
Red Hat
IBM

Installation of OCP

OpenShift Architecture Workshop for IBM Nordics

Alfred Bach
PESA RedHat EMEA
abach@redhat.com

Red Hat | IBM

Installation Paradigms

OPENSHIFT CONTAINER PLATFORM

Full Stack Automated (IPI)

Simplified opinionated "Best Practices" for cluster provisioning

Fully automated installation and updates including host container OS.

Red Hat Enterprise Linux CoreOS

Pre-existing Infrastructure (UPI)

Customer managed resources & infrastructure provisioning

Plug into existing DNS and security boundaries

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux

HOSTED OPENSHIFT

Red Hat OpenShift on IBM Cloud * (ROKS)

Deploy directly from the IBM Cloud console. An IBM service, master nodes are managed by IBM Cloud engineers.

Azure Red Hat OpenShift ** (ARO)

Deploy directly from the Azure console. A MSFT service, jointly managed by Red Hat and Microsoft

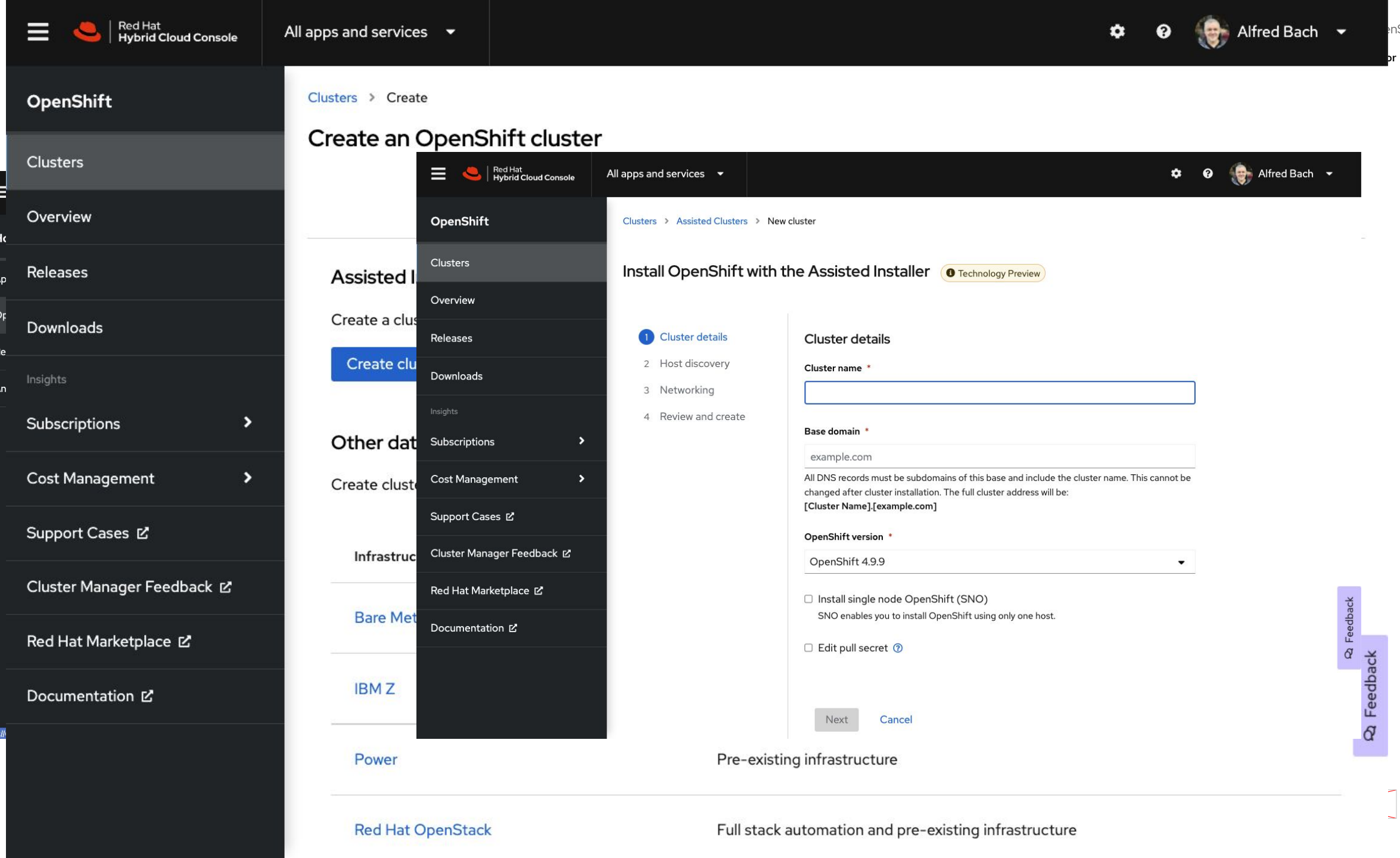
OpenShift on AWS (ROSA)

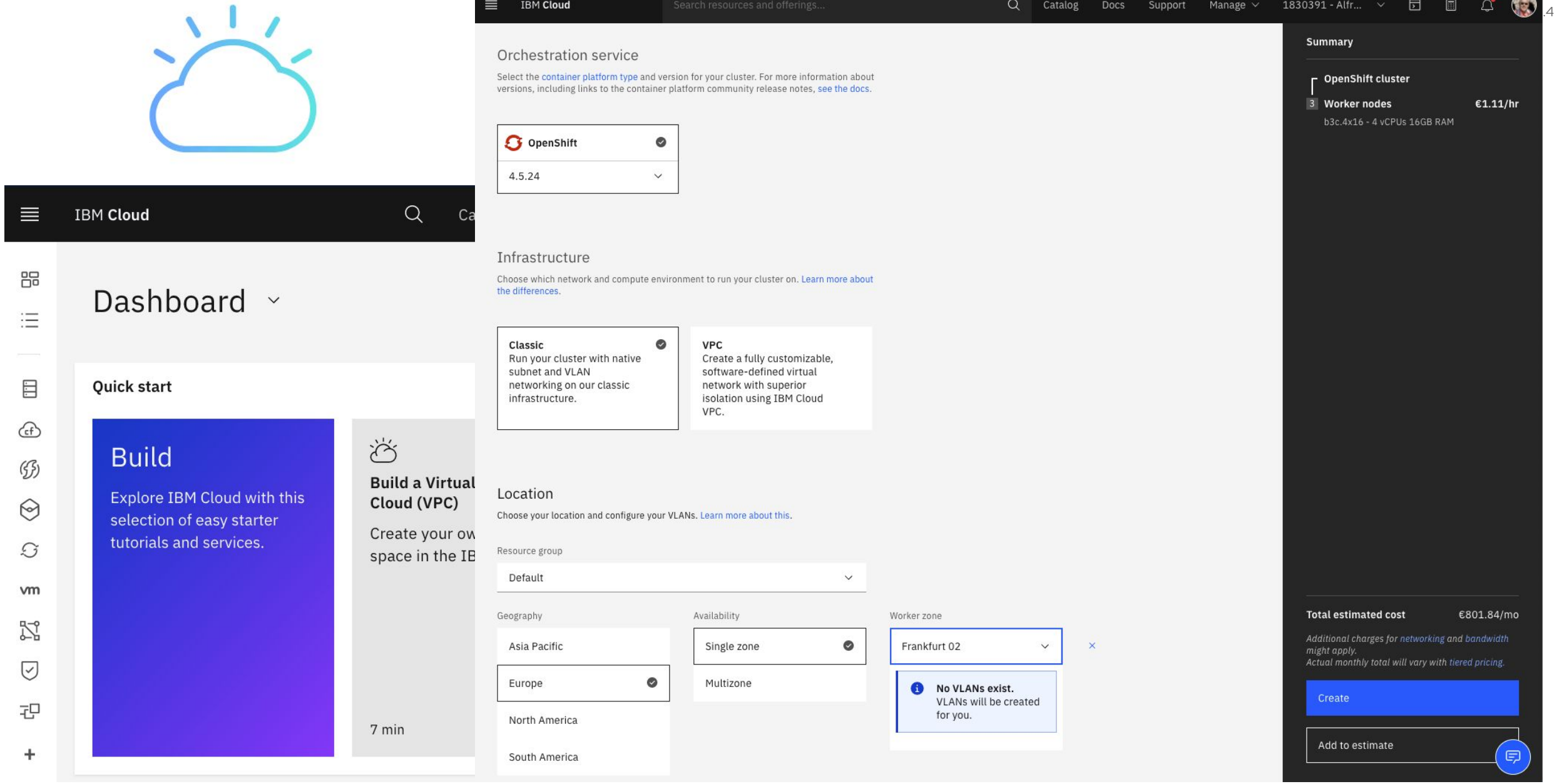
Get a powerful cluster, fully managed by Red Hat engineers and support; a Red Hat service.

