OpenShift 4.11 Update Review Pt. 1

Update Summary

Today, July 21st 2022, Red Hat announced the Technical Product Update of OpenShift 4.11. This is the latest minor version, and the 2nd of 2022. Remember, once 4.11 hits GA (date not yet announce), this will trigger the 3 month countdown for the end of 4.10 Full Support! Of course, Maintenance support will continue until September 2023.

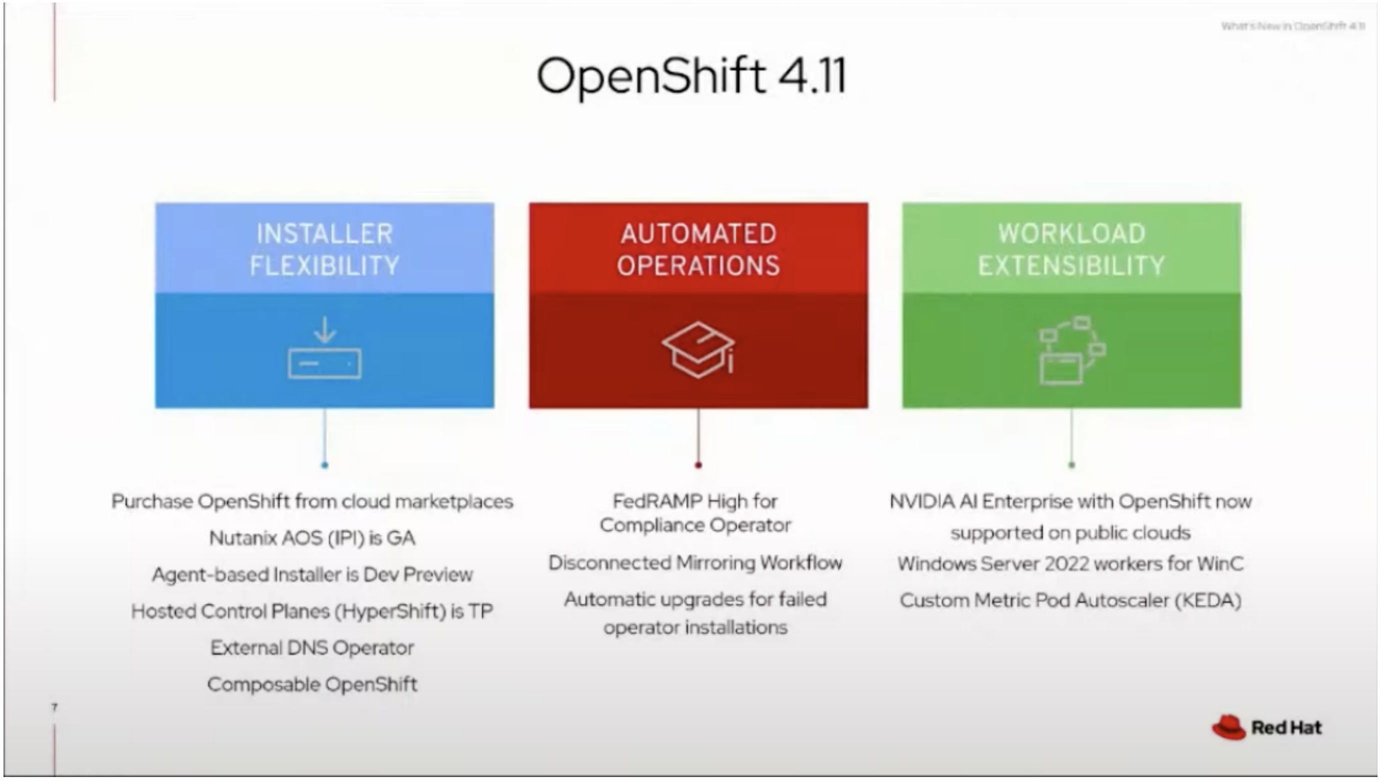
> Many of the below points and images are from Red Hat's live stream on July 21st, 2022 reviewing the OpenShift 4.11 Update. Go watch the recording for more details and even more features!

Technical Update List

Below, you will find a list of the many updates included in the 4.11 update.

> For any unknown abbreviations or terms, check here for more information:
>
> Terms, Abbreviations, and Definitions

- OCP from Cloud Marketplaces
- Nutanix AOS IPI (GA)
- Agent-based Installer (Dev Preview)
- Hosted Control Planes, based on the upstream *HyperShift* (TP)
- External DNS Operator
- Composable OpenShift
- FedRAMP High for Compliance Operator
- Disconnected Mirroring Workflow
- Auto upgrades for failed Operator Installs
- NVIDIA AI Enterprise w/ OpenShift supported on public clouds
- Windows Server 2022 workers for WinC
- Custom Metric Pod Autoscaler, based on upstream *KEDA*



What's New in OpenShift 4.11

OpenShift 4.11

INSTALLER FLEXIBILITY

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

AUTOMATED OPERATIONS

FedRAMP High for Compliance Operator

Disconnected Mirroring Workflow

Automatic upgrades for failed operator installations

WORKLOAD EXTENSIBILITY

NVIDIA AI Enterprise with OpenShift now supported on public clouds

Windows Server 2022 workers for WinC

Custom Metric Pod Autoscaler (KEDA)

7

Kubernetes 1.24

As part of the OpenShift update to 4.11, it will be basing changes on the Kubernetes and CRI-O versions of 1.24. This is following the typical model of releasing a few months after K8s is in GA, which is to allow specific changes to be pulled in and internally verified for security and compatibility.

