OpenShift Container Platform 4.11

Nodes

Configuring and managing nodes in OpenShift Container Platform
OpenShift Container Platform 4.11 Nodes

Configuring and managing nodes in OpenShift Container Platform
Abstract

This document provides instructions for configuring and managing the nodes, Pods, and containers in your cluster. It also provides information on configuring Pod scheduling and placement, using jobs and DaemonSets to automate tasks, and other tasks to ensure an efficient cluster.
Table of Contents

CHAPTER 1. OVERVIEW OF NODES

1.1. ABOUT NODES
   Read operations
   Management operations
   Enhancement operations
1.2. ABOUT PODS
   Read operations
   Management operations
   Enhancement operations
1.3. ABOUT CONTAINERS
1.4. COMMON TERMS

CHAPTER 2. WORKING WITH PODS

2.1. USING PODS
   2.1.1. Understanding pods
   2.1.2. Example pod configurations
   2.1.3. Additional resources
2.2. VIEWING PODS
   2.2.1. About pods
   2.2.2. Viewing pods in a project
   2.2.3. Viewing pod usage statistics
   2.2.4. Viewing resource logs
2.3. CONFIGURING AN OPENSFIFT CONTAINER PLATFORM CLUSTER FOR PODS
   2.3.1. Configuring how pods behave after restart
   2.3.2. Limiting the bandwidth available to pods
   2.3.3. Understanding how to use pod disruption budgets to specify the number of pods that must be up
      2.3.3.1. Specifying the number of pods that must be up with pod disruption budgets
   2.3.4. Preventing pod removal using critical pods
2.4. AUTOMATICALLY SCALING PODS WITH THE HORIZONTAL POD AUTOSCALER
   2.4.1. Understanding horizontal pod autoscalers
      2.4.1.1. Supported metrics
   2.4.2. How does the HPA work?
   2.4.3. About requests and limits
   2.4.4. Best practices
      2.4.4.1. Scaling policies
   2.4.5. Creating a horizontal pod autoscaler by using the web console
   2.4.6. Creating a horizontal pod autoscaler for CPU utilization by using the CLI
   2.4.7. Creating a horizontal pod autoscaler object for memory utilization by using the CLI
   2.4.8. Understanding horizontal pod autoscaler status conditions by using the CLI
      2.4.8.1. Viewing horizontal pod autoscaler status conditions by using the CLI
   2.4.9. Additional resources
2.5. AUTOMATICALLY SCALING PODS BASED ON CUSTOM METRICS
   2.5.1. Understanding the custom metrics autoscaler
   2.5.2. Installing the custom metrics autoscaler
   2.5.3. Understanding the custom metrics autoscaler triggers
      2.5.3.1. Understanding the Prometheus trigger
   2.5.4. Understanding custom metrics autoscaler trigger authentications
      2.5.4.1. Using trigger authentications
   2.5.5. Configuring the custom metrics autoscaler to use OpenShift Container Platform monitoring
   2.5.6. Understanding how to add custom metrics autoscalers
      2.5.6.1. Adding a custom metrics autoscaler to a workload
2.10.2. Understanding pod preemption
2.10.2.1. Non-preempting priority classes (Technology Preview)
2.10.2.2. Pod preemption and other scheduler settings
2.10.2.3. Graceful termination of preempted pods
2.10.3. Configuring priority and preemption
2.11. PLACING PODS ON SPECIFIC NODES USING NODE SELECTORS
2.11.1. Using node selectors to control pod placement

CHAPTER 3. CONTROLLING POD PLACEMENT ONTO NODES (SCHEDULING) ........................................ 117
3.1. CONTROLLING POD PLACEMENT USING THE SCHEDULER .............................................. 117
  3.1.1. About the default scheduler
  3.1.1.1. Understanding default scheduling
  3.1.2. Scheduler use cases
  3.1.2.1. Infrastructure topological levels
  3.1.2.2. Affinity
  3.1.2.3. Anti-affinity
3.2. SCHEDULING PODS USING A SCHEDULER PROFILE ....................................................... 118
  3.2.1. About scheduler profiles
  3.2.2. Configuring a scheduler profile
3.3. PLACING PODS RELATIVE TO OTHER PODS USING AFFINITY AND ANTI-AFFINITY RULES ...... 120
  3.3.1. Understanding pod affinity
  3.3.2. Configuring a pod affinity rule
  3.3.3. Configuring a pod anti-affinity rule
  3.3.4. Sample pod affinity and anti-affinity rules
    3.3.4.1. Pod Affinity
    3.3.4.2. Pod Anti-affinity
    3.3.4.3. Pod Affinity with no Matching Labels
3.4. CONTROLLING POD PLACEMENT ON NODES USING NODE AFFINITY RULES ..................... 126
  3.4.1. Understanding node affinity
  3.4.2. Configuring a required node affinity rule
  3.4.3. Configuring a preferred node affinity rule
  3.4.4. Sample node affinity rules
    3.4.4.1. Node affinity with matching labels
    3.4.4.2. Node affinity with no matching labels
  3.4.5. Additional resources
3.5. PLACING PODS ONTO OVERCOMMITTED NODES ............................................................. 133
  3.5.1. Understanding overcommitment
  3.5.2. Understanding nodes overcommitment
3.6. CONTROLLING POD PLACEMENT USING NODE TAINS ...................................................... 134
  3.6.1. Understanding taints and tolerations
    3.6.1.1. Understanding how to use toleration seconds to delay pod evictions
    3.6.1.2. Understanding how to use multiple taints
    3.6.1.3. Understanding pod scheduling and node conditions (taint node by condition)
    3.6.1.4. Understanding evicting pods by condition (taint-based evictions)
    3.6.1.5. Tolerating all taints
  3.6.2. Adding taints and tolerations
    3.6.2.1. Adding taints and tolerations using a machine set
    3.6.2.2. Binding a user to a node using taints and tolerations
    3.6.2.3. Creating a project with a node selector and toleration
    3.6.2.4. Controlling nodes with special hardware using taints and tolerations
  3.6.3. Removing taints and tolerations
3.7. PLACING PODS ON SPECIFIC NODES USING NODE SELECTORS ....................................... 147
  3.7.1. About node selectors
3.7.2. Using node selectors to control pod placement
3.7.3. Creating default cluster-wide node selectors
3.7.4. Creating project-wide node selectors

3.8. CONTROLLING POD PLACEMENT BY USING POD TOPOLOGY SPREAD CONSTRAINTS

3.8.1. About pod topology spread constraints
3.8.2. Configuring pod topology spread constraints
3.8.3. Example pod topology spread constraints
   3.8.3.1. Single pod topology spread constraint example
   3.8.3.2. Multiple pod topology spread constraints example
3.8.4. Additional resources

3.9. EVICTING PODS USING THE DESCHEDULER

3.9.1. About the descheduler
3.9.2. Descheduler profiles
3.9.3. Installing the descheduler
3.9.4. Configuring descheduler profiles
3.9.5. Configuring the descheduler interval
3.9.6. Uninstalling the descheduler

3.10. SECONDARY SCHEDULER

3.10.1. Secondary scheduler overview
   3.10.1.1. About the Secondary Scheduler Operator
3.10.2. Secondary Scheduler Operator for Red Hat OpenShift release notes
   3.10.2.1. Release notes for Secondary Scheduler Operator for Red Hat OpenShift 1.1.0
      3.10.2.1.1. New features and enhancements
      3.10.2.1.2. Known issues
   3.10.2.2. Release notes for Secondary Scheduler Operator for Red Hat OpenShift 1.0.1
      3.10.2.2.1. New features and enhancements
      3.10.2.2.2. Bug fixes
      3.10.2.2.3. Known issues
   3.10.2.3. Release notes for Secondary Scheduler Operator for Red Hat OpenShift 1.0.0
      3.10.2.3.1. New features and enhancements
      3.10.2.3.2. Known issues
3.10.3. Scheduling pods using a secondary scheduler
   3.10.3.1. Installing the Secondary Scheduler Operator
   3.10.3.2. Deploying a secondary scheduler
   3.10.3.3. Scheduling a pod using the secondary scheduler
3.10.4. Uninstalling the Secondary Scheduler Operator
   3.10.4.1. Uninstalling the Secondary Scheduler Operator
   3.10.4.2. Removing Secondary Scheduler Operator resources

CHAPTER 4. USING JOBS AND DAEMONSETS

4.1. RUNNING BACKGROUND TASKS ON NODES AUTOMATICALLY WITH DAEMON SETS

4.1.1. Scheduled by default scheduler
4.1.2. Creating daemonsets

4.2. RUNNING TASKS IN PODS USING JOBS

4.2.1. Understanding jobs and cron jobs
   4.2.1.1. Understanding how to create jobs
   4.2.1.2. Understanding how to set a maximum duration for jobs
   4.2.1.3. Understanding how to set a job back off policy for pod failure
   4.2.1.4. Understanding how to configure a cron job to remove artifacts
   4.2.1.5. Known limitations
4.2.2. Creating jobs
4.2.3. Creating cron jobs
CHAPTER 5. WORKING WITH NODES

5.1. VIEWING AND LISTING THE NODES IN YOUR OPENSHIFT CONTAINER PLATFORM CLUSTER

5.1.1. About listing all the nodes in a cluster

5.1.2. Listing pods on a node in your cluster

5.1.3. Viewing memory and CPU usage statistics on your nodes

5.2. WORKING WITH NODES

5.2.1. Understanding how to evacuate pods on nodes

5.2.2. Understanding how to update labels on nodes

5.2.3. Understanding how to mark nodes as unschedulable or schedulable

5.2.4. Configuring control plane nodes as schedulable

5.2.5. Deleting nodes

5.2.5.1. Deleting nodes from a cluster

5.2.5.2. Deleting nodes from a bare metal cluster

5.2.6. Setting SELinux booleans

5.2.7. Adding kernel arguments to nodes

5.2.8. Enabling Linux control groups version 2 (cgroups v2)

5.2.9. Enabling swap memory use on nodes

5.2.10. Migrating control plane nodes from one RHOSP host to another

5.3. MANAGING NODES

5.3.1. Modifying nodes

5.4. MANAGING THE MAXIMUM NUMBER OF PODS PER NODE

5.4.1. Configuring the maximum number of pods per node

5.5. USING THE NODE TUNING OPERATOR

5.5.1. Accessing an example Node Tuning Operator specification

5.5.2. Custom tuning specification

5.5.3. Default profiles set on a cluster

5.5.4. Supported TuneD daemon plug-ins

5.6. REMEDIATING NODES WITH THE SELF NODE REMEDIATION OPERATOR

5.6.1. About the Self Node Remediation Operator

5.6.1.1. Understanding the Self Node Remediation Operator configuration

5.6.1.2. Understanding the Self Node Remediation Template configuration

5.6.1.3. About watchdog devices

5.6.1.3.1. Understanding Self Node Remediation Operator behavior with watchdog devices

5.6.2. Installing the Self Node Remediation Operator by using the web console

5.6.3. Installing the Self Node Remediation Operator by using the CLI

5.6.4. Configuring machine health checks to use the Self Node Remediation Operator

5.6.5. Troubleshooting the Self Node Remediation Operator

5.6.5.1. General troubleshooting

5.6.5.2. Checking the daemon set

5.6.5.3. Unsuccessful remediation

5.6.5.4. Daemon set and other Self Node Remediation Operator resources exist even after uninstalling the Operator

5.6.6. Gathering data about the Self Node Remediation Operator

5.6.7. Additional resources

5.7. DEPLOYING NODE HEALTH CHECKS BY USING THE NODE HEALTH CHECK OPERATOR

5.7.1. About the Node Health Check Operator

5.7.1.1. Understanding the Node Health Check Operator workflow

5.7.1.2. About how node health checks prevent conflicts with machine health checks

5.7.2. Installing the Node Health Check Operator by using the web console

5.7.3. Installing the Node Health Check Operator by using the CLI

5.7.4. Gathering data about the Node Health Check Operator

5.7.5. Additional resources

5.8. USING THE NODE MAINTENANCE OPERATOR TO PLACE NODES IN MAINTENANCE MODE
5.8.1. About the Node Maintenance Operator

5.8.2. Installing the Node Maintenance Operator
   5.8.2.1. Installing the Node Maintenance Operator by using the web console
   5.8.2.2. Installing the Node Maintenance Operator by using the CLI

5.8.3. Setting a node to maintenance mode
   5.8.3.1. Setting a node to maintenance mode by using the web console
   5.8.3.2. Setting a node to maintenance mode by using the CLI
   5.8.3.3. Checking status of current NodeMaintenance CR tasks

5.8.4. Resuming a node from maintenance mode
   5.8.4.1. Resuming a node from maintenance mode by using the web console
   5.8.4.2. Resuming a node from maintenance mode by using the CLI

5.8.5. Working with bare-metal nodes
   5.8.5.1. Maintaining bare-metal nodes
   5.8.5.2. Setting a bare-metal node to maintenance mode
   5.8.5.3. Resuming a bare-metal node from maintenance mode

5.8.6. Gathering data about the Node Maintenance Operator

5.8.7. Additional resources

5.9. UNDERSTANDING NODE REBOOTING
   5.9.1. About rebooting nodes running critical infrastructure
   5.9.2. Rebooting a node using pod anti-affinity
   5.9.3. Understanding how to reboot nodes running routers
   5.9.4. Rebooting a node gracefully

5.10. FREEING NODE RESOURCES USING GARBAGE COLLECTION
   5.10.1. Understanding how terminated containers are removed through garbage collection
   5.10.2. Understanding how images are removed through garbage collection
   5.10.3. Configuring garbage collection for containers and images

5.11. ALLOCATING RESOURCES FOR NODES IN AN OPENSFC CONTAINER PLATFORM CLUSTER
   5.11.1. Understanding how to allocate resources for nodes
   5.11.1.1. How OpenShift Container Platform computes allocated resources
   5.11.1.2. How nodes enforce resource constraints
   5.11.1.3. Understanding Eviction Thresholds
   5.11.1.4. How the scheduler determines resource availability
   5.11.2. Automatically allocating resources for nodes
   5.11.3. Manually allocating resources for nodes

5.12. ALLOCATING SPECIFIC CPUS FOR NODES IN A CLUSTER
   5.12.1. Reserving CPUs for nodes

5.13. ENABLING TLS SECURITY PROFILES FOR THE KUBELET
   5.13.1. Understanding TLS security profiles
   5.13.2. Configuring the TLS security profile for the kubelet

5.14. MACHINE CONFIG Daemon METRICS
   5.14.1. Machine Config Daemon metrics

CHAPTER 6. WORKING WITH CONTAINERS

6.1. UNDERSTANDING CONTAINERS
   About containers and RHEL kernel memory
6.2. USING INIT CONTAINERS TO PERFORM TASKS BEFORE A POD IS DEPLOYED
   6.2.1. Understanding Init Containers
   6.2.2. Creating Init Containers
6.3. USING VOLUMES TO PERSIST CONTAINER DATA
   6.3.1. Understanding volumes
   6.3.2. Working with volumes using the OpenShift Container Platform CLI
   6.3.3. Listing volumes and volume mounts in a pod
   6.3.4. Adding volumes to a pod
6.3.5. Updating volumes and volume mounts in a pod
6.3.6. Removing volumes and volume mounts from a pod
6.3.7. Configuring volumes for multiple uses in a pod
6.4. MAPPING VOLUMES USING PROJECTED VOLUMES
   6.4.1. Understanding projected volumes
   6.4.1.1. Example Pod specs
   6.4.1.2. Pathing Considerations
   6.4.2. Configuring a Projected Volume for a Pod
6.5. ALLOWING CONTAINERS TO CONSUME API OBJECTS
   6.5.1. Expose pod information to Containers using the Downward API
   6.5.2. Understanding how to consume container values using the downward API
      6.5.2.1. Consuming container values using environment variables
      6.5.2.2. Consuming container values using a volume plug-in
   6.5.3. Understanding how to consume container resources using the Downward API
      6.5.3.1. Consuming container resources using environment variables
      6.5.3.2. Consuming container resources using a volume plug-in
   6.5.4. Consuming secrets using the Downward API
   6.5.5. Consuming configuration maps using the Downward API
   6.5.6. Referencing environment variables
   6.5.7. Escaping environment variable references
6.6. COPYING FILES TO OR FROM AN OPENSShift CONTAINER PLATFORM CONTAINER
   6.6.1. Understanding how to copy files
      6.6.1.1. Requirements
      6.6.2. Copying files to and from containers
      6.6.3. Using advanced Rsync features
6.7. EXECUTING REMOTE COMMANDS IN AN OPENSShift CONTAINER PLATFORM CONTAINER
   6.7.1. Executing remote commands in containers
   6.7.2. Protocol for initiating a remote command from a client
6.8. USING PORT FORWARDING TO ACCESS APPLICATIONS IN A CONTAINER
   6.8.1. Understanding port forwarding
   6.8.2. Using port forwarding
   6.8.3. Protocol for initiating port forwarding from a client
6.9. USING SYSCTLs IN CONTAINERS
   6.9.1. About sysctls
   6.9.2. Namespaced and node-level sysctls
   6.9.3. Safe and unsafe sysctls
   6.9.4. Starting a pod with safe sysctls
   6.9.5. Starting a pod with unsafe sysctls
   6.9.6. Enabling unsafe sysctls
   6.9.7. Additional resources

CHAPTER 7. WORKING WITH CLUSTERS

7.1. VIEWING SYSTEM EVENT INFORMATION IN AN OPENSShift CONTAINER PLATFORM CLUSTER
   7.1.1. Understanding events
   7.1.2. Viewing events using the CLI
   7.1.3. List of events
7.2. ESTIMATING THE NUMBER OF PODS YOUR OPENSShift CONTAINER PLATFORM NODES CAN HOLD
   7.2.1. Understanding the OpenShift Container Platform cluster capacity tool
   7.2.2. Running the cluster capacity tool on the command line
   7.2.3. Running the cluster capacity tool as a job inside a pod
7.3. RESTRICT RESOURCE CONSUMPTION WITH LIMIT RANGES
   7.3.1. About limit ranges
8.1.3. Latency spikes or temporary reduction in throughput to remote workers
8.1.4. Remote worker node strategies

CHAPTER 9. WORKER NODES FOR SINGLE-NODE OPENSHIFT CLUSTERS

9.1. ADDING WORKER NODES TO SINGLE-NODE OPENSHIFT CLUSTERS
   9.1.1. Requirements for installing single-node OpenShift worker nodes
   9.1.2. Adding worker nodes using the Assisted Installer and OpenShift Cluster Manager
   9.1.3. Adding worker nodes using the Assisted Installer API
       9.1.3.1. Authenticating against the Assisted Installer REST API
       9.1.3.2. Adding worker nodes using the Assisted Installer REST API
   9.1.4. Adding worker nodes to single-node OpenShift clusters manually
   9.1.5. Approving the certificate signing requests for your machines
CHAPTER 1. OVERVIEW OF NODES

1.1. ABOUT NODES

A node is a virtual or bare-metal machine in a Kubernetes cluster. Worker nodes host your application containers, grouped as pods. The control plane nodes run services that are required to control the Kubernetes cluster. In OpenShift Container Platform, the control plane nodes contain more than just the Kubernetes services for managing the OpenShift Container Platform cluster.

Having stable and healthy nodes in a cluster is fundamental to the smooth functioning of your hosted application. In OpenShift Container Platform, you can access, manage, and monitor a node through the Node object representing the node. Using the OpenShift CLI (oc) or the web console, you can perform the following operations on a node.

Read operations
The read operations allow an administrator or a developer to get information about nodes in an OpenShift Container Platform cluster.

- List all the nodes in a cluster.
- Get information about a node, such as memory and CPU usage, health, status, and age.
- List pods running on a node.

Management operations
As an administrator, you can easily manage a node in an OpenShift Container Platform cluster through several tasks:

- Add or update node labels. A label is a key-value pair applied to a Node object. You can control the scheduling of pods using labels.
- Change node configuration using a custom resource definition (CRD), or the kubeletConfig object.
- Configure nodes to allow or disallow the scheduling of pods. Healthy worker nodes with a Ready status allow pod placement by default while the control plane nodes do not; you can change this default behavior by configuring the worker nodes to be unschedulable and the control plane nodes to be schedulable.
- Allocate resources for nodes using the system-reserved setting. You can allow OpenShift Container Platform to automatically determine the optimal system-reserved CPU and memory resources for your nodes, or you can manually determine and set the best resources for your nodes.
- Configure the number of pods that can run on a node based on the number of processor cores on the node, a hard limit, or both.
- Reboot a node gracefully using pod anti-affinity.
- Delete a node from a cluster by scaling down the cluster using a machine set. To delete a node from a bare-metal cluster, you must first drain all pods on the node and then manually delete the node.

Enhancement operations
OpenShift Container Platform allows you to do more than just access and manage nodes; as an administrator, you can perform the following tasks on nodes to make the cluster more efficient, application-friendly, and to provide a better environment for your developers.

- Manage node-level tuning for high-performance applications that require some level of kernel tuning by using the Node Tuning Operator.
- Enable TLS security profiles on the node to protect communication between the kubelet and the Kubernetes API server.
- Run background tasks on nodes automatically with daemon sets. You can create and use daemon sets to create shared storage, run a logging pod on every node, or deploy a monitoring agent on all nodes.
- Free node resources using garbage collection. You can ensure that your nodes are running efficiently by removing terminated containers and the images not referenced by any running pods.
- Add kernel arguments to a set of nodes.
- Configure an OpenShift Container Platform cluster to have worker nodes at the network edge (remote worker nodes). For information on the challenges of having remote worker nodes in an OpenShift Container Platform cluster and some recommended approaches for managing pods on a remote worker node, see Using remote worker nodes at the network edge.

1.2. ABOUT PODS

A pod is one or more containers deployed together on a node. As a cluster administrator, you can define a pod, assign it to run on a healthy node that is ready for scheduling, and manage. A pod runs as long as the containers are running. You cannot change a pod once it is defined and is running. Some operations you can perform when working with pods are:

**Read operations**

As an administrator, you can get information about pods in a project through the following tasks:

- List pods associated with a project, including information such as the number of replicas and restarts, current status, and age.
- View pod usage statistics such as CPU, memory, and storage consumption.

**Management operations**

The following list of tasks provides an overview of how an administrator can manage pods in an OpenShift Container Platform cluster.

- Control scheduling of pods using the advanced scheduling features available in OpenShift Container Platform:
  - Node-to-pod binding rules such as pod affinity, node affinity, and anti-affinity.
  - Node labels and selectors.
  - Taints and tolerations.
  - Pod topology spread constraints.
  - Secondary scheduling.
- Configure the descheduler to evict pods based on specific strategies so that the scheduler reschedules the pods to more appropriate nodes.

- Configure how pods behave after a restart using pod controllers and restart policies.

- Limit both egress and ingress traffic on a pod.

- Add and remove volumes to and from any object that has a pod template. A volume is a mounted file system available to all the containers in a pod. Container storage is ephemeral; you can use volumes to persist container data.

**Enhancement operations**

You can work with pods more easily and efficiently with the help of various tools and features available in OpenShift Container Platform. The following operations involve using those tools and features to better manage pods.

<table>
<thead>
<tr>
<th>Operation</th>
<th>User</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and use a horizontal pod autoscaler.</td>
<td>Developer</td>
<td>You can use a horizontal pod autoscaler to specify the minimum and the maximum number of pods you want to run, as well as the CPU utilization or memory utilization your pods should target. Using a horizontal pod autoscaler, you can automatically scale pods.</td>
</tr>
<tr>
<td>Install and use a vertical pod autoscaler</td>
<td>Administrator and developer</td>
<td>As an administrator, use a vertical pod autoscaler to better use cluster resources by monitoring the resources and the resource requirements of workloads. As a developer, use a vertical pod autoscaler to ensure your pods stay up during periods of high demand by scheduling pods to nodes that have enough resources for each pod.</td>
</tr>
<tr>
<td>Provide access to external resources using device plug-ins.</td>
<td>Administrator</td>
<td>A device plug-in is a gRPC service running on nodes (external to the kubelet), which manages specific hardware resources. You can deploy a device plug-in to provide a consistent and portable solution to consume hardware devices across clusters.</td>
</tr>
<tr>
<td>Provide sensitive data to pods using the Secret object.</td>
<td>Administrator</td>
<td>Some applications need sensitive information, such as passwords and usernames. You can use the Secret object to provide such information to an application pod.</td>
</tr>
</tbody>
</table>

**1.3. ABOUT CONTAINERS**
A container is the basic unit of an OpenShift Container Platform application, which comprises the application code packaged along with its dependencies, libraries, and binaries. Containers provide consistency across environments and multiple deployment targets: physical servers, virtual machines (VMs), and private or public cloud.

Linux container technologies are lightweight mechanisms for isolating running processes and limiting access to only designated resources. As an administrator, You can perform various tasks on a Linux container, such as:

- Copy files to and from a container.
- Allow containers to consume API objects.
- Execute remote commands in a container.
- Use port forwarding to access applications in a container.

OpenShift Container Platform provides specialized containers called Init containers. Init containers run before application containers and can contain utilities or setup scripts not present in an application image. You can use an Init container to perform tasks before the rest of a pod is deployed.

Apart from performing specific tasks on nodes, pods, and containers, you can work with the overall OpenShift Container Platform cluster to keep the cluster efficient and the application pods highly available.

### 1.4. COMMON TERMS

This glossary defines common terms that are used in the node content. These terms help you understand nodes effectively.

**Container**

It is a lightweight and executable image that comprises software and all its dependencies. Containers virtualize the operating system, as a result, you can run containers anywhere from a data center to a public or private cloud to even a developer’s laptop.

**Daemon set**

Ensures that a replica of the pod runs on eligible nodes in an OpenShift Container Platform cluster.

**egress**

The process of data sharing externally through a network’s outbound traffic from a pod.

**garbage collection**

The process of cleaning up cluster resources, such as terminated containers and images that are not referenced by any running pods.

**Horizontal Pod Autoscaler (HPA)**

Implemented as a Kubernetes API resource and a controller. You can use the HPA to specify the minimum and maximum number of pods that you want to run. You can also specify the CPU or memory utilization that your pods should target. The HPA scales out and scales in pods when a given CPU or memory threshold is crossed.

**Ingress**

Incoming traffic to a pod.
Job
A process that runs to completion. A job creates one or more pod objects and ensures that the specified pods are successfully completed.

Labels
You can use labels, which are key-value pairs, to organise and select subsets of objects, such as a pod.

Node
A worker machine in the OpenShift Container Platform cluster. A node can be either a virtual machine (VM) or a physical machine.

Node Tuning Operator
You can use the Node Tuning Operator to manage node-level tuning by using the TuneD daemon. It ensures custom tuning specifications are passed to all containerized TuneD daemons running in the cluster in the format that the daemons understand. The daemons run on all nodes in the cluster, one per node.

Self Node Remediation Operator
The Operator runs on the cluster nodes and identifies and reboots nodes that are unhealthy.

Pod
One or more containers with shared resources, such as volume and IP addresses, running in your OpenShift Container Platform cluster. A pod is the smallest compute unit defined, deployed, and managed.

Toleration
Indicates that the pod is allowed (but not required) to be scheduled on nodes or node groups with matching taints. You can use tolerations to enable the scheduler to schedule pods with matching taints.

Taint
A core object that comprises a key, value, and effect. Taints and tolerations work together to ensure that pods are not scheduled on irrelevant nodes.
CHAPTER 2. WORKING WITH PODS

2.1. USING PODS

A pod is one or more containers deployed together on one host, and the smallest compute unit that can be defined, deployed, and managed.

2.1.1. Understanding pods

Pods are the rough equivalent of a machine instance (physical or virtual) to a Container. Each pod is allocated its own internal IP address, therefore owning its entire port space, and containers within pods can share their local storage and networking.

Pods have a lifecycle; they are defined, then they are assigned to run on a node, then they run until their container(s) exit or they are removed for some other reason. Pods, depending on policy and exit code, might be removed after exiting, or can be retained to enable access to the logs of their containers.

OpenShift Container Platform treats pods as largely immutable; changes cannot be made to a pod definition while it is running. OpenShift Container Platform implements changes by terminating an existing pod and recreating it with modified configuration, base image(s), or both. Pods are also treated as expendable, and do not maintain state when recreated. Therefore pods should usually be managed by higher-level controllers, rather than directly by users.

NOTE

For the maximum number of pods per OpenShift Container Platform node host, see the Cluster Limits.

WARNING

Bare pods that are not managed by a replication controller will be not rescheduled upon node disruption.

2.1.2. Example pod configurations

OpenShift Container Platform leverages the Kubernetes concept of a pod, which is one or more containers deployed together on one host, and the smallest compute unit that can be defined, deployed, and managed.

The following is an example definition of a pod from a Rails application. It demonstrates many features of pods, most of which are discussed in other topics and thus only briefly mentioned here:

Pod object definition (YAML)

```yaml
kind: Pod
apiVersion: v1
metadata:
  name: example
namespace: default
```
selfLink: /api/v1/namespaces/default/pods/example
uid: 5cc30063-0265780783bc
resourceVersion: '165032'
labels:
  - app: hello-openshift
    annotations:
      openshift.io/scc: anyuid
spec:
  restartPolicy: Always
  serviceAccountName: default
  imagePullSecrets:
  - name: default-dockercfg-5rhhb
    priority: 0
  schedulerName: default-scheduler
  terminationGracePeriodSeconds: 30
  nodeName: ip-10-0-140-16.us-east-2.compute.internal
  securityContext:
    seLinuxOptions:
      level: 's0:c11,c10'
containers:
  - resources: {}
    terminationMessagePath: /dev/termination-log
    name: hello-openshift
    securityContext:
      capabilities:
        drop:
          - MKNOD
    procMount: Default
    ports:
      - containerPort: 8080
        protocol: TCP
    imagePullPolicy: Always
    volumeMounts:
      - name: default-token-wbqsl
        readOnly: true
        mountPath: /var/run/secrets/kubernetes.io/serviceaccount
    terminationMessagePolicy: File
    image: registry.redhat.io/openshift4/ose-ogging-eventrouter:v4.3
  serviceAccount: default
  volumes:
    - name: default-token-wbqsl
      secret:
        secretName: default-token-wbqsl
        defaultMode: 420
  dnsPolicy: ClusterFirst
status:
  phase: Pending
  conditions:
  - type: Initialized
    status: 'True'
    lastProbeTime: null
  - type: Ready
    status: 'False'
Pods can be "tagged" with one or more labels, which can then be used to select and manage groups of pods in a single operation. The labels are stored in key/value format in the metadata hash.

The pod restart policy with possible values Always, OnFailure, and Never. The default value is Always.

OpenShift Container Platform defines a security context for containers which specifies whether they are allowed to run as privileged containers, run as a user of their choice, and more. The default context is very restrictive but administrators can modify this as needed.

containers specifies an array of one or more container definitions.

The container specifies where external storage volumes are mounted within the container. In this case, there is a volume for storing access to credentials the registry needs for making requests against the OpenShift Container Platform API.

Specify the volumes to provide for the pod. Volumes mount at the specified path. Do not mount to the container root, /, or any path that is the same in the host and the container. This can corrupt your host system if the container is sufficiently privileged, such as the host /dev/pts files. It is safe to mount the host by using /host.

Each container in the pod is instantiated from its own container image.

Pods making requests against the OpenShift Container Platform API is a common enough pattern that there is a serviceAccount field for specifying which service account user the pod should authenticate as when making the requests. This enables fine-grained access control for custom infrastructure components.
The pod defines storage volumes that are available to its container(s) to use. In this case, it provides an ephemeral volume for a **secret** volume containing the default service account tokens.

If you attach persistent volumes that have high file counts to pods, those pods can fail or can take a long time to start. For more information, see *When using Persistent Volumes with high file counts in OpenShift, why do pods fail to start or take an excessive amount of time to achieve “Ready” state?*.

**NOTE**

This pod definition does not include attributes that are filled by OpenShift Container Platform automatically after the pod is created and its lifecycle begins. The [Kubernetes pod documentation](https://kubernetes.io/docs/tasks-manage-storage/) has details about the functionality and purpose of pods.

### 2.1.3. Additional resources

- For more information on pods and storage see [Understanding persistent storage](https://docs.openshift.com/container-platform/latest/user-guide/persistent-storage.html) and [Understanding ephemeral storage](https://docs.openshift.com/container-platform/latest/user-guide/ephemeral-storage.html).

### 2.2. VIEWING PODS

As an administrator, you can view the pods in your cluster and to determine the health of those pods and the cluster as a whole.

#### 2.2.1. About pods

OpenShift Container Platform leverages the Kubernetes concept of a **pod**, which is one or more containers deployed together on one host, and the smallest compute unit that can be defined, deployed, and managed. Pods are the rough equivalent of a machine instance (physical or virtual) to a container.

You can view a list of pods associated with a specific project or view usage statistics about pods.

#### 2.2.2. Viewing pods in a project

You can view a list of pods associated with the current project, including the number of replica, the current status, number or restarts and the age of the pod.

**Procedure**

To view the pods in a project:

1. Change to the project:
   ```
   $ oc project <project-name>
   ```

2. Run the following command:
   ```
   $ oc get pods
   ```
   For example:
   ```
   $ oc get pods -n openshift-console
   ```
Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-698d866b78-bnshf</td>
<td>1/1</td>
<td>Running</td>
<td>2</td>
<td>165m</td>
</tr>
<tr>
<td>console-698d866b78-m87pm</td>
<td>1/1</td>
<td>Running</td>
<td>2</td>
<td>165m</td>
</tr>
</tbody>
</table>

Add the **-o wide** flags to view the pod IP address and the node where the pod is located.

```
$ oc get pods -o wide
```

Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
<th>IP</th>
<th>NODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOMINATED NODE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>console-698d866b78-bnshf</td>
<td>1/1</td>
<td>Running</td>
<td>2</td>
<td>166m</td>
<td>10.128.0.24</td>
<td>ip-10-0-152-71.ec2.internal &lt;none&gt;</td>
</tr>
<tr>
<td>console-698d866b78-m87pm</td>
<td>1/1</td>
<td>Running</td>
<td>2</td>
<td>166m</td>
<td>10.129.0.23</td>
<td>ip-10-0-173-237.ec2.internal &lt;none&gt;</td>
</tr>
</tbody>
</table>

### 2.2.3. Viewing pod usage statistics

You can display usage statistics about pods, which provide the runtime environments for containers. These usage statistics include CPU, memory, and storage consumption.

**Prerequisites**

- You must have **cluster-reader** permission to view the usage statistics.
- Metrics must be installed to view the usage statistics.

**Procedure**

To view the usage statistics:

1. Run the following command:

```
$ oc adm top pods
```

For example:

```
$ oc adm top pods -n openshift-console
```

Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>CPU(cores)</th>
<th>MEMORY(bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-7f58c69899-q8c8k</td>
<td>0m</td>
<td>22Mi</td>
</tr>
<tr>
<td>console-7f58c69899-xhbgg</td>
<td>0m</td>
<td>25Mi</td>
</tr>
<tr>
<td>downloads-594fccc94-bcxk8</td>
<td>3m</td>
<td>18Mi</td>
</tr>
<tr>
<td>downloads-594fccc94-kv4p6</td>
<td>2m</td>
<td>15Mi</td>
</tr>
</tbody>
</table>

2. Run the following command to view the usage statistics for pods with labels:

```
$ oc adm top pod --selector=""
```
You must choose the selector (label query) to filter on. Supports \(\leq\), \(\geq\), and \(!=\).

### 2.2.4. Viewing resource logs

You can view the log for various resources in the OpenShift CLI (oc) and web console. Logs read from the tail, or end, of the log.

**Prerequisites**

- Access to the OpenShift CLI (oc).

**Procedure (UI)**

1. In the OpenShift Container Platform console, navigate to *Workloads → Pods* or navigate to the pod through the resource you want to investigate.

   **NOTE**

   Some resources, such as builds, do not have pods to query directly. In such instances, you can locate the *Logs* link on the *Details* page for the resource.

2. Select a project from the drop-down menu.
3. Click the name of the pod you want to investigate.
4. Click *Logs*.

**Procedure (CLI)**

- View the log for a specific pod:

  ```
  $ oc logs -f <pod_name> -c <container_name>
  ```

  where:

  - `-f`
    - Optional: Specifies that the output follows what is being written into the logs.
  - `<pod_name>`
    - Specifies the name of the pod.
  - `<container_name>`
    - Optional: Specifies the name of a container. When a pod has more than one container, you must specify the container name.

  For example:

  ```
  $ oc logs ruby-58cd97df55-mww7r
  $ oc logs -f ruby-57f7f4855b-znl92 -c ruby
  ```

  The contents of log files are printed out.
• View the log for a specific resource:

```
$ oc logs <object_type>/<resource_name> 1
```

1 Specifies the resource type and name.

For example:

```
$ oc logs deployment/ruby
```

The contents of log files are printed out.

2.3. CONFIGURING AN OPENSIFT CONTAINER PLATFORM CLUSTER FOR PODS

As an administrator, you can create and maintain an efficient cluster for pods.

By keeping your cluster efficient, you can provide a better environment for your developers using such tools as what a pod does when it exits, ensuring that the required number of pods is always running, when to restart pods designed to run only once, limit the bandwidth available to pods, and how to keep pods running during disruptions.

2.3.1. Configuring how pods behave after restart

A pod restart policy determines how OpenShift Container Platform responds when Containers in that pod exit. The policy applies to all Containers in that pod.

The possible values are:

- **Always** - Tries restarting a successfully exited Container on the pod continuously, with an exponential back-off delay (10s, 20s, 40s) until the pod is restarted. The default is **Always**.

- **OnFailure** - Tries restarting a failed Container on the pod with an exponential back-off delay (10s, 20s, 40s) capped at 5 minutes.

- **Never** - Does not try to restart exited or failed Containers on the pod. Pods immediately fail and exit.

After the pod is bound to a node, the pod will never be bound to another node. This means that a controller is necessary in order for a pod to survive node failure:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Controller Type</th>
<th>Restart Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pods that are expected to terminate (such as batch computations)</td>
<td>Job</td>
<td><strong>OnFailure</strong> or <strong>Never</strong></td>
</tr>
<tr>
<td>Pods that are expected to not terminate (such as web servers)</td>
<td>Replication controller</td>
<td><strong>Always</strong></td>
</tr>
</tbody>
</table>
If a Container on a pod fails and the restart policy is set to **OnFailure**, the pod stays on the node and the Container is restarted. If you do not want the Container to restart, use a restart policy of **Never**.

If an entire pod fails, OpenShift Container Platform starts a new pod. Developers must address the possibility that applications might be restarted in a new pod. In particular, applications must handle temporary files, locks, incomplete output, and so forth caused by previous runs.

**NOTE**

Kubernetes architecture expects reliable endpoints from cloud providers. When a cloud provider is down, the kubelet prevents OpenShift Container Platform from restarting.

If the underlying cloud provider endpoints are not reliable, do not install a cluster using cloud provider integration. Install the cluster as if it was in a no-cloud environment. It is not recommended to toggle cloud provider integration on or off in an installed cluster.

For details on how OpenShift Container Platform uses restart policy with failed Containers, see the Example States in the Kubernetes documentation.

# 2.3.2. Limiting the bandwidth available to pods

You can apply quality-of-service traffic shaping to a pod and effectively limit its available bandwidth. Egress traffic (from the pod) is handled by policing, which simply drops packets in excess of the configured rate. Ingress traffic (to the pod) is handled by shaping queued packets to effectively handle data. The limits you place on a pod do not affect the bandwidth of other pods.

**Procedure**

To limit the bandwidth on a pod:

1. Write an object definition JSON file, and specify the data traffic speed using `kubernetes.io/ingress-bandwidth` and `kubernetes.io/egress-bandwidth` annotations. For example, to limit both pod egress and ingress bandwidth to 10M/s:

```
Limited Pod object definition

{  
  "kind": "Pod",
  "spec": {
    "containers": [
      
      
      "image": "openshift/hello-openshift",
      "name": "hello-openshift"
    ]
  },
  "apiVersion": "v1",
  "metadata": {

```
2. Create the pod using the object definition:

```
$ oc create -f <file_or_dir_path>
```

2.3.3. Understanding how to use pod disruption budgets to specify the number of
pods that must be up

A pod disruption budget is part of the Kubernetes API, which can be managed with oc commands like
other object types. They allow the specification of safety constraints on pods during operations, such as
draining a node for maintenance.

PodDisruptionBudget is an API object that specifies the minimum number or percentage of replicas
that must be up at a time. Setting these in projects can be helpful during node maintenance (such as
scaling a cluster down or a cluster upgrade) and is only honored on voluntary evictions (not on node
failures).

A PodDisruptionBudget object’s configuration consists of the following key parts:

- A label selector, which is a label query over a set of pods.
- An availability level, which specifies the minimum number of pods that must be available
  simultaneously, either:
  - minAvailable is the number of pods must always be available, even during a disruption.
  - maxUnavailable is the number of pods can be unavailable during a disruption.

NOTE

A maxUnavailable of 0% or 0 or a minAvailable of 100% or equal to the number of
replicas is permitted but can block nodes from being drained.

You can check for pod disruption budgets across all projects with the following:

```
$ oc poddisruptionbudget --all-namespaces
```

Example output

```
NAMESPACE     NAME    MIN-AVAILABLE SELECTOR
another-project another-pdb 4   bar=foo
test-project  my-pdb    2   foo=bar
```

The PodDisruptionBudget is considered healthy when there are at least minAvailable pods running in
the system. Every pod above that limit can be evicted.
NOTE

Depending on your pod priority and preemption settings, lower-priority pods might be removed despite their pod disruption budget requirements.

2.3.3.1. Specifying the number of pods that must be up with pod disruption budgets

You can use a **PodDisruptionBudget** object to specify the minimum number or percentage of replicas that must be up at a time.

**Procedure**

To configure a pod disruption budget:

1. Create a YAML file with the an object definition similar to the following:

   ```yaml
   apiVersion: policy/v1
   kind: PodDisruptionBudget
   metadata:
     name: my-pdb
   spec:
     minAvailable: 2
     selector:
       matchLabels:
         foo: bar
   ```

   - **1** `PodDisruptionBudget` is part of the **policy/v1** API group.
   - **2** The minimum number of pods that must be available simultaneously. This can be either an integer or a string specifying a percentage, for example, `20%`.
   - **3** A label query over a set of resources. The result of `matchLabels` and `matchExpressions` are logically conjoined. Leave this parameter blank, for example `selector {}`, to select all pods in the project.

   Or:

   ```yaml
   apiVersion: policy/v1
   kind: PodDisruptionBudget
   metadata:
     name: my-pdb
   spec:
     maxUnavailable: 25%
     selector:
       matchLabels:
         foo: bar
   ```

   - **1** `PodDisruptionBudget` is part of the **policy/v1** API group.
   - **2** The maximum number of pods that can be unavailable simultaneously. This can be either an integer or a string specifying a percentage, for example, `20%`.
   - **3**
A label query over a set of resources. The result of `matchLabels` and `matchExpressions` are logically conjoined. Leave this parameter blank, for example `selector {}`, to select all.

2. Run the following command to add the object to project:

   ```
   $ oc create -f </path/to/file> -n <project_name>
   ```

### 2.3.4. Preventing pod removal using critical pods

There are a number of core components that are critical to a fully functional cluster, but, run on a regular cluster node rather than the master. A cluster might stop working properly if a critical add-on is evicted.

Pods marked as critical are not allowed to be evicted.

**Procedure**

To make a pod critical:

1. Create a **Pod** spec or edit existing pods to include the `system-cluster-critical` priority class:

   ```
   spec:
     template:
       metadata:
         name: critical-pod
       priorityClassName: system-cluster-critical
   ```

   **1** Default priority class for pods that should never be evicted from a node.

   Alternatively, you can specify `system-node-critical` for pods that are important to the cluster but can be removed if necessary.

2. Create the pod:

   ```
   $ oc create -f <file-name>.yaml
   ```

### 2.4. AUTOMATICALLY SCALING PODS WITH THE HORIZONTAL POD AUTOSCALER

As a developer, you can use a horizontal pod autoscaler (HPA) to specify how OpenShift Container Platform should automatically increase or decrease the scale of a replication controller or deployment configuration, based on metrics collected from the pods that belong to that replication controller or deployment configuration. You can create an HPA for any deployment, deployment config, replica set, replication controller, or stateful set.

For information on scaling pods based on custom metrics, see [Automatically scaling pods based on custom metrics](#).

**NOTE**

It is recommended to use a **Deployment** object or **ReplicaSet** object unless you need a specific feature or behavior provided by other objects. For more information on these objects, see [Understanding Deployment and DeploymentConfig objects](#).
2.4.1. Understanding horizontal pod autoscalers

You can create a horizontal pod autoscaler to specify the minimum and maximum number of pods you want to run, as well as the CPU utilization or memory utilization your pods should target.

After you create a horizontal pod autoscaler, OpenShift Container Platform begins to query the CPU and/or memory resource metrics on the pods. When these metrics are available, the horizontal pod autoscaler computes the ratio of the current metric utilization with the desired metric utilization, and scales up or down accordingly. The query and scaling occurs at a regular interval, but can take one to two minutes before metrics become available.

For replication controllers, this scaling corresponds directly to the replicas of the replication controller. For deployment configurations, scaling corresponds directly to the replica count of the deployment configuration. Note that autoscaling applies only to the latest deployment in the Complete phase.

OpenShift Container Platform automatically accounts for resources and prevents unnecessary autoscaling during resource spikes, such as during start up. Pods in the unready state have 0 CPU usage when scaling up and the autoscaler ignores the pods when scaling down. Pods without known metrics have 0% CPU usage when scaling up and 100% CPU when scaling down. This allows for more stability during the HPA decision. To use this feature, you must configure readiness checks to determine if a new pod is ready for use.

To use horizontal pod autoscalers, your cluster administrator must have properly configured cluster metrics.

2.4.1.1. Supported metrics

The following metrics are supported by horizontal pod autoscalers:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>API version</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU utilization</td>
<td>Number of CPU cores used. Can be used to calculate a percentage of the pod’s requested CPU.</td>
<td>autoscaling/v1, autoscaling/v2</td>
</tr>
<tr>
<td>Memory utilization</td>
<td>Amount of memory used. Can be used to calculate a percentage of the pod’s requested memory.</td>
<td>autoscaling/v2</td>
</tr>
</tbody>
</table>
IMPORTANT

For memory-based autoscaling, memory usage must increase and decrease proportionally to the replica count. On average:

- An increase in replica count must lead to an overall decrease in memory (working set) usage per-pod.
- A decrease in replica count must lead to an overall increase in per-pod memory usage.

Use the OpenShift Container Platform web console to check the memory behavior of your application and ensure that your application meets these requirements before using memory-based autoscaling.

The following example shows autoscaling for the image-registry Deployment object. The initial deployment requires 3 pods. The HPA object increases the minimum to 5. If CPU usage on the pods reaches 75%, the pods increase to 7:

```
$ oc autoscale deployment/image-registry --min=5 --max=7 --cpu-percent=75
```

Example output

```
horizontalpodautoscaler.autoscaling/image-registry autoscaled
```

Sample HPA for the image-registry Deployment object with minReplicas set to 3

```
apiVersion: autoscaling/v1
class: HorizontalPodAutoscaler
metadata:
  name: image-registry
  namespace: default
spec:
  maxReplicas: 7
  minReplicas: 3
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: image-registry
  targetCPUUtilizationPercentage: 75
status:
  currentReplicas: 5
  desiredReplicas: 0
```

1. View the new state of the deployment:

```
$ oc get deployment image-registry
```

There are now 5 pods in the deployment:

Example output

```
NAME     REVISION DESIRED  CURRENT  TRIGGERED BY
image-registry 1  5  5  config
```
2.4.2. How does the HPA work?

The horizontal pod autoscaler (HPA) extends the concept of pod auto-scaling. The HPA lets you create and manage a group of load-balanced nodes. The HPA automatically increases or decreases the number of pods when a given CPU or memory threshold is crossed.

Figure 2.1. High level workflow of the HPA

The HPA is an API resource in the Kubernetes autoscaling API group. The autoscaler works as a control loop with a default of 15 seconds for the sync period. During this period, the controller manager queries the CPU, memory utilization, or both, against what is defined in the YAML file for the HPA. The controller manager obtains the utilization metrics from the resource metrics API for per-pod resource metrics like CPU or memory, for each pod that is targeted by the HPA.

If a utilization value target is set, the controller calculates the utilization value as a percentage of the equivalent resource request on the containers in each pod. The controller then takes the average of utilization across all targeted pods and produces a ratio that is used to scale the number of desired replicas. The HPA is configured to fetch metrics from `metrics.k8s.io`, which is provided by the metrics server. Because of the dynamic nature of metrics evaluation, the number of replicas can fluctuate during scaling for a group of replicas.

**NOTE**

To implement the HPA, all targeted pods must have a resource request set on their containers.

2.4.3. About requests and limits

The scheduler uses the resource request that you specify for containers in a pod, to decide which node to place the pod on. The kubelet enforces the resource limit that you specify for a container to ensure that the container is not allowed to use more than the specified limit. The kubelet also reserves the request amount of that system resource specifically for that container to use.

**How to use resource metrics?**

In the pod specifications, you must specify the resource requests, such as CPU and memory. The HPA uses this specification to determine the resource utilization and then scales the target up or down.
For example, the HPA object uses the following metric source:

```yaml
  type: Resource
  resource:
    name: cpu
  target:
    type: Utilization
    averageUtilization: 60
```

In this example, the HPA keeps the average utilization of the pods in the scaling target at 60%. Utilization is the ratio between the current resource usage to the requested resource of the pod.

### 2.4.4. Best practices

#### All pods must have resource requests configured

The HPA makes a scaling decision based on the observed CPU or memory utilization values of pods in an OpenShift Container Platform cluster. Utilization values are calculated as a percentage of the resource requests of each pod. Missing resource request values can affect the optimal performance of the HPA.

#### Configure the cool down period

During horizontal pod autoscaling, there might be a rapid scaling of events without a time gap. Configure the cool down period to prevent frequent replica fluctuations. You can specify a cool down period by configuring the `stabilizationWindowSeconds` field. The stabilization window is used to restrict the fluctuation of replicas count when the metrics used for scaling keep fluctuating. The autoscaling algorithm uses this window to infer a previous desired state and avoid unwanted changes to workload scale.

For example, a stabilization window is specified for the `scaleDown` field:

```yaml
  behavior:
    scaleDown:
      stabilizationWindowSeconds: 300
```

In the above example, all desired states for the past 5 minutes are considered. This approximates a rolling maximum, and avoids having the scaling algorithm frequently remove pods only to trigger recreating an equivalent pod just moments later.

#### 2.4.4.1. Scaling policies

The `autoscaling/v2` API allows you to add scaling policies to a horizontal pod autoscaler. A scaling policy controls how the OpenShift Container Platform horizontal pod autoscaler (HPA) scales pods. Scaling policies allow you to restrict the rate that HPAs scale pods up or down by setting a specific number or specific percentage to scale in a specified period of time. You can also define a stabilization window, which uses previously computed desired states to control scaling if the metrics are fluctuating. You can create multiple policies for the same scaling direction, and determine which policy is used, based on the amount of change. You can also restrict the scaling by timed iterations. The HPA scales pods during an iteration, then performs scaling, as needed, in further iterations.

#### Sample HPA object with a scaling policy

```yaml
apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
```
Specifies the direction for the scaling policy, either `scaleDown` or `scaleUp`. This example creates a policy for scaling down.

2. Defines the scaling policy.

3. Determines if the policy scales by a specific number of pods or a percentage of pods during each iteration. The default value is `pods`.

4. Determines the amount of scaling, either the number of pods or percentage of pods, during each iteration. There is no default value for scaling down by number of pods.

5. Determines the length of a scaling iteration. The default value is 15 seconds.

6. The default value for scaling down by percentage is 100%.

7. Determines which policy to use first, if multiple policies are defined. Specify `Max` to use the policy that allows the highest amount of change, `Min` to use the policy that allows the lowest amount of change, or `Disabled` to prevent the HPA from scaling in that policy direction. The default value is `Max`.

8. Determines the time period the HPA should look back at desired states. The default value is 0.

9. This example creates a policy for scaling up.

10. The amount of scaling up by the number of pods. The default value for scaling up the number of pods is 4%.

11. The amount of scaling up by the percentage of pods. The default value for scaling up by percentage is 100%.
Example policy for scaling down

apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
  name: hpa-resource-metrics-memory
  namespace: default
spec:
  minReplicas: 20
  behavior:
    scaleDown:
      stabilizationWindowSeconds: 300
      policies:
      - type: Pods
        value: 4
        periodSeconds: 30
      - type: Percent
        value: 10
        periodSeconds: 60
      selectPolicy: Max
    scaleUp:
      selectPolicy: Disabled

In this example, when the number of pods is greater than 40, the percent-based policy is used for scaling down, as that policy results in a larger change, as required by the selectPolicy.

If there are 80 pod replicas, in the first iteration the HPA reduces the pods by 8, which is 10% of the 80 pods (based on the type: Percent and value: 10 parameters), over one minute (periodSeconds: 60). For the next iteration, the number of pods is 72. The HPA calculates that 10% of the remaining pods is 7.2, which it rounds up to 8 and scales down 8 pods. On each subsequent iteration, the number of pods to be scaled is re-calculated based on the number of remaining pods. When the number of pods falls below 40, the pods-based policy is applied, because the pod-based number is greater than the percent-based number. The HPA reduces 4 pods at a time (type: Pods and value: 4), over 30 seconds (periodSeconds: 30), until there are 20 replicas remaining (minReplicas).

The selectPolicy: Disabled parameter prevents the HPA from scaling up the pods. You can manually scale up by adjusting the number of replicas in the replica set or deployment set, if needed.

If set, you can view the scaling policy by using the oc edit command:

$ oc edit hpa hpa-resource-metrics-memory

Example output

apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  annotations:
    autoscaling.alpha.kubernetes.io/behavior:
      
    
    ["ScaleUp":null,"StabilizationWindowSeconds":0,"SelectPolicy":null,"Policies":null]
    ["Type":"Pods","Value":4,"PeriodSeconds":15],
    ["Type":"Percent","Value":100,"PeriodSeconds":15])

2.4.5. Creating a horizontal pod autoscaler by using the web console

From the web console, you can create a horizontal pod autoscaler (HPA) that specifies the minimum and maximum number of pods you want to run on a Deployment or DeploymentConfig object. You can also define the amount of CPU or memory usage that your pods should target.

NOTE
An HPA cannot be added to deployments that are part of an Operator-backed service, Knative service, or Helm chart.

Procedure
To create an HPA in the web console:

1. In the Topology view, click the node to reveal the side pane.

2. From the Actions drop-down list, select Add HorizontalPodAutoscaler to open the Add HorizontalPodAutoscaler form.

3. From the Add HorizontalPodAutoscaler form, define the name, minimum and maximum pod limits, the CPU and memory usage, and click Save.

NOTE
If any of the values for CPU and memory usage are missing, a warning is displayed.

To edit an HPA in the web console:
1. In the **Topology** view, click the node to reveal the side pane.

2. From the **Actions** drop-down list, select **Edit HorizontalPodAutoscaler** to open the **Edit Horizontal Pod Autoscaler** form.

3. From the **Edit Horizontal Pod Autoscaler** form, edit the minimum and maximum pod limits and the CPU and memory usage, and click **Save**.

**NOTE**

While creating or editing the horizontal pod autoscaler in the web console, you can switch from **Form view** to **YAML view**.

To remove an HPA in the web console:

1. In the **Topology** view, click the node to reveal the side panel.

2. From the **Actions** drop-down list, select **Remove HorizontalPodAutoscaler**.

3. In the confirmation pop-up window, click **Remove** to remove the HPA.

### 2.4.6. Creating a horizontal pod autoscaler for CPU utilization by using the CLI

Using the OpenShift Container Platform CLI, you can create a horizontal pod autoscaler (HPA) to automatically scale an existing **Deployment**, **DeploymentConfig**, **ReplicaSet**, **ReplicationController**, or **StatefulSet** object. The HPA scales the pods associated with that object to maintain the CPU usage you specify.

**NOTE**

It is recommended to use a **Deployment** object or **ReplicaSet** object unless you need a specific feature or behavior provided by other objects.

The HPA increases and decreases the number of replicas between the minimum and maximum numbers to maintain the specified CPU utilization across all pods.

When autoscaling for CPU utilization, you can use the `oc autoscale` command and specify the minimum and maximum number of pods you want to run at any given time and the average CPU utilization your pods should target. If you do not specify a minimum, the pods are given default values from the OpenShift Container Platform server.

To autoscale for a specific CPU value, create a **HorizontalPodAutoscaler** object with the target CPU and pod limits.

### Prerequisites

To use horizontal pod autoscalers, your cluster administrator must have properly configured cluster metrics. You can use the `oc describe PodMetrics <pod-name>` command to determine if metrics are configured. If metrics are configured, the output appears similar to the following, with **Cpu** and **Memory** displayed under **Usage**.

```
$ oc describe PodMetrics openshift-kube-scheduler-ip-10-0-135-131.ec2.internal
```

**Example output**

-
Procedure

To create a horizontal pod autoscaler for CPU utilization:

1. Perform one of the following one of the following:
   - To scale based on the percent of CPU utilization, create a **HorizontalPodAutoscaler** object for an existing object:

     ```
     $ oc autoscale <object_type>/<name> \
     --min <number> \  
     --max <number> \ 
     --cpu-percent=<percent>  
     ```

     **1** Specify the type and name of the object to autoscale. The object must exist and be a **Deployment**, DeploymentConfig/dc, ReplicaSet/rs, ReplicationController/rc, or StatefulSet.

     **2** Optionally, specify the minimum number of replicas when scaling down.

     **3** Specify the maximum number of replicas when scaling up.

     **4** Specify the target average CPU utilization over all the pods, represented as a percent of requested CPU. If not specified or negative, a default autoscaling policy is used.

