



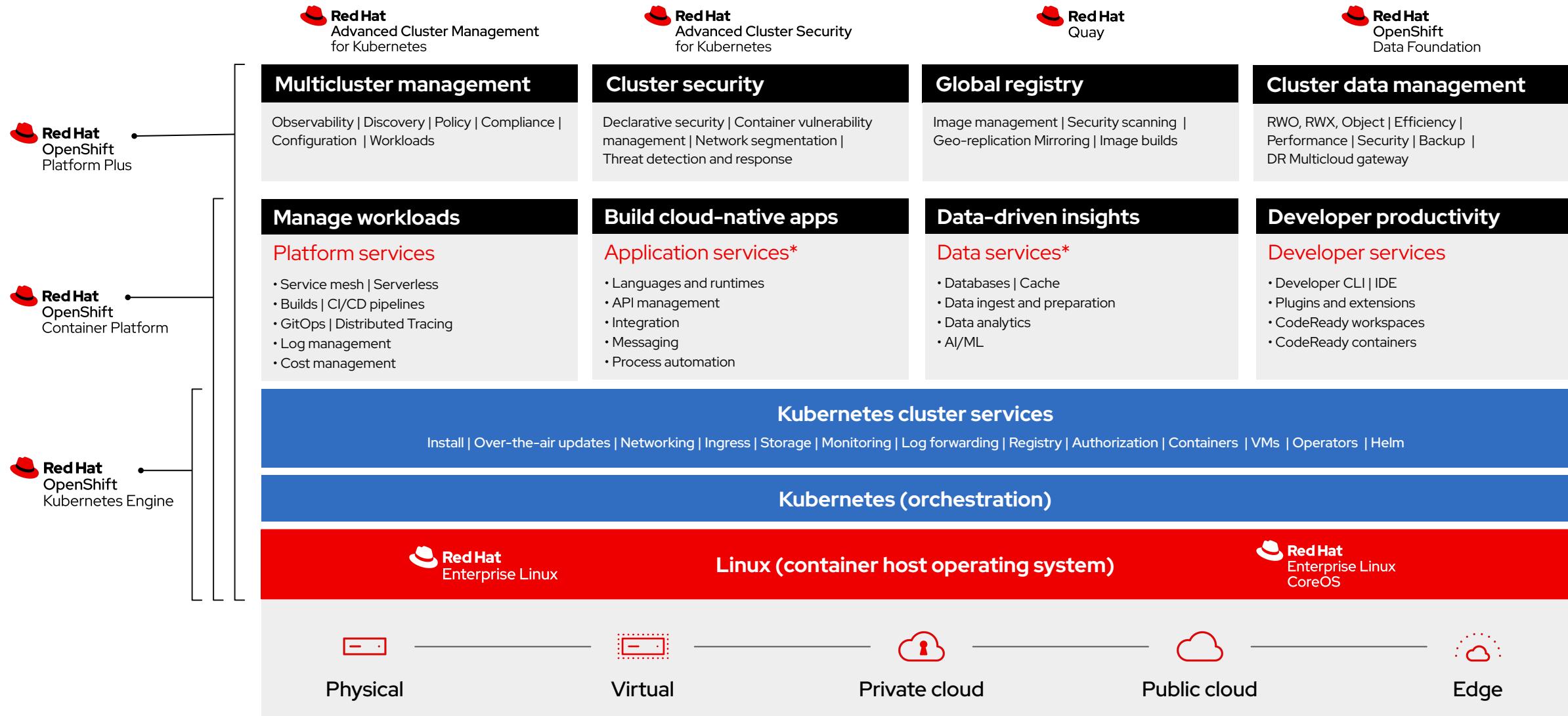
What's New in OpenShift 4.11

OpenShift Product Management

Table of Contents

- [4.11 Overview](#)
- [Spotlight Features](#)
 - [Cloud Marketplaces](#)
 - [Disconnected Mirroring](#)
 - [Nutanix](#)
 - [FedRAMP High](#)
 - [External DNS](#)
 - [VPA & Custom Metric Autoscaler](#)
- [Console](#)
- [Developer Experience](#)
- [Runtimes](#)
- [Platform Services](#)
- [Installer Flexibility](#)
- [Control Plane Updates](#)
- [Management & Security](#)
 - [Advanced Cluster Security](#)
 - [Advanced Cluster Management](#)
- [Observability](#)
 - [Monitoring](#)
- [Logging](#)
- [Networking & Routing](#)
- [Virtualization](#)
- [Specialized Workloads](#)
- [Operator Framework](#)
- [Quay](#)
- [Storage](#)
- [Telco 5G and Edge Computing](#)

Red Hat open hybrid cloud platform



OpenShift Roadmap

Near Term

(Q3 2022)

HOSTED	
DEV	<ul style="list-style-type: none">• Private Preview of App Studio, a hosted dev exp• OpenShift Dev CLI (odo onboarding & more)• GitOps: ApplicationSets GA, Notifications, P/Z• Pipelines: ARM, pipelines-as-code (GA)
APP	<ul style="list-style-type: none">• mTLS natively in Serverless (TP)• Serverless: Knative Kafka Broker and Sink (GA)• Operator SDK for Java/Quarkus (TP)• Custom Metric Autoscaler (KEDA)• OLM operator update retries
PLATFORM	<ul style="list-style-type: none">• Nutanix AOS IPI (GA)• AWS SC2S secret region• Agent-based Installer Dev Preview• Hosted Assisted Installer – vSphere support (GA)• Composable OpenShift• Hosted Control Planes for AWS in ACM/MCE (TP)• External DNS Operator• Additional capabilities for Windows containers (containerd, Windows Server 2022)• NetFlow/sFlow/IPFIX Collector• Introduce Gateway API• Disconnected mirroring simplification (GA)• Improve audit logging, API Server alerting• Pod Security Admission Integration
HOSTED	<ul style="list-style-type: none">• ROSA/OSD/ARO: GPU Support• ROSA/OSD: ISO27017+ISO27018• ROSA/OSD: instance types: metal, 6th-gens, AMDs• ROSA: New UI for Cluster Provisioning• ARO: Upgrades through cluster manager• Cost management understands IBM Cloud IaaS

Mid Term

(Q4 2022)

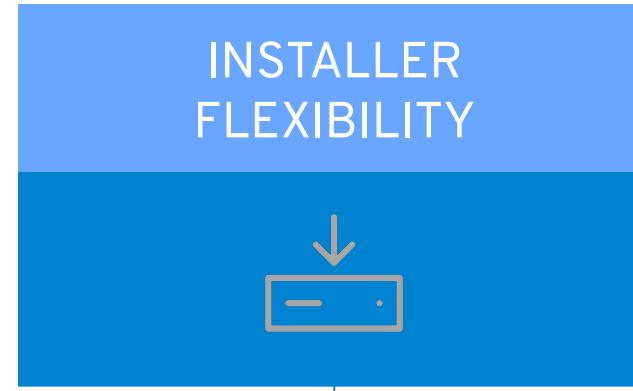
HOSTED	
DEV	<ul style="list-style-type: none">• Shared Resource CSI Driver (GA)• Image build cache• Pipelines: pipeline/task resolvers, extended retention• GitOps: namespace tenancy, Helm improvements
APP	<ul style="list-style-type: none">• File-based Operator catalog management• Operator SDK for optimized cache usage• OpenShift Serverless Functions (GA)• Dynamic Plugins (GA)• IBM Cloud IPI (GA) & IBM PowerVS IPI (GA)• AWS Local Zones• Custom tags on AWS, GCP and Azure• Agent-based Installer (GA)• Hosted Assisted Installer – Nutanix support (GA)• KMMS manages third party special devices (GA)• Enable user namespaces• Windows Containers (Health Mgmt, GCP support)• vSphere multi-cluster, multi-datacenter support (TP)• Gateway API / Ingress Controller support• Network Topology and Analysis Tooling• SmartNIC Integrations, eBPF Support• Network Policy v2 & OVN no-overlay option• BGP Advertised Services (FRR)• SigStore style image signature verification• Utilize cgroups v2 (TP); Crun in Openshift (TP)• Hosted Control Planes TP for Agent in ACM & MCE• KREW plugin manager (TP)• Cost mgmt integration to Subs Watch, ACM• ROSA/OSD: Dedicated instances + instance types• ROSA/OSD: Terraform provider• ROSA/OSD: FedRAMP High on AWS GovCloud
HOSTED	

Long Term

(H1 2023+)

HOSTED	
DEV	<ul style="list-style-type: none">• GitOps: ARM, progressive delivery, patching• Pipelines: pipelinerun artifacts, manual approval• Red Hat Tekton Hub• Multi Tenancy for Serverless• Integration of Knative (Serverless) with KEDA• mTLS natively in Serverless (GA)• Serverless Logic (TP)• OLM cluster-wide operators• OLM granular permission management• Unified Console (GA)• Alibaba Cloud IPI (GA)• Azure China• AWS Outposts• IPI for GCP shared VPC (XPN)• More cloud providers for OpenShift on ARM• Multi-Arch Hosted Control Planes (Hypershift)• Hosted Control Planes in ACM/MCE (GA)• Heterogeneous Cluster support• vSphere multi-cluster, multi-datacenter support (GA)• vSphere 8 support• CoreOS Layering for Package Management• Utilize cgroups v2 (GA); Crun in Openshift (GA)• Service Mesh IPv6 support• Integration with external KMS• GA cert-manager• KREW plugin manager (GA)• ROSA/OSD: HIPAA• OSD: AWS STS support• ROSA/OSD: Support OVN as default• ROSA/OSD: Wavelength
HOSTED	

OpenShift 4.11



Purchase OpenShift from cloud marketplaces
Nutanix AOS (IPI) is GA
Agent-based Installer is Dev Preview
Hosted Control Planes (HyperShift) is TP
External DNS Operator
Composable OpenShift



FedRAMP High for
Compliance Operator
Disconnected Mirroring Workflow
Automatic upgrades for failed
operator installations



NVIDIA AI Enterprise with OpenShift now
supported on public clouds
Windows Server 2022 workers for WinC
Custom Metric Pod Autoscaler (KEDA)

Kubernetes 1.24

Major Themes and Features

- ▶ gRPC startup, liveness and readiness probes have graduated to beta
- ▶ Container Storage Interface (CSI) Volume Expansion and Storage capacity tracking interfaces have graduated to stable (require driver implementation)
- ▶ Azure Disk and OpenStack Cinder in-tree to CSI plugin migration is complete (transparent change)
- ▶ Mixed protocol support in Services with “type: Loadbalancer” (Beta)

Significant list of other graduations to stable:

- ▶ Pod overhead accounting
- ▶ Efficient watch resumption
- ▶ Suspend field for Jobs API
- ▶ CertificateSigningRequest API certificate duration
- ▶ And more...!



Notable Top RFE's and Components

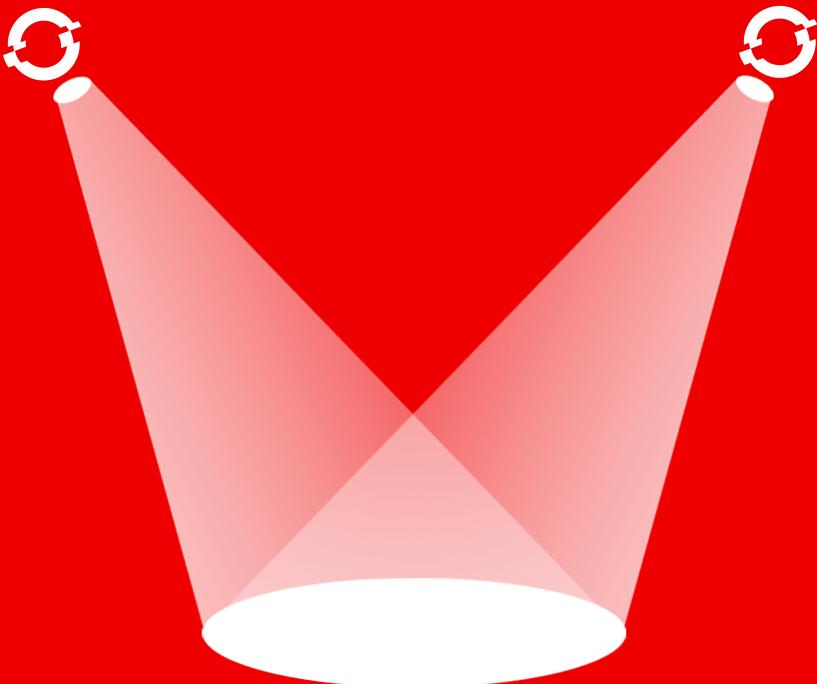
Top Requests for Enhancement (RFEs)

- ▶ Expose ROUTER_MAX_CONNECTIONS to be configurable
 - ▶ Expose and make configurable ROUTER_BACKEND_CHECK_INTERVAL in HAProxy's template to customize the length of time between subsequent liveness checks on backends.
- ▶ Set default subdomain for routes at Project/Namespace level
 - ▶ Customers typically use router sharding for one particular namespace/project, and would like to have all the routes in a shard default to a different default subdomain to the rest of the cluster/routers.
- ▶ Kerberos support on CoreOS nodes
 - ▶ Kerberos packages are now part of the RHEL CoreOS extensions functionality
- ▶ Expose port configuration to the ingress operator
 - ▶ Customers have the ability to run multiple 'routers' on the same node on different ports.

43 RFEs

shipped in
OpenShift 4.11
for customers

OpenShift 4.11 Spotlight Features



AWS / Azure / GCP Marketplaces

Pay for OpenShift with your Cloud Provider Budget

- ▶ Self-managed OpenShift, paid hourly or upfront right from AWS and Azure Marketplace through your cloud provider billing / committed spend
- ▶ Azure availability in North America, Azure Government (MAG) and EMEA
- ▶ AWS available in North America and GovCloud; EMEA availability by end of August
- ▶ GCP (global availability) coming towards end of Q3 2022
- ▶ Billing based on Marketplace VM images

The screenshot shows the Microsoft Azure Marketplace interface. At the top, there's a search bar labeled "Search Marketplace". Below it, a filter section allows users to "Browse apps" and refine results using various criteria: Trials (All), Operating System (All), Publisher (All), Pricing Model (All), and Product Type (All). The main content area displays a grid of marketplace items. On the left, a sidebar lists categories such as Analytics, AI + Machine Learning, Azure Active Directory, Blockchain, Compute, Containers, Databases, Developer Tools, DevOps, and Identity. The main grid shows several Red Hat offerings:

- Red Hat OpenShift Kubernetes Engine...** By Red Hat Inc. Starting from \$0.07/hr or from \$500.00/yr.
- Red Hat® OpenShift® Container Platform** By Red Hat Inc. Starting from \$0.30/hr or from \$2,000.00/yr.
- Red Hat OpenShift Kubernetes Engine...** By Red Hat Limited. Starting at €0.028/user/hour.
- Red Hat® OpenShift® Container Platform** By Red Hat Limited. Starting at €0.105/user/hour.
- IBM WebSphere Liberty and Open Liberty on...** By IBM WebSphere. Provisioning IBM WebSphere Liberty and Open Liberty on Azure Red Hat OpenShift.
- Leonardo Base Platform Stack** By Leonardo. A production-ready OpenShift reference architecture on Azure.

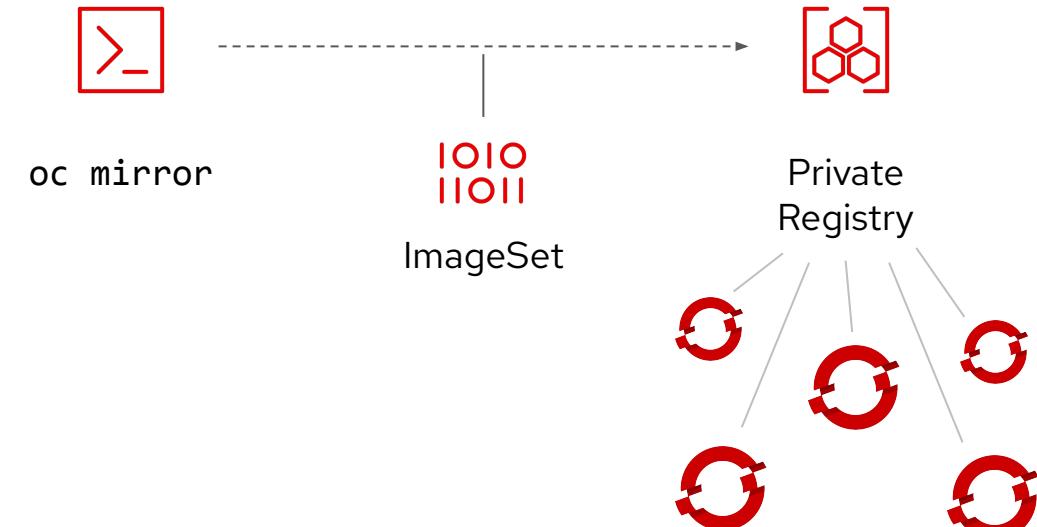
At the bottom of the grid, there are buttons for "Get it now" and "Contact me".



