastructure components.
Why	▸ Previous approaches required modifications to OpenShift source code and took multiple releases to onboard. ▸ Partners now have full control of their own infrastructure management components for release and lifecycle management.
Availability	▸ Applies to OpenShift 4.14+ clusters.
Notes	▸ Customers and partners can continue to use Installing a cluster on any platform for not yet tested RHEL certified virtualization, bare-metal host or cloud provider environments.

SCC Preemption Prevention and PSA Improvements

SCC Preemption: SCCs are part of the OpenShift API and are subject to modifications by customers. This would lead to preemption issues that resulted in:

- Modifications of out-of-the-box SCCs causing core workloads to malfunction
- Addition of new higher priority SCCs that overrule existing pinned out-of-the-box SCCs during SCC admission and cause core workloads to malfunction
- Often encountered with Layered Products as well such as ACS, Storage Operators from OpenShift partner teams

You can now pin your workload to specific SCC to prevent against SCC preemption issues

PSA Improvements:

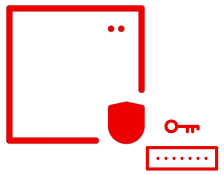
- Default and Kube System namespace have privileged enabled for Cloud provider ease of integration
- User should be able to modify pod-security.kubernetes.io-labels

```
apiVersion: config.openshift.io/v1
kind: Deployment
apiVersion: apps/v1
spec:
# ...
  template:
    metadata:
      annotations:
        openshift.io/required-scc: "my-scc"
# ...
```

New

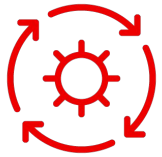
Secrets Store CSI Driver Operator (TechPreview)

Mount secrets from external secret storage solutions



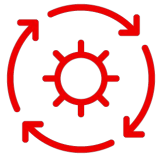
Mount Secrets directly for Application usage

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.

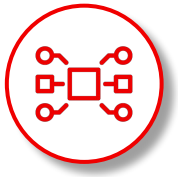
Available in OperatorHub

Systems Enablement

OpenShift on Arm

- Round out cloud platform support to all running OpenShift on highly efficient, high performance per watt architectures

  o----------o
- Support for Arm on GCP
- oc mirror parity with x86



Multi-architecture Cluster

- More cluster flexibility by allowing nodes of different architecture, now with more cloud platforms and a guided install experience

  o----------o
- Multi-architecture compute platforms:
  - GCP with Arm
  - Bare Metal Arm
  - Add IBM Power or IBM Z to x86 clusters
- Hosted Control Planes - Arm control plane, x86 compute, AWS (Tech preview)
- Assisted Installer support
- Autoscale from zero

IBM Power and IBM Z

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

  o----------o
- Single Node OpenShift support
- Hosted Control Planes - x86 control plane, Power or Z compute (Tech Preview)
- oc mirror parity with x86
- Install secured cluster services with Red Hat Advanced Cluster Security (RHACS) operator

Red Hat

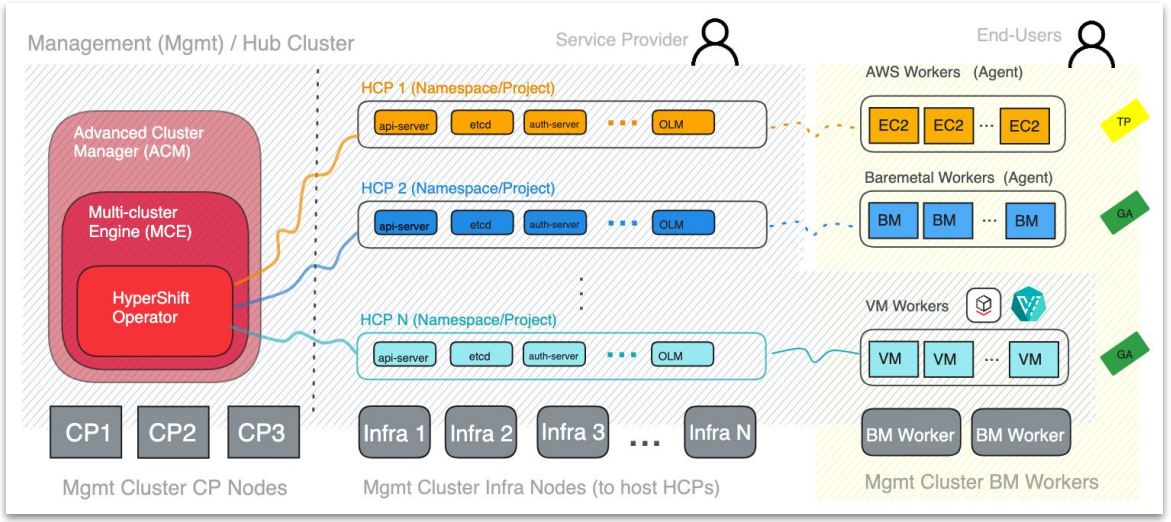
Longer lifecycle for Multi Architectures for EUS Releases

What	Match existing x86 lifecycle with additional 6 month of Extended Update Support (EUS) phase on **even numbered** OpenShift (OKE, OCP, OPP) releases and a subset of layered operators for multiple architectures ▸ ARM, IBM Power, and IBM Z
Who	Those with **Premium subscriptions**, [or Standard subscriptions + an **add-on SKU**]
When	Starting with **OpenShift 4.14** and applying to subsequent even numbered releases of OpenShift.
Why	▸ Support customers and partners struggling to maintain pace with 4.y cadence ▸ Align approach and offering rules of OCP EUS to RHEL's program rules
Note	▸ EUS to EUS upgrades continue the same behaviour. ▸ Layered operators/operands and products will continue to have their own lifecycle. ▸ Layered operator lifecycles are available on the OpenShift lifecycle page.

Hosted Control Planes for Red Hat OpenShift

What's new (w/ MCE 2.4)

- Baremetal with the Agent Provider (GA)
- OpenShift Virtualization Provider (GA)
- AWS provider [Continuation] (Tech Preview)
- Arm CP and x86 NodePools on AWS (Tech Preview)
- IBM Power/Z NodePools (Tech Preview)



Why it matters

Optimize your economics, Increase your Margins, and Meet your Eco-Friendly Goals (💰 ☘️)

- ~30% infra savings, ~65% for SREs/Operations savings.
- ~60% time-saving for devs (⬆️ Productivity), ~50% reductions in power & facility costs.

Streamline Role Management & Segmentation (🔐)

- Persona Decoupling no more clashing concerns between admins and users.
- Fewer mis-configuration errors 💥.

Reduce Multi-cluster Overhead (🔋)

- Solve for Multi-cluster, build on a efficient grounds.
- Build your Cluster-as-a-Service on top for speed and efficiency (check the cluster-template-operator)

Tailor the setup to your needs with high Flexibility (🔪)

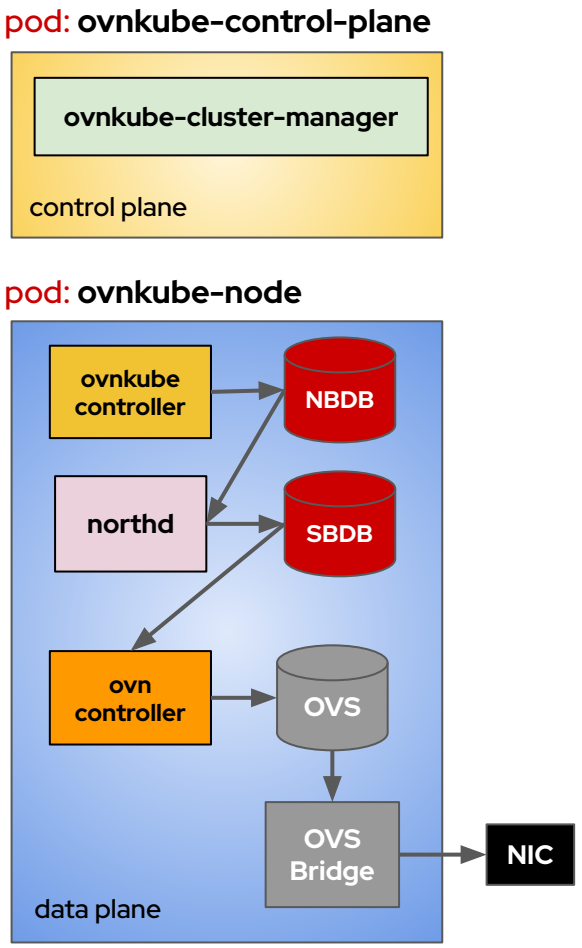
- Bare Metal (Agent), VM workers (OpenShift Virtualization), or even on the cloud (AWS)
- Mixed Architecture between CP/DP (Arm, Power/Z)

Red Hat

Open Virtual Network (OVN) Enhancements

Included in any upgrade to OpenShift 4.14+

- **Every cluster node hosts its own network flow data** versus querying control nodes for it
- **Improved scale**
  - Network flow data is localized on every node which reduces operational latency
  - Adding nodes to a cluster has a much smaller impact on cluster-wide traffic
  - Now scales linearly with node count: O(1) versus O(#workers / 3-control-nodes)
- **Improved stability**
  - No RAFT control node leader election, a major source of cluster instability
- **Isolated networking loss in case of issue**
  - Any cluster node lost affects just that node instead of the whole cluster network
  - Properly deployed apps (across nodes) are unaffected by any single node loss
- **Improved Security**
  - Cluster nodes don't need to know the networking of other cluster nodes, or communicate their own

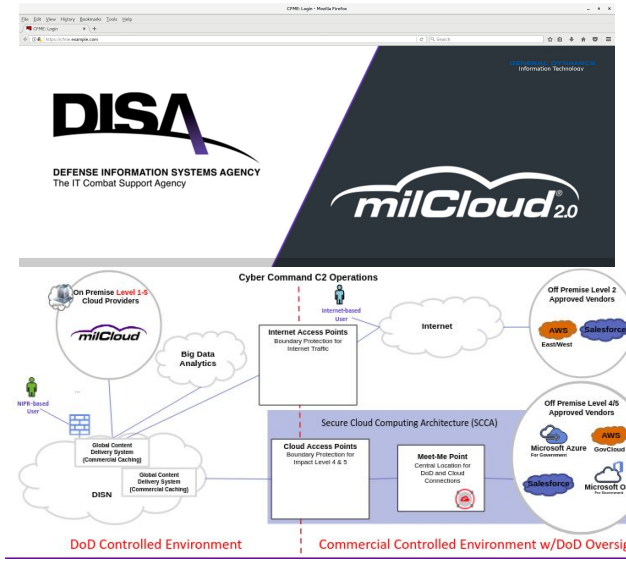


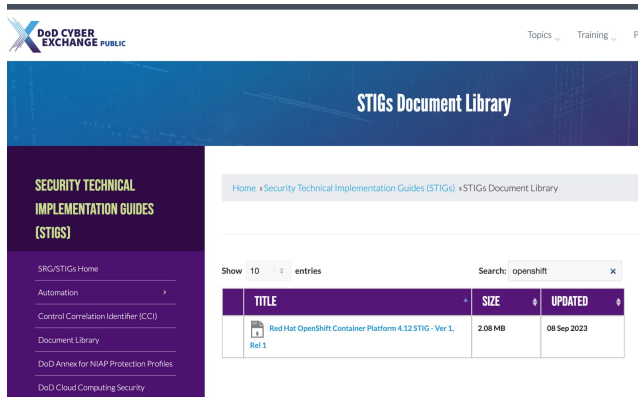
DISA STIG for OpenShift and Compliance Operator Profile

DISA is the US DoD's common IT service provider

Red Hat now ships fully automated tooling to implement the DISA STIG for OpenShift via the Compliance Operator

US DISA STIG is the MANDATED security baseline for the Department of Defense, and is widely used by civilian and commercial agencies





[DISA releases the Red Hat OpenShift Container Platform 4.12 Security Technical Implementation Guide – DoD Cyber Exchange]

https://docs.openshift.com/container-platform/4.13/security/compliance_operator/co-scans/compliance-operator-supported-profiles.html

Red Hat

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

Full List of all Red Hat operators and their tiers can be found at the end of this slide deck

Console

Dynamic Plugins Updates for the OCP Console

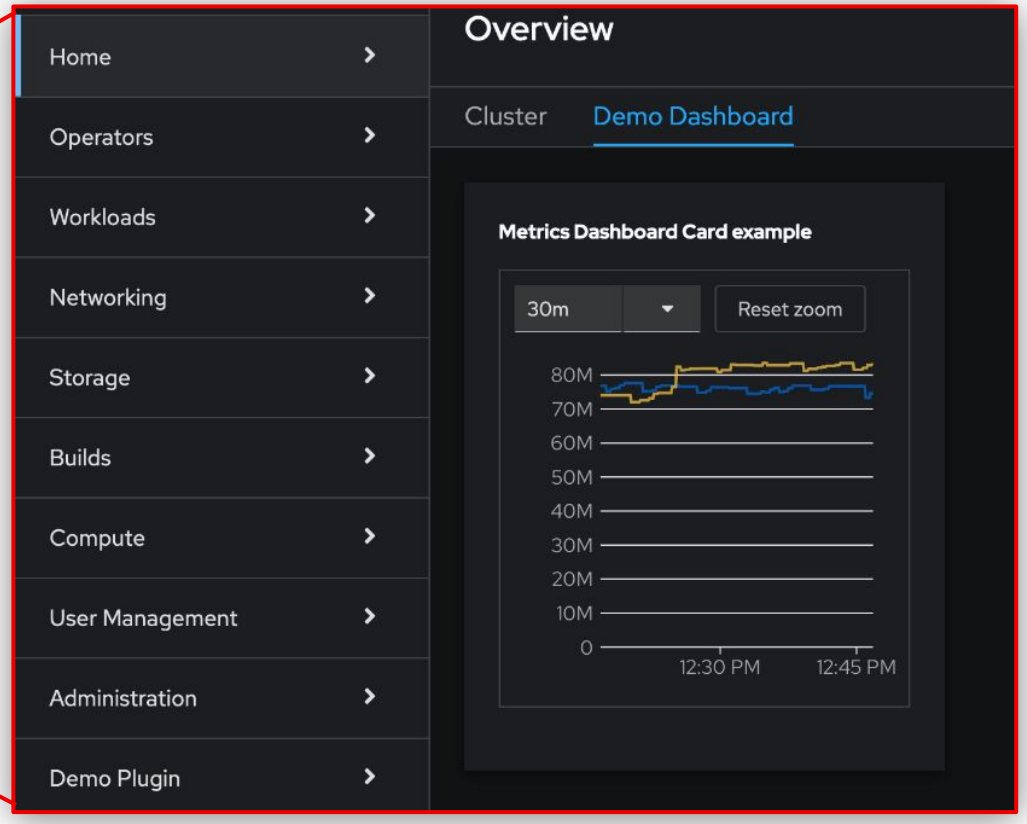
New Extension Points with Updated Examples

Examples

- Dynamic Demo Plugin
- CronTab Plugin
- Plugin Template

API

- QueryBrowser
- useAnnotationsModal
- useDeleteModal
- useLabelsModal
- useActiveNamespace
- ErrorBoundaryFallbackPage



Red Hat

Console RFEs

Direct Customer Requests → Customer Happiness

- RFE-2649 : Implement strict search in the OpenShift Console
- RFE-3979 : Add ability to show/hide tooltips in the yaml editor
- RFE-3775 : Make dynamic plugins proxy timeout customizable
- RFE-2678 : Disable static content available from OpenShift Console without authentication
- RFE-3260 : Notification banner over web-console for upgrade path blockage

Developer Tools Update

Developer Tools Update

Just the highlights today!

Check out:

- The **Developer Perspective** in **OpenShift Console** includes new Quick Starts to discover developer tools, improved OpenShift Pipelines user experience with autodetection of PAC in git import flow, inclusion of Serverless Functions in the samples catalog, and more!.
- **Podman Desktop** adds new capabilities to help developers run Docker Desktop extensions, install on Arm64 Windows systems.
- **OpenShift IDE** extension now has OpenShift Serverless & Helm Charts integrated in VSCode
- **IntelliJ Quarkus** plugin with improved performance and Qute template support
- **VSCode Java** crossing 28.4M downloads. Java 21 support coming soon.
- **Odo 3.15 is now available** with a new graphical UI
- **Developer Hub v0.2** wraps its Helm chart as an operator for OpenShift 4.14, bundles plugins such as ArgoCD, AzureDevOps, Datadog, Gitlab, OCM, Tekton, Topology view, Quay.

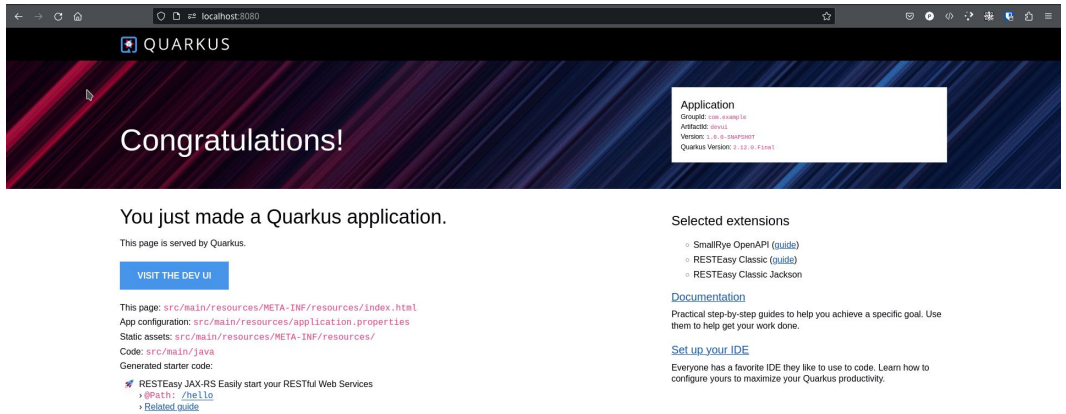
Watch out for a separate DEVELOPER EDITION presentation coming the next weeks!!
developers.redhat.com

Runtimes

Kube Native Java with Quarkus

Key Features & Updates (Quarkus 3.2)

- **New UI** improves navigation, metrics tracking, endpoint management
- **Upgrade to major dependencies**
  - Hibernate 6 (Highlighting, Mapping improvements)
  - Quarkus Cache extension supports Redis backend
- Improved **Native Builds**
  - Performance, debug, JFR events
- **Observability**
  - OpenTelemetry autoconfiguration, OTLP exporter included
- **Security**
  - OIDC: Front-channel logout, custom token verification
  - Dynamic @RolesAllowed naming
- **MicroProfile 6**: Observability, OpenAPI, JWT improvements
- **Tooling**
  - New **Dev Service**: Kubernetes
  - CLI extensible with plugins
  - `quarkus deploy` simplifies OpenShift integration, `quarkus image` simplifies container build/push.
  - `quarkus update` handles most tedious upgrade work
- Simplified **Azure Functions** development

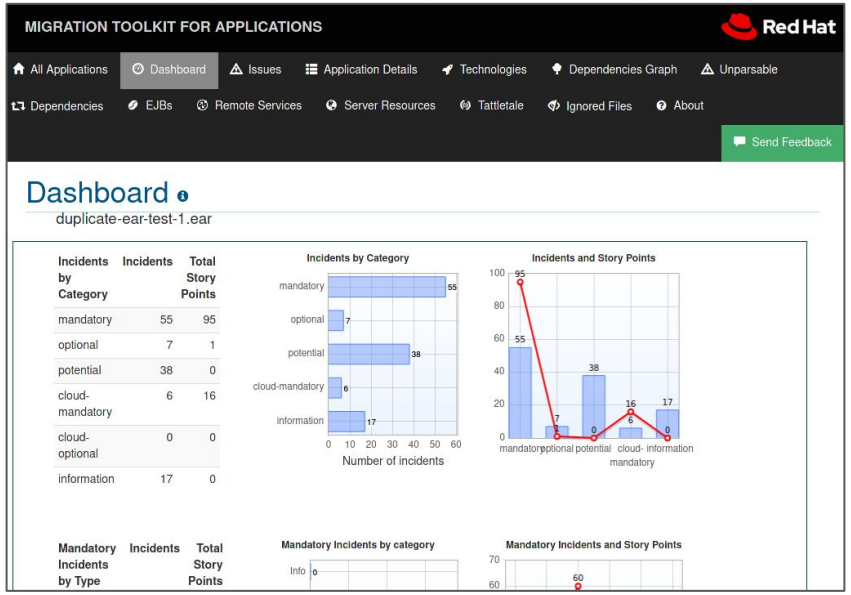


Revamped Dev UI

Red Hat

Application Modernization

- **Migration Toolkit for Applications (version 6.2)**
  - **Integration with Jira**: Applications in the inventory can now be exported as issues in Jira and report their status back to MTA.
  - **Migration Waves**: Enables Project Managers and Architects to break the portfolio into different waves and execute the adoption effort in an iterative fashion
  - **OpenShift Monitoring integration**: allows users to consume metrics from their MTA installation.
- **Migration Toolkit for Runtimes (version 1.2)**
  - Java 17 support
  - Decompilation and analysis of applications based on Java 17
  - Eclipse Plugin Java 17 compatibility
  - Operator upgrade, now based on Quarkus and the Quarkus Operator SDK.
  - New rulesets and targets: OpenJDK 21, JBoss Web Server 6 (Tomcat 10), Camel 4, Red Hat JBoss EAP 8 (expected to GA in Q4), Java/Jakarta EE to Quarkus migrations.