   For example, the following command shows autoscaling for the **image-registry** Deployment object. The initial deployment requires 3 pods. The HPA object increases the minimum to 5. If CPU usage on the pods reaches 75%, the pods will increase to 7:

     ```
     $ oc autoscale deployment/image-registry --min=5 --max=7 --cpu-percent=75
     ```
To scale for a specific CPU value, create a YAML file similar to the following for an existing object:

a. Create a YAML file similar to the following:

```
apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
  name: cpu-autoscale
  namespace: default
spec:
scaleTargetRef:
  apiVersion: apps/v1
  kind: Deployment
  name: example
  minReplicas: 1
  maxReplicas: 10
metrics:
- type: Resource
  resource:
    name: cpu
  target:
    type: AverageValue
    averageValue: 500m
```

1. Use the `autoscaling/v2` API.
2. Specify a name for this horizontal pod autoscaler object.
3. Specify the API version of the object to scale:
   - For a `Deployment`, `ReplicaSet`, `Statefulset` object, use `apps/v1`.
   - For a `ReplicationController`, use `v1`.
   - For a `DeploymentConfig`, use `apps.openshift.io/v1`.
4. Specify the type of object. The object must be a `Deployment`, `DeploymentConfig/dc`, `ReplicaSet/rs`, `ReplicationController/rc`, or `StatefulSet`.
5. Specify the name of the object to scale. The object must exist.
6. Specify the minimum number of replicas when scaling down.
7. Specify the maximum number of replicas when scaling up.
8. Use the `metrics` parameter for memory utilization.
9. Specify `cpu` for CPU utilization.
10. Set to `AverageValue`.
11. Set to `averageValue` with the targeted CPU value.

b. Create the horizontal pod autoscaler:
$ oc create -f <file-name>.yaml

2. Verify that the horizontal pod autoscaler was created:

$ oc get hpa cpu-autoscale

Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>REFERENCE</th>
<th>TARGETS</th>
<th>MINPODS</th>
<th>MAXPODS</th>
<th>REPLICAS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu-autoscale</td>
<td>Deployment/example</td>
<td>173m/500m</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>20m</td>
</tr>
</tbody>
</table>

2.4.7. Creating a horizontal pod autoscaler object for memory utilization by using the CLI

Using the OpenShift Container Platform CLI, you can create a horizontal pod autoscaler (HPA) to automatically scale an existing Deployment, DeploymentConfig, ReplicaSet, ReplicationController, or StatefulSet object. The HPA scales the pods associated with that object to maintain the average memory utilization you specify, either a direct value or a percentage of requested memory.

**NOTE**

It is recommended to use a Deployment object or ReplicaSet object unless you need a specific feature or behavior provided by other objects.

The HPA increases and decreases the number of replicas between the minimum and maximum numbers to maintain the specified memory utilization across all pods.

For memory utilization, you can specify the minimum and maximum number of pods and the average memory utilization your pods should target. If you do not specify a minimum, the pods are given default values from the OpenShift Container Platform server.

**Prerequisites**

To use horizontal pod autoscalers, your cluster administrator must have properly configured cluster metrics. You can use the `oc describe PodMetrics <pod-name>` command to determine if metrics are configured. If metrics are configured, the output appears similar to the following, with Cpu and Memory displayed under Usage.

$ oc describe PodMetrics openshift-kube-scheduler-ip-10-0-129-223.compute.internal -n openshift-kube-scheduler

**Example output**

Name: openshift-kube-scheduler-ip-10-0-129-223.compute.internal
Namespace: openshift-kube-scheduler
Labels: <none>
Annotations: <none>
API Version: metrics.k8s.io/v1beta1
Containers:
  Name: wait-for-host-port
Usage:
  Cpu: 0
Procedure

To create a horizontal pod autoscaler for memory utilization:

1. Create a YAML file for one of the following:

   - To scale for a specific memory value, create a `HorizontalPodAutoscaler` object similar to the following for an existing object:


```
apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
  name: hpa-resource-metrics-memory
  namespace: default
spec:
scaleTargetRef:
  apiVersion: apps/v1
  kind: Deployment
  name: example
  minReplicas: 1
  maxReplicas: 10
metrics:
  - type: Resource
    resource:
      name: memory
    target:
      type: AverageValue
      averageValue: 500Mi
behavior:
scaleDown:
  stabilizationWindowSeconds: 300
policies:
  - type: Pods
    value: 4
    periodSeconds: 60
  - type: Percent
    value: 10
    periodSeconds: 60
selectPolicy: Max
```
Use the `autoscaling/v2` API.

Specify a name for this horizontal pod autoscaler object.

Specify the API version of the object to scale:
- For a `Deployment`, `ReplicaSet`, or `Statefulset` object, use `apps/v1`.
- For a `ReplicationController`, use `v1`.
- For a `DeploymentConfig`, use `apps.openshift.io/v1`.

Specify the type of object. The object must be a `Deployment`, `DeploymentConfig`, `ReplicaSet`, `ReplicationController`, or `StatefulSet`.

Specify the name of the object to scale. The object must exist.

Specify the minimum number of replicas when scaling down.

Specify the maximum number of replicas when scaling up.

Use the `metrics` parameter for memory utilization.

Specify `memory` for memory utilization.

Set the type to `AverageValue`.

Specify `averageValue` and a specific memory value.

Optional: Specify a scaling policy to control the rate of scaling up or down.

- To scale for a percentage, create a `HorizontalPodAutoscaler` object similar to the following for an existing object:

```
apiVersion: autoscaling/v2
kind: HorizontalPodAutoscaler
metadata:
  name: memory-autoscale
  namespace: default
spec:
scaleTargetRef:
  apiVersion: apps/v1
  kind: Deployment
  name: example
minReplicas: 1
maxReplicas: 10
metrics:
  - type: Deployment
    resource:
      name: memory
    target:
      type: Utilization
      averageUtilization: 50
behavior: 12
```
Use the `autoscaling/v2` API.

Specify a name for this horizontal pod autoscaler object.

Specify the API version of the object to scale:
- For a ReplicationController, use `v1`.
- For a DeploymentConfig, use `apps.openshift.io/v1`.
- For a Deployment, ReplicaSet, Statefulset object, use `apps/v1`.

Specify the type of object. The object must be a `Deployment`, `DeploymentConfig`, `ReplicaSet`, `ReplicationController`, or `StatefulSet`.

Specify the name of the object to scale. The object must exist.

Specify the minimum number of replicas when scaling down.

Specify the maximum number of replicas when scaling up.

Use the `metrics` parameter for memory utilization.

Specify `memory` for memory utilization.

Set to `Utilization`.

Specify `averageUtilization` and a target average memory utilization over all the pods, represented as a percent of requested memory. The target pods must have memory requests configured.

Optional: Specify a scaling policy to control the rate of scaling up or down.

2. Create the horizontal pod autoscaler:

   ```bash
   $ oc create -f <file-name>.yaml
   $ oc create -f hpa.yaml
   ```

   For example:

   ```bash
   $ oc create -f hpa.yaml
   ```

   Example output

   ```bash
   horizontalpodautoscaler.autoscaling/hpa-resource-metrics-memory created
   ```
3. Verify that the horizontal pod autoscaler was created:

```
$ oc get hpa hpa-resource-metrics-memory
```

**Example output**

```
NAME                          REFERENCE            TARGETS         MINPODS   MAXPODS
REPLICAS   AGE              
hpa-resource-metrics-memory   Deployment/example   2441216/500Mi   1         10        1
20m
```

```
$ oc describe hpa hpa-resource-metrics-memory
```

**Example output**

```
Name:                        hpa-resource-metrics-memory
Namespace:                   default
Labels:                      <none>
Annotations:                 <none>
Reference:                   Deployment/example
Metrics:                     ( current / target )
   resource memory on pods:   2441216 / 500Mi
Min replicas:                1
Max replicas:                10
ReplicationController pods:  1 current / 1 desired
Conditions:
   Type            Status  Reason              Message
----            ------  ------              -------
   AbleToScale     True    ReadyForNewScale    recommended size matches current size
   ScalingActive   True    ValidMetricFound    the HPA was able to successfully calculate a
replica count from memory resource
   ScalingLimited  False   DesiredWithinRange  the desired count is within the acceptable
range
Events:
   Type     Reason                   Age                 From                       Message
   ----     ------                   ----                ----                       -------
   Normal   SuccessfulRescale        6m34s               horizontal-pod-autoscaler New size: 1;
reason: All metrics below target
```

### 2.4.8. Understanding horizontal pod autoscaler status conditions by using the CLI

You can use the status conditions set to determine whether or not the horizontal pod autoscaler (HPA) is able to scale and whether or not it is currently restricted in any way.

The HPA status conditions are available with the **v2** version of the autoscaling API.

The HPA responds with the following status conditions:

- **The AbleToScale** condition indicates whether HPA is able to fetch and update metrics, as well as whether any backoff-related conditions could prevent scaling.
  - A **True** condition indicates scaling is allowed.
- A **False** condition indicates scaling is not allowed for the reason specified.

- The **ScalingActive** condition indicates whether the HPA is enabled (for example, the replica count of the target is not zero) and is able to calculate desired metrics.
  - A **True** condition indicates metrics is working properly.
  - A **False** condition generally indicates a problem with fetching metrics.

- The **ScalingLimited** condition indicates that the desired scale was capped by the maximum or minimum of the horizontal pod autoscaler.
  - A **True** condition indicates that you need to raise or lower the minimum or maximum replica count in order to scale.
  - A **False** condition indicates that the requested scaling is allowed.

```bash
$ oc describe hpa cm-test
```

**Example output**

Name: cm-test  
Namespace: prom  
Labels: <none>  
Annotations: <none>  
CreationTimestamp: Fri, 16 Jun 2017 18:09:22 +0000  
Reference: ReplicationController/cm-test  
Metrics: ( current / target )  
"http_requests" on pods: 66m / 500m  
Min replicas: 1  
Max replicas: 4  
ReplicationController pods: 1 current / 1 desired  
Conditions: 

<table>
<thead>
<tr>
<th>Type</th>
<th>Status</th>
<th>Reason</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>AbleToScale</td>
<td>True</td>
<td>ReadyForNewScale</td>
<td>the last scale time was sufficiently old as to warrant a new scale</td>
</tr>
<tr>
<td>ScalingActive</td>
<td>True</td>
<td>ValidMetricFound</td>
<td>the HPA was able to successfully calculate a replica count from pods metric http_request</td>
</tr>
<tr>
<td>ScalingLimited</td>
<td>False</td>
<td>DesiredWithinRange</td>
<td>the desired replica count is within the acceptable range</td>
</tr>
</tbody>
</table>

Events:

**The horizontal pod autoscaler status messages.**

The following is an example of a pod that is unable to scale:

**Example output**

Conditions:

<table>
<thead>
<tr>
<th>Type</th>
<th>Status</th>
<th>Reason</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>AbleToScale</td>
<td>False</td>
<td>FailedGetScale</td>
<td>the HPA controller was unable to get the target's current scale: no matches for kind &quot;ReplicationController&quot; in group &quot;apps&quot;</td>
</tr>
</tbody>
</table>
The following is an example of a pod that could not obtain the needed metrics for scaling:

**Example output**

<table>
<thead>
<tr>
<th>Type</th>
<th>Reason</th>
<th>Age</th>
<th>From</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td>FailedGetScale</td>
<td>6s (x3 over 36s)</td>
<td>horizontal-pod-autoscaler</td>
<td>no matches for kind &quot;ReplicationController&quot; in group &quot;apps&quot;</td>
</tr>
</tbody>
</table>

The following is an example of a pod where the requested autoscaling was less than the required minimums:

**Example output**

<table>
<thead>
<tr>
<th>Type</th>
<th>Status</th>
<th>Reason</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>AbleToScale</td>
<td>True</td>
<td>SucceededGetScale</td>
<td>the HPA controller was able to get the target's current scale</td>
</tr>
<tr>
<td>ScalingActive</td>
<td>False</td>
<td>FailedGetResourceMetric</td>
<td>the HPA was unable to compute the replica count: failed to get cpu utilization: unable to get metrics for resource cpu: no metrics returned from resource metrics API</td>
</tr>
</tbody>
</table>

2.4.8.1. Viewing horizontal pod autoscaler status conditions by using the CLI

You can view the status conditions set on a pod by the horizontal pod autoscaler (HPA).

**NOTE**

The horizontal pod autoscaler status conditions are available with the v2 version of the autoscaling API.

**Prerequisites**

To use horizontal pod autoscalers, your cluster administrator must have properly configured cluster metrics. You can use the `oc describe PodMetrics <pod-name>` command to determine if metrics are configured. If metrics are configured, the output appears similar to the following, with **Cpu** and **Memory** displayed under **Usage**.

```
$ oc describe PodMetrics openshift-kube-scheduler-ip-10-0-135-131.ec2.internal
```

**Example output**
Procedure

To view the status conditions on a pod, use the following command with the name of the pod:

```
$ oc describe hpa <pod-name>
```

For example:

```
$ oc describe hpa cm-test
```

The conditions appear in the **Conditions** field in the output.

Example output

```
Name:             cm-test
Namespace:        prom
Labels:           <none>
Annotations:      <none>
CreationTimestamp: Fri, 16 Jun 2017 18:09:22 +0000
Reference:        ReplicationController/cm-test
Metrics:          ( current / target )
    "http_requests" on pods:  66m / 500m
Min replicas:     1
Max replicas:     4
ReplicationController pods:  1 current / 1 desired
Conditions: 1
    Type          Status    Reason               Message
                  -----    ------               -------
    AbleToScale   True      ReadyForNewScale   the last scale time was sufficiently old as to warrant a new scale
    ScalingActive True      ValidMetricFound   the HPA was able to successfully calculate a replica
```
2.4.9. Additional resources

- For more information on replication controllers and deployment controllers, see Understanding deployments and deployment configs.
- For an example on the usage of HPA, see Horizontal Pod Autoscaling of Quarkus Application Based on Memory Utilization.

2.5. AUTOMATICALLY SCALING PODS BASED ON CUSTOM METRICS

As a developer, you can use the custom metrics autoscaler to specify how OpenShift Container Platform should automatically increase or decrease the number of pods for a deployment, stateful set, custom resource, or job based on custom metrics that are not just based on CPU or memory.

**NOTE**

The custom metrics autoscaler currently supports only the Prometheus trigger, which can use the installed OpenShift Container Platform monitoring or an external Prometheus server as the metrics source.

**IMPORTANT**

The custom metrics autoscaler is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see [https://access.redhat.com/support/offerings/techpreview/](https://access.redhat.com/support/offerings/techpreview/).

2.5.1. Understanding the custom metrics autoscaler

The custom metrics autoscaler uses the Kubernetes-based Event Driven Autoscaler (KEDA) and is built on top of the OpenShift Container Platform horizontal pod autoscaler (HPA).

The Custom Metrics Autoscaler Operator scales your pods up and down based on custom, external metrics from specific applications. Your other applications continue to use other scaling methods. You configure *triggers*, also known as scalers, which are the source of events and metrics that the custom metrics autoscaler uses to determine how to scale. The custom metrics autoscaler uses a metrics API to convert the external metrics to a form that OpenShift Container Platform can use. The custom metrics autoscaler creates a horizontal pod autoscaler (HPA) that performs the actual scaling. The custom metrics autoscaler currently supports only the Prometheus trigger, which can use the installed OpenShift Container Platform monitoring or an external Prometheus server as the metrics source.

To use the custom metrics autoscaler, you create a *ScaledObject* or *ScaledJob* object, which defines the scaling metadata. You specify the deployment or job to scale, the source of the metrics to scale on (trigger), and other parameters such as the minimum and maximum replica counts allowed.
### NOTE

You can create only one scaled object or scaled job for each workload that you want to scale. Also, you cannot use a scaled object or scaled job and the horizontal pod autoscaler (HPA) on the same workload.

You can verify that the autoscaling has taken place by reviewing the number of pods in your custom resource or by reviewing the Custom Metrics Autoscaler Operator logs for messages similar to the following:

- Successfully set ScaleTarget replica count
- Successfully updated ScaleTarget

### 2.5.2. Installing the custom metrics autoscaler

You can use the OpenShift Container Platform web console to install the Custom Metrics Autoscaler Operator.

The installation creates five CRDs:

- `ClusterTriggerAuthentication`
- `KedaController`
- `ScaledJob`
- `ScaledObject`
- `TriggerAuthentication`

### Prerequisites

- If you use the community KEDA:
  - Uninstall the community KEDA. You cannot run both KEDA and the custom metrics autoscaler on the same OpenShift Container Platform cluster.
  - Remove the KEDA 1.x custom resource definitions by running the following commands:
    ```sh
    $ oc delete crd scaledobjects.keda.k8s.io
    $ oc delete crd triggerauthentications.keda.k8s.io
    ```

### Procedure

1. In the OpenShift Container Platform web console, click **Operators → OperatorHub**.

2. Choose **Custom Metrics Autoscaler** from the list of available Operators, and click **Install**.

3. On the **Install Operator** page, ensure that the **All namespaces on the cluster (default)** option is selected for **Installation Mode**. This installs the Operator in all namespaces.
4. Ensure that the **openshift-keda** namespace is selected for **Installed Namespace**. OpenShift Container Platform creates the namespace, if not present in your cluster.

5. Click **Install**.

6. Verify the installation by listing the Custom Metrics Autoscaler Operator components:
   a. Navigate to **Workloads → Pods**.
   b. Select the **openshift-keda** project from the drop-down menu and verify that the **custom-metrics-autoscaler-operator-** pod is running.
   c. Navigate to **Workloads → Deployments** to verify that the **custom-metrics-autoscaler-operator** deployment is running.

7. Optional: Verify the installation in the OpenShift CLI using the following commands:
   ```
   $ oc get all -n openshift-keda
   ```
   The output appears similar to the following:

   **Example output**
   ```
   NAME                                                      READY   STATUS     RESTARTS   AGE
   pod/custom-metrics-autoscaler-operator-5fd8d9fffd8-xt4xp   1/1     Running   0          18m
   NAME                                                 READY   UP-TO-DATE   AVAILABLE   AGE
   deployment.apps/custom-metrics-autoscaler-operator   1/1     1            1           18m
   NAME                                                            DESIRED   CURRENT   READY   AGE
   replicaset.apps/custom-metrics-autoscaler-operator-5fd8d9fffd8   1         1         1       18m
   ```

8. Install the **KedaController** custom resource, which creates the required CRDs:
   a. In the OpenShift Container Platform web console, click **Operators → Installed Operators**.
   b. Click **Custom Metrics Autoscaler**.
   c. On the **Operator Details** page, click the **KedaController** tab.
   d. On the **KedaController** tab, click **Create KedaController** and edit the file.
   ```
   kind: KedaController
   apiVersion: keda.sh/v1alpha1
   metadata:
     name: keda
     namespace: openshift-keda
   spec:
     watchNamespace: " (1)
     operator:
       logLevel: info (2)
       logEncoder: console (3)
       metricsServer:
         logLevel: '0' (4)
       serviceAccount: {}
1. Specifies the namespaces that the custom autoscaler should watch. Enter names in a comma-separated list. Omit or set empty to watch all namespaces. The default is.

2. Specifies the level of verbosity for the Custom Metrics Autoscaler Operator log messages. The allowed values are debug, info, error. The default is info.

3. Specifies the logging format for the Custom Metrics Autoscaler Operator log messages. The allowed values are console or json. The default is console.

4. Specifies the logging level for the Custom Metrics Autoscaler Metrics Server. The allowed values are 0 for info and 4 or debug. The default is 0.

e. Click Create to create the KEDAController.

2.5.3. Understanding the custom metrics autoscaler triggers

Triggers, also known as scalers, provide the metrics that the Custom Metrics Autoscaler Operator uses to scale your pods.

NOTE

The custom metrics autoscaler currently supports only the Prometheus trigger, which can use the installed OpenShift Container Platform monitoring or an external Prometheus server as the metrics source.

You use a ScaledObject or ScaledJob custom resource to configure triggers for specific objects, as described in the sections that follow.

2.5.3.1. Understanding the Prometheus trigger

Scale applications based on Prometheus metrics. See Additional resources for information on the configurations required to use the OpenShift Container Platform monitoring as a source for metrics.

NOTE

If Prometheus is taking metrics from the application that the custom metrics autoscaler is scaling, do not set the minimum replicas to 0 in the custom resource. If there are no application pods, the custom metrics autoscaler does not have any metrics to scale on.

Example scaled object with a Prometheus target

```yaml
apiVersion: keda.sh/v1alpha1
kind: ScaledObject
metadata:
  name: prom-scaledobject
  namespace: my-namespace
spec:
  ...
  triggers:
    - type: prometheus
      metadata:
        serverAddress: https://thanos-querier.openshift-monitoring.svc.cluster.local:9092
        namespace: kedatest
```
Specifies Prometheus as the scaler/trigger type. 

Specifies the address of the Prometheus server. This example uses OpenShift Container Platform monitoring. 

Optional: Specifies the namespace of the object you want to scale. This parameter is mandatory if OpenShift Container Platform monitoring as a source for the metrics. 

Specifies the name to identify the metric in the external.metrics.k8s.io API. If you are using more than one trigger, all metric names must be unique. 

Specifies the value to start scaling for. 

Specifies the Prometheus query to use. 

Specifies the authentication method to use. Prometheus scalers support bearer authentication, basic authentication, or TLS authentication. You configure the specific authentication parameters in a trigger authentication, as discussed in a following section. As needed, you can also use a secret. 

Additional resources 
- Configuring the custom metrics autoscaler to use OpenShift Container Platform monitoring 

2.5.4. Understanding custom metrics autoscaler trigger authentications 

A trigger authentication allows you to include authentication information in a scaled object or a scaled job that can be used by the associated containers. You can use trigger authentications to pass OpenShift Container Platform secrets, platform-native pod authentication mechanisms, environment variables, and so on. 

You define a TriggerAuthentication object in the same namespace as the object that you want to scale. That trigger authentication can be used only by objects in that namespace. 

Alternatively, to share credentials between objects in multiple namespaces, you can create a ClusterTriggerAuthentication object that can be used across all namespaces. 

Trigger authentications and cluster trigger authentication use the same configuration. However, a cluster trigger authentication requires an additional kind parameter in the authentication reference of the scaled object. 

Example trigger authentication with a secret 

```
kind: TriggerAuthentication
apiVersion: keda.sh/v1alpha1
metadata:
  name: secret-triggerauthentication
  namespace: my-namespace
spec:
  secretTargetRef:
```
Specifies the namespace of the object you want to scale.

Specifies that this trigger authentication uses a secret for authorization.

Specifies the authentication parameter to supply by using the secret.

Specifies the name of the secret to use.

Specifies the key in the secret to use with the specified parameter.

Example cluster trigger authentication with a secret

```
kind: ClusterTriggerAuthentication
apVersion: keda.sh/v1alpha1
metadata:
  name: secret-cluster-triggerauthentication
spec:
  secretTargetRef:
    - parameter: user-name
      name: my-secret
      key: USER_NAME
    - parameter: password
      name: my-secret
      key: PASSWORD
```

Note that no namespace is used with a cluster trigger authentication.

Specifies that this trigger authentication uses a secret for authorization.

Specifies the authentication parameter to supply by using the secret.

Specifies the name of the secret to use.

Specifies the key in the secret to use with the specified parameter.

Example trigger authentication with a token

```
kind: TriggerAuthentication
apiVersion: keda.sh/v1alpha1
metadata:
  name: token-triggerauthentication
  namespace: my-namespace
spec:
  secretTargetRef:
    - parameter: bearerToken
```

50
Specifies the namespace of the object you want to scale.

Specifies that this trigger authentication uses a secret for authorization.

Specifies the authentication parameter to supply by using the token.

Specifies the name of the token to use.

Specifies the key in the token to use with the specified parameter.

Example trigger authentication with an environment variable

```
kind: TriggerAuthentication
apiVersion: keda.sh/v1alpha1
metadata:
  name: env-var-triggerauthentication
namespace: my-namespace
spec:
  env:
    - parameter: access_key
      name: ACCESS_KEY
      containerName: my-container
```

1. Specifies the namespace of the object you want to scale.
2. Specifies that this trigger authentication uses environment variables for authorization.
3. Specify the parameter to set with this variable.
4. Specify the name of the environment variable.
5. Optional: Specify a container that requires authentication. The container must be in the same resource as referenced by `scaleTargetRef` in the scaled object.

Example trigger authentication with pod authentication providers

```
kind: TriggerAuthentication
apiVersion: keda.sh/v1alpha1
metadata:
  name: pod-id-triggerauthentication
namespace: my-namespace
spec:
  podIdentity:
    provider: aws-eks
```

1. Specifies the namespace of the object you want to scale.
2 Specifies that this trigger authentication uses a platform-native pod authentication method for authorization.

3 Specifies a pod identity. Supported values are none, azure, aws-eks, or aws-kiam. The default is none.

Additional references

- For information on OpenShift Container Platform secrets, see Providing sensitive data to pods.

2.5.4.1. Using trigger authentications

You use trigger authentications and cluster trigger authentications by using a custom resource to create the authentication, then add a reference to a scaled object or scaled job.

Prerequisites

- The Custom Metrics Autoscaler Operator must be installed.

- If you are using a secret, the Secret object must exist, for example:

  **Example secret**

  ```yaml
  apiVersion: v1
  kind: Secret
  metadata:
    name: my-secret
  data:
    user-name: <base64_username>
    password: <base64_password>
  ```

Procedure

1. Create the TriggerAuthentication or ClusterTriggerAuthentication object.

   a. Create a YAML file that defines the object:

      **Example trigger authentication with a secret**

      ```yaml
      kind: TriggerAuthentication
      apiVersion: keda.sh/v1alpha1
      metadata:
        name: prom-triggerauthentication
      namespace: my-namespace
      spec:
        secretTargetRef:
        - parameter: user-name
          name: my-secret
          key: USER_NAME
        - parameter: password
          name: my-secret
          key: PASSWORD
      ```
b. Create the **TriggerAuthentication** object:

```
$ oc create -f <file-name>.yaml
```

2. Create or edit a **ScaledObject** YAML file:

**Example scaled object**

```yaml
apiVersion: keda.sh/v1alpha1
kind: ScaledObject
metadata:
  name: scaledobject
  namespace: my-namespace
spec:
  scaleTargetRef:
    name: example-deployment
  maxReplicaCount: 100
  minReplicaCount: 0
  pollingInterval: 30
  triggers:
  - authenticationRef:
    type: prometheus
      metadata:
        serverAddress: https://thanos-querier.openshift-monitoring.svc.cluster.local:9092
        namespace: kedatest # replace <NAMESPACE>
        metricName: http_requests_total
        threshold: '5'
        query: sum(rate(http_requests_total{job="test-app"}[1m]))
        authModes: "basic"
  - authenticationRef: 1
    name: prom-triggerauthentication
    metadata:
      name: prom-triggerauthentication
      type: object
  - authenticationRef: 2
    name: prom-cluster-triggerauthentication
    kind: ClusterTriggerAuthentication
    metadata:
      name: prom-cluster-triggerauthentication
      type: object
```

1. Optional: Specify a trigger authentication.

2. Optional: Specify a cluster trigger authentication. You must include the **kind:** **ClusterTriggerAuthentication** parameter.

**NOTE**

It is not necessary to specify both a namespace trigger authentication and a cluster trigger authentication.

3. Create the object. For example:
2.5.5. Configuring the custom metrics autoscaler to use OpenShift Container Platform monitoring

You can use the installed OpenShift Container Platform monitoring as a source for the metrics used by the custom metrics autoscaler. However, there are some additional configurations you must perform.

**NOTE**

These steps are not required for an external Prometheus source.

You must perform the following tasks, as described in this section:

- Create a service account to get a token.
- Create a role.
- Add that role to the service account.
- Reference the token in the trigger authentication object used by Prometheus.

**Prerequisites**

- OpenShift Container Platform monitoring must be installed.
- Monitoring of user-defined workloads must be enabled in OpenShift Container Platform monitoring, as described in the Creating a user-defined workload monitoring config map section.
- The Custom Metrics Autoscaler Operator must be installed.

**Procedure**

1. Change to the project with the object you want to scale:

   ```bash
   $ oc project my-project
   ```

2. Use the following command to create a service account, if your cluster does not have one:

   ```bash
   $ oc create serviceaccount <service_account>
   ```

   where:

   `<service_account>`
   
   Specifies the name of the service account.

3. Use the following command to locate the token assigned to the service account:

   ```bash
   $ oc describe serviceaccount <service_account>
   ```

   where:
<service_account>
    Specifies the name of the service account.

**Example output**

Name: thanos
Namespace: my-project
Labels: <none>
Annotations: <none>
Image pull secrets: thanos-dockercfg-nnwgj
Mountable secrets: thanos-dockercfg-nnwgj
Tokens: thanos-token-9g4n5
Events: <none>

1. Use this token in the trigger authentication.

4. Create a trigger authentication with the service account token:
   a. Create a YAML file similar to the following:

```yaml
apiVersion: keda.sh/v1alpha1
class: TriggerAuthentication
metadata:
  name: keda-trigger-auth-prometheus
spec:
  secretTargetRef:
    - parameter: bearerToken
      name: thanos-token-9g4n5
      key: token
    - parameter: ca
      name: thanos-token-9g4n5
      key: ca.crt
```

   1. Specifies that this object uses a secret for authorization.
   2. Specifies the authentication parameter to supply by using the token.
   3. Specifies the name of the token to use.
   4. Specifies the key in the token to use with the specified parameter.

b. Create the CR object:

   ```bash
   $ oc create -f <file-name>.yaml
   ```

5. Create a role for reading Thanos metrics:
   a. Create a YAML file with the following parameters:

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: thanos-metrics-reader
```
Create the CR object:

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: thanos-metrics-reader
  namespace: my-project
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: thanos-metrics-reader
subjects:
  - kind: ServiceAccount
    name: thanos
    namespace: my-project
```

1. Specifies the name of the role you created.
2. Specifies the namespace of the object you want to scale.
3. Specifies the name of the service account to bind to the role.
4. Specifies the namespace of the object you want to scale.

You can now deploy a scaled object or scaled job to enable autoscaling for your application, as described in the following sections. To use OpenShift Container Platform monitoring as the source, in the trigger, or scaler, specify the `prometheus` type and use `https://thanos-querier.openshift-`
monitoring.svc.cluster.local:9092 as the serverAddress.

Additional references
- For information on enabling monitoring of user-defined workloads, see Creating a user-defined workload monitoring config map.

2.5.6. Understanding how to add custom metrics autoscalers

To add a custom metrics autoscaler, create a **ScaledObject** custom resource for a deployment, stateful set, or custom resource. Create a **ScaledJob** custom resource for a job.

You can create only one scaled object or scaled job for each workload that you want to scale. Also, you cannot use a scaled object or scaled job and the horizontal pod autoscaler (HPA) on the same workload.

2.5.6.1. Adding a custom metrics autoscaler to a workload

You can create a custom metrics autoscaler for a workload created by a **Deployment**, **StatefulSet**, or custom resource object.

**Prerequisites**
- The Custom Metrics Autoscaler Operator must be installed.

**Procedure**

1. Create a YAML file similar to the following:

   **Example scaled object**

   ```yaml
   apiVersion: keda.sh/v1alpha1
   kind: ScaledObject
   metadata:
     name: scaledobject
     namespace: my-namespace
   spec:
     scaleTargetRef:
       api: apps/v1
       name: example-deployment
       kind: Deployment
     envSourceContainerName: .spec.template.spec.containers[0]
     cooldownPeriod: 200
     maxReplicaCount: 100
     minReplicaCount: 0
     pollingInterval: 30
     advanced:
       restoreToOriginalReplicaCount: false
       horizontalPodAutoscalerConfig:
         behavior:
           scaleDown:
             stabilizationWindowSeconds: 300
             policies:
               - type: Percent
   ```
Optional: Specifies the API version of the target resource. The default is `apps/v1`.

2. Specifies the name of the object that you want to scale.

3. Specifies the kind as Deployment, StatefulSet or CustomResource.

4. Optional: Specifies the name of the container in the target resource, from which the custom autoscaler gets environment variables holding secrets and so forth. The default is `.spec.template.spec.containers[0]`.

5. Optional. Specifies the period in seconds to wait after the last trigger is reported before scaling the deployment back to 0 if the minReplicaCount is set to 0. The default is 300.

6. Optional: Specifies the maximum number of replicas when scaling up. The default is 100.

7. Optional: Specifies the minimum number of replicas when scaling down.

8. Optional: Specifies the interval in seconds to check each trigger on. The default is 30.

9. Optional: Specifies whether to scale back the target resource to the original replicas count after the scaled object is deleted. The default is `false`, which keeps the replica count as it is when the scaled object is deleted.

10. Optional: Specifies a scaling policy to use to control the rate to scale pods up or down. For more information, see the link in the "Additional resources" section that follows.

11. Specifies the trigger to use as the basis for scaling, as described in the "Understanding the custom metrics autoscaler triggers" section. This example uses OpenShift Container Platform monitoring.

12. Optional: Specifies a trigger authentication, as described in the "Creating a custom metrics autoscaler trigger authentication" section.

13. Optional: Specifies a cluster trigger authentication, as described in the "Creating a custom metrics autoscaler trigger authentication" section.
NOTE

It is not necessary to specify both a namespace trigger authentication and a cluster trigger authentication.

2. Create the custom metrics autoscaler:

   $ oc create -f <file-name>.yaml

Verification

- View the command output to verify that the custom metrics autoscaler was created:

   $ oc get scaledobject <scaled_object_name>

Example output

NAME            SCALETARGETKIND      SCALETARGETNAME        MIN   MAX   TRIGGERS AUTHENTICATION READY   ACTIVE   FALLBACK   AGE
scaledobject    apps/v1.Deployment   example-deployment     0     50    prometheus prom-triggerauthentication True    True     True       17s

Note the following fields in the output:

- **TRIGGERS**: Indicates the trigger, or scaler, that is being used.

- **AUTHENTICATION**: Indicates the name of any trigger authentication being used.

- **READY**: Indicates whether the scaled object is ready to start scaling:
  - If **True**, the scaled object is ready.
  - If **False**, the scaled object is not ready because of a problem in one or more of the objects you created.

- **ACTIVE**: Indicates whether scaling is taking place:
  - If **True**, scaling is taking place.
  - If **False**, scaling is not taking place because there are no metrics or there is a problem in one or more of the objects you created.

- **FALLBACK**: Indicates whether the custom metrics autoscaler is able to get metrics from the source
  - If **False**, the custom metrics autoscaler is getting metrics.
  - If **True**, the custom metrics autoscaler is getting metrics because there are no metrics or there is a problem in one or more of the objects you created.

Additional references

- Scaling policies
Understanding the custom metrics autoscaler triggers

Understanding custom metrics autoscaler trigger authentications

2.5.6.2. Adding a custom metrics autoscaler to a job

You can create a custom metrics autoscaler for any Job object.

Prerequisites

- The Custom Metrics Autoscaler Operator must be installed.

Procedure

1. Create a YAML file similar to the following:

```yaml
kind: ScaledJob
apiVersion: keda.sh/v1alpha1
metadata:
  name: scaledjob
  namespace: my-namespace
spec:
  failedJobsHistoryLimit: 5
  jobTargetRef:
    activeDeadlineSeconds: 600
    backoffLimit: 6
    parallelism: 1
    completions: 1
  template:
    metadata:
      name: pi
      spec:
        containers:
        - name: pi
          image: perl
          command: ["perl", "-Mbignum=bpi", "-wle", "print bpi(2000)"
          maxReplicaCount: 100
          pollingInterval: 30
          successfulJobsHistoryLimit: 5
          failedJobsHistoryLimit: 5
          envSourceContainerName: 10
          rolloutStrategy: gradual
          scalingStrategy:
            strategy: "custom"
            customScalingQueueLengthDeduction: 1
            customScalingRunningJobPercentage: "0.5"
          pendingPodConditions:
            - "Ready"
            - "PodScheduled"
            - "AnyOtherCustomPodCondition"
          multipleScalersCalculation: "max"
          triggers:
            - type: prometheus
```

OpenShift Container Platform 4.11 Nodes

60
metadata:
  serverAddress: https://thanos-querier.openshift-monitoring.svc.cluster.local:9092
  namespace: kedatest
  metricName: http_requests_total
  threshold: '5'
  query: sum(rate(http_requests_total{job="test-app"}[1m]))
  authModes: "bearer"
- authenticationRef: 14
  name: prom-triggerauthentication
  metadata:
    name: prom-triggerauthentication
    type: object
- authenticationRef: 15
  name: prom-cluster-triggerauthentication
  metadata:
    name: prom-cluster-triggerauthentication
    type: object

1. Specifies the maximum duration the job can run.
2. Specifies the number of retries for a job. The default is 6.
3. Optional: Specifies how many pod replicas a job should run in parallel; defaults to 1.
   - For non-parallel jobs, leave unset. When unset, the default is 1.
4. Optional: Specifies how many successful pod completions are needed to mark a job completed.
   - For non-parallel jobs, leave unset. When unset, the default is 1.
   - For parallel jobs with a fixed completion count, specify the number of completions.
   - For parallel jobs with a work queue, leave unset. When unset the default is the value of the `parallelism` parameter.
5. Specifies the template for the pod the controller creates.
6. Optional: Specifies the maximum number of replicas when scaling up. The default is 100.
7. Optional: Specifies the interval in seconds to check each trigger on. The default is 30.
8. Optional: Specifies the number of successful finished jobs should be kept. The default is 100.
9. Optional: Specifies how many failed jobs should be kept. The default is 100.
10. Optional: Specifies the name of the container in the target resource, from which the custom autoscaler gets environment variables holding secrets and so forth. The default is `.spec.template.spec.containers[0]`.
11. Optional: Specifies whether existing jobs are terminated whenever a scaled job is being updated:
   - **default**: The autoscaler terminates an existing job if its associated scaled job is updated. The autoscaler recreates the job with the latest specs.
- **gradual**: The autoscaler does not terminate an existing job if its associated scaled job is updated. The autoscaler creates new jobs with the latest specs.

12. Optional: Specifies a scaling strategy: **default**, **custom**, or **accurate**. The default is **default**. For more information, see the link in the "Additional resources" section that follows.

13. Specifies the trigger to use as the basis for scaling, as described in the "Understanding the custom metrics autoscaler triggers" section.

14. Optional: Specifies a trigger authentication, as described in the "Creating a custom metrics autoscaler trigger authentication" section.

15. Optional: Specifies a cluster trigger authentication, as described in the "Creating a custom metrics autoscaler trigger authentication" section.

**NOTE**

It is not necessary to specify both a namespace trigger authentication and a cluster trigger authentication.

2. Create the custom metrics autoscaler:

   $ oc create -f <file-name>.yaml

**Verification**

- View the command output to verify that the custom metrics autoscaler was created:

   $ oc get scaledjob <scaled_job_name>

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>MAX</th>
<th>TRIGGERS</th>
<th>AUTHENTICATION</th>
<th>READY</th>
<th>ACTIVE</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>scaledjob</td>
<td>100</td>
<td>prometheus</td>
<td>prom-triggerauthentication</td>
<td>True</td>
<td>True</td>
<td>8s</td>
</tr>
</tbody>
</table>

Note the following fields in the output:

- **TRIGGERS**: Indicates the trigger, or scaler, that is being used.

- **AUTHENTICATION**: Indicates the name of any trigger authentication being used.

- **READY**: Indicates whether the scaled object is ready to start scaling:
  - If **True**, the scaled object is ready.
  - If **False**, the scaled object is not ready because of a problem in one or more of the objects you created.

- **ACTIVE**: Indicates whether scaling is taking place:
  - If **True**, scaling is taking place.
  - If **False**, scaling is not taking place because there are no metrics or there is a problem in one or more of the objects you created.
Additional resources

- Understanding the custom metrics autoscaler triggers
- Understanding custom metrics autoscaler trigger authentications
- Running tasks in pods using jobs

2.5.7. Uninstalling the Custom Metrics Autoscaler Operator

You can remove the custom metrics autoscaler from your OpenShift Container Platform cluster. After removing the Custom Metrics Autoscaler Operator, remove other components associated with the Operator to avoid potential issues.

**NOTE**

You should delete the KedaController custom resource (CR) first. If you do not specifically delete the CR, OpenShift Container Platform can hang when you delete the openshift-keda project. If you delete the Custom Metrics Autoscaler Operator before deleting the CR, you are not able to delete the CR.

**Prerequisites**

- The Custom Metrics Autoscaler Operator must be installed.

**Procedure**

1. In the OpenShift Container Platform web console, click **Operators → Installed Operators**.
2. Switch to the openshift-keda project.
3. Remove the KedaController custom resource.
   a. Find the CustomMetricsAutoscaler Operator and click the KedaController tab.
   b. Find the custom resource, and then click **Delete KedaController**.
   c. Click **Uninstall**.
4. Remove the Custom Metrics Autoscaler Operator:
   a. Click **Operators → Installed Operators**.
   b. Find the CustomMetricsAutoscaler Operator and click the **Options** menu and select **Uninstall Operator**.
   c. Click **Uninstall**.
5. Optional: Use the OpenShift CLI to remove the custom metrics autoscaler components:
   a. Delete the custom metrics autoscaler CRDs:
      - **clustertriggerauthentications.keda.sh**
      - **kedacontrollers.keda.sh**
2.6. AUTOMATICALLY ADJUST POD RESOURCE LEVELS WITH THE VERTICAL POD AUTOSCALER

The OpenShift Container Platform Vertical Pod Autoscaler Operator (VPA) automatically reviews the historic and current CPU and memory resources for containers in pods and can update the resource limits and requests based on the usage values it learns. The VPA uses individual custom resources (CR) to update all of the pods associated with a workload object, such as a Deployment, DeploymentConfig, StatefulSet, Job, DaemonSet, ReplicaSet, or ReplicationController, in a project.

The VPA helps you to understand the optimal CPU and memory usage for your pods and can automatically maintain pod resources through the pod lifecycle.

2.6.1. About the Vertical Pod Autoscaler Operator

The Vertical Pod Autoscaler Operator (VPA) is implemented as an API resource and a custom resource (CR). The CR determines the actions the Vertical Pod Autoscaler Operator should take with the pods
associated with a specific workload object, such as a daemon set, replication controller, and so forth, in a project.

You can use the default recommender or use your own alternative recommender to autoscale based on your own algorithms.

The default recommender automatically computes historic and current CPU and memory usage for the containers in those pods and uses this data to determine optimized resource limits and requests to ensure that these pods are operating efficiently at all times. For example, the default recommender suggests reduced resources for pods that are requesting more resources than they are using and increased resources for pods that are not requesting enough.

The VPA then automatically deletes any pods that are out of alignment with these recommendations one at a time, so that your applications can continue to serve requests with no downtime. The workload objects then re-deploy the pods with the original resource limits and requests. The VPA uses a mutating admission webhook to update the pods with optimized resource limits and requests before the pods are admitted to a node. If you do not want the VPA to delete pods, you can view the VPA resource limits and requests and manually update the pods as needed.

**NOTE**

By default, workload objects must specify a minimum of two replicas in order for the VPA to automatically delete their pods. Workload objects that specify fewer replicas than this minimum are not deleted. If you manually delete these pods, when the workload object redeploys the pods, the VPA does update the new pods with its recommendations. You can change this minimum by modifying the `VerticalPodAutoscalerController` object as shown shown in Changing the VPA minimum value.

For example, if you have a pod that uses 50% of the CPU but only requests 10%, the VPA determines that the pod is consuming more CPU than requested and deletes the pod. The workload object, such as replica set, restarts the pods and the VPA updates the new pod with its recommended resources.

For developers, you can use the VPA to help ensure your pods stay up during periods of high demand by scheduling pods onto nodes that have appropriate resources for each pod.

Administrators can use the VPA to better utilize cluster resources, such as preventing pods from reserving more CPU resources than needed. The VPA monitors the resources that workloads are actually using and adjusts the resource requirements so capacity is available to other workloads. The VPA also maintains the ratios between limits and requests that are specified in initial container configuration.

**NOTE**

If you stop running the VPA or delete a specific VPA CR in your cluster, the resource requests for the pods already modified by the VPA do not change. Any new pods get the resources defined in the workload object, not the previous recommendations made by the VPA.

2.6.2. Installing the Vertical Pod Autoscaler Operator

You can use the OpenShift Container Platform web console to install the Vertical Pod Autoscaler Operator (VPA).

Procedure
1. In the OpenShift Container Platform web console, click Operators → OperatorHub.

2. Choose VerticalPodAutoscaler from the list of available Operators, and click Install.

3. On the Install Operator page, ensure that the Operator recommended namespace option is selected. This installs the Operator in the mandatory openshift-vertical-pod-autoscaler namespace, which is automatically created if it does not exist.

4. Click Install.

5. Verify the installation by listing the VPA Operator components:
   a. Navigate to Workloads → Pods.
   b. Select the openshift-vertical-pod-autoscaler project from the drop-down menu and verify that there are four pods running.
   c. Navigate to Workloads → Deployments to verify that there are four deployments running.

6. Optional. Verify the installation in the OpenShift Container Platform CLI using the following command:

   ```
   $ oc get all -n openshift-vertical-pod-autoscaler
   ```

   The output shows four pods and four deployments:

   Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>pod/vertical-pod-autoscaler-operator-85b4569c47-2gmhc</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>3m13s</td>
</tr>
<tr>
<td>pod/vpa-admission-plugin-default-67644fc87f-xq7k9</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>2m56s</td>
</tr>
<tr>
<td>pod/vpa-recommender-default-7c54764b59-8gckt</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>2m56s</td>
</tr>
<tr>
<td>pod/vpa-updater-default-7f6cc87858-47vw9</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>2m56s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>CLUSTER-IP</th>
<th>EXTERNAL-IP</th>
<th>PORT(S)</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>service/vpa-webhook</td>
<td>ClusterIP</td>
<td>172.30.53.206</td>
<td>&lt;none&gt;</td>
<td>443/TCP</td>
<td>2m56s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>UP-TO-DATE</th>
<th>AVAILABLE</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>deployment.apps/vertical-pod-autoscaler-operator</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>3m13s</td>
</tr>
<tr>
<td>deployment.apps/vpa-admission-plugin-default</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>2m56s</td>
</tr>
<tr>
<td>deployment.apps/vpa-recommender-default</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>2m56s</td>
</tr>
<tr>
<td>deployment.apps/vpa-updater-default</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>2m56s</td>
</tr>
</tbody>
</table>

   2.6.3. About Using the Vertical Pod Autoscaler Operator

   To use the Vertical Pod Autoscaler Operator (VPA), you create a VPA custom resource (CR) for a workload object in your cluster. The VPA learns and applies the optimal CPU and memory resources for the pods associated with that workload object. You can use a VPA with a deployment, stateful set, job, daemon set, replica set, or replication controller workload object. The VPA CR must be in the same project as the pods you want to monitor.
You use the VPA CR to associate a workload object and specify which mode the VPA operates in:

- The **Auto** and **Recreate** modes automatically apply the VPA CPU and memory recommendations throughout the pod lifetime. The VPA deletes any pods in the project that are out of alignment with its recommendations. When redeployed by the workload object, the VPA updates the new pods with its recommendations.

- The **Initial** mode automatically applies VPA recommendations only at pod creation.

- The **Off** mode only provides recommended resource limits and requests, allowing you to manually apply the recommendations. The **off** mode does not update pods.

You can also use the CR to opt-out certain containers from VPA evaluation and updates.

For example, a pod has the following limits and requests:

```yaml
resources:
  limits:
    cpu: 1
    memory: 500Mi
  requests:
    cpu: 500m
    memory: 100Mi
```

After creating a VPA that is set to **auto**, the VPA learns the resource usage and deletes the pod. When redeployed, the pod uses the new resource limits and requests:

```yaml
resources:
  limits:
    cpu: 50m
    memory: 1250Mi
  requests:
    cpu: 25m
    memory: 262144k
```

You can view the VPA recommendations using the following command:

```
$ oc get vpa <vpa-name> --output yaml
```

After a few minutes, the output shows the recommendations for CPU and memory requests, similar to the following:

**Example output**

```yaml
... status:
... recommendation:
  containerRecommendations:
  - containerName: frontend
    lowerBound:
      cpu: 25m
      memory: 262144k
    target:
      cpu: 25m
```
The output shows the recommended resources, **target**, the minimum recommended resources, **lowerBound**, the highest recommended resources, **upperBound**, and the most recent resource recommendations, **uncappedTarget**.

The VPA uses the **lowerBound** and **upperBound** values to determine if a pod needs to be updated. If a pod has resource requests below the **lowerBound** values or above the **upperBound** values, the VPA terminates and recreates the pod with the **target** values.

### 2.6.3.1. Changing the VPA minimum value

By default, workload objects must specify a minimum of two replicas in order for the VPA to automatically delete and update their pods. As a result, workload objects that specify fewer than two replicas are not automatically acted upon by the VPA. The VPA does update new pods from these workload objects if the pods are restarted by some process external to the VPA. You can change this cluster-wide minimum value by modifying the **minReplicas** parameter in the **VerticalPodAutoscalerController** custom resource (CR).

For example, if you set **minReplicas** to 3, the VPA does not delete and update pods for workload objects that specify fewer than three replicas.

**NOTE**

If you set **minReplicas** to 1, the VPA can delete the only pod for a workload object that specifies only one replica. You should use this setting with one-replica objects only if your workload can tolerate downtime whenever the VPA deletes a pod to adjust its resources. To avoid unwanted downtime with one-replica objects, configure the VPA CRs with the **podUpdatePolicy** set to **Initial**, which automatically updates the pod only when it is restarted by some process external to the VPA, or **Off**, which allows you to update the pod manually at an appropriate time for your application.

**Example VerticalPodAutoscalerController** object

```
apiVersion: autoscaling.openshift.io/v1
```
Specify the minimum number of replicas in a workload object for the VPA to act on. Any objects with replicas fewer than the minimum are not automatically deleted by the VPA.

2.6.3.2. Automatically applying VPA recommendations

To use the VPA to automatically update pods, create a VPA CR for a specific workload object with updateMode set to Auto or Recreate.

When the pods are created for the workload object, the VPA constantly monitors the containers to analyze their CPU and memory needs. The VPA deletes any pods that do not meet the VPA recommendations for CPU and memory. When redeployed, the pods use the new resource limits and requests based on the VPA recommendations, honoring any pod disruption budget set for your applications. The recommendations are added to the status field of the VPA CR for reference.

NOTE

By default, workload objects must specify a minimum of two replicas in order for the VPA to automatically delete their pods. Workload objects that specify fewer replicas than this minimum are not deleted. If you manually delete these pods, when the workload object redeploys the pods, the VPA does update the new pods with its recommendations. You can change this minimum by modifying the VerticalPodAutoscalerController object as shown shown in Changing the VPA minimum value.

Example VPA CR for the Auto mode

```yaml
apiVersion: autoscaling.k8s.io/v1
kind: VerticalPodAutoscaler
metadata:
  name: vpa-recommender
spec:
targetRef:
  apiVersion: "apps/v1"
  kind: Deployment
  name: frontend
updatePolicy:
  updateMode: "Auto"
```
The type of workload object you want this VPA CR to manage.

The name of the workload object you want this VPA CR to manage.

Set the mode to **Auto** or **Recreate**:

- **Auto**. The VPA assigns resource requests on pod creation and updates the existing pods by terminating them when the requested resources differ significantly from the new recommendation.

- **Recreate**. The VPA assigns resource requests on pod creation and updates the existing pods by terminating them when the requested resources differ significantly from the new recommendation. This mode should be used rarely, only if you need to ensure that the pods are restarted whenever the resource request changes.

**NOTE**

There must be operating pods in the project before the VPA can determine recommended resources and apply the recommendations to new pods.

### 2.6.3.3. Automatically applying VPA recommendations on pod creation

To use the VPA to apply the recommended resources only when a pod is first deployed, create a VPA CR for a specific workload object with `updateMode` set to **Initial**.

Then, manually delete any pods associated with the workload object that you want to use the VPA recommendations. In the **Initial** mode, the VPA does not delete pods and does not update the pods as it learns new resource recommendations.

#### Example VPA CR for the **Initial** mode

```yaml
apiVersion: autoscaling.k8s.io/v1
kind: VerticalPodAutoscaler
metadata:
  name: vpa-recommender
spec:
targetRef:
  apiVersion: "apps/v1"
  kind: Deployment
  name: frontend
updatePolicy:
  updateMode: "Initial"
```

1. The type of workload object you want this VPA CR to manage.
2. The name of the workload object you want this VPA CR to manage.
3. Set the mode to **Initial**. The VPA assigns resources when pods are created and does not change the resources during the lifetime of the pod.
NOTE
There must be operating pods in the project before a VPA can determine recommended resources and apply the recommendations to new pods.

2.6.3.4. Manually applying VPA recommendations

To use the VPA to only determine the recommended CPU and memory values, create a VPA CR for a specific workload object with `updateMode` set to `off`.

When the pods are created for that workload object, the VPA analyzes the CPU and memory needs of the containers and records those recommendations in the `status` field of the VPA CR. The VPA does not update the pods as it determines new resource recommendations.

Example VPA CR for the Off mode

```yaml
apiVersion: autoscaling.k8s.io/v1
kind: VerticalPodAutoscaler
metadata:
  name: vpa-recommender
spec:
targetRef:
  apiVersion: "apps/v1"
  kind:  Deployment
  name: frontend
updatePolicy:
  updateMode: "Off"
```

1. The type of workload object you want this VPA CR to manage.
2. The name of the workload object you want this VPA CR to manage.
3. Set the mode to `Off`.

You can view the recommendations using the following command.

```
$ oc get vpa <vpa-name> --output yaml
```

With the recommendations, you can edit the workload object to add CPU and memory requests, then delete and redeploy the pods using the recommended resources.

NOTE
There must be operating pods in the project before a VPA can determine recommended resources.

2.6.3.5. Exempting containers from applying VPA recommendations

If your workload object has multiple containers and you do not want the VPA to evaluate and act on all of the containers, create a VPA CR for a specific workload object and add a `resourcePolicy` to opt-out specific containers.
When the VPA updates the pods with recommended resources, any containers with a `resourcePolicy` are not updated and the VPA does not present recommendations for those containers in the pod.