Disconnected Mirroring Workflow

General availability of `oc mirror`

- ▶ A single command to manage OpenShift content in disconnected environments
- ▶ **Automated:** detects new releases or desired OCP and operator versions when run at regular intervals
- ▶ **Smart:** downloads content incrementally and resolves dependencies
- ▶ **Declarative:** file-based configuration with granular filtering
- ▶ **New in 4.11:**
 - Min / max version ranges of OCP and Operators
 - Auto-pruning of images outside the min/max range in the target registry
 - Output image list instead of mirroring for external tools
 - Integration into OpenShift Update Service



Deploy OpenShift on Nutanix AOS



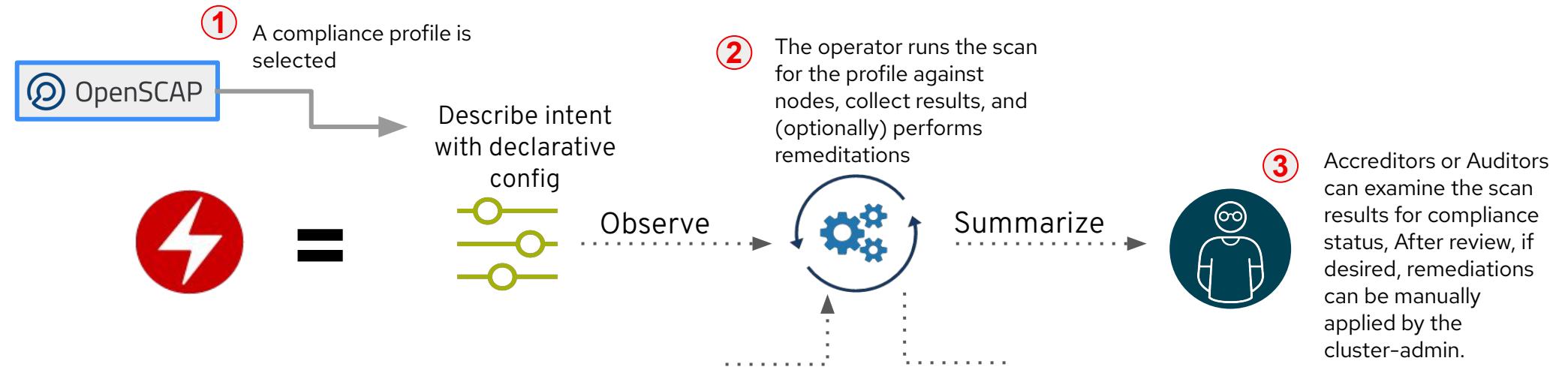
Installing a cluster using installer-provisioned infrastructure (IPI) on Nutanix AOS

- ▶ Allows an OpenShift cluster to be deployed using **installer-provisioned infrastructure** on Nutanix AOS
- ▶ Support for Long Term Support (LTS) and Short Term Support (STS) Nutanix AOS Releases
- ▶ Credentials integration support for “Manual” mode and CSI integration on day-2

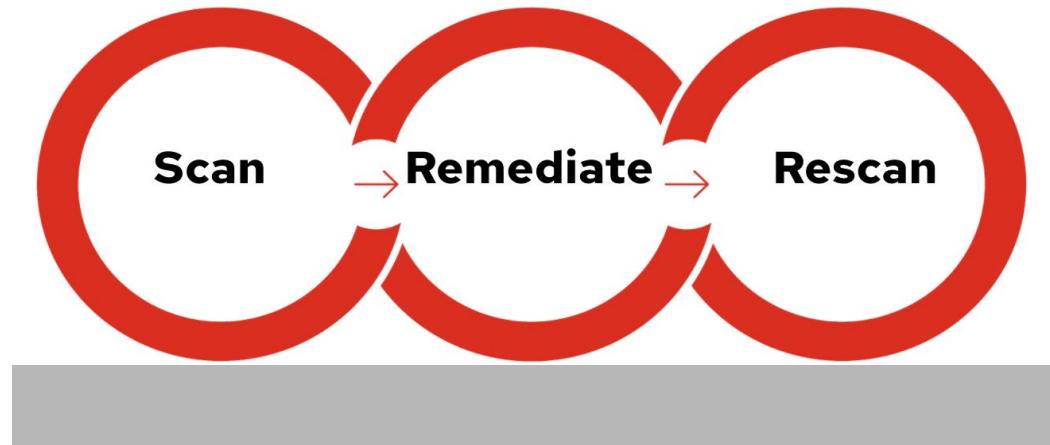
```
...
...
platform:
  nutanix:
    apiVIP: XX.XX.XX.XX
    ingressVIP: XX.XX.XX.XX
    prismCentral:
      endpoint:
        address: your.prismcentral.domainname
        port: 9440
      password: XXXXXXXXXXXXXXXX
      username: sampleadmin
    prismElements:
      - endpoint:
          address: your.prismelement.domainname
          port: 9440
          uuid: xxxxxx-xxx-xxxx-xxx-xxxxxxxx
        subnetUUIDs:
          - xxxx-xxxx-xxxx-xxxx-xxxxxx
  credentialsMode: Manual
  publish: External
  pullSecret: '{"auths": ...}'
  fips: false
  sshKey: ssh-ed25519 AAAA...
```

FedRAMP High for Compliance Operator

Customers is now able to Scan, Report and Remediate Compliance issues using the New FedRAMP High Profile

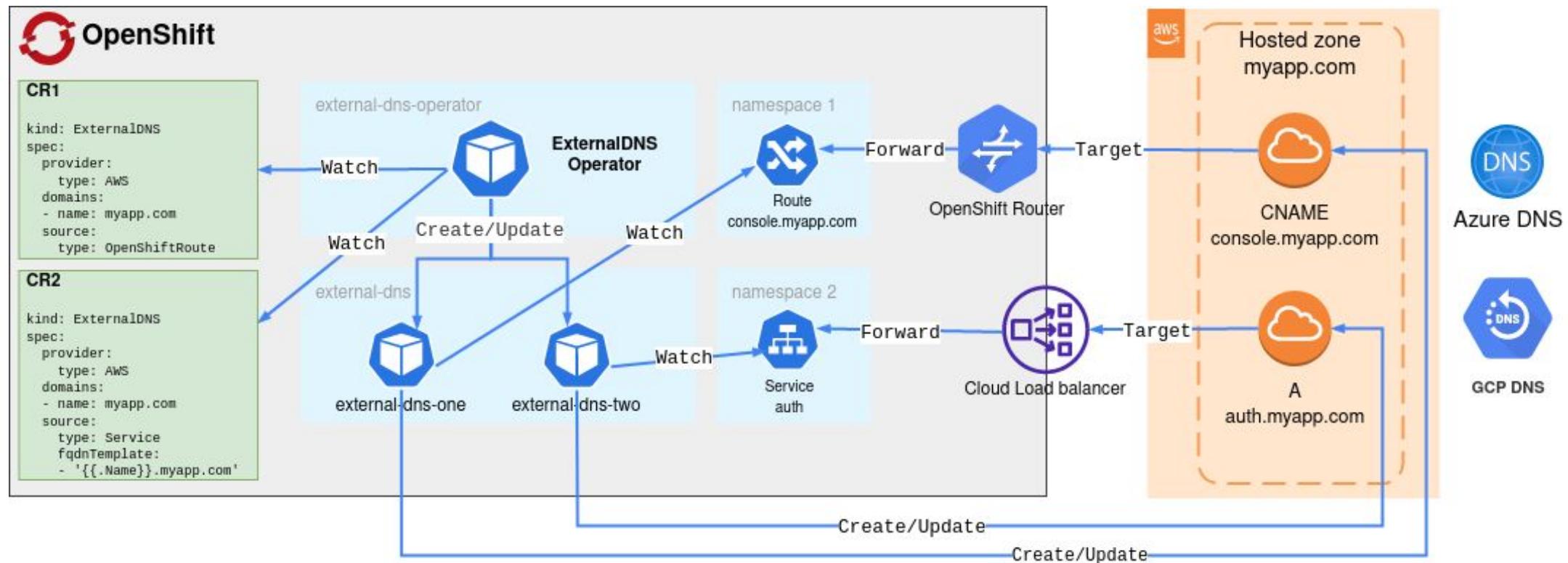


PM: Doron Caspin



External DNS Operator

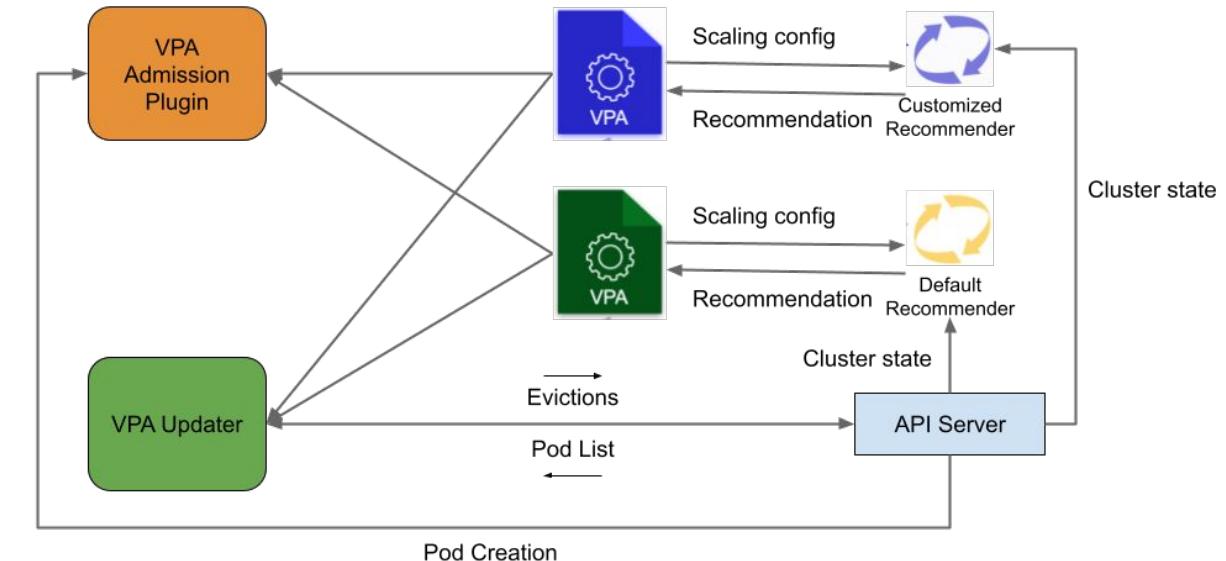
- Dynamic control of an external DNS server's records via Kubernetes resources (CRD) in a DNS provider-agnostic way
- Supported DNS providers include: AWS Route53, GCP Cloud DNS, Azure DNS, Infoblox
- Technical Preview support for the BlueCat DNS provider



Alternative recommender for Vertical Pod Autoscaler (VPA)

Bring your own VPA recommender in Openshift

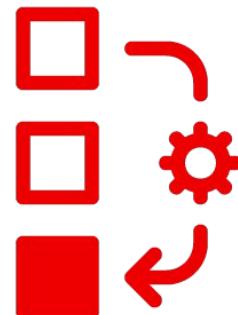
- Previously VPA recommended CPU/Mem requests and limits based on one recommender
- With 4.11, customer brings their own recommender to recommend which parameter to vertically scale pods based on their business need
- The support of a customized recommender can be implemented via a first-citizen approach. Namely, a dedicated field `recommenderName` can be added to the VPA object to indicate which recommender to use
- Example of alternative VPA recommender for reference : [predictive-vpa-recommenders](#)



Custom Metric Autoscaler (Technology Preview)

Scale workloads horizontally based on custom metrics

- Custom Metric Autoscaler is built on CNCF project [KEDA](#)
- Use Scalers example [Prometheus](#) , [Apache Kafka](#) and many [more](#) on which custom metric autoscaler can scale based on
- Manages workloads to scale to 0
- Registers itself as k8s Metric Adapter
- Provides metrics for Horizontal Pod Autoscaler (HPA) to scale on



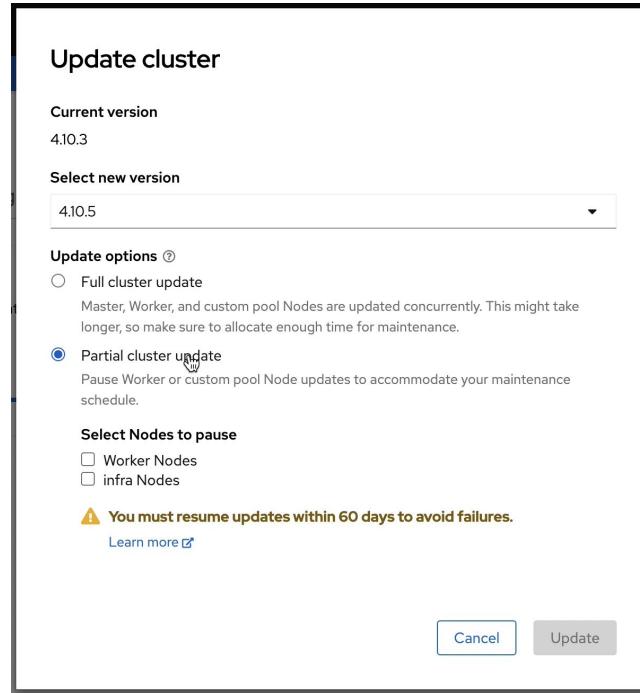
Console

Cluster Upgrade Improvements

Control Plane Upgrade

Ability to choose between a “full” cluster upgrade or “partial” control plane only upgrade in the console

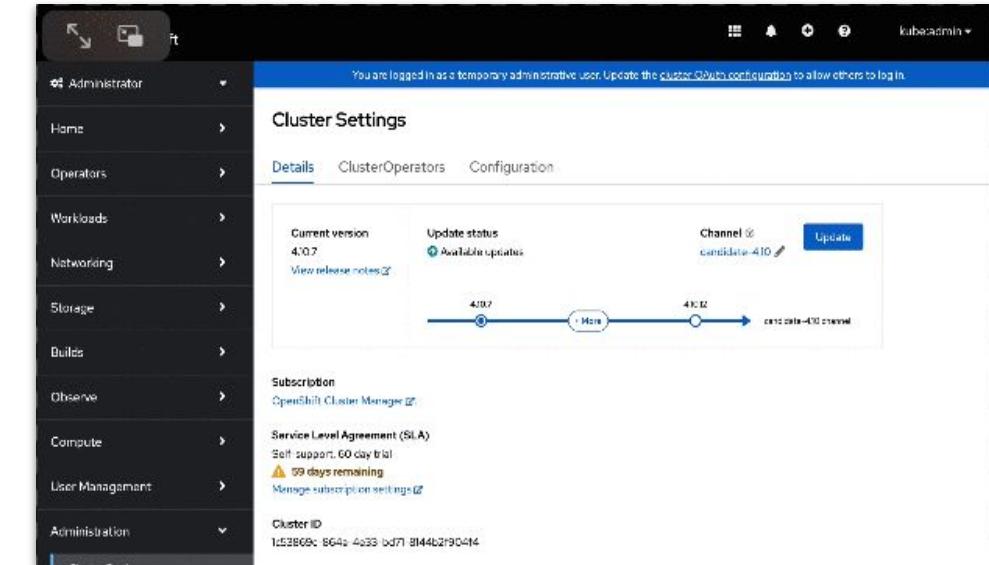
- ▶ Ability to pause upgrades per machine pool
- ▶ 60 day alert to complete upgrade



Conditional Updates

Clear communication to users about “supported but not recommended” versions

- ▶ New Supported but not recommended toggle
- ▶ Added transparency for blocked updates
- ▶ Dynamic alerts



Pod Disruption Budget

Managing Disruptions

Protect your applications from voluntary disruptions with PodDisruptionBudgets!

New UX Experience offers:

- ▶ Form creation
- ▶ List view in context of a single project or all projects
- ▶ Pods view per PDB
- ▶ All Workloads now link to associated PDB from their details page
- ▶ Create a PDB for any workload from the actions menu on the workloads details page

Name	Namespace	Selector	Availability	Allowed disruption
PDB alertmanager-main	NS openshift-monitoring	Q app.kubernetes.io/c	Max unavailable 1	1
PDB aws-ebs-csi-driver-controller-pdb	NS openshift-cluster-csi-drivers			
PDB console	NS openshift-console			
PDB csi-snapshot-controller	NS openshift-cluster-storage			

Name	Status	Ready	Restarts	Owner	Memory	CPU	Created
P alertmanager-main-0	Running	6/6	0	SS alertmanager-main	129.0 MiB	0.003 cores	Jul 15, 2022, 3:49 AM
P alertmanager-main-1	Running	6/6	0	SS alertmanager-main	116.6 MiB	0.003 cores	Jul 15, 2022, 3:48 AM

Customer Happiness

😎 Dark mode 😎 ([RFE-2716](#))

Welcome to the darkside!

- ▶ Your choice or let the system choose for you

The screenshot shows the Red Hat OpenShift web console interface. On the left is a dark sidebar menu with various navigation items like Home, Operators, Workloads, Networking, Storage, Builds, Observe, Compute, User Management, and Administration. The main area is titled 'Overview' under 'Cluster'. It features sections for 'Getting started resources', 'Build with guided documentation', and 'Explore new admin features'. A prominent 'User Preferences' dialog box is overlaid on the page. Inside the dialog, under the 'General' tab, there is a 'Theme' dropdown menu with options: 'System default', 'Light', and 'Dark'. The 'Dark' option is currently selected. At the bottom of the dialog, there are tabs for 'General', 'Language', 'Notifications', and 'Applications'.

Form Based Experiences ([RFE-1652](#), [RFE-1307](#))

YAML is ...

- ▶ Routes, Configmaps

The screenshot displays two separate views of the Red Hat OpenShift web console. The top view shows the 'ConfigMaps' page for the 'default' project, listing two entries: 'kube-root-ca.crt' and 'openshift-service-ca.crt', both created on Jul 15, 2022, at 6:39 AM. The bottom view shows the 'Routes' page for the 'serena-test-namespace' project, listing three routes: 'hello-openshift', 'hello-openshift222', and 'nodejs-ex-git', all in an 'Accepted' status. Both pages have a dark-themed header and sidebar, matching the 'User Preferences' shown in the previous screenshot.