Example analysis report

Red Hat

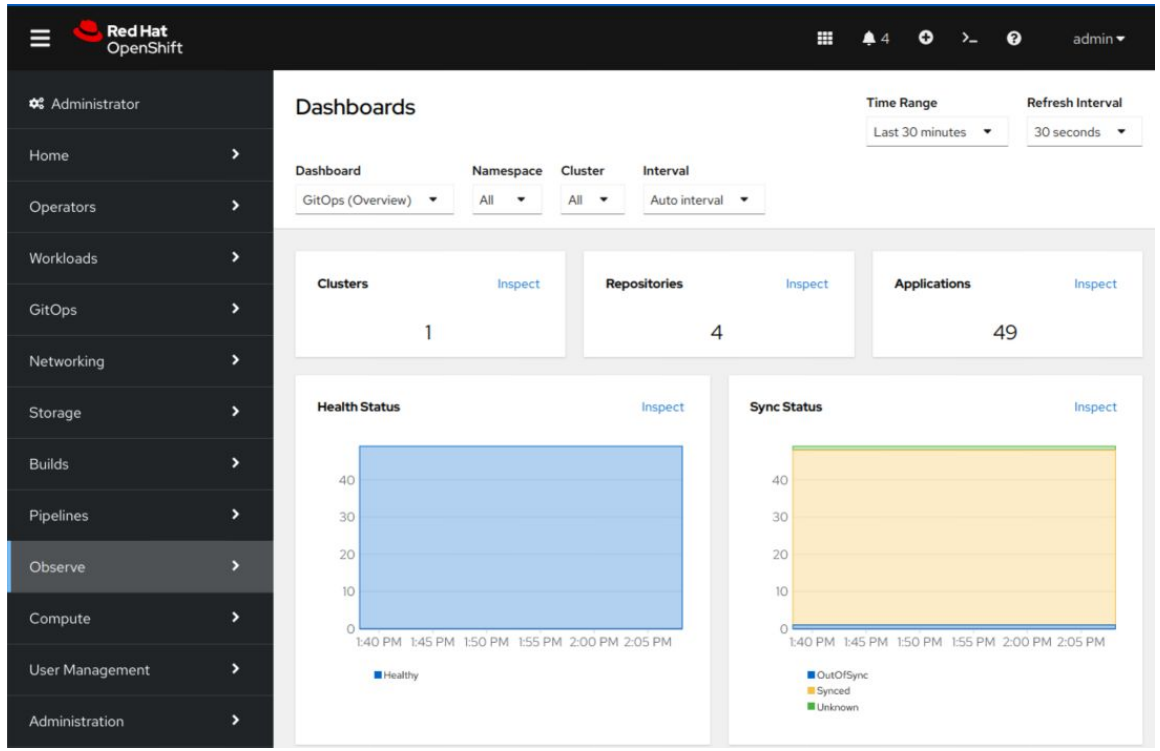
Platform Services

OpenShift Pipelines

- **OpenShift Pipelines 1.12 (Tekton Pipelines 0.50)**
- **Tekton Chains** is now Generally Available for use.
- **Tekton Results** for extended pipeline history retention (Tech Preview)
  - Support for external PostgreSQL server
  - Support for Google Storage Bucket, S3, etc as external log storage
  - Accessed via CLI or API (Console integration coming soon...)
- **Pipelines as code**
  - Custom Parameter support
  - Ability to limit GitHub token scope to repository or set as global
  - Improved integration of GitHub roles and policies for comment actions e.g. pull request/ok-to-test
- **Operator**:
  - Configure default and maximum SCC for namespaces for tasks and pipelineruns
  - Ability to enable experimental (non-supported) Tekton configs through the “options” field

OpenShift GitOps

- OpenShift GitOps 1.10
- Includes Argo CD 2.8
- Three monitoring dashboards in the OpenShift Admin console
- New standalone GitOps docs site (versioned)
- Dynamic scaling for the Application controller
- Option to ignore tracked resource updates

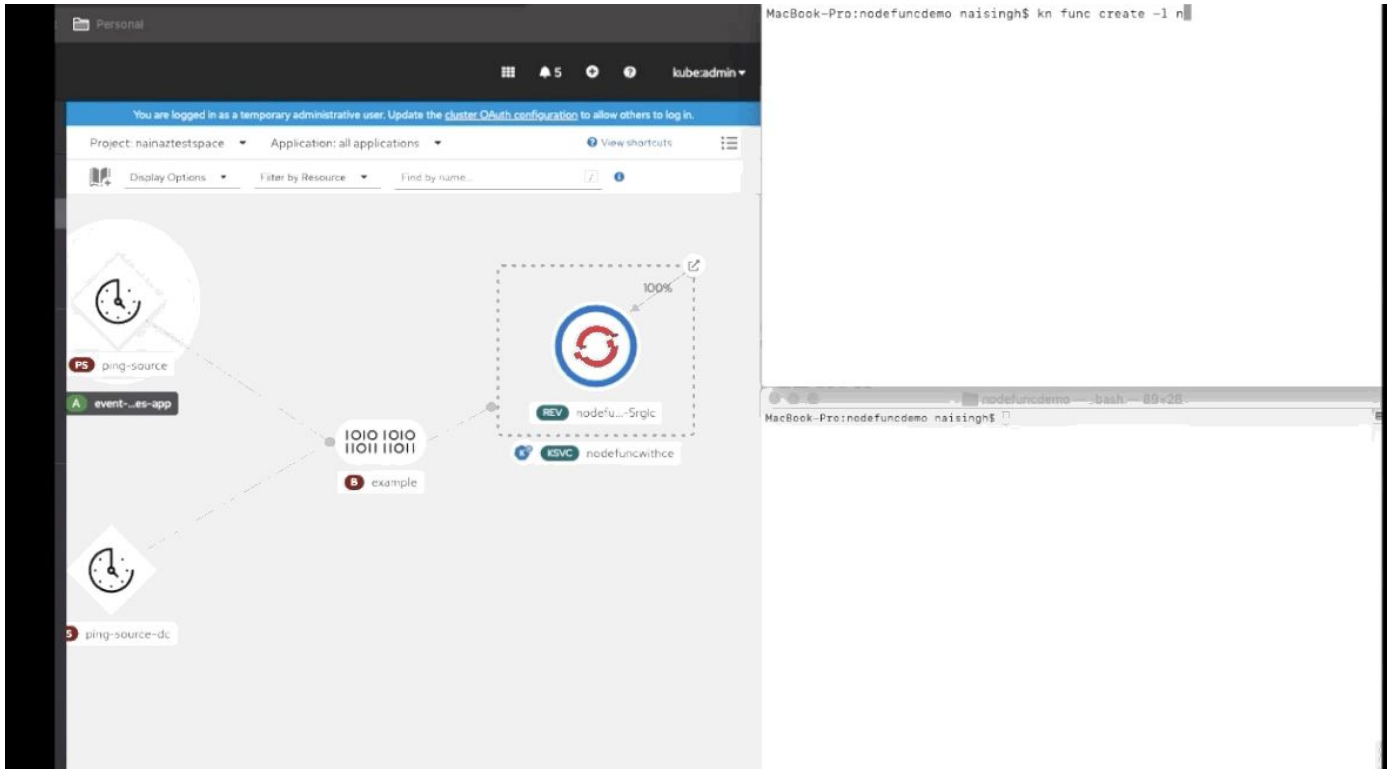


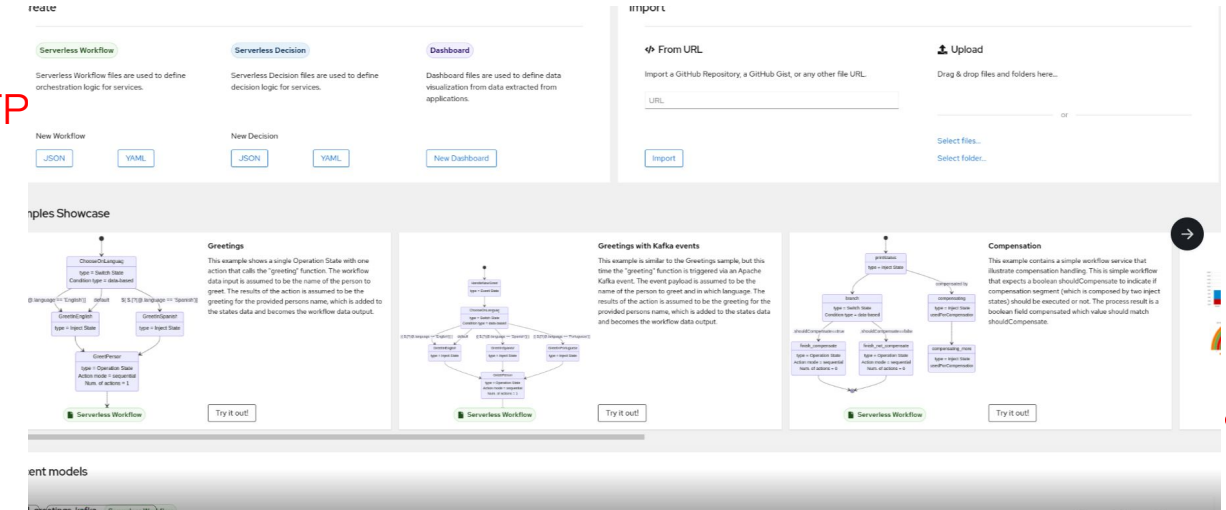
Red Hat

OpenShift Serverless

Key Features & Updates

- Serverless 1.30 : Update to Knative 1.9
- Serverless functions on IBM zSystems and Power
  - s2i builder
- Pipeline as a Code for Serverless Functions -TP
- Hosted Control Planes support
- More configuration options for net-Kourier
- Multi-Container support - GA
- Event Mesh integration with Service Mesh - TP
- Serverless Logic TP
  - Orchestration for Functions and Services
  - CLI and Workflow Editor(UX)

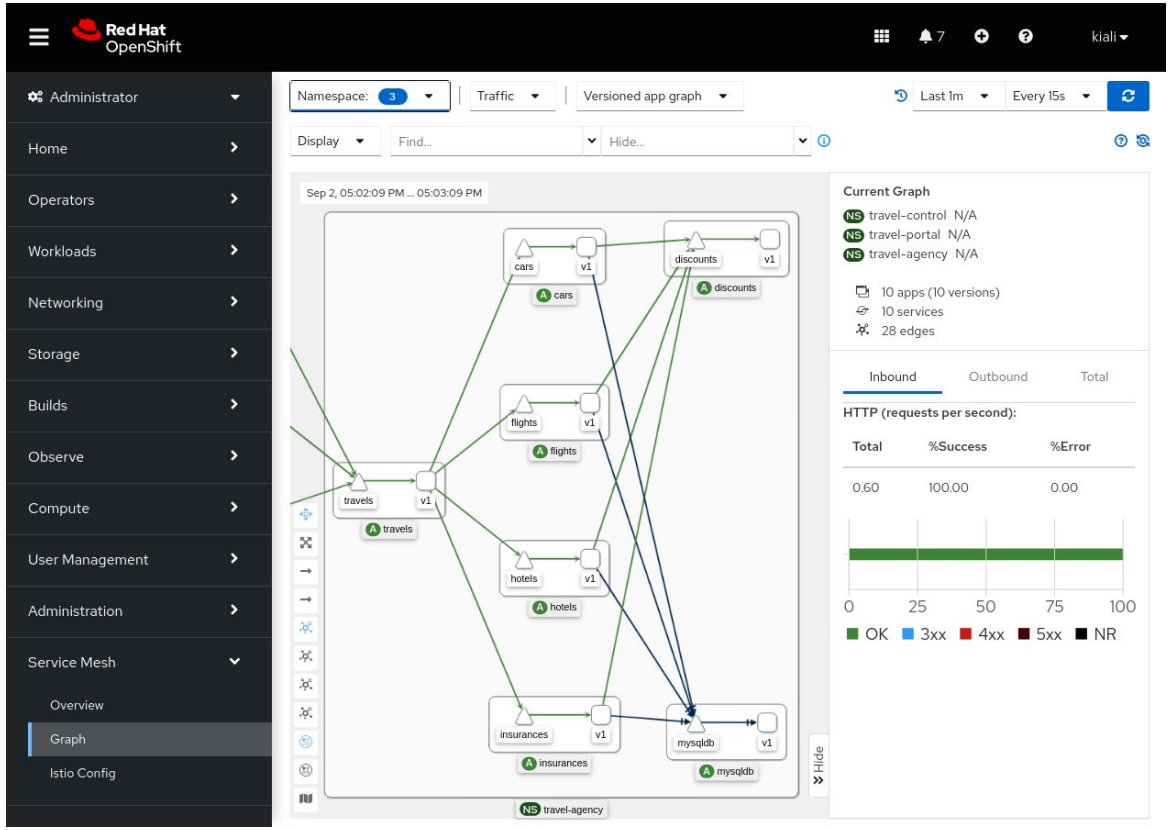




Red Hat

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 1.73**
  - Support for Service Mesh on ARM64
  - Developer preview of IPv4/IPv6 Dual-Stack
- "Sail Operator" - Developer Preview of OpenShift **Service Mesh 3** is now available:
  - Based directly on upstream Istio
  - See blog "A new operator for Istio on OpenShift"



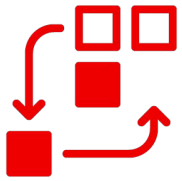
Red Hat

Installer Flexibility

OpenShift 4.14 Supported Providers

Installation Experiences

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



Automated

Installer Provisioned Infrastructure

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

Full Control

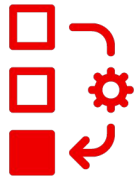
User Provisioned Infrastructure

- 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

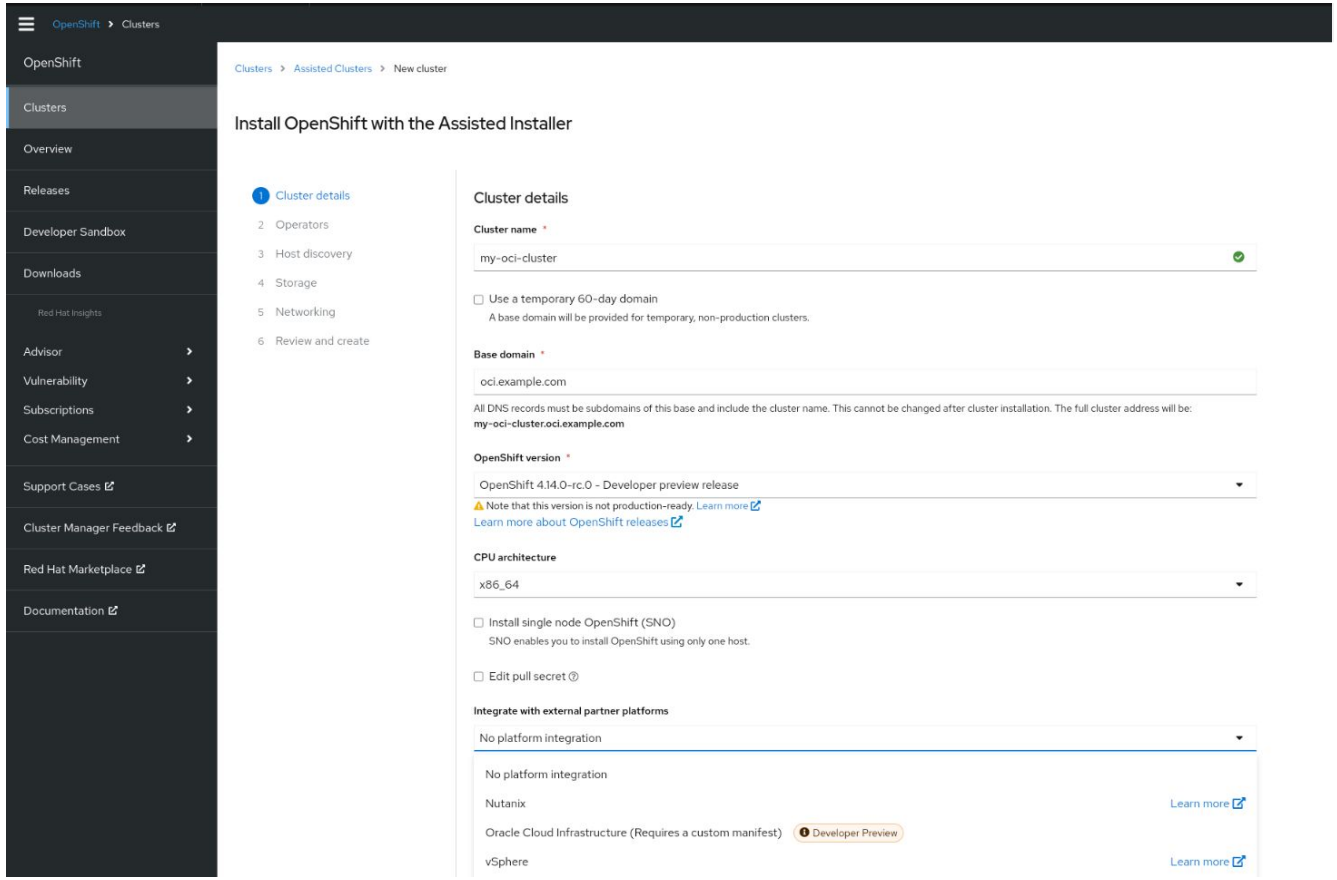
OpenShift on cloud providers

- Deploy OpenShift into a shared VPC in AWS using the existing Route53 DNS Zone
- Custom security groups in AWS for the user to attach control plane and compute nodes instances to enforce user specific network rules

- User defined tags in GCP (TP) to provide additional custom labels at install time
- Azure and Azure Stack Hub network restricted deployments
- User defined tags in Azure (GA) to provide additional custom labels at install time
- Support custom RHCOS image sources for GCP and Azure
- Support Nat Gateway in Azure to be used for the outbound traffic for OpenShift (TP)

ORACLE Cloud (Dev Preview)

OpenShift on Oracle Cloud Infrastructure (Dev Preview)



[How to deploy Red Hat OpenShift on Oracle Cloud Infrastructure Demo]

- Assisted Installer for connected deployments
- Agent-based Installer for restricted network deployments
- Leverages external platform type
- Includes partner provided components, e.g. Oracle Cloud Controller Manager (CCM) and Oracle Container Storage Interface (CSI)
- Must use RHEL certified OCI shapes with x86 and Arm64 architecture
- Bring Your Own Subscription (BYOS) OpenShift
- Available for preview by request

Red Hat

VMware vSphere Notable Changes in OpenShift 4.14

Feature	OpenShift 4.14	Guidance
Static IP addresses for vSphere nodes	Technology Preview	Provision and scale vSphere machines with static IPs How to perform an IPI installation of OpenShift on vSphere with static IP addresses blog
Quicker machine deployments	GA	vSphere Template support for RHCOS for faster installation
OpenShift on Oracle Cloud VMware Solution (OCVS)	GA	Available for OpenShift 4.12, 4.13 and 4.14 as a VMware Cloud Verified provider
Migration to vSphere CSI	GA	Enabled by default in OpenShift 4.14, more details in the Storage section.

Additional details and guidance at OpenShift 4.14 Release Notes.

Agent-Based Installer

Install On Any Platform (platform: none)

Install OpenShift on any infrastructure, including virtualization and cloud environments

Disk Encryption And Partitioning

To comply with security policies (e.g. PCI DSS)

PXE Boot Support

Create PXE artifacts to boot from the network

Oracle Cloud Infrastructure (Dev Preview)

Install OpenShift on Oracle Cloud Infrastructure with Agent Installer for restricted networks

```
apiVersion: v1
baseDomain: example.com
compute:
- name: worker
  replicas: 3
controlPlane:
  name: master
  replicas: 3
metadata:
  name: platform-agnostic-cluster
platform:
  none: {}

diskEncryption:
    enableOn: all
    mode: tpmv2
```

```
# openshift-install agent create pxe-files
```

OpenShift on Nutanix

Minimum Required Permissions Published

Use a restrictive set of permissions for Prism Central to comply with security policies

Egress IP Support

Configure OpenShift SDN to assign one or more egress IP addresses to a project

Control Plane Machine Sets Support

Automate the management of the control plane

Deploy on Nutanix Clusters from RHACM

Red Hat Advanced Cluster Management 2.9 deploys OpenShift clusters on Nutanix via CLI and UI

Three-node Clusters Support

Deploy 3-node compact clusters acting as control plane and compute machines

```
platform:
  nutanix:
    apiVIPs:
      - 10.40.142.7
    defaultMachinePlatform:
      bootType: Legacy
      categories:
      - key: <category_key_name>
        value: <category_value>
      project:
        type: name
        name: <project_name>
    ingressVIPs:
      - 10.40.142.8
    prismCentral:
      endpoint:
        address: your.prismcentral.domainname
        port: 9440
      password: <password>
      username: <username>
```

Deploy on Bare Metal from Cloud

The Bare Metal Operator Now Supports AWS, Azure, and Google Cloud

Use Red Hat Advanced Cluster Management or the Multicluster Engine in

Azure,

AWS, or

Google Cloud

to deploy bare metal clusters on your premises

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)
- More at Customize your Kubernetes - OpenShift gets composable and Installing Cluster Capabilities.