* Based on OCP v4.3 GA slated for March; public beta available now

** Entitlements of OCP obtained through a Cloud Pak purchase are not transferable to these environments

Hosted OpenShift


Red Hat
Hybrid Cloud Console
All apps and services
Alfred Bach
OpenShift
Clusters
Overview
Releases
Downloads
Insights
Subscriptions
Cost Management
Support Cases
Cluster Manager Feedback
Red Hat Marketplace
Documentation
Clusters > Create
Create an OpenShift cluster
Clusters > Assisted Clusters > New cluster
Install OpenShift with the Assisted Installer
Technology Preview
1 Cluster details
2 Host discovery
3 Networking
4 Review and create
Cluster details
Cluster name *
Base domain *
example.com
All DNS records must be subdomains of this base and include the cluster name. This cannot be changed after cluster installation. The full cluster address will be:
[Cluster Name].[example.com]
OpenShift version *
OpenShift 4.9.9
Install single node OpenShift (SNO)
SNO enables you to install OpenShift using only one host.
Edit pull secret
Next
Cancel
Feedback
Power
Pre-existing infrastructure
Red Hat OpenStack
Full stack automation and pre-existing infrastructure


IBM Cloud
Search resources and offerings...
Catalog
Docs
Support
Manage
1830391 - Alfr...
Dashboard
Quick start
Build
Explore IBM Cloud with this selection of easy starter tutorials and services.
Build a Virtual Cloud (VPC)
Create your ow space in the IB
7 min
Orchestration service
Select the container platform type and version for your cluster. For more information about versions, including links to the container platform community release notes, see the docs.
OpenShift
4.5.24
Infrastructure
Choose which network and compute environment to run your cluster on. Learn more about the differences.
Classic
Run your cluster with native subnet and VLAN networking on our classic infrastructure.
VPC
Create a fully customizable, software-defined virtual network with superior isolation using IBM Cloud VPC.
Location
Choose your location and configure your VLANs. Learn more about this.
Resource group
Default
Geography
Asia Pacific
Europe
North America
South America
Availability
Single zone
Multizone
Worker zone
Frankfurt 02
No VLANs exist.
VLANs will be created for you.
Summary
OpenShift cluster
3 Worker nodes
€1.11/hr
b3c.4x16 - 4 vCPUs 16GB RAM
Total estimated cost
€801.84/mo
Additional charges for networking and bandwidth might apply.
Actual monthly total will vary with tiered pricing.
Create
Add to estimate

OpenShift Container Platform (OCP)

OpenShift 4.12 Supported Providers

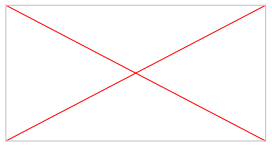
Installation Experiences

aws Outposts

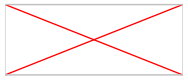
AWS Local Zones

Azure

Azure Stack Hub

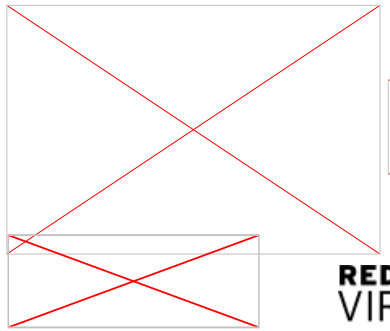


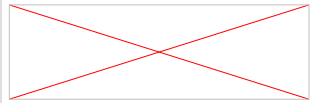
IBM Power Systems



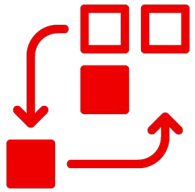
Bare Metal

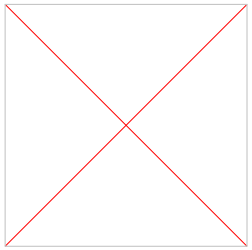
NUTANIX

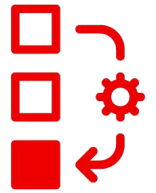




RED HAT VIRTUALIZATION







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

Local – Disconnected

Agent-based Installer

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

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

OpenShift 4.12 Supported Providers & Installation Experiences

Provider	**Full Stack Automation** *Installer-provisioned infrastructure*	**Pre-existing Infrastructure** *User-provisioned infrastructure*	**Interactive – Connected** *Assisted Installer*	**Local – Disconnected** *Agent-based Installer*	**Hosted Control Planes** *(via Multicluster Engine for Kubernetes)*
Alibaba	Technology Preview				
AWS	x	x			Technology Preview
AWS Local Zones		x			
AWS Outposts	x				
Azure	x	x			Developer Preview
Azure Stack Hub	x	x			
Bare Metal	x	x	x	x	Technology Preview
Google Cloud Platform	x	x			
IBM Cloud VPC	x				
IBM Power Systems		x			
IBM Z or LinuxONE		x			
Nutanix AOS	x				
OpenShift Virtualization	Post-installation option	Post-installation option	x		Developer Preview
Red Hat OpenStack Platform	x	x			
Red Hat Virtualization	x	x			
VMware vSphere	x	x	x	x	
Agnostic (untested platform)		x	x	x	