Web Terminal

Improvements

New commands:

- ▶ `help`
 - ▶ List of pre installed CLIs including version info
- ▶ `wtoctl`
 - ▶ Customize Web Terminals in OpenShift
- ▶ `history`
 - ▶ View all previous commands per tab

plus

Multiple Tabs (8 tabs max)

The screenshot shows the Red Hat OpenShift Web Terminal interface. The left sidebar has a dark theme with white text and includes sections for Administrator, Home, Operators, Workloads, Networking, Storage, Builds, Observe, Compute, User Management, and Administration. The Home section is currently selected. The main content area is titled "Overview" under the "Cluster" tab. It features a "Getting started resources" section with links to "Set up your cluster", "Build with guided documentation", and "Explore new admin features". Below this is a "Details" section with information about the Cluster API address (https://api.jephilli-4-12-07-15-0631.devcluster.openshift.com:6443), Cluster ID (2f4c301c-0268-4c67-8df8-2ece689c926e), OpenShift Cluster Manager, Infrastructure provider (AWS), and OpenShift version (4.12.0-nightly-2022-07-07-4). To the right of the details are "Status" and "Activity" sections. The Status section shows the Cluster, Control Plane, Operators, and Dynamic Plugins status. The Activity section shows recent events like "Updated ...", "Wrote up...", and "Paused". A bottom banner at the bottom of the screen says "You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in."

Developer Experience

Developer Experience

Watch the **What's New - Developer Edition**

HIGHLIGHTS

- ▶ **Developer Perspective** in OpenShift Console
- ▶ **odo v3 beta 1** with improved dev flows
- ▶ New container tooling initiatives to expand our footprint
 - ▶ **Podman Desktop** early development
 - ▶ **Docker Desktop extension** for OpenShift
- ▶ **OpenShift Dev Spaces 3.0** (*formerly known as CodeReady Workspaces*)
- ▶ **OpenShift Local** (*formerly known as CodeReady Containers*)
- ▶ Enhanced application development and deployment around IDE experience in Visual Studio Code, IntelliJ and Eclipse Tooling
- ▶ Richer experience in VSCode Java, Quarkus and YAML tooling



DEVELOPER EDITION slides [PDF](#) | [Google Presentation](#)

Runtimes

Kube Native Java with Quarkus

Key Features & Updates

- ▶ **Java 17** support for *native* executables ([Tech Preview](#))
- ▶ **GraphQL Support**
 - ▶ Only return data that was requested -> Prevents Over-fetching
 - ▶ Combines many resources in the same request -> Prevents Under-fetching
 - ▶ Includes Quarkus Dev UI integration
 - ▶ Reactive GraphQL Support ([Tech Preview](#))
- ▶ Enhanced Search with **Hibernate Search**
 - ▶ Automatically extracts data from Hibernate ORM entities to push it to Elasticsearch/OpenSearch indexes.
 - ▶ Full text search for entities, including “sounds like”
- ▶ Intelligent service discovery and selection with **Stork**
 - ▶ Write applications with a pluggable service discovery implementation (out of the box: static, K8s, Consul)
 - ▶ App-side load balancing (round robin, random, least used, least response time, etc)

```
{
  hero {
    name
    friends {
      name
      homeWorld {
        name
        climate
      }
      species {
        name
        lifespan
        origin {
          name
        }
      }
    }
  }
}

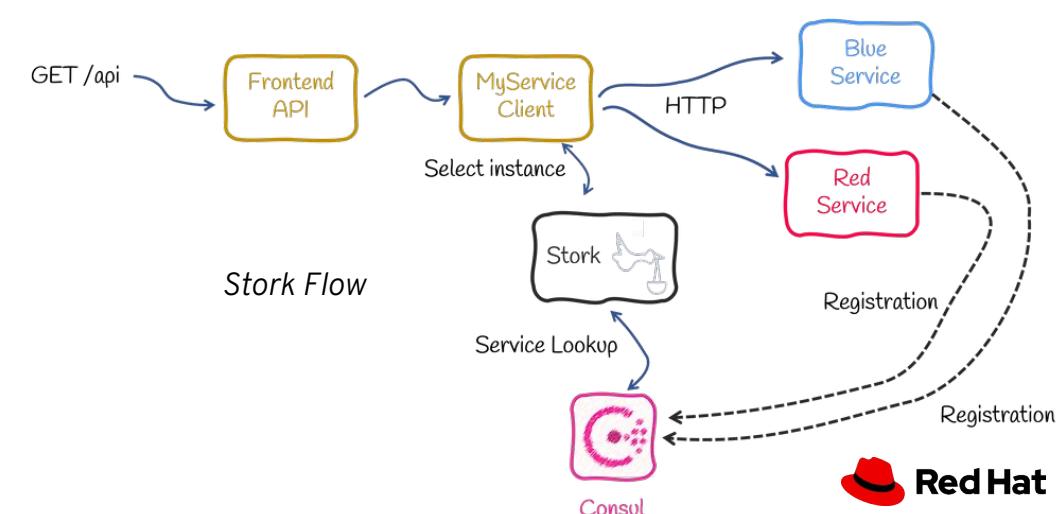
type Query {
  hero: Character!
}

type Character {
  name: String!
  friends: [Character!]!
  homeWorld: Planet!
  species: Species!
}

type Planet {
  name: String!
  climate: String!
}

type Species {
  name: String!
  lifespan: Int!
  origin: Planet!
}
```

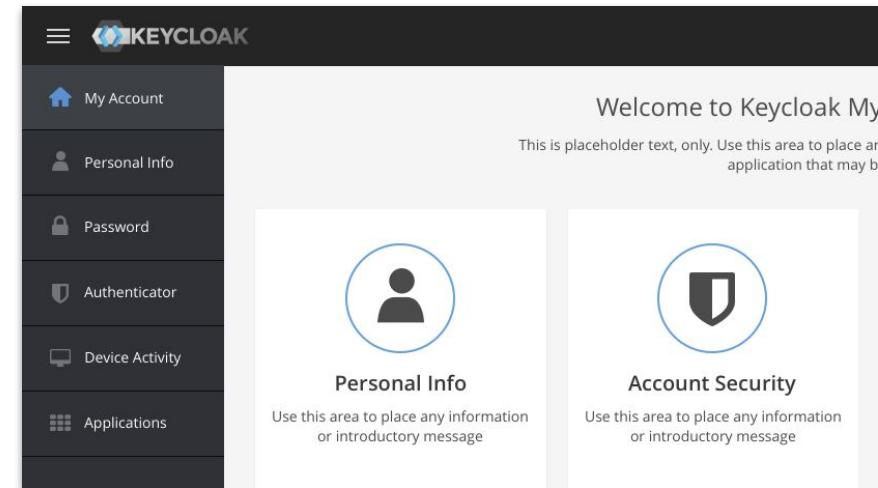
GraphQL in the Dev UI



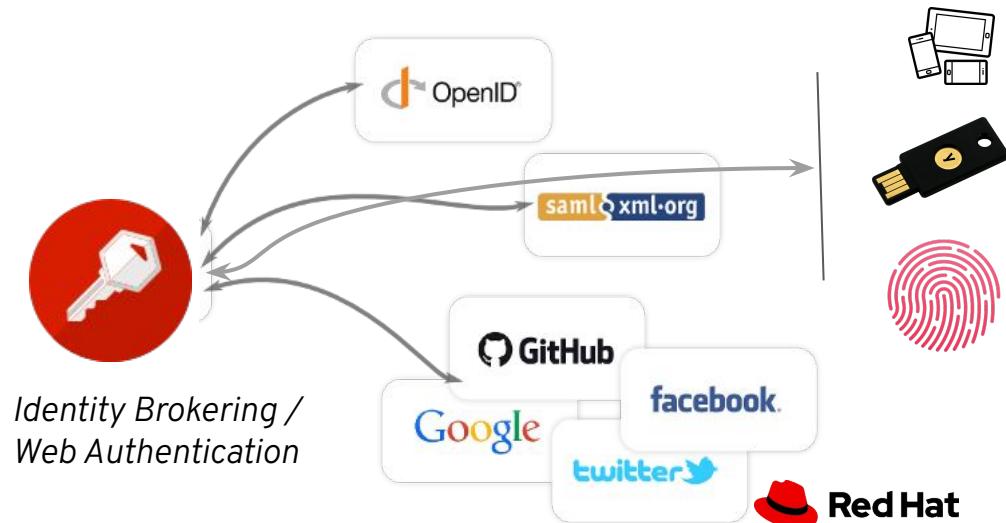
Red Hat Single Sign-On

Key Features & Updates

- ▶ Step-up Authentication
 - ▶ Allows access to clients or resources based on a specific authentication level of a user.
- ▶ Client Secret Rotation policy
 - ▶ Provides greater security to address challenges such as secret leakage (allows up to 2 active secrets/client)
- ▶ WebAuthn support is now GA
 - ▶ Passwordless authentication (biometrics, touch sensors) improves security. No replay attacks.
 - ▶ Pluggable implementations
- ▶ Configurable Session limits
- ▶ Support for RSA-OAEP with A256GCM algorithm for encryption keys.
- ▶ Federated login support for GitHub Enterprise Server
- ▶ Cross-site data replication, Token exchange, Fine-grained authorization permissions remain as **(Tech Preview)**



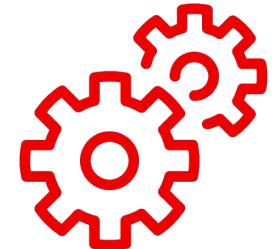
New console based on PatternFly 4 and React



Platform Services

OpenShift Builds

- ▶ Jenkins removed from OCP payload
 - ▶ moved to a new repository to decouple from the cadence of the Builds team
 - ▶ allows earlier access to fixes, CVEs, as now Jenkins is also decoupled from OpenShift versions (we now publish once, and no longer have to specifically build, test and deploy against each OpenShift version)
- ▶ Shared Resources Driver - shared secrets and configmaps
 - ▶ Utilizes volumes and CRDs to allow finer control over access to these resources
 - ▶ Allows ClusterAdmins greater flexibility in exposing sensitive information to developers and applications while maintaining “least privilege”



OpenShift Pipelines

- ▶ OpenShift Pipelines 1.8
- ▶ External database support in Tekton Hub
- ▶ Pipelines on Arm architecture (Tech Preview)
- ▶ Pipelines as code enhancements
 - ▶ Trigger multiple pipelines for Git event
 - ▶ GitLab and BitBucket support
 - ▶ CLI commands for configuring webhooks
 - ▶ Manual and third-party triggers
- ▶ Dev Console enhancements
 - ▶ Configure Git repositories with pipelines as code
 - ▶ Create GitHub App for pipelines as code

The image contains three screenshots related to OpenShift Pipelines:

- Screenshot 1:** Shows the Red Hat OpenShift Dev Console interface. A modal window titled "Add Git Repository" is open, prompting for a "Git Repo URL" (https://github.com/karthikjeeyar/demo-app) and a "Name" (git-demo-app). It also includes options to "Use GitHub App" or "Setup a webhook".
- Screenshot 2:** Shows a GitHub repository page for "siamaksade/quarkus-app". The "Code" tab is selected, displaying a green checkmark icon and the message "updated push pipeline". Below this, the "OpenShift Pipelines" section shows a "Success" status with the message "Pipelines as Code has successfully validated your commit." and a table with one row: "Status: Succeeded", "Duration: 28 seconds", and "Name: fetch-repository".
- Screenshot 3:** A close-up view of the GitHub pipeline status. It shows a list of events: "updated push pipeline" (by siamaksade, committed 33 seconds ago), "pipeline-as-code enabled" (by siamaksade, committed 5 minutes ago), and "updated" (by siamaksade, committed 8 minutes ago). A note at the top right says "Some checks haven't completed yet" with "1 in progress check". A "Details" button is visible next to the last event.

OpenShift GitOps

- ▶ OpenShift GitOps 1.6
- ▶ Provides Argo CD 2.4
- ▶ ApplicationSets (General Availability)
- ▶ Notifications (Tech Preview)
- ▶ Secret management guide
- ▶ Custom plugins in Argo CD
- ▶ Encrypted comms with Redis
- ▶ Deployment history in Dev console
- ▶ Support for running on IBM Power and Z

The screenshot shows the OpenShift Dev console interface. At the top, there are three tabs: 'LIVE MANIFEST' (which is selected), 'DIFF', and 'DESIRED MANIFEST'. Below the tabs, the 'LIVE MANIFEST' section displays the following YAML code:

```

1  apiVersion: argoproj.io/v1alpha1
2  kind: ApplicationSet
3  metadata:
4    annotations:
5      argocd.argoproj.io/sync-wave:
6        kubectl.kubernetes.io/last-applied/:
7          {"apiVersion":"argoproj.io/v1alpha1","kind":"ApplicationSet","metadata":{"name":"my-app-2","namespace":"default"}, "resourceVersion": "2022-03-31T10:45:23Z", "uid": "631f3e0c-0000-4a00-8000-000000000000"}, "creationTimestamp": "2022-03-31T10:45:23Z", "generation": 3, "labels": {"app.kubernetes.io/instance": "my-app-2", "app.kubernetes.io/name": "my-app-2", "app.kubernetes.io/version": "v1.0.0", "argocd.argoproj.io/revision": "1", "argocd.argoproj.io/sync-wave": "1"}, "resourceVersion": "2022-03-31T10:45:23Z", "uid": "631f3e0c-0000-4a00-8000-000000000000"}, "status": {"lastSynced": "2022-03-31T10:45:23Z", "operationState": {"phase": "Succeeded"}, "syncStatus": "Synced"}, "version": "v1alpha1"
8
9
10
11

```

Below the code, a success message is displayed: "Application my-app-2 has been successfully synced." with a timestamp of "Jun 23".

OpenShift Serverless

Key Features & Updates

- ▶ Update to Knative 1.3
- ▶ Support for Init Containers and PVC (**Tech Preview**)
- ▶ Serverless integration with Cost Management Service and Distributed Tracing
- ▶ Connection to externally managed Kafka Topic (**Tech Preview**)
- ▶ Developer Experience:
 - ▶ Addition of Event Sink on Dev Console
 - ▶ Serverless Dashboard for Developers perspective
- ▶ Functions (**Tech Preview**)
 - ▶ On cluster build using OpenShift Pipelines
 - ▶ Multiple build strategy support
 - ▶ IDE plugin for creating Functions on VScode and IntelliJ
- ▶ Serverless Logic (**Dev Preview**)
 - ▶ Orchestration for Functions and Services
 - ▶ CLI and Workflow Editor(UX)

The image displays two screenshots of the OpenShift Serverless interface.

Top Screenshot: Shows the "Serverless Logic Sandbox" in a browser window. It displays a workflow titled "order-saga-error-handling" with a JSON configuration file on the left and a state transition graph on the right. The graph shows nodes like "reserveStock", "processPayment", "scheduleShipping", etc., connected by arrows indicating dependencies and compensation logic.

```

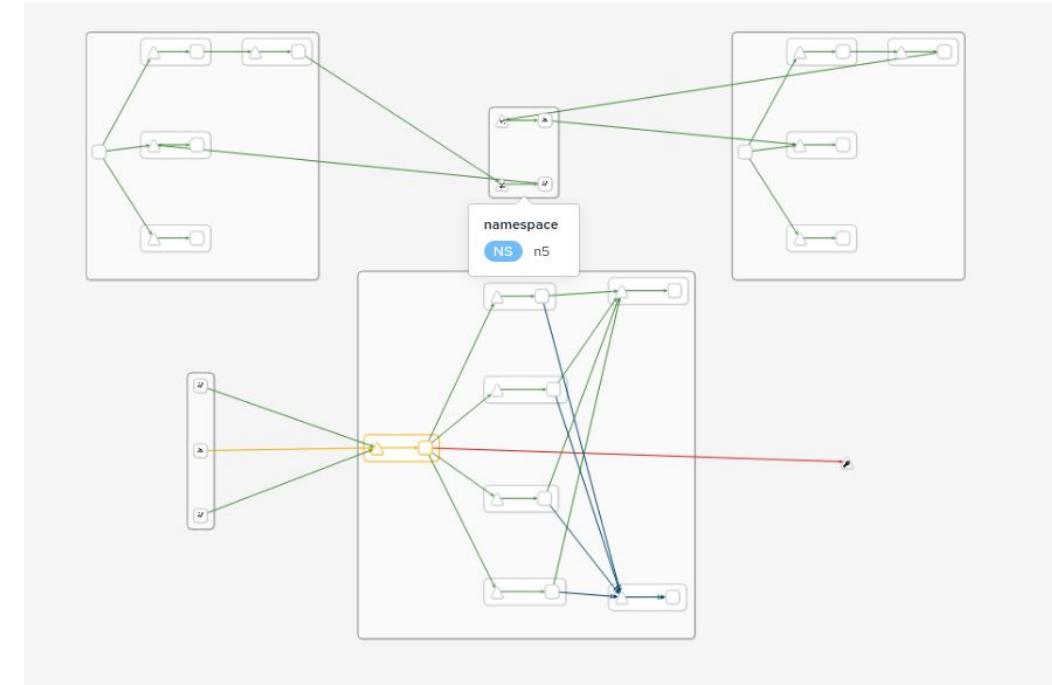
1 {
2   "id": "order_saga_error_handling",
3   "name": "Order Fulfillment Workflow Saga example",
4   "description": "An example of how to implement Saga for the Order Fulfillment example using Error Handling"
5   "steps": [
6     {
7       "name": "reserve stock failed",
8       "code": "org.kie.kogito.ServiceException"
9     },
10    {
11      "name": "process payment failed",
12      "code": "org.kie.kogito.ServiceException"
13    },
14    {
15      "name": "shipping failed",
16      "code": "org.kie.kogito.ServiceException"
17    }
18  ],
19  "start": "reserveStock",
20  "add function...": [
21    {
22      "name": "reserveStock",
23      "type": "custom",
24      "operation": "serviceorg.kie.kogito.StockService::reserveStock"
25    },
26    {
27      "name": "cancelStock",
28      "type": "custom",
29      "operation": "serviceorg.kie.kogito.StockService::cancelStock"
30    },
31    {
32      "name": "processPayment",
33      "type": "custom",
34      "operation": "serviceorg.kie.kogito.PaymentService::processPayment"
35    },
36    {
37      "name": "cancelPayment",
38      "type": "custom",
39      "operation": "serviceorg.kie.kogito.PaymentService::cancelPayment"
40    },
41    {
42      "name": "scheduleShipping",
43      "type": "custom",
44      "operation": "serviceorg.kie.kogito.ShippingService::scheduleShipping"
45    }
46  ]
47
  
```

Bottom Screenshot: Shows the "Developer Catalog" under the "Event Sinks" category. It lists various providers and their event sinks, such as AWS CloudWatch Metrics Sink, AWS DynamoDB Sink, AWS EC2 Sink, AWS Kinesis Firehose Sink, AWS Kinesis Sink, and AWS Lambda Sink.