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

Excerpt from Install-config.yaml

Cloud Controller Manager(CCM) and Cluster API

	Out-of-tree Cloud Controller Manager	Cluster API
What	We GA'ed out-of-tree Cloud controller Manager(CCM) for AWS, Azure platforms.	Create Machines and MachineSets in CAPI
Why	Originally, Kubernetes implemented cloud provider-specific functionalities natively within the main Kubernetes tree (as in-tree modules). With more infrastructure providers supporting Kubernetes, the in-tree method became impractical and no longer advised. New providers supporting Kubernetes must follow the out-of-tree model.	We gradually plan to replace the Machine API controllers/code with Cluster API controllers and API types to reduce the maintenance burden of maintaining two competing solutions across multiple products. Users will be able to create Machines and MachineSets in CAPI for the following platforms; Azure, vSphere, (Possibly OpenStack + Baremetal).AWS & GCP is already TP.
When	Starting with **OpenShift 4.14**	**OpenShift 4.15+**
Who	No impact on user in any way. The out-of-tree implementation is backward compatible and does not impact OpenShift.	Users benefit from CAPI as it improves the scope of Machine management. This feature will come out as a Tech Preview and will provide a migration path to CAPI when it GAs.

OpenShift On OpenStack 4.14 Update

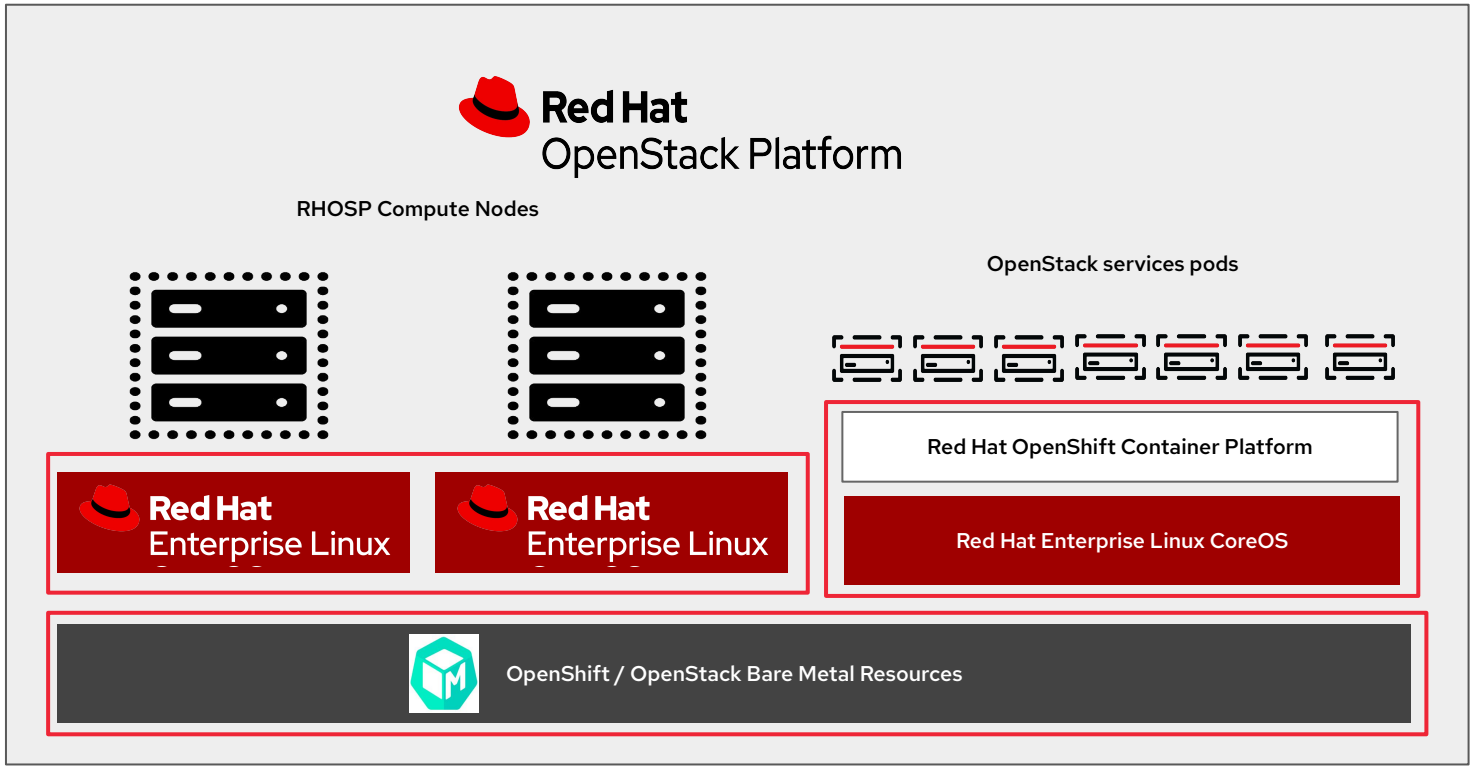
- MasterNode Root Volume types
  - Ability to choose root volume type for control plane vms at installation and in day2 (via CPMS)
  - Exposing local storage from the compute hosts for lower latency and I/Ops performance
  - Preserves the flexibility of using network attached storage such as ceph for th worker machines
- External Load Balancing with IPI
  - Support for MetalLB in BGP mode
  - BYOLB VIPs at install
- Master Node deployment Via MachieSets
  - Simplifies the controlplane recovery procedure
  - Enables better scaling

```
[...]
controlPlane:
  name: master
  platform:
    openstack:
      type: ${CONTROL_PLANE_FLAVOR}
      rootVolume:
        size: 100
        types:
        - performance.1
        - performance.2
        - performance.3
        zones:
        - cinder-1
        - cinder-2
        - cinder-3
      zones:
      - nova-1
      - nova-2
      - nova-3
  replicas: 3
compute:
- name: worker
  platform:
    openstack:
      type: ${COMPUTE_FLAVOR}
  replicas: 5
[...]
```

Red Hat OpenStack Services on OpenShift

Early access Dev Preview is Now available

- **Easier installation**
  - Contain-native installation reduces risk and creates better UX
- **Faster deployment**
  - Not just easier, but faster - reducing time to market
- **Unified management**
  - New management for today's applications
  - Shared bare metal resource inventory
- **For More information**
  - Announcement
  - Release Notes
  - Deployment guide

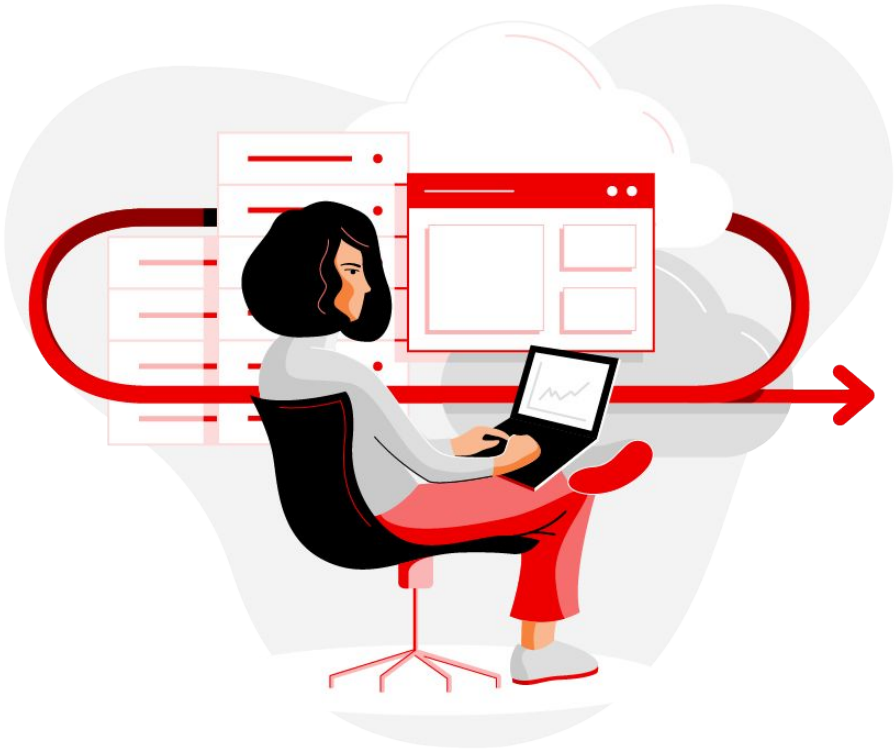


Red Hat

CoreOS Updates

Generally available in 4.14

RHEL CoreOS & Machine Config Operator Features

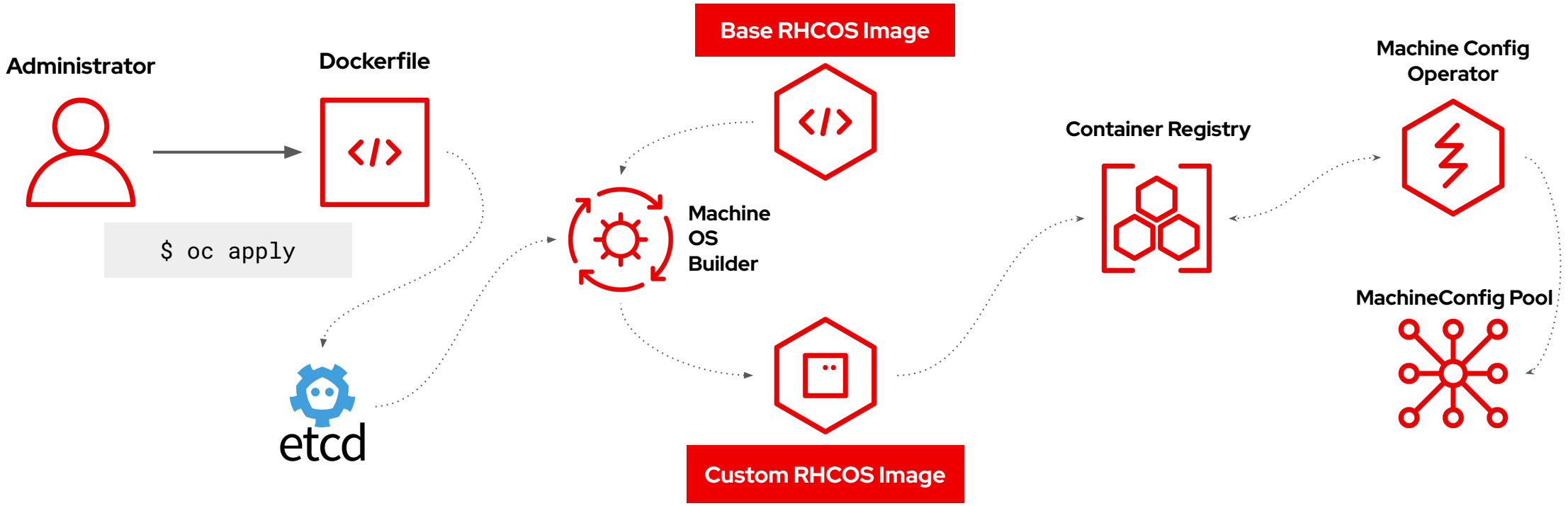


- Machine Config Operator (MCO) certificate rotation with paused pools
- Additional MCO metrics in Prometheus
- Offline provisioning of network-bound disk encryption
- NetworkManager-libreswan now available as an extension

Dev Preview in 4.14

CoreOS Layering on-cluster builds

Make it so!



Red Hat

Control Plane Updates

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

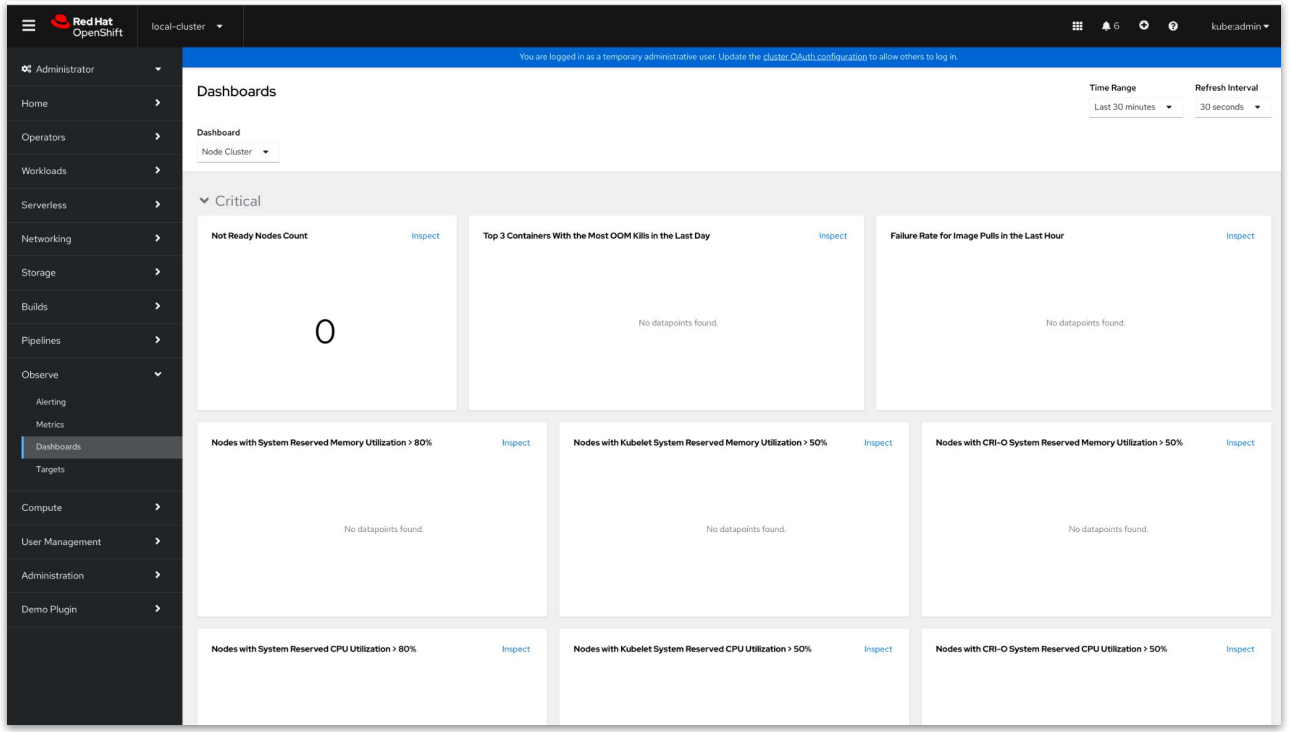
- Customer to check their java version compatibility with CgroupV2 (Please see release notes for more details)
- Cgroup V1 is available as non default
- All new cluster will be on CgroupV2
- All upgrading cluster will be on CgroupV1 with option to move to CgroupV2 as Day 2

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



Red Hat

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@sha256:1106aedc1b2e386520
oc2fb797d9a7af47d651db31d8e7ab472f2352da37d1b3
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+,
deploymentconfig.apps.openshift.io/registry-name1 created
[knarra@knarra zap]$
```

Enable customer to use Descheduler in big clusters

Removing memory limits in descheduler

Feature

- Due to default memory limit in descheduler it gets OOM kills especially in cluster with lot of pods where it needs more memory to deschedule lots of pods . We have removed memory limit in descheduler to avoid OOM kills

Previous

```
resources:
  limits:
    cpu: "100m"
    memory: "500Mi"
  requests:
    cpu: "100m"
    memory: "500Mi"
```

New Changes

```
resources:
  requests:
    cpu: "100m"
    memory: "500Mi"
```

Tech preview MaxUnavailableStatefulSet featureset

Technology Preview

Feature

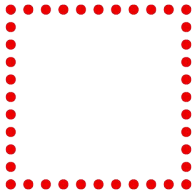
- The `MaxUnavailableStatefulSet` allows users to specify the maximum number of pods that can be unavailable during an upgrade. This means multiple pods can be upgraded in parallel, reducing the overall time taken for the upgrade and ensuring that a larger portion of the database remains available.

```
apiVersion: apps/v1
kind: StatefulSet
metadata:
  name: database-cluster
spec:
  replicas: 5
  updateStrategy:
    type: RollingUpdate
    rollingUpdate:
      maxUnavailable: 2
  ...
```

OCP Auth Updates in 4.14

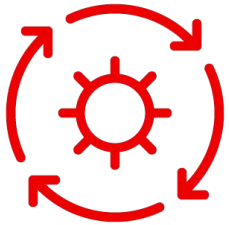
Secure OIDC token workflow with

`oc login –web`



PSa labels Modifications by user

when label sync on namespace is disabled



Auth Operator Proxy checks

Optimized to reduce frequent proxy config check

Networking & Routing

Red Hat OpenShift Networking Enhancements

OVN-Kubernetes as Secondary Interface [GA]

- Traditional secondary network plugins are simple / single-purpose and do not have the feature-rich capabilities of OVN
- For customers that want an additional (secondary) pod interface with the full feature set of OVN, OpenShift will support the ovn-kubernetes CNI plug-in on secondary interfaces
- Common use cases:
  - Traffic segregation
  - CNF development,
  - Virtualization (tenant networks, live-migration, etc.

Networking Enhancements

Admin Network Policy - Tech Preview

- 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
- Egress-specific policy targeting 4.15 for full GA of the feature

Red Hat OpenShift Networking Enhancements

OVN-Kubernetes North South IPsec [Tech Preview]

- OpenShift is adding support for North-South IPsec, and integrating it with the existing East-West IPsec capability
- Mechanics:
  - IPsec East-West: move to Host from cluster pod
  - IPsec North-South: join with E-W on Host
- Allows for encryption offload [Coming soon]
- Adds telemetry

Networking Enhancements

OVN-Kubernetes Multiple External Gateways

- Provides a declarative approach to defining the external gateways in a cluster
- Cluster Admin can use RBAC to control configuration