From K8s 1.24, there are several major new features being brought over:

- gTPC startup, liveness, and readiness probes
- CSI Volume Expansion and Storage capacity tracking interfaces
- Azure Disk and OpenStack Cinder in-tree to CSI plugin migration
- Mixed Protocol support for *“type: Loadbalancer”* Services

There were numerous other updates in 1.24, so please check the main documentation for an idea of what to expect.

Top RFEs included in 4.11

Like many software products, RH accepts RFEs, or Requests for Enhancement, from their customers. These are added in each minor release. 4.11 is no different, including 43 total RFEs. Some of the Notable inclusions are as follows:

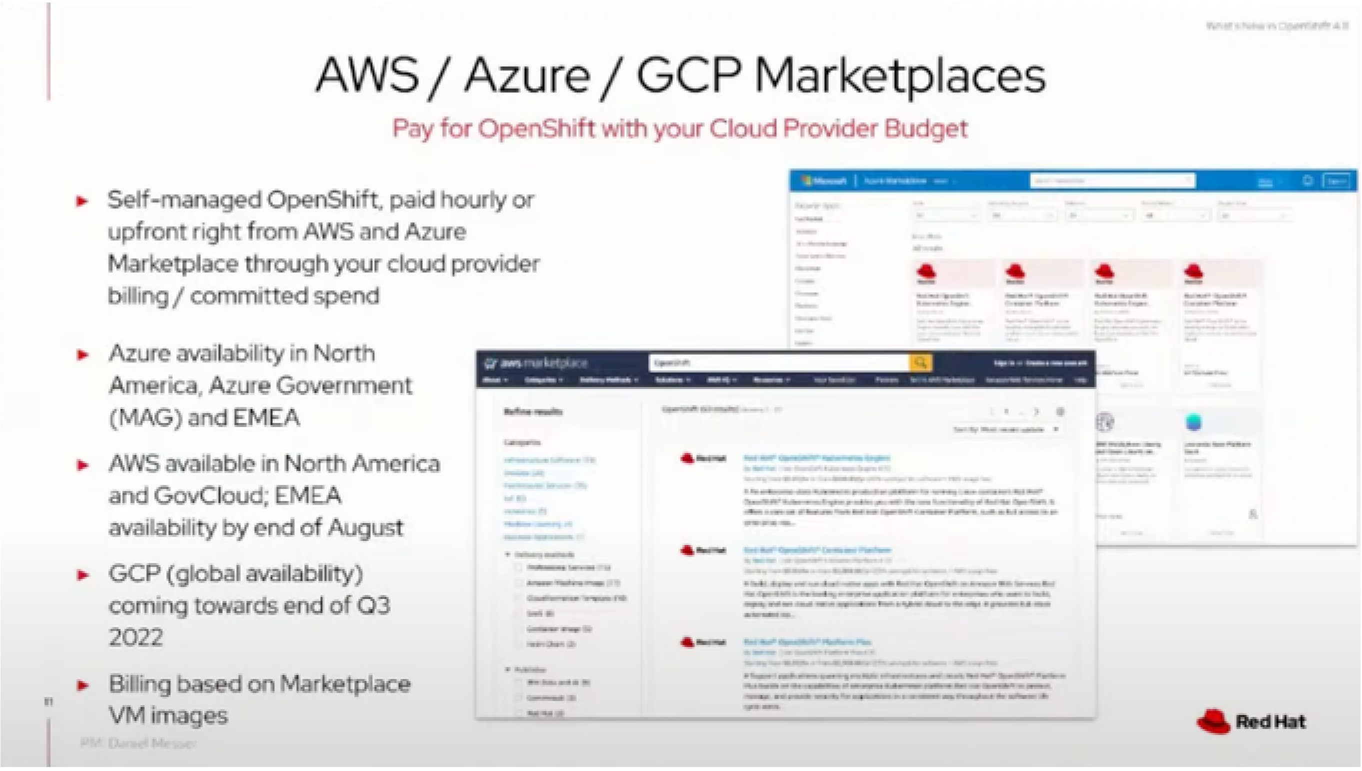
- Default Subdomain for routes at Project/Namespace level
  - With Project/Namespace level router sharding being a common deployment model, now all routes in a shard will default to a specific subdomain which can be different than the cluster default.
  - IE, if the cluster default for apps is *apps.bop-cluster.boxboat.com*, and there is a Project for GitLab, that Project could be configured for default routes at *gitlab.bop-cluster.boxboat.com*.
- Kerberos support for CoreOS nodes as now part of the RHEL CoreOS extensions functionality.
- Expose port configuration to the ingress operator
  - This allows multiple ‘routers’ to run on different ports on a single node.

Update Spotlights

That already looks like quite a bit of important updates! But some of the Technical Updates from above deserve expanding upon them further, so let’s do that here with the **Update Spotlights**!

AWS / Azure / GCP Marketplaces

Starting with 4.11, self-managed OCP can be paid hourly or upfront directly to the cloud provider with all other services, and only for time used.