Provider	Event Sinks
Apache Software Foundation (63)	AWS CloudWatch Metrics Sink AWS DynamoDB Sink AWS EC2 Sink AWS Kinesis Firehose Sink AWS Kinesis Sink AWS Lambda Sink

OpenShift Service Mesh

- ▶ OpenShift Service Mesh 2.2 is now available.
- ▶ Based on **Istio 1.12** and **Kiali 1.48**.
- ▶ Service Mesh, including federation, is now supported on Red Hat OpenShift on AWS (ROSA)
- ▶ Istio 1.12 introduces **WasmPlugin** API which deprecates the ServiceMeshExtensions API.
- ▶ **Kiali** updates in Service Mesh 2.2:
 - ▶ Improved views for larger service meshes
 - ▶ View internal certificate information
 - ▶ Set Envoy proxy log levels
- ▶ New **Istio** Tech preview features to try:
 - ▶ Kubernetes **Gateway API**
 - ▶ AuthPolicy "dry run"
 - ▶ gRPC "Proxyless" service mesh



Items to add:

- OpenShift/Arm
- AWS support for other network types (support for EFA)

Installer Flexibility

OpenShift 4.11 Supported Providers

Installation Experiences



Azure Stack Hub



Bare Metal

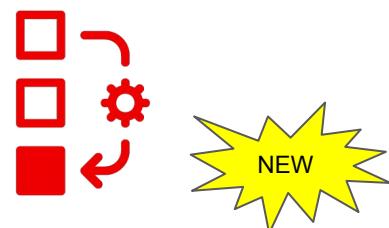
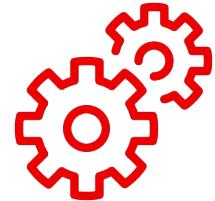
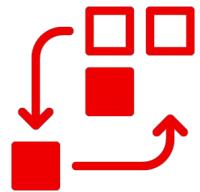


IBM Z



RED HAT[®]
OPENSTACK[®]
PLATFORM

RED HAT[®]
VIRTUALIZATION



Full Stack Automation

Installer Provisioned Infrastructure

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

Pre-existing Infrastructure

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, and vSphere only
- ISO Driven

Interactive – Disconnected

Agent-based Installer (Dev Preview)

- Disconnected bare metal deployments
- Automated installations via CLI
- ISO driven



OpenShift 4.11 Supported Providers & Installation Experiences

Provider	Full Stack Automation (installer-provisioned infrastructure)	Pre-existing Infrastructure (user-provisioned infrastructure)	Interactive – (Connected) (Assisted Installer)	Interactive – Disconnected Agent-based Installer Developer Preview
Alibaba <small>Technology Preview</small>	X			
AWS	X	X		
Azure	X	X		
Azure Stack Hub	X	X		
Bare Metal	X	X	X	X
Google Cloud Platform	X	X		
IBM Cloud <small>Technology Preview</small>	X			
IBM Power Systems		X		
IBM Z		X		
Nutanix AOS	X			
Red Hat OpenStack Platform	X	X		
Red Hat Virtualization	X	X		
VMware vSphere	X	X	X	

Azure additional features

Expand OpenShift integration on Azure public cloud with additional capabilities

- ▶ Add support for Azure ultra disks
- ▶ User-managed encryption keys
- ▶ Add support for accelerated networking

```
...
controlPlane:
...
platform:
  azure:
    ultraSSDCapability: Enabled
    osDisk:
      diskEncryptionSet:
        resourceGroup: disk_encryption_set_resource_group
        name: disk_encryption_set_name
compute:
...
platform:
  azure:
    ultraSSDCapability: Enabled
    osDisk:
      diskEncryptionSet:
        resourceGroup: disk_encryption_set_resource_group
        name: disk_encryption_set_name
platform:
  azure:
    defaultMachinePlatform:
      ultraSSDCapability: Enabled
...
...
```

Generally Available

Expand Secret Regions support for AWS

Add support to the Secret Commercial Cloud Services (SC2S) Secret Region on AWS

- ▶ IPI and UPI support for the **us-isob-east-1** Secret Commercial Cloud Services (SC2S) region
- ▶ Custom RHCOS AMI and custom endpoints required as **us-iso-east-1** (C2S)
- ▶ Custom CA certificate in the *additionalTrustBundle* field to access the AWS API

```
...
platform:
  aws:
    region: us-isob-east-1
    subnets:
      - subnet-1
      - subnet-2
      - subnet-3
    amiID: ami-96c6f8f7
    serviceEndpoints:
      - name: ec2
        url: https://vpce-id.ec2.us-west-2.vpce.amazonaws.com
    hostedZone: Z3URY6TWQ91KVV
    fips: false
...
additionalTrustBundle: |
  -----BEGIN CERTIFICATE-----
  <MY_TRUSTED_CA_CERT>
  -----END CERTIFICATE-----
```

External Load Balancers with VMware vSphere IPI

Support external load balancers with VMware vSphere IPI deployments

- ▶ Configure OpenShift to use an external load balancer in place of default load balancer
- ▶ TCP over ports 6443, 443, and 80 must be available to any users of your system
- ▶ Load balance API port 6443 between control plane nodes
- ▶ Load balance application ports 443 and 80 between all compute nodes
- ▶ On your load balancer, port 22623, should not be exposed outside the cluster as it's used to serve ignition startup configurations to nodes
- ▶ Your load balancer must have access to every machine in your cluster
- ▶ External load balancing services and control plane nodes must run on same L2 network and same VLAN (when applicable)

```
...
listen my-cluster-api-6443
  bind 0.0.0.0:6443
  mode tcp
  balance roundrobin
  server my-cluster-master-2 192.0.2.2:6443 check
  server my-cluster-master-0 192.0.2.3:6443 check
  server my-cluster-master-1 192.0.2.1:6443 check
listen my-cluster-apps-443
  bind 0.0.0.0:443
  mode tcp
  balance roundrobin
  server my-cluster-worker-0 192.0.2.6:443 check
  server my-cluster-worker-1 192.0.2.5:443 check
  server my-cluster-worker-2 192.0.2.4:443 check
listen my-cluster-apps-80
  bind 0.0.0.0:80
  mode tcp
  balance roundrobin
  server my-cluster-worker-0 192.0.2.7:80 check
  server my-cluster-worker-1 192.0.2.9:80 check
  server my-cluster-worker-2 192.0.2.8:80 check
```

Sample HAProxy configuration

Bugfix for 4.10 since this was a workaround in 4.10

No Need for DHCP Server for Bootstrap Node for Bare Metal IPI

Deploy OpenShift on Bare Metal with IPI using static IP addresses for bootstrap node

- ▶ Additional `install-config` parameters to use when there is no DHCP server

Parameters	Description
bootstrapExternalStaticIP	Static IP address for the bootstrap VM. You must set this value when deploying a cluster with static IP addresses when there is no DHCP server on the baremetal network.
bootstrapExternalStaticGateway	Static IP address of the gateway for the bootstrap VM. You must set this value when deploying a cluster with static IP addresses when there is no DHCP server on the baremetal network.

Cluster Infrastructure



Providers

- Continue to provide integration with and maximum choice of cloud providers
- o-----o
- Allow MAPI to add Arm instances
- Document how to prune machines of an older age



Cluster API (Tech Preview)

- APIs and patterns to automate cluster lifecycle management for platform operators
- Will eventually supersede MAPI
- o-----o
- Set up Cluster API cloud providers
- Work on Cluster API operator



Extensions

- Access more cloud provider functionality seamlessly via OpenShift
- o-----o
- **Azure:** Ultra SSD disk support
- **AWS:** EFA support
- **AWS:** IMDSv2 and IMDSv1 configuration
- **GCP:** pd-balanced disk type support

Azure, AWS, and vSphere Enhancements



▶ Expanded integrations with Azure

- Add support for Azure ultra disks
- User-managed encryption keys
- Add support for accelerated networking



▶ Added secret region and EFA support for AWS

- Added IPI and UPI support for the **us-isob-east-1** Secret Commercial Cloud Services (SC2S) region



- Added Elastic Fabric Adapter (EFA) support

▶ External load balancers supported with VMware vSphere IPI deployments

- Use your own load balancers for external API/ingress traffic with IPI
Generally Available

Agent-based Installer for Disconnected OpenShift Deployments

- ▶ Bootable image creates first OpenShift cluster
- ▶ Fully disconnected (including air-gapped) deployments
- ▶ Uses mirrored local registry
- ▶ Leverages Assisted Service (Assisted Installer engine)
- ▶ Single node (SNO), compact clusters, and highly available topologies
- ▶ In-place bootstrap, no extra node required
- ▶ Allows user-provided automation tooling for automating installations

```
Creates OpenShift clusters

Usage:
  openshift-install [command]

Available Commands:
  agent      Commands for supporting cluster installation using agent installer
  analyze    Analyze debugging data for a given installation failure
  completion Outputs shell completions for the openshift-install command
  coreos     Commands for operating on CoreOS boot images
  create     Create part of an OpenShift cluster
  destroy    Destroy part of an OpenShift cluster
  explain    List the fields for supported InstallConfig versions
  gather     Gather debugging data for a given installation failure
  graph     Outputs the internal dependency graph for installer
  help      Help about any command
  migrate   Do a migration
  version   Print version information
  wait-for  Wait for install-time events

Flags:
      --dir string            assets directory (default ".")
      -h, --help               help for openshift-install
```

Composable OpenShift

This feature provides a mechanism for cluster installers to exclude one or more optional components (capabilities) for their installation which will determine which payload components are/are not installed in their cluster. **OpenShift 4.11 allows you to disable the installation of the baremetal operator , marketplace, and the openshift-samples content that is stored in the openshift namespace.** You can disable these features by setting the *baselineCapabilitySet* and *additionalEnabledCapabilities* parameters in the *install-config.yaml* configuration file prior to installation.

- Defining an [install config api](#) field whereby the user can opt into specific capabilities.
- The installer will validate the pass the information through to the CVO for resource management, by setting *spec.capabilities* in [ClusterVersion](#).
- The CVO will calculate an effective status:

Capabilities delivered in 4.11 (Phase 1)

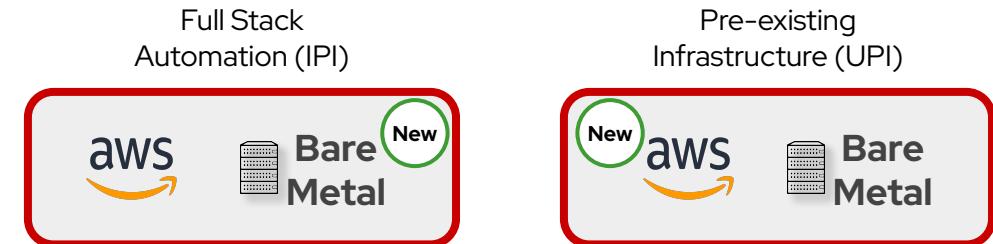
- Installer to allow users to select OpenShift components to be included/excluded
- Provide a way with CVO to allow disabling and enabling of operators
- Make oc aware of cluster capabilities
- Make the marketplace operator, samples operator, cluster baremetal operator optional

```
capabilities:
  baselineCapabilitySet: None
  additionalEnabledCapabilities:
    - openshift-samples
```

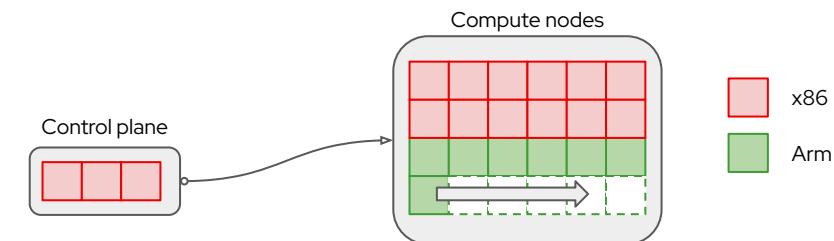
```
status:
  capabilities:
    enabledCapabilities:
      - openshift-samples
    knownCapabilities:
      - baremetal
      - marketplace
      - openshift-samples
```

Arm and Heterogeneous

- We are adding more platform support
 - AWS Pre-existing Infrastructure(UPI)
 - Bare Metal Full Stack Automation (IPI)
- Disconnected install now supported for those security conscious users
- Plugging the storage gaps
 - Local Storage Operator
 - iSCSI
 - Raw Block
 - MultiPath
 - HostPath
- Heterogeneous clusters (Tech Preview)
 - Very limited tech preview with limited use case
 - Add Arm compute nodes to an x86 cluster as a day 2 operation
 - Only works on Azure at this time
 - Source your payload from the nightlies



Add in different architecture nodes as a day 2 operation (Azure only for now)



RHEL CoreOS & Machine Config Operator

What's new in RHCOS 4.11

- ▶ MCO now updates nodes by **zone** and **age**
- ▶ Based on **RHEL 8.6 content** streams
- ▶ **Kdump** on AMD64 (x86_64) to Full GA support
- ▶ **Kerberos** packages (libkrb5, krb5workstation)
added to CoreOS extensions
- ▶ **nvme-cli** added to RHCOS base package set

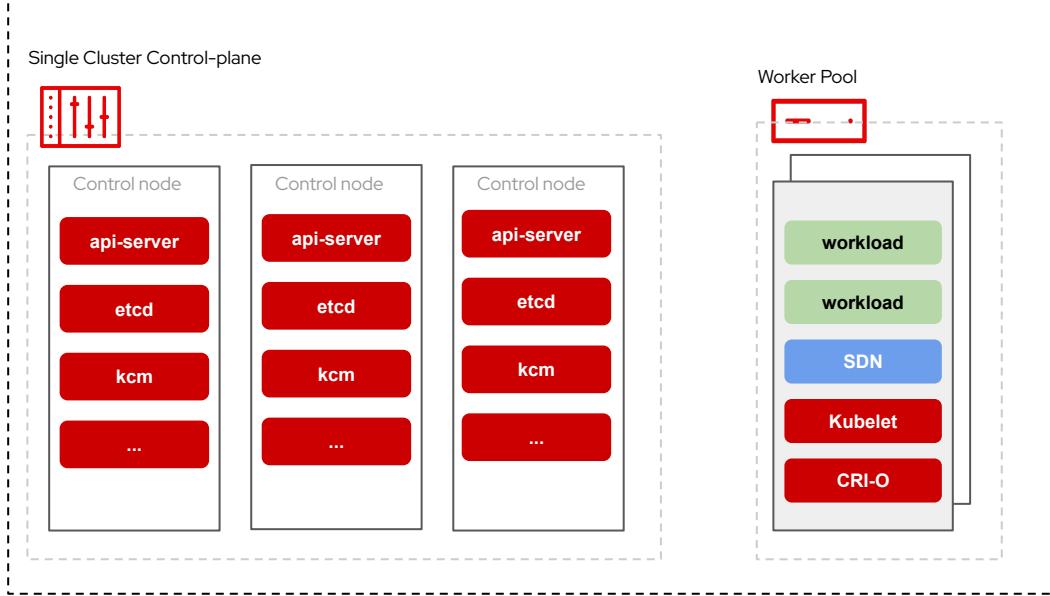
Control Plane Updates

What is Hosted Control Planes (Tech Preview)?