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

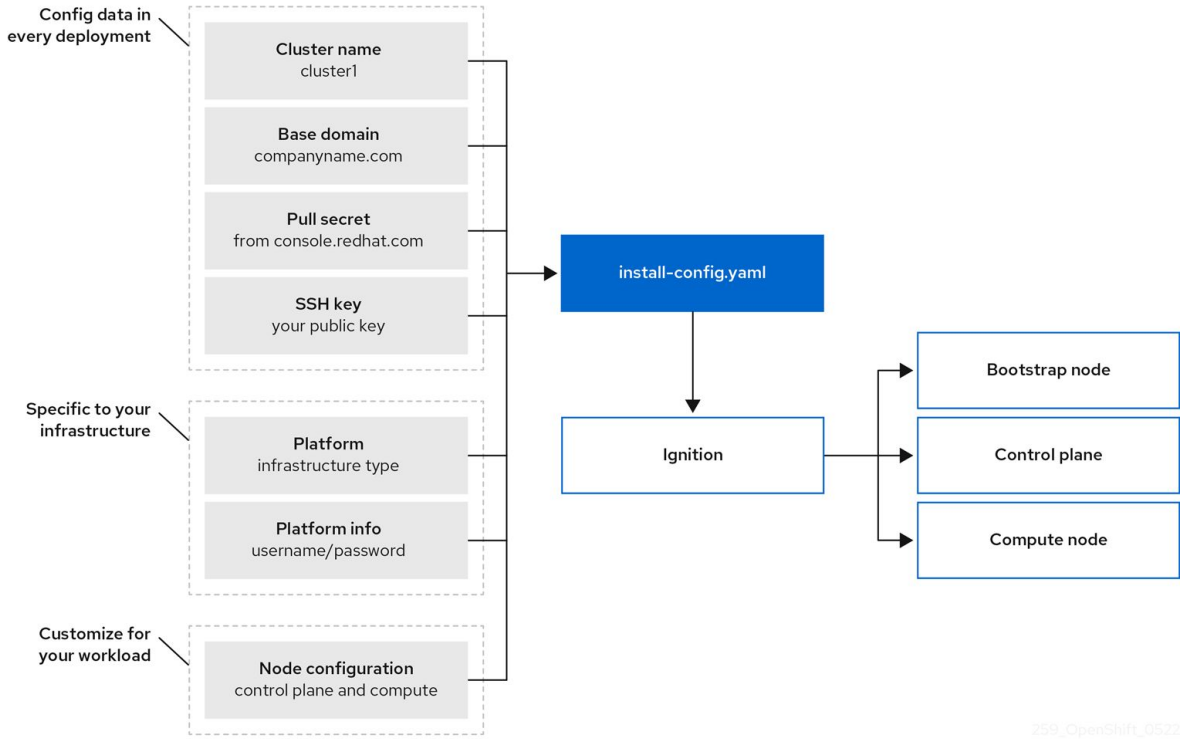
OpenShift 4 installation

Installer and user-provisioned infrastructure, bootstrap, and more

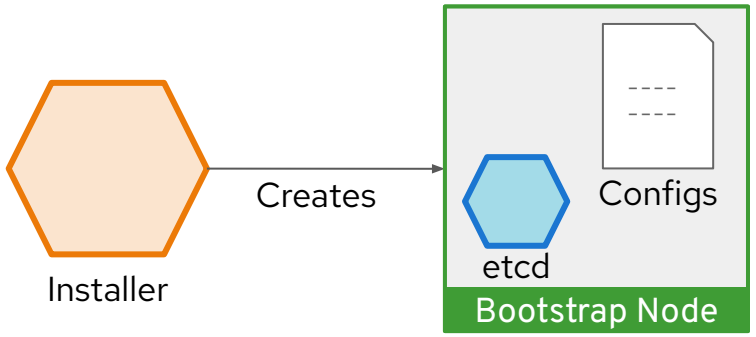
OpenShift Bootstrap Process: Self-Managed Kubernetes

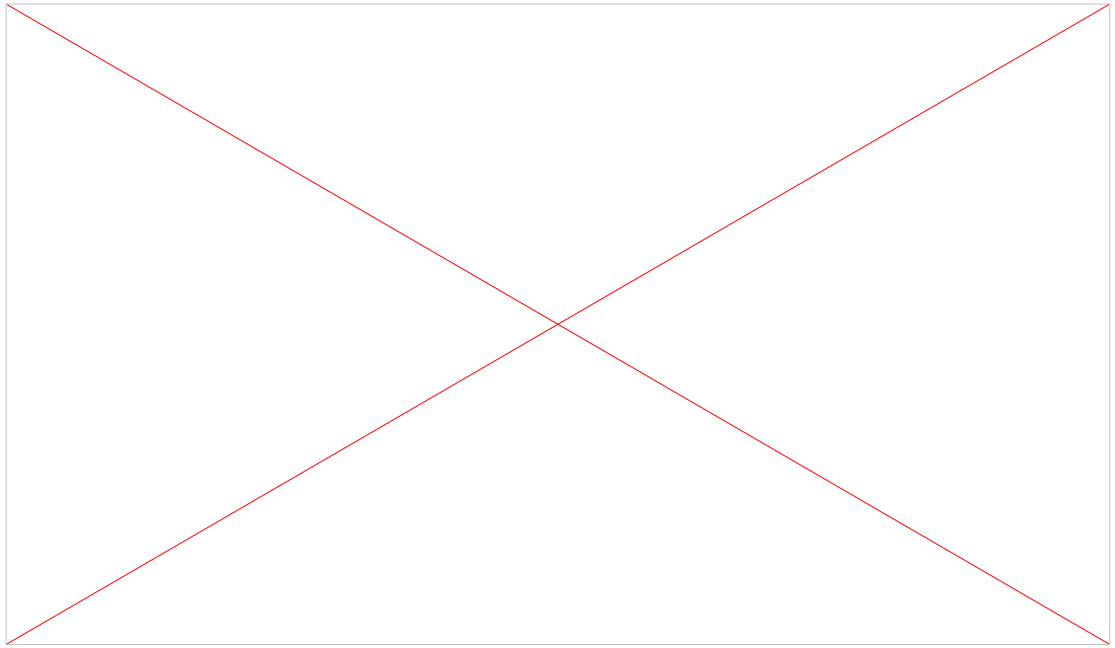
How to boot a self-managed cluster:

- OpenShift 4 is unique in that management extends all the way down to the operating system
- Every machine boots with a configuration that references resources hosted in the cluster it joins enabling cluster to manage itself
- Downside is that every machine looking to join the cluster is waiting on the cluster to be created
- Dependency loop is broken using a bootstrap machine, which acts as a temporary control plane whose sole purpose is bringing up the permanent control plane nodes
- Permanent control plane nodes get booted and join the cluster leveraging the control plane on the bootstrap machine
- Once the pivot to the permanent control plane takes place, the remaining worker nodes can be booted and join the cluster



OpenShift Bootstrap Process: Step by Step

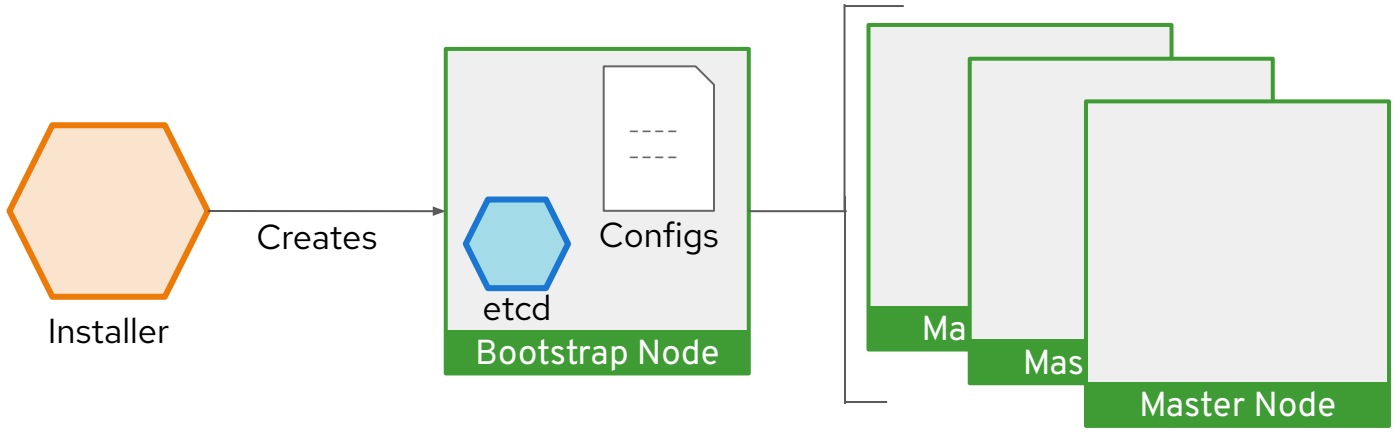




Bootstrapping process step by step:

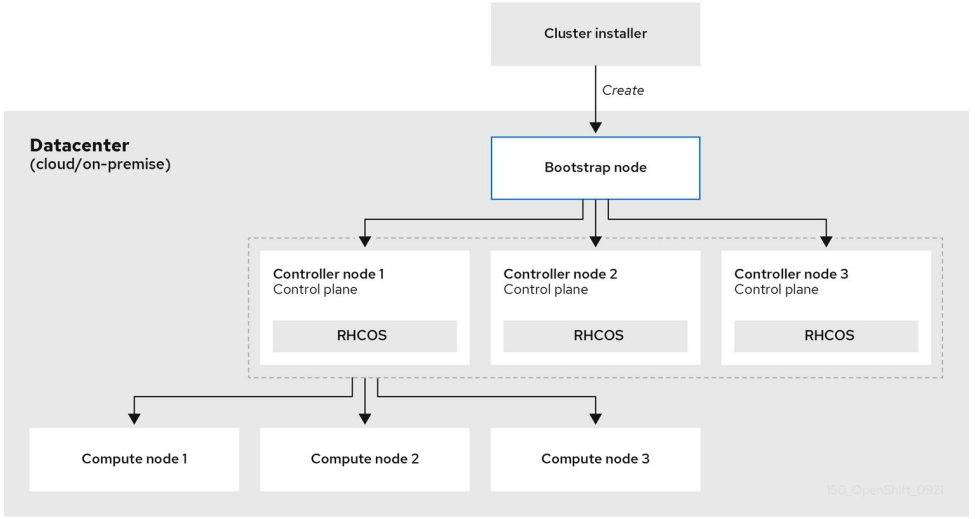
1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd

OpenShift Bootstrap Process: Step by Step

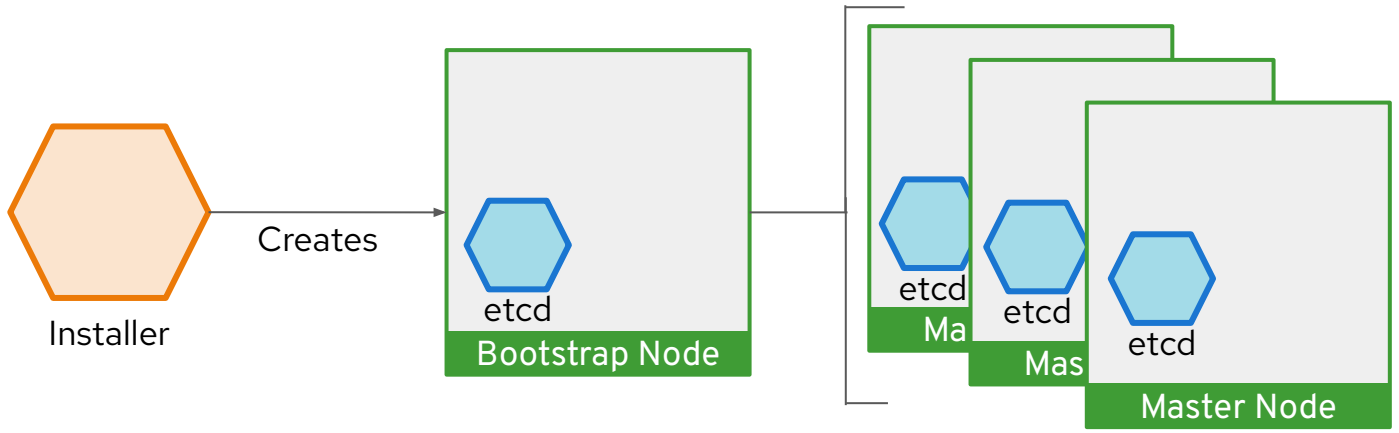


Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd
2. Master machines fetch the remote resources from the bootstrap machine and finish booting.



OpenShift Bootstrap Process: Step by Step

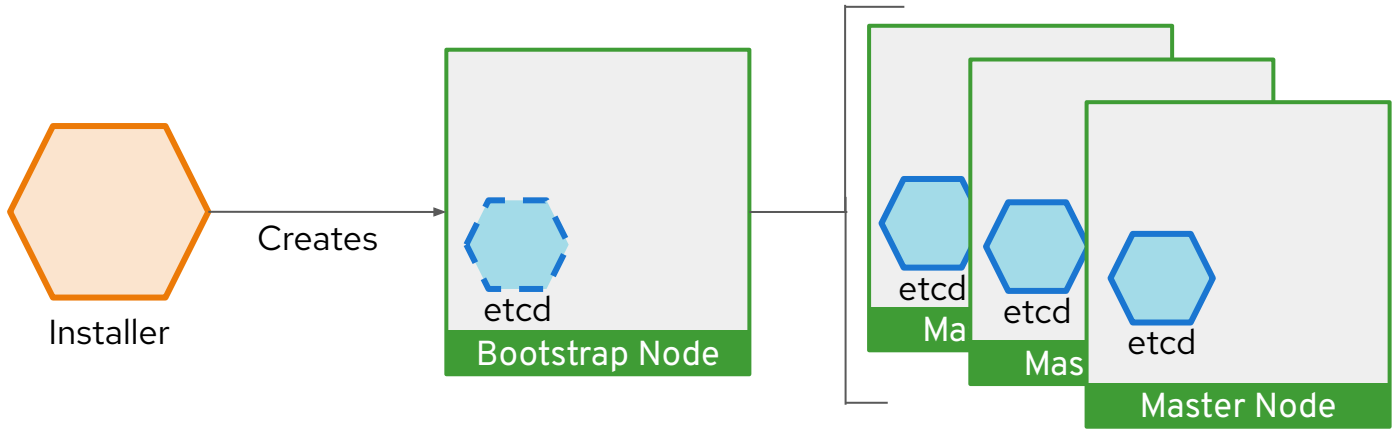


Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd
2. Master machines fetch the remote resources from the bootstrap machine and finish booting.
3. Master machines use the bootstrap node to scale the etcd cluster to 4 total instances.

OpenShift Installation

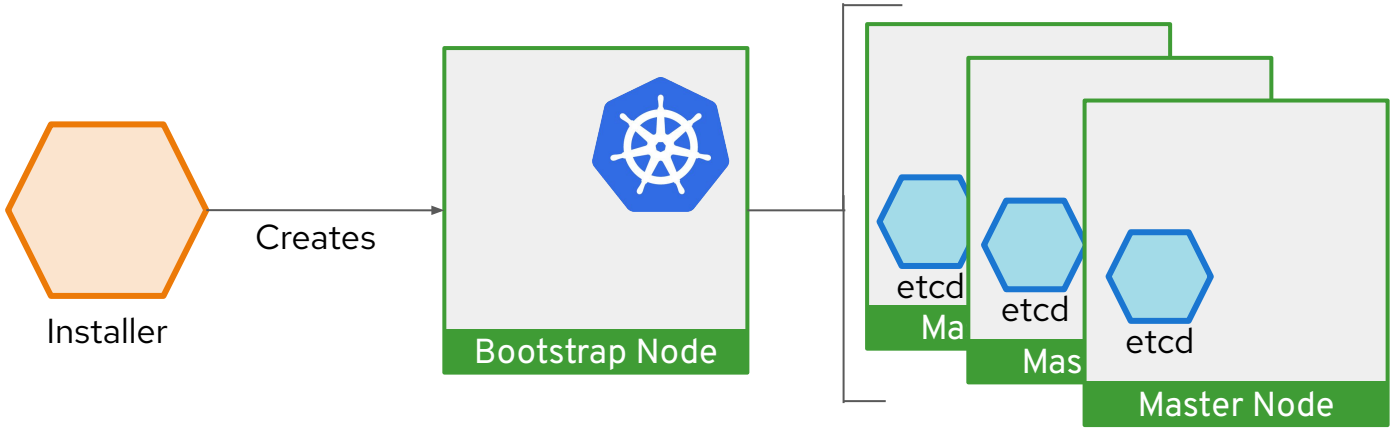
OpenShift Bootstrap Process: Step by Step



Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd
2. Master machines fetch the remote resources from the bootstrap machine and finish booting.
3. Master machines use the bootstrap node to scale the etcd cluster to 4 total instances.
4. The Etcd operator scales itself down off the bootstrap node, leaving the etcd instance count to 3

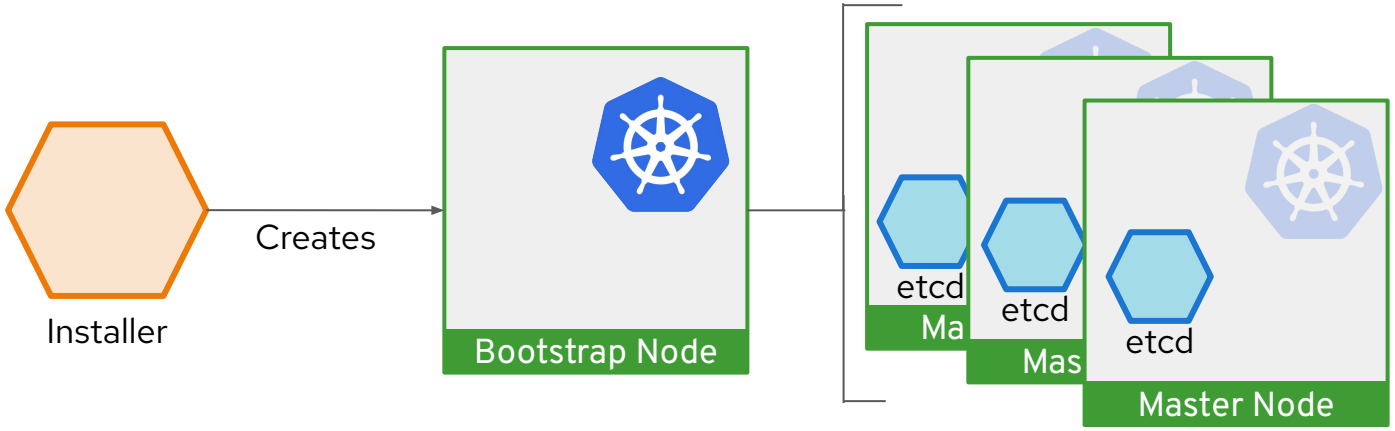
OpenShift Bootstrap Process: Step by Step



Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd
2. Master machines fetch the remote resources from the bootstrap machine and finish booting.
3. Master machines use the bootstrap node to scale the etcd cluster to 3 instances.
4. The Etcd operator scales itself down off the bootstrap node, then scales back up to 3; all on the Masters
5. Bootstrap node starts a temporary Kubernetes control plane using the newly-created etcd cluster.