What's New in OpenShift 4.11

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

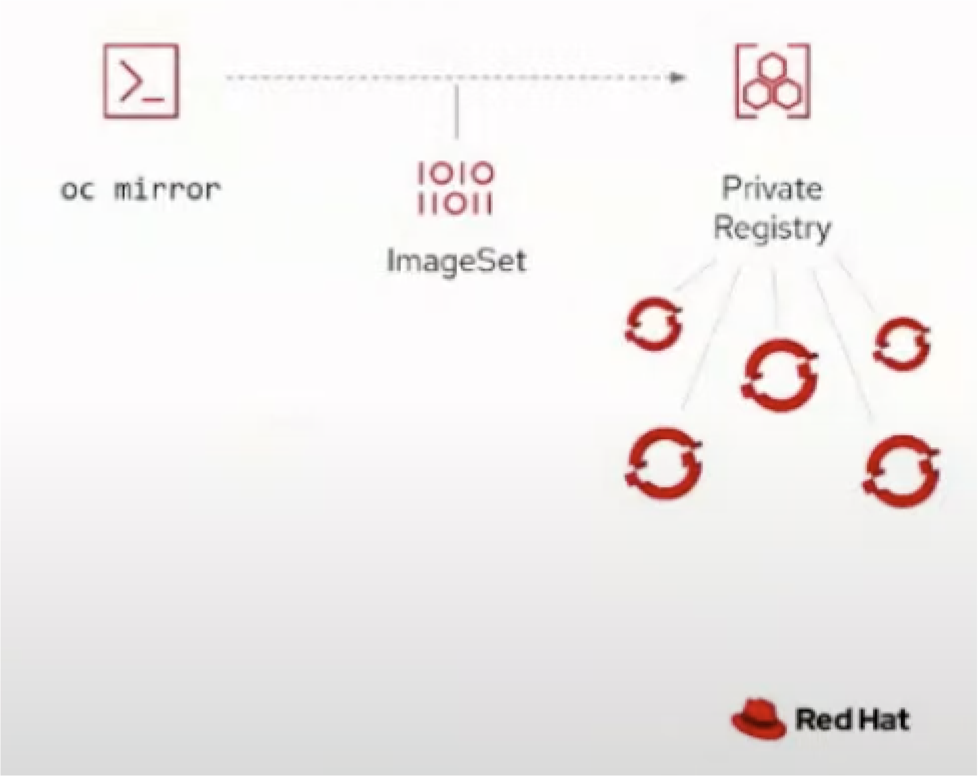
11

PM: Daniel Messer

Disconnected Mirroring Workflow

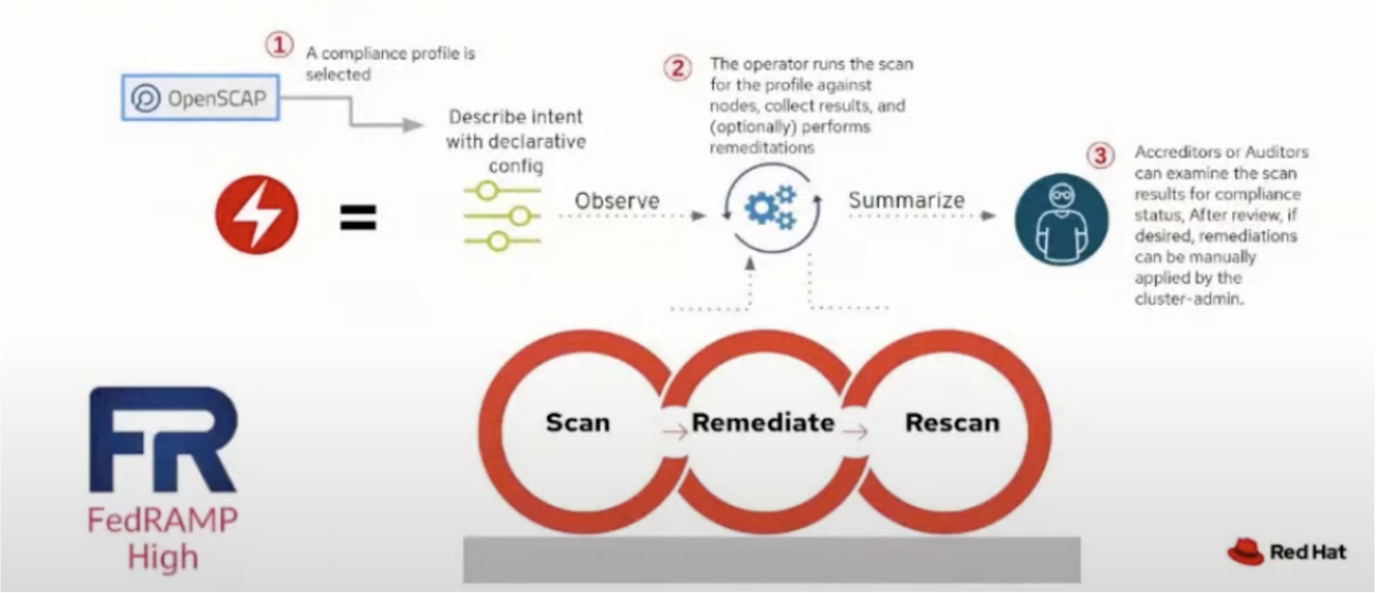
Due to the inherent security of OCP, among many other features, it is common to find OpenShift deployed in disconnected environments. Previously, this required a Bastion host within the private network from which all install files and configs would be transferred to manually. With 4.11, this is being simplified to a single command to manage OCP content in disconnected environments - *oc mirror.*

- **Automated** - detects new releases or pre-determined OCP & Operator versions when regularly run.
- **Smart** - content is downloaded incrementally and dependencies are auto-resolved.
- **Declarative** - file-based configuration with granular filtering