Standalone OpenShift

Control-Plane (CP) + Workers

Standalone OpenShift **Cluster** (dedicated CP nodes)



Lower your CAPEX and OPEX costs
(bundling of CPs + CP as pods)



Centrally Manage your CPs
(easy operation & maintenance)



Get Flexibility with Multi-arch support
(e.g. CP x86, workers ARM)



Enforce Network & Trust
segmentation



Save time Fast cluster bootstrapping
(CP as Pods)



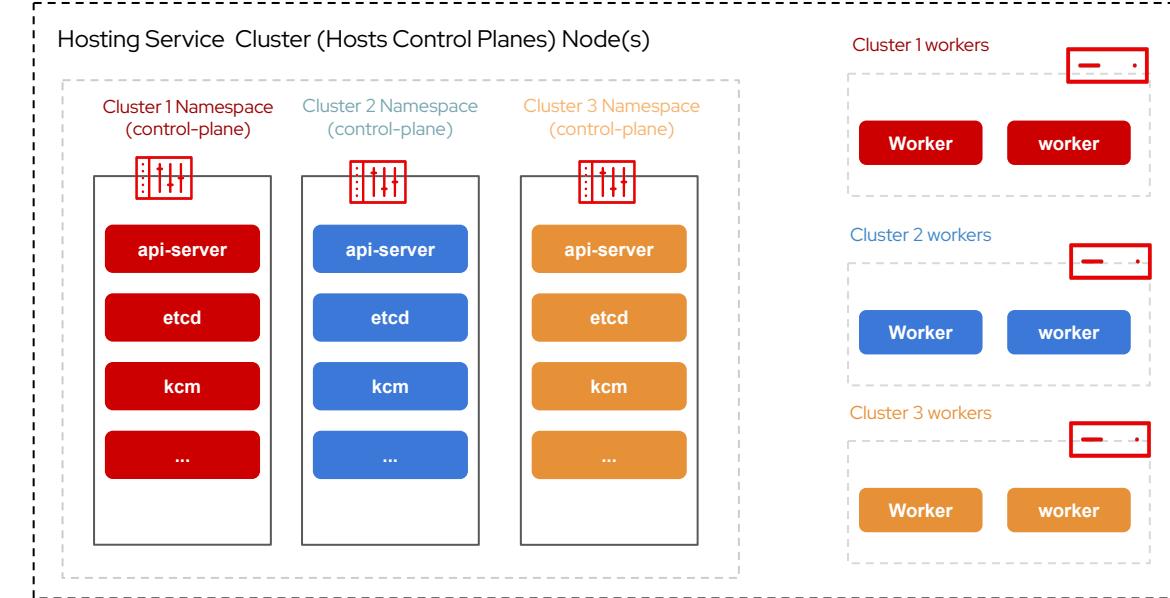
Hosted control planes for OpenShift

Control-Plane (CP)

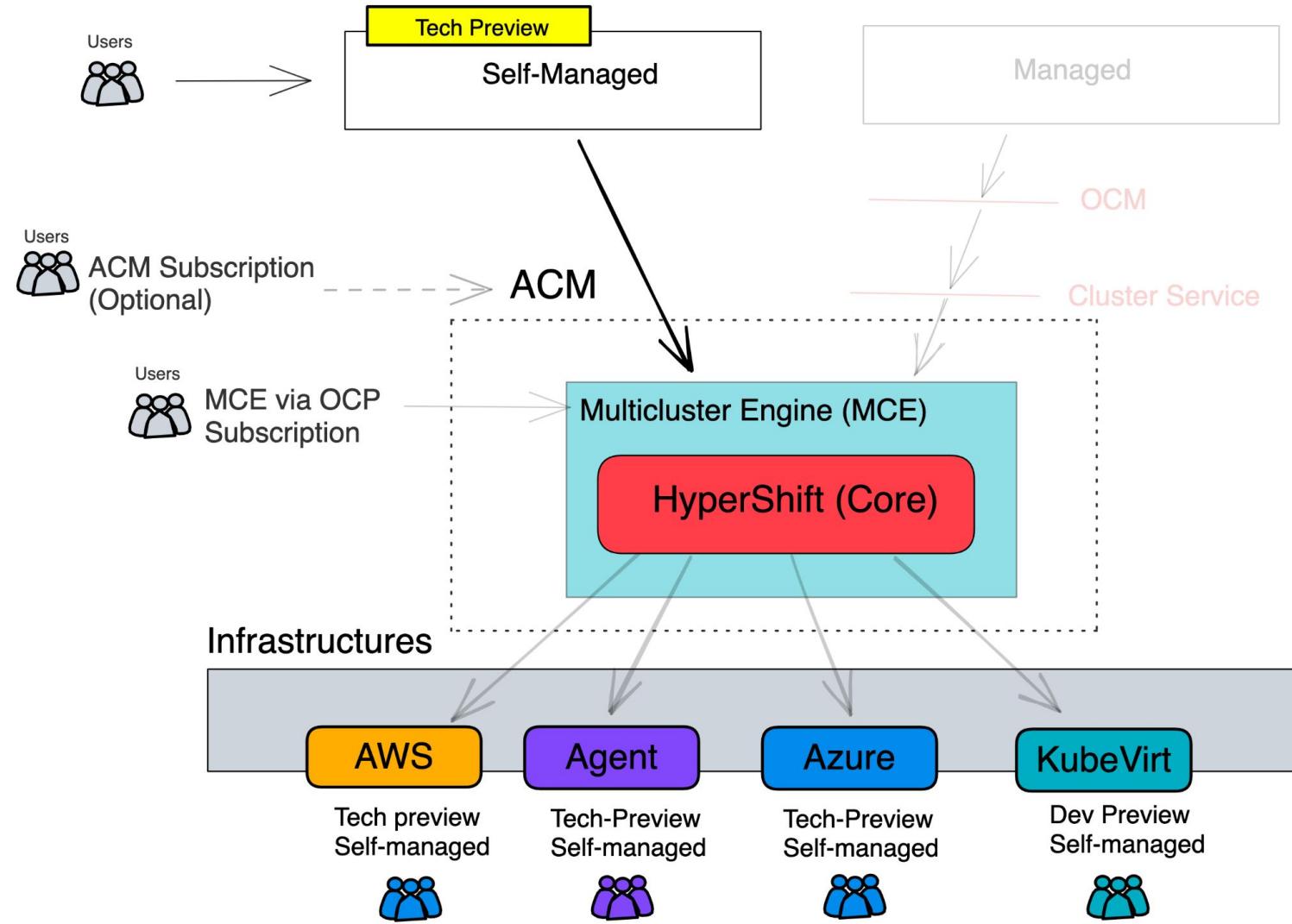


Workers

Hosting Service **Clusters** (decoupled CP and workers)



Hosted Control Planes (Tech Preview)



WorkerLatencyProfile

Improved OpenShift reaction time to node failure

In a use case where there is high network latency between control plane and worker.

- If the master's controller manager notices a node is unhealthy via the node-monitor-grace-period (Default is 40s), then it marks the node as unhealthy via the control manager.
- Then the controller manager waits for pod-eviction-timeout, (default is 300s) and updates the API server to remove the pod by setting terminate state.

Use below profiles to make openshift react faster when nodes fail

	Default Update And Default Reaction	Medium Update And Average Reaction	Low Update and Slow reaction
Kubelet	10s	20s	1m
Kube Controller Manager	40s	2m	5m
Kube API Server	300s	60s	60s

Blocking a payload registry

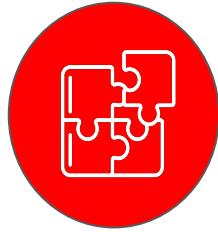
Block upstream payload registries in a disconnected environment

- For customers who require to block payload registry to remain in Minimal Acceptable Risk Standards for Exchanges (MARS-E) Compliance
- In a mirroring configuration, you can block upstream payload registries in a disconnected environment using a `ImageContentSourcePolicy` (ICSP) object

Security

Red Hat streamlines Kubernetes Security programs

Red Hat Advanced Cluster Security



Security Enhancements

Security Enhancements

- Improved detection of Spring vulnerabilities
- Scanning of the integrated OpenShift Container Registry
- Supply Chain: Verify image signatures against Cosign public keys
- Network segmentation: Identify Missing Kubernetes Network Policies



Policy



DevSecOps

DevSecOps

- Identify inactive software component
- Automatic Amazon ECR registry integration for AWS clusters

Policy

- operational deployment readiness
- Identify Spring critical vulnerabilities
- Improved validation of Pod Security Context

Scale

- Increased number of allowed inclusion and exclusion scopes



Red Hat Advanced Cluster Security for Kubernetes

Release 3.69.1

- Security
 - Improved detection of Spring vulnerabilities
 - Scanning of the integrated OpenShift Container Registry
- DevSecOps
 - Identify inactive software component
- Policy
 - operational deployment readiness



Release 3.70

- Security
 - Supply Chain: Verify image signatures against Cosign public keys
 - Network segmentation: Identify Missing Kubernetes Network Policies
- DevSecOps
 - Automatic Amazon ECR registry integration for AWS clusters
- Scale
 - Increased number of allowed inclusion and exclusion scopes
- Policy
 - Identify Spring critical vulnerabilities
 - Improved validation of Pod Security Context

Audit Logging Improvements: Logs contain login and login failure details

OAuth server events are now logged in the audit logs: OAuth server events, including failed login attempts, are now logged at the metadata level in the audit logs.

This is an audit log entry from the oauth-server's must gather audit logs.

The annotations section contain the **authentication.openshift.io/username** and **authentication.openshift.io/decision**.

Expected results: Login failures as well as login and logout events will be captured in audit logging.

```
{
  "kind": "Event",
  "apiVersion": "audit.k8s.io/v1",
  "level": "Metadata",
  "auditID": "1d9d3918-d009-4da5-935f-18cae42da30",
  "stage": "ResponseComplete",
  "requestURI": "/oauth/authorize?client_id=openshift-challenging-client&code_challenge=WIMss9c_3joFzJezl7wCW-z0YTug6yHuMxfetfnP5E4&code_challenge_method=S256&redirect_uri=https%3A%2F%2Foauth.openshift.apps.ci-in-g146s8k-72292.origin-ci-in-t-gce.dev.rhcloud.com%2Foauth%2Ftoken%2Fimplicit&response_type=code",
  "verb": "get",
  "user": {
    "username": "system:anonymous",
    "groups": [
      "system:unauthenticated"
    ]
  },
  "sourceIPs": [
    "10.128.2.11"
  ],
  "userAgent": "Go-http-client/1.1",
  "responseStatus": {
    "metadata": {},
    "code": 302
  },
  "requestReceivedTimestamp": "2022-04-11T09:23:31.220681Z",
  "stageTimestamp": "2022-04-11T09:23:31.347853Z",
  "annotations": {
    "authentication.openshift.io/decision": "allow",
    "authentication.openshift.io/username": "kostrows",
    "authorization.k8s.io/decision": "allow",
    "authorization.k8s.io/reason": ""
  }
}
```



Pod Security Admission Integration in OpenShift

This feature expands "**PodSecurity admission in OpenShift**". It introduces an opt-in mechanism that allows users to keep their workloads running when Pod Security Admission plugin gets turned on.

We want to adhere with the upstream pod security standards for our workloads but we also want to provide our users access to the Security Context Constraints (hereinafter SCCs) API that they are already used to. However, each of these admission plugins works a bit differently and so there must be a middle-man that synchronizes the privileges SCCs provide into privileges that Pod Security admission (hereinafter PSa) understands.

Pod Security admission validates pods' security according to the upstream [pod security standards](#) and distinguishes three different security levels:

- **privileged** - most privileged mode, anything is allowed
- **baseline** - minimally restrictive policy which prevents known privilege escalations
- **restricted** - heavily restricted policy, following current Pod hardening best practices

The default permission level is *restricted*. By default, there is a cluster-global configuration which enforces the configured policies on pods and known workloads. It is possible to override the cluster-global policy enforcement configuration on a per-namespace basis by using the [pod-security.kubernetes.io/enforce](#) label on given namespaces. It is also possible to exempt certain users, namespaces and runtime classes from the admission completely.

For more information, please review the [FAQ](#)

Management

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.6

Governance

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

The screenshot shows the RHACM UI under the 'Governance' tab. On the left, there's a sidebar with sections for 'openshift-plus-clusters' (status: reporting status), 'production-clusters' (status: pending), and 'openshift-plus-hub' (status: pending). The 'openshift-plus-hub' section is expanded, showing its policies: 'policy-compliance-operator-install', 'policy-advanced-managed-cluster-status', 'policy-acs-operator-central', 'policy-acs-central-status', and 'policy-acs-central-ca-bundle'. Each policy has a status of 'Enabled' and a remediation action of 'enforce'.

Policy name	Cluster violation	Status	Remediation
policy-compliance-operator-install	-	Enabled	enforce
policy-advanced-managed-cluster-status	-	Enabled	inform
policy-acs-operator-central	-	Enabled	enforce
policy-acs-central-status	-	Enabled	inform
policy-acs-central-ca-bundle	-	Enabled	enforce

- **ACM Policy-Controller-Improvements**
 - Select Namespaces via labels/expressions for better flexibility
 - Option to delete resources when Policies are removed
- **Kyverno and Gatekeeper community PolicySets – PolicySet for Multi Tenancy**
- **Multi Tenant/RBAC Guide** for Applications including Kyverno
- **Integration of PolicyGenerator** and OpenShift GitOps

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.6

Better Together

With key integrations across tools, we continue offering you the best experience across your Kubernetes fleet.

Applications

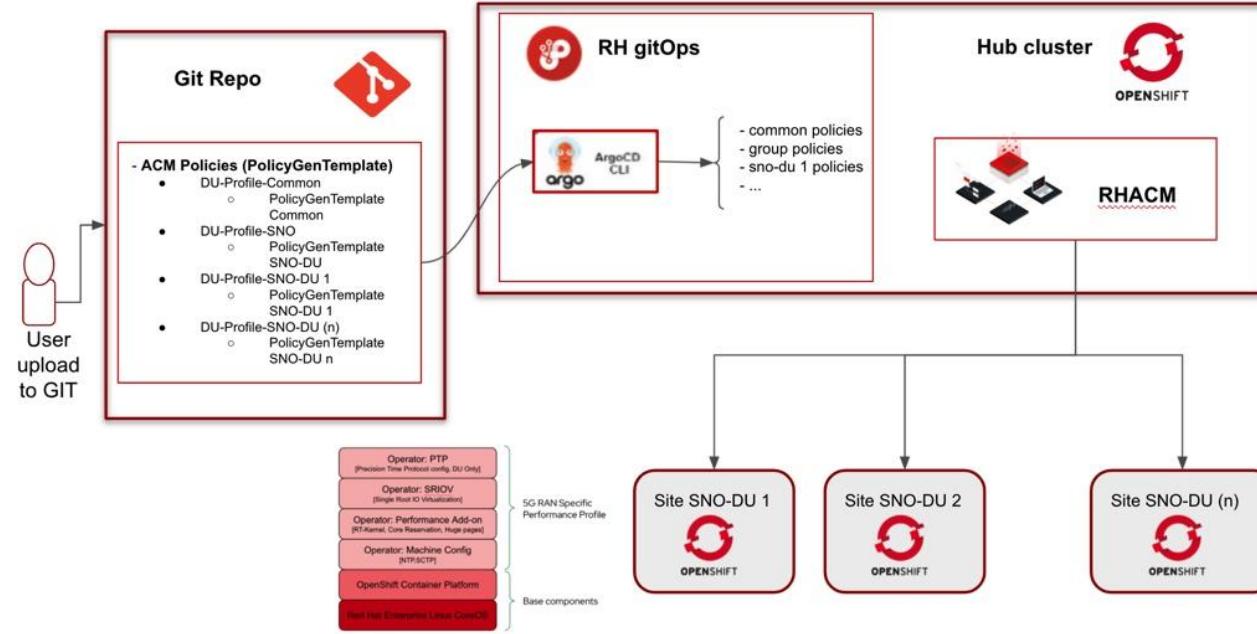
Overview	Advanced configuration		
csi-snapshot-controller-operator	OpenShift	openshift-cluster-storage-operator	1 Remote
etcd-operator	OpenShift	openshift-etcd-operator	Local
etcd-operator	OpenShift	openshift-etcd-operator	1 Remote
feng-nodejs-basic	OpenShift	feng-nodejs-basic	Local
flux	OpenShift	flux-system	Local
governance-policy-framework	OpenShift	open-cluster-management-agent-addon	Local
governance-policy-framework	OpenShift	open-cluster-management-agent-addon	1 Remote
grc	OpenShift	open-cluster-management	Local
helloworld-helm	Flux	feng-flux-helm	Local

- Visibility of **Flux** and **OpenShift** Applications in ACM
- **Manage** RHACM clusters from **Ansible** (AAP) (TP)
- ACM and MCE **community operators** – coming soon
- Enhanced integration with **VolSync** is now GA
- **Submariner** enhancements:
 - Automated configuration for Azure
 - Support for OVN SDN

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM 2.6

Manage At the Edge



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

- **Deploy & manage 2500 SNO (GA):** Support DU profile delivery with ACM in IPv6 connected and disconnected scenarios.
- **Search v2 Odyssey for high-scale environments - (Dev Preview):** Resilience and scalability of the collected Kubernetes resources (removal of RedisGraph dependency).
- **Configurable search data collection:** Get better controls for scale and security, limiting what we collect from the managed cluster.
- **Configurable dynamic metrics collection:** Improved controls on platform metrics that are dynamically pulled into the Hub during critical events.