```yaml
apiVersion: autoscaling.k8s.io/v1
kind: VerticalPodAutoscaler
metadata:
  name: vpa-recommender
spec:
targetRef:
  apiVersion: "apps/v1"
  kind:   Deployment
  name:   frontend
updatePolicy:
  updateMode: "Auto"
resourcePolicy:
  containerPolicies:
  - containerName: my-opt-sidecar
    mode: "Off"
```

1. The type of workload object you want this VPA CR to manage.
2. The name of the workload object you want this VPA CR to manage.
3. Set the mode to **Auto**, **Recreate**, or **Off**. The **Recreate** mode should be used rarely, only if you need to ensure that the pods are restarted whenever the resource request changes.
4. Specify the containers you want to opt-out and set `mode` to **Off**.

For example, a pod has two containers, the same resource requests and limits:

```yaml
# ... 
spec:
  containers:
  - name: frontend
    resources:
      limits:
        cpu: 1
        memory: 500Mi
      requests:
        cpu: 500m
        memory: 100Mi
  - name: backend
    resources:
      limits:
        cpu: "1"
        memory: 500Mi
      requests:
        cpu: 500m
        memory: 100Mi
# ...
```

After launching a VPA CR with the `backend` container set to opt-out, the VPA terminates and recreates the pod with the recommended resources applied only to the `frontend` container.
2.6.3.6. Using an alternative recommender

You can use your own recommender to autoscale based on your own algorithms. If you do not specify an alternative recommender, OpenShift Container Platform uses the default recommender, which suggests CPU and memory requests based on historical usage. Because there is no universal recommendation policy that applies to all types of workloads, you might want to create and deploy different recommenders for specific workloads.

For example, the default recommender might not accurately predict future resource usage when containers exhibit certain resource behaviors, such as cyclical patterns that alternate between usage spikes and idling as used by monitoring applications, or recurring and repeating patterns used with deep learning applications. Using the default recommender with these usage behaviors might result in significant over-provisioning and Out of Memory (OOM) kills for your applications.

**NOTE**

Instructions for how to create a recommender are beyond the scope of this documentation.

**Procedure**

To use an alternative recommender for your pods:

1. Create a service account for the alternative recommender and bind that service account to the required cluster role:

```yaml
apiVersion: v1 1
kind: ServiceAccount
metadata:
  name: alt-vpa-recommender-sa
  namespace: <namespace_name>
---
apiVersion: rbac.authorization.k8s.io/v1 2
```
kind: ClusterRoleBinding
metadata:
  name: system:example-metrics-reader
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: system:metrics-reader
subjects:
  - kind: ServiceAccount
    name: alt-vpa-recommender-sa
    namespace: <namespace_name>
---

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: system:example-vpa-actor
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: system:vpa-actor
subjects:
  - kind: ServiceAccount
    name: alt-vpa-recommender-sa
    namespace: <namespace_name>
---

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: system:example-vpa-target-reader-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: system:vpa-target-reader
subjects:
  - kind: ServiceAccount
    name: alt-vpa-recommender-sa
    namespace: <namespace_name>

1. Creates a service account for the recommender in the namespace where the recommender is deployed.

2. Binds the recommender service account to the `metrics-reader` role. Specify the namespace where the recommender is to be deployed.

3. Binds the recommender service account to the `vpa-actor` role. Specify the namespace where the recommender is to be deployed.

4. Binds the recommender service account to the `vpa-target-reader` role. Specify the namespace where the recommender is to be deployed.

2. To add the alternative recommender to the cluster, create a Deployment object similar to the following:

```yaml
apiVersion: apps/v1
kind: Deployment
```
metadata:
  name: alt-vpa-recommender
  namespace: <namespace_name>
spec:
  replicas: 1
  selector:
    matchLabels:
      app: alt-vpa-recommender
template:
  metadata:
    labels:
      app: alt-vpa-recommender
  spec:
    containers:
      - name: recommender
        image: quay.io/example/alt-recommender:latest
        imagePullPolicy: Always
        resources:
          limits:
            cpu: 200m
            memory: 1000Mi
          requests:
            cpu: 50m
            memory: 500Mi
        ports:
          - name: prometheus
            containerPort: 8942
        securityContext:
          allowPrivilegeEscalation: false
          capabilities:
            drop:
              - ALL
          seccompProfile:
            type: RuntimeDefault
          serviceAccountName: alt-vpa-recommender-sa
          securityContext:
            runAsNonRoot: true

1 Creates a container for your alternative recommender.
2 Specifies your recommender image.
3 Associates the service account that you created for the recommender.

A new pod is created for the alternative recommender in the same namespace.

$ oc get pods

Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>frontend-845d5478d-558zf</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>4m25s</td>
</tr>
<tr>
<td>frontend-845d5478d-7z9gx</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>4m25s</td>
</tr>
</tbody>
</table>
3. Configure a VPA CR that includes the name of the alternative recommender **Deployment** object.

**Example VPA CR to include the alternative recommender**

```yaml
apiVersion: autoscaling.k8s.io/v1
kind: VerticalPodAutoscaler
metadata:
  name: vpa-recommender
  namespace: <namespace_name>
spec:
  recommenders:
    - name: alt-vpa-recommender
  targetRef:
    apiVersion: "apps/v1"
    kind: Deployment
    name: frontend
```

1. Specifies the name of the alternative recommender deployment.
2. Specifies the name of an existing workload object you want this VPA to manage.

### 2.6.4. Using the Vertical Pod Autoscaler Operator

You can use the Vertical Pod Autoscaler Operator (VPA) by creating a VPA custom resource (CR). The CR indicates which pods it should analyze and determines the actions the VPA should take with those pods.

**Prerequisites**

- The workload object that you want to autoscale must exist.
- If you want to use an alternative recommender, a deployment including that recommender must exist.

**Procedure**

To create a VPA CR for a specific workload object:

1. Change to the project where the workload object you want to scale is located.
   a. Create a VPA CR YAML file:

```yaml
apiVersion: autoscaling.k8s.io/v1
kind: VerticalPodAutoscaler
metadata:
  name: vpa-recommender
spec:
  targetRef:
    apiVersion: "apps/v1"
    kind: Deployment
    name: frontend
```

1. OpenShift Container Platform 4.11 Nodes

76
Specify the type of workload object you want this VPA to manage: Deployment, StatefulSet, Job, DaemonSet, ReplicaSet, or ReplicationController.

Specify the name of an existing workload object you want this VPA to manage.

Specify the VPA mode:

- **auto** to automatically apply the recommended resources on pods associated with the controller. The VPA terminates existing pods and creates new pods with the recommended resource limits and requests.

- **recreate** to automatically apply the recommended resources on pods associated with the workload object. The VPA terminates existing pods and creates new pods with the recommended resource limits and requests. The **recreate** mode should be used rarely, only if you need to ensure that the pods are restarted whenever the resource request changes.

- **initial** to automatically apply the recommended resources when pods associated with the workload object are created. The VPA does not update the pods as it learns new resource recommendations.

- **off** to only generate resource recommendations for the pods associated with the workload object. The VPA does not update the pods as it learns new resource recommendations and does not apply the recommendations to new pods.

Optional. Specify the containers you want to opt-out and set the mode to **Off**.

Optional. Specify an alternative recommender.

b. Create the VPA CR:

```bash
$ oc create -f <file-name>.yaml
```

After a few moments, the VPA learns the resource usage of the containers in the pods associated with the workload object.

You can view the VPA recommendations using the following command:

```bash
$ oc get vpa <vpa-name> --output yaml
```

The output shows the recommendations for CPU and memory requests, similar to the following:

**Example output**

```yaml
name: frontend
updatePolicy:
  updateMode: "Auto"
resourcePolicy:
  containerPolicies:
    - containerName: my-opt-sidecar
      mode: "Off"
recommenders:
  - name: my-recommender
```
status:

recommendation:
  containerRecommendations:
  - containerName: frontend
    lowerBound: 1
      cpu: 25m
      memory: 262144k
    target: 2
      cpu: 25m
      memory: 262144k
    uncappedTarget: 3
      cpu: 25m
      memory: 262144k
    upperBound: 4
      cpu: 262m
      memory: "274357142"
  - containerName: backend
    lowerBound:
      cpu: 12m
      memory: 131072k
    target:
      cpu: 12m
      memory: 131072k
    uncappedTarget:
      cpu: 12m
      memory: 131072k
    upperBound:
      cpu: 476m
      memory: "498558823"


1. **lowerBound** is the minimum recommended resource levels.
2. **target** is the recommended resource levels.
3. **upperBound** is the highest recommended resource levels.
4. **uncappedTarget** is the most recent resource recommendations.

### 2.6.5. Uninstalling the Vertical Pod Autoscaler Operator

You can remove the Vertical Pod Autoscaler Operator (VPA) from your OpenShift Container Platform cluster. After uninstalling, the resource requests for the pods already modified by an existing VPA CR do not change. Any new pods get the resources defined in the workload object, not the previous recommendations made by the Vertical Pod Autoscaler Operator.
NOTE
You can remove a specific VPA using the `oc delete vpa <vpa-name>` command. The same actions apply for resource requests as uninstalling the vertical pod autoscaler.

After removing the VPA Operator, it is recommended that you remove other components associated with the Operator to avoid potential issues.

Prerequisites

- The Vertical Pod Autoscaler Operator must be installed.

Procedure

1. In the OpenShift Container Platform web console, click **Operators → Installed Operators**.
2. Switch to the **openshift-vertical-pod-autoscaler** project.
3. Find the **VerticalPodAutoscaler** Operator and click the Options menu. Select **Uninstall Operator**.
4. Optional: To remove all operands associated with the Operator, in the dialog box, select **Delete all operand instances for this operator** checkbox.
5. Click **Uninstall**.
6. Optional: Use the OpenShift CLI to remove the VPA components:
   a. Delete the VPA mutating webhook configuration:
      ```
      $ oc delete mutatingwebhookconfigurations/vpa-webhook-config
      ```
   b. List any VPA custom resources:
      ```
      $ oc get verticalpodautoscalercHECKPOINTS.autoscaling.k8s.io,verticalpodautoscalercontrollers.autoscaling.openshift.io,verticalpodautoscalers.autoscaling.k8s.io -o wide --all-namespaces
      ```
      Example output
      ```
      NAMESPACE      NAME                                                                       AGE
      my-project     verticalpodautoscalercheckpoint.autoscaling.k8s.io/vpa-recommender-httpd 5m46s

      NAMESPACE                           NAME                                                               AGE
      openshift-vertical-pod-autoscaler   verticalpodautoscalercontroller.autoscaling.openshift.io/default 11m

      NAMESPACE      NAME                                                       MODE   CPU   MEM
      PROVIDED   AGE
      my-project     verticalpodautoscaler.autoscaling.k8s.io/vpa-recommender   Auto   93m
      262144k   True       9m15s
      ```
   c. Delete the listed VPA custom resources. For example:
d. List any VPA custom resource definitions (CRDs):

```bash
$ oc get crd
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>CREATED AT</th>
</tr>
</thead>
<tbody>
<tr>
<td>verticalpodautoscalercheckpoints.autoscaling.k8s.io</td>
<td>2022-02-07T14:09:20Z</td>
</tr>
<tr>
<td>verticalpodautoscalercontrollers.autoscaling.openshift.io</td>
<td>2022-02-07T14:09:20Z</td>
</tr>
<tr>
<td>verticalpodautoscalers.autoscaling.k8s.io</td>
<td>2022-02-07T14:09:20Z</td>
</tr>
</tbody>
</table>

e. Delete the listed VPA CRDs:

```bash
$ oc delete crd verticalpodautoscalercheckpoints.autoscaling.k8s.io
verticalpodautoscalercontrollers.autoscaling.openshift.io
verticalpodautoscalers.autoscaling.k8s.io
```

Deleting the CRDs removes the associated roles, cluster roles, and role bindings. However, there might be a few cluster roles that must be manually deleted.

f. List any VPA cluster roles:

```bash
$ oc get clusterrole | grep openshift-vertical-pod-autoscaler
```

**Example output**

| openshift-vertical-pod-autoscaler-6896f-admin                        | 2022-02-02T15:29:55Z   |

g. Delete the listed VPA cluster roles. For example:

```bash
```

h. Delete the VPA Operator:

```bash
$ oc delete operator/vertical-pod-autoscaler.openshift-vertical-pod-autoscaler
```

### 2.7. PROVIDING SENSITIVE DATA TO PODS
Some applications need sensitive information, such as passwords and user names, that you do not want developers to have.

As an administrator, you can use Secret objects to provide this information without exposing that information in clear text.

### 2.7.1. Understanding secrets

The Secret object type provides a mechanism to hold sensitive information such as passwords, OpenShift Container Platform client configuration files, private source repository credentials, and so on. Secrets decouple sensitive content from the pods. You can mount secrets into containers using a volume plug-in or the system can use secrets to perform actions on behalf of a pod.

Key properties include:

- Secret data can be referenced independently from its definition.
- Secret data volumes are backed by temporary file-storage facilities (tmpfs) and never come to rest on a node.
- Secret data can be shared within a namespace.

**YAML Secret object definition**

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: test-secret
  namespace: my-namespace
type: Opaque
data:
  username: dmFsdWUtMQ0K
  password: dmFsdWUtMg0KDQo=
stringData:
  hostname: myapp.mydomain.com
```

1. Indicates the structure of the secret’s key names and values.
2. The allowable format for the keys in the data field must meet the guidelines in the DNS_SUBDOMAIN value in the Kubernetes identifiers glossary.
3. The value associated with keys in the data map must be base64 encoded.
4. Entries in the stringData map are converted to base64 and the entry will then be moved to the data map automatically. This field is write-only; the value will only be returned via the data field.
5. The value associated with keys in the stringData map is made up of plain text strings.

You must create a secret before creating the pods that depend on that secret.

When creating secrets:

- Create a secret object with secret data.
- Update the pod’s service account to allow the reference to the secret.
- Create a pod, which consumes the secret as an environment variable or as a file (using a secret volume).

### 2.7.1.1. Types of secrets

The value in the `type` field indicates the structure of the secret’s key names and values. The type can be used to enforce the presence of user names and keys in the secret object. If you do not want validation, use the `opaque` type, which is the default.

Specify one of the following types to trigger minimal server-side validation to ensure the presence of specific key names in the secret data:

- `kubernetes.io/service-account-token`. Uses a service account token.
- `kubernetes.io/basic-auth`. Use with Basic Authentication.
- `kubernetes.io/ssh-auth`. Use with SSH Key Authentication.
- `kubernetes.io/tls`. Use with TLS certificate authorities.

Specify `type: Opaque` if you do not want validation, which means the secret does not claim to conform to any convention for key names or values. An opaque secret, allows for unstructured `key:value` pairs that can contain arbitrary values.

**NOTE**

You can specify other arbitrary types, such as `example.com/my-secret-type`. These types are not enforced server-side, but indicate that the creator of the secret intended to conform to the key/value requirements of that type.

For examples of different secret types, see the code samples in Using Secrets.

### 2.7.1.2. Secret data keys

Secret keys must be in a DNS subdomain.

### 2.7.1.3. About automatically-generated service account token secrets

In 4.11, OpenShift Container Platform is adopting an enhancement from upstream Kubernetes, which enables the `LegacyServiceAccountTokenNoAutoGeneration` feature by default. As a result, when creating new service accounts (SA), a service account token secret is no longer automatically generated. Previously, OpenShift Container Platform automatically added a service account token to a secret for each new SA.

However, some features and workloads need service account token secrets to communicate with the Kubernetes API server, for example, the OpenShift Controller Manager. While this requirement will be changed in a future release, it remains in OpenShift Container Platform 4.11. As a result, if you need a service account token secret, you must manually use the TokenRequest API to request bound service account tokens or create a service account token secret.

After upgrading to 4.11, existing service account token secrets are not deleted and continue to function as expected.
NOTE
In 4.11, service account token secrets still appear to have been automatically generated. Although, instead creating two secrets per service account, OpenShift Container Platform now creates one token, which does not work. In a future release, the number will be further reduced to zero. Note that `dockercfg` secrets are still generated and no secrets are deleted during upgrades.

Additional resources
- For information about requesting bound service account tokens, see Using bound service account tokens
- For information about creating a service account token secret, see Creating a service account token secret.

2.7.2. Understanding how to create secrets
As an administrator you must create a secret before developers can create the pods that depend on that secret.

When creating secrets:

1. Create a secret object that contains the data you want to keep secret. The specific data required for each secret type is described in the following sections.

**Example YAML object that creates an opaque secret**

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: test-secret
type: Opaque
1
data:
  2
    username: dmFsdWUtMQ0K
    password: dmFsdWUtMQ0KDQo=
stringData:
  3
    hostname: myapp.mydomain.com
secret.properties: |
  property1=valueA
  property2=valueB
```

1. Specifies the type of secret.
2. Specifies encoded string and data.
3. Specifies decoded string and data.

Use either the `data` or `stringdata` fields, not both.

2. Update the pod’s service account to reference the secret:

**YAML of a service account that uses a secret**
3. Create a pod, which consumes the secret as an environment variable or as a file (using a secret volume):

**YAML of a pod populating files in a volume with secret data**

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: secret-example-pod
spec:
  containers:
    - name: secret-test-container
      image: busybox
      command: ["/bin/sh", "-c", "cat /etc/secret-volume/*"]
    volumes:
      - name: secret-volume
        mountPath: /etc/secret-volume
        readOnly: true
  restartPolicy: Never
```

1. Add a **volumeMounts** field to each container that needs the secret.
2. Specifies an unused directory name where you would like the secret to appear. Each key in the secret data map becomes the filename under **mountPath**.
3. Set to **true**. If true, this instructs the driver to provide a read-only volume.
4. Specifies the name of the secret.

**YAML of a pod populating environment variables with secret data**

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: secret-example-pod
spec:
  containers:
    - name: secret-test-container
      image: busybox
      command: ["/bin/sh", "-c", "export"]
    env:
      - name: TEST_SECRET_USERNAME_ENV_VAR
        valueFrom:
```

```yaml
OpenShift Container Platform 4.11 Nodes
```
Specifies the environment variable that consumes the secret key.

---

### YAML of a build config populating environment variables with secret data

```yaml
apiVersion: build.openshift.io/v1
kind: BuildConfig
metadata:
  name: secret-example-bc
spec:
  strategy:
    sourceStrategy:
      env:
      - name: TEST_SECRET_USERNAME_ENV_VAR
        valueFrom:
          secretKeyRef:
            name: test-secret
            key: username
```

---

1. Specifies the environment variable that consumes the secret key.

---

### 2.7.2.1. Secret creation restrictions

To use a secret, a pod needs to reference the secret. A secret can be used with a pod in three ways:

- To populate environment variables for containers.
- As files in a volume mounted on one or more of its containers.
- By kubelet when pulling images for the pod.

Volume type secrets write data into the container as a file using the volume mechanism. Image pull secrets use service accounts for the automatic injection of the secret into all pods in a namespace.

When a template contains a secret definition, the only way for the template to use the provided secret is to ensure that the secret volume sources are validated and that the specified object reference actually points to a `Secret` object. Therefore, a secret needs to be created before any pods that depend on it.

The most effective way to ensure this is to have it get injected automatically through the use of a service account.

---

Secret API objects reside in a namespace. They can only be referenced by pods in that same namespace.

---

Individual secrets are limited to 1MB in size. This is to discourage the creation of large secrets that could exhaust apiserver and kubelet memory. However, creation of a number of smaller secrets could also exhaust memory.

---

### 2.7.2.2. Creating an opaque secret
As an administrator, you can create an opaque secret, which allows you to store unstructured **key:value** pairs that can contain arbitrary values.

**Procedure**

1. Create a **Secret** object in a YAML file on a control plane node.
   
   For example:
   ```yaml
   apiVersion: v1
   kind: Secret
   metadata:
     name: mysecret
   type: Opaque
   data:
     username: dXNlcj1uYW1l
     password: cGFzc3dvcmQ=  
   ```
   
   1. Specifies an opaque secret.

2. Use the following command to create a **Secret** object:
   ```bash
   $ oc create -f <filename>.yaml  
   ```

3. To use the secret in a pod:
   a. Update the pod’s service account to reference the secret, as shown in the "Understanding how to create secrets" section.
   
   b. Create the pod, which consumes the secret as an environment variable or as a file (using a **secret** volume), as shown in the "Understanding how to create secrets" section.

**Additional resources**

- For more information on using secrets in pods, see [Understanding how to create secrets](#).

### 2.7.2.3. Creating a service account token secret

As an administrator, you can create a service account token secret, which allows you to distribute a service account token to applications that must authenticate to the API.

**NOTE**

It is recommended to obtain bound service account tokens using the TokenRequest API instead of using service account token secrets. The tokens obtained from the TokenRequest API are more secure than the tokens stored in secrets, because they have a bounded lifetime and are not readable by other API clients.

You should create a service account token secret only if you cannot use the TokenRequest API and if the security exposure of a non-expiring token in a readable API object is acceptable to you.

See the Additional references section that follows for information on creating bound service account tokens.
Procedure

1. Create a Secret object in a YAML file on a control plane node:

**Example secret object:**

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-sa-sample
  annotations:
    kubernetes.io/service-account.name: "sa-name" 1
  type: kubernetes.io/service-account-token 2
```

1. Specifies an existing service account name. If you are creating both the ServiceAccount and the Secret objects, create the ServiceAccount object first.

2. Specifies a service account token secret.

2. Use the following command to create the Secret object:

```
$ oc create -f <filename>.yaml
```

3. To use the secret in a pod:

   a. Update the pod’s service account to reference the secret, as shown in the "Understanding how to create secrets" section.

   b. Create the pod, which consumes the secret as an environment variable or as a file (using a secret volume), as shown in the "Understanding how to create secrets" section.

Additional resources

- For more information on using secrets in pods, see Understanding how to create secrets .
- For information on requesting bound service account tokens, see Using bound service account tokens
- For information on creating service accounts, see Understanding and creating service accounts .

**2.7.2.4. Creating a basic authentication secret**

As an administrator, you can create a basic authentication secret, which allows you to store the credentials needed for basic authentication. When using this secret type, the data parameter of the Secret object must contain the following keys encoded in the base64 format:

- **username**: the user name for authentication
- **password**: the password or token for authentication

**NOTE**

You can use the stringData parameter to use clear text content.
Procedure

1. Create a **Secret** object in a YAML file on a control plane node:

**Example secret object**

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-basic-auth
  type: kubernetes.io/basic-auth

data:
  username: admin
  password: t0p-Secret
```

1. Specifies a basic authentication secret.
2. Specifies the basic authentication values to use.

2. Use the following command to create the **Secret** object:

```bash
$ oc create -f <filename>.yaml
```

3. To use the secret in a pod:
   a. Update the pod’s service account to reference the secret, as shown in the “Understanding how to create secrets” section.
   b. Create the pod, which consumes the secret as an environment variable or as a file (using a **secret** volume), as shown in the “Understanding how to create secrets” section.

**Additional resources**

- For more information on using secrets in pods, see [Understanding how to create secrets](#).

### 2.7.2.5. Creating an SSH authentication secret

As an administrator, you can create an SSH authentication secret, which allows you to store data used for SSH authentication. When using this secret type, the **data** parameter of the **Secret** object must contain the SSH credential to use.

**Procedure**

1. Create a **Secret** object in a YAML file on a control plane node:

**Example secret object:**

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-ssh-auth
  type: kubernetes.io/ssh-auth
```

1.
CHAPTER 2. WORKING WITH PODS

data:
ssh-privatekey: | 2
MIIEpQIBAAKCAQEAulqb/Y ...
1

Specifies an SSH authentication secret.

2

Specifies the SSH key/value pair as the SSH credentials to use.

2. Use the following command to create the Secret object:
$ oc create -f <filename>.yaml
3. To use the secret in a pod:
a. Update the pod’s service account to reference the secret, as shown in the "Understanding
how to create secrets" section.
b. Create the pod, which consumes the secret as an environment variable or as a file (using a
secret volume), as shown in the "Understanding how to create secrets" section.
Additional resources
Understanding how to create secrets .

2.7.2.6. Creating a Docker configuration secret
As an administrator, you can create a Docker configuration secret, which allows you to store the
credentials for accessing a container image registry.
kubernetes.io/dockercfg. Use this secret type to store your local Docker configuration file. The
data parameter of the secret object must contain the contents of a .dockercfg file encoded in
the base64 format.
kubernetes.io/dockerconfigjson. Use this secret type to store your local Docker configuration
JSON file. The data parameter of the secret object must contain the contents of a
.docker/config.json file encoded in the base64 format.
Procedure
1. Create a Secret object in a YAML file on a control plane node.

Example Docker configuration secret object
apiVersion: v1
kind: Secret
metadata:
name: secret-docker-cfg
namespace: my-project
type: kubernetes.io/dockerconfig 1
data:
.dockerconfig:bm5ubm5ubm5ubm5ubm5ubm5ubm5ubmdnZ2dnZ2dnZ2dnZ2dnZ2dnZ2cgYXV
0aCBrZXlzCg== 2

89


1. Specifies that the secret is using a Docker configuration file.
2. The output of a base64-encoded Docker configuration file

**Example Docker configuration JSON secret object**

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-docker-json
  namespace: my-project
type: kubernetes.io/dockerconfig

data:
  .dockerconfigjson: bm5ubm5ubm5ubm5ubm5ubm5ubm5ubm5ubm5ubm5ubm5ubm6dnZ2dnZ2dnZ2dnZ2dnZ2dnZ2dnZ2dnZ2cg
YXV0aCBrZXlzCg==
```

1. Specifies that the secret is using a Docker configuration JSON file.
2. The output of a base64-encoded Docker configuration JSON file

2. Use the following command to create the **Secret** object

   ```bash
   $ oc create -f <filename>.yaml
   ```

3. To use the secret in a pod:
   
   a. Update the pod's service account to reference the secret, as shown in the "Understanding how to create secrets" section.

   b. Create the pod, which consumes the secret as an environment variable or as a file (using a **secret** volume), as shown in the "Understanding how to create secrets" section.

**Additional resources**

- For more information on using secrets in pods, see [Understanding how to create secrets](#).

### 2.7.3. Understanding how to update secrets

When you modify the value of a secret, the value (used by an already running pod) will not dynamically change. To change a secret, you must delete the original pod and create a new pod (perhaps with an identical PodSpec).

Updating a secret follows the same workflow as deploying a new Container image. You can use the `kubectl rolling-update` command.

The **resourceVersion** value in a secret is not specified when it is referenced. Therefore, if a secret is updated at the same time as pods are starting, the version of the secret that is used for the pod is not defined.
NOTE

Currently, it is not possible to check the resource version of a secret object that was used when a pod was created. It is planned that pods will report this information, so that a controller could restart ones using an old `resourceVersion`. In the interim, do not update the data of existing secrets, but create new ones with distinct names.

2.7.4. Creating and using secrets

As an administrator, you can create a service account token secret. This allows you to distribute a service account token to applications that must authenticate to the API.

Procedure

1. Create a service account in your namespace by running the following command:

   $ oc create sa <service_account_name> -n <your_namespace>

2. Save the following YAML example to a file named `service-account-token-secret.yaml`. The example includes a Secret object configuration that you can use to generate a service account token:

   ```yaml
   apiVersion: v1
   kind: Secret
   metadata:
     name: <secret_name>  
     annotations:
       kubernetes.io/service-account.name: "sa-name"
   type: kubernetes.io/service-account-token
   ```

   Replace `<secret_name>` with the name of your service token secret.

   Specifies an existing service account name. If you are creating both the ServiceAccount and the Secret objects, create the ServiceAccount object first.

   Specifies a service account token secret type.

3. Generate the service account token by applying the file:

   $ oc apply -f service-account-token-secret.yaml

4. Get the service account token from the secret by running the following command:

   $ oc get secret <sa_token_secret> -o jsonpath='{.data.token}' | base64 --decode

   Example output

   ```
   ayJhbGciOiJSUzI1NiIsIlI6InN0YW5jZSIsImV4cCI6MTc5ODk2MjczNiwiaXNzIjoiQcJ9
   ```
Replace `<sa_token_secret>` with the name of your service token secret.

5. Use your service account token to authenticate with the API of your cluster:

```bash
$ curl -X GET <openshift_cluster_api> --header "Authorization: Bearer <token>"
```

Replace `<token>` with the service account token that is output in the preceding command.

### 2.7.5. About using signed certificates with secrets

To secure communication to your service, you can configure OpenShift Container Platform to generate a signed serving certificate/key pair that you can add into a secret in a project.

A **service serving certificate secret** is intended to support complex middleware applications that need out-of-the-box certificates. It has the same settings as the server certificates generated by the administrator tooling for nodes and masters.

#### Service Pod spec configured for a service serving certificates secret.

```yaml
apiVersion: v1
class: Service
metadata:
  name: registry
  annotations:
    service.beta.openshift.io/serving-cert-secret-name: registry-cert
# ...
```

Specify the name for the certificate

Other pods can trust cluster-created certificates (which are only signed for internal DNS names), by using the CA bundle in the `/var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt` file that is automatically mounted in their pod.

The signature algorithm for this feature is **x509.SHA256WithRSA**. To manually rotate, delete the generated secret. A new certificate is created.

#### 2.7.5.1. Generating signed certificates for use with secrets

To use a signed serving certificate/key pair with a pod, create or edit the service to add the `service.beta.openshift.io/serving-cert-secret-name` annotation, then add the secret to the pod.
Procedure

To create a service serving certificate secret:

1. Edit the **Pod** spec for your service.

2. Add the `service.beta.openshift.io/serving-cert-secret-name` annotation with the name you want to use for your secret.

```yaml
kind: Service
apiVersion: v1
metadata:
  name: my-service
  annotations:
    service.beta.openshift.io/serving-cert-secret-name: my-cert
spec:
  selector:
    app: MyApp
  ports:
    - protocol: TCP
      port: 80
      targetPort: 9376
```

The certificate and key are in PEM format, stored in `tls.crt` and `tls.key` respectively.

3. Create the service:

```
$ oc create -f <file-name>.yaml
```

4. View the secret to make sure it was created:

   a. View a list of all secrets:

```
$ oc get secrets
```

   b. View details on your secret:

```
$ oc describe secret my-cert
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>DATA</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>my-cert</td>
<td>kubernetes.io/tls</td>
<td>2</td>
<td>9m</td>
</tr>
</tbody>
</table>

```
Name:       my-cert
Namespace:  openshift-console
Labels:     <none>
            service.beta.openshift.io/originating-service-name: my-service
            service.beta.openshift.io/originating-service-uid: 640f0ec3-afc2-4380-bf31-a8c784846a11
            service.beta.openshift.io/expiry: 2023-03-08T23:22:40Z
```
5. Edit your Pod spec with that secret.

apiVersion: v1
category: Pod
metadata:
  name: my-service-pod
spec:
  containers:
  - name: mypod
    image: redis
    volumes:
      - name: foo
        mountPath: "/etc/foo"
    volumeMounts:
      - name: foo
  secret:
    secretName: my-cert
    items:
      - key: username
        path: my-group/my-username
        mode: 511

When it is available, your pod will run. The certificate will be good for the internal service DNS name, `<service.name>.<service.namespace>.svc`.

The certificate/key pair is automatically replaced when it gets close to expiration. View the expiration date in the `service.beta.openshift.io/expiry` annotation on the secret, which is in RFC3339 format.

**NOTE**

In most cases, the service DNS name `<service.name>.<service.namespace>.svc` is not externally routable. The primary use of `<service.name>.<service.namespace>.svc` is for intracluster or intraservice communication, and with re-encrypt routes.

### 2.7.6. Troubleshooting secrets

If a service certificate generation fails with (service’s `service.beta.openshift.io/serving-cert-generation-error` annotation contains):

```
secret/ssl-key references serviceUID 62ad25ca-d703-11e6-9d6f-0e9c0057b608, which does not
match 77b6dd80-d716-11e6-9d6f-0e9c0057b60
```

The service that generated the certificate no longer exists, or has a different `serviceUID`. You must force certificates regeneration by removing the old secret, and clearing the following annotations on the service `service.beta.openshift.io/serving-cert-generation-error, service.beta.openshift.io/serving-...`
cert-generation-error-num:

1. Delete the secret:

   $ oc delete secret <secret_name>

2. Clear the annotations:

   $ oc annotate service <service_name> service.beta.openshift.io/serving-cert-generation-error-

   $ oc annotate service <service_name> service.beta.openshift.io/serving-cert-generation-error-num-

   **NOTE**
   
The command removing annotation has a - after the annotation name to be removed.

### 2.8. CREATING AND USING CONFIG MAPS

The following sections define config maps and how to create and use them.

#### 2.8.1. Understanding config maps

Many applications require configuration using some combination of configuration files, command line arguments, and environment variables. In OpenShift Container Platform, these configuration artifacts are decoupled from image content to keep containerized applications portable.

The **ConfigMap** object provides mechanisms to inject containers with configuration data while keeping containers agnostic of OpenShift Container Platform. A config map can be used to store fine-grained information like individual properties or coarse-grained information like entire configuration files or JSON blobs.

The **ConfigMap** API object holds key-value pairs of configuration data that can be consumed in pods or used to store configuration data for system components such as controllers. For example:

**ConfigMap Object Definition**

```yaml
kind: ConfigMap
apiVersion: v1
metadata:
  creationTimestamp: 2016-02-18T19:14:38Z
  name: example-config
  namespace: default
data: 1
  example.property.1: hello
  example.property.2: world
  example.property.file: |
    property.1=value-1
    property.2=value-2
    property.3=value-3
binaryData:
  bar: L3Jvb3QvMTAw
```
Contains the configuration data.

Points to a file that contains non-UTF8 data, for example, a binary Java keystore file. Enter the file data in Base 64.

NOTE
You can use the `binaryData` field when you create a config map from a binary file, such as an image.

Configuration data can be consumed in pods in a variety of ways. A config map can be used to:

- Populate environment variable values in containers
- Set command-line arguments in a container
- Populate configuration files in a volume

Users and system components can store configuration data in a config map.

A config map is similar to a secret, but designed to more conveniently support working with strings that do not contain sensitive information.

**Config map restrictions**

A config map must be created before its contents can be consumed in pods.

Controllers can be written to tolerate missing configuration data. Consult individual components configured by using config maps on a case-by-case basis.

**ConfigMap objects reside in a project.**

They can only be referenced by pods in the same project.

The Kubelet only supports the use of a config map for pods it gets from the API server.

This includes any pods created by using the CLI, or indirectly from a replication controller. It does not include pods created by using the OpenShift Container Platform node’s `--manifest-url` flag, its `--config` flag, or its REST API because these are not common ways to create pods.

### 2.8.2. Creating a config map in the OpenShift Container Platform web console

You can create a config map in the OpenShift Container Platform web console.

**Procedure**

- To create a config map as a cluster administrator:
  1. In the Administrator perspective, select **Workloads → Config Maps**.
  2. At the top right side of the page, select **Create Config Map**.
  3. Enter the contents of your config map.
  4. Select **Create**.
To create a config map as a developer:

1. In the Developer perspective, select **Config Maps**.
2. At the top right side of the page, select **Create Config Map**.
3. Enter the contents of your config map.
4. Select **Create**.

### 2.8.3. Creating a config map by using the CLI

You can use the following command to create a config map from directories, specific files, or literal values.

**Procedure**

- Create a config map:

  ```
  $ oc create configmap <configmap_name> [options]
  ```

#### 2.8.3.1. Creating a config map from a directory

You can create a config map from a directory. This method allows you to use multiple files within a directory to create a config map.

**Procedure**

The following example procedure outlines how to create a config map from a directory.

1. Start with a directory with some files that already contain the data with which you want to populate a config map:

  ```
  $ ls example-files
  ```

**Example output**

```
example-files

<table>
<thead>
<tr>
<th>game.properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>ui.properties</td>
</tr>
</tbody>
</table>
```

```
$ cat example-files/game.properties
```

**Example output**

```java
enemies=aliens
lives=3
enemies.cheat=true
enemies.cheat.level=noGoodRotten
secret.code.passphrase=UUDDLRLRBABAS
secret.code.allowed=true
secret.code.lives=30
```

```
$ cat example-files/ui.properties
```

**Example output**

```java
```

```
Example output

color.good=purple
color.bad=yellow
allow.textmode=true
how.nice.to.look=fairlyNice

2. Create a config map holding the content of each file in this directory by entering the following command:

    $ oc create configmap game-config \
        --from-file=example-files/

When the `--from-file` option points to a directory, each file directly in that directory is used to populate a key in the config map, where the name of the key is the file name, and the value of the key is the content of the file.

For example, the previous command creates the following config map:

    $ oc describe configmaps game-config

Example output

Name:           game-config
Namespace:      default
Labels:         <none>
Annotations:    <none>

Data

game.properties:        158 bytes
ui.properties:          83 bytes

You can see that the two keys in the map are created from the file names in the directory specified in the command. Because the content of those keys might be large, the output of `oc describe` only shows the names of the keys and their sizes.

3. Enter the `oc get` command for the object with the `-o` option to see the values of the keys:

    $ oc get configmaps game-config -o yaml

Example output

    apiVersion: v1
data:
    game.properties: |
        enemies=aliens
        lives=3
        enemies.cheat=true
        enemies.cheat.level=noGoodRotten
        secret.code.passphrase=UUDDLRLRBABAS
        secret.code.allowed=true
        secret.code.lives=30
2.8.3.2. Creating a config map from a file

You can create a config map from a file.

**Procedure**

The following example procedure outlines how to create a config map from a file.

```
NOTE

If you create a config map from a file, you can include files containing non-UTF8 data that are placed in this field without corrupting the non-UTF8 data. OpenShift Container Platform detects binary files and transparently encodes the file as MIME. On the server, the MIME payload is decoded and stored without corrupting the data.

You can pass the `--from-file` option multiple times to the CLI. The following example yields equivalent results to the creating from directories example.

1. Create a config map by specifying a specific file:

   ```bash
   $ oc create configmap game-config-2 \
   --from-file=example-files/game.properties \
   --from-file=example-files/ui.properties
   ```

2. Verify the results:

   ```bash
   $ oc get configmaps game-config-2 -o yaml
   ```

**Example output**

```yaml
apiVersion: v1
data:
game.properties: |
enemies=aliens
lives=3
enemies.cheat=true
enemies.cheat.level=noGoodRotten
secret.code.passphrase=UDDLRLRABAS
secret.code.allowed=true
secret.code.lives=30
```
You can specify the key to set in a config map for content imported from a file. This can be set by passing a `key=value` expression to the `--from-file` option. For example:

1. Create a config map by specifying a key-value pair:

   ```bash
   $ oc create configmap game-config-3 \
   --from-file=game-special-key=example-files/game.properties
   ```

2. Verify the results:

   ```bash
   $ oc get configmaps game-config-3 -o yaml
   ```

   **Example output**

   ```yaml
   apiVersion: v1
data:
  game-special-key: |
    enemies=aliens
    lives=3
    enemies.cheat=true
    enemies.cheat.level=noGoodRotten
    secret.code.passphrase=UUDDLRLRBABAS
    secret.code.allowed=true
    secret.code.lives=30
kind: ConfigMap
metadata:
  creationTimestamp: 2016-02-18T18:54:22Z
  name: game-config-3
  namespace: default
  resourceVersion: "530"
  selflink: /api/v1/namespaces/default/configmaps/game-config-3
  uid: 05f8da22-d671-11e5-8cd0-68f728dbf1985
   ```

   This is the key that you set in the preceding step.

### 2.8.3.3. Creating a config map from literal values

You can supply literal values for a config map.
Procedure

The `--from-literal` option takes a `key=value` syntax that allows literal values to be supplied directly on the command line.

1. Create a config map by specifying a literal value:

   ```
   $ oc create configmap special-config \
     --from-literal=special.how=very \
     --from-literal=special.type=charm
   ```

2. Verify the results:

   ```
   $ oc get configmaps special-config -o yaml
   ```

Example output

```
apiVersion: v1
data:
special.how: very
special.type: charm
kind: ConfigMap
metadata:
  creationTimestamp: 2016-02-18T19:14:38Z
  name: special-config
  namespace: default
  resourceVersion: "651"
selflink: /api/v1/namespaces/default/configmaps/special-config
uid: dadce046-d673-11e5-8cd0-68f728db1985
```

2.8.4. Use cases: Consuming config maps in pods

The following sections describe some uses cases when consuming `ConfigMap` objects in pods.

2.8.4.1. Populating environment variables in containers by using config maps

Config maps can be used to populate individual environment variables in containers or to populate environment variables in containers from all keys that form valid environment variable names.

As an example, consider the following config map:

**ConfigMap with two environment variables**

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: special-config
  namespace: default
data:
  special.how: very
  special.type: charm
```

1. Name of the config map.
The project in which the config map resides. Config maps can only be referenced by pods in the same project.

Environment variables to inject.

**ConfigMap with one environment variable**

```yaml
apiVersion: v1
class: ConfigMap
metadata:
  name: env-config
  namespace: default
data:
  log_level: INFO
 1 Name of the config map.
 2 Environment variable to inject.
```

**Procedure**

- You can consume the keys of this ConfigMap in a pod using `configMapKeyRef` sections.

**Sample Pod specification configured to inject specific environment variables**

```yaml
apiVersion: v1
class: Pod
metadata:
  name: dapi-test-pod
spec:
  containers:
    - name: test-container
      image: gcr.io/google_containers/busybox
      command: ["/bin/sh", "-c", "env"]
      env:
        1 Name of the config map.
        2 Environment variable to inject.
        - name: SPECIAL_LEVEL_KEY
          valueFrom:
            configMapKeyRef:
              name: special-config
              key: special.how
        - name: SPECIAL_TYPE_KEY
          valueFrom:
            configMapKeyRef:
              name: special-config
              key: special.type
              optional: true
      envFrom:
        8 - configMapRef:
            name: env-config
      restartPolicy: Never
```
1. Stanza to pull the specified environment variables from a **ConfigMap**.

2. Name of a pod environment variable that you are injecting a key’s value into.

3. Name of the **ConfigMap** to pull specific environment variables from.

4. Environment variable to pull from the **ConfigMap**.

5. Makes the environment variable optional. As optional, the pod will be started even if the specified **ConfigMap** and keys do not exist.

6. Stanza to pull all environment variables from a **ConfigMap**.

7. Name of the **ConfigMap** to pull all environment variables from.

When this pod is run, the pod logs will include the following output:

```
SPECIAL_LEVEL_KEY=very
log_level=INFO
```

**NOTE**

**SPECIAL_TYPE_KEY=charm** is not listed in the example output because **optional: true** is set.

### 2.8.4.2. Setting command-line arguments for container commands with config maps

A config map can also be used to set the value of the commands or arguments in a container. This is accomplished by using the Kubernetes substitution syntax **$(VAR_NAME)**. Consider the following config map:

```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: special-config
namespace: default
data:
  special.how: very
  special.type: charm
```

**Procedure**

- To inject values into a command in a container, you must consume the keys you want to use as environment variables, as in the consuming ConfigMaps in environment variables use case. Then you can refer to them in a container’s command using the **$(VAR_NAME)** syntax.

**Sample Pod specification configured to inject specific environment variables**

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: dapi-test-pod
spec:
```
Inject the values into a command in a container using the keys you want to use as environment variables.

When this pod is run, the output from the echo command run in the test-container container is as follows:

dpapi-test-pod

very charm

2.8.4.3. Injecting content into a volume by using config maps

You can inject content into a volume by using config maps.

Example ConfigMap custom resource (CR)

```yaml
apiVersion: v1
type: ConfigMap
metadata:
  name: special-config
  namespace: default
data:
  special.how: very
  special.type: charm
```

Procedure

You have a couple different options for injecting content into a volume by using config maps.

- The most basic way to inject content into a volume by using a config map is to populate the volume with files where the key is the file name and the content of the file is the value of the key:

```yaml
apiVersion: v1
type: Pod
metadata:
  name: dapi-test-pod
spec:
```
containers:
- name: test-container
  image: gcr.io/google_containers/busybox
  command: ["/bin/sh", "cat", "/etc/config/special.how"]
volumeMounts:
- name: config-volume
  mountPath: /etc/config
volumes:
- name: config-volume
  configMap:
    name: special-config
restartPolicy: Never

File containing key.

When this pod is run, the output of the cat command will be:

very

- You can also control the paths within the volume where config map keys are projected:

apiVersion: v1
kind: Pod
metadata:
  name: dapi-test-pod
spec:
  containers:
    - name: test-container
      image: gcr.io/google_containers/busybox
      command: ["/bin/sh", "cat", "/etc/config/path/to/special-key"]
      volumeMounts:
        - name: config-volume
          mountPath: /etc/config
      volumes:
        - name: config-volume
          configMap:
            name: special-config
          items:
            - key: special.how
              path: path/to/special-key
          restartPolicy: Never

Path to config map key.

When this pod is run, the output of the cat command will be:

very

2.9. USING DEVICE PLUG-INS TO ACCESS EXTERNAL RESOURCES WITH PODS
Device plug-ins allow you to use a particular device type (GPU, InfiniBand, or other similar computing resources that require vendor-specific initialization and setup) in your OpenShift Container Platform pod without needing to write custom code.

2.9.1. Understanding device plug-ins

The device plug-in provides a consistent and portable solution to consume hardware devices across clusters. The device plug-in provides support for these devices through an extension mechanism, which makes these devices available to Containers, provides health checks of these devices, and securely shares them.

**IMPORTANT**

OpenShift Container Platform supports the device plug-in API, but the device plug-in Containers are supported by individual vendors.

A device plug-in is a gRPC service running on the nodes (external to the kubelet) that is responsible for managing specific hardware resources. Any device plug-in must support following remote procedure calls (RPCs):

```plaintext
service DevicePlugin {
  // GetDevicePluginOptions returns options to be communicated with Device
  // Manager
  rpc GetDevicePluginOptions(Empty) returns (DevicePluginOptions) {}

  // ListAndWatch returns a stream of List of Devices
  // Whenever a Device state change or a Device disappears, ListAndWatch
  // returns the new list
  rpc ListAndWatch(Empty) returns (stream ListAndWatchResponse) {}

  // Allocate is called during container creation so that the Device
  // Plug-in can run device specific operations and instruct Kubelet
  // of the steps to make the Device available in the container
  rpc Allocate(AllocateRequest) returns (AllocateResponse) {}

  // PreStartcontainer is called, if indicated by Device Plug-in during
  // registration phase, before each container start. Device plug-in
  // can run device specific operations such as resetting the device
  // before making devices available to the container
  rpc PreStartcontainer(PreStartcontainerRequest) returns (PreStartcontainerResponse) {}
}
```

**Example device plug-ins**

- Nvidia GPU device plug-in for COS-based operating system
- Nvidia official GPU device plug-in
- Solarflare device plug-in
- KubeVirt device plug-ins: vfio and kvm
- Kubernetes device plug-in for IBM Crypto Express (CEX) cards
NOTE

For easy device plug-in reference implementation, there is a stub device plug-in in the Device Manager code:
```
vendor/k8s.io/kubernetes/pkg/kubelet/cm/deviceplugin/device_plugin_stub.go.
```

2.9.1.1. Methods for deploying a device plug-in

- Daemon sets are the recommended approach for device plug-in deployments.
- Upon start, the device plug-in will try to create a UNIX domain socket at `/var/lib/kubelet/device-plugin/` on the node to serve RPCs from Device Manager.
- Since device plug-ins must manage hardware resources, access to the host file system, as well as socket creation, they must be run in a privileged security context.
- More specific details regarding deployment steps can be found with each device plug-in implementation.

2.9.2. Understanding the Device Manager

Device Manager provides a mechanism for advertising specialized node hardware resources with the help of plug-ins known as device plug-ins.

You can advertise specialized hardware without requiring any upstream code changes.

IMPORTANT

OpenShift Container Platform supports the device plug-in API, but the device plug-in Containers are supported by individual vendors.

Device Manager advertises devices as **Extended Resources**. User pods can consume devices, advertised by Device Manager, using the same **Limit/Request** mechanism, which is used for requesting any other **Extended Resource**.

Upon start, the device plug-in registers itself with Device Manager invoking **Register** on the `/var/lib/kubelet/device-plugins/kubelet.sock` and starts a gRPC service at `/var/lib/kubelet/device-plugins/<plugin>.sock` for serving Device Manager requests.

Device Manager, while processing a new registration request, invokes **ListAndWatch** remote procedure call (RPC) at the device plug-in service. In response, Device Manager gets a list of **Device** objects from the plug-in over a gRPC stream. Device Manager will keep watching on the stream for new updates from the plug-in. On the plug-in side, the plug-in will also keep the stream open and whenever there is a change in the state of any of the devices, a new device list is sent to the Device Manager over the same streaming connection.

While handling a new pod admission request, Kubelet passes requested **Extended Resources** to the Device Manager for device allocation. Device Manager checks in its database to verify if a corresponding plug-in exists or not. If the plug-in exists and there are free allocatable devices as well as per local cache, **Allocate** RPC is invoked at that particular device plug-in.

Additionally, device plug-ins can also perform several other device-specific operations, such as driver installation, device initialization, and device resets. These functionalities vary from implementation to implementation.
2.9.3. Enabling Device Manager

Enable Device Manager to implement a device plug-in to advertise specialized hardware without any upstream code changes.

Device Manager provides a mechanism for advertising specialized node hardware resources with the help of plug-ins known as device plug-ins.

1. Obtain the label associated with the static `MachineConfigPool` CRD for the type of node you want to configure. Perform one of the following steps:

   a. View the machine config:

   ```shell
   # oc describe machineconfig <name>
   
   For example:
   
   # oc describe machineconfig 00-worker
   
   Example output
   
   Name: 00-worker
   Namespace:
   Labels: machineconfiguration.openshift.io/role=worker
   
   1 Label required for the Device Manager.
   
   Procedure
   
   1. Create a custom resource (CR) for your configuration change.

   Sample configuration for a Device Manager CR

   ```yaml
   apiVersion: machineconfiguration.openshift.io/v1
   kind: KubeletConfig
   metadata:
     name: devicemgr
   spec:
     machineConfigPoolSelector:
       matchLabels:
         machineconfiguration.openshift.io: devicemgr
     kubeletConfig:
       feature-gates:
         - DevicePlugins=true
   
   1 Assign a name to CR.
   
   2 Enter the label from the Machine Config Pool.
   
   3 Set `DevicePlugins` to 'true'.

   2. Create the Device Manager:
3. Ensure that Device Manager was actually enabled by confirming that `/var/lib/kubelet/device-plugins/kubelet.sock` is created on the node. This is the UNIX domain socket on which the Device Manager gRPC server listens for new plug-in registrations. This sock file is created when the Kubelet is started only if Device Manager is enabled.

### 2.10. INCLUDING POD PRIORITY IN POD SCHEDULING DECISIONS

You can enable pod priority and preemption in your cluster. Pod priority indicates the importance of a pod relative to other pods and queues the pods based on that priority. Pod preemption allows the cluster to evict, or preempt, lower-priority pods so that higher-priority pods can be scheduled if there is no available space on a suitable node pod priority also affects the scheduling order of pods and out-of-resource eviction ordering on the node.

To use priority and preemption, you create priority classes that define the relative weight of your pods. Then, reference a priority class in the pod specification to apply that weight for scheduling.

#### 2.10.1. Understanding pod priority

When you use the Pod Priority and Preemption feature, the scheduler orders pending pods by their priority, and a pending pod is placed ahead of other pending pods with lower priority in the scheduling queue. As a result, the higher priority pod might be scheduled sooner than pods with lower priority if its scheduling requirements are met. If a pod cannot be scheduled, scheduler continues to schedule other lower priority pods.

#### 2.10.1.1. Pod priority classes

You can assign pods a priority class, which is a non-namespaced object that defines a mapping from a name to the integer value of the priority. The higher the value, the higher the priority.

A priority class object can take any 32-bit integer value smaller than or equal to 1000000000 (one billion). Reserve numbers larger than or equal to one billion for critical pods that must not be preempted or evicted. By default, OpenShift Container Platform has two reserved priority classes for critical system pods to have guaranteed scheduling.

```
$ oc create -f devicemgr.yaml
kubeletconfig.machineconfiguration.openshift.io/devicemgr created
```

```
$ oc get priorityclasses

<table>
<thead>
<tr>
<th>NAME</th>
<th>VALUE</th>
<th>GLOBAL-DEFAULT</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>system-node-critical</td>
<td>2000001000</td>
<td>false</td>
<td>72m</td>
</tr>
<tr>
<td>system-cluster-critical</td>
<td>2000000000</td>
<td>false</td>
<td>72m</td>
</tr>
<tr>
<td>openshift-user-critical</td>
<td>1000000000</td>
<td>false</td>
<td>3d13h</td>
</tr>
<tr>
<td>cluster-logging</td>
<td>10000000</td>
<td>false</td>
<td>29s</td>
</tr>
</tbody>
</table>
```

- **system-node-critical** - This priority class has a value of 2000001000 and is used for all pods that should never be evicted from a node. Examples of pods that have this priority class are `sdn-ovs`, `sdn`, and so forth. A number of critical components include the `system-node-critical`
priority class by default, for example:

- master-api
- master-controller
- master-etcd
- sdn
- sdn-ovs
- sync

- **system-cluster-critical** - This priority class has a value of 2000000000 (two billion) and is used with pods that are important for the cluster. Pods with this priority class can be evicted from a node in certain circumstances. For example, pods configured with the **system-node-critical** priority class can take priority. However, this priority class does ensure guaranteed scheduling. Examples of pods that can have this priority class are fluentd, add-on components like descheduler, and so forth. A number of critical components include the **system-cluster-critical** priority class by default, for example:

  - fluentd
  - metrics-server
  - descheduler

- **openshift-user-critical** - You can use the *priorityClassName* field with important pods that cannot bind their resource consumption and do not have predictable resource consumption behavior. Prometheus pods under the **openshift-monitoring** and **openshift-user-workload-monitoring** namespaces use the **openshift-user-critical priorityClassName**. Monitoring workloads use **system-critical** as their first **priorityClass**, but this causes problems when monitoring uses excessive memory and the nodes cannot evict them. As a result, monitoring drops priority to give the scheduler flexibility, moving heavy workloads around to keep critical nodes operating.

- **cluster-logging** - This priority is used by Fluentd to make sure Fluentd pods are scheduled to nodes over other apps.

### 2.10.1.2. Pod priority names

After you have one or more priority classes, you can create pods that specify a priority class name in a *Pod* spec. The priority admission controller uses the priority class name field to populate the integer value of the priority. If the named priority class is not found, the pod is rejected.

### 2.10.2. Understanding pod preemption

When a developer creates a pod, the pod goes into a queue. If the developer configured the pod for pod priority or preemption, the scheduler picks a pod from the queue and tries to schedule the pod on a node. If the scheduler cannot find space on an appropriate node that satisfies all the specified requirements of the pod, preemption logic is triggered for the pending pod.

When the scheduler preempts one or more pods on a node, the *nominatedNodeName* field of higher-priority *Pod* spec is set to the name of the node, along with the *nodename* field. The scheduler uses the *nominatedNodeName* field to keep track of the resources reserved for pods and also provides information to the user about preemptions in the clusters.
After the scheduler preempts a lower-priority pod, the scheduler honors the graceful termination period of the pod. If another node becomes available while the scheduler is waiting for the lower-priority pod to terminate, the scheduler can schedule the higher-priority pod on that node. As a result, the nominatedNodeName field and nodeName field of the Pod spec might be different.

Also, if the scheduler preempts pods on a node and is waiting for termination, and a pod with a higher-priority pod than the pending pod needs to be scheduled, the scheduler can schedule the higher-priority pod instead. In such a case, the scheduler clears the nominatedNodeName of the pending pod, making the pod eligible for another node.

Preemption does not necessarily remove all lower-priority pods from a node. The scheduler can schedule a pending pod by removing a portion of the lower-priority pods.

The scheduler considers a node for pod preemption only if the pending pod can be scheduled on the node.

2.10.2.1. Non-preempting priority classes (Technology Preview)

Pods with the preemption policy set to Never are placed in the scheduling queue ahead of lower-priority pods, but they cannot preempt other pods. A non-preempting pod waiting to be scheduled stays in the scheduling queue until sufficient resources are free and it can be scheduled. Non-preempting pods, like other pods, are subject to scheduler back-off. This means that if the scheduler tries unsuccessfully to schedule these pods, they are retried with lower frequency, allowing other pods with lower priority to be scheduled before them.

Non-preempting pods can still be preempted by other, high-priority pods.

2.10.2.2. Pod preemption and other scheduler settings

If you enable pod priority and preemption, consider your other scheduler settings:

Pod priority and pod disruption budget

A pod disruption budget specifies the minimum number or percentage of replicas that must be up at a time. If you specify pod disruption budgets, OpenShift Container Platform respects them when preempting pods at a best effort level. The scheduler attempts to preempt pods without violating the pod disruption budget. If no such pods are found, lower-priority pods might be preempted despite their pod disruption budget requirements.

Pod priority and pod affinity

Pod affinity requires a new pod to be scheduled on the same node as other pods with the same label.

If a pending pod has inter-pod affinity with one or more of the lower-priority pods on a node, the scheduler cannot preempt the lower-priority pods without violating the affinity requirements. In this case, the scheduler looks for another node to schedule the pending pod. However, there is no guarantee that the scheduler can find an appropriate node and pending pod might not be scheduled.

To prevent this situation, carefully configure pod affinity with equal-priority pods.

2.10.2.3. Graceful termination of preempted pods

When preempting a pod, the scheduler waits for the pod graceful termination period to expire, allowing the pod to finish working and exit. If the pod does not exit after the period, the scheduler kills the pod. This graceful termination period creates a time gap between the point that the scheduler preempts the pod and the time when the pending pod can be scheduled on the node.

To minimize this gap, configure a small graceful termination period for lower-priority pods.
2.10.3. Configuring priority and preemption

You apply pod priority and preemption by creating a priority class object and associating pods to the priority using the `priorityClassName` in your Pod specs.

Sample priority class object

```
apiVersion: scheduling.k8s.io/v1
kind: PriorityClass
metadata:
  name: high-priority
value: 1000000
preemptionPolicy: PreemptLowerPriority
globalDefault: false
description: "This priority class should be used for XYZ service pods only."
```

1. The name of the priority class object.
2. The priority value of the object.
3. Optional field that indicates whether this priority class is preempting or non-preempting. The preemption policy defaults to `PreemptLowerPriority`, which allows pods of that priority class to preempt lower-priority pods. If the preemption policy is set to `Never`, pods in that priority class are non-preempting.
4. Optional field that indicates whether this priority class should be used for pods without a priority class name specified. This field is `false` by default. Only one priority class with `globalDefault` set to `true` can exist in the cluster. If there is no priority class with `globalDefault: true`, the priority of pods with no priority class name is zero. Adding a priority class with `globalDefault: true` affects only pods created after the priority class is added and does not change the priorities of existing pods.
5. Optional arbitrary text string that describes which pods developers should use with this priority class.

Procedure

To configure your cluster to use priority and preemption:

1. Create one or more priority classes:
   a. Specify a name and value for the priority.
   b. Optionally specify the `globalDefault` field in the priority class and a description.

2. Create a Pod spec or edit existing pods to include the name of a priority class, similar to the following:

   Sample Pod spec with priority class name

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
labels:
  env: test
```
Specify the priority class to use with this pod.

3. Create the pod:

$ oc create -f <file-name>.yaml

You can add the priority name directly to the pod configuration or to a pod template.

### 2.11. PLACING PODS ON SPECIFIC NODES USING NODE SELECTORS

A node selector specifies a map of key-value pairs. The rules are defined using custom labels on nodes and selectors specified in pods.

For the pod to be eligible to run on a node, the pod must have the indicated key-value pairs as the label on the node.

If you are using node affinity and node selectors in the same pod configuration, see the important considerations below.

#### 2.11.1. Using node selectors to control pod placement

You can use node selectors on pods and labels on nodes to control where the pod is scheduled. With node selectors, OpenShift Container Platform schedules the pods on nodes that contain matching labels.

You add labels to a node, a machine set, or a machine config. Adding the label to the machine set ensures that if the node or machine goes down, new nodes have the label. Labels added to a node or machine config do not persist if the node or machine goes down.

To add node selectors to an existing pod, add a node selector to the controlling object for that pod, such as a ReplicaSet object, DaemonSet object, StatefulSet object, Deployment object, or DeploymentConfig object. Any existing pods under that controlling object are recreated on a node with a matching label. If you are creating a new pod, you can add the node selector directly to the Pod spec.

**NOTE**

You cannot add a node selector directly to an existing scheduled pod.