```
apiVersion: k8s.ovn.org/v1
kind: AdminPolicyBasedExternalRoute
metadata:
  name: multi-hop-policy
spec:
  from:
    namespaceSelector:
      matchLabels:
        trafficType: "egress"
  nextHops:
    static:
      - ip: "172.18.0.8"
      - ip: "172.18.0.9"
    dynamic:
      - podSelector:
          matchLabels:
            gatewayPod: ""
        namespaceSelector:
          matchLabels:
            egressTraffic: ""
        networkAttachmentName: gigabyte
```

Red Hat OpenShift Networking Enhancements

- **Additional IPv6 Support**
  - Single-Stack IPv6 support for kubernetes-nmstate
  - Full Dual Stack support for vSphere
  - Support Dual Stack IP assignment for whereabouts CNI/**IPAM**

- **Dynamic Secondary Network Attachments**
  - Important for Virtualization deployed in Kubernetes
  - Dynamic network attachments require a CNI plugin that runs resident in memory (a "thick plugin") as opposed to as a one-shot ("thin plugin")
  - Multus 4.0 enables thick plugins with a client/server model
  - Consists of two binaries:
    - **multus-shim** – "client", the CNI plugin
    - **multus-daemon** – "server", local agent that runs on all nodes and supports new features such as metrics, logs

Networking Enhancements

- **Support for Migration from OpenShiftSDN to OVN-Kubernetes on Multi-NIC UPI Environments**
  - Most on-premises production deployments utilize multi-NIC cluster hosts
  - We now support seamless migration from OpenShiftSDN to OVN-Kubernetes CNI plugin for UPI in those environments

- **Egress IP Multi-NIC Support**
  - Ability to associate an Egress IP configuration with a non-primary NIC
  - Administrators are provided with a greater level of control over networking aspects, such as routing, addressing, segmentation, and security policies
  - For example, for traffic isolation: eth0 (mgmt network) and eth1 (default route towards external communication)

Red Hat OpenShift Networking Enhancements

- **OpenShift Router upgrade to HAProxy 2.6**

  HAProxy 2.6 brings:

  - Latest security features
  - Performance optimizations
  - Bug fixes
  - New features and API enhancements

- **Support the ability to add additional HTTP headers to HAProxy without needing to customize the haproxy.config template**

  - Enhance security for web applications
  - Improved Authentication and Authorization among multiple microservices
  - Standards compliance
  - Improved performance
  - Easier debugging and troubleshooting

Networking Enhancements

- **Ingress Node Firewall (with stateless firewall support) [GA]**

  - First line of defense for a network and plays a crucial role in ensuring the security, reliability, and compliance of the network infrastructure
  - Uses an extended Berkeley Packet Filter (eBPF) and eXpress Data Path (XDP) plugin to process node firewall rules, update statistics and generate events for dropped traffic

- **NMstate-Policy Management via console**

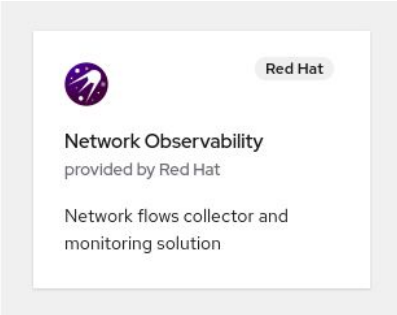
  - One can access the NMstate Operator and resources such as the
    - `NodeNetworkState` (NNS)
    - `NodeNetworkConfigurationPolicy` (NNCP)
    - `NodeNetworkConfigurationEnhancement` (NNCE) from the web console

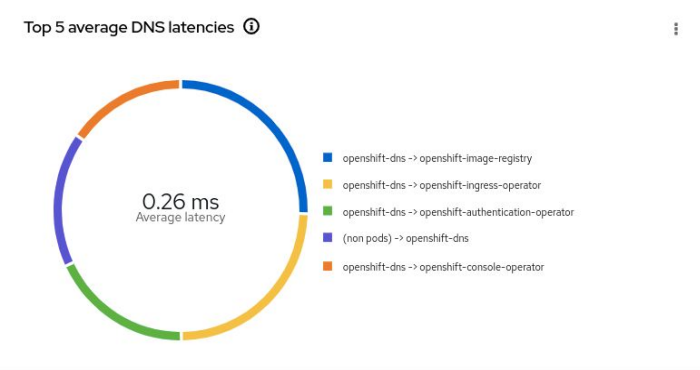
Network Observability Operator

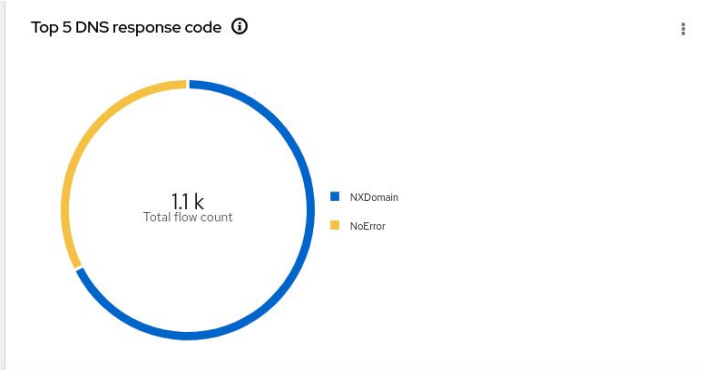
Network Observability Operator v1.4

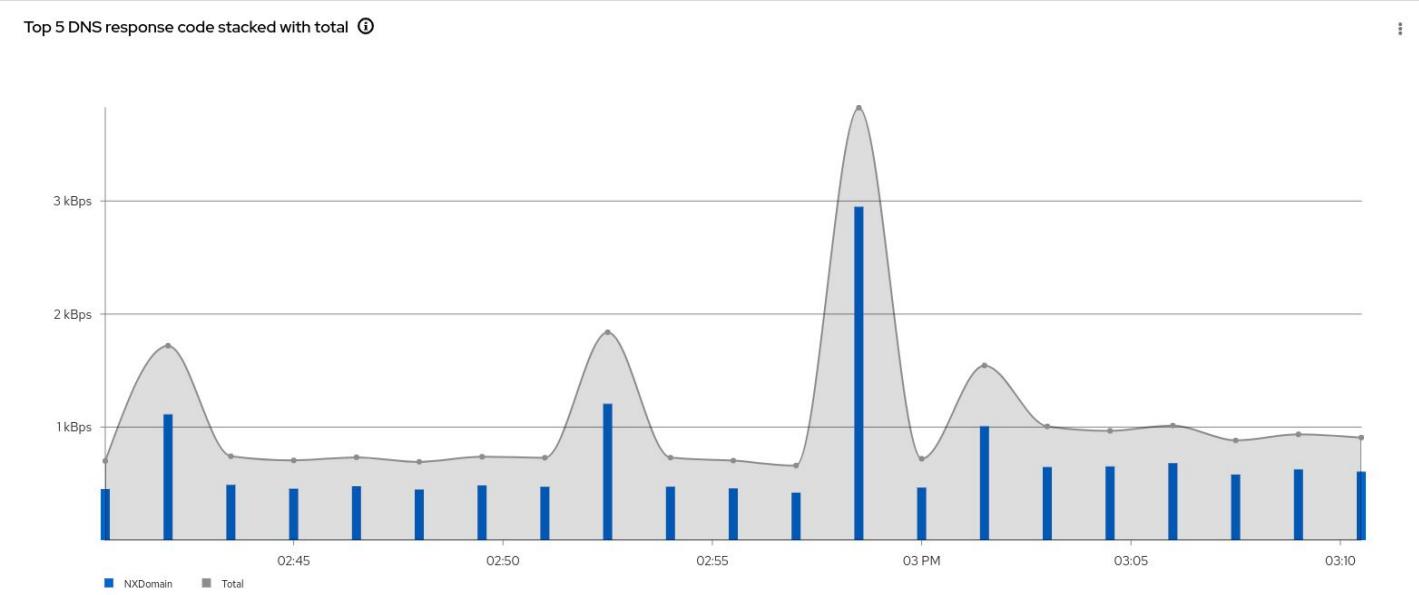
What's new:

- 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









Red Hat

Security

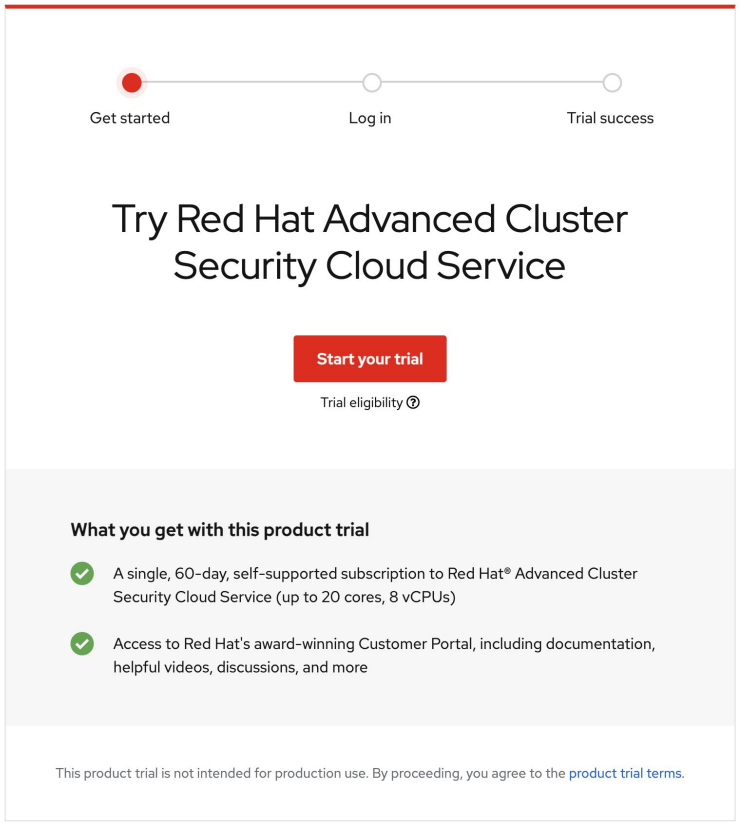
Red Hat Advanced Cluster Security (RHACS) for Kubernetes

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

- 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



Red Hat

RHACS for Kubernetes Highlights

New Features and Enhancements

New
Enhanced

Vulnerability Management

- Scanning Images from Registry Mirrors in OpenShift
- VM2.0: CVE Report

Network Security

- Enhanced: Run Time network policy generation
- New “Listening Endpoints” in GUI
- Build Time Network Policy Tools (TP)

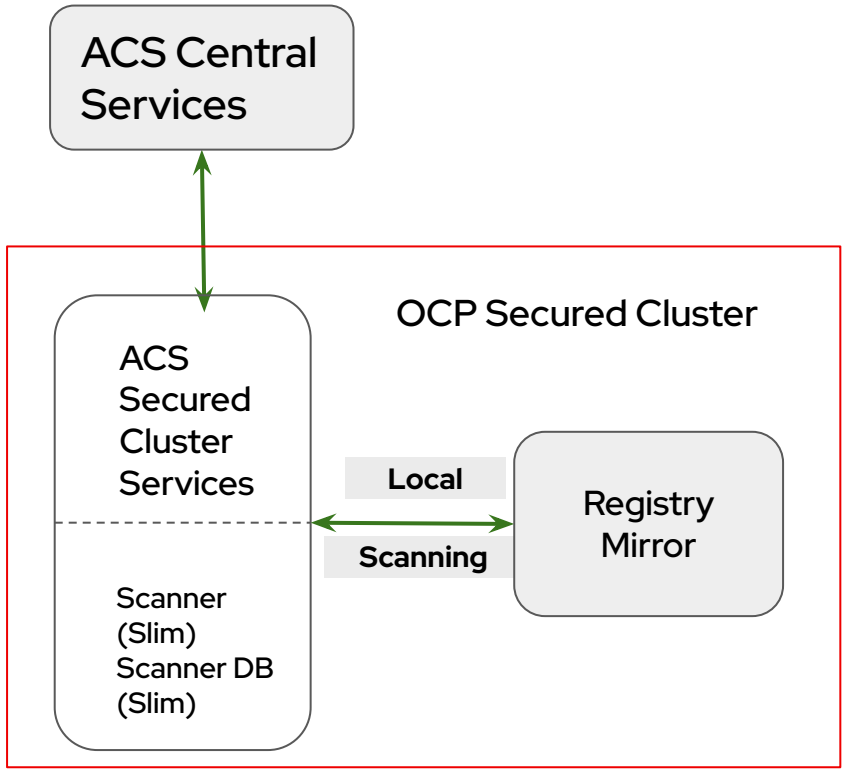
AuthN/Z

- Declarative Configuration for RBAC

Vulnerability Management

Scanning support for Images stored in Registry Mirrors

- Leverages : Delegated Scanning
  - Scan disconnected registries via the Secured Clusters
  - ACS 4.2+: Configure delegated image scanning in GUI
- Scan images from your registry mirrors in OCP
  - We read the mirror setup in OCP
  - ImageContentSourcePolicy, ImageDigestMirrorSet, and/or
  - ImageTagMirrorSet custom resources



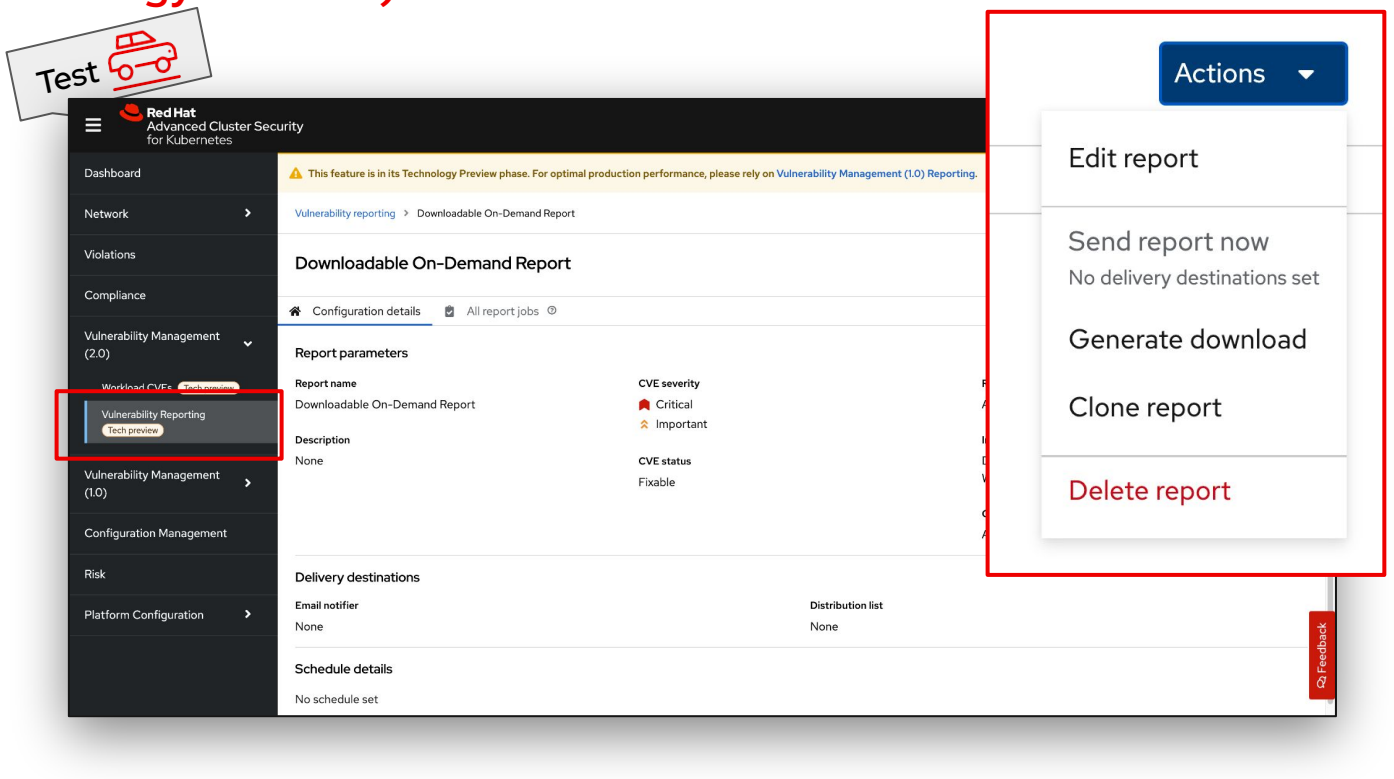
Vulnerability Management 2.0 (VM 2.0)

Workload CVEs and On-demand + Downloadable CVEs Report

(Technology Preview)

- **Workload CVEs**
  - Purpose built workflows to get users to accurate & actionable CVE data in just few clicks; to help with vulnerability remediation
  - Current Vulnerability Management 1.0 functionality will gradually transition to VM 2.0; feature by feature

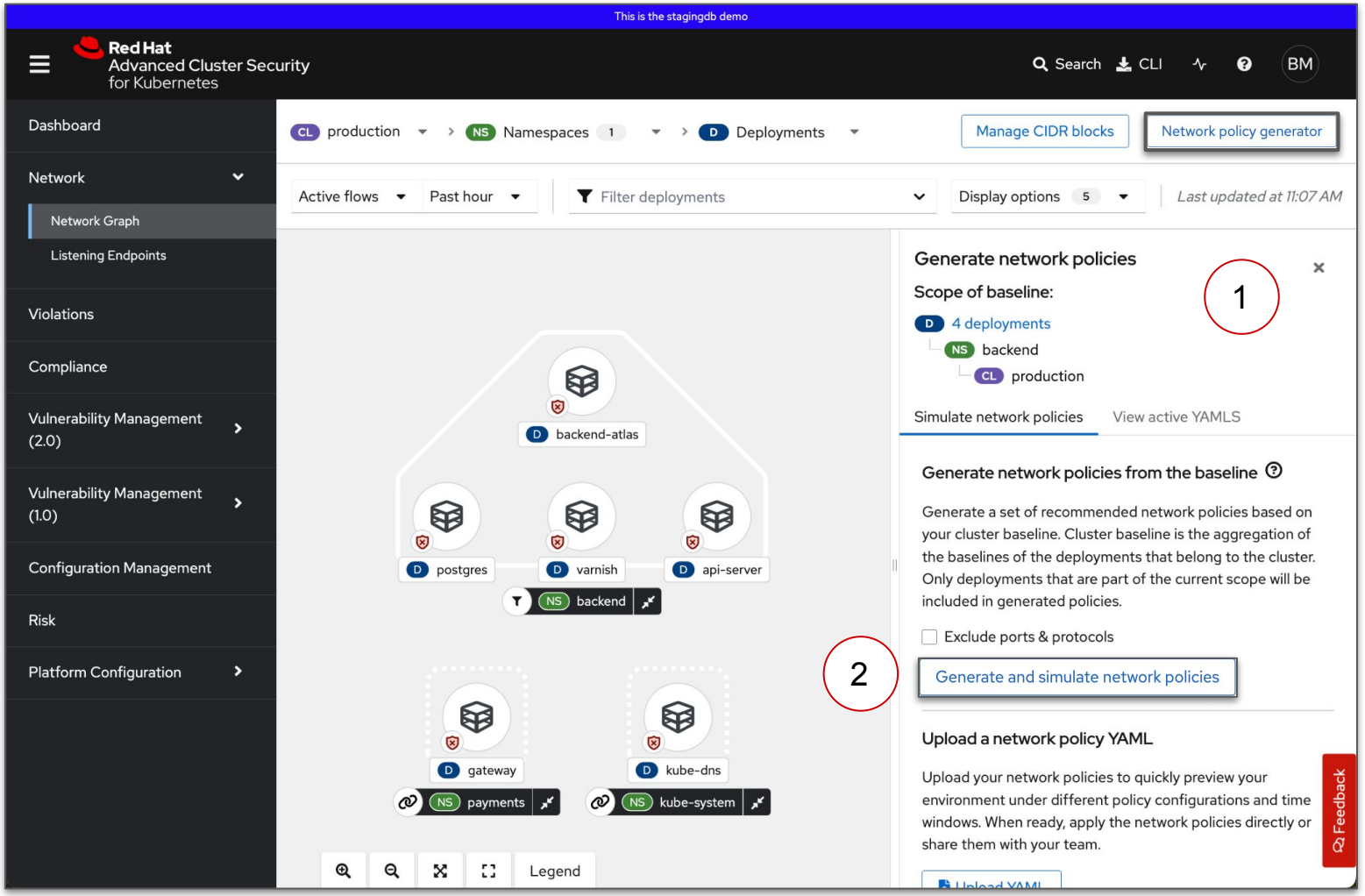
- **Create** & **Download** an **on-demand** workload **CVEs report in CSV format**
  - Easy to share with stakeholders or auditors
  - Includes all the necessary details to assist with CVE triage
  - Configurable report scope



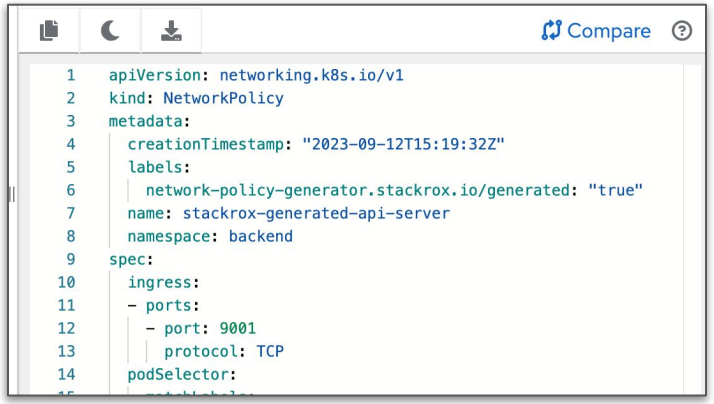
Red Hat

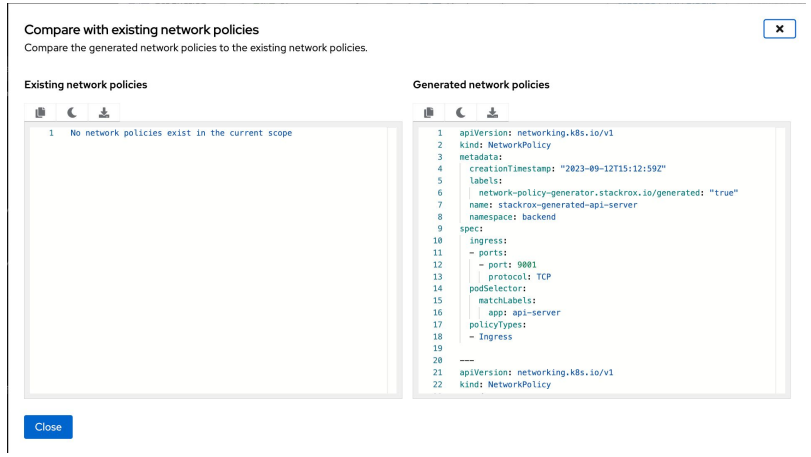
Red Hat Advanced Cluster Security for Kubernetes

Runtime Network Policy Generation



3

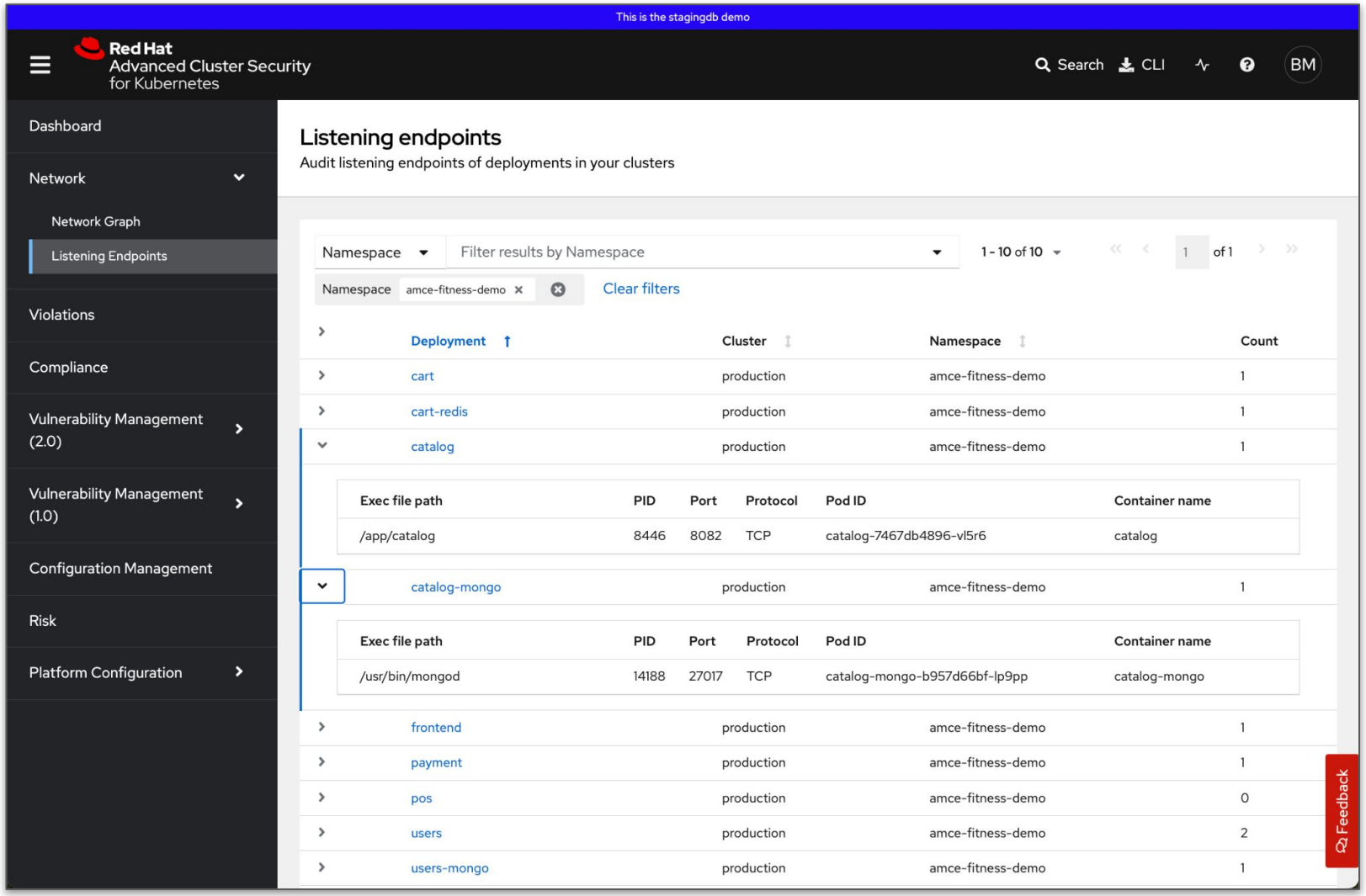




Red Hat

Red Hat Advanced Cluster Security for Kubernetes

ACS Audits Listening Endpoints



Red Hat

Red Hat Advanced Cluster Security for Kubernetes

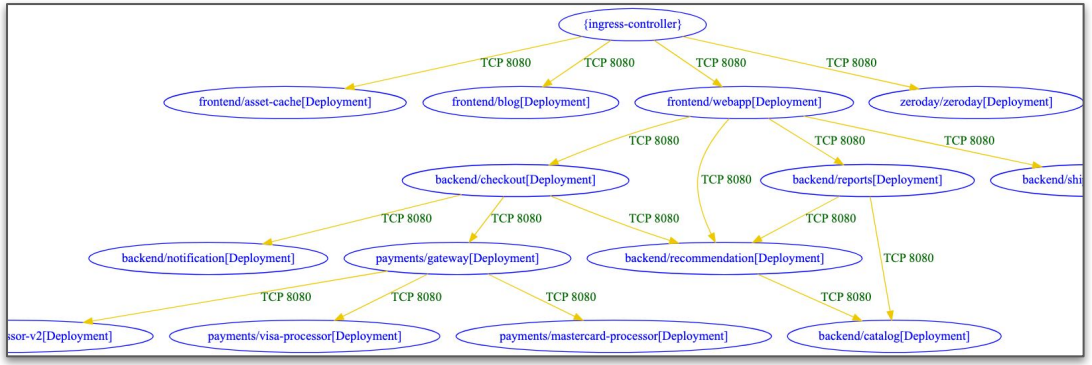
Built Time Network Policy Dev / DevOps Tools

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

Red Hat

Red Hat Advanced Cluster Security for Kubernetes

Manage ACS AuthN/Z configuration as code

Manage access, as code, the auditable and easy way

- Configure AuthN/Z resources declaratively
  - Authentication providers
  - Roles
  - Permission sets
  - Access scopes