Regional-DR

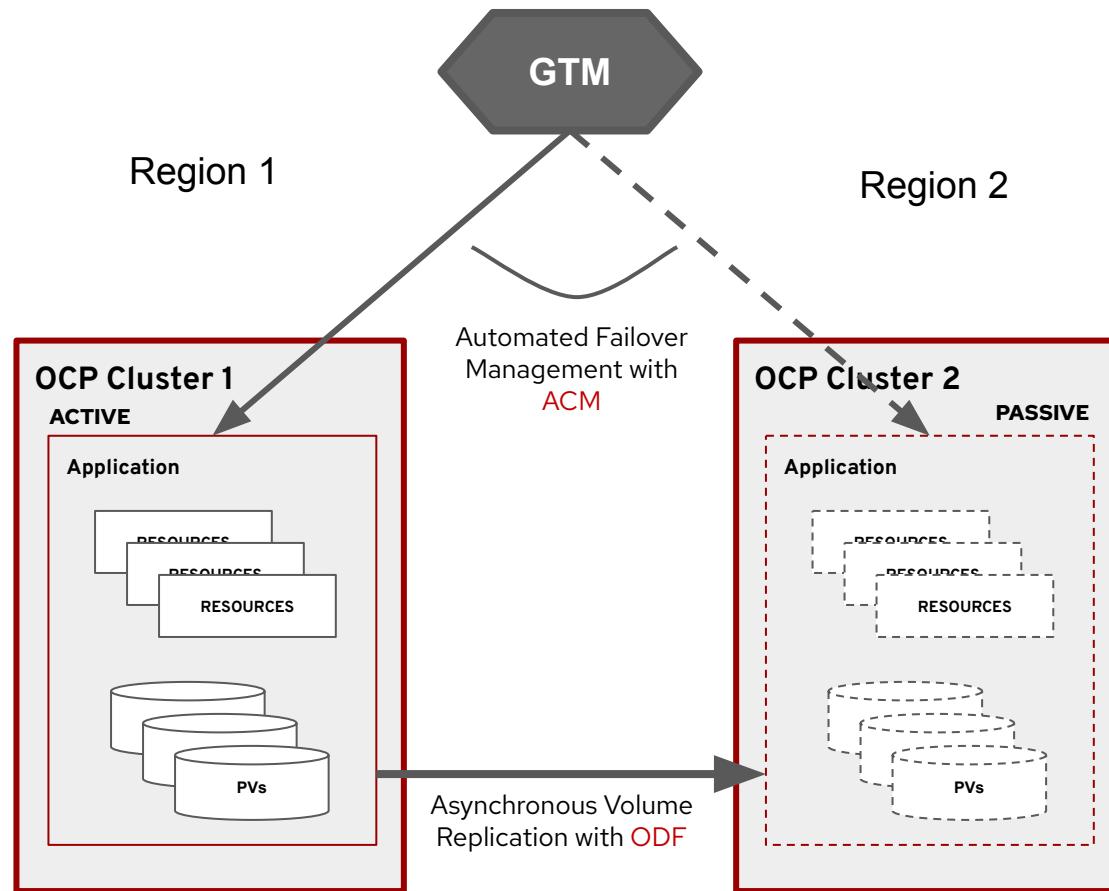
RPO – Mins

RTO – Mins

(Tech Preview) **Regional-DR with Failover Automation**

protection against
geographic-scale disasters

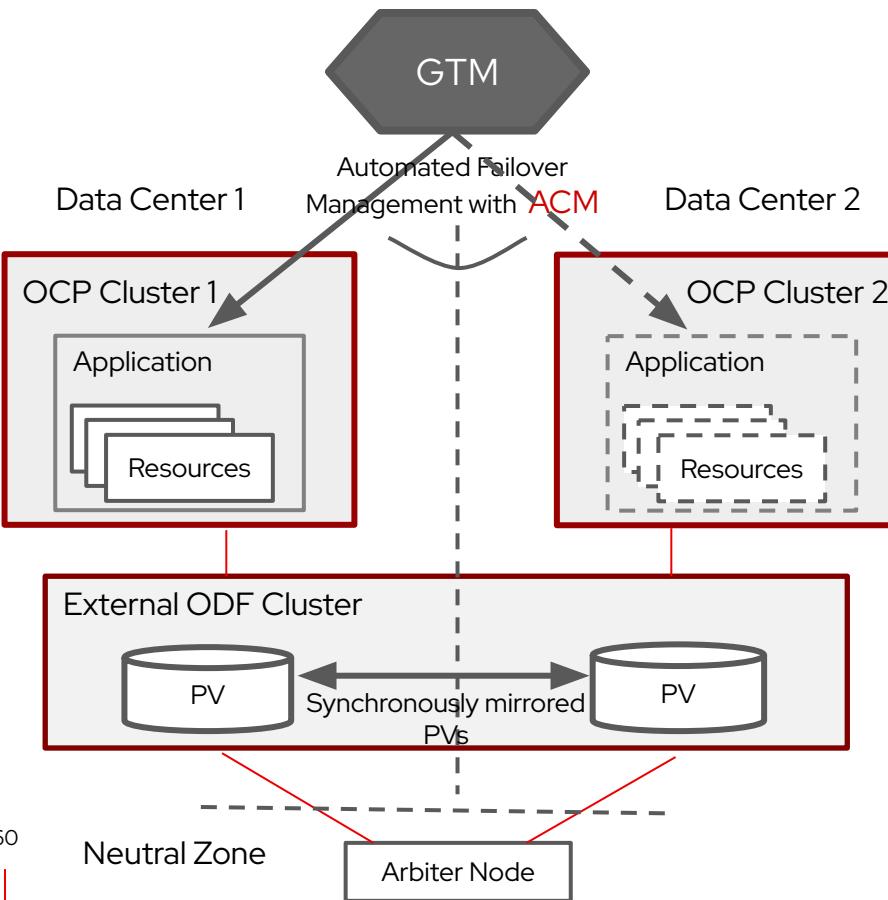
New with ODF 4.11 and ACM 2.5



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

(Tech Preview) Metro-DR with Failover Automation

protection against
metro-scale disasters

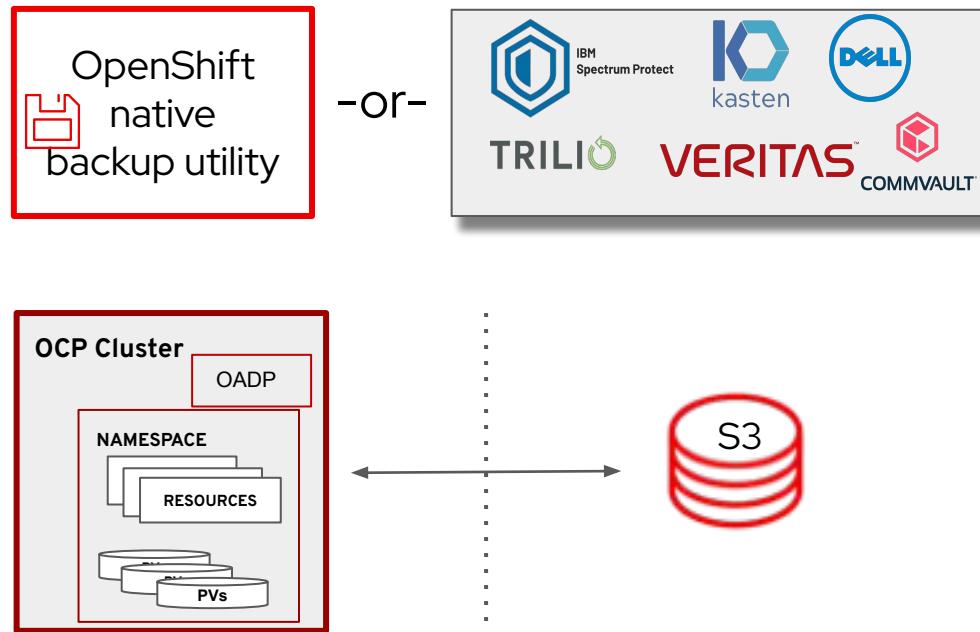


New with ODF 4.11 and ACM 2.5

- Multiple OCP clusters deployed in different AZs provide a complete fault isolated configuration
- External RHCS storage cluster provides persistent synchronous mirrored volumes across multiple OCP clusters enabling zero RPO
- ACM managed automated Application failover across clusters reduces RTO
- Requires Arbiter node in a third site for storage cluster
 - Arbiter node can be deployed over higher latency networks provided by public clouds

Backup Solutions for Red Hat OpenShift

Introducing OpenShift native backup utility with 4.11 (Tech Preview)



- **Application granular, cluster consistent backups with OADP**
- CLI based backup scheduling and management
- Built-in data mover enables CSI-based storage snapshots to be backed up to a remote S3 compatible object store.
- Backups solutions works for all OpenShift storage provisioners that support CSI Snapshots

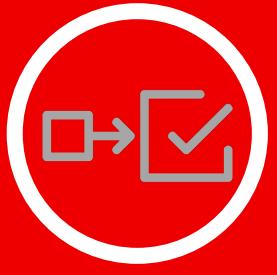
Observability



Monitoring



Logging



Distributed
Tracing



Networking

Summary Enhancement for OpenShift 4.11 Monitoring

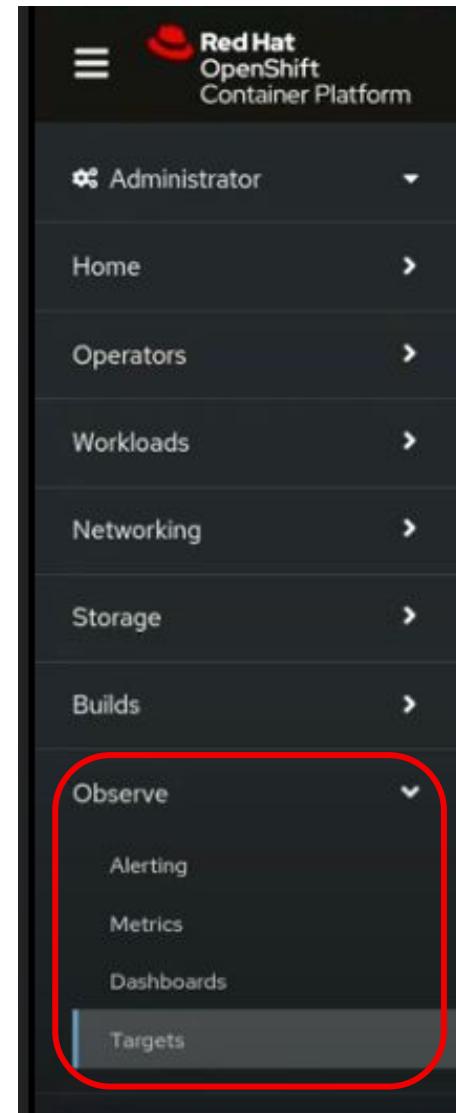
Security, reliability and customer facing experience

-
- ▶ Remove Prometheus UI (from 4.10)
 - ▶ Remove Grafana (feature-parity in OCP console)
 - ▶ Improve Observe > Metrics page UX
 - ▶ Additional authentication methods for `remote_write`
 - ▶ Several resilience and performance improvements
- UX**
- USER-FACING FEATURES**
- ▶ Support size-based retention
 - ▶ AlertManager config in user workload monitoring (GA)
 - ▶ Alert overrides for platform monitoring (TP)
 - ▶ Federation support for user workload monitoring
- SECURITY AND RELIABILITY**
- CONVENIENCE UPDATES**
- ▶ Double scrape_interval for CMO controlled Service Monitors for SNO
 - ▶ Option to add cluster ID to off-cluster integrations

Improved OpenShift Monitoring UI Experience

OpenShift Console Monitoring Experience

- ▶ Console Monitoring User Experience Enhancements to Observe OpenShift:
 - **Observe > Metrics:** Query Browser UX (e.g., autocomplete feature > now showing functions and metrics suggestions to users)
 - **Observe > Dashboards:** Higher data sampling rate > now showing more details to users
 - **Observe > Alerting:** Users can manage Alertmanager for user-defined alerts



Notes:

Prometheus user interfaces have been deprecated > console redirect for Prometheus alert backlinks added

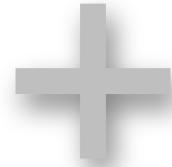
Grafana dashboards for visualization/customization out of the box are no longer provided

Logging 5.5 for OpenShift 4.11

<< NEW >>



Vector as alternate
collector



Loki as alternate log
store

Major updates and features

- ▶ maxUnavailable of 'collector' daemonset reducing upgrade time
- ▶ Log exploration natively inside the OpenShift Console
- ▶ Upgrade fluent to ruby 2.7 and latest dependencies
- ▶ Pod labels for k8s are preserved
- ▶ Support Cloudwatch output for Vector
- ▶ CloudWatch log forwarding add-on supports STS installations

Logging 5.5: OpenShift Logging UI Experience

OpenShift Console Logging Experience

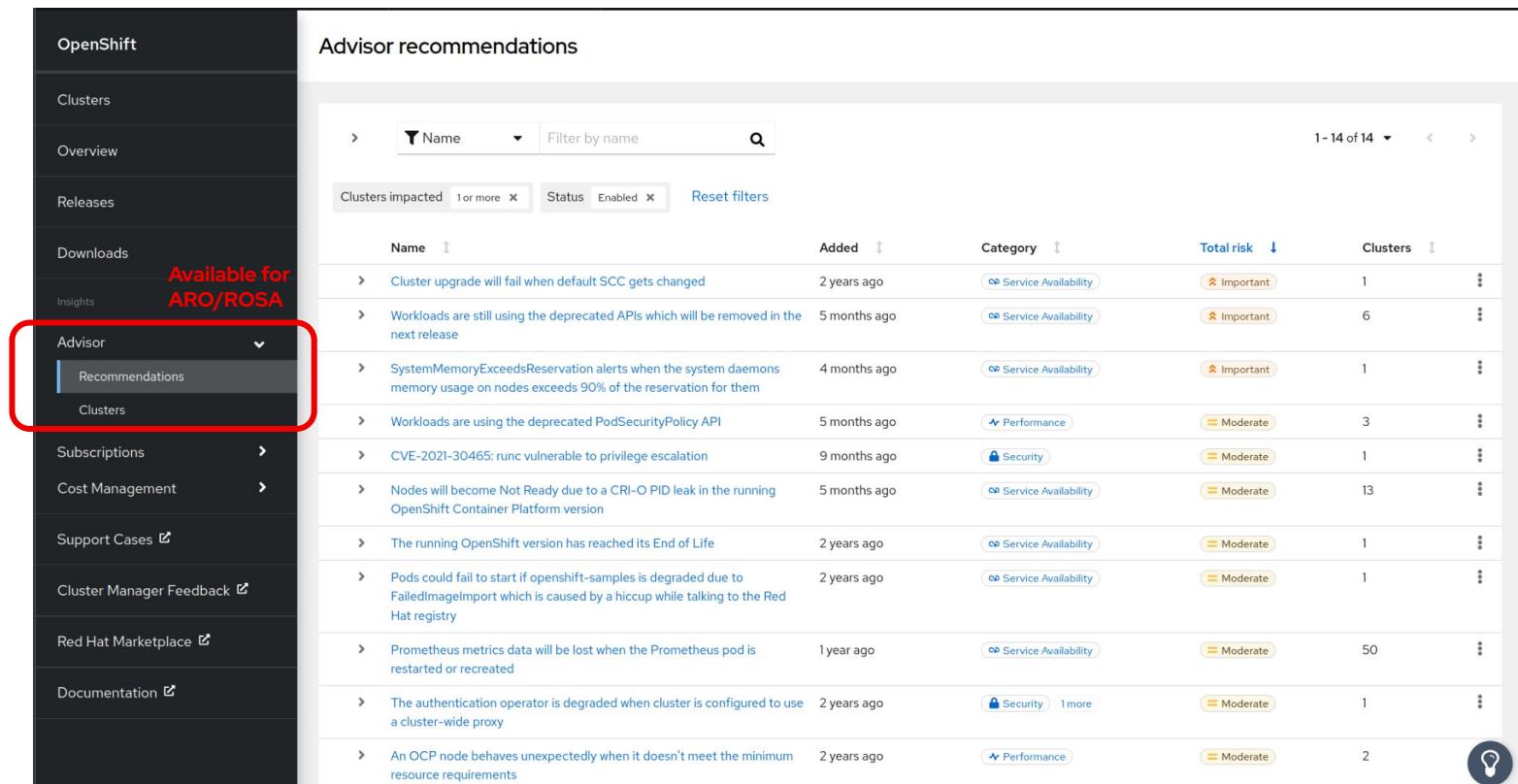
- Continue to work towards a **consistent** and **simplified Observability User Experience** by introducing a logging view in the console:
- Observe > Logs:** exposes log information from the underlying storage via an API, queried by the console to retrieve contextualized logs

The screenshot shows the OpenShift Console interface with a dark theme. The top navigation bar includes a user dropdown, a search bar, and various status indicators. The main content area is titled "Logging Experience". On the left, a sidebar menu lists categories like Home, Operators, Workloads, Networking, Storage, Builds, Pipelines, and Compute. Under the "Observe" category, there are sub-options for Alerting, Metrics, Dashboards, Targets, and Logs. The "Logs" option is highlighted with a yellow box. The right side of the screen displays a "Logs" view with a histogram at the top showing log volume over time, followed by a search bar, severity filters, and a detailed log list. The log list shows entries with timestamp, severity, message, file name, level, and job information.

Date	Message
18 Jul 2022, 08:26:57.4	loki_1 level=info ts=2022-05-13T09:51:02.06010152 caller=metrics.go:122 component=querier org_id=fake latency=fast query="sum by(job)(count_over_time({job=~\".+\"}{1m}))" query_type=metric range_type=range length=8m0s step=1m0s duration=11.3443ms status=200 limit=100 returned_lines=0 throughput=0B total_bytes=0B queue_time=189.674ms subqueries=1
18 Jul 2022, 08:26:57.3	loki_1 level=info ts=2022-05-13T09:51:02.05575382 caller=metrics.go:122 component=querier org_id=fake latency=fast query="sum by(job)(count_over_time({job=~\".+\"}{1m}))" query_type=metric range_type=range length=8m0s step=1m0s duration=5.4181ms status=200 limit=100 returned_lines=0 throughput=0B total_bytes=0B queue_time=188.5313ms subqueries=1
	filename /var/log/out.log job varlogs-duplicate level info
18 Jul 2022, 08:26:57.3	loki_1 level=info ts=2022-05-13T09:51:02.05373852 caller=metrics.go:122 component=querier org_id=fake latency=fast query="sum by(job)(count_over_time({job=~\".+\"}{1m}))" query_type=metric range_type=range length=22m0s step=1m0s duration=225.1158ms status=200 limit=100 returned_lines=0 throughput=81MB total_bytes=18MB queue_time=3.6511ms subqueries=1
18 Jul 2022, 08:26:57.3	loki_1 level=info ts=2022-05-13T09:51:02.04842762 caller=metrics.go:122 component=querier org_id=fake latency=fast query="sum by(job)(count_over_time({job=~\".+\"}{1m}))" query_type=metric range_type=range length=29m0s step=1m0s duration=12.2095ms status=200 limit=100 returned_lines=0 throughput=0B total_bytes=0B queue_time=175.1103ms subqueries=1
18 Jul 2022, 08:26:57.3	loki_1 level=info ts=2022-05-13T09:51:02.04752262 caller=metrics.go:122 component=querier org_id=fake latency=fast query="sum by(job)(count_over_time({job=~\".+\"}{1m}))" query_type=metric range_type=range length=22m0s step=1m0s duration=168.74ms status=200 limit=100 returned_lines=0 throughput=81MB total_bytes=14MB queue_time=49.3927ms subqueries=1

Insights Advisor for OpenShift

- ▶ Advisor now available for customers of ARO/ROSA/OSD with specific recommendations for managed clusters.
- ▶ Changing cluster ownership
 - ▶ Cluster ownership change no longer requires manually changing pull-secret. Insights operator takes care of updating pull-secret automatically
- ▶ Optimized payload with conditional data gathering
- ▶ New recommendations focused on Namespace compliance, better vSphere support, authentication LDAP issues etc.