**Prerequisites**

To add a node selector to existing pods, determine the controlling object for that pod. For example, the router-default-66d5cf9464-m2g75 pod is controlled by the router-default-66d5cf9464 replica set:

$ oc describe pod router-default-66d5cf9464-7pwkc

Name: router-default-66d5cf9464-7pwkc
Namespace: openshift-ingress

Controlled By: ReplicaSet/router-default-66d5cf9464

The web console lists the controlling object under ownerReferences in the pod YAML:

```yaml
ownerReferences:
- apiVersion: apps/v1
  kind: ReplicaSet
  name: router-default-66d5cf9464
  uid: d81dd094-da26-11e9-a48a-128e7edf0312
  controller: true
  blockOwnerDeletion: true
```

Procedure

1. Add labels to a node by using a machine set or editing the node directly:
   - Use a **MachineSet** object to add labels to nodes managed by the machine set when a node is created:
     a. Run the following command to add labels to a **MachineSet** object:

```
$ oc patch MachineSet <name> --type='json' -p='[
  {
    "op": "add",
    "path": "/spec/template/spec/metadata/labels",
    "value": {
      "<key>": "<value>",
      "$key": "$value"
    }
  }]
' -n openshift-machine-api
```
   
   For example:

```
$ oc patch MachineSet abc612-msrtw-worker-us-east-1c --type='json' -p='[
  {
    "op": "add",
    "path": "/spec/template/spec/metadata/labels",
    "value": {
      "type": "user-node",
      "region": "east"
    }
  }]
' -n openshift-machine-api
```

**TIP**

You can alternatively apply the following YAML to add labels to a machine set:

```yaml
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  name: <machineset>
namespace: openshift-machine-api
spec:
  template:
    spec:
      metadata:
        labels:
          region: "east"
          type: "user-node"
```
b. Verify that the labels are added to the **MachineSet** object by using the **oc edit** command:
   For example:

   ```
   $ oc edit MachineSet abc612-msrtw-worker-us-east-1c -n openshift-machine-api
   ```

**Example MachineSet object**

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
....
spec:
  ....
template:
    metadata:
      ....
spec:
    metadata:
      labels:
        region: east
        type: user-node
    ....
```

- Add labels directly to a node:
  a. Edit the **Node** object for the node:
     ```
     $ oc label nodes <name> <key>=<value>
     ```

     For example, to label a node:
     ```
     $ oc label nodes ip-10-0-142-25.ec2.internal type=user-node region=east
     ```

**TIP**

You can alternatively apply the following YAML to add labels to a node:

```
kind: Node
apiVersion: v1
metadata:
  name: <node_name>
lables:
  type: "user-node"
  region: "east"
```

b. Verify that the labels are added to the node:

   ```
   $ oc get nodes -l type=user-node,region=east
   ```

**Example output**
2. Add the matching node selector to a pod:

- To add a node selector to existing and future pods, add a node selector to the controlling object for the pods:

  **Example ReplicaSet object with labels**

  ```yaml
  kind: ReplicaSet
  ...
  spec:
  ...
  template:
    metadata:
      creationTimestamp: null
    labels:
      ingresscontroller.operator.openshift.io/deployment-ingresscontroller: default
      pod-template-hash: 66d5cf9464
    spec:
      nodeSelector:
        kubernetes.io/os: linux
        node-role.kubernetes.io/worker: "
    type: user-node
  ```

  Add the node selector.

- To add a node selector to a specific, new pod, add the selector to the **Pod** object directly:

  **Example Pod object with a node selector**

  ```yaml
  apiVersion: v1
  kind: Pod
  ...
  spec:
    nodeSelector:
      region: east
      type: user-node
  ```

  **NOTE**

  You cannot add a node selector directly to an existing scheduled pod.
CHAPTER 3. CONTROLLING POD PLACEMENT ONTO NODES (SCHEDULING)

3.1. CONTROLLING POD PLACEMENT USING THE SCHEDULER

Pod scheduling is an internal process that determines placement of new pods onto nodes within the cluster.

The scheduler code has a clean separation that watches new pods as they get created and identifies the most suitable node to host them. It then creates bindings (pod to node bindings) for the pods using the master API.

Default pod scheduling

OpenShift Container Platform comes with a default scheduler that serves the needs of most users. The default scheduler uses both inherent and customization tools to determine the best fit for a pod.

Advanced pod scheduling

In situations where you might want more control over where new pods are placed, the OpenShift Container Platform advanced scheduling features allow you to configure a pod so that the pod is required or has a preference to run on a particular node or alongside a specific pod.

You can control pod placement by using the following scheduling features:

- Scheduler profiles
- Pod affinity and anti-affinity rules
- Node affinity
- Node selectors
- Taints and tolerations
- Node overcommitment

3.1.1. About the default scheduler

The default OpenShift Container Platform pod scheduler is responsible for determining the placement of new pods onto nodes within the cluster. It reads data from the pod and finds a node that is a good fit based on configured profiles. It is completely independent and exists as a standalone solution. It does not modify the pod; it creates a binding for the pod that ties the pod to the particular node.

3.1.1.1. Understanding default scheduling

The existing generic scheduler is the default platform-provided scheduler engine that selects a node to host the pod in a three-step operation:

Filters the nodes

The available nodes are filtered based on the constraints or requirements specified. This is done by running each node through the list of filter functions called predicates, or filters.

Prioritizes the filtered list of nodes

This is achieved by passing each node through a series of priority, or scoring, functions that assign it a score between 0 - 10, with 0 indicating a bad fit and 10 indicating a good fit to host the pod. The
scheduler configuration can also take in a simple weight (positive numeric value) for each scoring function. The node score provided by each scoring function is multiplied by the weight (default weight for most scores is 1) and then combined by adding the scores for each node provided by all the scores. This weight attribute can be used by administrators to give higher importance to some scores.

Selects the best fit node

The nodes are sorted based on their scores and the node with the highest score is selected to host the pod. If multiple nodes have the same high score, then one of them is selected at random.

3.1.2. Scheduler use cases

One of the important use cases for scheduling within OpenShift Container Platform is to support flexible affinity and anti-affinity policies.

3.1.2.1. Infrastructure topological levels

Administrators can define multiple topological levels for their infrastructure (nodes) by specifying labels on nodes. For example: region=r1, zone=z1, rack=s1.

These label names have no particular meaning and administrators are free to name their infrastructure levels anything, such as city/building/room. Also, administrators can define any number of levels for their infrastructure topology, with three levels usually being adequate (such as: regions → zones → racks). Administrators can specify affinity and anti-affinity rules at each of these levels in any combination.

3.1.2.2. Affinity

Administrators should be able to configure the scheduler to specify affinity at any topological level, or even at multiple levels. Affinity at a particular level indicates that all pods that belong to the same service are scheduled onto nodes that belong to the same level. This handles any latency requirements of applications by allowing administrators to ensure that peer pods do not end up being too geographically separated. If no node is available within the same affinity group to host the pod, then the pod is not scheduled.

If you need greater control over where the pods are scheduled, see Controlling pod placement on nodes using node affinity rules and Placing pods relative to other pods using affinity and anti-affinity rules.

These advanced scheduling features allow administrators to specify which node a pod can be scheduled on and to force or reject scheduling relative to other pods.

3.1.2.3. Anti-affinity

Administrators should be able to configure the scheduler to specify anti-affinity at any topological level, or even at multiple levels. Anti-affinity (or ‘spread’) at a particular level indicates that all pods that belong to the same service are spread across nodes that belong to that level. This ensures that the application is well spread for high availability purposes. The scheduler tries to balance the service pods across all applicable nodes as evenly as possible.

If you need greater control over where the pods are scheduled, see Controlling pod placement on nodes using node affinity rules and Placing pods relative to other pods using affinity and anti-affinity rules.

These advanced scheduling features allow administrators to specify which node a pod can be scheduled on and to force or reject scheduling relative to other pods.

3.2. SCHEDULING PODS USING A SCHEDULER PROFILE
You can configure OpenShift Container Platform to use a scheduling profile to schedule pods onto nodes within the cluster.

### 3.2.1. About scheduler profiles

You can specify a scheduler profile to control how pods are scheduled onto nodes.

The following scheduler profiles are available:

- **LowNodeUtilization**
  
  This profile attempts to spread pods evenly across nodes to get low resource usage per node. This profile provides the default scheduler behavior.

- **HighNodeUtilization**
  
  This profile attempts to place as many pods as possible on to as few nodes as possible. This minimizes node count and has high resource usage per node.

- **NoScoring**
  
  This is a low-latency profile that strives for the quickest scheduling cycle by disabling all score plugins. This might sacrifice better scheduling decisions for faster ones.

### 3.2.2. Configuring a scheduler profile

You can configure the scheduler to use a scheduler profile.

**Prerequisites**

- Access to the cluster as a user with the `cluster-admin` role.

**Procedure**

1. Edit the `Scheduler` object:

   ```bash
   $ oc edit scheduler cluster
   ```

2. Specify the profile to use in the `spec.profile` field:

   ```yaml
   apiVersion: config.openshift.io/v1
   kind: Scheduler
   metadata:
     ... 
     name: cluster
     resourceVersion: "601"
     selfLink: /apis/config.openshift.io/v1/schedulers/cluster
     uid: b351d6d0-d06f-4a99-a26b-87af62e79f59
   spec:
     mastersSchedulable: false
     profile: HighNodeUtilization
   ```

   - Set to **LowNodeUtilization**, **HighNodeUtilization**, or **NoScoring**.

3. Save the file to apply the changes.
3.3. PLACING PODS RELATIVE TO OTHER PODS USING AFFINITY AND ANTI-AFFINITY RULES

Affinity is a property of pods that controls the nodes on which they prefer to be scheduled. Anti-affinity is a property of pods that prevents a pod from being scheduled on a node.

In OpenShift Container Platform pod affinity and pod anti-affinity allow you to constrain which nodes your pod is eligible to be scheduled on based on the key/value labels on other pods.

### 3.3.1. Understanding pod affinity

*Pod affinity* and *pod anti-affinity* allow you to constrain which nodes your pod is eligible to be scheduled on based on the key/value labels on other pods.

- Pod affinity can tell the scheduler to locate a new pod on the same node as other pods if the label selector on the new pod matches the label on the current pod.
- Pod anti-affinity can prevent the scheduler from locating a new pod on the same node as pods with the same labels if the label selector on the new pod matches the label on the current pod.

For example, using affinity rules, you could spread or pack pods within a service or relative to pods in other services. Anti-affinity rules allow you to prevent pods of a particular service from scheduling on the same nodes as pods of another service that are known to interfere with the performance of the pods of the first service. Or, you could spread the pods of a service across nodes, availability zones, or availability sets to reduce correlated failures.

There are two types of pod affinity rules: *required* and *preferred*.

Required rules must be met before a pod can be scheduled on a node. Preferred rules specify that, if the rule is met, the scheduler tries to enforce the rules, but does not guarantee enforcement.

**NOTE**

Depending on your pod priority and preemption settings, the scheduler might not be able to find an appropriate node for a pod without violating affinity requirements. If so, a pod might not be scheduled.

To prevent this situation, carefully configure pod affinity with equal-priority pods.

You configure pod affinity/anti-affinity through the **Pod** spec files. You can specify a required rule, a preferred rule, or both. If you specify both, the node must first meet the required rule, then attempts to meet the preferred rule.

The following example shows a **Pod** spec configured for pod affinity and anti-affinity.

In this example, the pod affinity rule indicates that the pod can schedule onto a node only if that node has at least one already-running pod with a label that has the key *security* and value *S1*. The pod anti-affinity rule says that the pod prefers to not schedule onto a node if that node is already running a pod with label having key *security* and value *S2*.

**Sample Pod config file with pod affinity**

```yaml
apiVersion: v1
kind: Pod
metadata:
```

OpenShift Container Platform 4.11 Nodes
Stanza to configure pod affinity.

Defines a required rule.

The key and value (label) that must be matched to apply the rule.

The operator represents the relationship between the label on the existing pod and the set of values in the `matchExpression` parameters in the specification for the new pod. Can be `In`, `NotIn`, `Exists`, or `DoesNotExist`.

Sample Pod config file with pod anti-affinity

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: with-pod-antiaffinity
spec:
  affinity:
    podAntiAffinity: 1
      preferredDuringSchedulingIgnoredDuringExecution: 2
        - weight: 100 3
          podAffinityTerm:
            labelSelector:
              matchExpressions:
                - key: security 4
                  operator: In 5
                  values:
                    - S2
topologyKey: kubernetes.io/hostname
containers:
  - name: with-pod-affinity
    image: docker.io/ocpqe/hello-pod
```
Specifies a weight for a preferred rule. The node with the highest weight is preferred.

Description of the pod label that determines when the anti-affinity rule applies. Specify a key and value for the label.

The operator represents the relationship between the label on the existing pod and the set of values in the `matchExpression` parameters in the specification for the new pod. Can be `In`, `NotIn`, `Exists`, or `DoesNotExist`.

**NOTE**

If labels on a node change at runtime such that the affinity rules on a pod are no longer met, the pod continues to run on the node.

### 3.3.2. Configuring a pod affinity rule

The following steps demonstrate a simple two-pod configuration that creates pod with a label and a pod that uses affinity to allow scheduling with that pod.

**Procedure**

1. Create a pod with a specific label in the **Pod** spec:

   ```yaml
   $ cat team4.yaml
   apiVersion: v1
   kind: Pod
   metadata:
     name: security-s1
   labels:
     security: S1
   spec:
     containers:
       - name: security-s1
         image: docker.io/ocpqe/hello-pod
   ``

2. When creating other pods, edit the **Pod** spec as follows:

   a. Use the `podAffinity` stanza to configure the `requiredDuringSchedulingIgnoredDuringExecution` parameter or `preferredDuringSchedulingIgnoredDuringExecution` parameter:

   ```yaml
   podAffinity:
     requiredDuringSchedulingIgnoredDuringExecution:
       - labelSelector:
           matchExpressions:
             - key: security
               operator: In
               values:
                 - S1
           topologyKey: failure-domain.beta.kubernetes.io/zone
   ```

   b. Specify the key and value that must be met. If you want the new pod to be scheduled with the other pod, use the same `key` and `value` parameters as the label on the first pod.

   ```yaml
   podAffinity:
     requiredDuringSchedulingIgnoredDuringExecution:
       - labelSelector:
           matchExpressions:
             - key: security
               operator: In
               values:
                 - S1
           topologyKey: failure-domain.beta.kubernetes.io/zone
   ```
c. Specify an operator. The operator can be In, NotIn, Exists, or DoesNotExist. For example, use the operator In to require the label to be in the node.

d. Specify a topologyKey, which is a prepopulated Kubernetes label that the system uses to denote such a topology domain.

3. Create the pod.

```bash
$ oc create -f <pod-spec>.yaml
```

### 3.3.3. Configuring a pod anti-affinity rule

The following steps demonstrate a simple two-pod configuration that creates pod with a label and a pod that uses an anti-affinity preferred rule to attempt to prevent scheduling with that pod.

**Procedure**

1. Create a pod with a specific label in the Pod spec:

```bash
$ cat team4.yaml
apiVersion: v1
kind: Pod
metadata:
  name: security-s2
labels:
  security: S2
spec:
  containers:
  - name: security-s2
    image: docker.io/ocpqe/hello-pod
    podAntiAffinity:
      preferredDuringSchedulingIgnoredDuringExecution:
      - weight: 100
        podAffinityTerm:
          labelSelector:
            matchExpressions:
            - key: security
              operator: In
              values:
              - S2
          topologyKey: kubernetes.io/hostname
```

2. When creating other pods, edit the Pod spec to set the following parameters:

3. Use the podAntiAffinity stanza to configure the requiredDuringSchedulingIgnoredDuringExecution parameter or preferredDuringSchedulingIgnoredDuringExecution parameter:

   a. Specify a weight for the node, 1-100. The node that with highest weight is preferred.

   b. Specify the key and values that must be met. If you want the new pod to not be scheduled with the other pod, use the same key and value parameters as the label on the first pod.

   ```yaml
   podAntiAffinity:
     preferredDuringSchedulingIgnoredDuringExecution:
     - weight: 100
       podAffinityTerm:
         labelSelector:
           matchExpressions:
           - key: security
             operator: In
             values:
             - S2
         topologyKey: kubernetes.io/hostname
   ```

   c. For a preferred rule, specify a weight, 1-100.
d. Specify an **operator**. The operator can be **In**, **NotIn**, **Exists**, or **DoesNotExist**. For example, use the operator **In** to require the label to be in the node.

4. Specify a **topologyKey**, which is a prepopulated **Kubernetes label** that the system uses to denote such a topology domain.

5. Create the pod.

```bash
$ oc create -f <pod-spec>.yaml
```

### 3.3.4. Sample pod affinity and anti-affinity rules

The following examples demonstrate pod affinity and pod anti-affinity.

#### 3.3.4.1. Pod Affinity

The following example demonstrates pod affinity for pods with matching labels and label selectors.

- The pod **team4** has the label **team:4**.

```yaml
$ cat team4.yaml
apiVersion: v1
kind: Pod
metadata:
  name: team4
labels:
  team: "4"
spec:
  containers:
    - name: ocp
      image: docker.io/ocpqe/hello-pod
```

- The pod **team4a** has the label selector **team:4** under **podAffinity**.

```yaml
$ cat pod-team4a.yaml
apiVersion: v1
kind: Pod
metadata:
  name: team4a
spec:
  affinity:
    podAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchExpressions:
              - key: team
                operator: In
                values:
                  - "4"
          topologyKey: kubernetes.io/hostname
    containers:
      - name: pod-affinity
        image: docker.io/ocpqe/hello-pod
```

OpenShift Container Platform 4.11 Nodes

124
The team4a pod is scheduled on the same node as the team4 pod.

3.3.4.2. Pod Anti-affinity

The following example demonstrates pod anti-affinity for pods with matching labels and label selectors.

- The pod pod-s1 has the label security:s1.

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: pod-s1
labels:
  security: s1
spec:
  containers:
    - name: ocp
      image: docker.io/ocpqe/hello-pod
```

- The pod pod-s2 has the label selector security:s1 under podAntiAffinity.

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: pod-s2
spec:
  affinity:
    podAntiAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchExpressions:
              - key: security
                operator: In
                values:
                - s1
          topologyKey: kubernetes.io/hostname
  containers:
    - name: pod-antiaffinity
      image: docker.io/ocpqe/hello-pod
```

- The pod pod-s2 cannot be scheduled on the same node as pod-s1.

3.3.4.3. Pod Affinity with no Matching Labels

The following example demonstrates pod affinity for pods without matching labels and label selectors.

- The pod pod-s1 has the label security:s1.

```bash
$ cat pod-s1.yaml
apiVersion: v1
kind: Pod
metadata:
  name: pod-s1
```
The pod `pod-s2` has the label selector `security:s2`.

```
labels:
  security: s1
spec:
  containers:
    - name: ocp
      image: docker.io/ocpqe/hello-pod
```

- The pod `pod-s2` is not scheduled unless there is a node with a pod that has the `security:s2` label. If there is no other pod with that label, the new pod remains in a pending state:

Example output

```
NAME      READY     STATUS    RESTARTS   AGE       IP        NODE
pod-s2    0/1       Pending   0          32s       <none>
```

### 3.4. CONTROLLING POD PLACEMENT ON NODES USING NODE AFFINITY RULES

Affinity is a property of pods that controls the nodes on which they prefer to be scheduled.

In OpenShift Container Platform node affinity is a set of rules used by the scheduler to determine where a pod can be placed. The rules are defined using custom labels on the nodes and label selectors specified in pods.

#### 3.4.1. Understanding node affinity

Node affinity allows a pod to specify an affinity towards a group of nodes it can be placed on. The node does not have control over the placement.

For example, you could configure a pod to only run on a node with a specific CPU or in a specific availability zone.
There are two types of node affinity rules: required and preferred.

Required rules must be met before a pod can be scheduled on a node. Preferred rules specify that, if the rule is met, the scheduler tries to enforce the rules, but does not guarantee enforcement.

**NOTE**

If labels on a node change at runtime that results in an node affinity rule on a pod no longer being met, the pod continues to run on the node.

You configure node affinity through the Pod spec file. You can specify a required rule, a preferred rule, or both. If you specify both, the node must first meet the required rule, then attempts to meet the preferred rule.

The following example is a Pod spec with a rule that requires the pod be placed on a node with a label whose key is **e2e-az-NorthSouth** and whose value is either **e2e-az-North** or **e2e-az-South**.

**Example pod configuration file with a node affinity required rule**

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: with-node-affinity
spec:
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
          - matchExpressions:
              - key: e2e-az-NorthSouth
                operator: In
                values:
                  - e2e-az-North
                  - e2e-az-South
          containers:
            - name: with-node-affinity
              image: docker.io/ocpqe/hello-pod
```

1. The stanza to configure node affinity.
2. Defines a required rule.
3. The key/value pair (label) that must be matched to apply the rule.
4. The operator represents the relationship between the label on the node and the set of values in the matchExpression parameters in the Pod spec. This value can be In, NotIn, Exists, or DoesNotExist, Lt, or Gt.
5. 
6. 

The following example is a node specification with a preferred rule that a node with a label whose key is **e2e-az-EastWest** and whose value is either **e2e-az-East** or **e2e-az-West** is preferred for the pod:

**Example pod configuration file with a node affinity preferred rule**

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: with-node-affinity
spec:
  affinity:
    nodeAffinity:
      preferredDuringSchedulingIgnoredDuringExecution:
        - weight: 100
          nodeSelectorTerms:
            - matchExpressions:
                - key: e2e-az-EastWest
                  operator: In
                  values:
                    - e2e-az-East
                    - e2e-az-West
          containers:
            - name: with-node-affinity
              image: docker.io/ocpqe/hello-pod
```
The stanza to configure node affinity.

Defines a preferred rule.

Specifies a weight for a preferred rule. The node with highest weight is preferred.

The key/value pair (label) that must be matched to apply the rule.

The operator represents the relationship between the label on the node and the set of values in the `matchExpressions` parameters in the `Pod` spec. This value can be `In`, `NotIn`, `Exists`, or `DoesNotExist`, `Lt`, or `Gt`.

There is no explicit `node anti-affinity` concept, but using the `NotIn` or `DoesNotExist` operator replicates that behavior.

**NOTE**

If you are using node affinity and node selectors in the same pod configuration, note the following:

- If you configure both `nodeSelector` and `nodeAffinity`, both conditions must be satisfied for the pod to be scheduled onto a candidate node.

- If you specify multiple `nodeSelectorTerms` associated with `nodeAffinity` types, then the pod can be scheduled onto a node if one of the `nodeSelectorTerms` is satisfied.

- If you specify multiple `matchExpressions` associated with `nodeSelectorTerms`, then the pod can be scheduled onto a node only if all `matchExpressions` are satisfied.

### 3.4.2. Configuring a required node affinity rule

Required rules must be met before a pod can be scheduled on a node.
**Procedure**

The following steps demonstrate a simple configuration that creates a node and a pod that the scheduler is required to place on the node.

1. Add a label to a node using the `oc label node` command:

   ```bash
   $ oc label node node1 e2e-az-name=e2e-az1
   ```

   **TIP**

   You can alternatively apply the following YAML to add the label:

   ```yaml
   kind: Node
   apiVersion: v1
   metadata:
     name: <node_name>
   labels:
     e2e-az-name: e2e-az1
   ```

2. In the Pod spec, use the `nodeAffinity` stanza to configure the `requiredDuringSchedulingIgnoredDuringExecution` parameter:

   a. Specify the key and values that must be met. If you want the new pod to be scheduled on the node you edited, use the same `key` and `value` parameters as the label in the node.

   b. Specify an `operator`. The operator can be `In`, `NotIn`, `Exists`, `DoesNotExist`, `Lt`, or `Gt`. For example, use the operator `In` to require the label to be in the node:

   ```yaml
   spec:
     affinity:
       nodeAffinity:
         requiredDuringSchedulingIgnoredDuringExecution:
           nodeSelectorTerms:
             - matchExpressions:
               - key: e2e-az-name
                 operator: In
               values:
                 - e2e-az1
                 - e2e-az2
   ```

3. Create the pod:

   ```bash
   $ oc create -f e2e-az2.yaml
   ```

### 3.4.3. Configuring a preferred node affinity rule

Preferred rules specify that, if the rule is met, the scheduler tries to enforce the rules, but does not guarantee enforcement.

**Procedure**
The following steps demonstrate a simple configuration that creates a node and a pod that the scheduler tries to place on the node.

1. Add a label to a node using the `oc label node` command:

   
   ```
   $ oc label node node1 e2e-az-name=e2e-az3
   ```

2. In the Pod spec, use the `nodeAffinity` stanza to configure the `preferredDuringSchedulingIgnoredDuringExecution` parameter:

   a. Specify a weight for the node, as a number 1-100. The node with highest weight is preferred.

   b. Specify the key and values that must be met. If you want the new pod to be scheduled on the node you edited, use the same key and value parameters as the label in the node:

   ```yaml
   spec:
   affinity:
   nodeAffinity:
   preferredDuringSchedulingIgnoredDuringExecution:
     - weight: 1
       preference:
       matchExpressions:
       - key: e2e-az-name
         operator: In
         values:
         - e2e-az3
   ```

   c. Specify an operator. The operator can be `In`, `NotIn`, `Exists`, `DoesNotExist`, `Lt`, or `Gt`. For example, use the Operator `In` to require the label to be in the node.

3. Create the pod.

   ```
   $ oc create -f e2e-az3.yaml
   ```

3.4.4. Sample node affinity rules

The following examples demonstrate node affinity.

3.4.4.1. Node affinity with matching labels

The following example demonstrates node affinity for a node and pod with matching labels:

- The Node1 node has the label `zone:us`:

  ```
  $ oc label node node1 zone=us
  ```
You can alternatively apply the following YAML to add the label:

```yaml
kind: Node
apiVersion: v1
metadata:
  name: <node_name>
  labels:
    zone: us
```

- The pod-s1 pod has the **zone** and **us** key/value pair under a required node affinity rule:

  ```bash
  $ cat pod-s1.yaml
  ```

**Example output**

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: pod-s1
spec:
  containers:
    - image: "docker.io/ocpqe/hello-pod"
      name: hello-pod
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
          - matchExpressions:
              - key: "zone"
                operator: In
                values:
                - us
```

- The pod-s1 pod can be scheduled on Node1:

  ```bash
  $ oc get pod -o wide
  ```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
<th>IP</th>
<th>NODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>pod-s1</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>4m</td>
<td>IP1</td>
<td>node1</td>
</tr>
</tbody>
</table>

### 3.4.4.2. Node affinity with no matching labels

The following example demonstrates node affinity for a node and pod without matching labels:

- The Node1 node has the label **zone:emea**:

  ```bash
  $ oc label node node1 zone=emea
  ```
TIP

You can alternatively apply the following YAML to add the label:

```yaml
kind: Node
apiVersion: v1
metadata:
  name: <node_name>
labels:
  zone: emea
```

- The pod-s1 pod has the **zone** and **us** key/value pair under a required node affinity rule:

```bash
$ cat pod-s1.yaml
```

**Example output**

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: pod-s1
spec:
  containers:
    - image: "docker.io/ocpqe/hello-pod"
      name: hello-pod
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
          - matchExpressions:
              - key: "zone"
                operator: In
                values:
                  - us
```

- The pod-s1 pod cannot be scheduled on Node1:

```bash
$ oc describe pod pod-s1
```

**Example output**

```bash
...  
Events:
  FirstSeen  LastSeen  Count  From    SubObjectPath  Type               Reason
  ---------  --------  -----  -------  --------------  --------            ------
  1m 33s      8        default-scheduler Warning  FailedScheduling  No nodes are available that match all of the following predicates:: MatchNodeSelector (1).
```

### 3.4.5. Additional resources

- For information about changing node labels, see Understanding how to update labels on nodes.
3.5. PLACING PODS ONTO OVERCOMMITTED NODES

In an **overcommitted** state, the sum of the container compute resource requests and limits exceeds the resources available on the system. Overcommitment might be desirable in development environments where a trade-off of guaranteed performance for capacity is acceptable.

Requests and limits enable administrators to allow and manage the overcommitment of resources on a node. The scheduler uses requests for scheduling your container and providing a minimum service guarantee. Limits constrain the amount of compute resource that may be consumed on your node.

### 3.5.1. Understanding overcommitment

Requests and limits enable administrators to allow and manage the overcommitment of resources on a node. The scheduler uses requests for scheduling your container and providing a minimum service guarantee. Limits constrain the amount of compute resource that may be consumed on your node.

OpenShift Container Platform administrators can control the level of overcommit and manage container density on nodes by configuring masters to override the ratio between request and limit set on developer containers. In conjunction with a per-project **LimitRange** object specifying limits and defaults, this adjusts the container limit and request to achieve the desired level of overcommit.

**NOTE**

That these overrides have no effect if no limits have been set on containers. Create a **LimitRange** object with default limits, per individual project, or in the project template, to ensure that the overrides apply.

After these overrides, the container limits and requests must still be validated by any **LimitRange** object in the project. It is possible, for example, for developers to specify a limit close to the minimum limit, and have the request then be overridden below the minimum limit, causing the pod to be forbidden. This unfortunate user experience should be addressed with future work, but for now, configure this capability and **LimitRange** objects with caution.

### 3.5.2. Understanding nodes overcommitment

In an overcommitted environment, it is important to properly configure your node to provide best system behavior.

When the node starts, it ensures that the kernel tunable flags for memory management are set properly. The kernel should never fail memory allocations unless it runs out of physical memory.

To ensure this behavior, OpenShift Container Platform configures the kernel to always overcommit memory by setting the `vm.overcommit_memory` parameter to 1, overriding the default operating system setting.

OpenShift Container Platform also configures the kernel not to panic when it runs out of memory by setting the `vm.panic_on_oom` parameter to 0. A setting of 0 instructs the kernel to call `oom_killer` in an Out of Memory (OOM) condition, which kills processes based on priority.

You can view the current setting by running the following commands on your nodes:

```
$ sysctl -a | grep commit
```

**Example output**
NOTE

The above flags should already be set on nodes, and no further action is required.

You can also perform the following configurations for each node:

- Disable or enforce CPU limits using CPU CFS quotas
- Reserve resources for system processes
- Reserve memory across quality of service tiers

3.6. CONTROLLING POD PLACEMENT USING NODE TAINTS

Taints and tolerations allow the node to control which pods should (or should not) be scheduled on them.

3.6.1. Understanding taints and tolerations

A taint allows a node to refuse a pod to be scheduled unless that pod has a matching toleration.

You apply taints to a node through the Node specification (NodeSpec) and apply tolerations to a pod through the Pod specification (PodSpec). When you apply a taint a node, the scheduler cannot place a pod on that node unless the pod can tolerate the taint.

Example taint in a node specification

```yaml
spec:
  ....
  template:
  ....
  spec:
    taints:
      - effect: NoExecute
        key: key1
        value: value1
    ....
```

Example toleration in a Pod spec

```yaml
spec:
  ....
  template:
  ....
```
Taints and tolerations consist of a key, value, and effect.

Table 3.1. Taint and toleration components

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>key</strong></td>
<td>The <em>key</em> is any string, up to 253 characters. The key must begin with a letter or number, and may contain letters, numbers, hyphens, dots, and underscores.</td>
</tr>
<tr>
<td><strong>value</strong></td>
<td>The <em>value</em> is any string, up to 63 characters. The value must begin with a letter or number, and may contain letters, numbers, hyphens, dots, and underscores.</td>
</tr>
<tr>
<td><strong>effect</strong></td>
<td>The effect is one of the following:</td>
</tr>
</tbody>
</table>
| **NoSchedule** | - New pods that do not match the taint are not scheduled onto that node.  
- Existing pods on the node remain. |
| **PreferNoSchedule** | - New pods that do not match the taint might be scheduled onto that node, but the scheduler tries not to.  
- Existing pods on the node remain. |
| **NoExecute** | - New pods that do not match the taint cannot be scheduled onto that node.  
- Existing pods on the node that do not have a matching toleration are removed. |
| **operator** | **Equal** | The *key/value/effect* parameters must match. This is the default. |
|           | **Exists** | The *key/effect* parameters must match. You must leave a blank *value* parameter, which matches any. |
1. If you add a `NoSchedule` taint to a control plane node, the node must have the `node-role.kubernetes.io/master=:NoSchedule` taint, which is added by default.

For example:

```yaml
apiVersion: v1
kind: Node
metadata:
  annotations:
    machine.openshift.io/machine: openshift-machine-api/ci-ln-62s7gtb-f76d1-v8jxv-master-0
    machineconfiguration.openshift.io/currentConfig: rendered-master-cdc1ab7da414629332cc4c3926e6e59c
spec:
  taints:
  - effect: NoSchedule
    key: node-role.kubernetes.io/master
```

A toleration matches a taint:

- If the `operator` parameter is set to `Equal`:
  - the `key` parameters are the same;
  - the `value` parameters are the same;
  - the `effect` parameters are the same.

- If the `operator` parameter is set to `Exists`:
  - the `key` parameters are the same;
  - the `effect` parameters are the same.

The following taints are built into OpenShift Container Platform:

- `node.kubernetes.io/not-ready`: The node is not ready. This corresponds to the node condition `Ready=False`.

- `node.kubernetes.io/unreachable`: The node is unreachable from the node controller. This corresponds to the node condition `Ready=Unknown`.

- `node.kubernetes.io/memory-pressure`: The node has memory pressure issues. This corresponds to the node condition `MemoryPressure=True`.

- `node.kubernetes.io/disk-pressure`: The node has disk pressure issues. This corresponds to the node condition `DiskPressure=True`.

- `node.kubernetes.io/network-unavailable`: The node network is unavailable.

- `node.kubernetes.io/unschedulable`: The node is unschedulable.

- `node.cloudprovider.kubernetes.io/uninitialized`: When the node controller is started with an external cloud provider, this taint is set on a node to mark it as unusable. After a controller from the cloud-controller-manager initializes this node, the kubelet removes this taint.
3.6.1.1. Understanding how to use toleration seconds to delay pod evictions

You can specify how long a pod can remain bound to a node before being evicted by specifying the `tolerationSeconds` parameter in the Pod specification or MachineSet object. If a taint with the NoExecute effect is added to a node, a pod that does tolerate the taint, which has the `tolerationSeconds` parameter, the pod is not evicted until that time period expires.

Example output

```yaml
spec:
  template:
    spec:
      tolerations:
      - key: "key1"
        operator: "Equal"
        value: "value1"
        effect: "NoExecute"
        tolerationSeconds: 3600
```

Here, if this pod is running but does not have a matching toleration, the pod stays bound to the node for 3,600 seconds and then be evicted. If the taint is removed before that time, the pod is not evicted.

3.6.1.2. Understanding how to use multiple taints

You can put multiple taints on the same node and multiple tolerations on the same pod. OpenShift Container Platform processes multiple taints and tolerations as follows:

1. Process the taints for which the pod has a matching toleration.

2. The remaining unmatched taints have the indicated effects on the pod:

   a. If there is at least one unmatched taint with effect NoSchedule, OpenShift Container Platform cannot schedule a pod onto that node.

   b. If there is no unmatched taint with effect NoSchedule but there is at least one unmatched taint with effect PreferNoSchedule, OpenShift Container Platform tries to not schedule the pod onto the node.

   c. If there is at least one unmatched taint with effect NoExecute, OpenShift Container Platform evicts the pod from the node if it is already running on the node, or the pod is not scheduled onto the node if it is not yet running on the node.

      - Pods that do not tolerate the taint are evicted immediately.

      - Pods that tolerate the taint without specifying `tolerationSeconds` in their Pod specification remain bound forever.
- Pods that tolerate the taint with a specified `tolerationSeconds` remain bound for the specified amount of time.

For example:

- Add the following taints to the node:
  
  ```
  $ oc adm taint nodes node1 key1=value1:NoSchedule
  $ oc adm taint nodes node1 key1=value1:NoExecute
  $ oc adm taint nodes node1 key2=value2:NoSchedule
  ```

- The pod has the following tolerations:

  ```
  spec:
  ....
  template:
  ....
  spec:
  tolerations:
  - key: "key1"
    operator: "Equal"
    value: "value1"
    effect: "NoSchedule"
  - key: "key1"
    operator: "Equal"
    value: "value1"
    effect: "NoExecute"
  ```

In this case, the pod cannot be scheduled onto the node, because there is no toleration matching the third taint. The pod continues running if it is already running on the node when the taint is added, because the third taint is the only one of the three that is not tolerated by the pod.

### 3.6.1.3. Understanding pod scheduling and node conditions (taint node by condition)

The Taint Nodes By Condition feature, which is enabled by default, automatically taints nodes that report conditions such as memory pressure and disk pressure. If a node reports a condition, a taint is added until the condition clears. The taints have the `NoSchedule` effect, which means no pod can be scheduled on the node unless the pod has a matching toleration.

The scheduler checks for these taints on nodes before scheduling pods. If the taint is present, the pod is scheduled on a different node. Because the scheduler checks for taints and not the actual node conditions, you configure the scheduler to ignore some of these node conditions by adding appropriate pod tolerations.

To ensure backward compatibility, the daemon set controller automatically adds the following tolerations to all daemons:

- `node.kubernetes.io/memory-pressure`
- `node.kubernetes.io/disk-pressure`
- `node.kubernetes.io/unschedulable` (1.10 or later)
• node.kubernetes.io/network-unavailable (host network only)

You can also add arbitrary tolerations to daemon sets.

**NOTE**

The control plane also adds the node.kubernetes.io/memory-pressure toleration on pods that have a QoS class. This is because Kubernetes manages pods in the Guaranteed or Burstable QoS classes. The new BestEffort pods do not get scheduled onto the affected node.

### 3.6.1.4. Understanding evicting pods by condition (taint-based evictions)

The Taint-Based Evictions feature, which is enabled by default, evicts pods from a node that experiences specific conditions, such as not-ready and unreachable. When a node experiences one of these conditions, OpenShift Container Platform automatically adds taints to the node, and starts evicting and rescheduling the pods on different nodes.

Taint Based Evictions have a NoExecute effect, where any pod that does not tolerate the taint is evicted immediately and any pod that does tolerate the taint will never be evicted, unless the pod uses the tolerationSeconds parameter.

The tolerationSeconds parameter allows you to specify how long a pod stays bound to a node that has a node condition. If the condition still exists after the tolerationSeconds period, the taint remains on the node and the pods with a matching toleration are evicted. If the condition clears before the tolerationSeconds period, pods with matching tolerations are not removed.

If you use the tolerationSeconds parameter with no value, pods are never evicted because of the not ready and unreachable node conditions.

**NOTE**

OpenShift Container Platform evicts pods in a rate–limited way to prevent massive pod evictions in scenarios such as the master becoming partitioned from the nodes.

By default, if more than 55% of nodes in a given zone are unhealthy, the node lifecycle controller changes that zone’s state to PartialDisruption and the rate of pod evictions is reduced. For small clusters (by default, 50 nodes or less) in this state, nodes in this zone are not tainted and evictions are stopped.

For more information, see Rate limits on eviction in the Kubernetes documentation.

OpenShift Container Platform automatically adds a toleration for node.kubernetes.io/not-ready and node.kubernetes.io/unreachable with tolerationSeconds=300, unless the Pod configuration specifies either toleration.

```yaml
spec:
  ....
  template:
    ....
    spec:
      tolerations:
        - key: node.kubernetes.io/not-ready
          operator: Exists
          effect: NoExecute
```

---

CHAPTER 3. CONTROLLING POD PLACEMENT ONTO NODES (SCHEDULING)
tolerationSeconds: 300
- key: node.kubernetes.io/unreachable
  operator: Exists
  effect: NoExecute
  tolerationSeconds: 300

These tolerations ensure that the default pod behavior is to remain bound for five minutes after one of these node conditions problems is detected.

You can configure these tolerations as needed. For example, if you have an application with a lot of local state, you might want to keep the pods bound to node for a longer time in the event of network partition, allowing for the partition to recover and avoiding pod eviction.

Pods spawned by a daemon set are created with NoExecute tolerations for the following taints with no tolerationSeconds:

- node.kubernetes.io/unreachable
- node.kubernetes.io/not-ready

As a result, daemon set pods are never evicted because of these node conditions.

3.6.1.5. Tolerating all taints

You can configure a pod to tolerate all taints by adding an operator: "Exists" toleration with no key and value parameters. Pods with this toleration are not removed from a node that has taints.

Pod spec for tolerating all taints

```yaml
spec:
  template:
    spec:
      tolerations:
      - operator: "Exists"
```

3.6.2. Adding taints and tolerations

You add tolerations to pods and taints to nodes to allow the node to control which pods should or should not be scheduled on them. For existing pods and nodes, you should add the toleration to the pod first, then add the taint to the node to avoid pods being removed from the node before you can add the toleration.

Procedure

1. Add a toleration to a pod by editing the Pod spec to include a tolerations stanza:

Sample pod configuration file with an Equal operator

```yaml
spec:
  template:
    spec:
      tolerations:
      - operator: "Equal"
```
The toleration parameters, as described in the **Taint and toleration components** table.

The **tolerationSeconds** parameter specifies how long a pod can remain bound to a node before being evicted.

For example:

**Sample pod configuration file with an Exists operator**

```
spec:
  ....
  template:
  ....
  spec:
    tolerations:
    - key: "key1"
      operator: "Exists"
      effect: "NoExecute"
      tolerationSeconds: 3600
```

1. The **Exists** operator does not take a **value**.

This example places a taint on **node1** that has key **key1**, value **value1**, and taint effect **NoExecute**.

2. Add a taint to a node by using the following command with the parameters described in the **Taint and toleration components** table:

   ```
   $ oc adm taint nodes <node_name> <key>=<value>:<effect>
   ```

   For example:

   ```
   $ oc adm taint nodes node1 key1=value1:NoExecute
   ```

   This command places a taint on **node1** that has key **key1**, value **value1**, and effect **NoExecute**.
NOTE

If you add a **NoSchedule** taint to a control plane node, the node must have the **node-role.kubernetes.io/master=:NoSchedule** taint, which is added by default.

For example:

```yaml
apiVersion: v1
kind: Node
metadata:
  annotations:
    machine.openshift.io/machine: openshift-machine-api/ci-ln-62s7gtb-f76d1-v8jxv-master-0
    machineconfiguration.openshift.io/currentConfig: rendered-master-cdc1ab7da414629332cc4c3926e6e59c

spec:
  taints:
    - effect: NoSchedule
      key: node-role.kubernetes.io/master

... 
```

The tolerations on the pod match the taint on the node. A pod with either toleration can be scheduled onto **node1**.

3.6.2.1. Adding taints and tolerations using a machine set

You can add taints to nodes using a machine set. All nodes associated with the **MachineSet** object are updated with the taint. Tolerations respond to taints added by a machine set in the same manner as taints added directly to the nodes.

Procedure

1. Add a toleration to a pod by editing the **Pod** spec to include a **tolerations** stanza:

```
Sample pod configuration file with Equal operator

spec:
  ....
  template:
    ....
      spec:
        tolerations:
        - key: "key1"  
          value: "value1"
          operator: "Equal"
          effect: "NoExecute"
          tolerationSeconds: 3600
```

1. The toleration parameters, as described in the **Taint and toleration components** table.

2. The **tolerationSeconds** parameter specifies how long a pod is bound to a node before being evicted.
For example:

**Sample pod configuration file with Exists operator**

```yaml
spec:
  tolerations:
  - key: "key1"
    operator: "Exists"
    effect: "NoExecute"
    tolerationSeconds: 3600
```

2. Add the taint to the **MachineSet** object:
   a. Edit the **MachineSet** YAML for the nodes you want to taint or you can create a new **MachineSet** object:

   ```bash
   $ oc edit machineset <machineset>
   ```

   b. Add the taint to the **spec.template.spec** section:

   **Example taint in a machine set specification**

   ```yaml
   spec:
   ....
   template:
   ....
   spec:
   spec:
   taints:
   - effect: NoExecute
     key: key1
     value: value1
   ....
   ```

   This example places a taint that has the key **key1**, value **value1**, and taint effect **NoExecute** on the nodes.

c. Scale down the machine set to 0:

   ```bash
   $ oc scale --replicas=0 machineset <machineset> -n openshift-machine-api
   ```

   **TIP**

   You can alternatively apply the following YAML to scale the machine set:

   ```yaml
   apiVersion: machine.openshift.io/v1beta1
   kind: MachineSet
   metadata:
     name: <machineset>
     namespace: openshift-machine-api
   spec:
     replicas: 0
   ```

   Wait for the machines to be removed.
3.6.2.2. Binding a user to a node using taints and tolerations

If you want to dedicate a set of nodes for exclusive use by a particular set of users, add a toleration to their pods. Then, add a corresponding taint to those nodes. The pods with the tolerations are allowed to use the tainted nodes or any other nodes in the cluster.

If you want ensure the pods are scheduled to only those tainted nodes, also add a label to the same set of nodes and add a node affinity to the pods so that the pods can only be scheduled onto nodes with that label.

Procedure

To configure a node so that users can use only that node:

1. Add a corresponding taint to those nodes:
   
   For example:

   ```bash
   $ oc adm taint nodes node1 dedicated=groupName:NoSchedule
   ```

   **TIP**

   You can alternatively apply the following YAML to add the taint:

   ```yaml
   kind: Node
   apiVersion: v1
   metadata:
     name: <node_name>
     labels:
     ...  
     spec:
     taints:
        - key: dedicated
          value: groupName
          effect: NoSchedule
   ```

2. Add a toleration to the pods by writing a custom admission controller.

3.6.2.3. Creating a project with a node selector and toleration

You can create a project that uses a node selector and toleration, which are set as annotations, to control the placement of pods onto specific nodes. Any subsequent resources created in the project are then scheduled on nodes that have a taint matching the toleration.
Prerequisites

- A label for node selection has been added to one or more nodes by using a machine set or editing the node directly.
- A taint has been added to one or more nodes by using a machine set or editing the node directly.

Procedure

1. Create a **Project** resource definition, specifying a node selector and toleration in the `metadata.annotations` section:

   **Example project.yaml file**

   ```yaml
   kind: Project
   apiVersion: project.openshift.io/v1
   metadata:
     name: <project_name>  # 1
     annotations:
       openshift.io/node-selector: '<label>'  # 2
       scheduler.alpha.kubernetes.io/defaultTolerations: >-
         - operator: "Exists", effect: "NoSchedule", key: "<key_name>"  # 3
   
   
   # 1 The project name.
   # 2 The default node selector label.
   # 3 The toleration parameters, as described in the Taint and toleration components table. This example uses the **NoSchedule** effect, which allows existing pods on the node to remain, and the **Exists** operator, which does not take a value.

2. Use the **oc apply** command to create the project:

   ```bash
   $ oc apply -f project.yaml
   
   Any subsequent resources created in the `<project_name>` namespace should now be scheduled on the specified nodes.

Additional resources

- Adding taints and tolerations manually to nodes or with machine sets
- Creating project-wide node selectors
- Pod placement of Operator workloads

3.6.2.4. Controlling nodes with special hardware using taints and tolerations

In a cluster where a small subset of nodes have specialized hardware, you can use taints and tolerations to keep pods that do not need the specialized hardware off of those nodes, leaving the nodes for pods that do need the specialized hardware. You can also require pods that need specialized hardware to use
specific nodes.

You can achieve this by adding a toleration to pods that need the special hardware and tainting the nodes that have the specialized hardware.

**Procedure**

To ensure nodes with specialized hardware are reserved for specific pods:

1. Add a toleration to pods that need the special hardware.
   
   For example:
   ```yaml
   spec:
   tolerations:
   - key: "disktype"
     value: "ssd"
     operator: "Equal"
     effect: "NoSchedule"
   toleranceSeconds: 3600
   ```

2. Taint the nodes that have the specialized hardware using one of the following commands:

   $ oc adm taint nodes <node-name> disktype=ssd:NoSchedule

   Or:

   $ oc adm taint nodes <node-name> disktype=ssd:PreferNoSchedule

   **TIP**

   You can alternatively apply the following YAML to add the taint:
   ```yaml
   kind: Node
   apiVersion: v1
   metadata:
     name: <node_name>
     labels:
     ...
   spec:
   taints:
   - key: disktype
     value: ssd
     effect: PreferNoSchedule
   ```

3.6.3. Removing taints and tolerations

You can remove taints from nodes and tolerations from pods as needed. You should add the toleration to the pod first, then add the taint to the node to avoid pods being removed from the node before you can add the toleration.

**Procedure**

To remove taints and tolerations:
1. To remove a taint from a node:

```
$ oc adm taint nodes <node-name> <key>-
```

For example:

```
$ oc adm taint nodes ip-10-0-132-248.ec2.internal key1-
```

Example output

```
node/ip-10-0-132-248.ec2.internal untainted
```

2. To remove a toleration from a pod, edit the **Pod** spec to remove the toleration:

```
spec:
  tolerations:
  - key: "key2"
    operator: "Exists"
    effect: "NoExecute"
    tolerationSeconds: 3600
```

### 3.7. PLACING PODS ON SPECIFIC NODES USING NODE SELECTORS

A **node selector** specifies a map of key/value pairs that are defined using custom labels on nodes and selectors specified in pods.

For the pod to be eligible to run on a node, the pod must have the same key/value node selector as the label on the node.

#### 3.7.1. About node selectors

You can use node selectors on pods and labels on nodes to control where the pod is scheduled. With node selectors, OpenShift Container Platform schedules the pods on nodes that contain matching labels.

You can use a node selector to place specific pods on specific nodes, cluster-wide node selectors to place new pods on specific nodes anywhere in the cluster, and project node selectors to place new pods in a project on specific nodes.

For example, as a cluster administrator, you can create an infrastructure where application developers can deploy pods only onto the nodes closest to their geographical location by including a node selector in every pod they create. In this example, the cluster consists of five data centers spread across two regions. In the U.S., label the nodes as **us-east**, **us-central**, or **us-west**. In the Asia-Pacific region (APAC), label the nodes as **apac-east** or **apac-west**. The developers can add a node selector to the pods they create to ensure the pods get scheduled on those nodes.

A pod is not scheduled if the **Pod** object contains a node selector, but no node has a matching label.
IMPORTANT

If you are using node selectors and node affinity in the same pod configuration, the following rules control pod placement onto nodes:

- If you configure both `nodeSelector` and `nodeAffinity`, both conditions must be satisfied for the pod to be scheduled onto a candidate node.

- If you specify multiple `nodeSelectorTerms` associated with `nodeAffinity` types, then the pod can be scheduled onto a node if one of the `nodeSelectorTerms` is satisfied.

- If you specify multiple `matchExpressions` associated with `nodeSelectorTerms`, then the pod can be scheduled onto a node only if all `matchExpressions` are satisfied.

Node selectors on specific pods and nodes

You can control which node a specific pod is scheduled on by using node selectors and labels. To use node selectors and labels, first label the node to avoid pods being descheduled, then add the node selector to the pod.

NOTE

You cannot add a node selector directly to an existing scheduled pod. You must label the object that controls the pod, such as deployment config.

For example, the following Node object has the `region: east` label:

**Sample Node object with a label**

```
kind: Node
apiVersion: v1
metadata:
  name: ip-10-0-131-14.ec2.internal
  selfLink: /api/v1/nodes/ip-10-0-131-14.ec2.internal
  uid: 7bc2580a-8b8e-11e9-8e01-021ab4174c74
  resourceVersion: '478704'
  creationTimestamp: '2019-06-10T14:46:08Z'
labels:
  kubernetes.io/os: linux
  failure-domain.beta.kubernetes.io/zone: us-east-1
  node.openshift.io/os_version: '4.5'
  node-role.kubernetes.io/worker: "
  failure-domain.beta.kubernetes.io/region: us-east-1
  node.openshift.io/os_id: rhcos
  beta.kubernetes.io/instance-type: m4.large
  kubernetes.io/hostname: ip-10-0-131-14
  beta.kubernetes.io/arch: amd64
  region: east

1 Label to match the pod node selector.
```

A pod has the `type: user-node,region: east` node selector:
Sample Pod object with node selectors

```yaml
apiVersion: v1
class: Pod
....

spec:
  nodeSelector:
    region: east
    type: user-node
```

Node selectors to match the node label.

When you create the pod using the example pod spec, it can be scheduled on the example node.

Default cluster-wide node selectors

With default cluster-wide node selectors, when you create a pod in that cluster, OpenShift Container Platform adds the default node selectors to the pod and schedules the pod on nodes with matching labels.

For example, the following `Scheduler` object has the default cluster-wide `region=east` and `type=user-node` node selectors:

**Example Scheduler Operator Custom Resource**

```yaml
apiVersion: config.openshift.io/v1
class: Scheduler
metadata:
  name: cluster
...

spec:
  defaultNodeSelector:
    type: user-node
    region: east
...
```

A node in that cluster has the `type=user-node,region=east` labels:

**Example Node object**

```yaml
apiVersion: v1
class: Node
metadata:
  name: ci-ln-qg1il3k-f76d1-hlmhl-worker-b-df2s4
...
  labels:
    region: east
    type: user-node
...
```

**Example Pod object with a node selector**

```yaml
apiVersion: v1
```
When you create the pod using the example pod spec in the example cluster, the pod is created with the cluster-wide node selector and is scheduled on the labeled node:

Example pod list with the pod on the labeled node

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
<th>IP</th>
<th>NODE</th>
<th>NOMINATED NODE</th>
<th>READINESS GATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>pod-s1</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>20s</td>
<td>10.131.2.6</td>
<td>ci-ln-qg1il3k-f76d1-hlmhl-worker-b-df2s4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;none&gt;</td>
<td></td>
<td>&lt;none&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE

If the project where you create the pod has a project node selector, that selector takes preference over a cluster-wide node selector. Your pod is not created or scheduled if the pod does not have the project node selector.

Project node selectors

With project node selectors, when you create a pod in this project, OpenShift Container Platform adds the node selectors to the pod and schedules the pods on a node with matching labels. If there is a cluster-wide default node selector, a project node selector takes preference.

For example, the following project has the `region=east` node selector:

Example Namespace object

```yaml
apiVersion: v1
kind: Namespace
metadata:
  name: east-region
annotations:
  openshift.io/node-selector: "region=east"
```

The following node has the `type=user-node,region=east` labels:

Example Node object

```yaml
apiVersion: v1
kind: Node
metadata:
  name: ci-ln-qg1il3k-f76d1-hlmhl-worker-b-df2s4
labels:
```

kind: Pod

```yaml
... spec:
  nodeSelector:
    region: east
...```
When you create the pod using the example pod spec in this example project, the pod is created with the project node selectors and is scheduled on the labeled node:

Example Pod object

```
apiVersion: v1
kind: Pod
metadata:
  namespace: east-region
...
spec:
  nodeSelector:
    region: east
    type: user-node
...
```

Example pod list with the pod on the labeled node

```
NAME     READY   STATUS    RESTARTS   AGE   IP           NODE
pod-s1   1/1     Running   0          20s   10.131.2.6   ci-ln-qg1il3k-f76d1-hlmhl-worker-b-df2s4
<none>           <none>
```

A pod in the project is not created or scheduled if the pod contains different node selectors. For example, if you deploy the following pod into the example project, it is not be created:

Example Pod object with an invalid node selector

```
apiVersion: v1
kind: Pod
...
spec:
  nodeSelector:
    region: west
...
```

### 3.7.2. Using node selectors to control pod placement

You can use node selectors on pods and labels on nodes to control where the pod is scheduled. With node selectors, OpenShift Container Platform schedules the pods on nodes that contain matching labels.

You add labels to a node, a machine set, or a machine config. Adding the label to the machine set ensures that if the node or machine goes down, new nodes have the label. Labels added to a node or machine config do not persist if the node or machine goes down.

To add node selectors to an existing pod, add a node selector to the controlling object for that pod, such
as a **ReplicaSet** object, **DaemonSet** object, **StatefulSet** object, **Deployment** object, or **DeploymentConfig** object. Any existing pods under that controlling object are recreated on a node with a matching label. If you are creating a new pod, you can add the node selector directly to the **Pod** spec.

**NOTE**

You cannot add a node selector directly to an existing scheduled pod.

**Prerequisites**

To add a node selector to existing pods, determine the controlling object for that pod. For example, the `router-default-66d5cf9464-m2g75` pod is controlled by the `router-default-66d5cf9464` replica set:

```
$ oc describe pod router-default-66d5cf9464-7pwkc
Name:               router-default-66d5cf9464-7pwkc
Namespace:          openshift-ingress
....
Controlled By:      ReplicaSet/router-default-66d5cf9464
```

The web console lists the controlling object under **ownerReferences** in the pod YAML:

```
ownerReferences:
  - apiVersion: apps/v1
    kind: ReplicaSet
    name: router-default-66d5cf9464
    uid: d81dd094-da26-11e9-a48a-128e7edf0312
    controller: true
    blockOwnerDeletion: true
```

**Procedure**

1. Add labels to a node by using a machine set or editing the node directly:
   
   a. Add labels to a **MachineSet** object to add labels to nodes managed by the machine set when a node is created:

      ```
      $ oc patch MachineSet <name> --type='json' -
p="["op":"add","path":"/spec/template/spec/metadata/labels","value":{"<key>":"<value>"}}"
      -n openshift-machine-api
      
      For example:
      
      $ oc patch MachineSet abc612-msrtw-worker-us-east-1c --type='json' -
p="["op":"add","path":"/spec/template/spec/metadata/labels","value":{"type":"user-node","region":"east"}}"
      -n openshift-machine-api
      ```
**TIP**

You can alternatively apply the following YAML to add labels to a machine set:

```yaml
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  name: <machineset>
  namespace: openshift-machine-api
spec:
template:
  spec:
    metadata:
      labels:
        region: "east"
        type: "user-node"
```

b. Verify that the labels are added to the `MachineSet` object by using the `oc edit` command:
For example:

```
$ oc edit MachineSet abc612-msrtw-worker-us-east-1c -n openshift-machine-api
```

**Example MachineSet object**

```yaml
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet

....

spec:
  ... 
  template: 
    metadata:
    .... 
  spec: 
    metadata: 
      labels: 
        region: east 
        type: user-node 
      .... 
```

- Add labels directly to a node:

a. Edit the `Node` object for the node:

```
$ oc label nodes <name> <key>=<value>
```

For example, to label a node:

```
$ oc label nodes ip-10-0-142-25.ec2.internal type=user-node region=east
```
**TIP**

You can alternatively apply the following YAML to add labels to a node:

```yaml
kind: Node
apiVersion: v1
metadata:
  name: <node_name>
labels:
  type: "user-node"
  region: "east"
```

b. Verify that the labels are added to the node:

```
$ oc get nodes -l type=user-node,region=east
```

**Example output**

```
NAME                          STATUS   ROLES    AGE   VERSION
ip-10-0-142-25.ec2.internal   Ready    worker   17m   v1.24.0
```

2. Add the matching node selector to a pod:

- To add a node selector to existing and future pods, add a node selector to the controlling object for the pods:

  **Example ReplicaSet object with labels**

  ```yaml
  kind: ReplicaSet
  ....
  spec:
  ....
  template:
  metadata:
    creationTimestamp: null
  labels:
    ingresscontroller.operator.openshift.io/deployment-ingresscontroller: default
    pod-template-hash: 66d5cf9464
  spec:
    nodeSelector:
      kubernetes.io/os: linux
      node-role.kubernetes.io/worker: "
    type: user-node
  ```

  Add the node selector.

- To add a node selector to a specific, new pod, add the selector to the Pod object directly:

  **Example Pod object with a node selector**
NOTE

You cannot add a node selector directly to an existing scheduled pod.

3.7.3. Creating default cluster-wide node selectors

You can use default cluster-wide node selectors on pods together with labels on nodes to constrain all pods created in a cluster to specific nodes.

With cluster-wide node selectors, when you create a pod in that cluster, OpenShift Container Platform adds the default node selectors to the pod and schedules the pod on nodes with matching labels.

You configure cluster-wide node selectors by editing the Scheduler Operator custom resource (CR). You add labels to a node, a machine set, or a machine config. Adding the label to the machine set ensures that if the node or machine goes down, new nodes have the label. Labels added to a node or machine config do not persist if the node or machine goes down.

NOTE

You can add additional key/value pairs to a pod. But you cannot add a different value for a default key.

Procedure

To add a default cluster-wide node selector:

1. Edit the Scheduler Operator CR to add the default cluster-wide node selectors:

   $ oc edit scheduler cluster

Example Scheduler Operator CR with a node selector

   apiVersion: config.openshift.io/v1
   kind: Scheduler
   metadata:
     name: cluster
   ...
   spec:
     defaultNodeSelector: type=user-node,region=east
     mastersSchedulable: false

1. Add a node selector with the appropriate <key>:<value> pairs.
After making this change, wait for the pods in the openshift-kube-apiserver project to redeploy. This can take several minutes. The default cluster-wide node selector does not take effect until the pods redeploy.