```
central:
  declarativeConfiguration:
    mounts:
      configMaps:
        - declarative-configs
      secrets:
        - sensitive-declarative-configs
```

- Manage AuthN/Z YAML configurations in Git repos
- Configurations are mounted during Central installation
- Store configurations for authentication providers in a secret for greater security, ConfigMap can be used for rest
- Multiple configurations can be added into a single ConfigMap or Secret

RHACS: Using declarative configuration

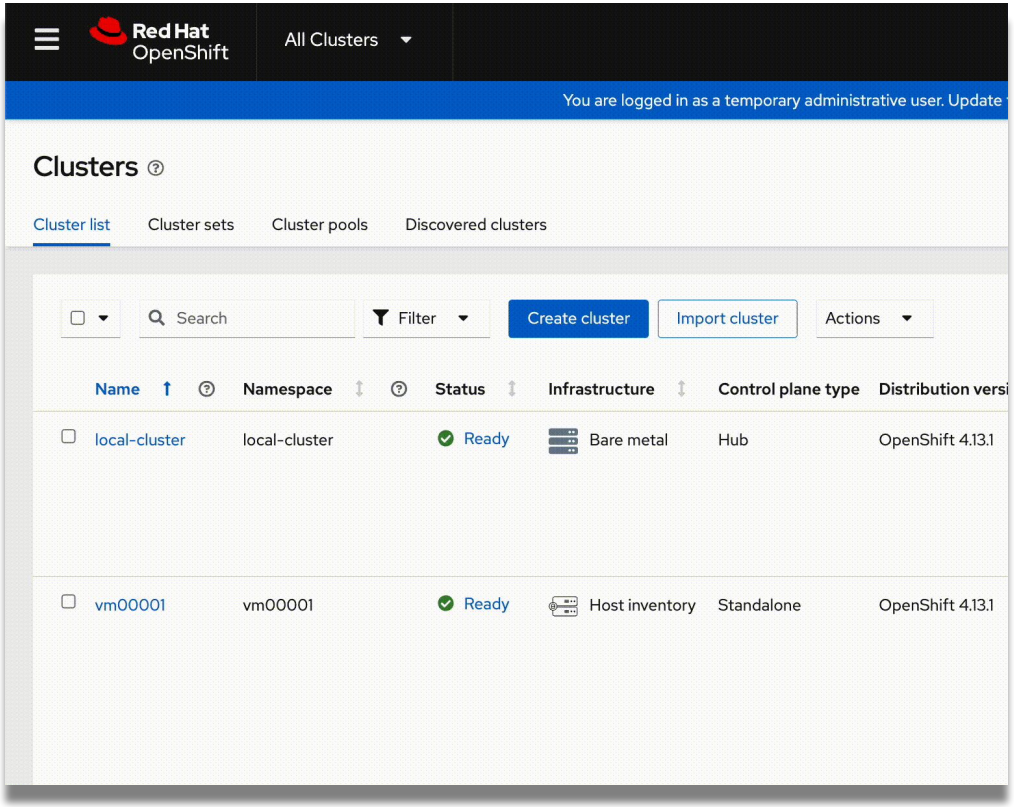
Management

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**
  - Nutanix available as a provider in Create Cluster UI flow from the RHACM Console
- **Adjust RHACM hub capacity directly**
  - Scale nodes for the RHACM hub local-cluster
- **Allow node disk-wiping with ZTP**
  - Reduces the need of manual intervention when setting up nodes for Zero Touch Provisioning (ZTP)
- **Hosted Control Planes Generally Available**
  - Hosted Control Planes reach its general availability on OpenShift Virtualization and Bare Metal with advantages such as optimized costs and reduced resource footprint

Red Hat

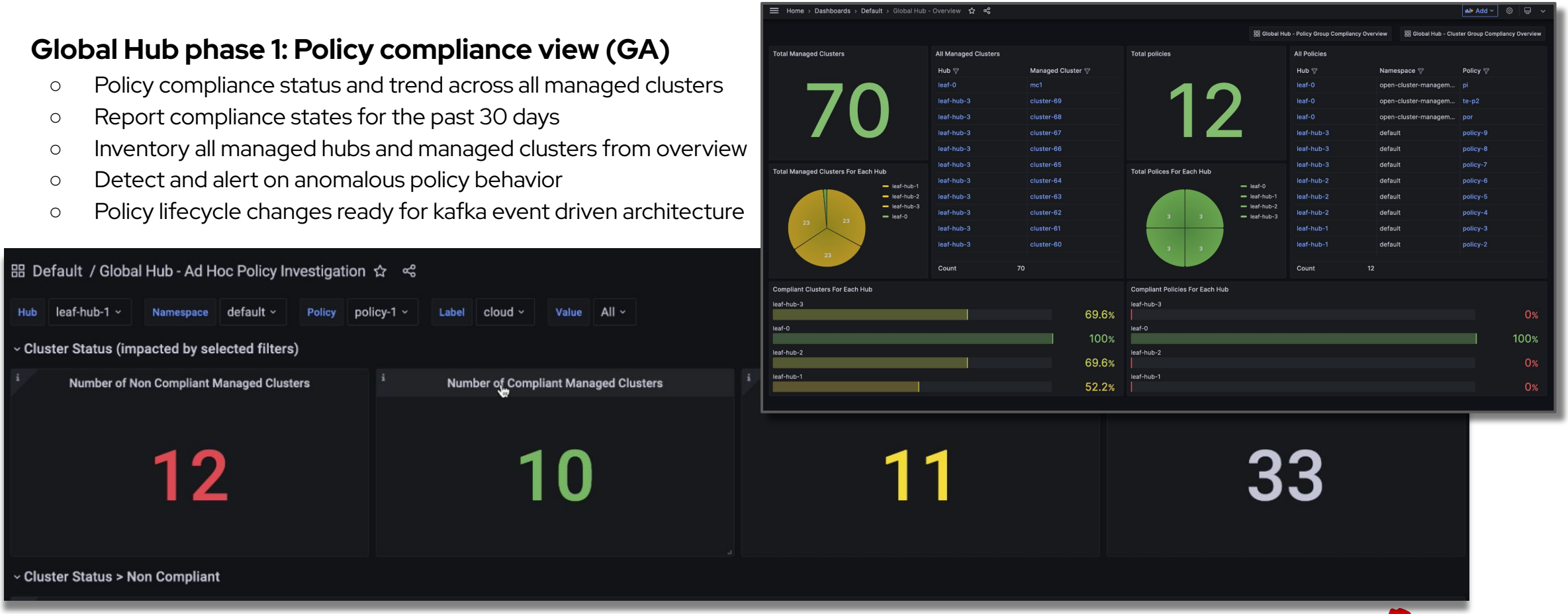
Red Hat Advanced Cluster Management for Kubernetes

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



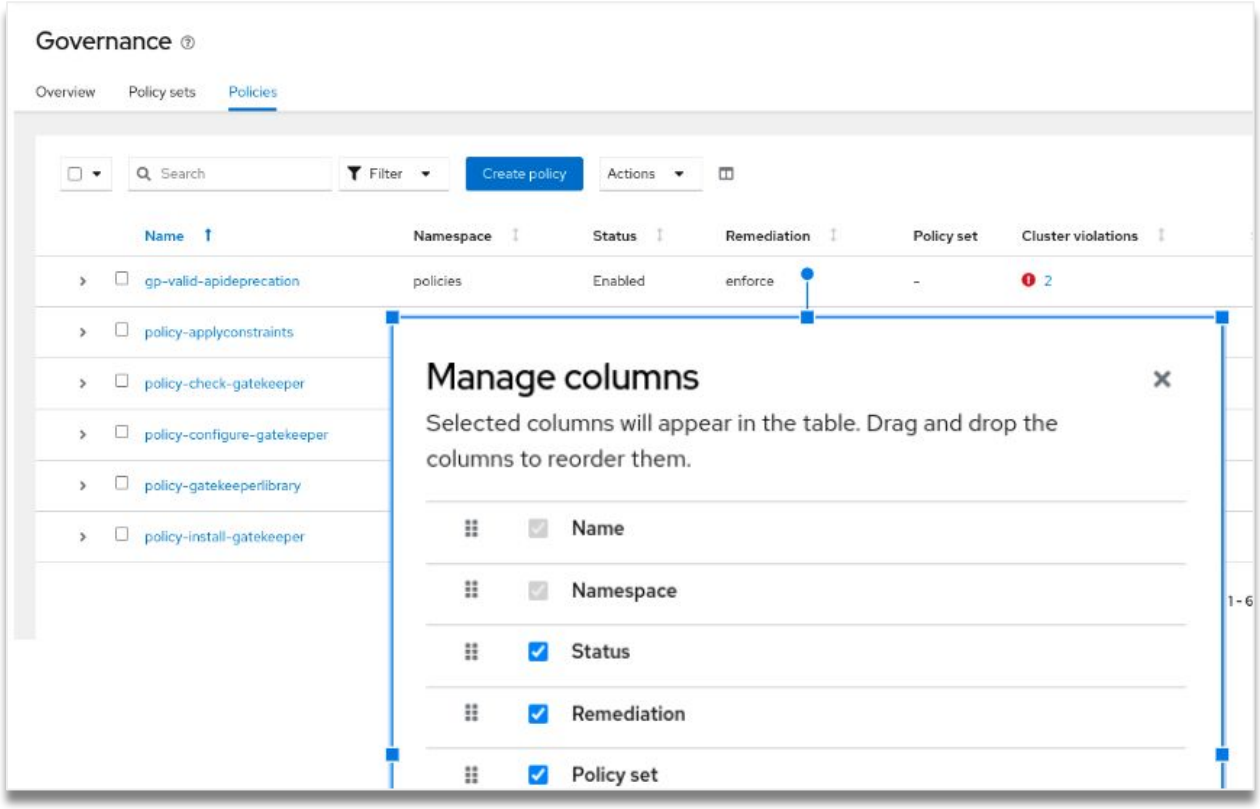
Red Hat

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.9

Governance

Red Hat Advanced Cluster Management Governance framework continues to evolve by keeping up with the growing Kubernetes policies landscape and enhancing user experience.



- **informOnly remediation**
  - more control and consistency of what is enforced and what is **only** informed in nested policies/rules
- **Gatekeeper operator uplift to 3.11.1**
  - staying up to date with the latest bits from the open source community
- **Policy view design customization**
  - users can now select what it's shown in the policies dashboard and improve persona usage
  - future work: custom columns
- **Improvements for selective policy enforcement**
  - Allow enforcing a policy to a subset of clusters that the policy applies to for a controlled rollout.
- **Enhancements for Policy Templating**
  - new functions available to use when using Policy templates e.g *trimAll*

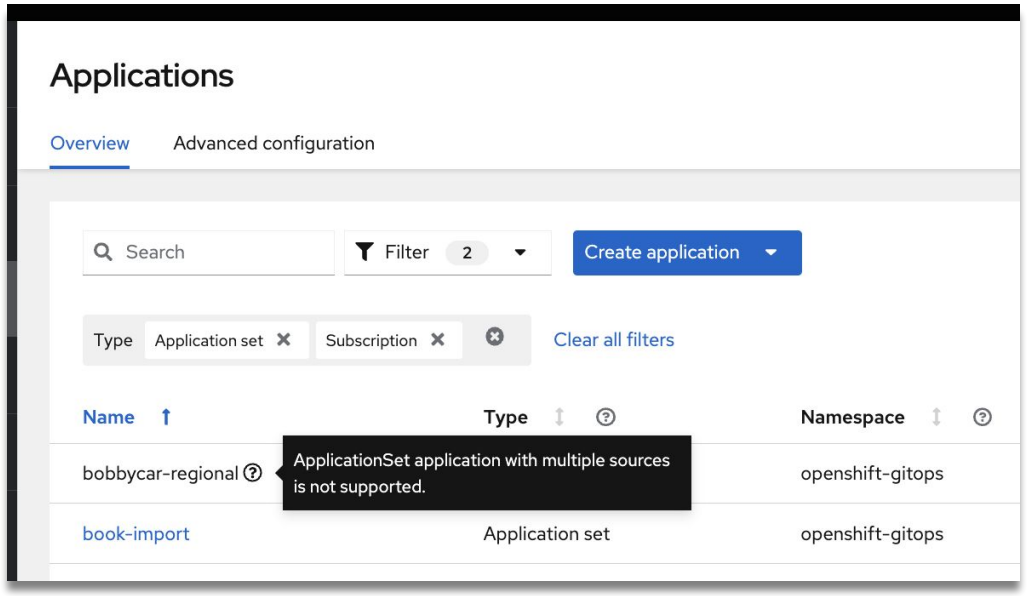
Red Hat

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.9

Application Lifecycle

RHACM extends platform GitOps capabilities by enhancing fleet level deployment patterns for applications and configurations.



- **UI Support for multi-source ArgoCD-Applications (TP)**
  - Support for deploying ArgoCD applications that follows a common multi-source pattern to be deployed from RHACM and be displayed in the Applications menu.

- **Customized Service Account with GitOpsOperator**
  - RHACM and the GitOps operator integration adds a new layer of customization and security now allowing for custom service accounts and permissions to be assigned.

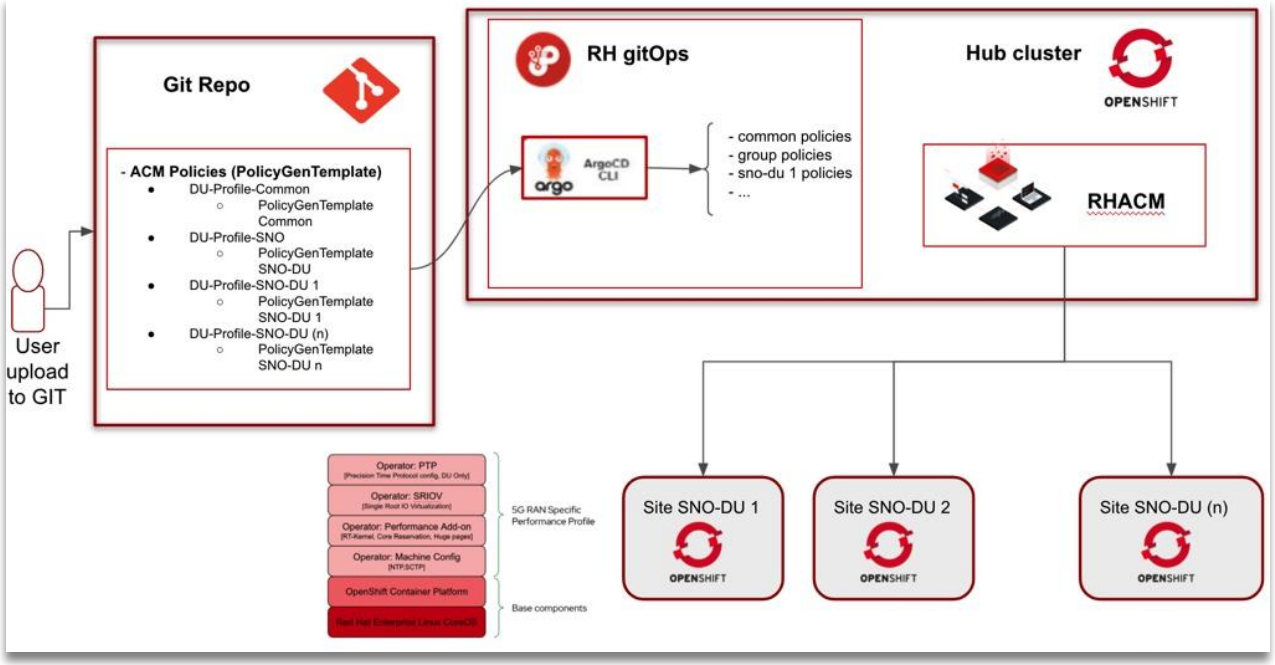
Red Hat

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.9

Manage At Scale

Consistency at scale for edge use cases across verticals such as Telco, Industrial and Commercial. RHACM provides a single API, CLI and UI to standardize regardless of where your application runs.



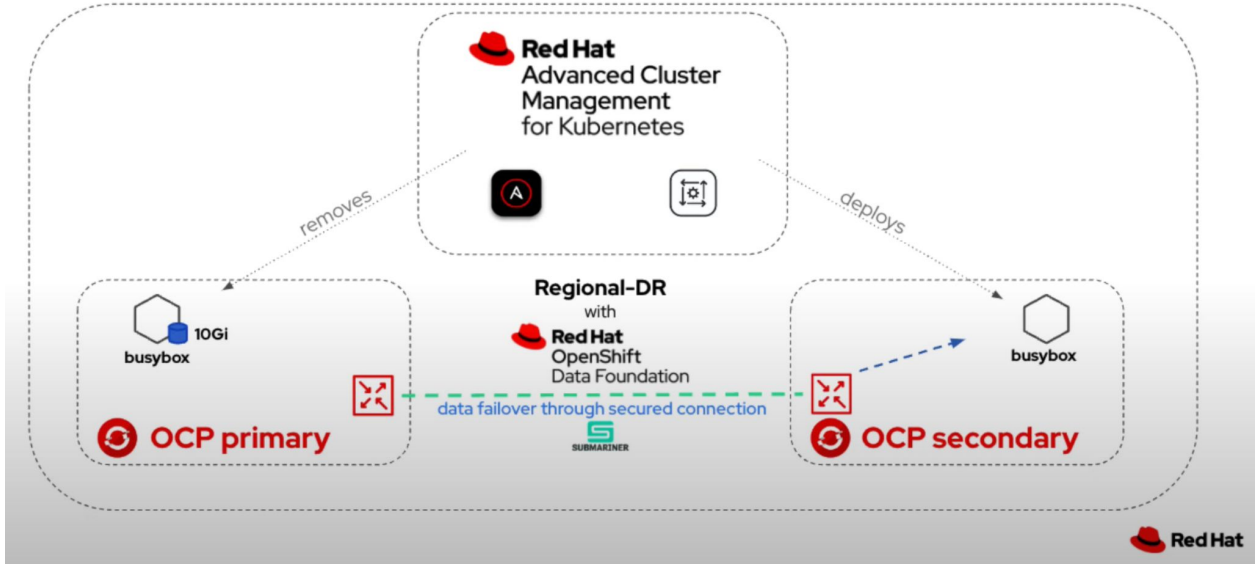
- **Extend scale** in a mixed fleet of OpenShift clusters:
  - TALM enhancements for Selective Policy Enforcement + Cluster Group Upgrade Timing
  - RHACM hub capacity-planning tooling
  - Improvements in performance and scale across mixed-fleet scenarios:
    - 5G-RAN: 3500 SNOs with the DU Profile
    - Mixed fleet: 857 SNOs, 200 3-node compact, 200 6-node with the DU Profile
    - Retail: 432 Compact Clusters deployed with the DU Profile
    - Standard: 207 6-node with the DU Profile

Red Hat

Red Hat Advanced Cluster Management for Kubernetes and OpenShift Data Foundation

Business Continuity

RHACM provides application disaster recovery solutions for your mission critical workloads.



** Check out these videos to see how Red Hat can automate your Business Continuity needs

https://www.youtube.com/watch?v=gqdJdVOqsrI

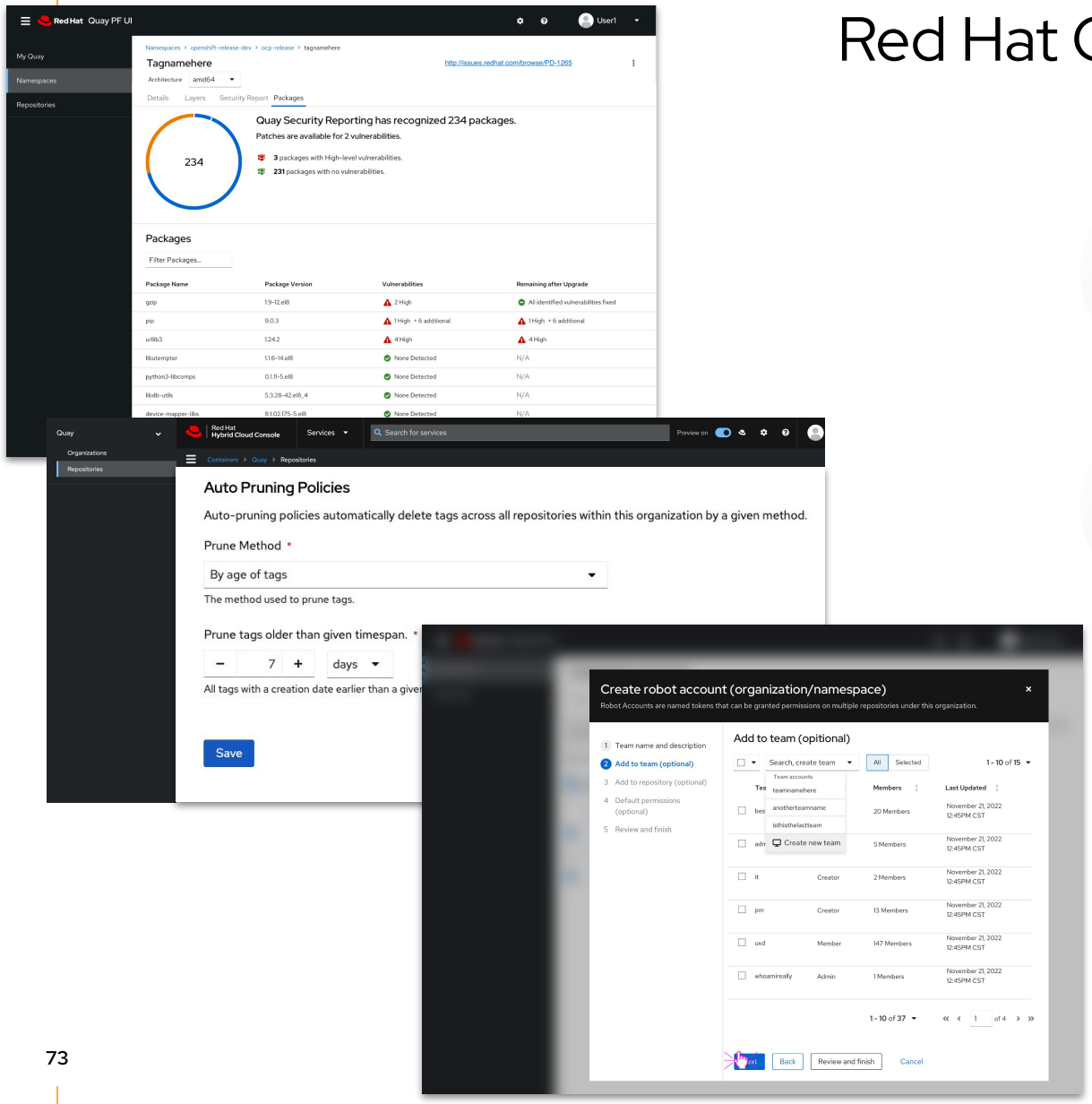
https://www.youtube.com/watch?v=rPZH0BaaiHc

- **Regional stateful app replication with ODF 4.14 (GA)**
  - Multicluster networking provided by Submariner for regional DR
- **Asynchronous Volume Replication => low RPO**
  - OpenShift Data Foundation (ODF) enables cross-cluster replication of RWO/RWX PVs with low replication intervals
- **Automated Failover Management => low RTO**
  - RHACM and ODF DR operators enables failover and failback automation at application granularity

** Regional DR provided in conjunction with OpenShift Data Foundation Advanced 4.14. Please review the ODF-Advanced release schedule for specific details.

Red Hat

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.

Red Hat

Observability

OpenShift Observability: Five Pillars

Store:
Metrics with *Prometheus/Thanos*
Logs with *Loki*
Traces with *Tempo*

2 **Data Storage**

1 **Data Collection**

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

Observability

"Turn your data into answers!"

Third Party Integration

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

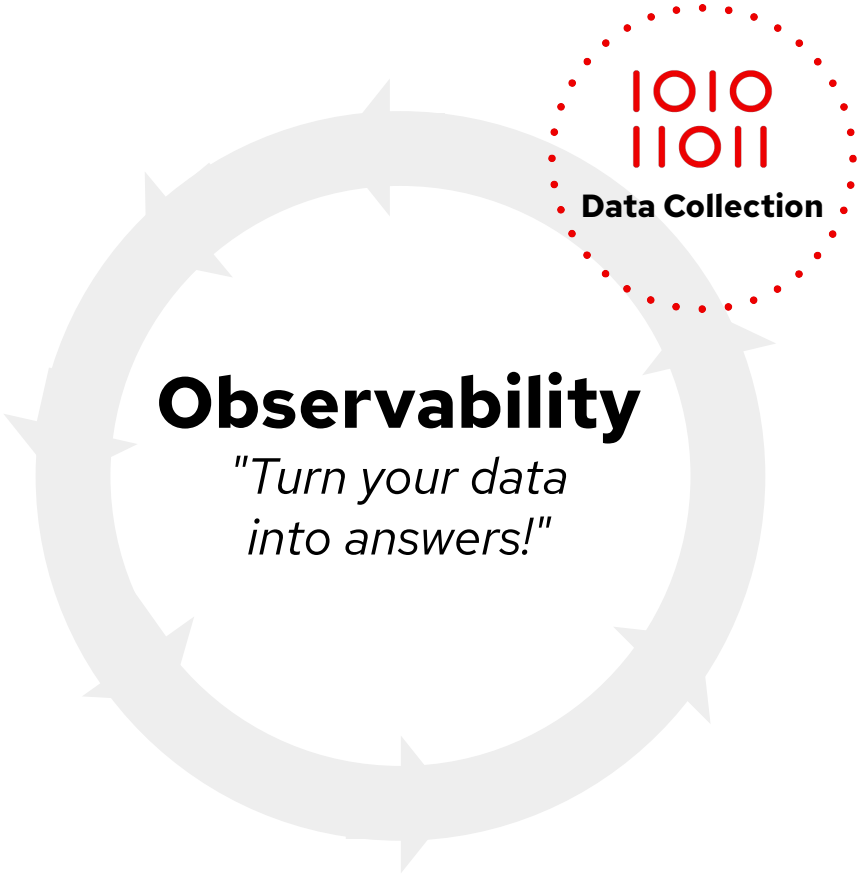
3 **Data Delivery**

5 **Data Analytics**

Analyze:
Query metrics
Search metrics targets
Filter logs by severity

4 **Data Visualization**

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



OpenShift 4.14 Monitoring