FedRAMP High for Compliance Operator

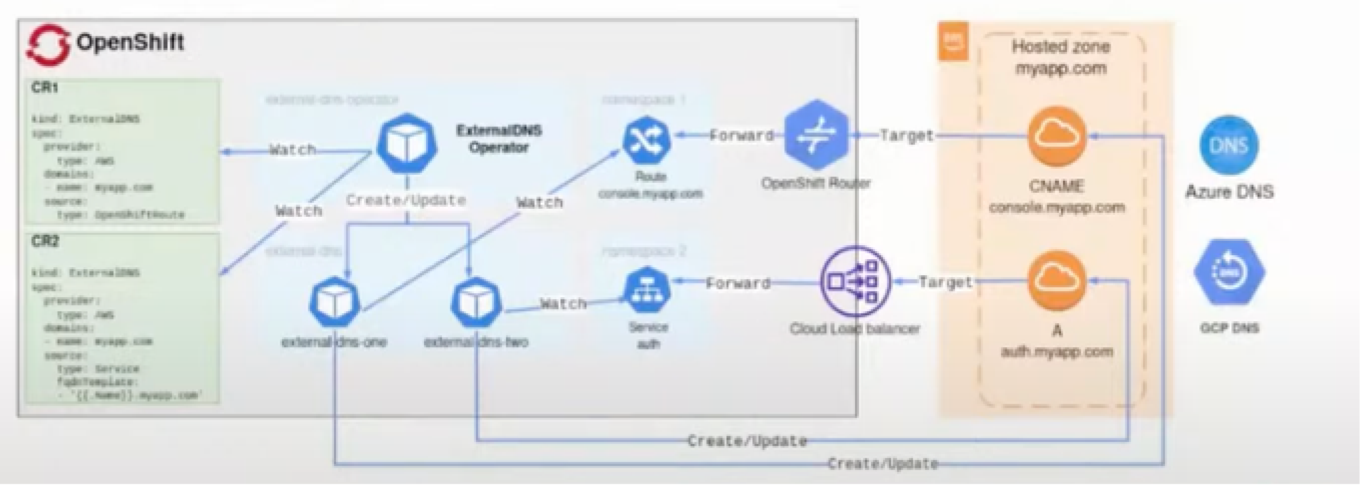
With the US State and Federal (especially DoD) Government’s proclivity for OCP, the ability to operate effectively in FedRAMP High is a necessity. 4.11 brings the ability to Scan, Report, and Remediate Compliance issues with the new FedRAMP High Profile.


① A compliance profile is selected
OpenSCAP
Describe intent with declarative config
② The operator runs the scan for the profile against nodes, collect results, and (optionally) performs remeditations
③ Accreditors or Auditors can examine the scan results for compliance status, After review, if desired, remediations can be manually applied by the cluster-admin.
=
Observe
Summarize
Scan
Remediate
Rescan
FR
FedRAMP High
Red Hat

External DNS

In OCP 4.11, External DNS is entering GA for several cloud services including: AWS Route53, GCP Cloud DNS, and Azure DNS.

The External DNS Operator, available via the OCP Operator Hub, allows dynamic control of an external DNS server’s records via CRD while remaining DNS provider-agnostic. This is vital for continuing the push to centralize all resources needed within a DevSecOps environments and administrating them with or through OCP.



CR1

```
kind: ExternalDNS
spec:
  provider:
    type: AWS
  domains:
  - name: myapp.com
  source:
    type: OpenShiftRoute
```

CR2

```
kind: ExternalDNS
spec:
  provider:
    type: AWS
  domains:
  - name: myapp.com
  source:
    type: Service
    fqdnTemplate:
    - '{{.Name}}.myapp.com'
```

Custom Metric Autoscaler (TP)

CMA is an optional native integration within OCP which can scale workloads horizontally based on custom metrics. Following the patterns of most other OpenShift integrations, CMA is based on a CNCF project, KEDA.

KEDA, and thus CMA, is an event based scaler for Kubernetes. This will allow OCP to dynamically scale workloads based on specific metrics from services such as Prometheus, AMQ/Kafka, etc. CMA will also scale applications to 0, saving resources until a specific workload is ready to be run. It also will register itself as k8s Metric Adapter, and will provide metrics for HPA scaling.

Console Cluster Upgrades

Partial Control Plane Upgrades

- Choose between full or partial upgrade, w/ 60 days to complete
- May pause upgrades per machine pool