2. Add labels to a node by using a machine set or editing the node directly:
   - Use a machine set to add labels to nodes managed by the machine set when a node is created:
     a. Run the following command to add labels to a MachineSet object:

     ```bash
     $ oc patch MachineSet <name> --type=json -p=
     ["op":"add","path":/spec/template/spec/metadata/labels","value":
     
     1 Add a <key>/value> pair for each label.

     For example:

     ```bash
     $ oc patch MachineSet ci-ln-l8nny52-f76d1-hl7m7-worker-c --type=json -p=
     ["op":"add","path":/spec/template/spec/metadata/labels","value":

     TIP

     You can alternatively apply the following YAML to add labels to a machine set:

     ```yaml
     apiVersion: machine.openshift.io/v1beta1
     kind: MachineSet
     metadata:
      name: <machineset>
      namespace: openshift-machine-api
     spec:
      template:
        spec:
         metadata:
          labels:
           region: "east"
           type: "user-node"

     b. Verify that the labels are added to the MachineSet object by using the oc edit command:
        For example:

        ```bash
        $ oc edit MachineSet abc612-msrtw-worker-us-east-1c -n openshift-machine-api

     Example MachineSet object

     ```yaml
     apiVersion: machine.openshift.io/v1beta1
     kind: MachineSet
     ... spec:
c. Redeploy the nodes associated with that machine set by scaling down to 0 and scaling up the nodes:
For example:

```
$ oc scale --replicas=0 MachineSet ci-ln-l8nry52-f76d1-hl7m7-worker-c -n openshift-machine-api
```

```
$ oc scale --replicas=1 MachineSet ci-ln-l8nry52-f76d1-hl7m7-worker-c -n openshift-machine-api
```

d. Verify that the labels are added to the MachineSet object by using the oc edit command:
For example:

```
$ oc edit MachineSet ci-ln-l8nry52-f76d1-hl7m7-worker-c -n openshift-machine-api
```

e. Redeploy the nodes associated with that machine set by scaling down to 0 and scaling up the nodes:
For example:

```
$ oc scale --replicas=0 MachineSet ci-ln-l8nry52-f76d1-hl7m7-worker-c -n openshift-machine-api
```

```
$ oc scale --replicas=1 MachineSet ci-ln-l8nry52-f76d1-hl7m7-worker-c -n openshift-machine-api
```

f. When the nodes are ready and available, verify that the label is added to the nodes by using the oc get command:

```
$ oc get nodes -l <key>=<value>
```
For example:

```
$ oc get nodes -l type=user-node
```

**Example output**

```
NAME                                       STATUS   ROLES    AGE   VERSION
ci-ln-l8nry52-f76d1-hl7m7-worker-c-vmqzp   Ready    worker   61s   v1.24.0
```
Add labels directly to a node:

a. Edit the **Node** object for the node:

```sh
$ oc label nodes <name> <key>=<value>
```

For example, to label a node:

```sh
$ oc label nodes ci-ln-l8nr52-f76d1-hl7m7-worker-b-tgq49 type=user-node region=east
```

**TIP**

You can alternatively apply the following YAML to add labels to a node:

```yaml
kind: Node
apiVersion: v1
metadata:
  name: <node_name>
labels:
  type: "user-node"
  region: "east"
```

b. Verify that the labels are added to the node using the **oc get** command:

```sh
$ oc get nodes -l <key>=<value>,<key>=<value>
```

For example:

```sh
$ oc get nodes -l type=user-node,region=east
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>ROLES</th>
<th>AGE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci-ln-l8nr52-f76d1-hl7m7-worker-b-tgq49</td>
<td>Ready</td>
<td>worker</td>
<td>17m</td>
<td>v1.24.0</td>
</tr>
</tbody>
</table>

### 3.7.4. Creating project-wide node selectors

You can use node selectors in a project together with labels on nodes to constrain all pods created in that project to the labeled nodes.

When you create a pod in this project, OpenShift Container Platform adds the node selectors to the pods in the project and schedules the pods on a node with matching labels in the project. If there is a cluster-wide default node selector, a project node selector takes preference.

You add node selectors to a project by editing the **Namespace** object to add the *openshift.io/node-selector* parameter. You add labels to a node, a machine set, or a machine config. Adding the label to the machine set ensures that if the node or machine goes down, new nodes have the label. Labels added to a node or machine config do not persist if the node or machine goes down.

A pod is not scheduled if the **Pod** object contains a node selector, but no project has a matching node selector. When you create a pod from that spec, you receive an error similar to the following message:
Example error message

Error from server (Forbidden): error when creating "pod.yaml": pods "pod-4" is forbidden: pod node label selector conflicts with its project node label selector

NOTE

You can add additional key/value pairs to a pod. But you cannot add a different value for a project key.

Procedure

To add a default project node selector:

1. Create a namespace or edit an existing namespace to add the `openshift.io/node-selector` parameter:

   $ oc edit namespace <name>

   Example output

   ```yaml
   apiVersion: v1
   kind: Namespace
   metadata:
     annotations:
       openshift.io/node-selector: "type=user-node,region=east"
       openshift.io/display-name: ""
       openshift.io/requester: kube:admin
       openshift.io/sa.scc.mcs: s0:c30,c5
       openshift.io/sa.scc.supplemental-groups: 1000880000/10000
       openshift.io/sa.scc.uid-range: 1000880000/10000
     creationTimestamp: "2021-05-10T12:35:04Z"
   labels:
     kubernetes.io/metadata.name: demo
   name: demo
   resourceVersion: "145537"
   uid: 3f8786e3-1fcb-42e3-a0e3-e2ac54d15001
   spec:
     finalizers:
     - kubernetes
   ```

   Add the `openshift.io/node-selector` with the appropriate `<key>:<value>` pairs.

2. Add labels to a node by using a machine set or editing the node directly:

   - Use a `MachineSet` object to add labels to nodes managed by the machine set when a node is created:
     a. Run the following command to add labels to a `MachineSet` object:
For example:

```
$ oc patch MachineSet <name> --type='json' -p='["\"op\":\"add\",\"path\":\"/spec/template/spec/metadata/labels\",\"value\":\{\"key\":\"<value>\",\"<key\":\"<value>\"]\}\]" -n openshift-machine-api
```

**TIP**

You can alternatively apply the following YAML to add labels to a machine set:

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  name: <machineset>
namespace: openshift-machine-api
spec:
  template:
    spec:
      metadata:
        labels:
          region: "east"
          type: "user-node"

$ oc edit MachineSet ci-ln-l8nry52-f76d1-hl7m7-worker-c -n openshift-machine-api
```

b. Verify that the labels are added to the MachineSet object by using the `oc edit` command:

For example:

```
$ oc edit MachineSet ci-ln-l8nry52-f76d1-hl7m7-worker-c -n openshift-machine-api
```

**Example output**

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata: ...
spec: ...
  template:
    spec:
      metadata:
        labels:
          region: east
          type: user-node

$ oc edit MachineSet ci-ln-l8nry52-f76d1-hl7m7-worker-c -n openshift-machine-api
```

c. Redeploy the nodes associated with that machine set:

For example:
When the nodes are ready and available, verify that the label is added to the nodes by using the `oc get` command:

```
$ oc get nodes -l <key>=<value>
```

For example:

```
$ oc get nodes -l type=user-node,region=east
```

**Example output**

```
NAME                                       STATUS   ROLES    AGE   VERSION
ci-ln-l8nry52-f76d1-hl7m7-worker-c-vmqzp   Ready    worker   61s   v1.24.0
```

- Add labels directly to a node:
  a. Edit the `Node` object to add labels:

```
$ oc label <resource> <name> <key>=<value>
```

For example, to label a node:

```
$ oc label nodes ci-ln-l8nry52-f76d1-hl7m7-worker-c-tgq49 type=user-node region=east
```

**TIP**

You can alternatively apply the following YAML to add labels to a node:

```
kind: Node
apiVersion: v1
metadata:
  name: <node_name>
labels:
  type: "user-node"
  region: "east"
```

b. Verify that the labels are added to the `Node` object using the `oc get` command:

```
$ oc get nodes -l <key>=<value>
```

For example:

```
$ oc get nodes -l type=user-node,region=east
```
3.8. CONTROLLING POD PLACEMENT BY USING POD TOPOLOGY SPREAD CONSTRAINTS

You can use pod topology spread constraints to control the placement of your pods across nodes, zones, regions, or other user-defined topology domains.

3.8.1. About pod topology spread constraints

By using a pod topology spread constraint, you provide fine-grained control over the distribution of pods across failure domains to help achieve high availability and more efficient resource utilization.

OpenShift Container Platform administrators can label nodes to provide topology information, such as regions, zones, nodes, or other user-defined domains. After these labels are set on nodes, users can then define pod topology spread constraints to control the placement of pods across these topology domains.

You specify which pods to group together, which topology domains they are spread among, and the acceptable skew. Only pods within the same namespace are matched and grouped together when spreading due to a constraint.

3.8.2. Configuring pod topology spread constraints

The following steps demonstrate how to configure pod topology spread constraints to distribute pods that match the specified labels based on their zone.

You can specify multiple pod topology spread constraints, but you must ensure that they do not conflict with each other. All pod topology spread constraints must be satisfied for a pod to be placed.

Prerequisites

- A cluster administrator has added the required labels to nodes.

Procedure

1. Create a Pod spec and specify a pod topology spread constraint:

```
Example pod-spec.yaml file
```

```
apiVersion: v1
kinding: Pod
metadata:
  name: my-pod
labels:
  foo: bar
```
spec:
topologySpreadConstraints:
- maxSkew: 1
  topologyKey: topology.kubernetes.io/zone
  whenUnsatisfiable: DoNotSchedule
  labelSelector:
    matchLabels:
      foo: bar
containers:
- image: "docker.io/ocpqe/hello-pod"
  name: hello-pod

1. The maximum difference in number of pods between any two topology domains. The default is 1, and you cannot specify a value of 0.

2. The key of a node label. Nodes with this key and identical value are considered to be in the same topology.

3. How to handle a pod if it does not satisfy the spread constraint. The default is DoNotSchedule, which tells the scheduler not to schedule the pod. Set to ScheduleAnyway to still schedule the pod, but the scheduler prioritizes honoring the skew to not make the cluster more imbalanced.

4. Pods that match this label selector are counted and recognized as a group when spreading to satisfy the constraint. Be sure to specify a label selector, otherwise no pods can be matched.

5. Be sure that this Pod spec also sets its labels to match this label selector if you want it to be counted properly in the future.

2. Create the pod:

   $ oc create -f pod-spec.yaml

3.8.3. Example pod topology spread constraints

The following examples demonstrate pod topology spread constraint configurations.

3.8.3.1. Single pod topology spread constraint example

This example Pod spec defines one pod topology spread constraint. It matches on pods labeled foo:bar, distributes among zones, specifies a skew of 1, and does not schedule the pod if it does not meet these requirements.

kind: Pod
apiVersion: v1
metadata:
  name: my-pod
labels:
  foo: bar
spec:
topologySpreadConstraints:
- maxSkew: 1
3.8.3.2. Multiple pod topology spread constraints example

This example Pod spec defines two pod topology spread constraints. Both match on pods labeled foo:bar, specify a skew of 1, and do not schedule the pod if it does not meet these requirements.

The first constraint distributes pods based on a user-defined label node, and the second constraint distributes pods based on a user-defined label rack. Both constraints must be met for the pod to be scheduled.

```yaml
kind: Pod
apiVersion: v1
metadata:
  name: my-pod-2
  labels:
    foo: bar
spec:
topologySpreadConstraints:
  - maxSkew: 1
topologyKey: node
whenUnsatisfiable: DoNotSchedule
labelSelector:
  matchLabels:
    foo: bar

- maxSkew: 1
topologyKey: rack
whenUnsatisfiable: DoNotSchedule
labelSelector:
  matchLabels:
    foo: bar
containers:
  - image: "docker.io/ocpqe/hello-pod"
    name: hello-pod
```

3.8.4. Additional resources

- Understanding how to update labels on nodes

3.9. EVICTING PODS USING THE DESCHEDULER

While the scheduler is used to determine the most suitable node to host a new pod, the descheduler can be used to evict a running pod so that the pod can be rescheduled onto a more suitable node.

3.9.1. About the descheduler
You can use the descheduler to evict pods based on specific strategies so that the pods can be rescheduled onto more appropriate nodes.

You can benefit from descheduling running pods in situations such as the following:

- Nodes are underutilized or overutilized.
- Pod and node affinity requirements, such as taints or labels, have changed and the original scheduling decisions are no longer appropriate for certain nodes.
- Node failure requires pods to be moved.
- New nodes are added to clusters.
- Pods have been restarted too many times.

**IMPORTANT**

The descheduler does not schedule replacement of evicted pods. The scheduler automatically performs this task for the evicted pods.

When the descheduler decides to evict pods from a node, it employs the following general mechanism:

- Pods in the `openshift-*` and `kube-system` namespaces are never evicted.
- Critical pods with `priorityClassName` set to `system-cluster-critical` or `system-node-critical` are never evicted.
- Static, mirrored, or stand-alone pods that are not part of a replication controller, replica set, deployment, or job are never evicted because these pods will not be recreated.
- Pods associated with daemon sets are never evicted.
- Pods with local storage are never evicted.
- Best effort pods are evicted before burstable and guaranteed pods.
- All types of pods with the `descheduler.alpha.kubernetes.io/evict` annotation are eligible for eviction. This annotation is used to override checks that prevent eviction, and the user can select which pod is evicted. Users should know how and if the pod will be recreated.
- Pods subject to pod disruption budget (PDB) are not evicted if descheduling violates its pod disruption budget (PDB). The pods are evicted by using eviction subresource to handle PDB.

### 3.9.2. Descheduler profiles

The following descheduler profiles are available:

**AffinityAndTaints**

This profile evicts pods that violate inter-pod anti-affinity, node affinity, and node taints. It enables the following strategies:

- **RemovePodsViolatingInterPodAntiAffinity**: removes pods that are violating inter-pod anti-affinity.
- **RemovePodsViolatingNodeAffinity**: removes pods that are violating node affinity.
- **RemovePodsViolatingNodeTaints**: removes pods that are violating NoSchedule taints on nodes. Pods with a node affinity type of requiredDuringSchedulingIgnoredDuringExecution are removed.

**TopologyAndDuplicates**
This profile evicts pods in an effort to evenly spread similar pods, or pods of the same topology domain, among nodes.
It enables the following strategies:

- **RemovePodsViolatingTopologySpreadConstraint**: finds unbalanced topology domains and tries to evict pods from larger ones when DoNotSchedule constraints are violated.

- **RemoveDuplicates**: ensures that there is only one pod associated with a replica set, replication controller, deployment, or job running on same node. If there are more, those duplicate pods are evicted for better pod distribution in a cluster.

**LifecycleAndUtilization**
This profile evicts long-running pods and balances resource usage between nodes.
It enables the following strategies:

- **RemovePodsHavingTooManyRestarts**: removes pods whose containers have been restarted too many times. Pods where the sum of restarts over all containers (including Init Containers) is more than 100.

- **LowNodeUtilization**: finds nodes that are underutilized and evicts pods, if possible, from overutilized nodes in the hope that recreation of evicted pods will be scheduled on these underutilized nodes.

  A node is considered underutilized if its usage is below 20% for all thresholds (CPU, memory, and number of pods).

  A node is considered overutilized if its usage is above 50% for any of the thresholds (CPU, memory, and number of pods).

- **PodLifeTime**: evicts pods that are too old.
  By default, pods that are older than 24 hours are removed. You can customize the pod lifetime value.

**SoftTopologyAndDuplicates**
This profile is the same as TopologyAndDuplicates, except that pods with soft topology constraints, such as whenUnsatisfiable: ScheduleAnyway, are also considered for eviction.

**NOTE**
Do not enable both SoftTopologyAndDuplicates and TopologyAndDuplicates. Enabling both results in a conflict.

**EvictPodsWithLocalStorage**
This profile allows pods with local storage to be eligible for eviction.

**EvictPodsWithPVC**
This profile allows pods with persistent volume claims to be eligible for eviction.
3.9.3. Installing the descheduler

The descheduler is not available by default. To enable the descheduler, you must install the Kube Descheduler Operator from OperatorHub and enable one or more descheduler profiles.

By default, the descheduler runs in predictive mode, which means that it only simulates pod evictions. You must change the mode to automatic for the descheduler to perform the pod evictions.

IMPORTANT

If you have enabled hosted control planes in your cluster, set a custom priority threshold to lower the chance that pods in the hosted control plane namespaces are evicted. Set the priority threshold class name to **hypershift-control-plane**, because it has the lowest priority value (100000000) of the hosted control plane priority classes.

Prerequisites

- Cluster administrator privileges.
- Access to the OpenShift Container Platform web console.

Procedure

1. Log in to the OpenShift Container Platform web console.

2. Create the required namespace for the Kube Descheduler Operator.
   a. Navigate to **Administration → Namespaces** and click **Create Namespace**.
   b. Enter `openshift-kube-descheduler-operator` in the **Name** field, enter `openshift.io/cluster-monitoring=true` in the **Labels** field to enable descheduler metrics, and click **Create**.

3. Install the Kube Descheduler Operator.
   a. Navigate to **Operators → OperatorHub**.
   b. Type **Kube Descheduler Operator** into the filter box.
   c. Select the **Kube Descheduler Operator** and click **Install**.
   d. On the **Install Operator** page, select **A specific namespace on the cluster** Select `openshift-kube-descheduler-operator` from the drop-down menu.
   e. Adjust the values for the **Update Channel** and **Approval Strategy** to the desired values.
   f. Click **Install**.

4. Create a descheduler instance.
   a. From the **Operators → Installed Operators** page, click the **Kube Descheduler Operator**.
   b. Select the **Kube Descheduler** tab and click **Create KubeDescheduler**.
   c. Edit the settings as necessary.
      i. To evict pods instead of simulating the evictions, change the **Mode** field to **Automatic**.
ii. Expand the **Profiles** section to select one or more profiles to enable. The **AffinityAndTaints** profile is enabled by default. Click **Add Profile** to select additional profiles.

**NOTE**

Do not enable both **TopologyAndDuplicates** and **SoftTopologyAndDuplicates**. Enabling both results in a conflict.

iii. Optional: Expand the **Profile Customizations** section to set optional configurations for the descheduler.

- Set a custom pod lifetime value for the **LifecycleAndUtilization** profile. Use the `podLifetime` field to set a numerical value and a valid unit (s, m, or h). The default pod lifetime is 24 hours (24h).

- Set a custom priority threshold to consider pods for eviction only if their priority is lower than a specified priority level. Use the `thresholdPriority` field to set a numerical priority threshold or use the `thresholdPriorityClassName` field to specify a certain priority class name.

**NOTE**

Do not specify both `thresholdPriority` and `thresholdPriorityClassName` for the descheduler.

- Set specific namespaces to exclude or include from descheduler operations. Expand the `namespaces` field and add namespaces to the excluded or included list. You can only either set a list of namespaces to exclude or a list of namespaces to include.

- Experimental: Set thresholds for underutilization and overutilization for the **LowNodeUtilization** strategy. Use the `devLowNodeUtilizationThresholds` field to set one of the following values:
  - **Low**: 10% underutilized and 30% overutilized
  - **Medium**: 20% underutilized and 50% overutilized (Default)
  - **High**: 40% underutilized and 70% overutilized

**NOTE**

This setting is experimental and should not be used in a production environment.

iv. Optional: Use the **Descheduling Interval Seconds** field to change the number of seconds between descheduler runs. The default is **3600** seconds.

d. Click **Create**.

You can also configure the profiles and settings for the descheduler later using the OpenShift CLI (**oc**). If you did not adjust the profiles when creating the descheduler instance from the web console, the **AffinityAndTaints** profile is enabled by default.
3.9.4. Configuring descheduler profiles

You can configure which profiles the descheduler uses to evict pods.

Prerequisites

- Cluster administrator privileges

Procedure

1. Edit the KubeDescheduler object:

   ```
   $ oc edit kubedeschedulers.operator.openshift.io cluster -n openshift-kube-descheduler-operator
   ```

2. Specify one or more profiles in the spec.profiles section.

   ```
   apiVersion: operator.openshift.io/v1
   kind: KubeDescheduler
   metadata:
     name: cluster
     namespace: openshift-kube-descheduler-operator
   spec:
     deschedulingIntervalSeconds: 3600
     logLevel: Normal
     managementState: Managed
     operatorLogLevel: Normal
     profileCustomizations:
       namespaces:
         excluded:
         - my-namespace
       podLifetime: 48h
       thresholdPriorityClassName: my-priority-class-name
   profiles:
     - AffinityAndTaints
     - TopologyAndDuplicates
     - LifecycleAndUtilization
     - EvictPodsWithLocalStorage
     - EvictPodsWithPVC
   ```

   1. Optional: Set a list of user-created namespaces to include or exclude from descheduler operations. Use `excluded` to set a list of namespaces to exclude or use `included` to set a list of namespaces to include. Note that protected namespaces (`openshift-*`, `kube-system`, `hypershift`) are always excluded.

   2. Optional: Enable a custom pod lifetime value for the LifecycleAndUtilization profile. Valid units are `s`, `m`, or `h`. The default pod lifetime is 24 hours.

   3. Optional: Specify a priority threshold to consider pods for eviction only if their priority is lower than the specified level. Use the `thresholdPriority` field to set a numerical priority threshold (for example, `10000`) or use the `thresholdPriorityClassName` field to specify a certain priority class name (for example, `my-priority-class-name`). If you specify a priority class name, it must already exist or the descheduler will throw an error. Do not set both `thresholdPriority` and `thresholdPriorityClassName`. 

   4. 

   5. 

   6. 

Add one or more profiles to enable. Available profiles: **AffinityAndTaints**, **TopologyAndDuplicates**, **LifecycleAndUtilization**, **SoftTopologyAndDuplicates**.

Do not enable both **TopologyAndDuplicates** and **SoftTopologyAndDuplicates**. Enabling both results in a conflict.

You can enable multiple profiles; the order that the profiles are specified in is not important.

3. Save the file to apply the changes.

### 3.9.5. Configuring the descheduler interval

You can configure the amount of time between descheduler runs. The default is 3600 seconds (one hour).

**Prerequisites**

- Cluster administrator privileges

**Procedure**

1. Edit the **KubeDescheduler** object:

   ```bash
   $ oc edit kubedeschedulers.operator.openshift.io cluster -n openshift-kube-descheduler-operator
   ```

2. Update the **deschedulingIntervalSeconds** field to the desired value:

   ```json
   apiVersion: operator.openshift.io/v1
   kind: KubeDescheduler
   metadata:  
     name: cluster
     namespace: openshift-kube-descheduler-operator
   spec:
     deschedulingIntervalSeconds: 3600
   ...
   ```

   **1** Set the number of seconds between descheduler runs. A value of 0 in this field runs the descheduler once and exits.

3. Save the file to apply the changes.

### 3.9.6. Uninstalling the descheduler

You can remove the descheduler from your cluster by removing the descheduler instance and uninstalling the Kube Descheduler Operator. This procedure also cleans up the **KubeDescheduler** CRD and **openShift-kube-descheduler-operator** namespace.

**Prerequisites**

- Cluster administrator privileges.
- Access to the OpenShift Container Platform web console.
Procedure

1. Log in to the OpenShift Container Platform web console.

2. Delete the descheduler instance.
   a. From the Operators → Installed Operators page, click Kube Descheduler Operator.
   b. Select the Kube Descheduler tab.
   c. Click the Options menu next to the cluster entry and select Delete KubeDescheduler.
   d. In the confirmation dialog, click Delete.

3. Uninstall the Kube Descheduler Operator.
   a. Navigate to Operators → Installed Operators.
   b. Click the Options menu next to the Kube Descheduler Operator entry and select Uninstall Operator.
   c. In the confirmation dialog, click Uninstall.

4. Delete the openshift-kube-descheduler-operator namespace.
   a. Navigate to Administration → Namespaces.
   b. Enter openshift-kube-descheduler-operator into the filter box.
   c. Click the Options menu next to the openshift-kube-descheduler-operator entry and select Delete Namespace.
   d. In the confirmation dialog, enter openshift-kube-descheduler-operator and click Delete.

5. Delete the KubeDescheduler CRD.
   a. Navigate to Administration → Custom Resource Definitions
   b. Enter KubeDescheduler into the filter box.
   c. Click the Options menu next to the KubeDescheduler entry and select Delete CustomResourceDefinition.
   d. In the confirmation dialog, click Delete.

3.10. SECONDARY SCHEDULER

3.10.1. Secondary scheduler overview
You can install the Secondary Scheduler Operator to run a custom secondary scheduler alongside the default scheduler to schedule pods.

### 3.10.1.1. About the Secondary Scheduler Operator

The Secondary Scheduler Operator for Red Hat OpenShift provides a way to deploy a custom secondary scheduler in OpenShift Container Platform. The secondary scheduler runs alongside the default scheduler to schedule pods. Pod configurations can specify which scheduler to use.

The custom scheduler must have the `bin/kube-scheduler` binary and be based on the Kubernetes scheduling framework.

**IMPORTANT**

You can use the Secondary Scheduler Operator to deploy a custom secondary scheduler in OpenShift Container Platform, but Red Hat does not directly support the functionality of the custom secondary scheduler.

The Secondary Scheduler Operator creates the default roles and role bindings required by the secondary scheduler. You can specify which scheduling plug-ins to enable or disable by configuring the `KubeSchedulerConfiguration` resource for the secondary scheduler.

### 3.10.2. Secondary Scheduler Operator for Red Hat OpenShift release notes

The Secondary Scheduler Operator for Red Hat OpenShift allows you to deploy a custom secondary scheduler in your OpenShift Container Platform cluster.

These release notes track the development of the Secondary Scheduler Operator for Red Hat OpenShift.

For more information, see About the Secondary Scheduler Operator.

#### 3.10.2.1. Release notes for Secondary Scheduler Operator for Red Hat OpenShift 1.1.0

**Issued:** 2022-9-1

The following advisory is available for the Secondary Scheduler Operator for Red Hat OpenShift 1.1.0:

- RHSA-2022:6152

#### 3.10.2.1.1. New features and enhancements

- The Secondary Scheduler Operator security context configuration has been updated to comply with pod security admission enforcement.

#### 3.10.2.1.2. Known issues

- Currently, you cannot deploy additional resources, such as config maps, CRDs, or RBAC policies through the Secondary Scheduler Operator. Any resources other than roles and role bindings that are required by your custom secondary scheduler must be applied externally. (BZ#2071684)

#### 3.10.2.2. Release notes for Secondary Scheduler Operator for Red Hat OpenShift 1.0.1
The following advisory is available for the Secondary Scheduler Operator for Red Hat OpenShift 1.0.1:

- RHSA-2022:5699

### 3.10.2.2.1. New features and enhancements

- The maximum OpenShift Container Platform version for Secondary Scheduler Operator for Red Hat OpenShift 1.0.1 is 4.11.

### 3.10.2.2.2. Bug fixes

- Previously, the secondary scheduler deployment was not deleted after the secondary scheduler custom resource (CR) was deleted, which prevented the Secondary Scheduler Operator and operand from being fully uninstalled. The secondary scheduler deployment is now deleted when the secondary scheduler CR is deleted, so that the Secondary Scheduler Operator can now be fully uninstalled. ([BZ#2100923](#))

### 3.10.2.2.3. Known issues

- Currently, you cannot deploy additional resources, such as config maps, CRDs, or RBAC policies through the Secondary Scheduler Operator. Any resources other than roles and role bindings that are required by your custom secondary scheduler must be applied externally. ([BZ#2071684](#))

### 3.10.2.3. Release notes for Secondary Scheduler Operator for Red Hat OpenShift 1.0.0

Issued: 2022-04-18

The following advisory is available for the Secondary Scheduler Operator for Red Hat OpenShift 1.0.0:

- RHEA-2022:1346

### 3.10.2.3.1. New features and enhancements

- This is the initial release of the Secondary Scheduler Operator for Red Hat OpenShift.

### 3.10.2.3.2. Known issues

- Currently, you cannot deploy additional resources, such as config maps, CRDs, or RBAC policies through the Secondary Scheduler Operator. Any resources other than roles and role bindings that are required by your custom secondary scheduler must be applied externally. ([BZ#2071684](#))

### 3.10.3. Scheduling pods using a secondary scheduler

You can run a custom secondary scheduler in OpenShift Container Platform by installing the Secondary Scheduler Operator, deploying the secondary scheduler, and setting the secondary scheduler in the pod definition.

#### 3.10.3.1. Installing the Secondary Scheduler Operator

You can use the web console to install the Secondary Scheduler Operator for Red Hat OpenShift.
Prerequisites

- You have access to the cluster with `cluster-admin` privileges.
- You have access to the OpenShift Container Platform web console.

Procedure

1. Log in to the OpenShift Container Platform web console.
   a. Navigate to Administration → Namespaces and click Create Namespace.
   b. Enter `openshift-secondary-scheduler-operator` in the Name field and click Create.
   a. Navigate to Operators → OperatorHub.
   b. Enter Secondary Scheduler Operator for Red Hat OpenShift into the filter box.
   c. Select the Secondary Scheduler Operator for Red Hat OpenShift and click Install.
   d. On the Install Operator page:
      i. The Update channel is set to stable, which installs the latest stable release of the Secondary Scheduler Operator for Red Hat OpenShift.
      ii. Select A specific namespace on the cluster and select `openshift-secondary-scheduler-operator` from the drop-down menu.
      iii. Select an Update approval strategy.
         - The Automatic strategy allows Operator Lifecycle Manager (OLM) to automatically update the Operator when a new version is available.
         - The Manual strategy requires a user with appropriate credentials to approve the Operator update.
      iv. Click Install.

Verification

1. Navigate to Operators → Installed Operators.
2. Verify that Secondary Scheduler Operator for Red Hat OpenShift is listed with a Status of Succeeded.

3.10.3.2. Deploying a secondary scheduler

After you have installed the Secondary Scheduler Operator, you can deploy a secondary scheduler.

Prerequisites

- You have access to the cluster with `cluster-admin` privileges.
- You have access to the OpenShift Container Platform web console.
- The Secondary Scheduler Operator for Red Hat OpenShift is installed.

**Procedure**

1. Log in to the OpenShift Container Platform web console.

2. Create config map to hold the configuration for the secondary scheduler.
   a. Navigate to Workloads → ConfigMaps.
   b. Click Create ConfigMap.
   c. In the YAML editor, enter the config map definition that contains the necessary `KubeSchedulerConfiguration` configuration. For example:

   ```yaml
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: "secondary-scheduler-config"
     namespace: "openshift-secondary-scheduler-operator"
   data:
     "config.yaml": |
     apiVersion: kubescheduler.config.k8s.io/v1beta3
     kind: KubeSchedulerConfiguration
     leaderElection:
       leaderElect: false
     profiles:
       - schedulerName: secondary-scheduler
         plugins:
           score:
             disabled:
               - name: NodeResourcesBalancedAllocation
               - name: NodeResourcesLeastAllocated
   ``

   1 The name of the config map. This is used in the **Scheduler Config** field when creating the **SecondaryScheduler** CR.
   2 The config map must be created in the `openshift-secondary-scheduler-operator` namespace.
   3 The `KubeSchedulerConfiguration` resource for the secondary scheduler. For more information, see `KubeSchedulerConfiguration` in the Kubernetes API documentation.
   4 The name of the secondary scheduler. Pods that set their **spec.schedulerName** field to this value are scheduled with this secondary scheduler.
   5 The plug-ins to enable or disable for the secondary scheduler. For a list default scheduling plug-ins, see `Scheduling plugins` in the Kubernetes documentation.
   d. Click Create.

3. Create the **SecondaryScheduler** CR:
3.10.3.3. Scheduling a pod using the secondary scheduler

To schedule a pod using the secondary scheduler, set the `schedulerName` field in the pod definition.

**Prerequisites**

- You have access to the cluster with `cluster-admin` privileges.
- You have access to the OpenShift Container Platform web console.
- The Secondary Scheduler Operator for Red Hat OpenShift is installed.
- A secondary scheduler is configured.

**Procedure**

1. Log in to the OpenShift Container Platform web console.

2. Navigate to Workloads → Pods.

3. Click Create Pod.

4. In the YAML editor, enter the desired pod configuration and add the `schedulerName` field:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: nginx
  namespace: default
spec:
  containers:
  - name: nginx
    image: nginx:1.14.2
```
The schedulerName field must match the name that is defined in the config map when you configured the secondary scheduler.

5. Click Create.

Verification

1. Log in to the OpenShift CLI.

2. Describe the pod using the following command:

   $ oc describe pod nginx -n default

   **Example output**

   Name:         nginx
   Namespace:    default
   Priority:     0
   Node:         ci-ln-t0w4r1k-72292-xkqs4-worker-b-xqkxp/10.0.128.3
   ...
   Events:
   Type    Reason          Age   From                 Message
   ----    ------          ----  ----                 -------
   Normal  Scheduled       12s   secondary-scheduler  Successfully assigned default/nginx to ci-ln-t0w4r1k-72292-xkqs4-worker-b-xqkxp
   ...

3. In the events table, find the event with a message similar to **Successfully assigned <namespace>/<pod_name> to <node_name>**.

4. In the "From" column, verify that the event was generated from the secondary scheduler and not the default scheduler.

   **NOTE**

   You can also check the secondary-scheduler-* pod logs in the openshift-secondary-scheduler-namespace to verify that the pod was scheduled by the secondary scheduler.

3.10.4. Uninstalling the Secondary Scheduler Operator

You can remove the Secondary Scheduler Operator for Red Hat OpenShift from OpenShift Container Platform by uninstalling the Operator and removing its related resources.

3.10.4.1. Uninstalling the Secondary Scheduler Operator

You can uninstall the Secondary Scheduler Operator for Red Hat OpenShift by using the web console.
Prerequisites

- You have access to the cluster with `cluster-admin` privileges.
- You have access to the OpenShift Container Platform web console.
- The Secondary Scheduler Operator for Red Hat OpenShift is installed.

Procedure

1. Log in to the OpenShift Container Platform web console.

   a. Navigate to **Operators → Installed Operators**.
   b. Click the Options menu next to the **Secondary Scheduler Operator** entry and click **Uninstall Operator**.
   c. In the confirmation dialog, click **Uninstall**.

3.10.4.2. Removing Secondary Scheduler Operator resources

Optionally, after uninstalling the Secondary Scheduler Operator for Red Hat OpenShift, you can remove its related resources from your cluster.

Prerequisites

- You have access to the cluster with `cluster-admin` privileges.
- You have access to the OpenShift Container Platform web console.

Procedure

1. Log in to the OpenShift Container Platform web console.

2. Remove CRDs that were installed by the Secondary Scheduler Operator:
   a. Navigate to **Administration → CustomResourceDefinitions**.
   b. Enter **SecondaryScheduler** in the **Name** field to filter the CRDs.
   c. Click the Options menu next to the **SecondaryScheduler** CRD and select **Delete Custom Resource Definition**:

3. Remove the **openshift-secondary-scheduler-operator** namespace.
   a. Navigate to **Administration → Namespaces**.
   b. Click the Options menu next to the **openshift-secondary-scheduler-operator** and select **Delete Namespace**.
c. In the confirmation dialog, enter `openshift-secondary-scheduler-operator` in the field and click Delete.
CHAPTER 4. USING JOBS AND DAEMONSETS

4.1. RUNNING BACKGROUND TASKS ON NODES AUTOMATICALLY WITH DAEMON SETS

As an administrator, you can create and use daemon sets to run replicas of a pod on specific or all nodes in an OpenShift Container Platform cluster.

A daemon set ensures that all (or some) nodes run a copy of a pod. As nodes are added to the cluster, pods are added to the cluster. As nodes are removed from the cluster, those pods are removed through garbage collection. Deleting a daemon set will clean up the pods it created.

You can use daemon sets to create shared storage, run a logging pod on every node in your cluster, or deploy a monitoring agent on every node.

For security reasons, only cluster administrators can create daemon sets.

For more information on daemon sets, see the Kubernetes documentation.

IMPORTANT

Daemon set scheduling is incompatible with project’s default node selector. If you fail to disable it, the daemon set gets restricted by merging with the default node selector. This results in frequent pod recreates on the nodes that got unselected by the merged node selector, which in turn puts unwanted load on the cluster.

4.1.1. Scheduled by default scheduler

A daemon set ensures that all eligible nodes run a copy of a pod. Normally, the node that a pod runs on is selected by the Kubernetes scheduler. However, previously daemon set pods are created and scheduled by the daemon set controller. That introduces the following issues:

- Inconsistent pod behavior: Normal pods waiting to be scheduled are created and in Pending state, but daemon set pods are not created in Pending state. This is confusing to the user.

- Pod preemption is handled by default scheduler. When preemption is enabled, the daemon set controller will make scheduling decisions without considering pod priority and preemption.

The ScheduleDaemonSetPods feature, enabled by default in OpenShift Container Platform, lets you to schedule daemon sets using the default scheduler instead of the daemon set controller, by adding the NodeAffinity term to the daemon set pods, instead of the spec.nodeName term. The default scheduler is then used to bind the pod to the target host. If node affinity of the daemon set pod already exists, it is replaced. The daemon set controller only performs these operations when creating or modifying daemon set pods, and no changes are made to the spec.template of the daemon set.

```
nodeAffinity:
  requiredDuringSchedulingIgnoredDuringExecution:
    nodeSelectorTerms:
      - matchFields:
          - key: metadata.name
            operator: In
            values:
          - target-host-name
```
In addition, a `node.kubernetes.io/unschedulable:NoSchedule` toleration is added automatically to daemon set pods. The default scheduler ignores unschedulable Nodes when scheduling daemon set pods.

### 4.1.2. Creating daemonsets

When creating daemon sets, the `nodeSelector` field is used to indicate the nodes on which the daemon set should deploy replicas.

**Prerequisites**

- Before you start using daemon sets, disable the default project-wide node selector in your namespace, by setting the namespace annotation `openshift.io/node-selector` to an empty string:

  ```
  $ oc patch namespace myproject -p \
  '{"metadata": {"annotations": {"openshift.io/node-selector": ""}}}"
  ```

**TIP**

You can alternatively apply the following YAML to disable the default project-wide node selector for a namespace:

```yaml
apiVersion: v1
kind: Namespace
metadata:
  name: <namespace>
  annotations:
    openshift.io/node-selector: ""
```

- If you are creating a new project, overwrite the default node selector:

  ```
  $ oc adm new-project <name> --node-selector=""
  ```

**Procedure**

To create a daemon set:

1. Define the daemon set yaml file:

   ```yaml
   apiVersion: apps/v1
   kind: DaemonSet
   metadata:
     name: hello-daemonset
   spec:
     selector:
       matchLabels:
         name: hello-daemonset 1
   template:
     metadata:
       labels:
         name: hello-daemonset 2
   spec:
   ```
nodeSelector:  
  role: worker 
containers: 
  - image: openshift/hello-openshift 
    imagePullPolicy: Always 
    name: registry 
    ports: 
      - containerPort: 80 
        protocol: TCP 
    resources: {} 
    terminationMessagePath: /dev/termination-log 
    serviceAccount: default 
    terminationGracePeriodSeconds: 10 

1. The label selector that determines which pods belong to the daemon set.
2. The pod template’s label selector. Must match the label selector above.
3. The node selector that determines on which nodes pod replicas should be deployed. A matching label must be present on the node.

2. Create the daemon set object:

```bash
$ oc create -f daemonset.yaml
```

3. To verify that the pods were created, and that each node has a pod replica:
   a. Find the daemonset pods:

```bash
$ oc get pods
```

**Example output**

```
hello-daemonset-cx6md   1/1       Running   0          2m
hello-daemonset-e3md9   1/1       Running   0          2m
```

   b. View the pods to verify the pod has been placed onto the node:

```bash
$ oc describe pod/hello-daemonset-cx6md|grep Node
```

**Example output**

```
```

```bash
$ oc describe pod/hello-daemonset-e3md9|grep Node
```

**Example output**

```
```
IMPORTANT

- If you update a daemon set pod template, the existing pod replicas are not affected.

- If you delete a daemon set and then create a new daemon set with a different template but the same label selector, it recognizes any existing pod replicas as having matching labels and thus does not update them or create new replicas despite a mismatch in the pod template.

- If you change node labels, the daemon set adds pods to nodes that match the new labels and deletes pods from nodes that do not match the new labels.

To update a daemon set, force new pod replicas to be created by deleting the old replicas or nodes.

4.2. RUNNING TASKS IN PODS USING JOBS

A job executes a task in your OpenShift Container Platform cluster.

A job tracks the overall progress of a task and updates its status with information about active, succeeded, and failed pods. Deleting a job will clean up any pod replicas it created. Jobs are part of the Kubernetes API, which can be managed with `oc` commands like other object types.

**Sample Job specification**

```yaml
apiVersion: batch/v1
kind: Job
metadata:
  name: pi
spec:
  parallelism: 1
  completions: 1
  activeDeadlineSeconds: 1800
  backoffLimit: 6
  template:
    metadata:
      name: pi
    spec:
      containers:
        - name: pi
          image: perl
          command: ['perl', '-Mbignum=bpi', '-wle', 'print bpi(2000)']
      restartPolicy: OnFailure
```

1. The pod replicas a job should run in parallel.
2. Successful pod completions are needed to mark a job completed.
3. The maximum duration the job can run.
4. The number of retries for a job.
5. The template for the pod the controller creates.
The restart policy of the pod.

See the Kubernetes documentation for more information about jobs.

### 4.2.1. Understanding jobs and cron jobs

A job tracks the overall progress of a task and updates its status with information about active, succeeded, and failed pods. Deleting a job cleans up any pods it created. Jobs are part of the Kubernetes API, which can be managed with `oc` commands like other object types.

There are two possible resource types that allow creating run-once objects in OpenShift Container Platform:

**Job**

A regular job is a run-once object that creates a task and ensures the job finishes.

There are three main types of task suitable to run as a job:

- **Non-parallel jobs:**
  - A job that starts only one pod, unless the pod fails.
  - The job is complete as soon as its pod terminates successfully.

- **Parallel jobs with a fixed completion count:**
  - A job that starts multiple pods.
  - The job represents the overall task and is complete when there is one successful pod for each value in the range $1$ to the `completions` value.

- **Parallel jobs with a work queue:**
  - A job with multiple parallel worker processes in a given pod.
  - OpenShift Container Platform coordinates pods to determine what each should work on or use an external queue service.
  - Each pod is independently capable of determining whether or not all peer pods are complete and that the entire job is done.
  - When any pod from the job terminates with success, no new pods are created.
  - When at least one pod has terminated with success and all pods are terminated, the job is successfully completed.
  - When any pod has exited with success, no other pod should be doing any work for this task or writing any output. Pods should all be in the process of exiting.

For more information about how to make use of the different types of job, see Job Patterns in the Kubernetes documentation.

**Cron job**

A job can be scheduled to run multiple times, using a cron job.
A cron job builds on a regular job by allowing you to specify how the job should be run. Cron jobs are part of the Kubernetes API, which can be managed with `oc` commands like other object types.

Cron jobs are useful for creating periodic and recurring tasks, like running backups or sending emails. Cron jobs can also schedule individual tasks for a specific time, such as if you want to schedule a job for a low activity period. A cron job creates a **Job** object based on the timezone configured on the control plane node that runs the cronjob controller.

**WARNING**

A cron job creates a **Job** object approximately once per execution time of its schedule, but there are circumstances in which it fails to create a job or two jobs might be created. Therefore, jobs must be idempotent and you must configure history limits.

### 4.2.1.1. Understanding how to create jobs

Both resource types require a job configuration that consists of the following key parts:

- A pod template, which describes the pod that OpenShift Container Platform creates.
- The **parallelism** parameter, which specifies how many pods running in parallel at any point in time should execute a job.
  - For non-parallel jobs, leave unset. When unset, defaults to 1.
- The **completions** parameter, specifying how many successful pod completions are needed to finish a job.
  - For non-parallel jobs, leave unset. When unset, defaults to 1.
  - For parallel jobs with a fixed completion count, specify a value.
  - For parallel jobs with a work queue, leave unset. When unset defaults to the **parallelism** value.

### 4.2.1.2. Understanding how to set a maximum duration for jobs

When defining a job, you can define its maximum duration by setting the **activeDeadlineSeconds** field. It is specified in seconds and is not set by default. When not set, there is no maximum duration enforced.

The maximum duration is counted from the time when a first pod gets scheduled in the system, and defines how long a job can be active. It tracks overall time of an execution. After reaching the specified timeout, the job is terminated by OpenShift Container Platform.

### 4.2.1.3. Understanding how to set a job back off policy for pod failure

A job can be considered failed, after a set amount of retries due to a logical error in configuration or other similar reasons. Failed pods associated with the job are recreated by the controller with an exponential back off delay (10s, 20s, 40s ...) capped at six minutes. The limit is reset if no new failed pods appear between controller checks.
Use the `spec.backoffLimit` parameter to set the number of retries for a job.

### 4.2.1.4. Understanding how to configure a cron job to remove artifacts

Cron jobs can leave behind artifact resources such as jobs or pods. As a user it is important to configure history limits so that old jobs and their pods are properly cleaned. There are two fields within cron job’s `spec` responsible for that:

- `spec.successfulJobsHistoryLimit`. The number of successful finished jobs to retain (defaults to 3).
- `spec.failedJobsHistoryLimit`. The number of failed finished jobs to retain (defaults to 1).

**TIP**

- Delete cron jobs that you no longer need:
  
  ```bash
  $ oc delete cronjob/<cron_job_name>
  
  Doing this prevents them from generating unnecessary artifacts.
  ```

- You can suspend further executions by setting the `spec.suspend` to true. All subsequent executions are suspended until you reset to `false`.

### 4.2.1.5. Known limitations

The job specification restart policy only applies to the `pods`, and not the `job controller`. However, the job controller is hard-coded to keep retrying jobs to completion.

As such, `restartPolicy: Never` or `--restart=Never` results in the same behavior as `restartPolicy: OnFailure` or `--restart=OnFailure`. That is, when a job fails it is restarted automatically until it succeeds (or is manually discarded). The policy only sets which subsystem performs the restart.

With the `Never` policy, the `job controller` performs the restart. With each attempt, the job controller increments the number of failures in the job status and create new pods. This means that with each failed attempt, the number of pods increases.

With the `OnFailure` policy, `kubelet` performs the restart. Each attempt does not increment the number of failures in the job status. In addition, kubelet will retry failed jobs starting pods on the same nodes.

### 4.2.2. Creating jobs

You create a job in OpenShift Container Platform by creating a job object.

**Procedure**

To create a job:

1. Create a YAML file similar to the following:

   ```yaml
   apiVersion: batch/v1
   kind: Job
   metadata:
     name: pi
   spec:
   ```
Optional: Specify how many pod replicas a job should run in parallel; defaults to 1.

- For non-parallel jobs, leave unset. When unset, defaults to 1.

Optional: Specify how many successful pod completions are needed to mark a job completed.

- For non-parallel jobs, leave unset. When unset, defaults to 1.
- For parallel jobs with a fixed completion count, specify the number of completions.
- For parallel jobs with a work queue, leave unset. When unset defaults to the parallelism value.

Optional: Specify the maximum duration the job can run.

Optional: Specify the number of retries for a job. This field defaults to six.

Specify the template for the pod the controller creates.

Specify the restart policy of the pod:

- **Never**. Do not restart the job.
- **OnFailure**. Restart the job only if it fails.
- **Always**. Always restart the job.
  For details on how OpenShift Container Platform uses restart policy with failed containers, see the Example States in the Kubernetes documentation.

2. Create the job:

```bash
$ oc create -f <file-name>.yaml
```
NOTE

You can also create and launch a job from a single command using `oc create job`. The following command creates and launches a job similar to the one specified in the previous example:

```
$ oc create job pi --image=perl -- perl -Mbignum=bpi -wle 'print bpi(2000)'
```

4.2.3. Creating cron jobs

You create a cron job in OpenShift Container Platform by creating a job object.

Procedure

To create a cron job:

1. Create a YAML file similar to the following:

   ```yaml
   apiVersion: batch/v1
   kind: CronJob
   metadata:
     name: pi
   spec:
     schedule: "*/1 * * * *"  # Schedule for the job specified in cron format. In this example, the job will run every minute.
     concurrencyPolicy: "Replace"  # An optional concurrency policy, specifying how to treat concurrent jobs within a cron job. Only one of the following concurrent policies may be specified. If not specified, this defaults to allowing concurrent executions.
     startingDeadlineSeconds: 200  # An optional startingDeadlineSeconds
     suspend: true  # A boolean that indicates if the CronJob should be suspended or not.
     successfulJobsHistoryLimit: 3  # The maximum number of successful jobs that should be kept.
     failedJobsHistoryLimit: 1  # The maximum number of failed jobs that should be kept.
   jobTemplate:
     spec:
       template:
         metadata:
           labels:
             parent: "cronjobpi"
         spec:
           containers:
             - name: pi
               image: perl
               command: ["perl", "-Mbignum=bpi", "-wle", "print bpi(2000)"
      restartPolicy: OnFailure  # How to handle failed executions.
   ```

(1) Schedule for the job specified in cron format. In this example, the job will run every minute.

(2) An optional concurrency policy, specifying how to treat concurrent jobs within a cron job. Only one of the following concurrent policies may be specified. If not specified, this defaults to allowing concurrent executions.

- **Allow** allows cron jobs to run concurrently.
- **Forbid** forbids concurrent runs, skipping the next run if the previous has not finished yet.
- **Replace** cancels the currently running job and replaces it with a new one.
An optional deadline (in seconds) for starting the job if it misses its scheduled time for any reason. Missed jobs executions will be counted as failed ones. If not specified, there is no deadline.

An optional flag allowing the suspension of a cron job. If set to true, all subsequent executions will be suspended.

The number of successful finished jobs to retain (defaults to 3).

The number of failed finished jobs to retain (defaults to 1).

Job template. This is similar to the job example.

Sets a label for jobs spawned by this cron job.

The restart policy of the pod. This does not apply to the job controller.

**NOTE**

The `.spec.successfulJobsHistoryLimit` and `.spec.failedJobsHistoryLimit` fields are optional. These fields specify how many completed and failed jobs should be kept. By default, they are set to 3 and 1 respectively. Setting a limit to 0 corresponds to keeping none of the corresponding kind of jobs after they finish.

2. Create the cron job:

```
$ oc create -f <file-name>.yaml
```

**NOTE**

You can also create and launch a cron job from a single command using `oc create cronjob`. The following command creates and launches a cron job similar to the one specified in the previous example:

```
$ oc create cronjob pi --image=perl --schedule="*/1 * * * *" -- perl -Mbignum=bpi -wle 'print bpi(2000)'
```

With `oc create cronjob`, the `--schedule` option accepts schedules in cron format.
CHAPTER 5. WORKING WITH NODES

5.1. VIEWING AND LISTING THE NODES IN YOUR OPENSHEET CONTAINER PLATFORM CLUSTER

You can list all the nodes in your cluster to obtain information such as status, age, memory usage, and details about the nodes.

When you perform node management operations, the CLI interacts with node objects that are representations of actual node hosts. The master uses the information from node objects to validate nodes with health checks.

5.1.1. About listing all the nodes in a cluster

You can get detailed information on the nodes in the cluster.

- The following command lists all nodes:

  $ oc get nodes

  The following example is a cluster with healthy nodes:

  Example output

  NAME     STATUS    ROLES     AGE       VERSION
  master.example.com     Ready     master    7h       v1.24.0
  node1.example.com      Ready     worker    7h       v1.24.0
  node2.example.com      Ready     worker    7h       v1.24.0

  The following example is a cluster with one unhealthy node:

  $ oc get nodes

  Example output

  NAME     STATUS                      ROLES     AGE       VERSION
  master.example.com     Ready                       master    7h       v1.24.0
  node1.example.com      NotReady,SchedulingDisabled worker 7h       v1.24.0
  node2.example.com      Ready                       worker    7h       v1.24.0

  The conditions that trigger a NotReady status are shown later in this section.

- The -o wide option provides additional information on nodes.

  $ oc get nodes -o wide

  Example output

  NAME     STATUS    ROLES    AGE       VERSION  INTERNAL-IP  EXTERNAL-IP
  master.example.com     Ready     master    7h       v1.24.0
  node1.example.com      NotReady,SchedulingDisabled worker 7h       v1.24.0
  node2.example.com      Ready     worker    7h       v1.24.0
The following command lists information about a single node:

```
$ oc get node <node>
```

For example:

```
$ oc get node node1.example.com
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>ROLES</th>
<th>AGE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1.example.com</td>
<td>Ready</td>
<td>worker</td>
<td>7h</td>
<td>v1.24.0</td>
</tr>
</tbody>
</table>

The following command provides more detailed information about a specific node, including the reason for the current condition:

```
$ oc describe node <node>
```

For example:

```
$ oc describe node node1.example.com
```

**Example output**

Name: node1.example.com
Roles: worker
Labels: beta.kubernetes.io/arch=amd64
beta.kubernetes.io/instance-type=m4.large
beta.kubernetes.io/os=linux
failure-domain.beta.kubernetes.io/region=us-east-2
failure-domain.beta.kubernetes.io/zone=us-east-2a
kubernetes.io/hostname=ip-10-0-140-16
node-role.kubernetes.io/worker=
Annotations: cluster.k8s.io/machine: openshift-machine-api/ahardin-worker-us-east-2a-q5dzc
machineconfiguration.openshift.io/currentConfig: worker-309c228e8b3a92e2235edd544c62feaa8
machineconfiguration.openshift.io/desiredConfig: worker-309c228e8b3a92e2235edd544c62feaa8
machineconfiguration.openshift.io/state: Done
volumes.kubernetes.io/controller-managed-attach-detach: true
Taints: <none>
Unschedulable: false
Conditions:

<table>
<thead>
<tr>
<th>Type</th>
<th>Status</th>
<th>LastHeartbeatTime</th>
<th>LastTransitionTime</th>
<th>Reason</th>
</tr>
</thead>
</table>

Ready: True
KubeletReady: kubelet is posting ready status
Addresses:
InternalIP: 10.0.140.16
InternalDNS: ip-10-0-140-16.us-east-2.compute.internal
Hostname: ip-10-0-140-16.us-east-2.compute.internal
Capacity:
attachable-volumes-aws-ebs: 39
cpu: 2
hugepages-1Gi: 0
hugepages-2Mi: 0
memory: 8172516Ki
pods: 250
Allocatable:
attachable-volumes-aws-ebs: 39
cpu: 1500m
hugepages-1Gi: 0
hugepages-2Mi: 0
memory: 7558116Ki
pods: 250
System Info:
Machine ID: 63787c9534c24fde9a0cde35c13f1f66
System UUID: EC2BF97-A006-4A58-6AF8-0A38DEEA122A
Boot ID: f24ad37d-2594-46b4-8830-775555918325
Kernel Version: 3.10.0-957.5.1.el7.x86_64
OS Image: Red Hat Enterprise Linux CoreOS 410.8.20190520.0 (Ootpa)
Operating System: linux
Architecture: amd64
Container Runtime Version: cri-o://1.24.0-0.6.dev.rhcos4.3.git9ad059b.el8-rc2
Kubelet Version: v1.24.0
Kube-Proxy Version: v1.24.0
PodCIDR: 10.128.4.0/24
ProviderID: aws:///us-east-2a/i-04e87b31dc6b3e171
Non-terminated Pods: (12 in total)

<table>
<thead>
<tr>
<th>Namespace</th>
<th>Name</th>
<th>CPU Requests</th>
<th>CPU Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>

OpenShift Container Platform 4.11 Nodes
192
<table>
<thead>
<tr>
<th>Node Name</th>
<th>Role</th>
<th>Allocated Resources</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>openshift-dns</td>
<td>dns-default-l69zr</td>
<td>0 (0%)</td>
<td>Normal NodeHasSufficientPID 6d (x5 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientPID</td>
</tr>
<tr>
<td>openshift-image-registry</td>
<td>node-ca-9hmcg</td>
<td>0 (0%) 0 (0%)</td>
<td>Normal NodeAllocatableEnforced 6d kubelet, m01.example.com Updated Node Allocatable limit across pods</td>
</tr>
<tr>
<td>openshift-ingress</td>
<td>router-default-76455c45c-c5ptv</td>
<td>0 (0%)</td>
<td>Normal NodeHasSufficientMemory 6d (x6 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientMemory</td>
</tr>
<tr>
<td>openshift-machine-config-operator</td>
<td>machine-config-daemon-cvqw9</td>
<td>20m (1%) 0 (0%)</td>
<td>Normal NodeHasNoDiskPressure 6d (x6 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasNoDiskPressure</td>
</tr>
<tr>
<td>openshift-machine-config-operator</td>
<td>machine-config-daemon-cvqw9</td>
<td>20m (1%) 0 (0%)</td>
<td>Normal NodeHasSufficientDisk 6d (x6 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientDisk</td>
</tr>
<tr>
<td>openshift-marketplace</td>
<td>community-operators-f67fh</td>
<td>0 (0%)</td>
<td>Normal NodeHasSufficientPID 6d kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientPID</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>alertmanager-main-0</td>
<td>50m (3%) 50m (3%)</td>
<td>Normal Starting 6d kubelet, m01.example.com Starting kubelet.</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>node-exporter-l7q8d</td>
<td>10m (0%) 20m (1%)</td>
<td>Normal NodeHasSufficientPID 6d kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientPID</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>prometheus-adapter-75d769c874-hvb85</td>
<td>0 (0%)</td>
<td>Normal Starting 6d kubelet, m01.example.com Starting kubelet.</td>
</tr>
<tr>
<td>openshift-machine-config-operator</td>
<td>machine-config-daemon-cvqw9</td>
<td>20m (1%) 0 (0%)</td>
<td>Normal NodeHasSufficientDisk 6d (x6 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientDisk</td>
</tr>
<tr>
<td>openshift-marketplace</td>
<td>community-operators-f67fh</td>
<td>0 (0%)</td>
<td>Normal NodeHasSufficientPID 6d kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientPID</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>alertmanager-main-0</td>
<td>50m (3%) 50m (3%)</td>
<td>Normal Starting 6d kubelet, m01.example.com Starting kubelet.</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>node-exporter-l7q8d</td>
<td>10m (0%) 20m (1%)</td>
<td>Normal NodeHasSufficientDisk 6d (x6 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientDisk</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>prometheus-adapter-75d769c874-hvb85</td>
<td>0 (0%)</td>
<td>Normal Starting 6d kubelet, m01.example.com Starting kubelet.</td>
</tr>
<tr>
<td>openshift-machine-config-operator</td>
<td>machine-config-daemon-cvqw9</td>
<td>20m (1%) 0 (0%)</td>
<td>Normal NodeHasSufficientDisk 6d (x6 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientDisk</td>
</tr>
<tr>
<td>openshift-marketplace</td>
<td>community-operators-f67fh</td>
<td>0 (0%)</td>
<td>Normal NodeHasSufficientPID 6d kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientPID</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>alertmanager-main-0</td>
<td>50m (3%) 50m (3%)</td>
<td>Normal Starting 6d kubelet, m01.example.com Starting kubelet.</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>node-exporter-l7q8d</td>
<td>10m (0%) 20m (1%)</td>
<td>Normal NodeHasSufficientDisk 6d (x6 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientDisk</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>prometheus-adapter-75d769c874-hvb85</td>
<td>0 (0%)</td>
<td>Normal Starting 6d kubelet, m01.example.com Starting kubelet.</td>
</tr>
<tr>
<td>openshift-machine-config-operator</td>
<td>machine-config-daemon-cvqw9</td>
<td>20m (1%) 0 (0%)</td>
<td>Normal NodeHasSufficientDisk 6d (x6 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientDisk</td>
</tr>
<tr>
<td>openshift-marketplace</td>
<td>community-operators-f67fh</td>
<td>0 (0%)</td>
<td>Normal NodeHasSufficientPID 6d kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientPID</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>alertmanager-main-0</td>
<td>50m (3%) 50m (3%)</td>
<td>Normal Starting 6d kubelet, m01.example.com Starting kubelet.</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>node-exporter-l7q8d</td>
<td>10m (0%) 20m (1%)</td>
<td>Normal NodeHasSufficientDisk 6d (x6 over 6d) kubelet, m01.example.com Node m01.example.com status is now: NodeHasSufficientDisk</td>
</tr>
<tr>
<td>openshift-monitoring</td>
<td>prometheus-adapter-75d769c874-hvb85</td>
<td>0 (0%)</td>
<td>Normal Starting 6d kubelet, m01.example.com Starting kubelet.</td>
</tr>
</tbody>
</table>

1. The name of the node.
2. The role of the node, either master or worker.
3. The labels applied to the node.
4. The annotations applied to the node.
5. The taints applied to the node.
The node conditions and status. The conditions stanza lists the Ready, PIDPressure, MemoryPressure, DiskPressure and OutOfDisk status. These condition

The IP address and hostname of the node.