The screenshot shows the OpenShift Insights Advisor interface. On the left, there is a sidebar with various links: Clusters, Overview, Releases, Downloads, Insights, Advisor (which is currently selected), Recommendations (highlighted with a red box), Clusters, Subscriptions, Cost Management, Support Cases, Cluster Manager Feedback, Red Hat Marketplace, and Documentation. A red box highlights the 'Recommendations' link. Above the sidebar, a red banner says 'Available for ARO/ROSA'. To the right, the main area is titled 'Advisor recommendations' and displays a table of 14 items. The table columns include Name, Added, Category, Total risk, and Clusters. Each row contains a brief description of a recommendation, its age, category (e.g., Service Availability, Performance, Security), risk level (Important, Moderate), and the number of clusters it impacts. At the bottom right of the table is a lightbulb icon.

Name	Added	Category	Total risk	Clusters
Cluster upgrade will fail when default SCC gets changed	2 years ago	Service Availability	Important	1
Workloads are still using the deprecated APIs which will be removed in the next release	5 months ago	Service Availability	Important	6
SystemMemoryExceedsReservation alerts when the system daemons memory usage on nodes exceeds 90% of the reservation for them	4 months ago	Service Availability	Important	1
Workloads are using the deprecated PodSecurityPolicy API	5 months ago	Performance	Moderate	3
CVE-2021-30465: runc vulnerable to privilege escalation	9 months ago	Security	Moderate	1
Nodes will become Not Ready due to a CRI-O PID leak in the running OpenShift Container Platform version	5 months ago	Service Availability	Moderate	13
The running OpenShift version has reached its End of Life	2 years ago	Service Availability	Moderate	1
Pods could fail to start if openshift-samples is degraded due to FailedImageImport which is caused by a hiccup while talking to the Red Hat registry	2 years ago	Service Availability	Moderate	1
Prometheus metrics data will be lost when the Prometheus pod is restarted or recreated	1 year ago	Service Availability	Moderate	50
The authentication operator is degraded when cluster is configured to use a cluster-wide proxy	2 years ago	Security	Moderate	1
An OCP node behaves unexpectedly when it doesn't meet the minimum resource requirements	2 years ago	Performance	Moderate	2

Networking & Routing

General Networking Enhancements

MetalLB: Load Balancer for Bare-metal

- Per-node selector configuration [Tech Preview]
- IP Pool service advertisement per BGP peers list

```
apiVersion: metallb.io/v1beta1
kind: BGPAdvertisement
metadata:
  name: bgpadvertisement
  namespace: metallb-system
spec:
  ipaddresspools:
    - pool1
    - pool2
  nodeSelector:
    # Top of Rack label
```

DNS Support CoreDNS forwarding DNS requests over TLS

- This feature enables cluster admins to configure TLS for forwarded DNS queries.
- This applies only to the cluster-dns-operator (not the CoreDNS instance managed by MCO).

Security Support Runtime Enabling/Disabling of IPSec

```
$ oc patch network.operator.openshift.io/cluster
--type=merge -p \
'{
  "spec": { "defaultNetwork": {
    "ovnKubernetesConfig": { "ipsecConfig":{} } }
  }
}'
```

Ingress Enhancements

Ingress Updates

ALB support for OpenShift on AWS

- Technical Preview
- The aws-load-balancer-operator can be installed by the user, to deploy and manage an instance of the [AWS Load Balance Controller](#)
- This operator will be distributed through the operator hub

Set default subdomain for routes at Project/namespace level

- Users can specify a custom subdomain: <subdomain>. <cluster ingress domain> using spec.subdomain instead of spec.host

Ingress Updates

Support for configuring HAProxy parameters

`ROUTER_MAX_CONNECTIONS`
`ROUTER_BACKEND_CHECK_INTERVAL`

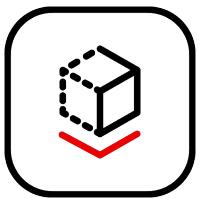
Expose port configuration to the ingress operator

- HostNetwork has a hostNetwork field with the following default values for the optional binding ports:
 - httpPort: 80
 - httpsPort: 443
 - statsPort: 1936
- One can deploy multiple Ingress Controllers on the same node for the HostNetwork strategy

Virtualization

OpenShift Virtualization

Modernize workloads, bring VMs to Kubernetes



Enterprise Virtualization Enhancements

- ▶ Windows 11 and RHEL 9 Guest Support
- ▶ Intuitive UI for VM admins
 - Improved new VM wizard & VM catalog
 - VM overview page to manage individual VMs
- ▶ Robust applications with *RHEL High Availability*

VMs and Containers in Private/Hybrid Cloud

- ▶ Provide self-tuned VM instances
- ▶ RBAC control on VM templates
- ▶ Easily share vGPU w/ NVIDIA operator (Tech Preview)

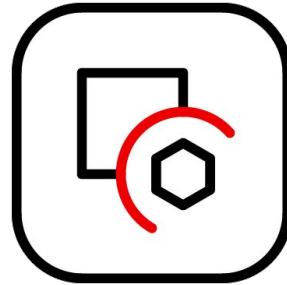
Edge and Telco

- ▶ Low latency network self test suite for validation

Proven Performance

- ▶ [Large Scale Tuning and Performance whitepaper](#)

Name	Drive	Size
disk0	Hotplugged disk	30 GiB
containerdisk	disk	20 GiB



OpenShift sandboxed containers

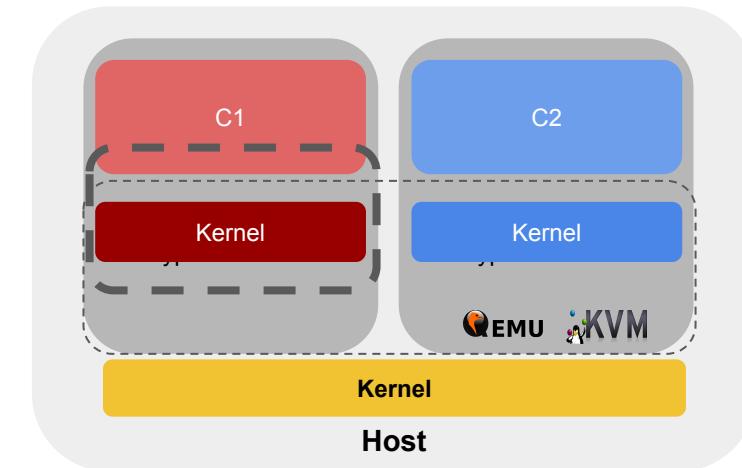
Kernel Isolation for containerized workloads

Edge and Cloud Support

- **Bare metal support on AWS - Tech Preview**
Ability to install OpenShift sandboxed containers on AWS BM instances
- **Sandboxed Containers available and supported on SNO**
Ensured that Sandboxed Containers can run on SNO

Enhanced Observability

- **Additional Upstream Kata Specific Metrics**
Better administration with visible metrics on performance, health or potential bottlenecks



Specialized Workloads

Windows Workers



Previously, the Docker container runtime was used in Windows nodes. Kubernetes [deprecated](#) Docker as a container runtime and removed dockershim; you can reference the Kubernetes documentation for more information in [Docker deprecation](#). [ContainerD](#) will be the new supported container runtime for Windows nodes in version 6.0.0 of the Windows Machine Config Operator (WMCO).

ContainerD is an open-source industry-standard container runtime that is supported by the community. Important considerations

Question – All of my Docker CLIs I depend on my local machine for build process are broken!

Answer – Docker CLIs on your dev box are not being affected, and you may continue to use them to build container images. All this works thanks to the way Docker, containerd, and other tools conform to the [Open Container Initiative](#) (OCI) – a set of standards which help ensure tools used to build, publish, and run containers all interoperate together.

Question – If I upgrade my Windows Machine Config Operator on OpenShift cluster to 6.0.0 (available on OpenShift 4.11) my Windows containers won't run!

Answer – The upgrade will deploy the new containerd runtime on the Windows nodes and the containers will run just fine.

Question - I must rebuild all my containers and OpenShift clusters to use containerd!

Answer – The containerd change is only on the host runtime. Container images built with Docker and other tools that are OCI compliant do not require you to rebuild. You can still use the same container image to run with OpenShift and containerd. If you are using OpenShift, all you need to do is deploy your workload on a host which has containerd runtime.

Windows Workers



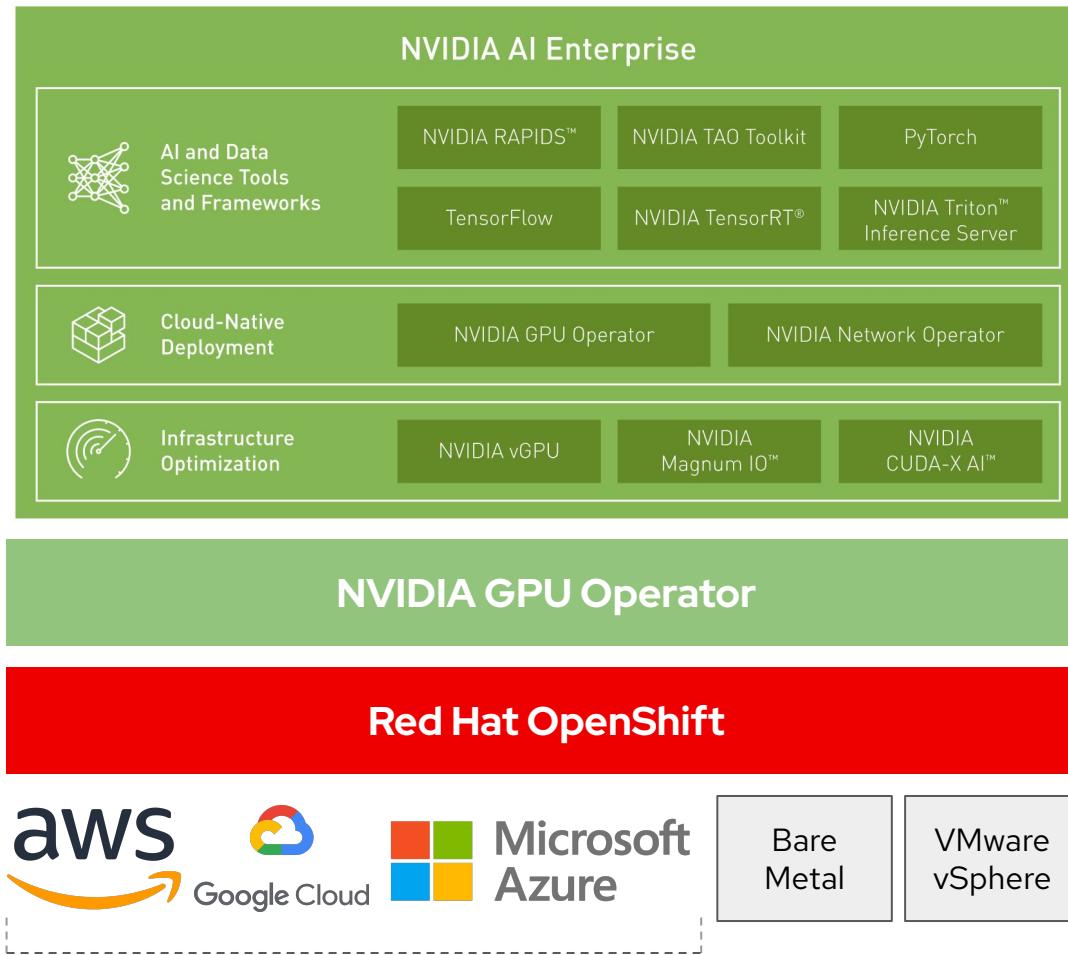
Windows Server 2022

Now with Windows Server 2022!

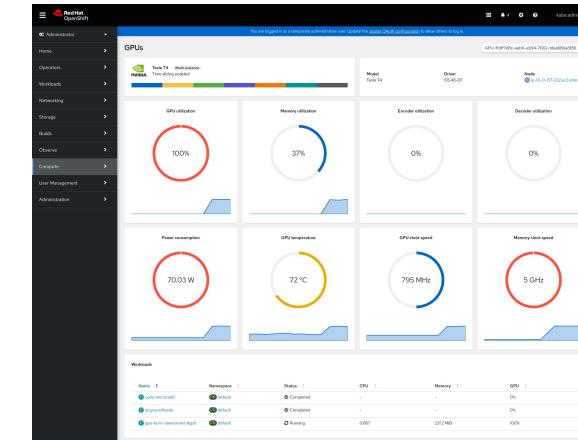
The following table lists the [Windows Server Versions](#) that are supported by WMCO 6.0.0, based on the applicable platform. Windows Server versions not listed are not supported and attempting to use them will cause errors. To prevent these errors, use only an appropriate version for your platform. Note that Windows Server 2022 has a [mainstream end date](#) of Oct 2026, with an extended date of Oct 2031

Platforms	Windows Server Versions
Amazon Web Services (AWS)	Windows Server 2019 (version 1809) Windows Server 2022 with the Windows KB5012637 patch
Microsoft Azure	Windows Server 2019 (version 1809) Windows Server 2022 with the Windows KB5012637 patch
VMware vSphere	Windows Server 20H2 Windows Server 2022 with the Windows KB5012637 patch
Bare-metal or provider agnostic	Windows Server 20H2 Windows Server 2022 with the Windows KB5012637 patch

NVIDIA AI Enterprise hybrid cloud



- ▶ NVIDIA AI Enterprise with OpenShift is now supported on public clouds: AWS, Google Cloud, and Azure
- ▶ Sharing GPUs: multiple pods allowed per GPU with time-sharing and replicas (no MIG requirement)
- ▶ GPU Dashboard in OpenShift 4.11 console



- ▶ OpenShift Virtualization vGPU enablement with the NVIDIA GPU Operator (Tech Preview)
- ▶ OpenShift on Arm (Tech Preview)
- ▶ Try OpenShift+NVIDIA AI Enterprise two weeks with NVIDIA Launchpad



Operator Framework

Operator SDK Enhancement

Enable Java developers to write Operators using Operator SDK and manage them via OLM

Java Operator SDK plugin (Tech Preview)

- ▶ Jump start Operator development with **project scaffolding** includes **Java Operator SDK** and **Quarkus** to manage distributed Java apps also in **Java** without steep learning curve.
- ▶ **Quarkus** framework makes Java efficient for containers, cloud, and serverless environments with **memory consumption optimization** and a **fast first response time**.
- ▶ Support OLM integration including **generate/validate Operator bundle** and more to help join our **Operator ecosystem** and **manage workloads with OpenShift**.



```
$ operator-sdk init --plugins quarkus --domain example.com --project-name memcached-quarkus-operator
$ operator-sdk create api --plugins quarkus --group cache --version v1 --kind Memcached
$ make bundle bundle-build bundle-push
$ operator-sdk run bundle quay.io/tlwu2013/memcached-operator-bundle:v0.0.1
```

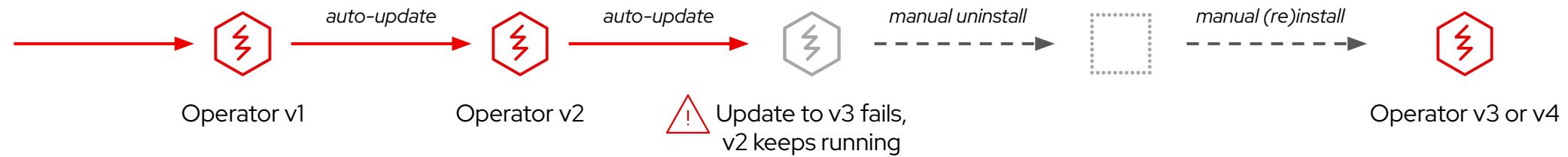
Operator Lifecycle Management



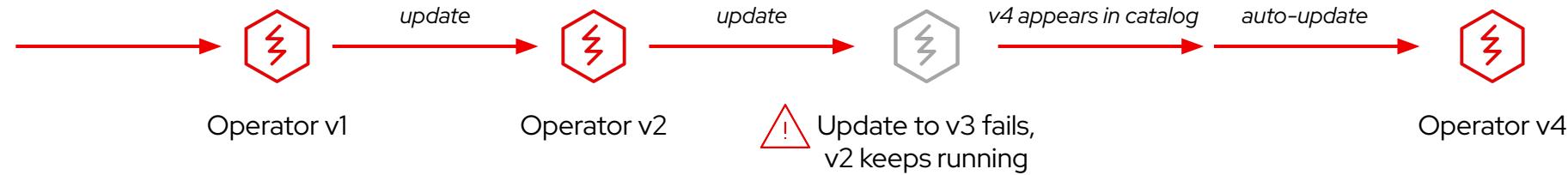
Fail-forward updates

Avoid manual cleanup of failed operator updates. When enabled, OLM automatically re-attempts failed operator updates as soon as a newer version than the failed update becomes available in the operator catalog. Helps operating large amounts of clusters at scale while leaving auto-updates enabled.