- Add option to specify resource limits for all components
- Customizations for node-exporter collectors (Phase 2)
- Extend user customizable TopologySpreadConstraints to all relevant pods (will finish in 4.15)

Logging 5.8

- Kube-API audit log filtering to reduce log sizes

OpenTelemetry Operator (Tech Preview)

- Support to collect OTLP metrics
- OpenTelemetry collector operator level 4 (Deep insights)

Observability

"Turn your data into answers!"

OpenShift 4.14 Monitoring

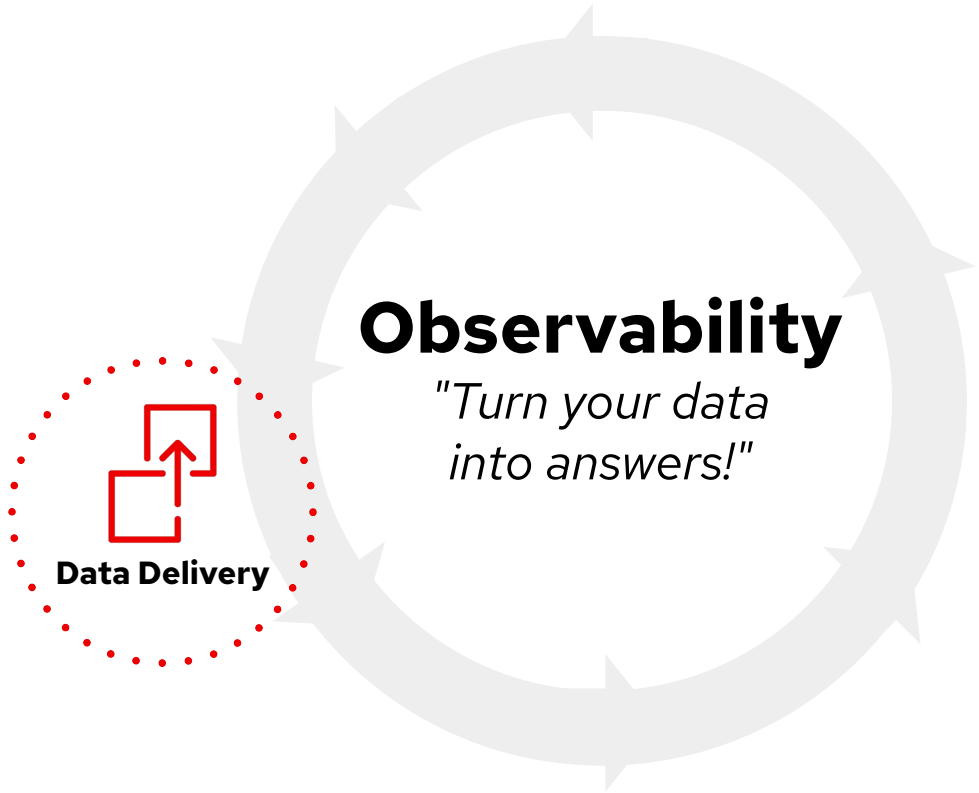
- Prometheus labels: reduce memory by changing the implementation of labels

Logging 5.8

- Loki - zone-aware replication
- Loki - cluster restart hardening
- Loki - Reliability hardening

Distributed Tracing

- Tempo support for Jaeger Thrift, Jaeger gRPC and Zipkin.
- Tempo operator level 4 (Deep insights)
- Tempo Gateway: Query frontend with authorization and authentication



OpenShift 4.14 Monitoring

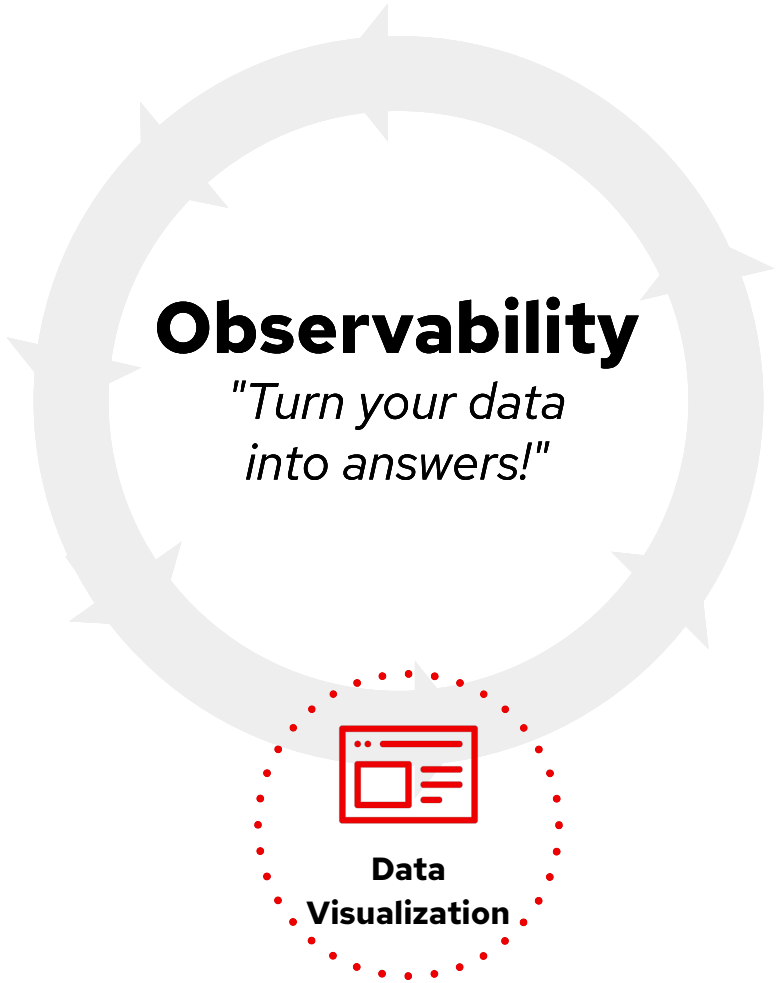
- Allow admin users to create new alerting rules based on platform metrics
- Deploy the monitoring console plugin resources via CMO

Logging 5.8

- Multiple log forwarders allow users to forward logs to multiple endpoints

OpenTelemetry Operator (Tech Preview)

- Forward OpenTelemetry metrics outside OpenShift via OTLP HTTP(s) & gRPC
- Convert OpenTelemetry metrics to Prometheus
- New processors: resourcedetection and k8sattributesprocessor to enrich metrics



OpenShift 4.14 Monitoring

- Expire silences **in bulk**
- **Silences Tab** added to the Web Console - Developer Perspective

Logging 5.8

- **Log-based Alerts** in Web Console - Developer Perspective
- LokiStack Console Plugin allows **searching for patterns across all namespaces** Developers have access to
- Loki **Health Dashboards** allows users to see the overall health and status of their Loki storage

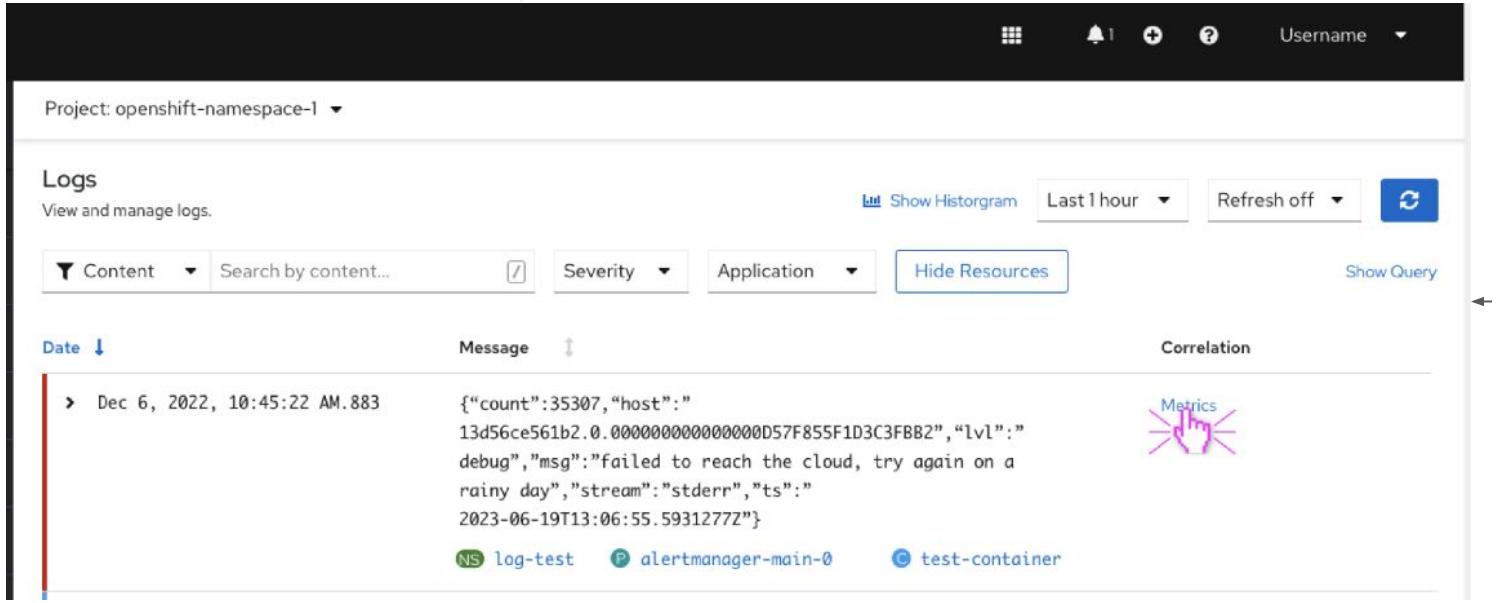
Observability

"Turn your data into answers!"

Data Analytics

Logging 5.8

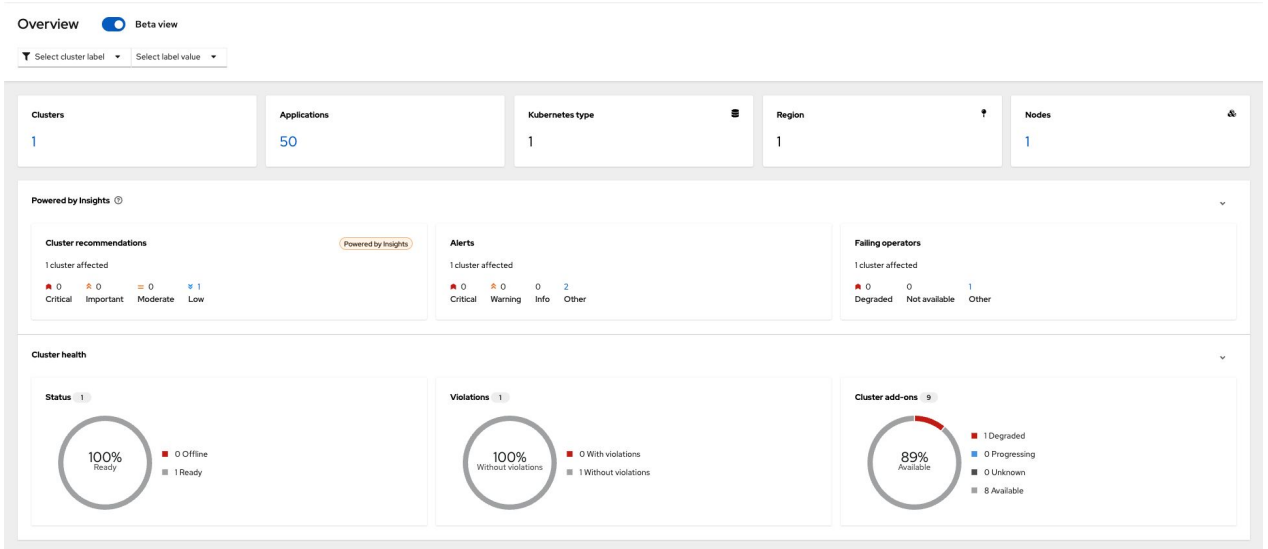
- **Dev Preview**: Correlation Experience in Web Console (**Links** - Alerts to Logs & Logs to Metrics)
- Powered by **korrel8r**



Red Hat

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
- **Red Hat Advanced Cluster integration** - new integration with ACM 2.9 in FleetManagement
- **On-demand data gathering** - gain quick update on applied recommendations by manually triggering data upload
- **Workload recommendations** available to on-premise customers (soon to be certified), also features recommendations with real names of resources

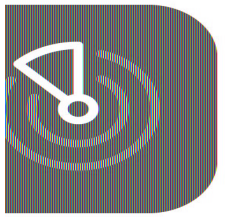


RHACM 2.9 Overview page

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

Red Hat

Insights Cost Management



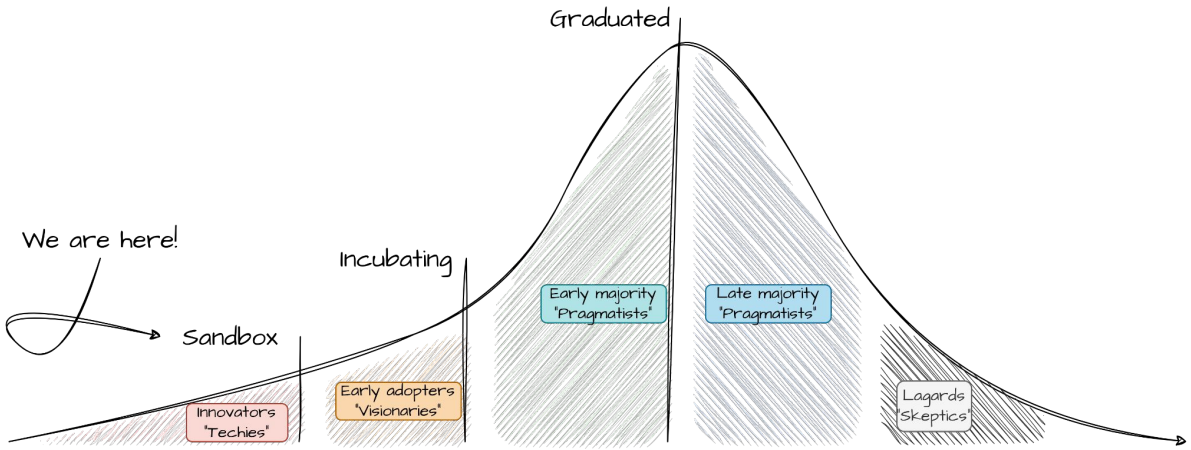
- **Free service to monitor per-resource (namespace, cluster, node, tag) usage and spending on-prem and major clouds**
- **Report vCPU count, RAM, and storage capacity**
  - Advanced cost model definition with distribution based on requested, used, or effective CPU or RAM usage, distributing the overhead costs of Kubernetes/OpenShift control plane.
- **Settings page**
  - New settings page has been redesigned and moved into to the Cost management application
- **Performance improvements** for customers with large data pipeline
  - Improvements to process data from large accounts in the most efficient way so you can gain quick feedback and up2date reports
- **Cost Management Metrics Operator 3.0.0**
  - Lots of bug fixes and small enhancements
  - Create default distinct Source name for users to quickly identify their clusters

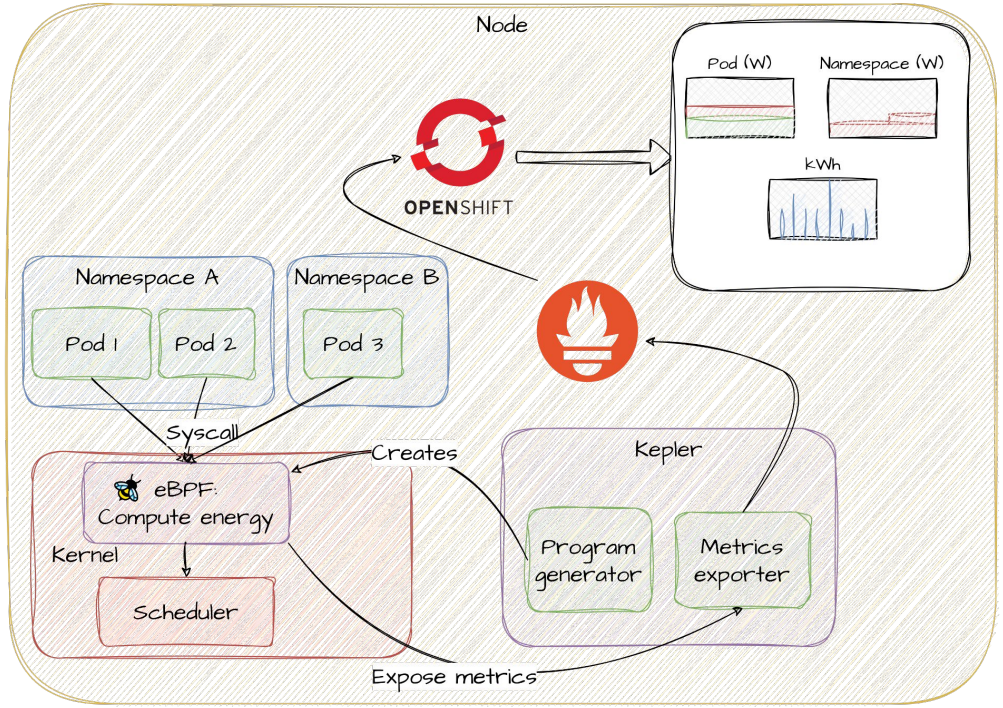
https://www.redhat.com/en/blog/whats-new-red-hat-insights-cost-management

Sustainability

In previous episodes... Kepler!

- **Kepler** (Kubernetes-based Efficient Power Level Exporter) that offers a way to estimate power consumption at the process, container, and Kubernetes pod levels.
- Kepler provides **granular power consumption** data for Kubernetes Pods and Nodes.
- It uses eBPF to collect energy-related system stats and export them.
- RAPL and ACPI when available or trained models for specific hardware otherwise.





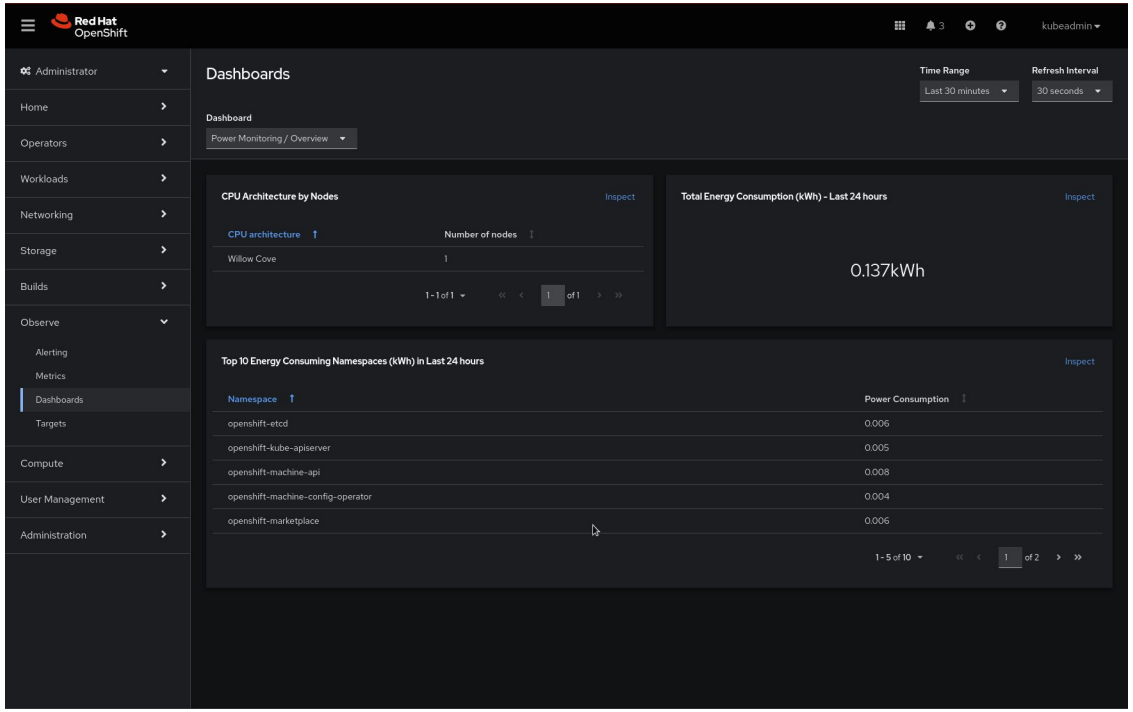
- Kepler was accepted to **CNCF** on May 17, 2023 and is at the **Sandbox project** maturity level.

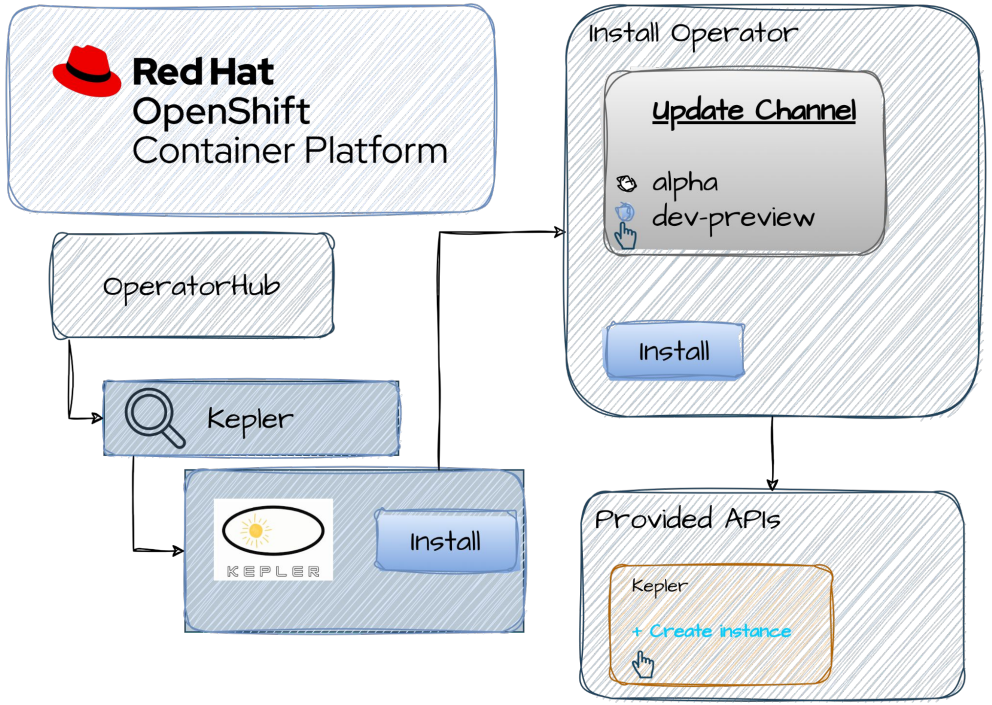
Red Hat

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**





Red Hat

Virtualization

OpenShift Virtualization

Modernize your operations with comprehensive lifecycle and infrastructure management

More deployment options

- ROSA and AWS support
- Quickly deploy OpenShift tenant clusters on OpenShift with Hosted Control Planes

Protect your business critical workloads

- Recover from catastrophic failures with Metro-DR with ODF / ACM
- Support for Microsoft Windows Server Failover Cluster (WSFC)

Improved VM networking

- Microsoft Windows 11 support
- Enhanced VM networking with Secondary Networks for OVN-Kubernetes
- Dynamic reconfiguration - NIC hotplug

Migration Toolkit for Virtualization 2.5

- OpenShift to Openshift Migration
- Openstack Provider GA
- OVA Imports

Modern Virtualization

- Cloud Elasticity + Scalability
- Reduce Operating Cost
- Increase IT efficiency + reliability

Generally Available in OCP 4.14 + ACM 2.9

Consolidate OpenShift Clusters with OpenShift Virtualization

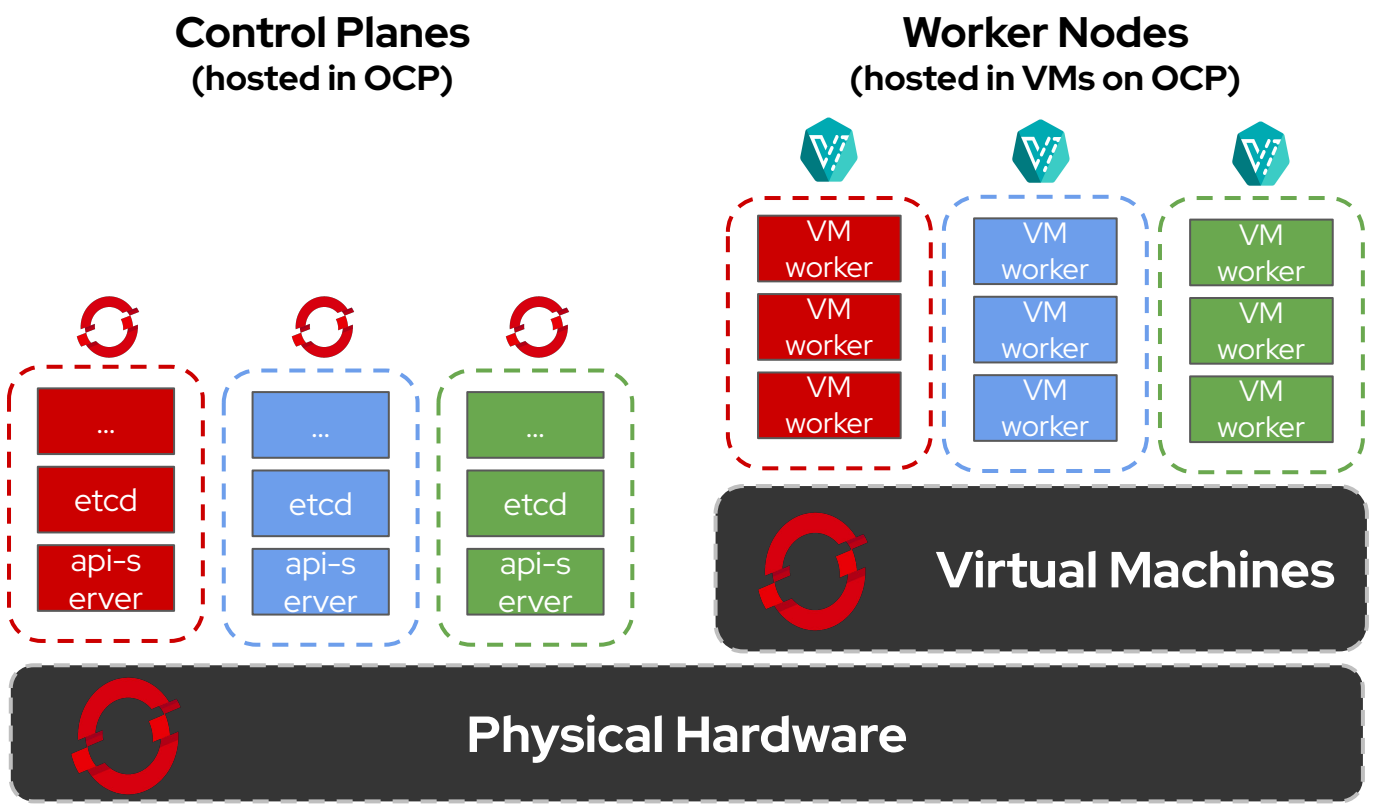
Hosted Control Planes with KubeVirt provider

Increase Utilization of Infrastructure

- Consolidate multiple control planes to reduce unused and underutilized infrastructure