The pod resources and allocatable resources.

Information about the node host.

The pods on the node.

The events reported by the node.

Among the information shown for nodes, the following node conditions appear in the output of the commands shown in this section:

Table 5.1. Node Conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>If true, the node is healthy and ready to accept pods. If false, the node is not healthy and is not accepting pods. If unknown, the node controller has not received a heartbeat from the node for the node-monitor-grace-period (the default is 40 seconds).</td>
</tr>
<tr>
<td>DiskPressure</td>
<td>If true, the disk capacity is low.</td>
</tr>
<tr>
<td>MemoryPressure</td>
<td>If true, the node memory is low.</td>
</tr>
<tr>
<td>PIDPressure</td>
<td>If true, there are too many processes on the node.</td>
</tr>
<tr>
<td>OutOfDisk</td>
<td>If true, the node has insufficient free space on the node for adding new pods.</td>
</tr>
<tr>
<td>NetworkUnavailable</td>
<td>If true, the network for the node is not correctly configured.</td>
</tr>
<tr>
<td>NotReady</td>
<td>If true, one of the underlying components, such as the container runtime or network, is experiencing issues or is not yet configured.</td>
</tr>
<tr>
<td>SchedulingDisabled</td>
<td>Pods cannot be scheduled for placement on the node.</td>
</tr>
</tbody>
</table>

5.1.2. Listing pods on a node in your cluster

You can list all the pods on a specific node.

Procedure

- To list all or selected pods on one or more nodes:

  $ oc describe node <node1> <node2>

  For example:
To list all or selected pods on selected nodes:

$ oc describe node ip-10-0-128-218.ec2.internal

- To list all pods on a specific node, including terminated pods:

  $ oc describe node --selector=kubernetes.io/os

  Or:

  $ oc describe --selector=<node_selector>

  $ oc describe node -l node-role.kubernetes.io/worker

- To list all pods on a specific node, including terminated pods:

  $ oc get pod --all-namespaces --field-selector=spec.nodeName=<nodename>

### 5.1.3. Viewing memory and CPU usage statistics on your nodes

You can display usage statistics about nodes, which provide the runtime environments for containers. These usage statistics include CPU, memory, and storage consumption.

**Prerequisites**

- You must have **cluster-reader** permission to view the usage statistics.
- Metrics must be installed to view the usage statistics.

**Procedure**

- To view the usage statistics:

  $ oc adm top nodes

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>CPU(cores)</th>
<th>CPU%</th>
<th>MEMORY(bytes)</th>
<th>MEMORY%</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-10-0-12-143.ec2.compute.internal</td>
<td>1503m</td>
<td>100%</td>
<td>4533Mi</td>
<td>61%</td>
</tr>
<tr>
<td>ip-10-0-132-16.ec2.compute.internal</td>
<td>76m</td>
<td>5%</td>
<td>1391Mi</td>
<td>18%</td>
</tr>
<tr>
<td>ip-10-0-140-137.ec2.compute.internal</td>
<td>398m</td>
<td>26%</td>
<td>2473Mi</td>
<td>33%</td>
</tr>
<tr>
<td>ip-10-0-142-44.ec2.compute.internal</td>
<td>656m</td>
<td>43%</td>
<td>6119Mi</td>
<td>82%</td>
</tr>
<tr>
<td>ip-10-0-146-165.ec2.compute.internal</td>
<td>188m</td>
<td>12%</td>
<td>3367Mi</td>
<td>45%</td>
</tr>
<tr>
<td>ip-10-0-19-62.ec2.compute.internal</td>
<td>896m</td>
<td>59%</td>
<td>5754Mi</td>
<td>77%</td>
</tr>
<tr>
<td>ip-10-0-44-193.ec2.compute.internal</td>
<td>632m</td>
<td>42%</td>
<td>5349Mi</td>
<td>72%</td>
</tr>
</tbody>
</table>

- To view the usage statistics for nodes with labels:

  $ oc adm top node --selector=""
5.2. WORKING WITH NODES

As an administrator, you can perform a number of tasks to make your clusters more efficient.

5.2.1. Understanding how to evacuate pods on nodes

Evacuating pods allows you to migrate all or selected pods from a given node or nodes.

You can only evacuate pods backed by a replication controller. The replication controller creates new pods on other nodes and removes the existing pods from the specified node(s).

Bare pods, meaning those not backed by a replication controller, are unaffected by default. You can evacuate a subset of pods by specifying a pod-selector. Pod selectors are based on labels, so all the pods with the specified label will be evacuated.

Procedure

1. Mark the nodes unschedulable before performing the pod evacuation.
   a. Mark the node as unschedulable:
      $ oc adm cordon <node1>
      
      Example output

      node/<node1> cordoned
   b. Check that the node status is `Ready,SchedulingDisabled`:
      $ oc get node <node1>
      
      Example output

      NAME        STATUS                     ROLES     AGE       VERSION
      <node1>     Ready,SchedulingDisabled   worker    1d        v1.24.0

2. Evacuate the pods using one of the following methods:
   - Evacuate all or selected pods on one or more nodes:
     $ oc adm drain <node1> <node2> [--pod-selector=<pod_selector>]
   - Force the deletion of bare pods using the `--force` option. When set to `true`, deletion continues even if there are pods not managed by a replication controller, replica set, job, daemon set, or stateful set:
     $ oc adm drain <node1> <node2> --force=true
   - Set a period of time in seconds for each pod to terminate gracefully, use `--grace-period`. If negative, the default value specified in the pod will be used:
     $ oc adm drain <node1> <node2> --grace-period=-1
• Ignore pods managed by daemon sets using the `--ignore-daemonsets` flag set to `true`:

  $ oc adm drain <node1> <node2> --ignore-daemonsets=true

• Set the length of time to wait before giving up using the `--timeout` flag. A value of `0` sets an infinite length of time:

  $ oc adm drain <node1> <node2> --timeout=5s

• Delete pods even if there are pods using `emptyDir` volumes by setting the `--delete-emptydir-data` flag to `true`. Local data is deleted when the node is drained:

  $ oc adm drain <node1> <node2> --delete-emptydir-data=true

• List objects that will be migrated without actually performing the evacuation, using the `--dry-run` option set to `true`:

  $ oc adm drain <node1> <node2> --dry-run=true

  Instead of specifying specific node names (for example, `<node1> <node2>`), you can use the `--selector=<node_selector>` option to evacuate pods on selected nodes.

3. Mark the node as schedulable when done.

  $ oc adm uncordon <node1>

5.2.2. Understanding how to update labels on nodes

You can update any label on a node.

Node labels are not persisted after a node is deleted even if the node is backed up by a Machine.

**NOTE**

Any change to a `MachineSet` object is not applied to existing machines owned by the machine set. For example, labels edited or added to an existing `MachineSet` object are not propagated to existing machines and nodes associated with the machine set.

• The following command adds or updates labels on a node:

  $ oc label node <node> <key_1>=<value_1> ... <key_n>=<value_n>

  For example:

  $ oc label nodes webconsole-7f7f6 unhealthy=true
TIP

You can alternatively apply the following YAML to apply the label:

```yaml
kind: Node
apiVersion: v1
metadata:
  name: webconsole-7f7f6
labels:
  unhealthy: 'true'
```

- The following command updates all pods in the namespace:

  ```bash
  $ oc label pods --all <key_1>=<value_1>
  ```

  For example:

  ```bash
  $ oc label pods --all status=unhealthy
  ```

5.2.3. Understanding how to mark nodes as unschedulable or schedulable

By default, healthy nodes with a **Ready** status are marked as schedulable, which means that you can place new pods on the node. Manually marking a node as unschedulable blocks any new pods from being scheduled on the node. Existing pods on the node are not affected.

- The following command marks a node or nodes as unschedulable:

  **Example output**

  ```bash
  $ oc adm cordon <node>
  ```

  For example:

  ```bash
  $ oc adm cordon node1.example.com
  ```

  **Example output**

  ```
  node/node1.example.com cordoned
  NAME                  LABELS                                                                 STATUS
  node1.example.com     kubernetes.io/hostname=node1.example.com                      Ready,SchedulingDisabled
  ```

- The following command marks a currently unschedulable node or nodes as schedulable:

  ```bash
  $ oc adm uncordon <node1>
  ```

  Alternatively, instead of specifying specific node names (for example, `<node>`), you can use the `--selector=<node_selector>` option to mark selected nodes as schedulable or unschedulable.

5.2.4. Configuring control plane nodes as schedulable
You can configure control plane nodes to be schedulable, meaning that new pods are allowed for placement on the master nodes. By default, control plane nodes are not schedulable.

You can set the masters to be schedulable, but must retain the worker nodes.

**NOTE**

You can deploy OpenShift Container Platform with no worker nodes on a bare metal cluster. In this case, the control plane nodes are marked schedulable by default.

You can allow or disallow control plane nodes to be schedulable by configuring the `mastersSchedulable` field.

**IMPORTANT**

When you configure control plane nodes from the default unschedulable to schedulable, additional subscriptions are required. This is because control plane nodes then become worker nodes.

**Procedure**

1. Edit the ` schedulers.config.openshift.io` resource.
   ```
   $ oc edit schedulers.config.openshift.io cluster
   ```

2. Configure the `mastersSchedulable` field.

   ```yaml
   apiVersion: config.openshift.io/v1
   kind: Scheduler
   metadata:
     creationTimestamp: "2019-09-10T03:04:05Z"
     generation: 1
     name: cluster
     resourceVersion: "433"
     selfLink: /apis/config.openshift.io/v1/schedulers/cluster
     uid: a636d30a-d377-11e9-88d4-0a60097bee62
   spec:
     mastersSchedulable: false
   status: {}
   ```

   Set to **true** to allow control plane nodes to be schedulable, or **false** to disallow control plane nodes to be schedulable.

3. Save the file to apply the changes.

**5.2.5. Deleting nodes**

**5.2.5.1. Deleting nodes from a cluster**

When you delete a node using the CLI, the node object is deleted in Kubernetes, but the pods that exist on the node are not deleted. Any bare pods not backed by a replication controller become inaccessible to OpenShift Container Platform. Pods backed by replication controllers are rescheduled to other
available nodes. You must delete local manifest pods.

**Procedure**

To delete a node from the OpenShift Container Platform cluster, edit the appropriate `MachineSet` object:

**NOTE**

If you are running cluster on bare metal, you cannot delete a node by editing `MachineSet` objects. Machine sets are only available when a cluster is integrated with a cloud provider. Instead you must unschedule and drain the node before manually deleting it.

1. View the machine sets that are in the cluster:

   ```bash
   $ oc get machinesets -n openshift-machine-api
   
   The machine sets are listed in the form of <clusterid>-worker-<aws-region-az>.
   
   2. Scale the machine set:

   ```bash
   $ oc scale --replicas=2 machineset <machineset> -n openshift-machine-api
   
   Or:

   ```bash
   $ oc edit machineset <machineset> -n openshift-machine-api
   
   **TIP**

   You can alternatively apply the following YAML to scale the machine set:

   ```yaml
   apiVersion: machine.openshift.io/v1beta1
   kind: MachineSet
   metadata:
     name: <machineset>
     namespace: openshift-machine-api
   spec:
     replicas: 2
   ```

**Additional resources**

- For more information on scaling your cluster using a MachineSet, see [Manually scaling a MachineSet](#).

5.2.5.2. Deleting nodes from a bare metal cluster

When you delete a node using the CLI, the node object is deleted in Kubernetes, but the pods that exist on the node are not deleted. Any bare pods not backed by a replication controller become inaccessible to OpenShift Container Platform. Pods backed by replication controllers are rescheduled to other available nodes. You must delete local manifest pods.

**Procedure**
Delete a node from an OpenShift Container Platform cluster running on bare metal by completing the following steps:

1. Mark the node as unschedulable:
   
   ```bash
   $ oc adm cordon <node_name>
   ```

2. Drain all pods on the node:
   
   ```bash
   $ oc adm drain <node_name> --force=true
   ```

   This step might fail if the node is offline or unresponsive. Even if the node does not respond, it might still be running a workload that writes to shared storage. To avoid data corruption, power down the physical hardware before you proceed.

3. Delete the node from the cluster:
   
   ```bash
   $ oc delete node <node_name>
   ```

   Although the node object is now deleted from the cluster, it can still rejoin the cluster after reboot or if the kubelet service is restarted. To permanently delete the node and all its data, you must decommission the node.

4. If you powered down the physical hardware, turn it back on so that the node can rejoin the cluster.

5.2.6. Setting SELinux booleans

OpenShift Container Platform allows you to enable and disable an SELinux boolean on a Red Hat Enterprise Linux CoreOS (RHCOS) node. The following procedure explains how to modify SELinux booleans on nodes using the Machine Config Operator (MCO). This procedure uses `container_manage_cgroup` as the example boolean. You can modify this value to whichever boolean you need.

**Prerequisites**

- You have installed the OpenShift CLI (oc).

**Procedure**

1. Create a new YAML file with a **MachineConfig** object, displayed in the following example:

   ```yaml
   apiVersion: machineconfiguration.openshift.io/v1
   kind: MachineConfig
   metadata:
     labels:
       machineconfiguration.openshift.io/role: worker
   name: 99-worker-setsebool
   spec:
     config:
       ignition:
         version: 2.2.0
       systemd:
         units:
         - contents: |
         ```
Create the new MachineConfig object by running the following command:

```bash
$ oc create -f 99-worker-setsebool.yaml
```

**NOTE**

Applying any changes to the MachineConfig object causes all affected nodes to gracefully reboot after the change is applied.

### 5.2.7. Adding kernel arguments to nodes

In some special cases, you might want to add kernel arguments to a set of nodes in your cluster. This should only be done with caution and clear understanding of the implications of the arguments you set.

**WARNING**

Improper use of kernel arguments can result in your systems becoming unbootable.

Examples of kernel arguments you could set include:

- **enforcing=0**: Configures Security Enhanced Linux (SELinux) to run in permissive mode. In permissive mode, the system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not supported for production systems, permissive mode can be helpful for debugging.

- **nosmt**: Disables symmetric multithreading (SMT) in the kernel. Multithreading allows multiple logical threads for each CPU. You could consider **nosmt** in multi-tenant environments to reduce risks from potential cross-thread attacks. By disabling SMT, you essentially choose security over performance.

- **systemd.unified_cgroup_hierarchy**: Enables Linux control groups version 2 (cgroups v2). Cgroup v2 is the next version of the kernel control groups and offers multiple improvements.

See [Kernel.org kernel parameters](https://kernel.org) for a list and descriptions of kernel arguments.
In the following procedure, you create a **MachineConfig** object that identifies:

- A set of machines to which you want to add the kernel argument. In this case, machines with a worker role.
- Kernel arguments that are appended to the end of the existing kernel arguments.
- A label that indicates where in the list of machine configs the change is applied.

**Prerequisites**

- Have administrative privilege to a working OpenShift Container Platform cluster.

**Procedure**

1. List existing **MachineConfig** objects for your OpenShift Container Platform cluster to determine how to label your machine config:

   ```
   $ oc get MachineConfig
   ```

   **Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>GENERATEDBYCONTROLLER</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-master</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0</td>
</tr>
<tr>
<td>00-worker</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0</td>
</tr>
<tr>
<td>01-master-container-runtime</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0</td>
</tr>
<tr>
<td>01-master-kubelet</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0</td>
</tr>
<tr>
<td>01-worker-container-runtime</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0</td>
</tr>
<tr>
<td>01-worker-kubelet</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0</td>
</tr>
<tr>
<td>99-master-generated-registries</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0</td>
</tr>
<tr>
<td>99-master-ssh</td>
<td>3.2.0 40m</td>
</tr>
<tr>
<td>99-worker-generated-registries</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0</td>
</tr>
<tr>
<td>99-worker-ssh</td>
<td>3.2.0 40m</td>
</tr>
<tr>
<td>rendered-master-23e785de7587df95a4b517e0647e5ab7</td>
<td>3.2.0 33m</td>
</tr>
<tr>
<td>rendered-worker-5d596d9293ca3ea80c896a11191735bb1</td>
<td>3.2.0 33m</td>
</tr>
</tbody>
</table>

2. Create a **MachineConfig** object file that identifies the kernel argument (for example, **05-worker-kernelarg-selinuxpermissive.yaml**)

   ```yaml
   apiVersion: machineconfiguration.openshift.io/v1
   kind: MachineConfig
   metadata:
     labels:
       machineconfiguration.openshift.io/role: worker
   ```
Applies the new kernel argument only to worker nodes.

Named to identify where it fits among the machine configs (05) and what it does (adds a kernel argument to configure SELinux permissive mode).

Identifies the exact kernel argument as `enforcing=0`.

3. Create the new machine config:

```
$ oc create -f 05-worker-kernelarg-selinuxpermissive.yaml
```

4. Check the machine configs to see that the new one was added:

```
$ oc get MachineConfig
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>GENERATEDBYCONTROLLER</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGNITIONVERSION</td>
<td>AGE</td>
</tr>
<tr>
<td>00-master</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
<tr>
<td>00-worker</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
<tr>
<td>01-master-container-runtime</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
<tr>
<td>01-master-kubelet</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
<tr>
<td>01-worker-container-runtime</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
<tr>
<td>01-worker-kubelet</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
<tr>
<td>05-worker-kernelarg-selinuxpermissive</td>
<td>3.2.0</td>
</tr>
<tr>
<td>99-master-generated-registries</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
<tr>
<td>99-master-ssh</td>
<td>3.2.0</td>
</tr>
<tr>
<td>99-worker-generated-registries</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
<tr>
<td>99-worker-ssh</td>
<td>3.2.0</td>
</tr>
<tr>
<td>rendered-master-23e785de7587df95a4b517e0647e5ab7</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
<tr>
<td>rendered-worker-5d596d9293ca3ea80c896a1191735bb1</td>
<td>52dd3ba6a9a527fc3ab42afac8d12b693534c8c9</td>
</tr>
</tbody>
</table>

5. Check the nodes:
You can see that scheduling on each worker node is disabled as the change is being applied.

6. Check that the kernel argument worked by going to one of the worker nodes and listing the kernel command line arguments (in `/proc/cmdline` on the host):

```
$ oc debug node/ip-10-0-141-105.ec2.internal
```

Example output

```
Starting pod/ip-10-0-141-105ec2internal-debug ...
To use host binaries, run `chroot /host`
```

```
sh-4.2# cat /host/proc/cmdline
BOOT_IMAGE=/ostree/rhcos-... console=tty0 console=ttyS0,115200n8
rootflags=defaults,prjquota rw root=UUID=fd0... ostree=/ostree/boot.0/rhcos/16...
coreos.oem.id=qemu coreos.oem.id=ec2 ignition.platform.id=ec2 enforcing=0
```

```
sh-4.2# exit
```

You should see the `enforcing=0` argument added to the other kernel arguments.

### 5.2.8. Enabling Linux control groups version 2 (cgroups v2)

You can enable Linux control groups version 2 (cgroups v2) on specific nodes in your cluster by using a machine config. The OpenShift Container Platform process for enabling cgroups v2 disables all cgroups version 1 controllers and hierarchies.

**IMPORTANT**

The OpenShift Container Platform cgroups version 2 feature is in Developer Preview and is not supported by Red Hat at this time.

**Prerequisites**

- You have a running OpenShift Container Platform cluster that uses version 4.10 or later.
- You are logged in to the cluster as a user with administrative privileges.
- You have the `node-role.kubernetes.io` value for the node(s) you want to configure.

```
$ oc describe node <node-name>
```
Example output

Name: ci-in-v05w5m2-72292-5s9ht-worker-a-r6fpg
Roles: worker
Labels: beta.kubernetes.io/arch=amd64
        beta.kubernetes.io/instance-type=n1-standard-4
        beta.kubernetes.io/os=linux
        failure-domain.beta.kubernetes.io/region=us-central1
        failure-domain.beta.kubernetes.io/zone=us-central1-a
        kubernetes.io/arch=amd64
        kubernetes.io/hostname=ci-in-v05w5m2-72292-5s9ht-worker-a-r6fpg
        kubernetes.io/os=linux
        node-role.kubernetes.io/worker=  
#...

This value is the node role you need.

Procedure

1. Enable cgroups v2 on nodes:
   - Create a machine config file YAML, such as `worker-cgroups-v2.yaml`:

     ```yaml
     apiVersion: machineconfiguration.openshift.io/v1
     kind: MachineConfig
     metadata:
       labels:
         machineconfiguration.openshift.io/role: "worker"  
     name: worker-enable-cgroups-v2
     spec:
       kernelArguments:
         - systemd.unified_cgroup_hierarchy=1  
         - cgroup_no_v1="all"  
     ```

     1 Specifies the `node-role.kubernetes.io` value for the nodes you want to configure, such as `master`, `worker`, or `infra`.

     2 Enables cgroups v2 in systemd.

     3 Disables cgroups v1.

   - Create the new machine config:

     ```
     $ oc create -f worker-enable-cgroups-v2.yaml
     ```

2. Check the machine configs to see that the new one was added:

   ```
   $ oc get MachineConfig
   ```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>GENERATEDBYCONTROLLER</th>
</tr>
</thead>
</table>
3. Check the nodes to see that scheduling on each affected node is disabled. This indicates that the change is being applied:

$ oc get nodes

Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>ROLES</th>
<th>AGE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci-ln-fm1qnwt-72292-99kt6-master-0</td>
<td>Ready</td>
<td>master</td>
<td>58m</td>
<td>v1.24.0</td>
</tr>
<tr>
<td>ci-ln-fm1qnwt-72292-99kt6-master-1</td>
<td>Ready</td>
<td>master</td>
<td>58m</td>
<td>v1.24.0</td>
</tr>
<tr>
<td>ci-ln-fm1qnwt-72292-99kt6-master-2</td>
<td>Ready</td>
<td>master</td>
<td>58m</td>
<td>v1.24.0</td>
</tr>
<tr>
<td>ci-ln-fm1qnwt-72292-99kt6-worker-a-h5gt4</td>
<td>Ready,SchedulingDisabled</td>
<td>worker</td>
<td>48m</td>
<td>v1.24.0</td>
</tr>
<tr>
<td>ci-ln-fm1qnwt-72292-99kt6-worker-b-7vtmd</td>
<td>Ready</td>
<td>worker</td>
<td>48m</td>
<td>v1.24.0</td>
</tr>
<tr>
<td>ci-ln-fm1qnwt-72292-99kt6-worker-c-rhzkv</td>
<td>Ready</td>
<td>worker</td>
<td>48m</td>
<td>v1.24.0</td>
</tr>
</tbody>
</table>

4. After a node returns to the **Ready** state, you can verify that cgroups v2 is enabled by checking that the `sys/fs/cgroup/cgroup.controllers` file is present on the node. This file is created by cgroups v2.

- Start a debug session for that node:
  
  $ oc debug node/<node_name>

- Locate the `sys/fs/cgroup/cgroup.controllers` file. If this file is present, cgroups v2 is enabled on that node.

Example output

```
IGNITIONVERSION  AGE
00-master              52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
00-worker              52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
01-master-container-runtime  52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
01-master-kubelet       52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
01-worker-container-runtime  52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
01-worker-kubelet       52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
99-master-generated-registries  52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
99-master-ssh           3.2.0 40m
99-worker-generated-registries  52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
99-worker-ssh           3.2.0 40m
rendered-master-23e785de7587df95a4b517e0647e5ab7 52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
rendered-worker-5d596d9293ca3ea80c896a1191735bb1 52dd3ba6a9a527fc3ab42afac8d12b693534c8c9 3.2.0 33m
worker-enable-cgroups-v2        3.2.0 10s
```
5.2.9. Enabling swap memory use on nodes

IMPORTANT

Enabling swap memory use on nodes is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see https://access.redhat.com/support/offerings/techpreview/.

You can enable swap memory use for OpenShift Container Platform workloads on a per-node basis.

WARNING

Enabling swap memory can negatively impact workload performance and out-of-resource handling. Do not enable swap memory on control plane nodes.

To enable swap memory, create a `kubeletconfig` custom resource (CR) to set the `swapbehavior` parameter. You can set limited or unlimited swap memory:

- Limited: Use the `LimitedSwap` value to limit how much swap memory workloads can use. Any workloads on the node that are not managed by OpenShift Container Platform can still use swap memory. The `LimitedSwap` behavior depends on whether the node is running with Linux control groups version 1 (cgroups v1) or version 2 (cgroups v2):
  - cgroups v1: OpenShift Container Platform workloads can use any combination of memory and swap, up to the pod's memory limit, if set.
  - cgroups v2: OpenShift Container Platform workloads cannot use swap memory.

- Unlimited: Use the `UnlimitedSwap` value to allow workloads to use as much swap memory as they request, up to the system limit.

Because the kubelet will not start in the presence of swap memory without this configuration, you must
enable swap memory in OpenShift Container Platform before enabling swap memory on the nodes. If there is no swap memory present on a node, enabling swap memory in OpenShift Container Platform has no effect.

Prerequisites

- You have a running OpenShift Container Platform cluster that uses version 4.10 or later.
- You are logged in to the cluster as a user with administrative privileges.
- You have enabled the TechPreviewNoUpgrade feature set on the cluster (see Nodes → Enabling features using feature gates).

**NOTE**

Enabling the TechPreviewNoUpgrade feature set cannot be undone and prevents minor version updates. These feature sets are not recommended on production clusters.

- If cgroups v2 is enabled on a node, you must enable swap accounting on the node, by setting the swapaccount=1 kernel argument.

Procedure

1. Apply a custom label to the machine config pool where you want to allow swap memory.

   ```bash
   $ oc label machineconfigpool worker kubelet-swap=enabled
   ```

2. Create a custom resource (CR) to enable and configure swap settings.

   ```yaml
   apiVersion: machineconfiguration.openshift.io/v1
   kind: KubeletConfig
   metadata:
     name: swap-config
   spec:
     machineConfigPoolSelector:
       matchLabels:
         kubelet-swap: enabled
     kubeletConfig:
       failSwapOn: false
       memorySwap:
         swapBehavior: LimitedSwap
   ```

   **1** Set to `false` to enable swap memory use on the associated nodes. Set to `true` to disable swap memory use.

   **2** Specify the swap memory behavior. If unspecified, the default is `LimitedSwap`.

3. Enable swap memory on the machines.

5.2.10. Migrating control plane nodes from one RHOSP host to another
You can run a script that moves a control plane node from one Red Hat OpenStack Platform (RHOSP) node to another.

Prerequisites

- The environment variable `OS_CLOUD` refers to a `clouds` entry that has administrative credentials in a `clouds.yaml` file.
- The environment variable `KUBECONFIG` refers to a configuration that contains administrative OpenShift Container Platform credentials.

Procedure

- From a command line, run the following script:

```bash
#!/usr/bin/env bash
set -Eeuo pipefail
if [ $# -lt 1 ]; then
  echo "Usage: '$0 node_name'"
  exit 64
fi

# Check for admin OpenStack credentials
openstack server list --all-projects >/dev/null || { >&2
  echo "The script needs OpenStack admin credentials. Exiting";
  exit 77;
}
# Check for admin OpenShift credentials
oc adm top node >/dev/null || { >&2 echo "The script needs OpenShift admin credentials. Exiting"; exit 77; }

set -x
declare -r node_name="$1"
declare server_id
server_id="$(openstack server list --all-projects -f value -c ID -c Name | grep "$node_name" | cut -d' ' -f1)"
readonly server_id

# Drain the node
oc adm cordon "$node_name"
oc adm drain "$node_name" --delete-emptydir-data --ignore-daemonsets --force

# Power off the server
oc debug "node/${node_name}" -- chroot /host shutdown -h 1

# Verify the server is shut off
until openstack server show "$server_id" -f value -c status | grep -q 'SHUTOFF'; do sleep 5; done

# Migrate the node
openstack server migrate --wait "$server_id"

# Resize the VM
openstack server resize confirm "$server_id"
```
# Wait for the resize confirm to finish
until openstack server show "$server_id" -f value -c status | grep -q 'SHUTOFF'; do sleep 5; done

# Restart the VM
openstack server start "$server_id"

# Wait for the node to show up as Ready:
until oc get node "$node_name" | grep -q "^$node_name[[:space:]]+Ready"; do sleep 5; done

# Uncordon the node
oc adm uncordon "$node_name"

# Wait for cluster operators to stabilize
until oc get co -o go-template='statuses: {{ range .items }}{{ range .status.conditions }}{{ if eq .type "Degraded" }}DEGRADED{{ end }}{{ else if eq .type "Progressing" }}PROGRESSING{{ end }}{{ else if eq .type "Available" }}AVAILABLE{{ end }}{{ end }}| grep -q \(DEGRADED\|PROGRESSING\|AVAILABLE\)'; do sleep 5; done

If the script completes, the control plane machine is migrated to a new RHOSP node.

## 5.3. MANAGING NODES

OpenShift Container Platform uses a KubeletConfig custom resource (CR) to manage the configuration of nodes. By creating an instance of a KubeletConfig object, a managed machine config is created to override setting on the node.

### NOTE

Logging in to remote machines for the purpose of changing their configuration is not supported.

### 5.3.1. Modifying nodes

To make configuration changes to a cluster, or machine pool, you must create a custom resource definition (CRD), or kubletConfig object. OpenShift Container Platform uses the Machine Config Controller to watch for changes introduced through the CRD to apply the changes to the cluster.

### NOTE

Because the fields in a kubletConfig object are passed directly to the kubelet from upstream Kubernetes, the validation of those fields is handled directly by the kubelet itself. Please refer to the relevant Kubernetes documentation for the valid values for these fields. Invalid values in the kubletConfig object can render cluster nodes unusable.

### Procedure

1. Obtain the label associated with the static CRD, Machine Config Pool, for the type of node you want to configure. Perform one of the following steps:
   a. Check current labels of the desired machine config pool.
      For example:
Example output

```
NAME   CONFIG                                             UPDATED   UPDATING   DEGRADED
LABELS
master  rendered-master-e05b81f5ca4db1d249a1bf32f9ec24fd   True      False
False   operator.machineconfiguration.openshift.io/required-for-upgrade=
worker  rendered-worker-f50e78e1bc06d8e82327763145bf62 False
```

b. Add a custom label to the desired machine config pool.
For example:

```
$ oc label machineconfigpool worker custom-kubelet=enabled
```

2. Create a `kubeletconfig` custom resource (CR) for your configuration change.
For example:

**Sample configuration for a custom-config CR**

```yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: custom-config
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: enabled
  kubeletConfig:
    podsPerCore: 10
    maxPods: 250
    systemReserved:
      cpu: 2000m
      memory: 1Gi
```

1. Assign a name to CR.
2. Specify the label to apply the configuration change, this is the label you added to the machine config pool.
3. Specify the new value(s) you want to change.

3. Create the CR object.

```
$ oc create -f <file-name>
```
For example:

```
$ oc create -f master-kube-config.yaml
```
Most Kubelet Configuration options can be set by the user. The following options are not allowed to be overwritten:

- CgroupDriver
- ClusterDNS
- ClusterDomain
- RuntimeRequestTimeout
- StaticPodPath

## 5.4. MANAGING THE MAXIMUM NUMBER OF PODS PER NODE

In OpenShift Container Platform, you can configure the number of pods that can run on a node based on the number of processor cores on the node, a hard limit or both. If you use both options, the lower of the two limits the number of pods on a node.

Exceeding these values can result in:

- Increased CPU utilization by OpenShift Container Platform.
- Slow pod scheduling.
- Potential out-of-memory scenarios, depending on the amount of memory in the node.
- Exhausting the IP address pool.
- Resource overcommitting, leading to poor user application performance.

**NOTE**

A pod that is holding a single container actually uses two containers. The second container sets up networking prior to the actual container starting. As a result, a node running 10 pods actually has 20 containers running.

The `podsPerCore` parameter limits the number of pods the node can run based on the number of processor cores on the node. For example, if `podsPerCore` is set to 10 on a node with 4 processor cores, the maximum number of pods allowed on the node is 40.

The `maxPods` parameter limits the number of pods the node can run to a fixed value, regardless of the properties of the node.

### 5.4.1. Configuring the maximum number of pods per node

Two parameters control the maximum number of pods that can be scheduled to a node: `podsPerCore` and `maxPods`. If you use both options, the lower of the two limits the number of pods on a node.

For example, if `podsPerCore` is set to 10 on a node with 4 processor cores, the maximum number of pods allowed on the node will be 40.

**Prerequisites**
1. Obtain the label associated with the static **MachineConfigPool** CRD for the type of node you want to configure. Perform one of the following steps:

   a. View the machine config pool:

   ```
   $ oc describe machineconfigpool <name>
   
   For example:
   
   $ oc describe machineconfigpool worker
   ```

   **Example output**

   ```
   apiVersion: machineconfiguration.openshift.io/v1
   kind: MachineConfigPool
   metadata:
     creationTimestamp: 2019-02-08T14:52:39Z
     generation: 1
     labels:
       custom-kubelet: small-pods
   ```

   If a label has been added it appears under **labels**.

   b. If the label is not present, add a key/value pair:

   ```
   $ oc label machineconfigpool worker custom-kubelet=small-pods
   ```

   **TIP**

   You can alternatively apply the following YAML to add the label:

   ```
   apiVersion: machineconfiguration.openshift.io/v1
   kind: MachineConfigPool
   metadata:
     labels:
       custom-kubelet: small-pods
   name: worker
   ```

**Procedure**

1. Create a custom resource (CR) for your configuration change.

**Sample configuration for a max-pods CR**

```
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: set-max-pods
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: small-pods
```
Assign a name to CR.

Specify the label to apply the configuration change.

Specify the number of pods the node can run based on the number of processor cores on the node.

Specify the number of pods the node can run to a fixed value, regardless of the properties of the node.

**NOTE**

Setting `podsPerCore` to 0 disables this limit.

In the above example, the default value for `podsPerCore` is 10 and the default value for `maxPods` is 250. This means that unless the node has 25 cores or more, by default, `podsPerCore` will be the limiting factor.

2. List the MachineConfigPool CRDs to see if the change is applied. The **UPDATING** column reports True if the change is picked up by the Machine Config Controller:

   $ oc get machineconfigpools

   **Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>CONFIG</th>
<th>UPDATED</th>
<th>UPDATING</th>
<th>DEGRADED</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>master-9cc2c72f205e103bb534</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>worker</td>
<td>worker-8cecd1236b33ee3f8a5e</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
</tbody>
</table>

   Once the change is complete, the **UPDATED** column reports True.

   $ oc get machineconfigpools

   **Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>CONFIG</th>
<th>UPDATED</th>
<th>UPDATING</th>
<th>DEGRADED</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>master-9cc2c72f205e103bb534</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>worker</td>
<td>worker-8cecd1236b33ee3f8a5e</td>
<td>True</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>

### 5.5. USING THE NODE TUNING OPERATOR

Learn about the Node Tuning Operator and how you can use it to manage node-level tuning by orchestrating the tuned daemon.

The Node Tuning Operator helps you manage node-level tuning by orchestrating the TuneD daemon and achieves low latency performance by using the Performance Profile controller. The majority of high-performance applications require some level of kernel tuning. The Node Tuning Operator provides a
unified management interface to users of node-level sysctls and more flexibility to add custom tuning specified by user needs.

The Operator manages the containerized TuneD daemon for OpenShift Container Platform as a Kubernetes daemon set. It ensures the custom tuning specification is passed to all containerized TuneD daemons running in the cluster in the format that the daemons understand. The daemons run on all nodes in the cluster, one per node.

Node-level settings applied by the containerized TuneD daemon are rolled back on an event that triggers a profile change or when the containerized TuneD daemon is terminated gracefully by receiving and handling a termination signal.

The Node Tuning Operator uses the Performance Profile controller to implement automatic tuning to achieve low latency performance for OpenShift Container Platform applications. The cluster administrator configures a performance profile to define node-level settings such as the following:

- Updating the kernel to kernel-rt.
- Choosing CPUs for housekeeping.
- Choosing CPUs for running workloads.

The Node Tuning Operator is part of a standard OpenShift Container Platform installation in version 4.1 and later.

**NOTE**

In earlier versions of OpenShift Container Platform, the Performance Addon Operator was used to implement automatic tuning to achieve low latency performance for OpenShift applications. In OpenShift Container Platform 4.11, these functions are part of the Node Tuning Operator.

### 5.5.1. Accessing an example Node Tuning Operator specification

Use this process to access an example Node Tuning Operator specification.

**Procedure**

- Run the following command to access an example Node Tuning Operator specification:

  ```bash
  $ oc get Tuned/default -o yaml -n openshift-cluster-node-tuning-operator
  ```

The default CR is meant for delivering standard node-level tuning for the OpenShift Container Platform platform and it can only be modified to set the Operator Management state. Any other custom changes to the default CR will be overwritten by the Operator. For custom tuning, create your own Tuned CRs. Newly created CRs will be combined with the default CR and custom tuning applied to OpenShift Container Platform nodes based on node or pod labels and profile priorities.
WARNING

While in certain situations the support for pod labels can be a convenient way of automatically delivering required tuning, this practice is discouraged and strongly advised against, especially in large-scale clusters. The default Tuned CR ships without pod label matching. If a custom profile is created with pod label matching, then the functionality will be enabled at that time. The pod label functionality will be deprecated in future versions of the Node Tuning Operator.

5.5.2. Custom tuning specification

The custom resource (CR) for the Operator has two major sections. The first section, `profile`, is a list of TuneD profiles and their names. The second, `recommend`, defines the profile selection logic.

Multiple custom tuning specifications can co-exist as multiple CRs in the Operator’s namespace. The existence of new CRs or the deletion of old CRs is detected by the Operator. All existing custom tuning specifications are merged and appropriate objects for the containerized TuneD daemons are updated.

Management state

The Operator Management state is set by adjusting the default Tuned CR. By default, the Operator is in the Managed state and the `spec.managementState` field is not present in the default Tuned CR. Valid values for the Operator Management state are as follows:

- Managed: the Operator will update its operands as configuration resources are updated
- Unmanaged: the Operator will ignore changes to the configuration resources
- Removed: the Operator will remove its operands and resources the Operator provisioned

Profile data

The `profile` section lists TuneD profiles and their names.

```
profile:
- name: tuned_profile_1
  data: |
    # TuneD profile specification
    [main]
    summary=Description of tuned_profile_1 profile

    [sysctl]
    net.ipv4.ip_forward=1
    # ... other sysctl's or other TuneD daemon plugins supported by the containerized TuneD

    # ...

- name: tuned_profile_n
  data: |
    # TuneD profile specification
    [main]
```
**Recommended profiles**

The **profile**: selection logic is defined by the **recommend**: section of the CR. The **recommend**: section is a list of items to recommend the profiles based on a selection criteria.

```yaml
recommend:
  <recommend-item-1>
  # ...
  <recommend-item-n>
```

The individual items of the list:

```yaml
- machineConfigLabels:
  <mcLabels>
  match:
  <match>
  priority: <priority>
  profile: <tuned_profile_name>
  operand:
    debug: <bool>
    tunedConfig:
      reapply_sysctl: <bool>
```

1. Optional.
2. A dictionary of key/value **MachineConfig** labels. The keys must be unique.
3. If omitted, profile match is assumed unless a profile with a higher priority matches first or **machineConfigLabels** is set.
4. An optional list.
5. Profile ordering priority. Lower numbers mean higher priority (0 is the highest priority).
6. A TuneD profile to apply on a match. For example **tuned_profile_1**.
7. Optional operand configuration.
8. Turn debugging on or off for the TuneD daemon. Options are **true** for on or **false** for off. The default is **false**.
9. Turn **reapply_sysctl** functionality on or off for the TuneD daemon. Options are **true** for on and **false** for off.

**<match>** is an optional list recursively defined as follows:

```yaml
- label: <label_name>
  value: <label_value>
  type: <label_type>
```
<match> 4

1. Node or pod label name.
2. Optional node or pod label value. If omitted, the presence of `<label_name>` is enough to match.
3. Optional object type (node or pod). If omitted, node is assumed.
4. An optional `<match>` list.

If `<match>` is not omitted, all nested `<match>` sections must also evaluate to true. Otherwise, false is assumed and the profile with the respective `<match>` section will not be applied or recommended. Therefore, the nesting (child `<match>` sections) works as logical AND operator. Conversely, if any item of the `<match>` list matches, the entire `<match>` list evaluates to true. Therefore, the list acts as logical OR operator.

If `machineConfigLabels` is defined, machine config pool based matching is turned on for the given recommend: list item. `<mcLabels>` specifies the labels for a machine config. The machine config is created automatically to apply host settings, such as kernel boot parameters, for the profile `<tuned_profile_name>`. This involves finding all machine config pools with machine config selector matching `<mcLabels>` and setting the profile `<tuned_profile_name>` on all nodes that are assigned the found machine config pools. To target nodes that have both master and worker roles, you must use the master role.

The list items match and machineConfigLabels are connected by the logical OR operator. The match item is evaluated first in a short-circuit manner. Therefore, if it evaluates to true, the machineConfigLabels item is not considered.

**IMPORTANT**

When using machine config pool based matching, it is advised to group nodes with the same hardware configuration into the same machine config pool. Not following this practice might result in TuneD operands calculating conflicting kernel parameters for two or more nodes sharing the same machine config pool.

**Example: node or pod label based matching**

- match:
  - label: tuned.openshift.io/elasticsearch
    match:
      - label: node-role.kubernetes.io/master
      - label: node-role.kubernetes.io/infra
    type: pod
    priority: 10
    profile: openshift-control-plane-es
- match:
  - label: node-role.kubernetes.io/master
  - label: node-role.kubernetes.io/infra
  priority: 20
  profile: openshift-control-plane
- priority: 30
  profile: openshift-node

The CR above is translated for the containerized TuneD daemon into its `recommend.conf` file based on
the profile priorities. The profile with the highest priority (10) is openshift-control-plane-es and, therefore, it is considered first. The containerized TuneD daemon running on a given node looks to see if there is a pod running on the same node with the tuned.openshift.io/elasticsearch label set. If not, the entire <match> section evaluates as false. If there is such a pod with the label, in order for the <match> section to evaluate to true, the node label also needs to be node-role.kubernetes.io/master or node-role.kubernetes.io/infra.

If the labels for the profile with priority 10 matched, openshift-control-plane-es profile is applied and no other profile is considered. If the node/pod label combination did not match, the second highest priority profile (openshift-control-plane) is considered. This profile is applied if the containerized TuneD pod runs on a node with labels node-role.kubernetes.io/master or node-role.kubernetes.io/infra.

Finally, the profile openshift-node has the lowest priority of 30. It lacks the <match> section and, therefore, will always match. It acts as a profile catch-all to set openshift-node profile, if no other profile with higher priority matches on a given node.

Example: machine config pool based matching

```yaml
apiVersion: tuned.openshift.io/v1
kind: Tuned
metadata:
  name: openshift-node-custom
  namespace: openshift-cluster-node-tuning-operator
spec:
  profile:
  - data:
    [main]
      summary=Custom OpenShift node profile with an additional kernel parameter
```
To minimize node reboots, label the target nodes with a label the machine config pool's node selector will match, then create the Tuned CR above and finally create the custom machine config pool itself.

Cloud provider-specific TuneD profiles

With this functionality, all Cloud provider-specific nodes can conveniently be assigned a TuneD profile specifically tailored to a given Cloud provider on a OpenShift Container Platform cluster. This can be accomplished without adding additional node labels or grouping nodes into machine config pools.

This functionality takes advantage of `spec.providerID` node object values in the form of `<cloud-provider>://<cloud-provider-specific-id>` and writes the file `/var/lib/tuned/provider` with the value `<cloud-provider>` in NTO operand containers. The content of this file is then used by TuneD to load `provider-<cloud-provider>` profile if such profile exists.

The `openshift` profile that both `openshift-control-plane` and `openshift-node` profiles inherit settings from is now updated to use this functionality through the use of conditional profile loading. Neither NTO nor TuneD currently ship any Cloud provider-specific profiles. However, it is possible to create a custom profile `provider-<cloud-provider>` that will be applied to all Cloud provider-specific cluster nodes.

Example GCE Cloud provider profile

```
apiVersion: tuned.openshift.io/v1
kind: Tuned
metadata:
  name: provider-gce
namespace: openshift-cluster-node-tuning-operator
spec:
  profile:
    - data: |
      [main]
        summary=GCE Cloud provider-specific profile
        # Your tuning for GCE Cloud provider goes here.
    name: provider-gce
```

**NOTE**

Due to profile inheritance, any setting specified in the `provider-<cloud-provider>` profile will be overwritten by the `openshift` profile and its child profiles.

5.5.3. Default profiles set on a cluster

The following are the default profiles set on a cluster.

```
apiVersion: tuned.openshift.io/v1
```
Starting with OpenShift Container Platform 4.9, all OpenShift TuneD profiles are shipped with the TuneD package. You can use the `oc exec` command to view the contents of these profiles:

```
$ oc exec $tuned_pod -n openshift-cluster-node-tuning-operator -- find /usr/lib/tuned/openshift-<control-plane,-node} -name tuned.conf -exec grep -H ^ {} \;
```

### 5.5.4. Supported TuneD daemon plug-ins

Excluding the `[main]` section, the following TuneD plug-ins are supported when using custom profiles defined in the `profile` section of the Tuned CR:

- audio
- cpu
- disk
- eeepc_she
- modules
- mounts
- net
- scheduler
- scsi_host
- selinux
- sysctl
- sysfs
- usb
- video
- vm
There is some dynamic tuning functionality provided by some of these plug-ins that is not supported. The following TuneD plug-ins are currently not supported:

- script
- systemd

**WARNING**

The TuneD bootloader plug-in is currently supported on Red Hat Enterprise Linux CoreOS (RHCOS) 8.x worker nodes. For Red Hat Enterprise Linux (RHEL) 7.x worker nodes, the TuneD bootloader plug-in is currently not supported.

See [Available TuneD Plug-ins](#) and [Getting Started with TuneD](#) for more information.

### 5.6. REMEDIATING NODES WITH THE SELF NODE REMEDIATION OPERATOR

You can use the Self Node Remediation Operator to automatically reboot unhealthy nodes. This remediation strategy minimizes downtime for stateful applications and ReadWriteOnce (RWO) volumes, and restores compute capacity if transient failures occur.

#### 5.6.1. About the Self Node Remediation Operator

The Self Node Remediation Operator runs on the cluster nodes and reboots nodes that are identified as unhealthy. The Operator uses the `MachineHealthCheck` or `NodeHealthCheck` controller to detect the health of a node in the cluster. When a node is identified as unhealthy, the `MachineHealthCheck` or the `NodeHealthCheck` resource creates the `SelfNodeRemediation` custom resource (CR), which triggers the Self Node Remediation Operator.

The `SelfNodeRemediation` CR resembles the following YAML file:

```yaml
apiVersion: self-node-remediation.medik8s.io/v1alpha1
kind: SelfNodeRemediation
metadata:
  name: selfnoderemediation-sample
  namespace: openshift-operators
spec:
status:
  lastError: <last_error_message>
```

1. Displays the last error that occurred during remediation. When remediation succeeds or if no errors occur, the field is left empty.

The Self Node Remediation Operator minimizes downtime for stateful applications and restores compute capacity if transient failures occur. You can use this Operator regardless of the management interface, such as IPMI or an API to provision a node, and regardless of the cluster installation type, such
as installer-provisioned infrastructure or user-provisioned infrastructure.

5.6.1.1. Understanding the Self Node Remediation Operator configuration

The Self Node Remediation Operator creates the `SelfNodeRemediationConfig` CR with the name `self-node-remediation-config`. The CR is created in the namespace of the Self Node Remediation Operator.

A change in the `SelfNodeRemediationConfig` CR re-creates the Self Node Remediation daemon set.

The `SelfNodeRemediationConfig` CR resembles the following YAML file:

```yaml
apiVersion: self-node-remediation.medik8s.io/v1alpha1
kind: SelfNodeRemediationConfig
metadata:
  name: self-node-remediation-config
  namespace: openshift-operators
spec:
  safeTimeToAssumeNodeRebootedSeconds: 180
  watchdogFilePath: /dev/watchdog
  isSoftwareRebootEnabled: true
  apiServerTimeout: 15s
  apiCheckInterval: 5s
  maxApiErrorThreshold: 3
  peerApiServerTimeout: 5s
  peerDialTimeout: 5s
  peerRequestTimeout: 5s
  peerUpdateInterval: 15m
```

1. Specify the timeout duration for the surviving peer, after which the Operator can assume that an unhealthy node has been rebooted. The Operator automatically calculates the lower limit for this value. However, if different nodes have different watchdog timeouts, you must change this value to a higher value.

2. Specify the file path of the watchdog device in the nodes. If you enter an incorrect path to the watchdog device, the Self Node Remediation Operator automatically detects the softdog device path.

If a watchdog device is unavailable, the `SelfNodeRemediationConfig` CR uses a software reboot.

3. Specify if you want to enable software reboot of the unhealthy nodes. By default, the value of `isSoftwareRebootEnabled` is set to `true`. To disable the software reboot, set the parameter value to `false`.

4. Specify the timeout duration to check connectivity with each API server. When this duration elapses, the Operator starts remediation. The timeout duration must be more than or equal to 10 milliseconds.

5. Specify the frequency to check connectivity with each API server. The timeout duration must be more than or equal to 1 second.

6. Specify a threshold value. After reaching this threshold, the node starts contacting its peers. The threshold value must be more than or equal to 1 second.
7. Specify the duration of the timeout for the peer to connect the API server. The timeout duration must be more than or equal to 10 milliseconds.

8. Specify the duration of the timeout for establishing connection with the peer. The timeout duration must be more than or equal to 10 milliseconds.

9. Specify the duration of the timeout to get a response from the peer. The timeout duration must be more than or equal to 10 milliseconds.

10. Specify the frequency to update peer information, such as IP address. The timeout duration must be more than or equal to 10 seconds.

**NOTE**

You can edit the `self-node-remediation-config` CR that is created by the Self Node Remediation Operator. However, when you try to create a new CR for the Self Node Remediation Operator, the following message is displayed in the logs:

```
controllers.SelfNodeRemediationConfig
ignoring selfnoderemediationconfig CRs that are not named 'self-node-remediation-config'
or not in the namespace of the operator:
'openshift-operators' ("selfnoderemediationconfig":
"openshift-operators/selfnoderemediationconfig-copy")
```

5.6.1.2. Understanding the Self Node Remediation Template configuration

The Self Node Remediation Operator also creates the `SelfNodeRemediationTemplate` Custom Resource Definition (CRD). This CRD defines the remediation strategy for the nodes. The following remediation strategies are available:

**ResourceDeletion**

This remediation strategy removes the pods and associated volume attachments on the node rather than the node object. This strategy helps to recover workloads faster. **ResourceDeletion** is the default remediation strategy.

**NodeDeletion**

This remediation strategy removes the node object.

The Self Node Remediation Operator creates the following `SelfNodeRemediationTemplate` CRs for each strategy:

- `self-node-remediation-resource-deletion-template`, which the **ResourceDeletion** remediation strategy uses

- `self-node-remediation-node-deletion-template`, which the **NodeDeletion** remediation strategy uses

The `SelfNodeRemediationTemplate` CR resembles the following YAML file:

```
apiVersion: self-node-remediation.medik8s.io/v1alpha1
kind: SelfNodeRemediationTemplate
metadata:
  creationTimestamp: "2022-03-02T08:02:40Z"
```
5.6.1.3. About watchdog devices

Watchdog devices can be any of the following:

- Independently powered hardware devices
- Hardware devices that share power with the hosts they control
- Virtual devices implemented in software, or softdog

Hardware watchdog and softdog devices have electronic or software timers, respectively. These watchdog devices are used to ensure that the machine enters a safe state when an error condition is detected. The cluster is required to repeatedly reset the watchdog timer to prove that it is in a healthy state. This timer might elapse due to fault conditions, such as deadlocks, CPU starvation, and loss of network or disk access. If the timer expires, the watchdog device assumes that a fault has occurred and the device triggers a forced reset of the node.

Hardware watchdog devices are more reliable than softdog devices.

5.6.1.3.1. Understanding Self Node Remediation Operator behavior with watchdog devices

The Self Node Remediation Operator determines the remediation strategy based on the watchdog devices that are present.

If a hardware watchdog device is configured and available, the Operator uses it for remediation. If a hardware watchdog device is not configured, the Operator enables and uses a softdog device for remediation.

If neither watchdog devices are supported, either by the system or by the configuration, the Operator remediates nodes by using software reboot.

Additonal resources

Configuring a watchdog

5.6.2. Installing the Self Node Remediation Operator by using the web console

You can use the OpenShift Container Platform web console to install the Self Node Remediation Operator.

Prerequisites

```yaml
name: self-node-remediation-<remediation_object>-deletion-template
namespace: openshift-operators
spec:
template:
  spec:
    remediationStrategy: <remediation_strategy>
```

1. Specifies the type of remediation template based on the remediation strategy. Replace `<remediation_object>` with either resource or node, for example, `self-node-remediation-resource-deletion-template`.

2. Specifies the remediation strategy. The remediation strategy can either be `ResourceDeletion` or `NodeDeletion`. 
Log in as a user with `cluster-admin` privileges.

Procedure

1. In the OpenShift Container Platform web console, navigate to Operators → OperatorHub.

2. Search for the Self Node Remediation Operator from the list of available Operators, and then click Install.

3. Keep the default selection of Installation mode and namespace to ensure that the Operator is installed to the openshift-operators namespace.

4. Click Install.

Verification

To confirm that the installation is successful:

1. Navigate to the Operators → Installed Operators page.

2. Check that the Operator is installed in the openshift-operators namespace and its status is Succeeded.

If the Operator is not installed successfully:

1. Navigate to the Operators → Installed Operators page and inspect the Status column for any errors or failures.

2. Navigate to the Workloads → Pods page and check the logs in any pods in the self-node-remediation-controller-manager project that are reporting issues.

5.6.3. Installing the Self Node Remediation Operator by using the CLI

You can use the OpenShift CLI (`oc`) to install the Self Node Remediation Operator.

You can install the Self Node Remediation Operator in your own namespace or in the `openshift-operators` namespace.

To install the Operator in your own namespace, follow the steps in the procedure.

To install the Operator in the `openshift-operators` namespace, skip to step 3 of the procedure because the steps to create a new Namespace custom resource (CR) and an OperatorGroup CR are not required.

Prerequisites

- Install the OpenShift CLI (`oc`).

- Log in as a user with `cluster-admin` privileges.

Procedure

1. Create a Namespace custom resource (CR) for the Self Node Remediation Operator:

   a. Define the Namespace CR and save the YAML file, for example, `self-node-remediation-namespace.yaml`:
b. To create the **Namespace** CR, run the following command:

```
$ oc create -f self-node-remediation-namespace.yaml
```

2. Create an **OperatorGroup** CR:

a. Define the **OperatorGroup** CR and save the YAML file, for example, **self-node-remediation-operator-group.yaml**:

```yaml
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: self-node-remediation-operator
namespace: self-node-remediation
```

b. To create the **OperatorGroup** CR, run the following command:

```
$ oc create -f self-node-remediation-operator-group.yaml
```

3. Create a **Subscription** CR:

a. Define the **Subscription** CR and save the YAML file, for example, **self-node-remediation-subscription.yaml**:

```yaml
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: self-node-remediation-operator
namespace: self-node-remediation
spec:
  channel: stable
  installPlanApproval: Manual
  name: self-node-remediation-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
  package: self-node-remediation
```

Specify the **Namespace** where you want to install the Self Node Remediation Operator. To install the Self Node Remediation Operator in the **openshift-operators** namespace, specify **openshift-operators** in the **Subscription** CR.

Set the approval strategy to Manual in case your specified version is superseded by a later version in the catalog. This plan prevents an automatic upgrade to a later version and requires manual approval before the starting CSV can complete the installation.

b. To create the **Subscription** CR, run the following command:

```
$ oc create -f self-node-remediation-subscription.yaml
```
CHAPTER 5. WORKING WITH NODES

Verification

1. Verify that the installation succeeded by inspecting the CSV resource:

   ```
   $ oc get csv -n self-node-remediation
   ```

   Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>DISPLAY</th>
<th>VERSION</th>
<th>REPLACES</th>
<th>PHASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>self-node-remediation.v.0.4.0</td>
<td>Self Node Remediation Operator</td>
<td>v.0.4.0</td>
<td></td>
<td>Succeeded</td>
</tr>
</tbody>
</table>

2. Verify that the Self Node Remediation Operator is up and running:

   ```
   $ oc get deploy -n self-node-remediation
   ```

   Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>UP-TO-DATE</th>
<th>AVAILABLE</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>self-node-remediation-controller-manager</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>28h</td>
</tr>
</tbody>
</table>

3. Verify that the Self Node Remediation Operator created the `SelfNodeRemediationConfig` CR:

   ```
   $ oc get selfnoderemediationconfig -n self-node-remediation
   ```

   Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>self-node-remediation-config</td>
<td>28h</td>
</tr>
</tbody>
</table>

4. Verify that each self node remediation pod is scheduled and running on each worker node:

   ```
   $ oc get daemonset -n self-node-remediation
   ```

   Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESIRED</th>
<th>CURRENT</th>
<th>READY</th>
<th>UP-TO-DATE</th>
<th>AVAILABLE</th>
<th>NODE SELECTOR</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>self-node-remediation-ds</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>&lt;none&gt;</td>
<td>28h</td>
</tr>
</tbody>
</table>

   **NOTE**

   This command is unsupported for the control plane nodes.

5.6.4. Configuring machine health checks to use the Self Node Remediation Operator

Use the following procedure to configure the machine health checks to use the Self Node Remediation Operator as a remediation provider.

Prerequisites
- Install the OpenShift CLI (`oc`).
- Log in as a user with `cluster-admin` privileges.

**Procedure**

1. Create a **SelfNodeRemediationTemplate** CR:
   
   a. Define the **SelfNodeRemediationTemplate** CR:
      
      ```yaml
      apiVersion: self-node-remediation.medik8s.io/v1alpha1
      kind: SelfNodeRemediationTemplate
      metadata:
      namespace: openshift-machine-api
      name: selfnoderemediationtemplate-sample
      spec:
        template:
          spec:
            remediationStrategy: ResourceDeletion
      ```
      
      1. Specifies the remediation strategy. The default strategy is **ResourceDeletion**.
   
   b. To create the **SelfNodeRemediationTemplate** CR, run the following command:
      
      ```bash
      $ oc create -f <snr-name>.yaml
      ```

2. Create or update the **MachineHealthCheck** CR to point to the **SelfNodeRemediationTemplate** CR:

   a. Define or update the **MachineHealthCheck** CR:
      
      ```yaml
      apiVersion: machine.openshift.io/v1beta1
      kind: MachineHealthCheck
      metadata:
      namespace: openshift-machine-api
      name: machine-health-check
      spec:
        selector:
          matchLabels:
          - machine.openshift.io/cluster-api-machine-role: "worker"
          - machine.openshift.io/cluster-api-machine-type: "worker"
        unhealthyConditions:
        - type: "Ready"
          timeout: "300s"
          status: "False"
        - type: "Ready"
          timeout: "300s"
          status: "Unknown"
        maxUnhealthy: "40%"
        nodeStartupTimeout: "10m"
        remediationTemplate:
          kind: SelfNodeRemediationTemplate
          apiVersion: self-node-remediation.medik8s.io/v1alpha1
          name: selfnoderemediationtemplate-sample
      ```
Specifies the details for the remediation template.

b. To create a `MachineHealthCheck` CR, run the following command:

```
$ oc create -f <file-name>.yaml
```

c. To update a `MachineHealthCheck` CR, run the following command:

```
$ oc apply -f <file-name>.yaml
```

5.6.5. Troubleshooting the Self Node Remediation Operator

5.6.5.1. General troubleshooting

**Issue**
You want to troubleshoot issues with the Self Node Remediation Operator.

**Resolution**
Check the Operator logs.

5.6.5.2. Checking the daemon set

**Issue**
The Self Node Remediation Operator is installed but the daemon set is not available.

**Resolution**
Check the Operator logs for errors or warnings.

5.6.5.3. Unsuccessful remediation

**Issue**
An unhealthy node was not remediated.

**Resolution**
Verify that the `SelfNodeRemediation` CR was created by running the following command:

```
$ oc get snr -A
```

If the `MachineHealthCheck` controller did not create the `SelfNodeRemediation` CR when the node turned unhealthy, check the logs of the `MachineHealthCheck` controller. Additionally, ensure that the `MachineHealthCheck` CR includes the required specification to use the remediation template.

If the `SelfNodeRemediation` CR was created, ensure that its name matches the unhealthy node or the machine object.

5.6.5.4. Daemon set and other Self Node Remediation Operator resources exist even after uninstalling the Operator

**Issue**
The Self Node Remediation Operator resources, such as the daemon set, configuration CR, and the remediation template CR, exist even after after uninstalling the Operator.
Resolution

To remove the Self Node Remediation Operator resources, delete the resources by running the following commands for each resource type:

```bash
$ oc delete ds <self-node-remediation-ds> -n <namespace>
$ oc delete snrc <self-node-remediation-config> -n <namespace>
$ oc delete snrt <self-node-remediation-template> -n <namespace>
```

5.6.6. Gathering data about the Self Node Remediation Operator

To collect debugging information about the Self Node Remediation Operator, use the `must-gather` tool. For information about the `must-gather` image for the Self Node Remediation Operator, see Gathering data about specific features.

5.6.7. Additional resources

- The Self Node Remediation Operator is supported in a restricted network environment. For more information, see Using Operator Lifecycle Manager on restricted networks.
- Deleting Operators from a cluster

5.7. DEPLOYING NODE HEALTH CHECKS BY USING THE NODE HEALTH CHECK OPERATOR

Use the Node Health Check Operator to identify unhealthy nodes. The Operator uses the Self Node Remediation Operator to remediate the unhealthy nodes.

Additional resources

Remediating nodes with the Self Node Remediation Operator

5.7.1. About the Node Health Check Operator

The Node Health Check Operator detects the health of the nodes in a cluster. The `NodeHealthCheck` controller creates the `NodeHealthCheck` custom resource (CR), which defines a set of criteria and thresholds to determine the health of a node.

The Node Health Check Operator also installs the Self Node Remediation Operator as a default remediation provider.

When the Node Health Check Operator detects an unhealthy node, it creates a remediation CR that triggers the remediation provider. For example, the controller creates the `SelfNodeRemediation` CR, which triggers the Self Node Remediation Operator to remediate the unhealthy node.

The `NodeHealthCheck` CR resembles the following YAML file:

```yaml
apiVersion: remediation.medik8s.io/v1alpha1
kind: NodeHealthCheck
metadata:
```
Specifies the amount of healthy nodes (in percentage or number) required for a remediation provider to concurrently remediate nodes in the targeted pool. If the number of healthy nodes equals to or exceeds the limit set by `minHealthy`, remediation occurs. The default value is 51%.

Prevents any new remediation from starting, while allowing any ongoing remediations to persist. The default value is empty. However, you can enter an array of strings that identify the cause of pausing the remediation. For example, `pause-test-cluster`.

**NOTE**

During the upgrade process, nodes in the cluster might become temporarily unavailable and get identified as unhealthy. In the case of worker nodes, when the Operator detects that the cluster is upgrading, it stops remediating new unhealthy nodes to prevent such nodes from rebooting.

Specifies a remediation template from the remediation provider. For example, from the Self Node Remediation Operator.

Specifies a selector that matches labels or expressions that you want to check. The default value is empty, which selects all nodes.

Specifies a list of the conditions that determine whether a node is considered unhealthy.

Specifies the timeout duration for a node condition. If a condition is met for the duration of the timeout, the node will be remediated. Long timeouts can result in long periods of downtime for a workload on an unhealthy node.

### 5.7.1.1. Understanding the Node Health Check Operator workflow

When a node is identified as unhealthy, the Node Health Check Operator checks how many other nodes...
are unhealthy. If the number of healthy nodes exceeds the amount that is specified in the `minHealthy` field of the `NodeHealthCheck` CR, the controller creates a remediation CR from the details that are provided in the external remediation template by the remediation provider. After remediation, the kubelet updates the node’s health status.

When the node turns healthy, the controller deletes the external remediation template.

5.7.1.2. About how node health checks prevent conflicts with machine health checks

When both, node health checks and machine health checks are deployed, the node health check avoids conflict with the machine health check.

**NOTE**

OpenShift Container Platform deploys `machine-api-termination-handler` as the default `MachineHealthCheck` resource.

The following list summarizes the system behavior when node health checks and machine health checks are deployed:

- If only the default machine health check exists, the node health check continues to identify unhealthy nodes. However, the node health check ignores unhealthy nodes in a Terminating state. The default machine health check handles the unhealthy nodes with a Terminating state.

**Example log message**

```
INFO MHCChecker ignoring unhealthy Node, it is terminating and will be handled by MHC
("NodeName": "node-1.example.com")
```

- If the default machine health check is modified (for example, the `unhealthyConditions` is `Ready`), or if additional machine health checks are created, the node health check is disabled.

**Example log message**

```
INFO controllers.NodeHealthCheck disabling NHC in order to avoid conflict with custom
MHCs configured in the cluster ("NodeHealthCheck": "/nhc-worker-default")
```

- When, again, only the default machine health check exists, the node health check is re-enabled.

**Example log message**

```
INFO controllers.NodeHealthCheck re-enabling NHC, no conflicting MHC configured in the
cluster ("NodeHealthCheck": "/nhc-worker-default")
```

5.7.2. Installing the Node Health Check Operator by using the web console

You can use the OpenShift Container Platform web console to install the Node Health Check Operator.

**Prerequisites**

- Log in as a user with `cluster-admin` privileges.
Procedure

1. In the OpenShift Container Platform web console, navigate to **Operators → OperatorHub**.

2. Search for the Node Health Check Operator, then click **Install**.

3. Keep the default selection of **Installation mode** and **namespace** to ensure that the Operator will be installed to the **openshift-operators** namespace.

4. Click **Install**.

Verification

To confirm that the installation is successful:

1. Navigate to the **Operators → Installed Operators** page.

2. Check that the Operator is installed in the **openshift-operators** namespace and that its status is **Succeeded**.

If the Operator is not installed successfully:

1. Navigate to the **Operators → Installed Operators** page and inspect the **Status** column for any errors or failures.

2. Navigate to the **Workloads → Pods** page and check the logs in any pods in the **openshift-operators** project that are reporting issues.

5.7.3. Installing the Node Health Check Operator by using the CLI

You can use the OpenShift CLI (**oc**) to install the Node Health Check Operator.

To install the Operator in your own namespace, follow the steps in the procedure.

To install the Operator in the **openshift-operators** namespace, skip to step 3 of the procedure because the steps to create a new **Namespace** custom resource (CR) and an **OperatorGroup** CR are not required.

Prerequisites

- Install the OpenShift CLI (**oc**).
- Log in as a user with **cluster-admin** privileges.

Procedure

1. Create a **Namespace** custom resource (CR) for the Node Health Check Operator:
   
   a. Define the **Namespace** CR and save the YAML file, for example, **node-health-check-namespaced.yaml**:

   ```yaml
   apiVersion: v1
   kind: Namespace
   metadata:
     name: node-health-check
   
   b. To create the **Namespace** CR, run the following command:
$ oc create -f node-health-check-namespaces.yaml

2. Create an **OperatorGroup** CR:
   
a. Define the **OperatorGroup** CR and save the YAML file, for example, *node-health-check-operator-group.yaml*:

   ```yaml
   apiVersion: operators.coreos.com/v1
   kind: OperatorGroup
   metadata:
     name: node-health-check-operator
     namespace: node-health-check
   
   b. To create the **OperatorGroup** CR, run the following command:

   ```bash
   $ oc create -f node-health-check-operator-group.yaml
   ```

3. Create a **Subscription** CR:
   
a. Define the **Subscription** CR and save the YAML file, for example, *node-health-check-subscription.yaml*:

   ```yaml
   apiVersion: operators.coreos.com/v1alpha1
   kind: Subscription
   metadata:
     name: node-health-check-operator
     namespace: node-health-check
   spec:
     channel: candidate
     installPlanApproval: Manual
     name: node-healthcheck-operator
     source: redhat-operators
     sourceNamespace: openshift-marketplace
     package: node-healthcheck-operator
   
   1 Specify the **Namespace** where you want to install the Node Health Check Operator. To install the Node Health Check Operator in the **openshift-operators** namespace, specify **openshift-operators** in the **Subscription** CR.
   
   2 Specify the channel name for your subscription. To upgrade to the latest version of the Node Health Check Operator, you must manually change the channel name for your subscription from **alpha** to **candidate**.
   
   3 Set the approval strategy to Manual in case your specified version is superseded by a later version in the catalog. This plan prevents an automatic upgrade to a later version and requires manual approval before the starting CSV can complete the installation.

   b. To create the **Subscription** CR, run the following command:

   ```bash
   $ oc create -f node-health-check-subscription.yaml
   ```

**Verification**
1. Verify that the installation succeeded by inspecting the CSV resource:

   ```bash
   $ oc get csv -n openshift-operators
   ``

   **Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>DISPLAY</th>
<th>VERSION</th>
<th>REPLACES</th>
<th>PHASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-healthcheck-operator.v0.2.0. Node Health Check Operator</td>
<td>0.2.0</td>
<td>Succeeded</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Verify that the Node Health Check Operator is up and running:

   ```bash
   $ oc get deploy -n openshift-operators
   ``

   **Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>UP-TO-DATE</th>
<th>AVAILABLE</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-health-check-operator-controller-manager</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>10d</td>
</tr>
</tbody>
</table>

5.7.4. Gathering data about the Node Health Check Operator

To collect debugging information about the Node Health Check Operator, use the `must-gather` tool. For information about the `must-gather` image for the Node Health Check Operator, see Gathering data about specific features.

5.7.5. Additional resources

- Changing the update channel for an Operator
- The Node Health Check Operator is supported in a restricted network environment. For more information, see Using Operator Lifecycle Manager on restricted networks.

5.8. USING THE NODE MAINTENANCE OPERATOR TO PLACE NODES IN MAINTENANCE MODE

You can use the Node Maintenance Operator to place nodes in maintenance mode by using the `oc adm` utility or `NodeMaintenance` custom resources (CRs).

5.8.1. About the Node Maintenance Operator

The Node Maintenance Operator watches for new or deleted `NodeMaintenance` CRs. When a new `NodeMaintenance` CR is detected, no new workloads are scheduled and the node is cordoned off from the rest of the cluster. All pods that can be evicted are evicted from the node. When a `NodeMaintenance` CR is deleted, the node that is referenced in the CR is made available for new workloads.

**NOTE**

Using a `NodeMaintenance` CR for node maintenance tasks achieves the same results as the `oc adm cordon` and `oc adm drain` commands using standard OpenShift Container Platform CR processing.
5.8.2. Installing the Node Maintenance Operator

You can install the Node Maintenance Operator using the web console or the OpenShift CLI (`oc`).

**NOTE**

If OpenShift Virtualization version 4.10 or less is installed in your cluster, it includes an outdated version of the Node Maintenance Operator version.

5.8.2.1. Installing the Node Maintenance Operator by using the web console

You can use the OpenShift Container Platform web console to install the Node Maintenance Operator.

**Prerequisites**

- Log in as a user with `cluster-admin` privileges.

**Procedure**

1. In the OpenShift Container Platform web console, navigate to Operators → OperatorHub.

2. Search for the Node Maintenance Operator, then click Install.

3. Keep the default selection of **Installation mode** and **namespace** to ensure that the Operator will be installed to the `openshift-operators` namespace.

4. Click Install.

**Verification**

To confirm that the installation is successful:

1. Navigate to the Operators → Installed Operators page.

2. Check that the Operator is installed in the `openshift-operators` namespace and that its status is Succeeded.

If the Operator is not installed successfully:

1. Navigate to the Operators → Installed Operators page and inspect the Status column for any errors or failures.

2. Navigate to the Operators → Installed Operators → Node Maintenance Operator → Details page, and inspect the Conditions section for errors before pod creation.

3. Navigate to the Workloads → Pods page, search for the Node Maintenance Operator pod in the installed namespace, and check the logs in the Logs tab.

5.8.2.2. Installing the Node Maintenance Operator by using the CLI

You can use the OpenShift CLI (`oc`) to install the Node Maintenance Operator.

You can install the Node Maintenance Operator in your own namespace or in the `openshift-operators` namespace.

To install the Operator in your own namespace, follow the steps in the procedure.
To install the Operator in the `openshift-operators` namespace, skip to step 3 of the procedure because the steps to create a new `Namespace` custom resource (CR) and an `OperatorGroup` CR are not required.

**Prerequisites**

- Install the OpenShift CLI (`oc`).
- Log in as a user with `cluster-admin` privileges.

**Procedure**

1. Create a `Namespace` CR for the Node Maintenance Operator:
   
   a. Define the `Namespace` CR and save the YAML file, for example, `node-maintenance-namespace.yaml`:

   ```yaml
   apiVersion: v1
   kind: Namespace
   metadata:
     name: nmo-test
   ```

   b. To create the `Namespace` CR, run the following command:

   ```sh
   $ oc create -f node-maintenance-namespace.yaml
   ```

2. Create an `OperatorGroup` CR:
   
   a. Define the `OperatorGroup` CR and save the YAML file, for example, `node-maintenance-operator-group.yaml`:

   ```yaml
   apiVersion: operators.coreos.com/v1
   kind: OperatorGroup
   metadata:
     name: node-maintenance-operator
     namespace: nmo-test
   ```

   b. To create the `OperatorGroup` CR, run the following command:

   ```sh
   $ oc create -f node-maintenance-operator-group.yaml
   ```

3. Create a `Subscription` CR:
   
   a. Define the `Subscription` CR and save the YAML file, for example, `node-maintenance-subscription.yaml`:

   ```yaml
   apiVersion: operators.coreos.com/v1alpha1
   kind: Subscription
   metadata:
     name: node-maintenance-operator
     namespace: nmo-test
   spec:
     channel: stable
     InstallPlaneApproval: Automatic
   ```
Specify the **Namespace** where you want to install the Node Maintenance Operator.

### IMPORTANT

To install the Node Maintenance Operator in the `openshift-operators` namespace, specify `openshift-operators` in the `Subscription` CR.

b. To create the `Subscription` CR, run the following command:

```bash
$ oc create -f node-maintenance-subscription.yaml
```

#### Verification

1. Verify that the installation succeeded by inspecting the CSV resource:

```bash
$ oc get csv -n openshift-operators
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>DISPLAY</th>
<th>VERSION</th>
<th>REPLACES</th>
<th>PHASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-maintenance-operator.v4.11</td>
<td>Node Maintenance Operator</td>
<td>4.11</td>
<td></td>
<td>Succeeded</td>
</tr>
</tbody>
</table>

2. Verify that the Node Maintenance Operator is running:

```bash
$ oc get deploy -n openshift-operators
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>UP-TO-DATE</th>
<th>AVAILABLE</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-maintenance-operator-controller-manager</td>
<td>1/1</td>
<td>1</td>
<td>1</td>
<td>10d</td>
</tr>
</tbody>
</table>

The Node Maintenance Operator is supported in a restricted network environment. For more information, see [Using Operator Lifecycle Manager on restricted networks](#).

### 5.8.3. Setting a node to maintenance mode

You can place a node into maintenance mode from the web console or from the CLI by using a `NodeMaintenance` CR.

#### 5.8.3.1. Setting a node to maintenance mode by using the web console

To set a node to maintenance mode, you can create a `NodeMaintenance` custom resource (CR) by using the web console.

**Prerequisites**
• Log in as a user with `cluster-admin` privileges.

• Install the Node Maintenance Operator from the OperatorHub.

**Procedure**

1. From the Administrator perspective in the web console, navigate to Operators → Installed Operators.

2. Select the Node Maintenance Operator from the list of Operators.

3. In the Node Maintenance tab, click Create NodeMaintenance.

4. In the Create NodeMaintenance page, select the Form view or the YAML view to configure the NodeMaintenance CR.

5. To apply the NodeMaintenance CR that you have configured, click Create.

**Verification**

In the Node Maintenance tab, inspect the Status column and verify that its status is Succeeded.

5.8.3.2. Setting a node to maintenance mode by using the CLI

You can put a node into maintenance mode with a NodeMaintenance custom resource (CR). When you apply a NodeMaintenance CR, all allowed pods are evicted and the node is rendered unschedulable. Evicted pods are queued to be moved to another node in the cluster.

**Prerequisites**

• Install the OpenShift Container Platform CLI `oc`.

• Log in to the cluster as a user with `cluster-admin` privileges.

**Procedure**

1. Create the following NodeMaintenance CR, and save the file as `nodemaintenance-cr.yaml`:

   ```yaml
   apiVersion: nodemaintenance.medik8s.io/v1beta1
   kind: NodeMaintenance
   metadata:
     name: nodemaintenance-cr
   spec:
     nodeName: node-1.example.com
     reason: "NIC replacement"
   ```

   1. The name of the node maintenance CR.
   2. The name of the node to be put into maintenance mode.
   3. A plain text description of the reason for maintenance.

2. Apply the node maintenance CR by running the following command:
Verification

1. Check the progress of the maintenance task by running the following command:

   ```shell
   $ oc describe node <node-name>
   ```

   where `<node-name>` is the name of your node; for example, `node-1.example.com`

2. Check the example output:

   ```plaintext
   Events:
   Type     Reason                     Age                   From     Message
   ----     ------                     ----                  ----     -------
   Normal   NodeNotSchedulable         61m                   kubelet  Node node-1.example.com status is now: NodeNotSchedulable
   ```

5.8.3.3. Checking status of current NodeMaintenance CR tasks

You can check the status of current `NodeMaintenance` CR tasks.

Prerequisites

- Install the OpenShift Container Platform CLI `oc`.
- Log in as a user with `cluster-admin` privileges.

Procedure

- Check the status of current node maintenance tasks, for example the `NodeMaintenance` CR or `nm` object, by running the following command:

  ```shell
  $ oc get nm -o yaml
  ```

Example output

```json
apiVersion: v1
items:
- apiVersion: nodemaintenance.medik8s.io/v1beta1
  kind: NodeMaintenance
  metadata:
  ...
  spec:
    nodeName: node-1.example.com
    reason: Node maintenance
    status:
      drainProgress: 100
      evictionPods: 3
      lastError: "Last failure message"
      lastUpdate: "2022-06-23T11:43:18Z"
```
The percentage completion of draining the node.

2. The number of pods scheduled for eviction.

3. The latest eviction error, if any.

4. The last time the status was updated.

5. The total number of pods before the node entered maintenance mode.

5.8.4. Resuming a node from maintenance mode

You can resume a node from maintenance mode from the web console or from the CLI by using a `NodeMaintenance` CR. Resuming a node brings it out of maintenance mode and makes it schedulable again.

5.8.4.1. Resuming a node from maintenance mode by using the web console

To resume a node from maintenance mode, you can delete a `NodeMaintenance` custom resource (CR) by using the web console.

**Prerequisites**

- Log in as a user with `cluster-admin` privileges.
- Install the Node Maintenance Operator from the OperatorHub.

**Procedure**

1. From the Administrator perspective in the web console, navigate to `Operators → Installed Operators`.

2. Select the Node Maintenance Operator from the list of Operators.

3. In the `Node Maintenance` tab, select the `NodeMaintenance` CR that you want to delete.

4. Click the Options menu at the end of the node and select `Delete NodeMaintenance`.

**Verification**

1. In the OpenShift Container Platform console, click `Compute → Nodes`.

2. Inspect the `Status` column of the node for which you deleted the `NodeMaintenance` CR and verify that its status is `Ready`.

5.8.4.2. Resuming a node from maintenance mode by using the CLI
You can resume a node from maintenance mode that was initiated with a `NodeMaintenance` CR by deleting the `NodeMaintenance` CR.

**Prerequisites**

- Install the OpenShift Container Platform CLI `oc`.
- Log in to the cluster as a user with `cluster-admin` privileges.

**Procedure**

- When your node maintenance task is complete, delete the active `NodeMaintenance` CR:
  
  ```
  $ oc delete -f nodemaintenance-cr.yaml
  ```

**Example output**

```
nodemaintenance.nodemaintenance.medik8s.io "maintenance-example" deleted
```

**Verification**

1. Check the progress of the maintenance task by running the following command:

   ```
   $ oc describe node <node-name>
   ```

   where `<node-name>` is the name of your node; for example, `node-1.example.com`

2. Check the example output:

   ```
   Events:
   Type     Reason                  Age                   From     Message
   ----     ------                  ----                  ----     -------
   Normal   NodeSchedulable         2m                    kubelet  Node node-1.example.com status is now: NodeSchedulable
   ```

**5.8.5. Working with bare-metal nodes**

For clusters with bare-metal nodes, you can place a node into maintenance mode, and resume a node from maintenance mode, by using the web console `Actions` control.

**NOTE**

Clusters with bare-metal nodes can also place a node into maintenance mode, and resume a node from maintenance mode, by using the web console and CLI, as outlined. These methods, by using the web console `Actions` control, are applicable to bare-metal clusters only.

**5.8.5.1. Maintaining bare-metal nodes**

When you deploy OpenShift Container Platform on bare-metal infrastructure, you must take additional considerations into account compared to deploying on cloud infrastructure. Unlike in cloud environments, where the cluster nodes are considered ephemeral, reprovisioning a bare-metal node requires significantly more time and effort for maintenance tasks.
When a bare-metal node fails due to a kernel error or a NIC card hardware failure, workloads on the failed node need to be restarted on another node in the cluster while the problem node is repaired or replaced. Node maintenance mode allows cluster administrators to gracefully turn-off nodes, move workloads to other parts of the cluster, and ensure that workloads do not get interrupted. Detailed progress and node status details are provided during maintenance.

5.8.5.2. Setting a bare-metal node to maintenance mode

Set a bare-metal node to maintenance mode using the Options menu found on each node in the Compute → Nodes list, or using the Actions control of the Node Details screen.

Procedure

1. From the Administrator perspective of the web console, click Compute → Nodes.

2. You can set the node to maintenance from this screen, which makes it easier to perform actions on multiple nodes, or from the Node Details screen, where you can view comprehensive details of the selected node:

   • Click the Options menu at the end of the node and select Start Maintenance.
   • Click the node name to open the Node Details screen and click Actions → Start Maintenance.

3. Click Start Maintenance in the confirmation window.

The node is no longer schedulable. If it had virtual machines with the LiveMigration eviction strategy, then it will live migrate them. All other pods and virtual machines on the node are deleted and recreated on another node.

Verification

• Navigate to the Compute → Nodes page and verify that the corresponding node has a status of Under maintenance.

5.8.5.3. Resuming a bare-metal node from maintenance mode

Resume a bare-metal node from maintenance mode using the Options menu found on each node in the Compute → Nodes list, or using the Actions control of the Node Details screen.

Procedure

1. From the Administrator perspective of the web console, click Compute → Nodes.

2. You can resume the node from this screen, which makes it easier to perform actions on multiple nodes, or from the Node Details screen, where you can view comprehensive details of the selected node:

   • Click the Options menu at the end of the node and select Stop Maintenance.
3. Click the node name to open the Node Details screen and click Actions → Stop Maintenance.

The node becomes schedulable. If it had virtual machine instances that were running on the node prior to maintenance, then they will not automatically migrate back to this node.

Verification

- Navigate to the Compute → Nodes page and verify that the corresponding node has a status of Ready.

5.8.6. Gathering data about the Node Maintenance Operator

To collect debugging information about the Node Maintenance Operator, use the must-gather tool. For information about the must-gather image for the Node Maintenance Operator, see Gathering data about specific features.

5.8.7. Additional resources

- Gathering data about your cluster
- Understanding how to evacuate pods on nodes
- Understanding how to mark nodes as unschedulable or schedulable

5.9. UNDERSTANDING NODE REBOOTING

To reboot a node without causing an outage for applications running on the platform, it is important to first evacuate the pods. For pods that are made highly available by the routing tier, nothing else needs to be done. For other pods needing storage, typically databases, it is critical to ensure that they can remain in operation with one pod temporarily going offline. While implementing resiliency for stateful pods is different for each application, in all cases it is important to configure the scheduler to use node anti-affinity to ensure that the pods are properly spread across available nodes.

Another challenge is how to handle nodes that are running critical infrastructure such as the router or the registry. The same node evacuation process applies, though it is important to understand certain edge cases.

5.9.1. About rebooting nodes running critical infrastructure

When rebooting nodes that host critical OpenShift Container Platform infrastructure components, such as router pods, registry pods, and monitoring pods, ensure that there are at least three nodes available to run these components.

The following scenario demonstrates how service interruptions can occur with applications running on OpenShift Container Platform when only two nodes are available:

- Node A is marked unschedulable and all pods are evacuated.
- The registry pod running on that node is now redeployed on node B. Node B is now running both registry pods.
- Node B is now marked unschedulable and is evacuated.
The service exposing the two pod endpoints on node B loses all endpoints, for a brief period of time, until they are redeployed to node A.

When using three nodes for infrastructure components, this process does not result in a service disruption. However, due to pod scheduling, the last node that is evacuated and brought back into rotation does not have a registry pod. One of the other nodes has two registry pods. To schedule the third registry pod on the last node, use pod anti-affinity to prevent the scheduler from locating two registry pods on the same node.

Additional information

- For more information on pod anti-affinity, see Placing pods relative to other pods using affinity and anti-affinity rules.

5.9.2. Rebooting a node using pod anti-affinity

Pod anti-affinity is slightly different than node anti-affinity. Node anti-affinity can be violated if there are no other suitable locations to deploy a pod. Pod anti-affinity can be set to either required or preferred.

With this in place, if only two infrastructure nodes are available and one is rebooted, the container image registry pod is prevented from running on the other node. `oc get pods` reports the pod as unready until a suitable node is available. Once a node is available and all pods are back in ready state, the next node can be restarted.

Procedure

To reboot a node using pod anti-affinity:

1. Edit the node specification to configure pod anti-affinity:

```yaml
apiVersion: v1
defspec:

spec:
  .....
```

   1. Stanza to configure pod anti-affinity.
   2. Defines a preferred rule.
   3. Specifies a weight for a preferred rule. The node with the highest weight is preferred.
Description of the pod label that determines when the anti-affinity rule applies. Specify a key and value for the label.

The operator represents the relationship between the label on the existing pod and the set of values in the `matchExpression` parameters in the specification for the new pod. Can be `In`, `NotIn`, `Exists`, or `DoesNotExist`.

This example assumes the container image registry pod has a label of `registry=default`. Pod anti-affinity can use any Kubernetes match expression.

2. Enable the `MatchInterPodAffinity` scheduler predicate in the scheduling policy file.

3. Perform a graceful restart of the node.

5.9.3. Understanding how to reboot nodes running routers

In most cases, a pod running an OpenShift Container Platform router exposes a host port.

The `PodFitsPorts` scheduler predicate ensures that no router pods using the same port can run on the same node, and pod anti-affinity is achieved. If the routers are relying on IP failover for high availability, there is nothing else that is needed.

For router pods relying on an external service such as AWS Elastic Load Balancing for high availability, it is that service's responsibility to react to router pod restarts.

In rare cases, a router pod may not have a host port configured. In those cases, it is important to follow the recommended restart process for infrastructure nodes.

5.9.4. Rebooting a node gracefully

Before rebooting a node, it is recommended to backup etcd data to avoid any data loss on the node.

**NOTE**

For single-node OpenShift clusters that require users to perform the `oc login` command rather than having the certificates in `kubeconfig` file to manage the cluster, the `oc adm` commands might not be available after cordon and draining the node. This is because the `openshift-oauth-apiserver` pod is not running due to the cordon. You can use SSH to access the nodes as indicated in the following procedure.

In a single-node OpenShift cluster, pods cannot be rescheduled when cordon and draining. However, doing so gives the pods, especially your workload pods, time to properly stop and release associated resources.

**Procedure**

To perform a graceful restart of a node:

1. Mark the node as unschedulable:

   ```
   $ oc adm cordon <node1>
   ```

2. Drain the node to remove all the running pods:
You might receive errors that pods associated with custom pod disruption budgets (PDB) cannot be evicted.

Example error

```
error when evicting "rails-postgresql-example-1-72v2w" -n "rails" (will retry after 5s):
Cannot evict pod as it would violate the pod's disruption budget.
```

In this case, run the drain command again, adding the `disable-eviction` flag, which bypasses the PDB checks:

```
$ oc adm drain <node1> --ignore-daemonsets --delete-emptydir-data --force --disable-eviction
```

3. Access the node in debug mode:

```
$ oc debug node/<node1>
```

4. Change your root directory to the host:

```
$ chroot /host
```

5. Restart the node:

```
$ systemctl reboot
```

In a moment, the node enters the `NotReady` state.

**NOTE**

With some single-node OpenShift clusters, the `oc` commands might not be available after you cordon and drain the node because the `openshift-oauth-apiserver` pod is not running. You can use SSH to connect to the node and perform the reboot.

```
$ ssh core@<master-node>.<cluster_name>.<base_domain>
```

```
$ sudo systemctl reboot
```

6. After the reboot is complete, mark the node as schedulable by running the following command:

```
$ oc adm uncordon <node1>
```
NOTE

With some single-node OpenShift clusters, the `oc` commands might not be available after you cordon and drain the node because the `openshift-oauth-apiserver` pod is not running. You can use SSH to connect to the node and uncordon it.

```
$ ssh core@<target_node>

$ sudo oc adm uncordon <node> --kubeconfig /etc/kubernetes/static-pod-resources/kube-apiserver-certs/secrets/node-kubeconfigs/localhost.kubeconfig
```

7. Verify that the node is ready:

```
$ oc get node <node1>
```

Example output

```
NAME    STATUS  ROLES    AGE     VERSION
<node1>  Ready   worker   6d22h   v1.18.3+b0068a8
```

Additional information

For information on etcd data backup, see Backing up etcd data.

5.10. FREEING NODE RESOURCES USING GARBAGE COLLECTION

As an administrator, you can use OpenShift Container Platform to ensure that your nodes are running efficiently by freeing up resources through garbage collection.

The OpenShift Container Platform node performs two types of garbage collection:

- Container garbage collection: Removes terminated containers.
- Image garbage collection: Removes images not referenced by any running pods.

5.10.1. Understanding how terminated containers are removed through garbage collection

Container garbage collection can be performed using eviction thresholds.

When eviction thresholds are set for garbage collection, the node tries to keep any container for any pod accessible from the API. If the pod has been deleted, the containers will be as well. Containers are preserved as long the pod is not deleted and the eviction threshold is not reached. If the node is under disk pressure, it will remove containers and their logs will no longer be accessible using `oc logs`.

- `eviction-soft` - A soft eviction threshold pairs an eviction threshold with a required administrator-specified grace period.
- `eviction-hard` - A hard eviction threshold has no grace period, and if observed, OpenShift Container Platform takes immediate action.
The following table lists the eviction thresholds:

Table 5.2. Variables for configuring container garbage collection

<table>
<thead>
<tr>
<th>Node condition</th>
<th>Eviction signal</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MemoryPressure</td>
<td>memory.available</td>
<td>The available memory on the node.</td>
</tr>
<tr>
<td>DiskPressure</td>
<td>nodefs.available, nodefs.inodesFree, imagefs.available, imagefs.inodesFree</td>
<td>The available disk space or inodes on the node root file system, nodefs, or image file system, imagefs.</td>
</tr>
</tbody>
</table>

NOTE

For **evictionHard** you must specify all of these parameters. If you do not specify all parameters, only the specified parameters are applied and the garbage collection will not function properly.

If a node is oscillating above and below a soft eviction threshold, but not exceeding its associated grace period, the corresponding node would constantly oscillate between true and false. As a consequence, the scheduler could make poor scheduling decisions.

To protect against this oscillation, use the **eviction-pressure-transition-period** flag to control how long OpenShift Container Platform must wait before transitioning out of a pressure condition. OpenShift Container Platform will not set an eviction threshold as being met for the specified pressure condition for the period specified before toggling the condition back to false.

**5.10.2. Understanding how images are removed through garbage collection**

Image garbage collection relies on disk usage as reported by cAdvisor on the node to decide which images to remove from the node.

The policy for image garbage collection is based on two conditions:

- The percent of disk usage (expressed as an integer) which triggers image garbage collection. The default is 85.
- The percent of disk usage (expressed as an integer) to which image garbage collection attempts to free. Default is 80.

For image garbage collection, you can modify any of the following variables using a custom resource.

Table 5.3. Variables for configuring image garbage collection
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>imageMinimumGCAge</td>
<td>The minimum age for an unused image before the image is removed by garbage collection. The default is 2m.</td>
</tr>
<tr>
<td>imageGCHighThresholdPercent</td>
<td>The percent of disk usage, expressed as an integer, which triggers image garbage collection. The default is 85.</td>
</tr>
<tr>
<td>imageGCLowThresholdPercent</td>
<td>The percent of disk usage, expressed as an integer, to which image garbage collection attempts to free. The default is 80.</td>
</tr>
</tbody>
</table>

Two lists of images are retrieved in each garbage collector run:

1. A list of images currently running in at least one pod.
2. A list of images available on a host.

As new containers are run, new images appear. All images are marked with a time stamp. If the image is running (the first list above) or is newly detected (the second list above), it is marked with the current time. The remaining images are already marked from the previous spins. All images are then sorted by the time stamp.

Once the collection starts, the oldest images get deleted first until the stopping criterion is met.

### 5.10.3. Configuring garbage collection for containers and images

As an administrator, you can configure how OpenShift Container Platform performs garbage collection by creating a `kubeletConfig` object for each machine config pool.

**NOTE**

OpenShift Container Platform supports only one `kubeletConfig` object for each machine config pool.

You can configure any combination of the following:

- Soft eviction for containers
- Hard eviction for containers
- Eviction for images

**Prerequisites**

1. Obtain the label associated with the static `MachineConfigPool` CRD for the type of node you want to configure. Perform one of the following steps:
   a. View the machine config pool:

   ```bash
   $ oc describe machineconfigpool <name>
   ```
For example:

```bash
$ oc describe machineconfigpool worker
```

**Example output**

```
Name:     worker
Namespace: 
Labels:   custom-kubelet=small-pods
```

If a label has been added it appears under **Labels**.

b. If the label is not present, add a key/value pair:

```bash
$ oc label machineconfigpool worker custom-kubelet=small-pods
```

**TIP**

You can alternatively apply the following YAML to add the label:

```yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
metadata:
  name: worker
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: small-pods
```

**Procedure**

1. Create a custom resource (CR) for your configuration change.

**IMPORTANT**

If there is one file system, or if `/var/lib/kubelet` and `/var/lib/containers/` are in the same file system, the settings with the highest values trigger evictions, as those are met first. The file system triggers the eviction.

**Sample configuration for a container garbage collection CR:**

```yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: worker-kubeconfig
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: small-pods
  kubeletConfig:
    evictionSoft:
      memory.available: "500Mi"
```
Name for the object.

Selector label.

Type of eviction: **evictionSoft** or **evictionHard**.

Eviction thresholds based on a specific eviction trigger signal.

Grace periods for the soft eviction. This parameter does not apply to **eviction-hard**.

Eviction thresholds based on a specific eviction trigger signal. For **evictionHard** you must specify all of these parameters. If you do not specify all parameters, only the specified parameters are applied and the garbage collection will not function properly.

The duration to wait before transitioning out of an eviction pressure condition.

The minimum age for an unused image before the image is removed by garbage collection.

The percent of disk usage (expressed as an integer) that triggers image garbage collection.

The percent of disk usage (expressed as an integer) that image garbage collection attempts to free.

2. Create the object:

```
$ oc create -f <file-name>.yaml
```

For example:

```
$ oc create -f gc-container.yaml
```

**Example output**
3. Verify that garbage collection is active. The Machine Config Pool you specified in the custom resource appears with **UPDATING** as ‘true’ until the change is fully implemented:

```
$ oc get machineconfigpool
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>CONFIG</th>
<th>UPDATED</th>
<th>UPDATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>rendered-master-546383f80705bd5aeaba93</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>worker</td>
<td>rendered-worker-b4c51bb33ccaae6fc4a6a5</td>
<td>False</td>
<td>True</td>
</tr>
</tbody>
</table>

### 5.11. ALLOCATING RESOURCES FOR NODES IN AN OPENSIGHT CONTAINER PLATFORM CLUSTER

To provide more reliable scheduling and minimize node resource overcommitment, reserve a portion of the CPU and memory resources for use by the underlying node components, such as **kubelet** and **kube-proxy**, and the remaining system components, such as **sshd** and **NetworkManager**. By specifying the resources to reserve, you provide the scheduler with more information about the remaining CPU and memory resources that a node has available for use by pods. You can allow OpenShift Container Platform to **automatically determine the optimal system-reserved CPU and memory resources** for your nodes or you can **manually determine and set the best resources** for your nodes.

#### 5.11.1. Understanding how to allocate resources for nodes

CPU and memory resources reserved for node components in OpenShift Container Platform are based on two node settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>kube-reserved</strong></td>
<td>This setting is not used with OpenShift Container Platform. Add the CPU and memory resources that you planned to reserve to the <strong>system-reserved</strong> setting.</td>
</tr>
<tr>
<td><strong>system-reserved</strong></td>
<td>This setting identifies the resources to reserve for the node components and system components, such as CRI-O and Kubelet. The default settings depend on the OpenShift Container Platform and Machine Config Operator versions. Confirm the default <strong>systemReserved</strong> parameter on the <strong>machine-config-operator</strong> repository.</td>
</tr>
</tbody>
</table>

If a flag is not set, the defaults are used. If none of the flags are set, the allocated resource is set to the node’s capacity as it was before the introduction of allocatable resources.

**NOTE**

Any CPUs specifically reserved using the **reservedSystemCPUs** parameter are not available for allocation using **kube-reserved** or **system-reserved**.

#### 5.11.1.1. How OpenShift Container Platform computes allocated resources
An allocated amount of a resource is computed based on the following formula:

\[
\text{[Allocatable]} = \text{[Node Capacity]} - \text{[system-reserved]} - \text{[Hard-Eviction-Thresholds]}
\]

**NOTE**

The withholding of Hard-Eviction-Thresholds from Allocatable improves system reliability because the value for Allocatable is enforced for pods at the node level.

If Allocatable is negative, it is set to 0.

Each node reports the system resources that are used by the container runtime and kubelet. To simplify configuring the system-reserved parameter, view the resource use for the node by using the node summary API. The node summary is available at /api/v1/nodes/<node>/proxy/stats/summary.

### 5.11.1.2. How nodes enforce resource constraints

The node is able to limit the total amount of resources that pods can consume based on the configured allocatable value. This feature significantly improves the reliability of the node by preventing pods from using CPU and memory resources that are needed by system services such as the container runtime and node agent. To improve node reliability, administrators should reserve resources based on a target for resource use.

The node enforces resource constraints by using a new cgroup hierarchy that enforces quality of service. All pods are launched in a dedicated cgroup hierarchy that is separate from system daemons.

Administrators should treat system daemons similar to pods that have a guaranteed quality of service. System daemons can burst within their bounding control groups and this behavior must be managed as part of cluster deployments. Reserve CPU and memory resources for system daemons by specifying the amount of CPU and memory resources in system-reserved.

Enforcing system-reserved limits can prevent critical system services from receiving CPU and memory resources. As a result, a critical system service can be ended by the out-of-memory killer. The recommendation is to enforce system-reserved only if you have profiled the nodes exhaustively to determine precise estimates and you are confident that critical system services can recover if any process in that group is ended by the out-of-memory killer.

### 5.11.1.3. Understanding Eviction Thresholds

If a node is under memory pressure, it can impact the entire node and all pods running on the node. For example, a system daemon that uses more than its reserved amount of memory can trigger an out-of-memory event. To avoid or reduce the probability of system out-of-memory events, the node provides out-of-resource handling.

You can reserve some memory using the `--eviction-hard` flag. The node attempts to evict pods whenever memory availability on the node drops below the absolute value or percentage. If system daemons do not exist on a node, pods are limited to the memory capacity - eviction-hard. For this reason, resources set aside as a buffer for eviction before reaching out of memory conditions are not available for pods.

The following is an example to illustrate the impact of node allocatable for memory:

- Node capacity is 32Gi
- `--system-reserved` is 3Gi
--eviction-hard is set to 100Mi.

For this node, the effective node allocatable value is 28.9Gi. If the node and system components use all their reservation, the memory available for pods is 28.9Gi, and kubelet evicts pods when it exceeds this threshold.

If you enforce node allocatable, 28.9Gi, with top-level cgroups, then pods can never exceed 28.9Gi. Evictions are not performed unless system daemons consume more than 3.1Gi of memory.

If system daemons do not use up all their reservation, with the above example, pods would face memcg OOM kills from their bounding cgroup before node evictions kick in. To better enforce QoS under this situation, the node applies the hard eviction thresholds to the top-level cgroup for all pods to be Node Allocatable + Eviction Hard Thresholds.

If system daemons do not use up all their reservation, the node will evict pods whenever they consume more than 28.9Gi of memory. If eviction does not occur in time, a pod will be OOM killed if pods consume 29Gi of memory.

5.11.1.4. How the scheduler determines resource availability

The scheduler uses the value of node.Status.Allocatable instead of node.Status.Capacity to decide if a node will become a candidate for pod scheduling.

By default, the node will report its machine capacity as fully schedulable by the cluster.

5.11.2. Automatically allocating resources for nodes

OpenShift Container Platform can automatically determine the optimal system-reserved CPU and memory resources for nodes associated with a specific machine config pool and update the nodes with those values when the nodes start.

To automatically determine and allocate the system-reserved resources on nodes, create a KubeletConfig custom resource (CR) to set the autoSizingReserved: true parameter. A script on each node calculates the optimal values for the respective reserved resources based on the installed CPU and memory capacity on each node. The script takes into account that increased capacity requires a corresponding increase in the reserved resources.

Automatically determining the optimal system-reserved settings ensures that your cluster is running efficiently and prevents node failure due to resource starvation of system components, such as CRI-O and kubelet, without your needing to manually calculate and update the values.

This feature is disabled by default.

Prerequisites

1. Obtain the label associated with the static MachineConfigPool object for the type of node you want to configure. Perform one of the following steps:
   
   a. View the machine config pool:

   ```
   $ oc describe machineconfigpool <name>
   ```

   For example:

   ```
   $ oc describe machineconfigpool worker
   ```
Example output

<table>
<thead>
<tr>
<th>Name: worker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Namespace:</td>
</tr>
<tr>
<td>Labels:</td>
</tr>
<tr>
<td>machineconfiguration.openshift.io/mco-built-in=</td>
</tr>
<tr>
<td>pools.operator.machineconfiguration.openshift.io/worker=</td>
</tr>
<tr>
<td>Annotations: &lt;none&gt;</td>
</tr>
<tr>
<td>API Version: machineconfiguration.openshift.io/v1</td>
</tr>
<tr>
<td>Kind:</td>
</tr>
<tr>
<td>MachineConfigPool</td>
</tr>
<tr>
<td>Metadata:</td>
</tr>
<tr>
<td>creationTimestamp: 2019-02-08T14:52:39Z</td>
</tr>
<tr>
<td>generation: 1</td>
</tr>
<tr>
<td>labels:</td>
</tr>
<tr>
<td>pools.operator.machineconfiguration.openshift.io/worker: &quot;&quot;</td>
</tr>
</tbody>
</table>

1. If a label has been added it appears under **labels**.

b. If the label is not present, add a key/value pair:

```
$ oc label machineconfigpool worker custom-kubelet=small-pods
```

**TIP**

You can alternatively apply the following YAML to add the label:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
metadata:
  labels:
    custom-kubelet: small-pods
name: worker
```

**Procedure**

1. Create a custom resource (CR) for your configuration change:

   **Sample configuration for a resource allocation CR**

```
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: dynamic-node
spec:
  autoSizingReserved: true
  machineConfigPoolSelector:
    matchLabels:
      pools.operator.machineconfiguration.openshift.io/worker: ""
```

1. Assign a name to CR.
Add the `autoSizingReserved` parameter set to `true` to allow OpenShift Container Platform to automatically determine and allocate the `system-reserved` resources on the

Specify the label from the machine config pool.

The previous example enables automatic resource allocation on all worker nodes. OpenShift Container Platform drains the nodes, applies the kubelet config, and restarts the nodes.

2. Verify the `system-reserved` value:
   a. Log in to a node you configured:
      ```
      $ oc debug node/<node_name>
      ```
   b. View details on the kubelet process:
      ```
      # ps -ef | grep kubelet
      ```

Example output

```
root  1613  1 11 06:49 ?  00:00:05 kubelet --config=/etc/kubernetes/kubelet.conf --bootstrap-kubeconfig=/etc/kubernetes/kubeconfig --kubeconfig=/var/lib/kubelet/kubeconfig --container-runtime=remote --container-runtime-endpoint=/var/run/crio/crio.sock --runtime-cgroups=/system.slice/crio.service --node-labels=node-role.kubernetes.io/worker,node.openshift.io/os_id=rhcos --node-ip= --minimum-container-ttl-duration=6m0s --volume-plugin-dir=/etc/kubernetes/kubelet-plugins/volume/exec --cloud-provider=azure --cloud-config=/etc/kubernetes/cloud.conf --pod-infra-container-image=quay.io/openshift-release-dev/ocp-v4.0-art-dev@sha256:7b8e2e2857d8ac3499c9eb4e449cc3296409f1da21aa21d0140134d611e65b84 --system-reserved=cpu=0.07,memory=2.5Gi --v=2
```

In the previous example, the worker nodes are allocated **0.07** CPU and 2.5 Gi of memory. It can take several minutes for the optimal values to appear.

5.11.3. Manually allocating resources for nodes

OpenShift Container Platform supports the CPU and memory resource types for allocation. The `ephemeral-resource` resource type is supported as well. For the `cpu` type, the resource quantity is specified in units of cores, such as **200m**, **0.5**, or **1**. For `memory` and `ephemeral-storage`, it is specified in units of bytes, such as **200Ki**, **50Mi**, or **5Gi**.

As an administrator, you can set these using a custom resource (CR) through a set of `<resource_type>=<resource_quantity>` pairs (e.g., `cpu=200m,memory=512Mi`).

For details on the recommended `system-reserved` values, refer to the recommended system-reserved values.

Prerequisites

1. Obtain the label associated with the static `MachineConfigPool` CRD for the type of node you want to configure. Perform one of the following steps:
   a. View the Machine Config Pool:
$ oc describe machineconfigpool <name>

For example:

$ oc describe machineconfigpool worker

**Example output**

```yaml
custom-kubelet: small-pods
```

1. If a label has been added it appears under **labels**.

b. If the label is not present, add a key/value pair:

```bash
$ oc label machineconfigpool worker custom-kubelet=small-pods
```

**TIP**

You can alternatively apply the following YAML to add the label:

```yaml
custom-kubelet: small-pods
```

**Procedure**

1. Create a custom resource (CR) for your configuration change.

**Sample configuration for a resource allocation CR**

```yaml
name: set-allocatable
matchLabels:
  custom-kubelet: small-pods
kubeletConfig:
  systemReserved:
    cpu: 1000m
    memory: 1Gi
```
Assign a name to CR.

Specify the label from the Machine Config Pool.

Specify the resources to reserve for the node components and system components.

5.12. ALLOCATING SPECIFIC CPUS FOR NODES IN A CLUSTER

When using the static CPU Manager policy, you can reserve specific CPUs for use by specific nodes in your cluster. For example, on a system with 24 CPUs, you could reserve CPUs numbered 0 - 3 for the control plane allowing the compute nodes to use CPUs 4 - 23.

5.12.1. Reserving CPUs for nodes

To explicitly define a list of CPUs that are reserved for specific nodes, create a KubeletConfig custom resource (CR) to define the reservedSystemCPUs parameter. This list supersedes the CPUs that might be reserved using the systemReserved and kubeReserved parameters.

Procedure

1. Obtain the label associated with the machine config pool (MCP) for the type of node you want to configure:

   $ oc describe machineconfigpool <name>

   For example:

   $ oc describe machineconfigpool worker

   Example output

   ```yaml
   Name: worker
   Namespace: 
   Labels: machineconfiguration.openshift.io/mco-built-in="pools.operator.machineconfiguration.openshift.io/worker=1"
   Annotations: <none>
   API Version: machineconfiguration.openshift.io/v1
   Kind: MachineConfigPool
   ...
   1 Get the MCP label.
   
   2 Create a YAML file for the KubeletConfig CR:

   ```yaml
   apiVersion: machineconfiguration.openshift.io/v1
   kind: KubeletConfig
   metadata:
     name: set-reserved-cpus 1
   spec:
     kubletConfig:
       reservedSystemCPUs: "0,1,2,3" 2
   ```
machineConfigPoolSelector:
  matchLabels:
    pools.operator.machineconfiguration.openshift.io/worker: ""

1. Specify a name for the CR.

2. Specify the core IDs of the CPUs you want to reserve for the nodes associated with the MCP.

3. Specify the label from the MCP.

3. Create the CR object:

   $ oc create -f <file_name>.yaml

Additional resources

- For more information on the `systemReserved` and `kubeReserved` parameters, see Allocating resources for nodes in an OpenShift Container Platform cluster.

### 5.13. ENABLING TLS SECURITY PROFILES FOR THE KUBELET

You can use a TLS (Transport Layer Security) security profile to define which TLS ciphers are required by the kubelet when it is acting as an HTTP server. The kubelet uses its HTTP/GRPC server to communicate with the Kubernetes API server, which sends commands to pods, gathers logs, and runs exec commands on pods through the kubelet.

A TLS security profile defines the TLS ciphers that the Kubernetes API server must use when connecting with the kubelet to protect communication between the kubelet and the Kubernetes API server.

**NOTE**

By default, when the kubelet acts as a client with the Kubernetes API server, it automatically negotiates the TLS parameters with the API server.

### 5.13.1. Understanding TLS security profiles

You can use a TLS (Transport Layer Security) security profile to define which TLS ciphers are required by various OpenShift Container Platform components. The OpenShift Container Platform TLS security profiles are based on Mozilla recommended configurations.

You can specify one of the following TLS security profiles for each component:

<table>
<thead>
<tr>
<th>Table 5.4. TLS security profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile</strong></td>
</tr>
</tbody>
</table>

---
### Profile Description

<table>
<thead>
<tr>
<th>Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Old</strong></td>
<td>This profile is intended for use with legacy clients or libraries. The profile is based on the Old backward compatibility recommended configuration. The <strong>Old</strong> profile requires a minimum TLS version of 1.0.</td>
</tr>
<tr>
<td><strong>Intermediate</strong></td>
<td>This profile is the recommended configuration for the majority of clients. It is the default TLS security profile for the Ingress Controller, kubelet, and control plane. The profile is based on the Intermediate compatibility recommended configuration. The <strong>Intermediate</strong> profile requires a minimum TLS version of 1.2.</td>
</tr>
<tr>
<td><strong>Modern</strong></td>
<td>This profile is intended for use with modern clients that have no need for backwards compatibility. This profile is based on the Modern compatibility recommended configuration. The <strong>Modern</strong> profile requires a minimum TLS version of 1.3.</td>
</tr>
<tr>
<td><strong>Custom</strong></td>
<td>This profile allows you to define the TLS version and ciphers to use.</td>
</tr>
</tbody>
</table>

#### NOTE

When using one of the predefined profile types, the effective profile configuration is subject to change between releases. For example, given a specification to use the Intermediate profile deployed on release X.Y.Z, an upgrade to release X.Y.Z+1 might cause a new profile configuration to be applied, resulting in a rollout.

### 5.13.2. Configuring the TLS security profile for the kubelet

To configure a TLS security profile for the kubelet when it is acting as an HTTP server, create a **KubeletConfig** custom resource (CR) to specify a predefined or custom TLS security profile for specific nodes. If a TLS security profile is not configured, the default TLS security profile is **Intermediate**.

Sample **KubeletConfig** CR that configures the **Old** TLS security profile on worker nodes
You can see the ciphers and the minimum TLS version of the configured TLS security profile in the `kubelet.conf` file on a configured node.

**IMPORTANT**

The kubelet does not support TLS 1.3 and because the Modern profile requires TLS 1.3, it is not supported. The kubelet converts the Modern profile to Intermediate.

The kubelet also converts the TLS 1.0 of an Old or Custom profile to 1.1, and TLS 1.3 of a Custom profile to 1.2.

**Prerequisites**

- You have access to the cluster as a user with the cluster-admin role.

**Procedure**

1. Create a KubeletConfig CR to configure the TLS security profile:

   **Sample KubeletConfig CR for a Custom profile**

   ```yaml
   apiVersion: machineconfiguration.openshift.io/v1
   kind: KubeletConfig
   metadata:
     name: set-kubelet-tls-security-profile
   spec:
     tlsSecurityProfile:
       type: Custom
       custom:
         ciphers:
         - ECDHE-ECDSA-CHACHA20-POLY1305
         - ECDHE-RSA-CHACHA20-POLY1305
         - ECDHE-RSA-AES128-GCM-SHA256
         - ECDHE-ECDSA-AES128-GCM-SHA256
       minTLSVersion: VersionTLS11
   machineConfigPoolSelector:
     matchLabels:
       pools.operator.machineconfiguration.openshift.io/worker: ""
   ```

   1. Specify the TLS security profile type (Old, Intermediate, or Custom). The default is Intermediate.
2. Specify the appropriate field for the selected type:
   - old: {}
   - intermediate: {}
   - custom:

3. For the custom type, specify a list of TLS ciphers and minimum accepted TLS version.

4. Optional: Specify the machine config pool label for the nodes you want to apply the TLS security profile.

2. Create the KubeletConfig object:

   $ oc create -f <filename>

   Depending on the number of worker nodes in the cluster, wait for the configured nodes to be rebooted one by one.

Verification

To verify that the profile is set, perform the following steps after the nodes are in the Ready state:

1. Start a debug session for a configured node:

   $ oc debug node/<node_name>

2. Set /host as the root directory within the debug shell:

   sh-4.4# chroot /host

3. View the kubelet.conf file:

   sh-4.4# cat /etc/kubernetes/kubelet.conf

Example output

```
kind: KubeletConfiguration
apiVersion: kubelet.config.k8s.io/v1beta1
...
"TlsCipherSuites": [
  "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
  "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
  "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
  "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
  "TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256",
  "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
  "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"
],
"TlsMinVersion": "VersionTLS12",
```

5.14. MACHINE CONFIGDaemon METRICS
The Machine Config Daemon is a part of the Machine Config Operator. It runs on every node in the cluster. The Machine Config Daemon manages configuration changes and updates on each of the nodes.

5.14.1. Machine Config Daemon metrics

Beginning with OpenShift Container Platform 4.3, the Machine Config Daemon provides a set of metrics. These metrics can be accessed using the Prometheus Cluster Monitoring stack.

The following table describes this set of metrics.

**NOTE**

Metrics marked with * in the *Name* and Description columns represent serious errors that might cause performance problems. Such problems might prevent updates and upgrades from proceeding.

**NOTE**

While some entries contain commands for getting specific logs, the most comprehensive set of logs is available using the `oc adm must-gather` command.

### Table 5.5. MCO metrics

<table>
<thead>
<tr>
<th>Name</th>
<th>Format</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>mcd_host_os_and_version</td>
<td><code>[]string{&quot;os&quot;, &quot;version&quot;}</code></td>
<td>Shows the OS that MCD is running on, such as RHCOS or RHEL. In case of RHCOS, the version is provided.</td>
<td></td>
</tr>
<tr>
<td>mcd_drain_err*</td>
<td><code>{&quot;drain_time&quot;, &quot;err&quot;}</code></td>
<td>Logs errors received during failed drain. *</td>
<td>While drains might need multiple tries to succeed, terminal failed drains prevent updates from proceeding. The <code>drain_time</code> metric, which shows how much time the drain took, might help with troubleshooting. For further investigation, see the logs by running: $ oc logs -f -n openshift-machine-config-operator machine-config-daemon-&lt;hash&gt; -c machine-config-daemon</td>
</tr>
</tbody>
</table>

OpenShift Container Platform 4.11 Nodes

266
<table>
<thead>
<tr>
<th>Name</th>
<th>Format</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| mcd_pivot_err* | []string{"err", "node", "pivot_target"} | Logs errors encountered during pivot. * | Pivot errors might prevent OS upgrades from proceeding. For further investigation, run this command to access the node and see all its logs:  

```bash
$ oc debug node/<node> — chroot /host journalctl -u pivot.service
```
| mcd_state | []string{"state", "reason"} | State of Machine Config Daemon for the indicated node. Possible states are "Done", "Working", and "Degraded". In case of "Degraded", the reason is included. | For further investigation, see the logs by running:  

```bash
$ oc logs -f -n openshift-machine-config-operator machine-config-daemon-<hash> -c machine-config-daemon
```
| mcd_kubelet_state* | []string{"err"} | Logs kubelet health failures. * | This is expected to be empty, with failure count of 0. If failure count exceeds 2, the error indicating threshold is exceeded. This indicates a possible issue with the health of the kubelet. For further investigation, run this command to access the node and see all its logs:  

```bash
$ oc debug node/<node> — chroot /host journalctl -u kubelet
```
<table>
<thead>
<tr>
<th>Name</th>
<th>Format</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| mcd_reboot_err*     | []string{"message", "err", "node"} | Logs the failed reboots and the corresponding errors. *                    | This is expected to be empty, which indicates a successful reboot. For further investigation, see the logs by running: 
$ oc logs -f -n openshift-machine-config-operator machine-config-daemon-<hash> -c machine-config-daemon |
| mcd_update_state    | []string{"config", "err"}  | Logs success or failure of configuration updates and the corresponding errors. | The expected value is rendered-master/rendered-worker-XXXX. If the update fails, an error is present. For further investigation, see the logs by running: 
$ oc logs -f -n openshift-machine-config-operator machine-config-daemon-<hash> -c machine-config-daemon |

**Additional resources**

- See [Monitoring overview](#).
- See [the documentation on gathering data about your cluster](#).
CHAPTER 6. WORKING WITH CONTAINERS

6.1. UNDERSTANDING CONTAINERS

The basic units of OpenShift Container Platform applications are called containers. Linux container technologies are lightweight mechanisms for isolating running processes so that they are limited to interacting with only their designated resources.

Many application instances can be running in containers on a single host without visibility into each others' processes, files, network, and so on. Typically, each container provides a single service (often called a “micro-service”), such as a web server or a database, though containers can be used for arbitrary workloads.

The Linux kernel has been incorporating capabilities for container technologies for years. OpenShift Container Platform and Kubernetes add the ability to orchestrate containers across multi-host installations.

About containers and RHEL kernel memory
Due to Red Hat Enterprise Linux (RHEL) behavior, a container on a node with high CPU usage might seem to consume more memory than expected. The higher memory consumption could be caused by the `kmem_cache` in the RHEL kernel. The RHEL kernel creates a `kmem_cache` for each cgroup. For added performance, the `kmem_cache` contains a `cpu_cache`, and a node cache for any NUMA nodes. These caches all consume kernel memory.

The amount of memory stored in those caches is proportional to the number of CPUs that the system uses. As a result, a higher number of CPUs results in a greater amount of kernel memory being held in these caches. Higher amounts of kernel memory in these caches can cause OpenShift Container Platform containers to exceed the configured memory limits, resulting in the container being killed.

To avoid losing containers due to kernel memory issues, ensure that the containers request sufficient memory. You can use the following formula to estimate the amount of memory consumed by the `kmem_cache`, where `nproc` is the number of processing units available that are reported by the `nproc` command. The lower limit of container requests should be this value plus the container memory requirements:

\[
\text{Memory} = (nproc) \times 1/2 \text{MiB}
\]

6.2. USING INIT CONTAINERS TO PERFORM TASKS BEFORE A POD IS DEPLOYED

OpenShift Container Platform provides init containers, which are specialized containers that run before application containers and can contain utilities or setup scripts not present in an app image.

6.2.1. Understanding Init Containers

You can use an Init Container resource to perform tasks before the rest of a pod is deployed.

A pod can have Init Containers in addition to application containers. Init containers allow you to reorganize setup scripts and binding code.

An Init Container can:

- Contain and run utilities that are not desirable to include in the app Container image for security reasons.
• Contain utilities or custom code for setup that is not present in an app image. For example, there is no requirement to make an image FROM another image just to use a tool like sed, awk, python, or dig during setup.

• Use Linux namespaces so that they have different filesystem views from app containers, such as access to secrets that application containers are not able to access.

Each Init Container must complete successfully before the next one is started. So, Init Containers provide an easy way to block or delay the startup of app containers until some set of preconditions are met.

For example, the following are some ways you can use Init Containers:

• Wait for a service to be created with a shell command like:

```bash
for i in {1..100}; do sleep 1; if dig myservice; then exit 0; fi; done; exit 1
```

• Register this pod with a remote server from the downward API with a command like:

```bash
$ curl -X POST
http://$MANAGEMENT_SERVICE_HOST:$MANAGEMENT_SERVICE_PORT/register -d
'instance=$( )&ip=$( )'
```

• Wait for some time before starting the app Container with a command like `sleep 60`.

• Clone a git repository into a volume.

• Place values into a configuration file and run a template tool to dynamically generate a configuration file for the main app Container. For example, place the POD_IP value in a configuration and generate the main app configuration file using Jinja.

See the Kubernetes documentation for more information.

### 6.2.2. Creating Init Containers

The following example outlines a simple pod which has two Init Containers. The first waits for `myservice` and the second waits for `mydb`. After both containers complete, the pod begins.

**Procedure**

1. Create a YAML file for the Init Container:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: myapp-pod
labels:
  app: myapp
spec:
  containers:
  - name: myapp-container
    image: registry.access.redhat.com/ubi8/ubi:latest
    command: ['sh', '-c', 'echo The app is running! && sleep 3600']

  initContainers:
  - name: init-myservice
```

OpenShift Container Platform 4.11 Nodes

270
2. Create a YAML file for the `myservice` service.

```yaml
kind: Service
apiVersion: v1
metadata:
  name: myservice
spec:
  ports:
  - protocol: TCP
    port: 80
    targetPort: 9376
```

3. Create a YAML file for the `mydb` service.

```yaml
kind: Service
apiVersion: v1
metadata:
  name: mydb
spec:
  ports:
  - protocol: TCP
    port: 80
    targetPort: 9377
```

4. Run the following command to create the `myapp-pod`:

```bash
$ oc create -f myapp.yaml
```

**Example output**

```
pod/myapp-pod created
```

5. View the status of the pod:

```bash
$ oc get pods
```

**Example output**

```
NAME        READY     STATUS             RESTARTS   AGE
myapp-pod   0/1        Init:0/2          0          5s
```

Note that the pod status indicates it is waiting.