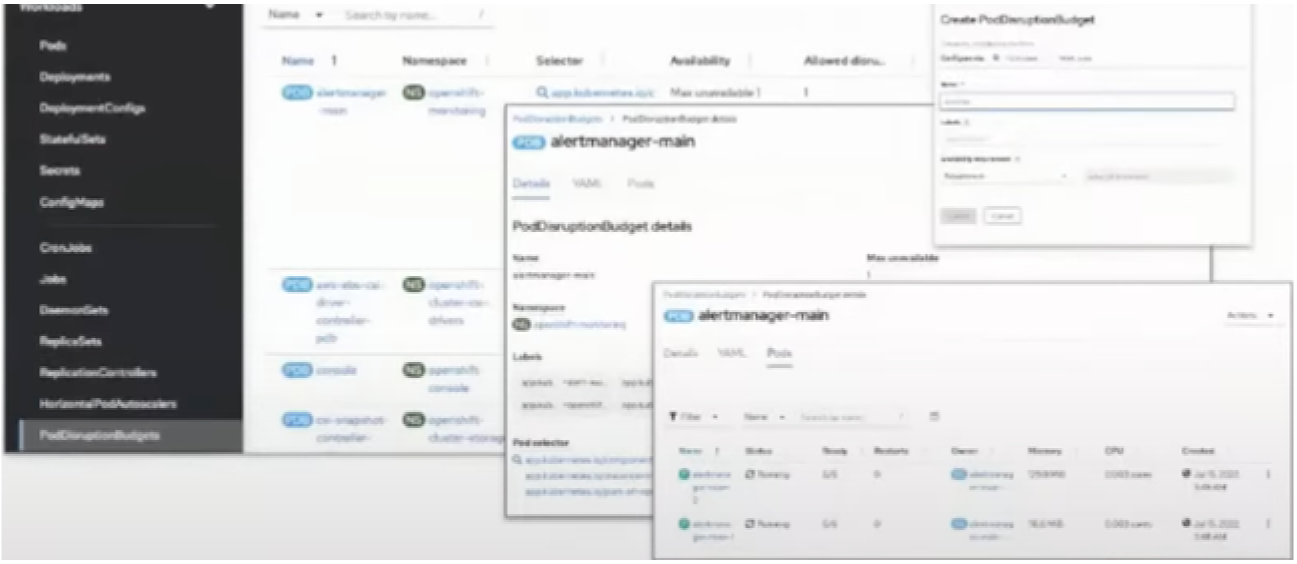
Conditional Upgrades

- “Supported but not recommended” toggle

Pod Disruption Budget

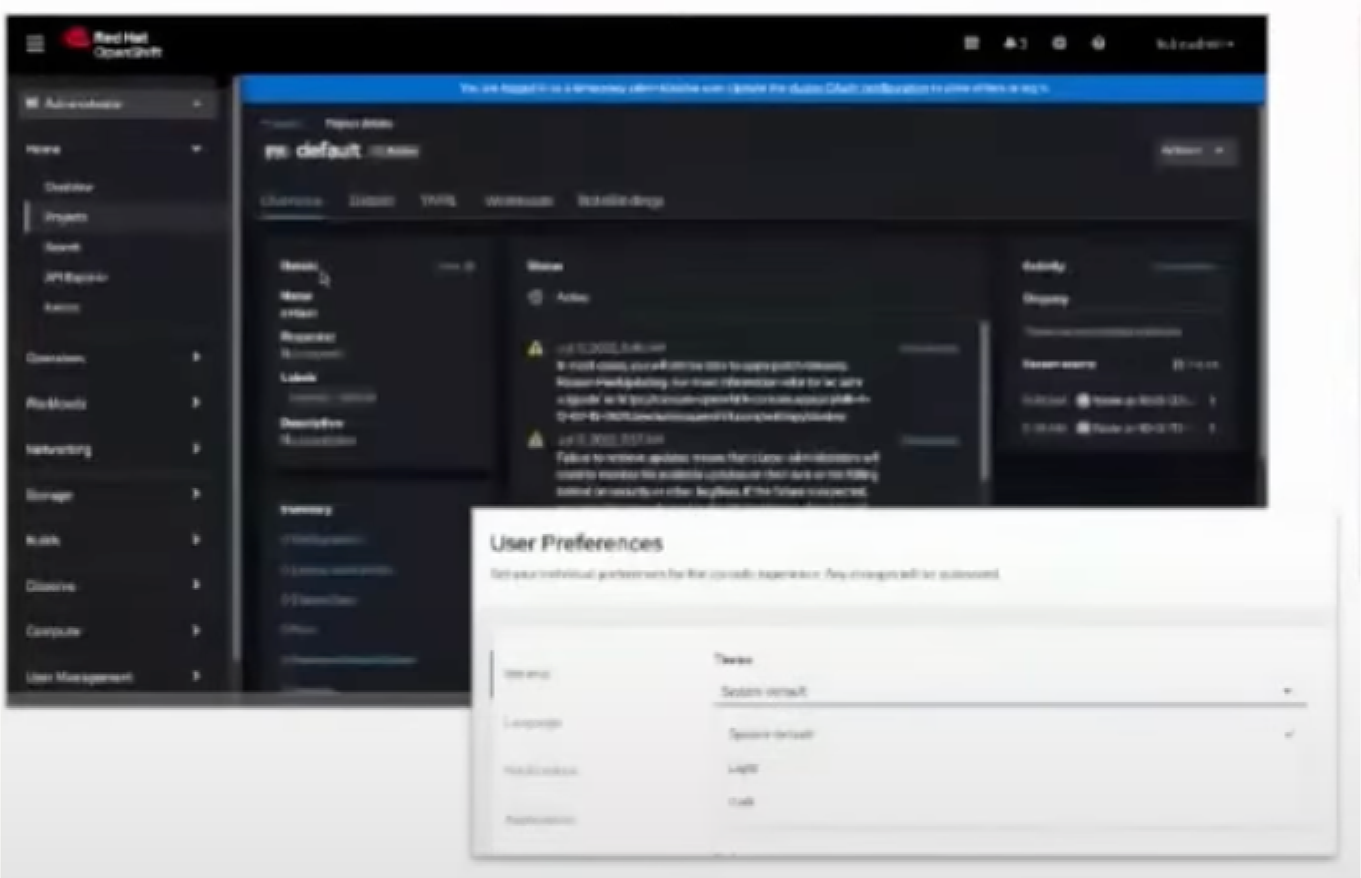
This adds a new UI to the Console under Workloads - PodDisruptionBudgets.