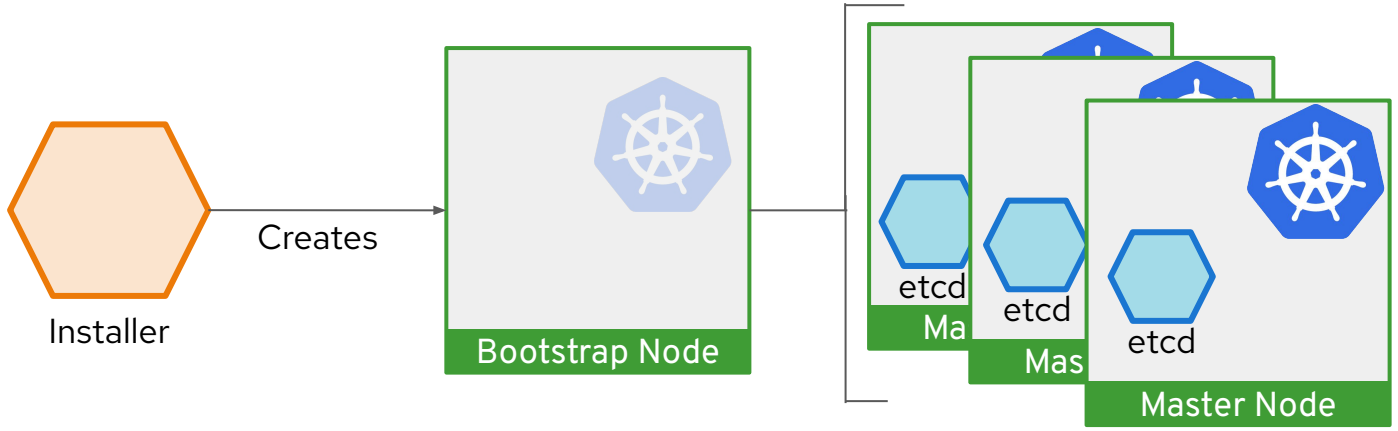
OpenShift Bootstrap Process: Step by Step



Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd
2. Master machines fetch the remote resources from the bootstrap machine and finish booting.
3. Master machines use the bootstrap node to scale the etcd cluster to 3 instances.
4. The Etcd operator scales itself down off the bootstrap node, then scales back up to 3; all on the Masters
5. Bootstrap node starts a temporary Kubernetes control plane using the newly-created etcd cluster.
6. Temporary control plane schedules the production control plane to the master machines.

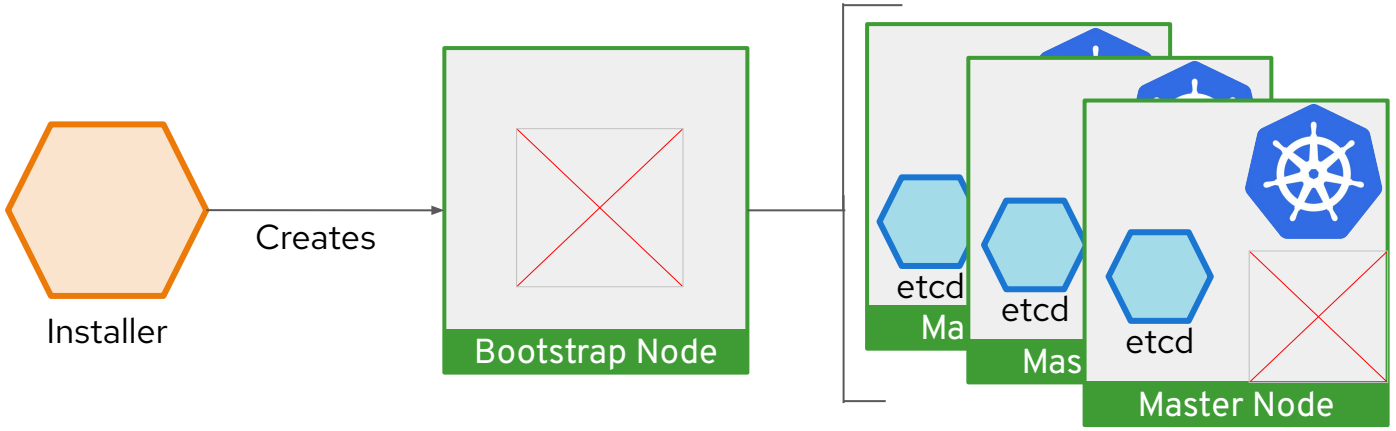
OpenShift Bootstrap Process: Step by Step



Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd
2. Master machines fetch the remote resources from the bootstrap machine and finish booting.
3. Master machines use the bootstrap node to scale the etcd cluster to 3 instances.
4. The Etcd operator scales itself down off the bootstrap node, then scales back up to 3; all on the Masters
5. Bootstrap node starts a temporary Kubernetes control plane using the newly-created etcd cluster.
6. Temporary control plane schedules the production control plane to the master machines.
7. Temporary control plane shuts down, yielding to the production control plane.

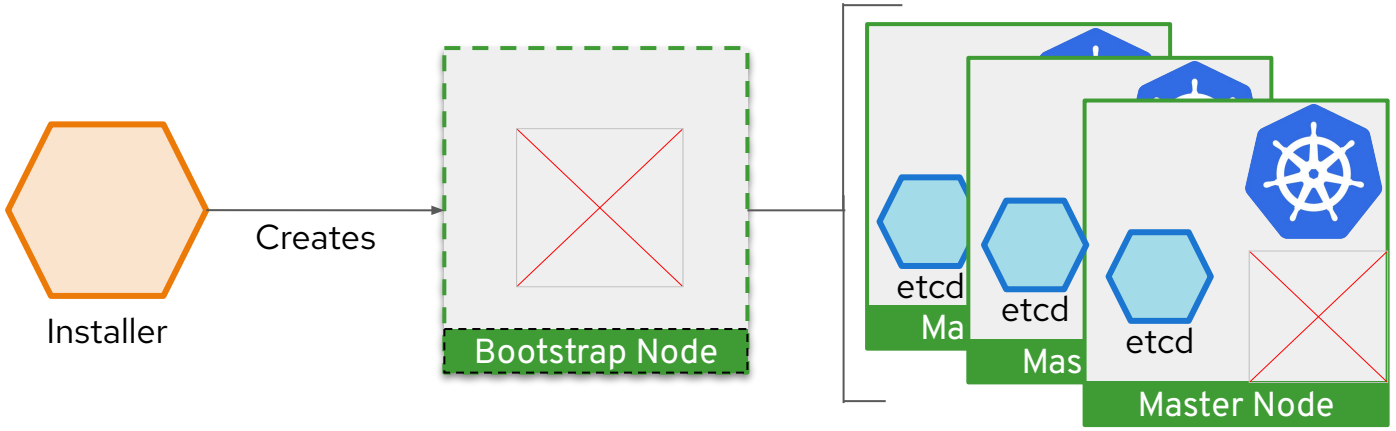
OpenShift Bootstrap Process: Step by Step



Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd
2. Master machines fetch the remote resources from the bootstrap machine and finish booting.
3. Master machines use the bootstrap node to scale the etcd cluster to 3 instances.
4. The Etcd operator scales itself down off the bootstrap node, then scales back up to 3; all on the Masters
5. Bootstrap node starts a temporary Kubernetes control plane using the newly-created etcd cluster.
6. Temporary control plane schedules the production control plane to the master machines.
7. Temporary control plane shuts down, yielding to the production control plane.
8. Bootstrap node injects OpenShift-specific components into the newly formed control plane.