Before:



Now (4.11):



Quay 3.8

(GA end of Q3 '22)

Red Hat Quay 3.8: Preview of new UI

Modern PatternFly-based user interface aligned with Red Hat portfolio

- ▶ Sleek design and user-friendly interface concept
- ▶ In 3.8: Repository and Organization management
- ▶ In Q4: Preview of integration of quay.io into console.redhat.com
- ▶ **Planned:**
 - Advanced filtering, sorting and search
 - More batch operations
 - Shorter flows for common actions
 - In-place configuration changes
 - Visualization of Helm Chart and signed content
 - API token management

The image displays two screenshots of the Red Hat Quay PF UI. The top screenshot shows a detailed view of a tag named 'tagnamehere' within a namespace 'openshift-release-dev' under 'ocp-release'. It includes a security report section with a gauge showing 13 vulnerabilities, 7 of which are high-level, and a note that patches are available for 2 of them. The bottom screenshot shows the 'Organization' page, which lists two organizations: 'ProjectA' and 'ProjectB'. ProjectA has 2 public and 1 private repository, 4 users, 16 tags, 1.1 GB size, 4578 pulls, was last pulled a month ago, and was last modified 2 months ago. ProjectB has 23 public and 7 private repositories, 33 users, 2 tags, 1.1 GB size, 108 pulls, was last pulled a year ago, and was last modified 4 months ago. A 'Create organization' button is visible at the top of this page. A modal window titled 'Create repository' is also shown, prompting for a name ('myrepo'), visibility ('Public' selected), and connection options for Dockerfile, GitHub, GitLab, and bitbucket.

Red Hat Quay 3.8: Superuser UX

Quay admins can introspect all content

Name	Visibility	Tags	Size	Pulls	Last Pull	Last Modified
User1/myrepo	Public	16	1.1 GB	4578	1 month ago	2 months ago
User1/test	Private	2	1.1 GB	108	1 year ago	4 months ago
User1/newstuff	Public	16	1.1 GB	4578	1 month ago	2 months ago
<input checked="" type="checkbox"/> ProjectA/locator	Private	2	1.1 GB	108	1 year ago	4 months ago
<input checked="" type="checkbox"/> ProjectA/petclinic	Public	16	1.1 GB	4578	1 month ago	2 months ago
ProjectB/cartapp	Private	2	1.1 GB	108	1 year ago	4 months ago
ProjectB/twipper	Public	16	1.1 GB	4578	1 month ago	2 months ago
ProjectB/instacarp	Private	2	1.1 GB	108	1 year ago	4 months ago

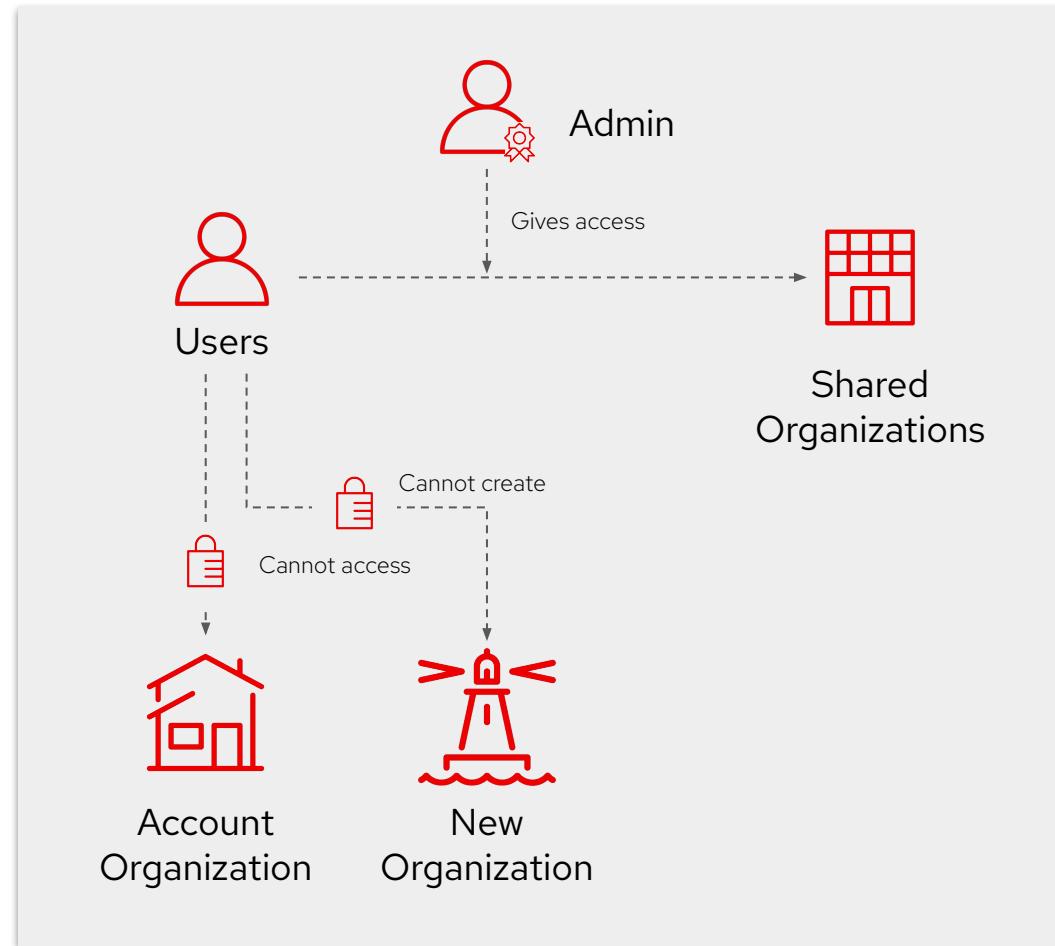
- ▶ **Before:** Quay superusers have to add themselves to organizations as owners in order to introspect content
- ▶ **Now:** Superusers can see and introspect all content in the system using the new UI components
- ▶ **Planned:**
 - new Superuser panel design
 - Global read-only users (auditor access)
 - Embedded dashboards for monitoring registry health and growth

Voice your opinion!

<https://red.ht/quay-survey>

Red Hat Quay 3.8: New Permission Model

Restricted Users



- ▶ **Today:** every user with access to Quay can create new content and new organizations
- ▶ **New:** restricted users can not store new content by default until they are given permission to by the superuser
- ▶ **New:** restricted users cannot create new organizations
- ▶ **Goal:** better support environments with heightened access control and prevent unbound storage growth
- ▶ *Configured via LDAP query or as a default for all new users*

Red Hat Quay 3.8: Other improvements



IPv6 support

Native support for environments where only IPv6 is available. Includes OpenShift and RHEL-based deployments.



Proxy-Caching moves to General Availability

Granular caching of third party registries.

Introduces cache size limit with automatic eviction of least-recently used images.

Can prevent outages due to temporary unavailability of upstream registries.



Container Security Operator

Support for disconnected environments by adhering to ImageContentSourcePolicy and cluster-wide proxy settings. Improved credential management.

Storage

OpenShift Storage - Journey to CSI

- CSI Operators - plugable, built-in upgrade, storage integration
 - Azure File (**GA**)
 - CIFS only
 - No snapshot support
- CSI Migration in 4.11
 - Azure Disk (**GA**)
 - OpenStack Cinder (**GA**)
- CSI Migration
 - No data migration
 - Translate calls to CSI on the fly
 - Transparent & enabled by default when GA
 - CSI storage class is default for new clusters
 - For upgraded clusters, the default SC is not changed
 - Recommended to set the CSI SC as default

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

OpenShift Storage - CSI Expansion GA

- Online expansion including FileSystem
- Simply update the PVC's field
- Driver support required
- No shrinking
- Make sure SC has allowVolumeExpansion: true

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: my_storage_class
provisioner: kubernetes.io/aws-ebs
parameters:
allowVolumeExpansion: true
(...)
```

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: myclaim
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi # New size here
```

OpenShift Storage - Generic Ephemeral Volumes GA

- Similar to emptyDir for **scratch data**
- Defined **in-line** pod spec
- Define a **fixed size**
- PV follows the pod's lifecycle
- Supported by all CSI drivers*
- Backed by CSI, **can be network attached**
- Support for snapshots, expansion, clone

```
kind: Pod
apiVersion: v1
metadata:
  name: my-app
spec:
  containers:
    - name: my-frontend
      image: busybox:1.28
      volumeMounts:
        - mountPath: "/scratch"
          name: scratch-volume
          command: [ "sleep", "1000000" ]
  volumes:
    - name: scratch-volume
      ephemeral:
        volumeClaimTemplate:
          metadata:
            labels:
              type: my-frontend-volume
          spec:
            accessModes: [ "ReadWriteOnce" ]
            storageClassName: "my_storage_class"
            resources:
              requests:
                storage: 1Gi
```

Other OpenShift Data Foundation 4.11 updates

- ODF Support for Disaster Recovery solutions (covered in ACM Management section)
 - Regional Disaster Recovery (Tech Preview)
 - Metro Disaster Recovery (Tech Preview)
- NFS support (Tech Preview)
- Multi-cluster ODF monitoring with ACM UI
- LVMO - support for Single Node OpenShift with thin provisioning, snapshots and clone (Tech Preview)

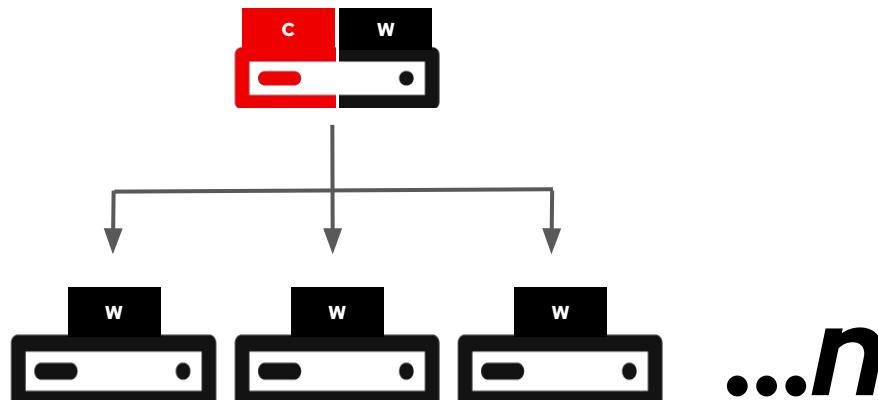
Out of the box support	
Block, File, Object	
Platforms	
AWS/Azure	Google Cloud (Tech Preview)
RHV	OSP (Tech Preview)
Bare metal/IBM Z/Power	VMWare Thin/Thick IPI/UPI
ARO - Self managed OCS	IBM ROKS & Satellite - Managed ODF (GA)
ROSA - Managed ODF (Limited availability, GA in OCT 2022)	
Deployment modes	
Disconnected environment and Proxied environments	

Telco 5G and Edge Computing

Single Node OpenShift

Site capacity expansion via additional workers

- In edge environments with a site failover HA model, additional per site capacity is sometimes required without adding within site HA
- It is now possible to add worker nodes to Single node OpenShift installations created with 4.11+:
 - Via the Assisted Installer at cloud.redhat.com
 - Via Red Hat Advanced Cluster Management (ACM)
 - Manually using generated **worker.ign**
- By default, Ingress will remain pinned to the Single node OpenShift control plane
- For capacity reasons, a single node OpenShift will not be able to manage the same number of workers or Kubernetes objects as a full three node control plane



PAO becomes part OpenShift core components

PAO is becoming a sub-controller of the Node Tuning Operator (NTO)

Today's install workflow

1. Install OpenShift
2. Install PAO Operator
3. Apply the PerformanceProfile

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: myprofile
spec:
  cpu:
    isolated: "2-21,26-37"
    reserved: "0-1,24-25"
.../...
```

Future install workflow

1. Install OpenShift
2. Apply the PerformanceProfile

Upgrade workflow: almost transparent

1. PerformanceProfile API is unchanged
2. PAO Operator is automatically uninstalled
 - a. PerformanceProfile is now implemented by NTO!

Permanently* offline CPUs via PerformanceProfile

*until next configuration change (implies a reboot)

Use case: the worker nodes of the cluster have been deployed with extra CPU capacity that will be used in the future. How to turn them off until we need them?

- ▶ Performance profile has a new parameter listing the CPUs to shutdown
- ▶ This is done at boot time, so any configuration change requires a reboot (as any Performance profile change).

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: myprofile
spec:
  cpu:
    isolated: "2-21,26-37"
    reserved: "0-1,24-25"
    offlined: "38-42"
.../...
```

./performance-profile-creator --reserved-cpu-count 2 --offlined-cpu-count 4

Secondary interfaces sysctl

macvlan, SR-IOV (kernel only, **not** DPDK)

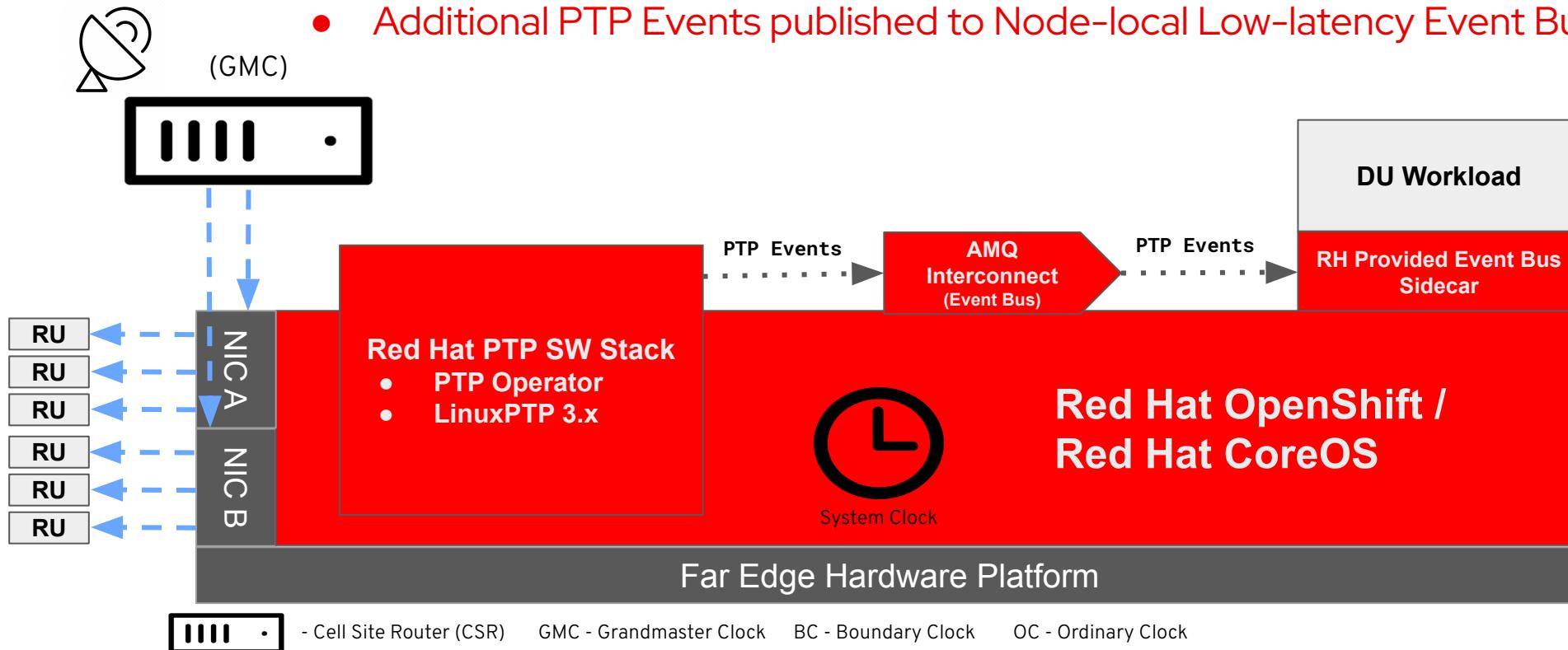
Safe, per interface, sysctls:

```
net.ipv4.conf.IFNAME.accept_ra
net.ipv4.conf.IFNAME.accept_redirects
net.ipv4.conf.IFNAME.accept_source_route
net.ipv4.conf.IFNAME.arp_accept
net.ipv4.conf.IFNAME.arp_notify
net.ipv4.conf.IFNAME.disable_policy
net.ipv4.conf.IFNAME.secure_redirects
net.ipv4.conf.IFNAME.send_redirects
net.ipv6.conf.IFNAME.accept_ra
net.ipv6.conf.IFNAME.accept_redirects
net.ipv6.conf.IFNAME.accept_source_route
net.ipv6.conf.IFNAME.arp_accept
net.ipv6.conf.IFNAME.arp_notify
net.ipv6.neigh.IFNAME.base_reachable_time_ms
net.ipv6.neigh.IFNAME.retrans_time_ms
```

```
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: macvlan-net
spec:
  config: '{'
    "cniVersion": "0.4.0",
    "name": "macvlan-net",
    "plugins": [
      {
        "type": "macvlan",
        "master": "bond2"
      },
      {
        "type": "tuning",
        "sysctl": {
          "net.ipv4.conf.IFNAME.accept_redirects": "1"
        }
      }
    ]
  }
```

PTP Enhancements

- Boundary Clock support on multiple NICs (assumes NIC PTP support)
- LinuxPTP 3.x
- Additional PTP Events published to Node-local Low-latency Event Bus



PTP Operating Modes: OpenShift Node as an Ordinary Clock [GA] and Boundary Clock [TP]

Failed Single Node OpenShift Upgrade Recovery

What is it?

Using the Topology Aware Lifecycle Manager (TALM), a cluster operator can **backup Single Node OpenShift artifacts** prior to an upgrade and a **restore script** is provided to be used if the upgrade fails.

What gets backed up?

- **Cluster:** A snapshot of etcd and static pod manifests.
- **Content:** Backups of folders, for example, /etc, /usr/local, /var/lib/kubelet.
- **Changed files:** Any file managed by machine-config that has been changed.
- **Deployment:** A pinned ostree deployment.
- **Images:** Any container images that are in use.

```
apiVersion: ran.openshift.io/v1alpha1
kind: ClusterGroupUpgrade
metadata:
  name: du-upgrade-4918
  namespace: ztp-group-du-sno
spec:
  preCaching: true
  backup: true
  clusters:
    - cnfdb1
    - cnfdb2
  enable: false
  managedPolicies:
    - du-upgrade-platform-upgrade
  remediationStrategy:
    maxConcurrency: 2
    timeout: 240
```



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