- Form/YAML creation
- View PDBs in context of single project or all projects
- View pods per PDB
- Link to related PDB added to Workload Details
- PDB’s can be created directly from the Workloads' actions menu under Details



Customer Experiences

Dark Mode!!!



Personally, I’m a huge Dark Mode fan, and the OCP console is one of the few views on my displays stilling blinding me; not anymore! With 4.11, User’s can now choose Dark mode, or take the System Default as is common with most software.

More Form Based Experiences

Forms are a huge QoL enhancement when configuring objects within OCP, or even for generating YAML. However, several areas are still lacking this functionality. 4.11 will be introducing Forms to the following:

- Routes
- ConfigMaps

Web Terminal Updates

As you probably know, starting in OCP 4.7, the web terminal has been included within the console with several pre-installed CLIs, such as *oc, kubectl, helm, tkn*, etc. This is an optional integration which provides a terminal icon in the Console tool bar that, upon clicking, creates a terminal within a set project and auto-logs in via the user’s credentials. The following enhancements are being added in 4.11:

- help - list the pre-installed CLIs w/ versions
- wtoctl - customize the terminal with any additional CLI images the user desires, plus others.
- Multiple tabs - there are now up to 8 tabs within the terminal session

Platform Services

OpenShift Builds

Jenkins Removed from OCP Payload

- Jenkins will now move to a separate repo, decoupling from the main build
- Being decoupled from OpenShift versions, fixes and CVEs for Jenkins can be made separate from OpenShift.

Shared Resources CSI Driver

- Shared secrets and configmaps
- Utilizes volumes and CRDs to allow finer control over access to these resources, including revocation.
- Admins can provide sensitive info to other users and applications while maintain least privilege.

OpenShift Pipelines

- Pipelines 1.8
- Tekton Hub now supports External databases
- Pipelines on Arm architecture (TP)
- Pipelines as code enhancements
  - Trigger multiple pipelines for single Git event
  - GitLab and BitBucket support
  - Webhook configuration via CLI
  - Manual and 3rd party triggers
- Dev console
  - Configure Git repositories w/ Pipelines as code
  - Create GH app

OpenShift GitOps

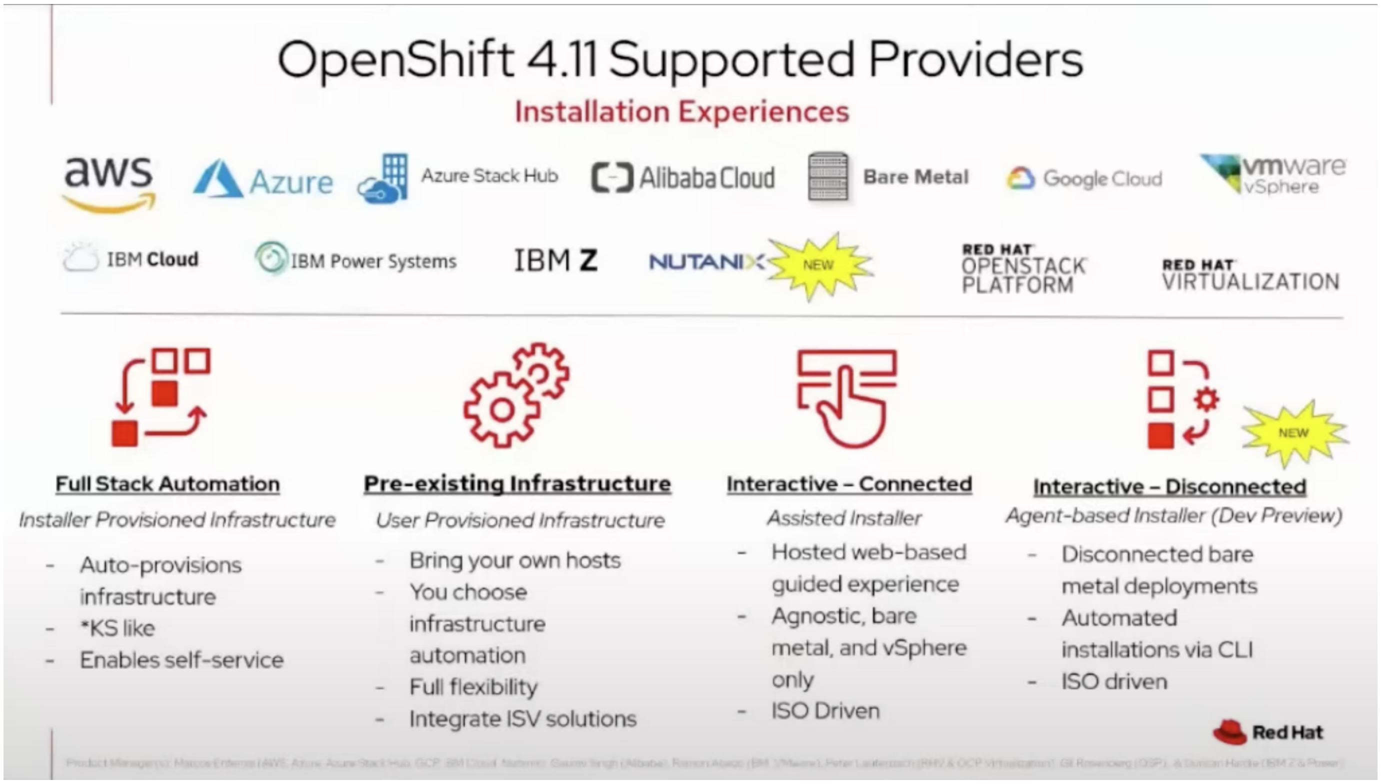
- OpenShift GitOps 1.6 (based on ArgoCD 2.4)
- ApplicationSets (GA)
- Notifications - ie Health Degraded (TP)
- Custom Plugins - utilize tooling not part of Argo core, ie new package versions, SOPs, etc.
- IBM Power and Z architecture support