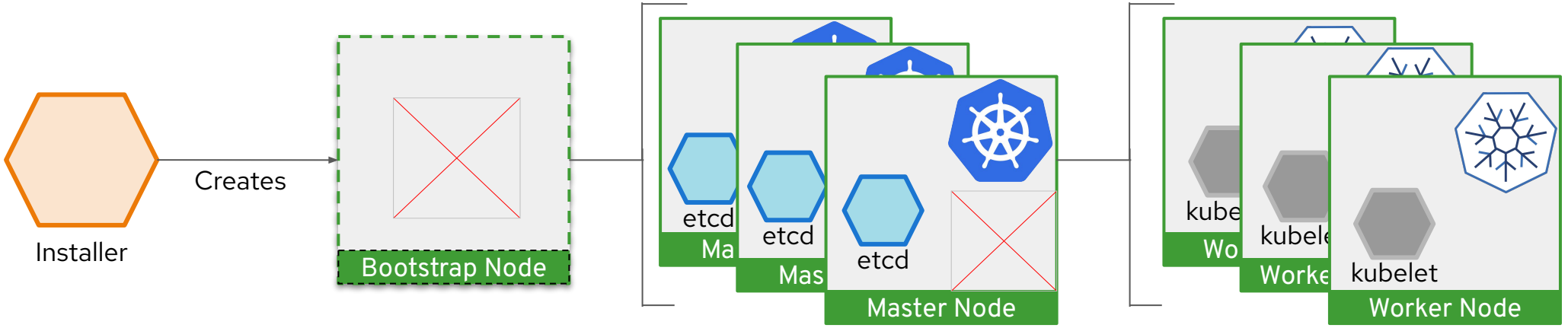
OpenShift Bootstrap Process: Step by Step



Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd
2. Master machines fetch the remote resources from the bootstrap machine and finish booting.
3. Master machines use the bootstrap node to scale the etcd cluster to 3 instances.
4. The Etcd operator scales itself down off the bootstrap node, then scales back up to 3; all on the Masters
5. Bootstrap node starts a temporary Kubernetes control plane using the newly-created etcd cluster.
6. Temporary control plane schedules the production control plane to the master machines.
7. Temporary control plane shuts down, yielding to the production control plane.
8. Bootstrap node injects OpenShift-specific components into the newly formed control plane.
9. Installer then tears down the bootstrap node or if user-provisioned, this needs to be performed by the administrator.

OpenShift Bootstrap Process: Step by Step



Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot. Runs one instance of etcd
2. Master machines fetch the remote resources from the bootstrap machine and finish booting.
3. Master machines use the bootstrap node to scale the etcd cluster to 3 instances.
4. The Etcd operator scales itself down off the bootstrap node, then scales back up to 3; all on the Masters
5. Bootstrap node starts a temporary Kubernetes control plane using the newly-created etcd cluster.
6. Temporary control plane schedules the production control plane to the master machines.
7. Temporary control plane shuts down, yielding to the production control plane.
8. Bootstrap node injects OpenShift-specific components into the newly formed control plane.
9. Installer then tears down the bootstrap node or if user-provisioned, this needs to be performed by the administrator.
10. Worker machines fetch remote resources from masters and finish booting.

How everything deployed comes under management

Masters (Special)

- Full Stack Automated: Installer provisions minimal viable masters
- User Provisioned: User/Administrator provisions minimal viable masters
- Machine API adopts existing masters post-provision
- Each master is a standalone Machine object
- Termination protection (avoid self-destruction)

Workers

- Each Machine Pool corresponds to MachineSet
- Optionally autoscale (min,max) and health check (replace if not ready > X minutes)

Multi-AZ

- MachineSets scoped to single AZ
- Installer stripes N machine sets across AZs by default
- Post-install best effort balance via cluster autoscaler

One Touch provisioning via Ignition

Machine generated; Machine validated

Ignition applies a declarative node configuration early in the boot process. Unifies kickstart and cloud-init.

- Generated via openshift-install
- Configures storage, systemd units, users, & remote configs
- Executed in the initramfs
- Configuration for masters & workers is served from the control plane and sourced from Machine Configs

```
{
  "ignition": {
    "config": {},
    "timeouts": {},
    "version": "2.1.0"
  },
  "passwd": {
    "users": [
      {
        "name": "core",
        "passwordHash": "$6$43y3tkl...",
        "sshAuthorizedKeys": [
          "key1"
        ]
      }
    ]
  },
  "storage": {},
  "systemd": {}
}
```

Full Stack Automated Deployments

Simplified Cluster Creation

Designed to easily provision a “best practices” OpenShift cluster

- New CLI-based installer with interactive guided workflow that allows for customization at each step
- Installer takes care of provisioning the underlying Infrastructure significantly reducing deployment complexity
- Leverages RHEL CoreOS for all node types enabling full stack automation of installation and updates of both platform and host OS content