- Increase physical host utilization by hosting virtual worker nodes for multiple clusters

Reduce Dependency on Legacy Virtualization

- Eliminate needing a legacy hypervisor to host your containerized infrastructure
- Virtual compute nodes require core-based subscriptions.
- Hosting OpenShift cluster uses included infrastructure subscriptions.



Red Hat

OpenShift sandboxed containers

Kernel Isolation for containerized workloads

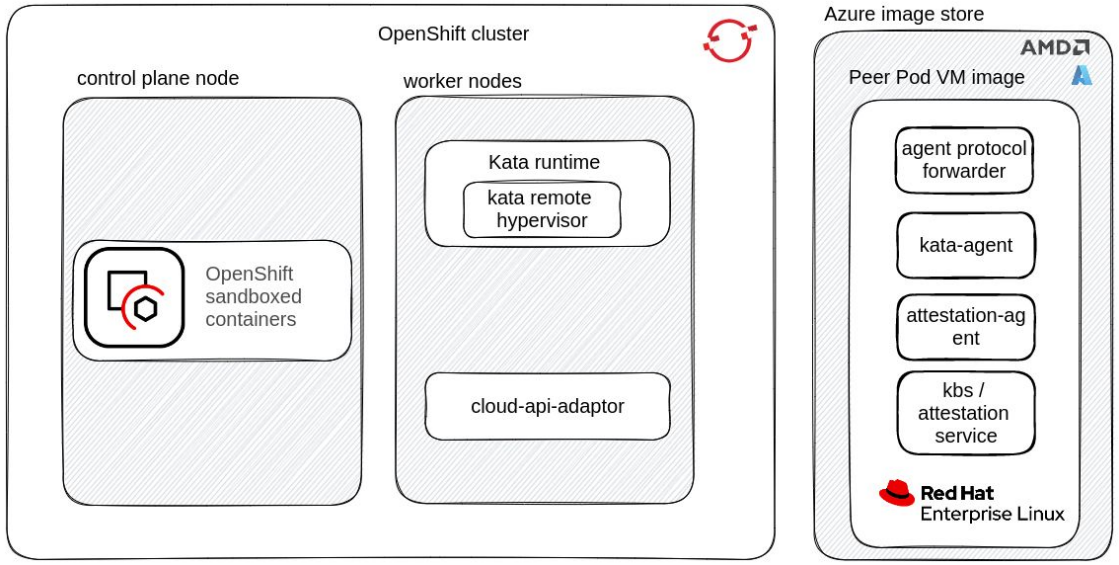
Cloud Support

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

Confidential Containers (Dev Preview)

- Support for encrypted containers
- Secure Key Release for encrypted containers

Sandboxed Container on IBM z (Tech Preview)



Red Hat

Specialized Workloads

Boost AI workloads with the NVIDIA L40S GPU

New NVIDIA support with OpenShift:

- NVIDIA L40S GPU accelerator
- AWS P4de (NVIDIA A100 80GB) and P5 (NVIDIA H100)
- OCI GPU shapes with NVIDIA A100

Red Hat OpenShift helps power next-generation data center workloads:

- Large language model (LLM) training and inference
- Generative Artificial Intelligence (AI)
- Intelligent chatbots
- Video processing applications

NVIDIA GPU accelerators on Cloud providers:

- AWS
- GCP
- Azure
- OCI (TP)

Kernel Module Management (KMM) Operator 2.0

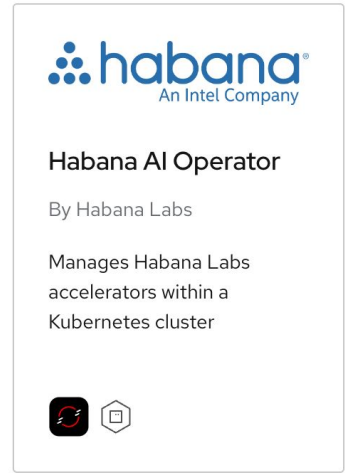
The KMM Operator manages kernel modules and device plugins in OpenShift as a day 2 operator and helps enable new specialized hardware as AI accelerators

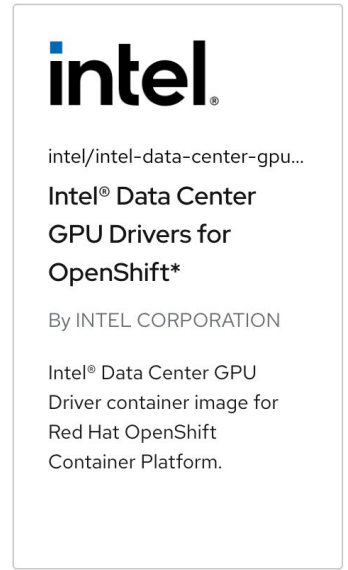
Following the 1.0 GA, these features are now available:

- Disconnected support
- Customizable steps for kernel module upgrades
- Replacement of inbox kernel module
- Multiple independent kernel modules deployment via a single KMM Module
- Hub and spoke GA support with Red Hat Advanced Cluster Management

Kernel Module Management Operator 2.0:

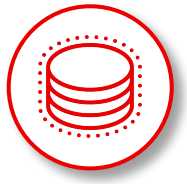
- Reduce resource utilization
- Support for firmware files without MachineConfig objects
- Provide a better upgrade experience





Red Hat

Windows Containers on OpenShift



Storage and CSI Proxy

- Intree drivers for vSphere and Azure are being removed
- Users will need to source their own CSI Drivers (from vendors or upstream) for these filesystems and put them on the appropriate nodes **before** upgrade
- Users will also need to make sure they are on latest minor release of their current major release
- WMCO operator will try it's best to **block** upgrades where attached volumes are detected (rest of cluster will upgrade as normal)
- User will need to add a label (per node) to allow upgrade to proceed

Cluster Wide Proxy

- Match the functionality already available on Linux
- Used for clusters where direct internet access isn't possible and HTTP/HTTPD proxies are required

New Cloud Platforms

- Windows Containers with OpenShift will be fully supported on the Nutanix platform
- Adds to the the choices of where you can run Windows Containers fully tested and supported

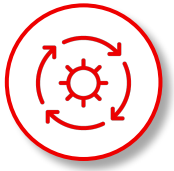
NUTANIX

Red Hat

Operator Framework

Operator Framework

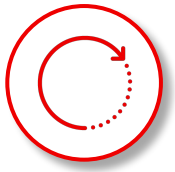
OLM 1.0 Preview **phase I**: Enable flexibility depending on your operational model



Fully declarative/GitOps-friendly workflows

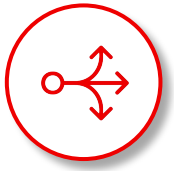
A **reduced user-facing API surface area** for managing your Operator fleet.

- "`Operator`": a single API to manage installed operators.
- "`Catalog`": a new API to serve catalog content.



Improved control over operator update

With the richer insight to catalog content, admins can also specify a **target version** to **install** and/or **update** to another **available target versions** in the catalog.



Greater visibility to the catalog content

New "`Catalog`" API provides greater details to operator packages about **all available operator bundle versions**, **operator bundle details**, **channels**, **update edges**, etc.

Flexible Operator packaging format

Release operator bundles containing **arbitrary k8s manifests** and **bundle size** is **no longer constrained** by the **etcd value size limit**.

Storage

OpenShift Storage - Journey to CSI

CSI Operators & Drivers

- GCP Filestore
  - Now GA!
- Azure File CSI
  - Now supports NFS
    - Manual SC creation
    - Backport to 4.12 & 4.13
- Secret Store (TP)
  - Mount secrets to pods
  - Relies on third party providers
- LVM Storage
  - Support ext4 PVs
  - Simplify device selector logic

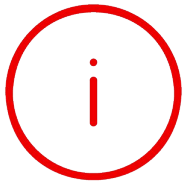
CSI Migration

- vSphere (more in next slide)
  - Enabled by default for all clusters

CSI Operators		
Operator	**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
GCP Filestore	n/a	**GA**
IBM Cloud	n/a	GA
RH-OSP Cinder	GA	GA
vSphere	**GA**	GA
SecretStore	n/a	**TP**

Red Hat

vSphere CSI migration



Status

vSphere bugs are present in <7.0u3L or <8.0u2

OCP 4.13: CSI migration was enabled for new clusters and opt-in for upgraded

OCP 4.14: CSI migration is fully supported and enabled by default in for all clusters

Strategy

Upgrades to 4.14 are prevented* if OCP is not running on vSphere 7.0u3L+ or 8.0u2+

Option to bypass and upgrade with an admin ack

vSphere 7.0u3L+ or 8.0u2+ is NOT required on new 4.14 clusters

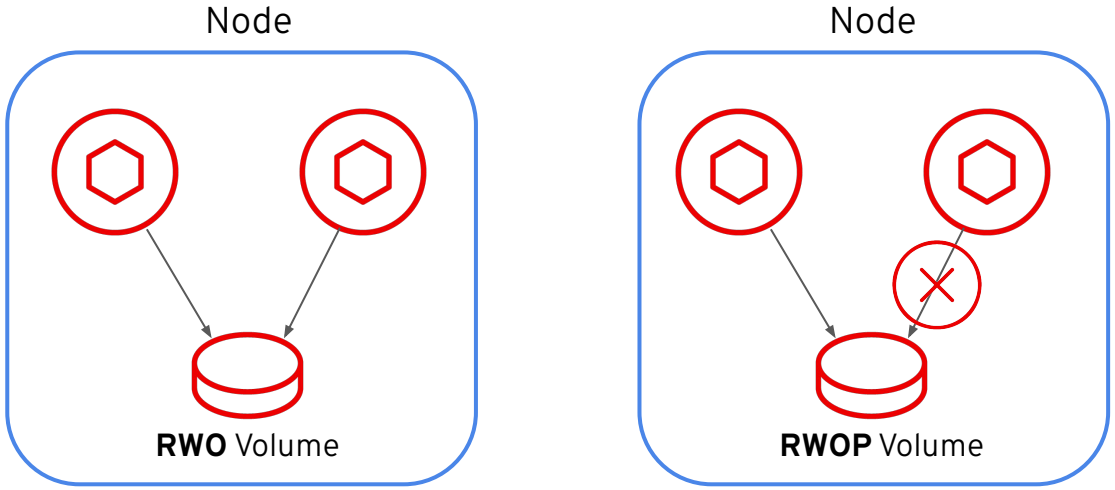
* Does not apply to clusters that already have CSI migration enabled or don't use in-tree PVs.

Red Hat

ReadWriteOncePod access mode (TP)

- New RWOP access mode
  - Ensure volume is accessed by only one pod
- Same field as the current access modes
- No driver support required

```yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: myclaim
spec:
  accessModes:
    - ReadWriteOncePod
  resources:
    requests:
      storage: 1Gi
```



OpenShift Data Foundation 4.14 updates

- Data Resiliency
  - Regional DR for block and file with ACM 2.9 (GA)
  - DR policy management enabled for ACM Application users
- NFS
  - Support export sharing across namespaces
- Network
  - IPv6 auto discovery and configuration
- Support up to 16TB disks
- Tech Preview
  - Non resilient storage class (Replica 1)

Out of the box support	
Block, File, Object, NFS	
Platforms	
AWS/Azure	Google Cloud (Tech Preview)
RHV	OSP (Tech Preview)
Bare metal/IBM Z/Power	VMWare Thin/Thick IPI/UPI
ARO - Self managed ODF (4.12)	IBM ROKS & Satellite - Managed ODF (GA)
Any platform using agnostic deployment mode	
Deployment modes	
Disconnected environment and Proxied environments	

Edge

General Availability

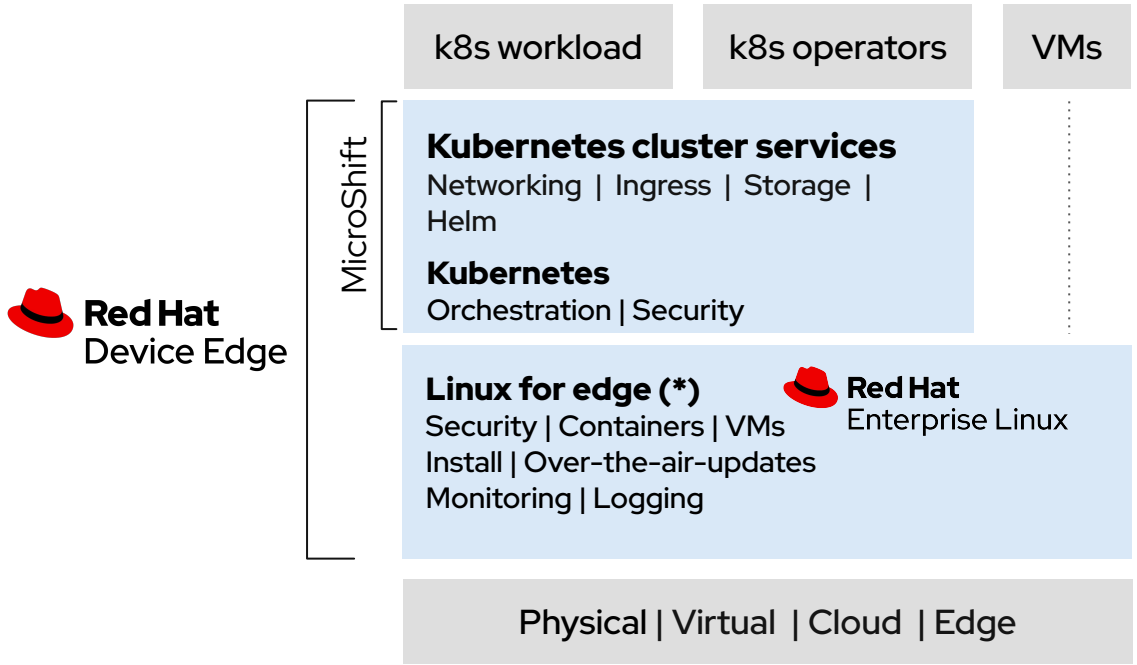
Red Hat Device Edge and MicroShift

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.

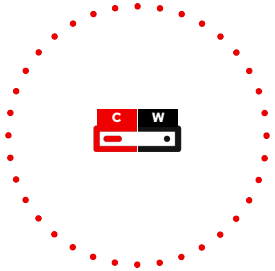
New Features:

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



Red Hat

Single Node OpenShift and LVM Storage provider



SNO added providers:

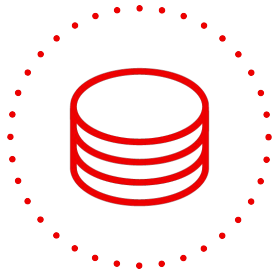
awsarm

Azure

IBM Power

IBM Z

Google Cloud



LVM Storage CSI driver enhancements:

- Support ext4 Persistent Volumes
- Simplified deviceSelector logic
- User experience enhancements

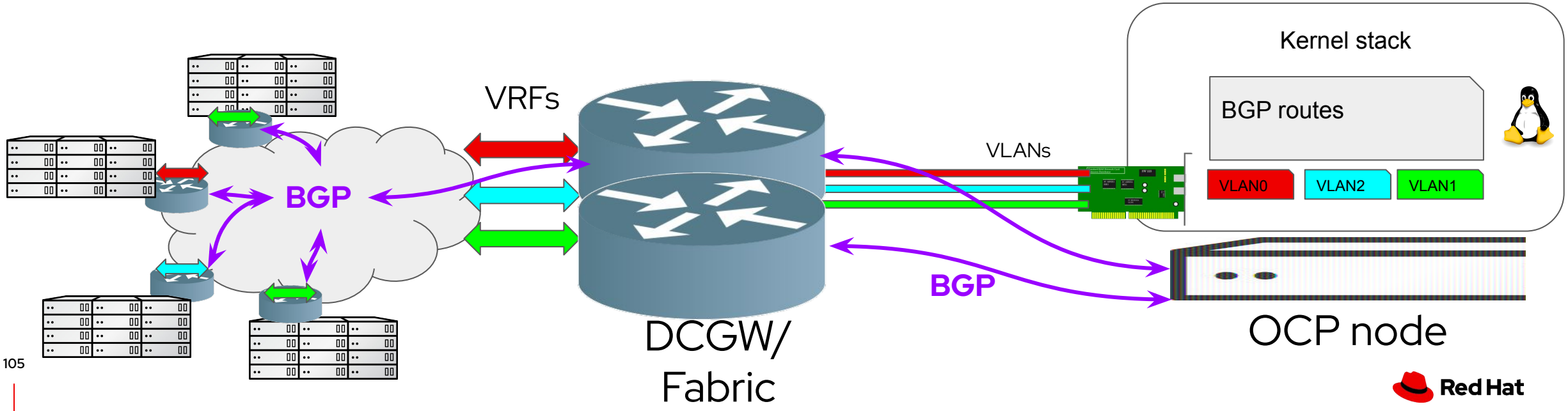
Red Hat

Telco 5G

OCP nodes route learning via BGP

When using static routes isn't effective

- OCP4.14 - Tech Preview - based on MetalLB FRR
- Depending on the route failure detection requirements, BFD may be used instead of BGP timeouts
- Active/Backup & Active/Active (ECMP)
- Technical blog post: https://cloud.redhat.com/blog/learning-kubernetes-nodes-networking-routes-via-bgp



Efficient NUMA Aware scheduling

How to use both NUMA node of your server with DPDK pods

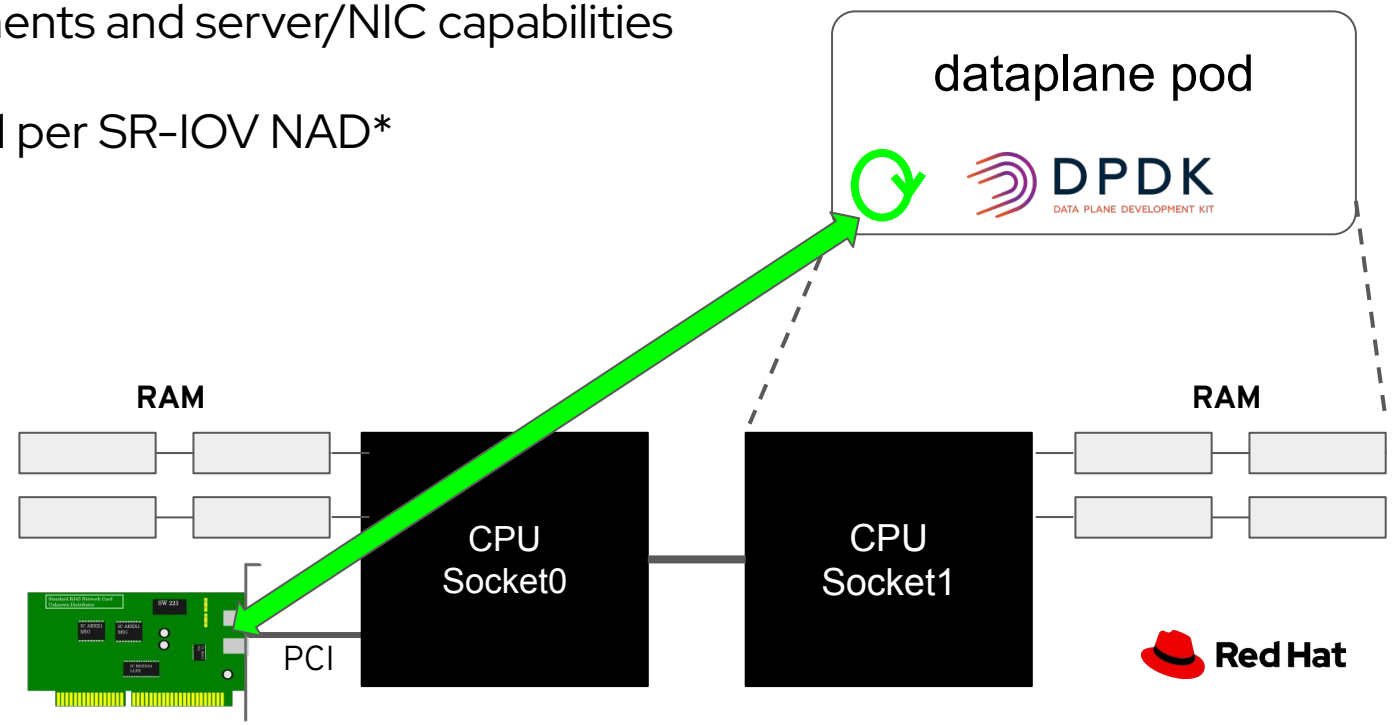
1st rule of NUMA for DPDK applications: CPUs and Memory are part of the SAME numa node.

2nd rule of NUMA: NICs should be also on the same numa node… or not!

⇒ This depends on the application requirements and server/NIC capabilities

⇒ The NUMA affinity can now be configured per SR-IOV NAD*

*NetworkAttachmentDefinition



Improved Operational Efficiency

Precache User Specified Images with TALM

What

- Reduce CNF upgrade time by pre-downloading CNF workload-images prior to initiating an upgrade
- No waiting for images to download when CNF upgrade is initiated

How

- New Custom Resource PreCachingConfig that allows the cluster operator to provide a user specified list of images and tags that will be cached on the SNO
- Use TALM to pre-cache images based on this CR to SNOs in a fleet of cluster

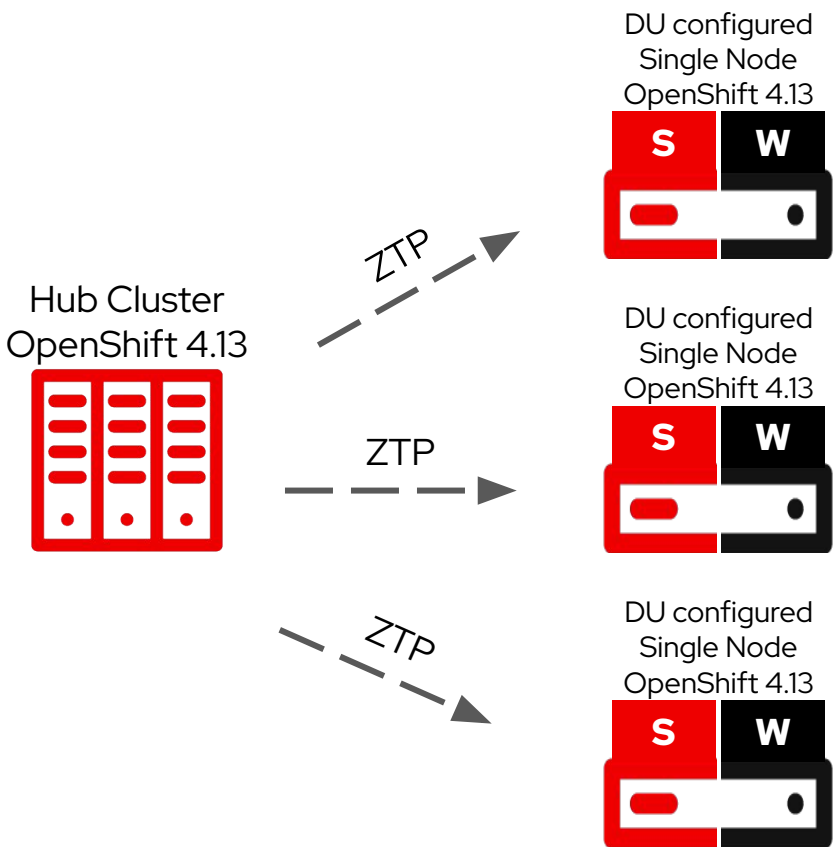
Limitations

- SNO only

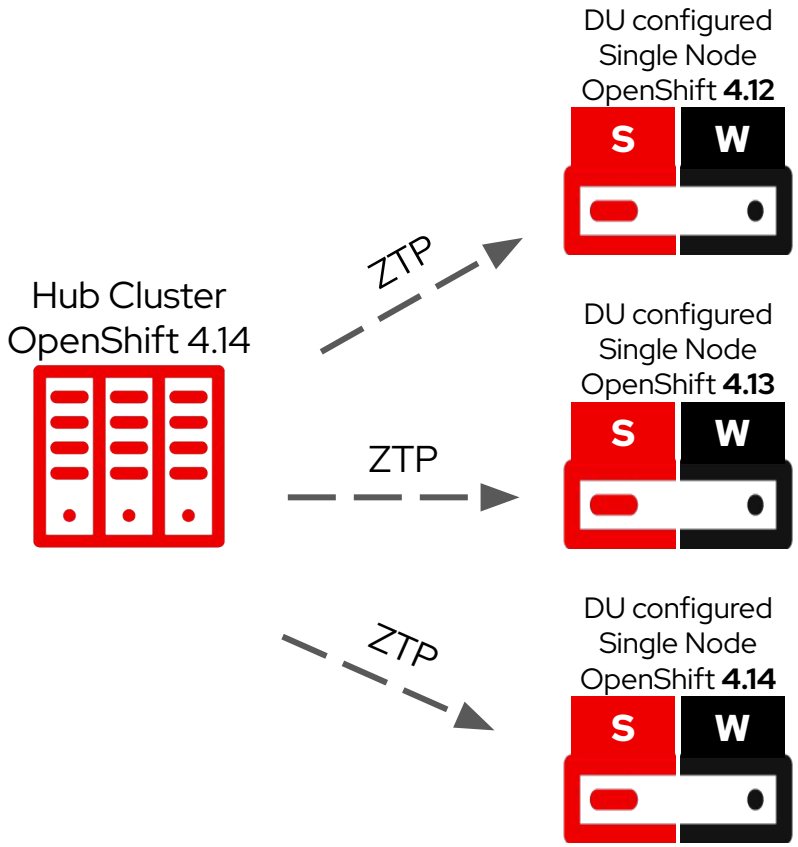
```
apiVersion: ran.openshift.io/v1alpha1
kind: PreCachingConfig
metadata:
  name: nginx-precache-config
  namespace: config-ns
spec:
  additionalImages:
    - quay.io/nginx/nginx-ingress:latest
```

Version Independence with DU GitOps Plugin

OpenShift 4.13 (and older releases)



OpenShift 4.14 (and later releases)



Git Repository

```
policies/
├── kustomization.yaml
├── version_4.12
│   ├── common.yaml
│   ├── group-du-sno.yaml
│   ├── source-crs/
│   └── kustomization.yaml
└── version_4.13
    ├── common.yaml
    ├── group-du-sno.yaml
    ├── source-crs/
    └── kustomization.yaml
```

Telco Support for 4th Gen Intel® Xeon® Scalable Processors with Intel® vRAN Boost

Intel's 4th Generation Xeon Scalable Processors, SP, formerly known as Sapphire Rapids, has been certified with Red Hat Enterprise Linux 8 and 9 and they are fully supported by Red Hat. Furthermore, Red Hat has validated this platform for RAN vDU workloads using Intel vRAN Boost for FEC offloading.

Not only does this platform bring increased computing performance, but the Sapphire Rapids Edge Enhanced (SPR-EE) SKU moves FEC acceleration (vRAN Boost) on-die and removes the need for a discrete accelerator card, like ACC100.

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