OpenShift Service Mesh

- OCP SM 2.2, based on Istio 1.12 and Kiali 1.48
- Service Mesh w/ federation is now supported on ROSA
- Includes WasmPlugin API from Istio 1.12
- Kiali updates
  - Several improved functions for managing large service meshes, such as Improved views.
  - Ability to view internal certification info.

- Istio TP Features
  - Kubernetes Gateway API
  - AuthPolicy “dry run”
  - gRPC “Proxyless” service mesh

Installer Flexibility



OpenShift 4.11 Supported Providers

Installation Experiences

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

Product Manager(s): Marcos Entenza (AWS, Azure, Azure Stack Hub, GCP, IBM Cloud, Nutanix), Gaurav Singh (Alibaba), Ramon Acedo (IBM, VMware), Peter Lauterbach (RHV & OCP Virtualization), Gil Rosenberg (OSP), & Duncan Hardie (IBM Z & Power)

Azure, AWS, and vSphere Enhancements

Azure

- Support for Azure ultra disks
- User-managed encryption keys
- Support for accelerated networking

AWS

- secret region and EFA support
  - IPI and UPI support for **us-isob-east-1** Secret Commercial Cloud Services Region

VMware vSphere

- External load balancers supported with IPI deployments for external API/ingress traffic

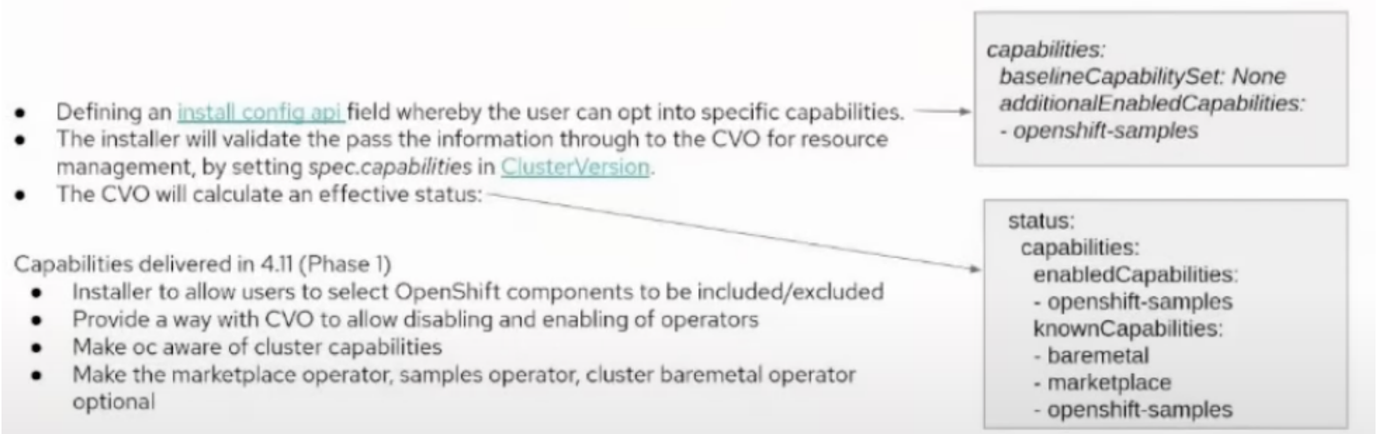
Agent-based Installer for Disconnected OCP Deployments

While OCP’s highly-opinionated deployment model is one of its perks in many environments, when it comes to Disconnected deployments, it can add considerable complexity. So, the new Agent-based Installer was created to simplify these deployments. This uses a bootable image for in-place bootstrapping without the need for a Bastion. Other features of the Agent are as follows:

- Air-gapped deployments are now supported
- Use of a mirrored local registry
- Leverages the Assisted Installer (AI) engine
- SNO, compact, and HA topologies
- Allows usage of user-provided automation tooling for install

Composable OpenShift

As mentioned above, OCP is deployed in a highly opinionated manner, with numerous integrations chosen to enable operations from Day 1. However, there are situations where a user might want to customize these integrations. OpenShift has allowed a degree of customization of the Ignition configs via Butane, however these were still limited. 4.11 allows disabling the installation of: **Baremetal Operator**, **marketplace**, and the **openshift-samples content** in the openshift namespace.