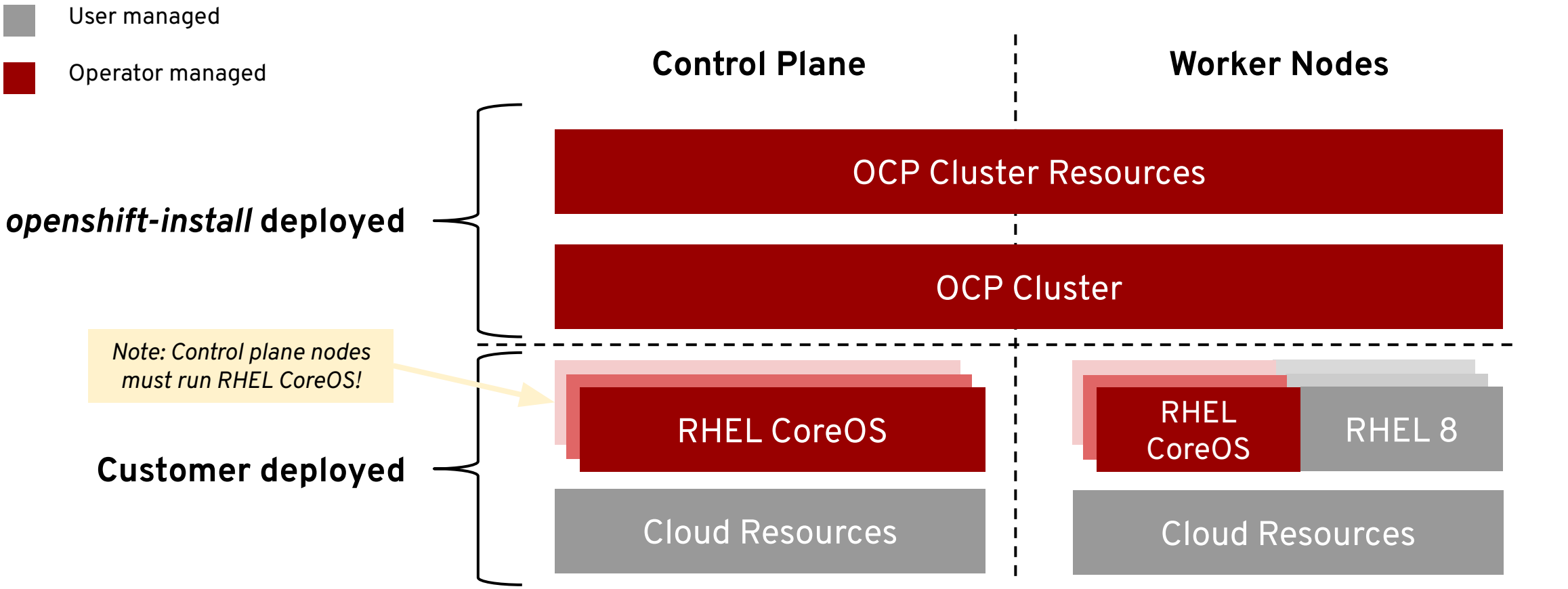
Faster Install

The installer typically finishes within 30 minutes

- Only minimal user input needed with all non-essential install config options now handled by component operator CRD’s
- See the OpenShift documentation for more details

```
$ ./openshift-install --dir ./demo create cluster
? SSH Public Key /Users/demo/.ssh/id_rsa.pub
? Platform aws
? Region us-west-2
? Base Domain example.com
? Cluster Name demo
? Pull Secret [? for help]
************************************************************
INFO Creating cluster...
INFO Waiting up to 30m0s for the Kubernetes API...
INFO API v1.11.0+c69f926354 up
INFO Waiting up to 30m0s for the bootstrap-complete event...
INFO Destroying the bootstrap resources...
INFO Waiting up to 10m0s for the openshift-console route to be created...
INFO Install complete!
INFO Run 'export KUBECONFIG=<your working directory>/auth/kubeconfig' to
manage the cluster with 'oc', the OpenShift CLI.
INFO The cluster is ready when 'oc login -u kubeadmin -p <provided>'
succeeds (wait a few minutes).
INFO Access the OpenShift web-console here:
https://console-openshift-console.apps.demo.example.com
INFO Login to the console with user: kubeadmin, password: <provided>
```

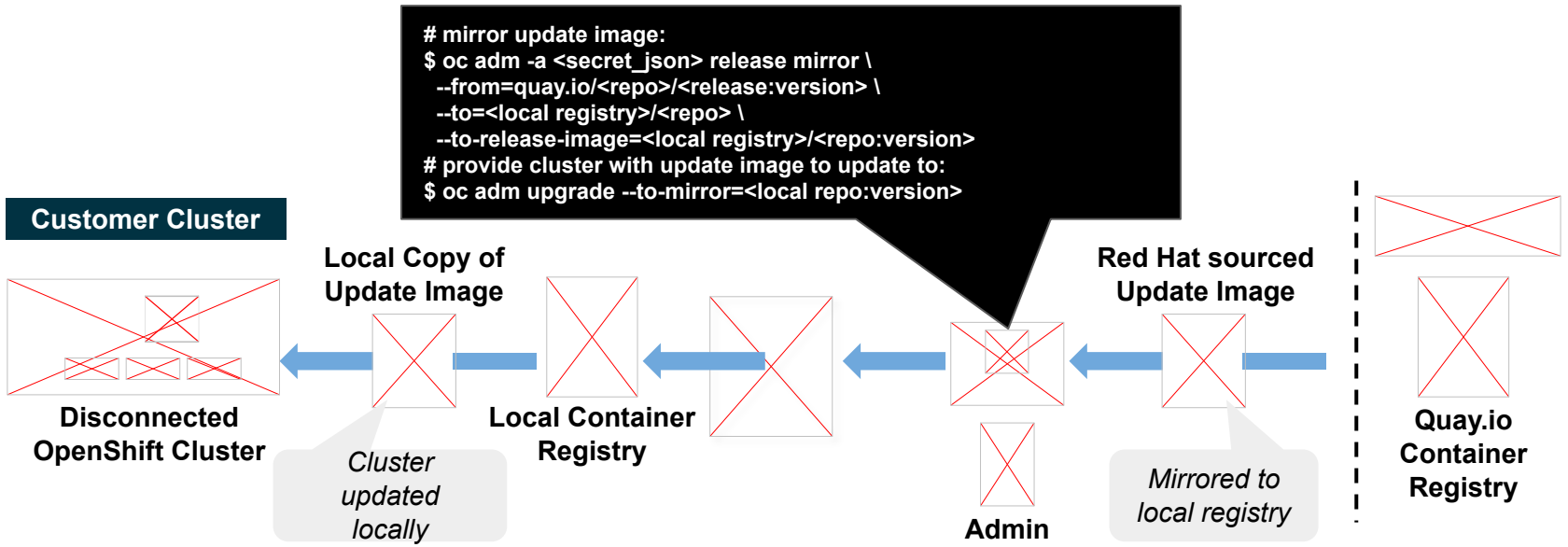

Pre-existing Infrastructure Installation (aka UPI)



Comparison of Paradigms

	Full Stack Automation	Pre-existing Infrastructure
Build Network	Installer	User
Setup Load Balancers	Installer	User
Configure DNS	Installer	User
Hardware/VM Provisioning	Installer	User
OS Installation	Installer	User
Generate Ignition Configs	Installer	Installer
OS Support	Installer: RHEL CoreOS	User: RHEL CoreOS + RHEL 8
Node Provisioning / Autoscaling	Yes	Only for providers with OpenShift Machine API support

Disconnected “Air-gapped” Installation & Upgrading



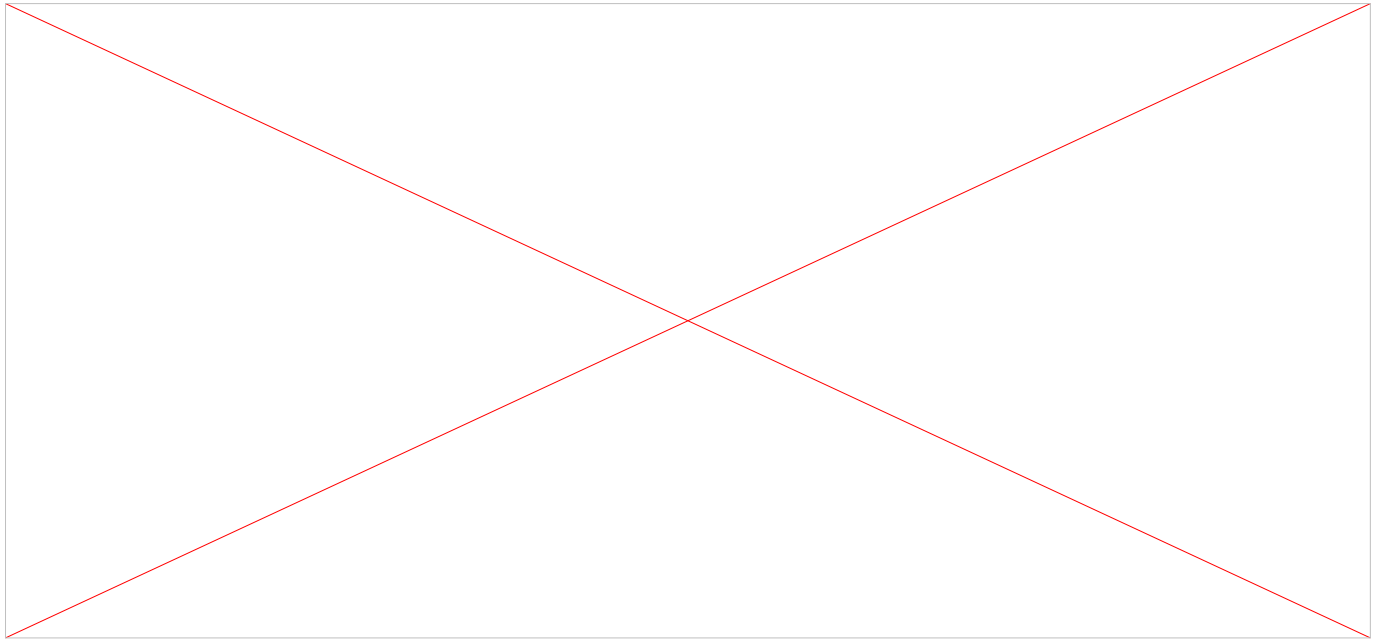
Overview

- 4.2 introduces support for installing and updating OpenShift clusters in disconnected environments
- Requires local Docker 2.2 spec compliant container registry to host OpenShift content
- Designed to work with the user provisioned infrastructure deployment method
  - *Note: Will not work with Installer provisioned infrastructure deployments*

Installation Procedure

- Mirror OpenShift content to local container registry in the disconnected environment
- Generate install-config.yaml: $ ./openshift-install create install-config --dir <dir>
  - Edit and add pull secret (PullSecret), CA certificate (AdditionalTrustBundle), and image content sources (ImageContentSources) to install-config.yaml
- Set the OPENSHIFT_INSTALL_RELEASE_IMAGE_OVERRIDE environment variable during the creation of the ignition configs
- Generate the ignition configuration: $ ./openshift-install create ignition-configs --dir <dir>
- Use the resulting ignition files to bootstrap the cluster deployment

Mirror the Registry with QUAY



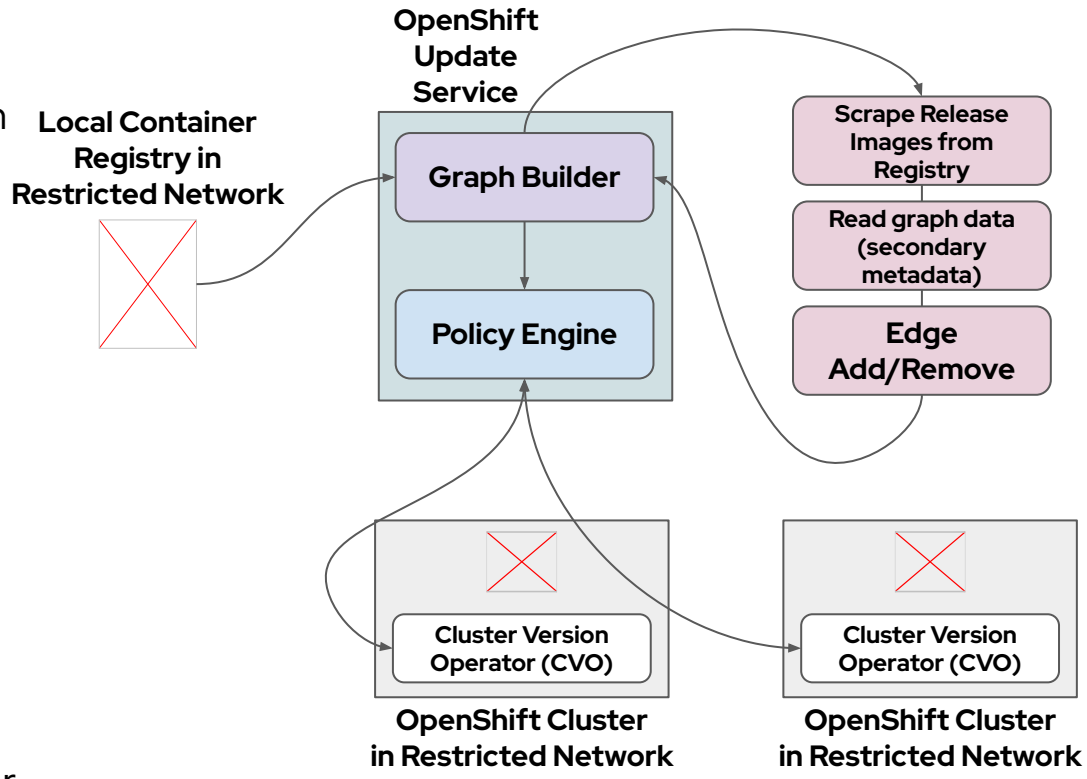
3.2.1. Prerequisites

- An OpenShift Container Platform subscription.
- **Red Hat Enterprise Linux (RHEL) 8 with Podman 3.3 installed.**
- Fully qualified domain name for the Red Hat Quay service, which must resolve through a DNS server.
- Passwordless `sudo` access on the target host.
- Key-based SSH connectivity on the target host. SSH keys are automatically generated for local installs. For remote hosts, you must generate your own SSH keys.

OpenShift Update Service

Update manager for your clusters in restricted or disconnected networks

- OpenShift Update Service (OSUS) is the on-premise release of Red Hat's hosted update service
- Supports the publishing of upgrade graph information to clusters in restricted networks
- Provides clusters with a list of next recommended update versions based on the current version installed on the cluster
- Comprised of two services:
  - **Graph Builder:** Fetches OpenShift release payload information (primary metadata) from any container registry (compatible with Docker registry V2 API) and builds a directed acyclic graph (DAG) representing valid upgrade edges
  - **Policy Engine:** Responsible for selectively serving updates to every cluster by altering a client's view of the graph with a set of filters
- GA release planned for post-4.6 and will be distributed on Operator Hub as an optional add-on operator
- Blog post announcing OpenShift Update Service
- https://github.com/openshift/cincinnati-operator



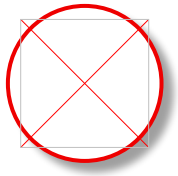
Cluster Infrastructure

Providers

- Continue to provide integration with and maximum choice of cloud providers

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

- Updated tested/supported list to be same as installer - reduced confusion, eliminate lag of support

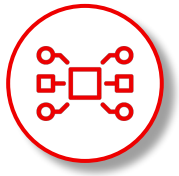


Managed Control Planes

- Bring flexibility and operational simplicity to the control plane

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

- Control plane can scale up/down via Machine API and Machine Controller
- Use for vertical scaling and replacement of control plane machines
- Allow setting verbosity of Cluster Autoscaler



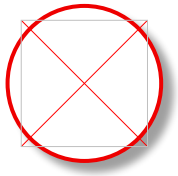
Extensions

- Access more cloud provider functionality seamlessly via OpenShift

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

- **Azure:** config of boot diagnostics on compute nodes
- **GCP:** handle userDataSecret for Windows MachineSets

Systems Enablement

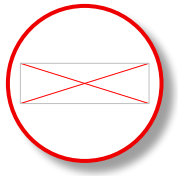


Multi-architecture Compute

- Allow more flexibility in a clusters by mixing compute node architectures (aka Heterogeneous Compute)

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

- Azure offering remains in Tech preview for now
- Multi-arch payload there but only for above
- No upgrade yet though you can --force

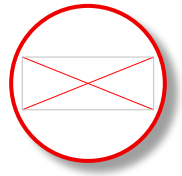


OpenShift on Arm

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

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

- **OCP for Arm on Azure IPI**
- AWS Graviton 3 support



IBM Power and zSystems

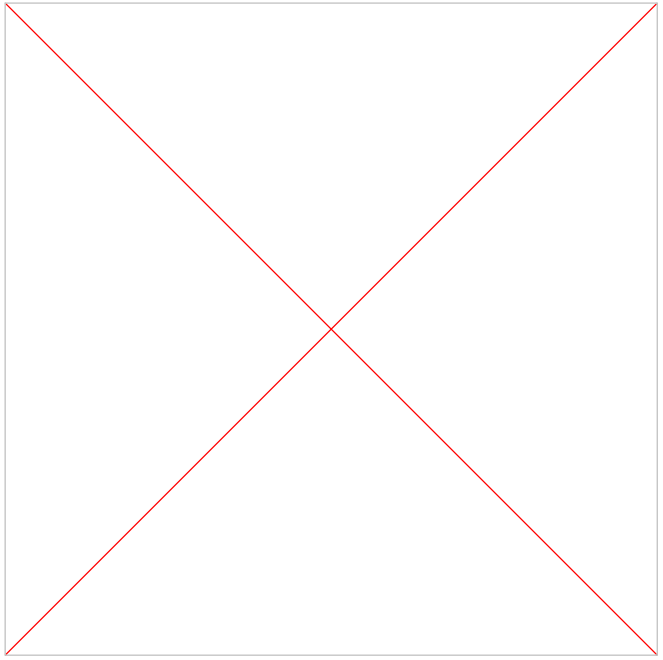
- Run OpenShift on highly available, highly secure, scalable hardware

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

- **IBM Power:**
  - Working on IPI for PowerVS
- **IBM zSystems:**
  - Secure Execution TP
- Notification of deprecated systems

RHEL CoreOS

We're making containers ***bootable***



RHEL CoreOS will ship as bootable **node base image** which you can customize with any OCI-container tooling before using with your bare metal or virtual OpenShift machines.

- Support for adding RHEL hotfix packages is **GA in 4.12!**
- **Developer Preview in 4.12**: anything you want to try! Pre-install additional software, copy configuration files in directly, even run Ansible playbooks against the image pre-deployment!

More info:
https://coreos.github.io/rpm-ostree/container/
https://github.com/containers/bootc

PM: Mark Russell

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat | IBM