- 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

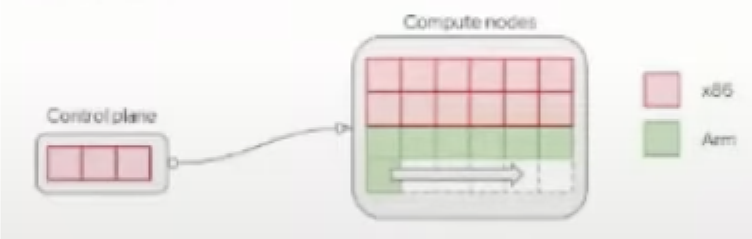
```
capabilities:
  baselineCapabilitySet: None
  additionalEnabledCapabilities:
  - openshift-samples
```

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

ARM and Heterogenous

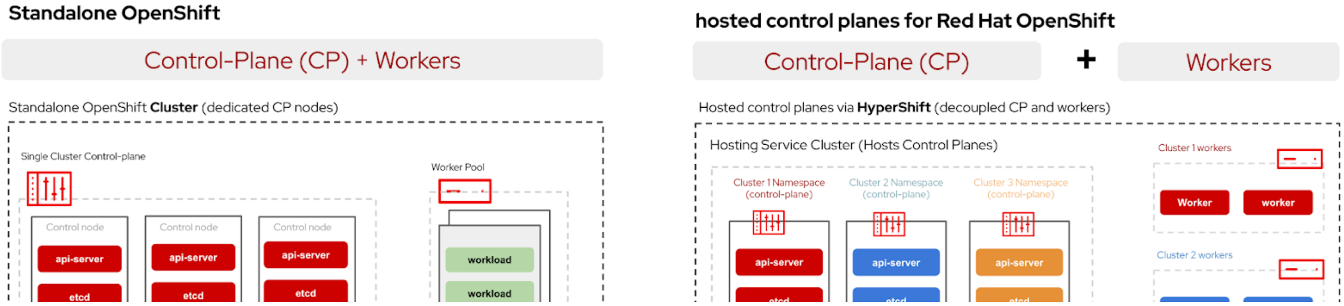
Like many other vendors in the industry, Red Hat is continuing the push towards ARM support for OpenShift.

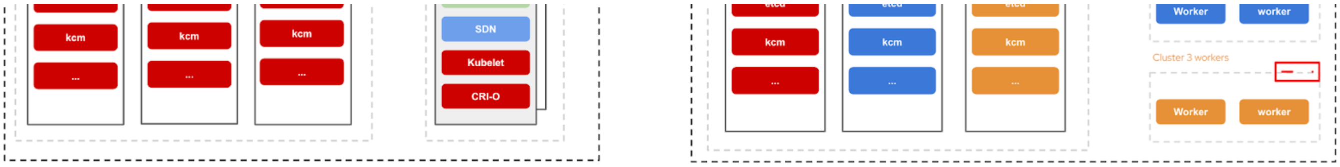
- New supported ARM platforms and deployments
  - AWS pre-existing Infrastructure (UPI)
  - Bare Metal Full Stack Automation (IPI)
  - Disconnected Install
- Additional Storage options
  - Local Storage Operator
  - iSCSI
  - Raw Block
  - MultiPath and HostPath
- Heterogeneous Cluster (TP)
  - Add ARM compute nodes to x86 cluster as day 2 operation
  - Only on Azure currently
  - Source payload from nightlies



Hosted Control Planes (TP)

Based on the newly developed upstream project HyperShift, Hosted Control Planes is an entirely new architecture for deploying OpenShift clusters. Rather than the traditional method of a coupled control plane and data plane per cluster, Hosted Control Planes provides the option to separate the 2; in this model, a separate cluster provides control planes to numerous “worker” clusters via a shared interface.


Standalone OpenShift
Control-Plane (CP) + Workers
Standalone OpenShift Cluster (dedicated CP nodes)
Single Cluster Control-plane
Control node
api-server
etcd
Control node
api-server
etcd
Control node
api-server
etcd
Worker Pool
workload
workload
hosted control planes for Red Hat OpenShift
Control-Plane (CP)
+
Workers
Hosted control planes via HyperShift (decoupled CP and workers)
Hosting Service Cluster (Hosts Control Planes)
Cluster 1 Namespace (control-plane)
api-server
etcd
Cluster 2 Namespace (control-plane)
api-server
etcd
Cluster 3 Namespace (control-plane)
api-server
etcd
Cluster 1 workers
Worker
worker
Cluster 2 workers



The technology is extremely interesting, but why is it necessary? One reason is the growing need for distributed, hybrid clusters vs 1-2 large clusters. RHACM was the initial answer to this movement, providing a single pane of glass and various tools for multi-cluster management. The Hosted Control Planes model extends this by further reducing the cost, complexity, and time to deploy new worker clusters. For more information, or if you'd like to try Hosted Control Planes yourself, see RH's recent Blog post on the subject!

Summary

And that concludes this 1st segment of OpenShift 4.11! In Part 2, we will review the updates on the OpenShift Control Plane, Observability /Monitoring, Network/Routing, and Telco 5G. Stay tuned, there are some very exciting updates there!

If you can't wait, or you'd like to hear RH's takes on the 4.11 update, go watch their recorded live stream. They should also update their What's New in OpenShift page soon with the video and Slides.

Lastly, if you can't wait for the GA release of 4.11 to try Dark mode or other exciting updates, remember that you can always upgrade early! Just change your cluster release channel to *4.11-fast* and let the cluster perform the updates.

> While *4.11-fast* is close to GA, it is not an officially supported release. Therefore, absolutely do not perform this update in production, or anywhere else where downtime is unacceptable. Also, remember that your cluster must be in good health in order to perform an automated update!

If you would like to try out OpenShift yourself, check out the new page Trying OpenShift for the many options available to you. And if you have any questions, feel free to reach out to the OpenShift Practice on Slack at #eng-openshift, or email me directly at nmiethe@boxboat.com.