6. Run the following commands to create the services:

```bash
$ oc create -f mydb.yaml
```
6.3. USING VOLUMES TO PERSIST CONTAINER DATA

Files in a container are ephemeral. As such, when a container crashes or stops, the data is lost. You can use *volumes* to persist the data used by the containers in a pod. A volume is a directory, accessible to the Containers in a pod, where data is stored for the life of the pod.

6.3.1. Understanding volumes

Volumes are mounted file systems available to pods and their containers which may be backed by a number of host-local or network attached storage endpoints. Containers are not persistent by default; on restart, their contents are cleared.

To ensure that the file system on the volume contains no errors and, if errors are present, to repair them when possible, OpenShift Container Platform invokes the `fsck` utility prior to the `mount` utility. This occurs when either adding a volume or updating an existing volume.

The simplest volume type is *emptyDir*, which is a temporary directory on a single machine. Administrators may also allow you to request a persistent volume that is automatically attached to your pods.

**NOTE**

*emptyDir* volume storage may be restricted by a quota based on the pod’s FSGroup, if the FSGroup parameter is enabled by your cluster administrator.

6.3.2. Working with volumes using the OpenShift Container Platform CLI

You can use the CLI command `oc set volume` to add and remove volumes and volume mounts for any object that has a pod template like replication controllers or deployment configs. You can also list volumes in pods or any object that has a pod template.

The `oc set volume` command uses the following general syntax:

```
$ oc set volume <object_selection> <operation> <mandatory_parameters> <options>
```

**Object selection**

Specify one of the following for the `object_selection` parameter in the `oc set volume` command:

**Table 6.1. Object Selection**
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;object_type&gt; &lt;name&gt;</code></td>
<td>Selects <code>&lt;name&gt;</code> of type <code>&lt;object_type&gt;</code>.</td>
<td>deploymentConfig registry</td>
</tr>
<tr>
<td><code>&lt;object_type&gt;/&lt;name&gt;</code></td>
<td>Selects <code>&lt;name&gt;</code> of type <code>&lt;object_type&gt;</code>.</td>
<td>deploymentConfig/registry</td>
</tr>
<tr>
<td><code>&lt;object_type&gt;--selector=&lt;object_label_selector&gt;</code></td>
<td>Selects resources of type <code>&lt;object_type&gt;</code> that matched the given label selector.</td>
<td>deploymentConfig--selector=&quot;name=registry&quot;</td>
</tr>
<tr>
<td><code>&lt;object_type&gt; --all</code></td>
<td>Selects all resources of type <code>&lt;object_type&gt;</code>.</td>
<td>deploymentConfig --all</td>
</tr>
<tr>
<td><code>-f or --filename=&lt;file_name&gt;</code></td>
<td>File name, directory, or URL to file to use to edit the resource.</td>
<td>-f registry-deployment-config.json</td>
</tr>
</tbody>
</table>

**Operation**

Specify `--add` or `--remove` for the operation parameter in the `oc set volume` command.

**Mandatory parameters**

Any mandatory parameters are specific to the selected operation and are discussed in later sections.

**Options**

Any options are specific to the selected operation and are discussed in later sections.

### 6.3.3. Listing volumes and volume mounts in a pod

You can list volumes and volume mounts in pods or pod templates:

**Procedure**

To list volumes:

```
$ oc set volume <object_type>/<name> [options]
```

List volume supported options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--name</code></td>
<td>Name of the volume.</td>
<td></td>
</tr>
<tr>
<td><code>-c, --containers</code></td>
<td>Select containers by name. It can also take wildcard <code>*</code> that matches any character.</td>
<td><code>*</code></td>
</tr>
</tbody>
</table>

For example:

- To list all volumes for pod `p1`:
  ```
  -
  ```
To list volume v1 defined on all deployment configs:

$ oc set volume dc --all --name=v1

### 6.3.4. Adding volumes to a pod

You can add volumes and volume mounts to a pod.

**Procedure**

To add a volume, a volume mount, or both to pod templates:

```bash
$ oc set volume <object_type>/<name> --add [options]
```

**Table 6.2. Supported Options for Adding Volumes**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--name</code></td>
<td>Name of the volume.</td>
<td>Automatically generated, if not specified.</td>
</tr>
<tr>
<td><code>-t, --type</code></td>
<td>Name of the volume source. Supported values: emptyDir, hostPath, secret, configmap, persistentVolumeClaim or projected.</td>
<td>emptyDir</td>
</tr>
<tr>
<td><code>-c, --containers</code></td>
<td>Select containers by name. It can also take wildcard <code>*</code> that matches any character.</td>
<td><code>*</code></td>
</tr>
<tr>
<td><code>-m, --mount-path</code></td>
<td>Mount path inside the selected containers. Do not mount to the container root, /, or any path that is the same in the host and the container. This can corrupt your host system if the container is sufficiently privileged, such as the host /dev/pts files. It is safe to mount the host by using /host.</td>
<td></td>
</tr>
</tbody>
</table>
For example:

- To add a new volume source `emptyDir` to the `registry DeploymentConfig` object:
  ```bash
  $ oc set volume dc/registry --add
  ```
TIP

You can alternatively apply the following YAML to add the volume:

Example 6.1. Sample deployment config with an added volume

```
kind: DeploymentConfig
apiVersion: apps.openshift.io/v1
metadata:
  name: registry
  namespace: registry
spec:
  replicas: 3
  selector:
    app: httpd
template:
  metadata:
    labels:
      app: httpd
  spec:
    volumes:
    - name: volume-pppsw
      emptyDir: {}
    containers:
    - name: httpd
      image: >-
        image-registry.openshift-image-registry.svc:5000/openshift/httpd:latest
      ports:
        - containerPort: 8080
          protocol: TCP
```

1 Add the volume source `emptyDir`.

- To add volume `v1` with secret `secret1` for replication controller `r1` and mount inside the containers at `/data`:

  ```
  $ oc set volume rc/r1 --add --name=v1 --type=secret --secret-name='secret1' --mount-path=/data
  ```

OpenShift Container Platform 4.11 Nodes

276
TIP

You can alternatively apply the following YAML to add the volume:

Example 6.2. Sample replication controller with added volume and secret

```yaml
kind: ReplicationController
apiVersion: v1
metadata:
  name: example-1
  namespace: example
spec:
  replicas: 0
  selector:
    app: httpd
    deployment: example-1
    deploymentconfig: example
template:
  metadata:
    creationTimestamp: null
  labels:
    app: httpd
    deployment: example-1
    deploymentconfig: example
spec:
  volumes:
  - name: v1
    secret:
      secretName: secret1
      defaultMode: 420
  containers:
  - name: httpd
    image: image-registry.openshift-image-registry.svc:5000/openshift/httpd:latest
    volumeMounts:
      - name: v1
        mountPath: /data
```

1. Add the volume and secret.
2. Add the container mount path.

- To add existing persistent volume v1 with claim name pvc1 to deployment configuration dc.json on disk, mount the volume on container c1 at /data, and update the DeploymentConfig object on the server:

  ```bash
  $ oc set volume -f dc.json --add --name=v1 --type=persistentVolumeClaim --claim-name=pvc1 --mount-path=/data --containers=c1
  ```
TIP

You can alternatively apply the following YAML to add the volume:

Example 6.3. Sample deployment config with persistent volume added

```yaml
kind: DeploymentConfig
apiVersion: apps.openshift.io/v1
metadata:
  name: example
  namespace: example
spec:
  replicas: 3
  selector:
    app: httpd
  template:
    metadata:
      labels:
        app: httpd
    spec:
      volumes:
      - name: volume-pppsw
        emptyDir: {}
      - name: v1
        persistentVolumeClaim:
          claimName: pvc1
      containers:
      - name: httpd
        image: image-registry.openshift-image-registry.svc:5000/openshift/httpd:latest
        ports:
        - containerPort: 8080
          protocol: TCP
        volumeMounts:
        - name: v1
          mountPath: /data
```

1. Add the persistent volume claim named `pvc1`.
2. Add the container mount path.

To add a volume `v1` based on Git repository `https://github.com/namespace1/project1` with revision `5125c45f9f563` for all replication controllers:

```bash
$ oc set volume rc --all --add --name=v1 \
  --source='"gitRepo": {
    "repository": "https://github.com/namespace1/project1",
    "revision": "5125c45f9f563"
  }'
```

6.3.5. Updating volumes and volume mounts in a pod

You can modify the volumes and volume mounts in a pod.
Procedure

Updating existing volumes using the `--overwrite` option:

```bash
$ oc set volume <object_type>/<name> --add --overwrite [options]
```

For example:

- To replace existing volume `v1` for replication controller `r1` with existing persistent volume claim `pvc1`:

```bash
$ oc set volume rc/r1 --add --overwrite --name=v1 --type=persistentVolumeClaim --claim-name=pvc1
```
TIP

You can alternatively apply the following YAML to replace the volume:

Example 6.4. Sample replication controller with persistent volume claim named pvc1

```yaml
kind: ReplicationController
apiVersion: v1
metadata:
  name: example-1
  namespace: example
spec:
  replicas: 0
  selector:
    app: httpd
    deployment: example-1
    deploymentconfig: example
  template:
    metadata:
      labels:
        app: httpd
        deployment: example-1
        deploymentconfig: example
    spec:
      volumes:
      - name: v1
        persistentVolumeClaim:
          claimName: pvc1
      containers:
      - name: httpd
        image: registry-10.10.17.205/openshift/httpd:latest
        ports:
        - containerPort: 8080
          protocol: TCP
        volumeMounts:
        - name: v1
          mountPath: /data
```

Set persistent volume claim to pvc1.

- To change the DeploymentConfig object d1 mount point to /opt for volume v1:

  ```bash
  $ oc set volume dc/d1 --add --overwrite --name=v1 --mount-path=/opt
  ```
You can alternatively apply the following YAML to change the mount point:

Example 6.5. Sample deployment config with mount point set to `/opt`.

```yaml
kind: DeploymentConfig
apiVersion: apps.openshift.io/v1
metadata:
  name: example
  namespace: example
spec:
  replicas: 3
  selector:
    app: httpd
  template:
    metadata:
      labels:
        app: httpd
    spec:
      volumes:
        - name: volume-pppsw
          emptyDir: {}
        - name: v2
          persistentVolumeClaim:
            claimName: pvc1
        - name: v1
          persistentVolumeClaim:
            claimName: pvc1
      containers:
        - name: httpd
          image: image-registry.openshift-image-registry.svc:5000/openshift/httpd:latest
          ports:
            - containerPort: 8080
              protocol: TCP
          volumeMounts:
            - name: v1
              mountPath: /opt
```

Set the mount point to `/opt`.

### 6.3.6. Removing volumes and volume mounts from a pod

You can remove a volume or volume mount from a pod.

**Procedure**

To remove a volume from pod templates:

```
$ oc set volume <object_type>/<name> --remove [options]
```

**Table 6.3. Supported options for removing volumes**
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>--name</td>
<td>Name of the volume.</td>
<td></td>
</tr>
<tr>
<td>-c, --containers</td>
<td>Select containers by name. It can also take wildcard '*' that matches any character.</td>
<td>'*'</td>
</tr>
<tr>
<td>--confirm</td>
<td>Indicate that you want to remove multiple volumes at once.</td>
<td></td>
</tr>
<tr>
<td>-o, --output</td>
<td>Display the modified objects instead of updating them on the server. Supported values: json, yaml.</td>
<td></td>
</tr>
<tr>
<td>--output-version</td>
<td>Output the modified objects with the given version.</td>
<td>api-version</td>
</tr>
</tbody>
</table>

For example:

- To remove a volume v1 from the DeploymentConfig object d1:
  ```
  $ oc set volume dc/d1 --remove --name=v1
  ```

- To unmount volume v1 from container c1 for the DeploymentConfig object d1 and remove the volume v1 if it is not referenced by any containers on d1:
  ```
  $ oc set volume dc/d1 --remove --name=v1 --containers=c1
  ```

- To remove all volumes for replication controller r1:
  ```
  $ oc set volume rc/r1 --remove --confirm
  ```

6.3.7. Configuring volumes for multiple uses in a pod

You can configure a volume to allows you to share one volume for multiple uses in a single pod using the `volumeMounts.subPath` property to specify a `subPath` value inside a volume instead of the volume’s root.

**Procedure**

1. View the list of files in the volume, run the `oc rsh` command:
   ```
   $ oc rsh <pod>
   ```

   **Example output**
   ```
   sh-4.2$ ls /path/to/volume/subpath/mount example_file1 example_file2 example_file3
   ```
2. Specify the **subPath**:

**Example Pod spec with subPath parameter**

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: my-site
spec:
  containers:
    - name: mysql
      image: mysql
      volumeMounts:
        - mountPath: /var/lib/mysql
          name: site-data
          subPath: mysql
    - name: php
      image: php
      volumeMounts:
        - mountPath: /var/www/html
          name: site-data
          subPath: html
  volumes:
    - name: site-data
      persistentVolumeClaim:
        claimName: my-site-data
```

1. Databases are stored in the **mysql** folder.
2. HTML content is stored in the **html** folder.

### 6.4. MAPPING VOLUMES USING PROJECTED VOLUMES

A **projected volume** maps several existing volume sources into the same directory.

The following types of volume sources can be projected:

- Secrets
- Config Maps
- Downward API

**NOTE**

All sources are required to be in the same namespace as the pod.

#### 6.4.1. Understanding projected volumes

Projected volumes can map any combination of these volume sources into a single directory, allowing the user to:
- automatically populate a single volume with the keys from multiple secrets, config maps, and with downward API information, so that I can synthesize a single directory with various sources of information;

- populate a single volume with the keys from multiple secrets, config maps, and with downward API information, explicitly specifying paths for each item, so that I can have full control over the contents of that volume.

**IMPORTANT**

When the RunAsUser permission is set in the security context of a Linux-based pod, the projected files have the correct permissions set, including container user ownership. However, when the Windows equivalent RunAsUsername permission is set in a Windows pod, the kubelet is unable to correctly set ownership on the files in the projected volume.

Therefore, the RunAsUsername permission set in the security context of a Windows pod is not honored for Windows projected volumes running in OpenShift Container Platform.

The following general scenarios show how you can use projected volumes.

**Config map, secrets, Downward API.**

Projected volumes allow you to deploy containers with configuration data that includes passwords. An application using these resources could be deploying Red Hat OpenStack Platform (RHOSP) on Kubernetes. The configuration data might have to be assembled differently depending on if the services are going to be used for production or for testing. If a pod is labeled with production or testing, the downward API selector metadata.labels can be used to produce the correct RHOSP configs.

**Config map + secrets.**

Projected volumes allow you to deploy containers involving configuration data and passwords. For example, you might execute a config map with some sensitive encrypted tasks that are decrypted using a vault password file.

**ConfigMap + Downward API.**

Projected volumes allow you to generate a config including the pod name (available via the metadata.name selector). This application can then pass the pod name along with requests to easily determine the source without using IP tracking.

**Secrets + Downward API.**

Projected volumes allow you to use a secret as a public key to encrypt the namespace of the pod (available via the metadata.namespace selector). This example allows the Operator to use the application to deliver the namespace information securely without using an encrypted transport.

**6.4.1.1. Example Pod specs**

The following are examples of Pod specs for creating projected volumes.

**Pod with a secret, a Downward API, and a config map**

```yaml
apiVersion: v1
description: Pod
metadata:
  name: volume-test
spec:
  containers:
  - name: container-test
```
Add a `volumeMounts` section for each container that needs the secret.

Specify a path to an unused directory where the secret will appear.

Set `readOnly` to `true`.

Add a `volumes` block to list each projected volume source.

Set any name for the volume.

Set the execute permission on the files.

Add a secret. Enter the name of the secret object. Each secret you want to use must be listed.

Specify the path to the secrets file under the `mountPath`. Here, the secrets file is in `/projected-volume/my-group/my-username`.

Add a Downward API source.

Add a ConfigMap source.

Set the mode for the specific projection.
NOTE
If there are multiple containers in the pod, each container needs a `volumeMounts` section, but only one `volumes` section is needed.

Pod with multiple secrets with a non-default permission mode set

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: volume-test
spec:
  containers:
    - name: container-test
      image: busybox
      volumeMounts:
        - name: all-in-one
          mountPath: /projected-volume
          readOnly: true
  volumes:
    - name: all-in-one
      projected:
        defaultMode: 0755
        sources:
          - secret:
              name: mysecret
              items:
                - key: username
                  path: my-group/my-username
              - secret:
                  name: mysecret2
                  items:
                    - key: password
                      path: my-group/my-password
                    mode: 511
```

NOTE
The `defaultMode` can only be specified at the projected level and not for each volume source. However, as illustrated above, you can explicitly set the `mode` for each individual projection.

6.4.1.2. Pathing Considerations

**Collisions Between Keys when Configured Paths are Identical**
If you configure any keys with the same path, the pod spec will not be accepted as valid. In the following example, the specified path for `mysecret` and `myconfigmap` are the same:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: volume-test
spec:
  containers:
```
Consider the following situations related to the volume file paths.

**Collisions Between Keys without Configured Paths**

The only run-time validation that can occur is when all the paths are known at pod creation, similar to the above scenario. Otherwise, when a conflict occurs the most recent specified resource will overwrite anything preceding it (this is true for resources that are updated after pod creation as well).

**Collisions when One Path is Explicit and the Other is Automatically Projected**

In the event that there is a collision due to a user specified path matching data that is automatically projected, the latter resource will overwrite anything preceding it as before.

### 6.4.2. Configuring a Projected Volume for a Pod

When creating projected volumes, consider the volume file path situations described in *Understanding projected volumes*.

The following example shows how to use a projected volume to mount an existing secret volume source. The steps can be used to create a user name and password secrets from local files. You then create a pod that runs one container, using a projected volume to mount the secrets into the same shared directory.

**Procedure**

To use a projected volume to mount an existing secret volume source.

1. Create files containing the secrets, entering the following, replacing the password and user information as appropriate:

   ```yaml
   apiVersion: v1
   kind: Secret
   metadata:
     name: mysecret
   type: Opaque
   ```
The user and pass values can be any valid string that is base64 encoded.

The following example shows admin in base64:

```
$ echo -n "admin" | base64
```

**Example output**

YWRtaW4=

The following example shows the password 1f2d1e2e67df in base64:

```
$ echo -n "1f2d1e2e67df" | base64
```

**Example output**

MWYyZDFlMmU2N2Rm

2. Use the following command to create the secrets:

```
$ oc create -f <secrets-filename>
```

For example:

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

**Example output**

secret "mysecret" created

3. You can check that the secret was created using the following commands:

```
$ oc get secret <secret-name>
```

For example:

```
$ oc get secret mysecret
```

**Example output**

```
NAME       TYPE      DATA      AGE
mysecret   Opaque    2         17h
```

```
$ oc get secret <secret-name> -o yaml
```

For example:
$ oc get secret mysecret -o yaml

apiVersion: v1
data:
  pass: MWYyZDFIMmU2N2Rm
  user: YWRtaW4=
kind: Secret
metadata:
  name: mysecret
  namespace: default
  resourceVersion: "2107"
  selfLink: /api/v1/namespaces/default/secrets/mysecret
  uid: 959e0424-4575-11e7-9f97-fa163e4bd54c
  type: Opaque

4. Create a pod configuration file similar to the following that includes a `volumes` section:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: test-projected-volume
spec:
  containers:
    - name: test-projected-volume
      image: busybox
      args:
        - sleep
        - "86400"
      volumeMounts:
        - name: all-in-one
          mountPath: /projected-volume
          readOnly: true
  volumes:
    - name: all-in-one
      projected:
        sources:
          - secret:
            name: user
          - secret:
            name: pass

1 2 The name of the secret you created.

5. Create the pod from the configuration file:

```
$ oc create -f <your_yaml_file>.yaml
```

For example:

```
$ oc create -f secret-pod.yaml
```

Example output
6. Verify that the pod container is running, and then watch for changes to the pod:

```bash
$ oc get pod <name>
```

For example:

```bash
$ oc get pod test-projected-volume
```

The output should appear similar to the following:

**Example output**

```
NAME                    READY     STATUS    RESTARTS   AGE
---                     -----     --------    ---------   ---
test-projected-volume   1/1       Running   0          14s
```

7. In another terminal, use the `oc exec` command to open a shell to the running container:

```bash
$ oc exec -it <pod> <command>
```

For example:

```bash
$ oc exec -it test-projected-volume -- /bin/sh
```

8. In your shell, verify that the `projected-volumes` directory contains your projected sources:

```
/ # ls
```

**Example output**

```
bin       home       root       tmp
dev       proc       run    usr
etc       projected-volume sys     var
```

### 6.5. ALLOWING CONTAINERS TO CONSUME API OBJECTS

The *Downward API* is a mechanism that allows containers to consume information about API objects without coupling to OpenShift Container Platform. Such information includes the pod’s name, namespace, and resource values. Containers can consume information from the downward API using environment variables or a volume plug-in.

#### 6.5.1. Expose pod information to Containers using the Downward API

The Downward API contains such information as the pod’s name, project, and resource values. Containers can consume information from the downward API using environment variables or a volume plug-in.

Fields within the pod are selected using the *FieldRef* API type. *FieldRef* has two fields:
### Field | Description
--- | ---
fieldPath | The path of the field to select, relative to the pod.
apiVersion | The API version to interpret the fieldPath selector within.

Currently, the valid selectors in the v1 API include:

| Selector | Description |
--- | ---
metadata.name | The pod’s name. This is supported in both environment variables and volumes.
metadata.namespace | The pod’s namespace. This is supported in both environment variables and volumes.
metadata.labels | The pod’s labels. This is only supported in volumes and not in environment variables.
metadata.annotations | The pod’s annotations. This is only supported in volumes and not in environment variables.
status.podIP | The pod’s IP. This is only supported in environment variables and not volumes.

The apiVersion field, if not specified, defaults to the API version of the enclosing pod template.

### 6.5.2. Understanding how to consume container values using the downward API

You containers can consume API values using environment variables or a volume plug-in. Depending on the method you choose, containers can consume:

- Pod name
- Pod project/namespace
- Pod annotations
- Pod labels

Annotations and labels are available using only a volume plug-in.

#### 6.5.2.1. Consuming container values using environment variables

When using a container’s environment variables, use the EnvVar type’s valueFrom field (of type EnvVarSource) to specify that the variable’s value should come from a FieldRef source instead of the literal value specified by the value field.
Only constant attributes of the pod can be consumed this way, as environment variables cannot be updated once a process is started in a way that allows the process to be notified that the value of a variable has changed. The fields supported using environment variables are:

- Pod name
- Pod project/namespace

**Procedure**

To use environment variables

1. Create a **pod.yaml** file:

   ```yaml
   apiVersion: v1
   kind: Pod
   metadata:
     name: dapi-env-test-pod
   spec:
     containers:
       - name: env-test-container
         image: gcr.io/google_containers/busybox
         command: ["/bin/sh", "-c", "env"]
         env:
           - name: MY_POD_NAME
             valueFrom:
               fieldRef:
                 fieldPath: metadata.name
           - name: MY_POD_NAMESPACE
             valueFrom:
               fieldRef:
                 fieldPath: metadata.namespace
     restartPolicy: Never
   
2. Create the pod from the **pod.yaml** file:

   ```bash
   $ oc create -f pod.yaml
   
3. Check the container’s logs for the **MY_POD_NAME** and **MY_POD_NAMESPACE** values:

   ```bash
   $ oc logs -p dapi-env-test-pod
   
6.5.2.2. Consuming container values using a volume plug-in

You containers can consume API values using a volume plug-in.

Containers can consume:

- Pod name
- Pod project/namespace
- Pod annotations
- Pod labels
Procedure

To use the volume plug-in:

1. Create a `volume-pod.yaml` file:

   ```yaml
   kind: Pod
   apiVersion: v1
   metadata:
     labels:
       zone: us-east-coast
       cluster: downward-api-test-cluster1
       rack: rack-123
       name: dapi-volume-test-pod
     annotations:
       annotation1: "345"
       annotation2: "456"
   spec:
     containers:
     - name: volume-test-container
       image: gcr.io/google_containers/busybox
       command: ["sh", "-c", "cat /tmp/etc/pod_labels /tmp/etc/pod_annotations"]
       volumeMounts:
       - name: podinfo
         mountPath: /tmp/etc
         readOnly: false
     volumes:
     - name: podinfo
       downwardAPI:
       defaultMode: 420
       items:
       - fieldRef:
         fieldPath: metadata.name
         path: pod_name
       - fieldRef:
         fieldPath: metadata.namespace
         path: pod_namespace
       - fieldRef:
         fieldPath: metadata.labels
         path: pod_labels
       - fieldRef:
         fieldPath: metadata.annotations
         path: pod_annotations
     restartPolicy: Never
   ```

2. Create the pod from the `volume-pod.yaml` file:

   ```bash
   $ oc create -f volume-pod.yaml
   ```

3. Check the container’s logs and verify the presence of the configured fields:

   ```bash
   $ oc logs -p dapi-volume-test-pod
   ```

Example output
6.5.3. Understanding how to consume container resources using the Downward API

When creating pods, you can use the Downward API to inject information about computing resource requests and limits so that image and application authors can correctly create an image for specific environments.

You can do this using environment variable or a volume plug-in.

6.5.3.1. Consuming container resources using environment variables

When creating pods, you can use the Downward API to inject information about computing resource requests and limits using environment variables.

Procedure

To use environment variables:

1. When creating a pod configuration, specify environment variables that correspond to the contents of the `resources` field in the `spec.container` field:

```yaml
cluster=downward-api-test-cluster1
rack=rack-123
zone=us-east-coast
annotation1=345
annotation2=456
kubernetes.io/config.source=api

spec:
  containers:
    - name: test-container
      image: gcr.io/google_containers/busybox:1.24
      command: ["/bin/sh", "-c", "env"]
      resources:
        requests:
          memory: "32Mi"
          cpu: "125m"
        limits:
          memory: "64Mi"
          cpu: "250m"
      env:
        - name: MY_CPU_REQUEST
          valueFrom:
            resourceFieldRef:
              resource: requests.cpu
        - name: MY_CPU_LIMIT
          valueFrom:
            resourceFieldRef:
              resource: limits.cpu
        - name: MY_MEM_REQUEST
          valueFrom:
            resourceFieldRef:
              resource: requests.memory
        - name: MY_MEM_LIMIT
          valueFrom:
```
If the resource limits are not included in the container configuration, the downward API defaults to the node’s CPU and memory allocatable values.

2. Create the pod from the *pod.yaml* file:

   $ oc create -f pod.yaml

### 6.5.3.2. Consuming container resources using a volume plug-in

When creating pods, you can use the Downward API to inject information about computing resource requests and limits using a volume plug-in.

**Procedure**

To use the Volume Plug-in:

1. When creating a pod configuration, use the `spec.volumes.downwardAPI.items` field to describe the desired resources that correspond to the `spec.resources` field:

   ```yaml
   spec:
     containers:
       - name: client-container
         image: gcr.io/google_containers/busybox:1.24
         command: ["sh", "-c", "while true; do echo; if [[ -e /etc/cpu_limit ]]; then cat /etc/cpu_limit; fi; if [[ -e /etc/cpu_request ]]; then cat /etc/cpu_request; fi; if [[ -e /etc/mem_limit ]]; then cat /etc/mem_limit; fi; if [[ -e /etc/mem_request ]]; then cat /etc/mem_request; fi; sleep 5; done"]
         resources:
           requests:
             memory: "32Mi"
             cpu: "125m"
           limits:
             memory: "64Mi"
             cpu: "250m"
         volumeMounts:
           - name: podinfo
             mountPath: /etc
             readOnly: false
       volumes:
         - name: podinfo
           downwardAPI:
             items:
               - path: "cpu_limit"
                 resourceFieldRef:
                   containerName: client-container
                   resource: limits.cpu
               - path: "cpu_request"
                 resourceFieldRef:
                   containerName: client-container
                   resource: requests.cpu
               - path: "mem_limit"
                 resourceFieldRef:
                   containerName: client-container
                   resource: limits.memory
   ```
If the resource limits are not included in the container configuration, the Downward API defaults to the node’s CPU and memory allocatable values.

2. Create the pod from the `volume-pod.yaml` file:

```
$ oc create -f volume-pod.yaml
```

### 6.5.4. Consuming secrets using the Downward API

When creating pods, you can use the downward API to inject secrets so image and application authors can create an image for specific environments.

**Procedure**

1. Create a `secret.yaml` file:

```yaml
apiVersion: v1
group: v1
kind: Secret
metadata:
  name: mysecret
data:
  username: ZGV2ZWxvcGVy
  password: cGFzc3dvcmQ=
type: kubernetes.io/basic-auth
```

2. Create a `Secret` object from the `secret.yaml` file:

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

3. Create a `pod.yaml` file that references the `username` field from the above `Secret` object:

```yaml
apiVersion: v1
group: v1
kind: Pod
metadata:
  name: dapi-env-test-pod
spec:
  containers:
  - name: env-test-container
    image: gcr.io/google_containers/busybox
    command: ['"bin/sh"', '"-c"', '"env"']
    env:
      - name: MY_SECRET_USERNAME
        valueFrom:
          secretKeyRef:
```
Create the pod from the `pod.yaml` file:

```shell
$ oc create -f pod.yaml
```

5. Check the container’s logs for the `MY_SECRET_USERNAME` value:

```shell
$ oc logs -p dapi-env-test-pod
```

### 6.5.5. Consuming configuration maps using the Downward API

When creating pods, you can use the Downward API to inject configuration map values so image and application authors can create an image for specific environments.

**Procedure**

1. Create a `configmap.yaml` file:

```yaml
apiVersion: v1
do: ConfigMap
metadata:
  name: myconfigmap
data:
  mykey: myvalue
```

2. Create a `ConfigMap` object from the `configmap.yaml` file:

```shell
$ oc create -f configmap.yaml
```

3. Create a `pod.yaml` file that references the above `ConfigMap` object:

```yaml
apiVersion: v1
do: Pod
metadata:
  name: dapi-env-test-pod
spec:
  containers:
  - name: env-test-container
    image: gcr.io/google_containers/busybox
    command: ['/bin/sh', '-c', 'env']
    env:
      - name: MY_CONFIGMAP_VALUE
        valueFrom:
          configMapKeyRef:
            name: myconfigmap
            key: mykey
    restartPolicy: Always
```

4. Create the pod from the `pod.yaml` file:
5. Check the container’s logs for the `MY_CONFIGMAP_VALUE` value:

```
$ oc logs -p dapi-env-test-pod
```

### 6.5.6. Referencing environment variables

When creating pods, you can reference the value of a previously defined environment variable by using the `$()` syntax. If the environment variable reference cannot be resolved, the value will be left as the provided string.

**Procedure**

1. Create a `pod.yaml` file that references an existing environment variable:

   ```yaml
   apiVersion: v1
   kind: Pod
   metadata:
     name: dapi-env-test-pod
   spec:
     containers:
     - name: env-test-container
       image: gcr.io/google_containers/busybox
       command: [ "bin/sh", "-c", "env" ]
       env:
       - name: MY_EXISTING_ENV
         value: my_value
       - name: MY_ENV_VAR_REF_ENV
         value: $(MY_EXISTING_ENV)
     restartPolicy: Never
   ```

2. Create the pod from the `pod.yaml` file:

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

3. Check the container’s logs for the `MY_ENV_VAR_REF_ENV` value:

   ```
   $ oc logs -p dapi-env-test-pod
   ```

### 6.5.7. Escaping environment variable references

When creating a pod, you can escape an environment variable reference by using a double dollar sign. The value will then be set to a single dollar sign version of the provided value.

**Procedure**

1. Create a `pod.yaml` file that references an existing environment variable:

   ```yaml
   apiVersion: v1
   kind: Pod
   metadata:
   ```
2. Create the pod from the `pod.yaml` file:

```bash
$ oc create -f pod.yaml
```

3. Check the container’s logs for the `MY_NEW_ENV` value:

```bash
$ oc logs -p dapi-env-test-pod
```

### 6.6. COPYING FILES TO OR FROM AN OPENSSHIFT CONTAINER

#### PLATFORM CONTAINER

You can use the CLI to copy local files to or from a remote directory in a container using the `rsync` command.

### 6.6.1. Understanding how to copy files

The `oc rsync` command, or remote sync, is a useful tool for copying database archives to and from your pods for backup and restore purposes. You can also use `oc rsync` to copy source code changes into a running pod for development debugging, when the running pod supports hot reload of source files.

```bash
$ oc rsync <source> <destination> [-c <container>]
```

### 6.6.1.1. Requirements

#### Specifying the Copy Source

The source argument of the `oc rsync` command must point to either a local directory or a pod directory. Individual files are not supported.

When specifying a pod directory the directory name must be prefixed with the pod name:

```bash
<pod name>:<dir>
```

If the directory name ends in a path separator (`/`), only the contents of the directory are copied to the destination. Otherwise, the directory and its contents are copied to the destination.

#### Specifying the Copy Destination

The destination argument of the `oc rsync` command must point to a directory. If the directory does not exist, but `rsync` is used for copy, the directory is created for you.

Deleting Files at the Destination
The `--delete` flag may be used to delete any files in the remote directory that are not in the local directory.

**Continuous Syncing on File Change**

Using the `--watch` option causes the command to monitor the source path for any file system changes, and synchronizes changes when they occur. With this argument, the command runs forever.

Synchronization occurs after short quiet periods to ensure a rapidly changing file system does not result in continuous synchronization calls.

When using the `--watch` option, the behavior is effectively the same as manually invoking `oc rsync` repeatedly, including any arguments normally passed to `oc rsync`. Therefore, you can control the behavior via the same flags used with manual invocations of `oc rsync`, such as `--delete`.

### 6.6.2. Copying files to and from containers

Support for copying local files to or from a container is built into the CLI.

**Prerequisites**

When working with `oc rsync`, note the following:

**rsync must be installed**

The `oc rsync` command uses the local `rsync` tool if present on the client machine and the remote container.

If `rsync` is not found locally or in the remote container, a `tar` archive is created locally and sent to the container where the `tar` utility is used to extract the files. If `tar` is not available in the remote container, the copy will fail.

The `tar` copy method does not provide the same functionality as `oc rsync`. For example, `oc rsync` creates the destination directory if it does not exist and only sends files that are different between the source and the destination.

**NOTE**

In Windows, the `cwRsync` client should be installed and added to the PATH for use with the `oc rsync` command.

**Procedure**

- To copy a local directory to a pod directory:

  ```bash
  $ oc rsync <local-dir> <pod-name>:/<remote-dir> -c <container-name>
  ```

  For example:

  ```bash
  $ oc rsync /home/user/source devpod1234:/src -c user-container
  ```

- To copy a pod directory to a local directory:

  ```bash
  $ oc rsync devpod1234:/src /home/user/source
  ```

**Example output**

```
6.6.3. Using advanced Rsync features

The `oc rsync` command exposes fewer command line options than standard `rsync`. In the case that you want to use a standard `rsync` command line option that is not available in `oc rsync`, for example the `--exclude-from=FILE` option, it might be possible to use standard `rsync`’s `--rsh (-e)` option or `RSYNC_RSH` environment variable as a workaround, as follows:

```
$ oc rsync devpod1234:/src/status.txt /home/user/
```

or:

```
$ rsync --rsh='oc rsh' --exclude-from=FILE SRC POD:DEST
```

Export the `RSYNC_RSH` variable:

```
$ export RSYNC_RSH='oc rsh'
```

Then, run the rsync command:

```
$ rsync --exclude-from=FILE SRC POD:DEST
```

Both of the above examples configure standard `rsync` to use `oc rsh` as its remote shell program to enable it to connect to the remote pod, and are an alternative to running `oc rsync`.

6.7. EXECUTING REMOTE COMMANDS IN AN OPENSUIT CONTAINER PLATFORM CONTAINER

You can use the CLI to execute remote commands in an OpenShift Container Platform container.

6.7.1. Executing remote commands in containers

Support for remote container command execution is built into the CLI.

**Procedure**

To run a command in a container:

```
$ oc exec <pod> [-c <container>] <command> [<arg_1> ... <arg_n>]
```

For example:

```
$ oc exec mypod date
Thu Apr  9 02:21:53 UTC 2015
```

**Example output**

```
Thu Apr  9 02:21:53 UTC 2015
```

**IMPORTANT**

For security purposes, the `oc exec` command does not work when accessing privileged containers except when the command is executed by a `cluster-admin` user.
6.7.2. Protocol for initiating a remote command from a client

Clients initiate the execution of a remote command in a container by issuing a request to the Kubernetes API server:

```
/proxy/nodes/<node_name>/exec/<namespace>/<pod>/<container>?command=<command>
```

In the above URL:

- `<node_name>` is the FQDN of the node.
- `<namespace>` is the project of the target pod.
- `<pod>` is the name of the target pod.
- `<container>` is the name of the target container.
- `<command>` is the desired command to be executed.

For example:

```
/proxy/nodes/node123.openshift.com/exec/myns/mypod/mycontainer?command=date
```

Additionally, the client can add parameters to the request to indicate if:

- the client should send input to the remote container’s command (stdin).
- the client’s terminal is a TTY.
- the remote container’s command should send output from stdout to the client.
- the remote container’s command should send output from stderr to the client.

After sending an `exec` request to the API server, the client upgrades the connection to one that supports multiplexed streams; the current implementation uses HTTP/2.

The client creates one stream each for stdin, stdout, and stderr. To distinguish among the streams, the client sets the `streamType` header on the stream to one of stdin, stdout, or stderr.

The client closes all streams, the upgraded connection, and the underlying connection when it is finished with the remote command execution request.

6.8. USING PORT FORWARDING TO ACCESS APPLICATIONS IN A CONTAINER

OpenShift Container Platform supports port forwarding to pods.

6.8.1. Understanding port forwarding

You can use the CLI to forward one or more local ports to a pod. This allows you to listen on a given or random port locally, and have data forwarded to and from given ports in the pod.

Support for port forwarding is built into the CLI:

```
$ oc port-forward <pod> [local_port:<remote_port> [::<remote_port>]]
```
The CLI listens on each local port specified by the user, forwarding using the protocol described below.

Ports may be specified using the following formats:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>The client listens on port 5000 locally and forwards to 5000 in the pod.</td>
</tr>
<tr>
<td>6000:5000</td>
<td>The client listens on port 6000 locally and forwards to 5000 in the pod.</td>
</tr>
<tr>
<td>:5000 or 0:5000</td>
<td>The client selects a free local port and forwards to 5000 in the pod.</td>
</tr>
</tbody>
</table>

OpenShift Container Platform handles port-forward requests from clients. Upon receiving a request, OpenShift Container Platform upgrades the response and waits for the client to create port-forwarding streams. When OpenShift Container Platform receives a new stream, it copies data between the stream and the pod’s port.

Architecturally, there are options for forwarding to a pod’s port. The supported OpenShift Container Platform implementation invokes `nsenter` directly on the node host to enter the pod’s network namespace, then invokes `socat` to copy data between the stream and the pod’s port. However, a custom implementation could include running a helper pod that then runs `nsenter` and `socat`, so that those binaries are not required to be installed on the host.

### 6.8.2. Using port forwarding

You can use the CLI to port-forward one or more local ports to a pod.

**Procedure**

Use the following command to listen on the specified port in a pod:

```
$ oc port-forward <pod> [<local_port>:]<remote_port> [...[<local_port_n>:]<remote_port_n>]
```

For example:

- Use the following command to listen on ports 5000 and 6000 locally and forward data to and from ports 5000 and 6000 in the pod:

```
$ oc port-forward <pod> 5000 6000
```

**Example output**

```
Forwarding from 127.0.0.1:5000 -> 5000
Forwarding from [::1]:5000 -> 5000
Forwarding from 127.0.0.1:6000 -> 6000
Forwarding from [::1]:6000 -> 6000
```

- Use the following command to listen on port 8888 locally and forward to 5000 in the pod:

```
$ oc port-forward <pod> 8888:5000
```

**Example output**

```
Forwarding from 127.0.0.1:8888 -> 5000
Forwarding from [::1]:8888 -> 5000
```
Use the following command to listen on a free port locally and forward to 5000 in the pod:

```
$ oc port-forward <pod> :5000
```

Example output

```
Forwarding from 127.0.0.1:8888 -> 5000
Forwarding from [::1]:8888 -> 5000
```

Or:

```
$ oc port-forward <pod> 0:5000
```

### 6.8.3. Protocol for initiating port forwarding from a client

Clients initiate port forwarding to a pod by issuing a request to the Kubernetes API server:

```
/proxy/nodes/<node_name>/portForward/<namespace>/<pod>
```

In the above URL:

- `<node_name>` is the FQDN of the node.
- `<namespace>` is the namespace of the target pod.
- `<pod>` is the name of the target pod.

For example:

```
/proxy/nodes/node123.openshift.com/portForward/myns/mypod
```

After sending a port forward request to the API server, the client upgrades the connection to one that supports multiplexed streams; the current implementation uses Hypertext Transfer Protocol Version 2 (HTTP/2).

The client creates a stream with the `port` header containing the target port in the pod. All data written to the stream is delivered via the kubelet to the target pod and port. Similarly, all data sent from the pod for that forwarded connection is delivered back to the same stream in the client.

The client closes all streams, the upgraded connection, and the underlying connection when it is finished with the port forwarding request.

### 6.9. USING SYSCTLs IN CONTAINERS

Sysctl settings are exposed through Kubernetes, allowing users to modify certain kernel parameters at runtime. Only syseets that are namespaced can be set independently on pods. If a sysctl is not namespaced, called node-level, you must use another method of setting the sysctl, such as by using the Node Tuning Operator.

Network syseets are a special category of sysctl. Network syseets include:
- System-wide sysctls, for example `net.ipv4.ip_local_port_range`, that are valid for all networking. You can set these independently for each pod on a node.

- Interface-specific sysctls, for example `net.ipv4.conf.eth0.accept_local`, that only apply to a specific interface. You cannot set these independently for each pod on a node. You set these by using a configuration in the `tuning-cni` after the network interfaces are created.

Moreover, only those sysctls considered safe are whitelisted by default; you can manually enable other unsafe sysctls on the node to be available to the user.

Additional resources

- Node Tuning Operator

### 6.9.1. About sysctls

In Linux, the sysctl interface allows an administrator to modify kernel parameters at runtime. Parameters are available from the `/proc/sys/` virtual process file system. The parameters cover various subsystems, such as:

- kernel (common prefix: `kernel`)
- networking (common prefix: `net`)
- virtual memory (common prefix: `vm`)
- MDADM (common prefix: `dev`)

More subsystems are described in Kernel documentation. To get a list of all parameters, run:

```
$ sudo sysctl -a
```

### 6.9.2. Namespaced and node-level sysctls

A number of sysctls are namespaced in the Linux kernels. This means that you can set them independently for each pod on a node. Being namespaced is a requirement for sysctls to be accessible in a pod context within Kubernetes.

The following sysctls are known to be namespaced:

- `kernel.shm*`
- `kernel.msg*`
- `kernel.sem`
- `fs.mqueue.*`

Additionally, most of the sysctls in the `net.*` group are known to be namespaced. Their namespace adoption differs based on the kernel version and distributor.

Sysctls that are not namespaced are called node-level and must be set manually by the cluster administrator, either by means of the underlying Linux distribution of the nodes, such as by modifying the `/etc/sysctls.conf` file, or by using a daemon set with privileged containers. You can use the Node Tuning Operator to set node-level sysctls.
Consider marking nodes with special sysctls as tainted. Only schedule pods onto them that need those sysctl settings. Use the taints and toleration feature to mark the nodes.

### 6.9.3. Safe and unsafe sysctls

Sysctls are grouped into **safe** and **unsafe** sysctls.

For system-wide sysctls to be considered safe, they must be namespaced. A namespaced sysctl ensures there is isolation between namespaces and therefore pods. If you set a sysctl for one pod it must not add any of the following:

- Influence any other pod on the node
- Harm the node health
- Gain CPU or memory resources outside of the resource limits of a pod

**NOTE**

Being namespaced alone is not sufficient for the sysctl to be considered safe.

Any sysctl that is not added to the allowed list on OpenShift Container Platform is considered unsafe for OpenShift Container Platform.

Unsafe sysctls are not allowed by default. For system-wide sysctls the cluster administrator must manually enable them on a per-node basis. Pods with disabled unsafe sysctls are scheduled but do not launch.

**NOTE**

You cannot manually enable interface-specific unsafe sysctls.

OpenShift Container Platform adds the following system-wide and interface-specific safe sysctls to an allowed safe list:

**Table 6.4. System-wide safe sysctls**

<table>
<thead>
<tr>
<th>sysctl</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kernel.shm_rmid_forced</td>
<td>When set to 1, all shared memory objects in current IPC namespace are automatically forced to use IPC_RMID. For more information, see <a href="#">shm_rmid_forced</a>.</td>
</tr>
<tr>
<td>net.ipv4.ip_local_port_range</td>
<td>Defines the local port range that is used by TCP and UDP to choose the local port. The first number is the first port number, and the second number is the last local port number. If possible, it is better if these numbers have different parity (one even and one odd value). They must be greater than or equal to <a href="#">ip_unprivileged_port_start</a>. The default values are 32768 and 60999 respectively. For more information, see <a href="#">ip_local_port_range</a>.</td>
</tr>
</tbody>
</table>
When `net.ipv4.tcp_syncookies` is set, the kernel handles TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. This functionality allows the system to keep accepting valid connections, even if under a denial-of-service attack. For more information, see `tcp_syncookies`.

This restricts `ICMP_PROTO` datagram sockets to users in the group range. The default is `1 0`, meaning that nobody, not even root, can create ping sockets. For more information, see `ping_group_range`.

This defines the first unprivileged port in the network namespace. To disable all privileged ports, set this to `0`. Privileged ports must not overlap with the `ip_local_port_range`. For more information, see `ip_unprivileged_port_start`.

| `net.ipv4.tcp_syncookies` | When `net.ipv4.tcp_syncookies` is set, the kernel handles TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. This functionality allows the system to keep accepting valid connections, even if under a denial-of-service attack. For more information, see `tcp_syncookies`.
| `net.ipv4.ping_group_range` | This restricts `ICMP_PROTO` datagram sockets to users in the group range. The default is `1 0`, meaning that nobody, not even root, can create ping sockets. For more information, see `ping_group_range`.
| `net.ipv4.ip_unprivileged_port_start` | This defines the first unprivileged port in the network namespace. To disable all privileged ports, set this to `0`. Privileged ports must not overlap with the `ip_local_port_range`. For more information, see `ip_unprivileged_port_start`.

### Table 6.5. Interface-specific safe sysctls

<table>
<thead>
<tr>
<th><code>sysctl</code></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>net.ipv4.conf.IFNAME.accept_ra</code></td>
<td>Accept IPv4 Router Advertisements; autoconfigure using them. It also determines whether or not to transmit router solicitations. Router solicitations are transmitted only if the functional setting is to accept router advertisements.</td>
</tr>
<tr>
<td><code>net.ipv4.conf.IFNAME.accept_redirects</code></td>
<td>Accept IPv4 ICMP redirect messages.</td>
</tr>
<tr>
<td><code>net.ipv4.conf.IFNAME.accept_source_route</code></td>
<td>Accept IPv4 packets with strict source route (SRR) option.</td>
</tr>
</tbody>
</table>
| `net.ipv4.conf.IFNAME.arp_accept` | Define behavior for gratuitous ARP frames with an IPv4 address that is not already present in the ARP table:

- **0** - Do not create new entries in the ARP table.
- **1** - Create new entries in the ARP table. |
| `net.ipv4.conf.IFNAME.arp_notify` | Define mode for notification of IPv4 address and device changes. |
| `net.ipv4.conf.IFNAME.disable_policy` | Disable IPSEC policy (SPD) for this IPv4 interface. |
| `net.ipv4.conf.IFNAME.security_redirects` | Accept ICMP redirect messages only to gateways listed in the interface’s current gateway list. |
### sysctl

<table>
<thead>
<tr>
<th>sysctl</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net.ipv4.conf.IFNAME.send_redirects</td>
<td>Send redirects is enabled only if the node acts as a router. That is, a host should not send an ICMP redirect message. It is used by routers to notify the host about a better routing path that is available for a particular destination.</td>
</tr>
<tr>
<td>net.ipv6.conf.IFNAME.accept_ra</td>
<td>Accept IPv6 Router advertisements; autoconfigure using them. It also determines whether or not to transmit router solicitations. Router solicitations are transmitted only if the functional setting is to accept router advertisements.</td>
</tr>
<tr>
<td>net.ipv6.conf.IFNAME.accept_redirects</td>
<td>Accept IPv6 ICMP redirect messages.</td>
</tr>
<tr>
<td>net.ipv6.conf.IFNAME.accept_source_route</td>
<td>Accept IPv6 packets with SRR option.</td>
</tr>
<tr>
<td>net.ipv6.conf.IFNAME.arp_accept</td>
<td>Define behavior for gratuitous ARP frames with an IPv6 address that is not already present in the ARP table:</td>
</tr>
<tr>
<td></td>
<td>- 0 - Do not create new entries in the ARP table.</td>
</tr>
<tr>
<td></td>
<td>- 1 - Create new entries in the ARP table.</td>
</tr>
<tr>
<td>net.ipv6.conf.IFNAME.arp_notify</td>
<td>Define mode for notification of IPv6 address and device changes.</td>
</tr>
<tr>
<td>net.ipv6.neigh.IFNAME.base_reachable_time_ms</td>
<td>This parameter controls the hardware address to IP mapping lifetime in the neighbour table for IPv6.</td>
</tr>
<tr>
<td>net.ipv6.neigh.IFNAME.retrans_time_ms</td>
<td>Set the retransmit timer for neighbor discovery messages.</td>
</tr>
</tbody>
</table>

**NOTE**

The interface name is represented by the `IFNAME` token, and is replaced with the actual name of the interface at runtime.

Additional resources

- [Linux networking documentation](#)

### 6.9.4. Starting a pod with safe sysctls

You can set sysctls on pods using the pod’s `securityContext`. The `securityContext` applies to all containers in the same pod.

Safe sysctls are allowed by default.
This example uses the pod `securityContext` to set the following safe sysctls:

- `kernel.shm_rmid_forced`
- `net.ipv4.ip_local_port_range`
- `net.ipv4.tcp_syncookies`
- `net.ipv4.ping_group_range`

**WARNING**
To avoid destabilizing your operating system, modify sysctl parameters only after you understand their effects.

Use this procedure to start a pod with the configured sysctl settings.

**NOTE**
In most cases you modify an existing pod definition and add the `securityContext` spec.

**Procedure**

1. Create a YAML file `sysctl_pod.yaml` that defines an example pod and add the `securityContext` spec, as shown in the following example:

```yaml
apiVersion: v1
class: Pod
metadata:
  name: sysctl-example
  namespace: default
spec:
  containers:
    - name: podexample
      image: centos
      command: ['bin/bash', '-c', 'sleep INF']
      securityContext:
        runAsUser: 2000
        runAsGroup: 3000
        allowPrivilegeEscalation: false
        capabilities:
          drop: ['ALL']
        securityContext:
          runAsNonRoot: true
        seccompProfile:
          type: RuntimeDefault
      sysctls:
        - name: kernel.shm_rmid_forced
          value: "1"
        - name: net.ipv4.ip_local_port_range
```

CHAPTER 6. WORKING WITH CONTAINERS

309
runAsUser controls which user ID the container is run with.

runAsGroup controls which primary group ID the containers is run with.

allowPrivilegeEscalation determines if a pod can request to allow privilege escalation. If unspecified, it defaults to true. This boolean directly controls whether the no_new_privs flag gets set on the container process.

capabilities permit privileged actions without giving full root access. This policy ensures all capabilities are dropped from the pod.

runAsNonRoot: true requires that the container will run with a user with any UID other than 0.

RuntimeDefault enables the default seccomp profile for a pod or container workload.

2. Create the pod by running the following command:

   $ oc apply -f sysctl_pod.yaml

3. Verify that the pod is created by running the following command:

   $ oc get pod

   **Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysctl-example</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>14s</td>
</tr>
</tbody>
</table>

4. Log in to the pod by running the following command:

   $ oc rsh sysctl-example

5. Verify the values of the configured sysctl flags. For example, find the value **kernel.shm_rmid_forced** by running the following command:

   `sh-4.4# sysctl kernel.shm_rmid_forced`

   **Expected output**

   kernel.shm_rmid_forced = 1

6.9.5. Starting a pod with unsafe sysctls
A pod with unsafe sysctls fails to launch on any node unless the cluster administrator explicitly enables unsafe sysctls for that node. As with node-level sysctls, use the taints and toleration feature or labels on nodes to schedule those pods onto the right nodes.

The following example uses the pod `securityContext` to set a safe sysctl `kernel.shm_rmid_forced` and two unsafe sysctls, `net.core.somaxconn` and `kernel.msgmax`. There is no distinction between safe and unsafe sysctls in the specification.

**WARNING**

To avoid destabilizing your operating system, modify sysctl parameters only after you understand their effects.

The following example illustrates what happens when you add safe and unsafe sysctls to a pod specification:

**Procedure**

1. Create a YAML file `sysctl-example-unsafe.yaml` that defines an example pod and add the `securityContext` specification, as shown in the following example:

   ```yaml
   apiVersion: v1
   kind: Pod
   metadata:
     name: sysctl-example-unsafe
   spec:
     containers:
     - name: podexample
       image: centos
       command: ["bin/bash", "-c", "sleep INF"]
       securityContext:
         runAsUser: 2000
         runAsGroup: 3000
         allowPrivilegeEscalation: false
         capabilities:
           drop: ["ALL"]
         securityContext:
           runAsNonRoot: true
       seccompProfile:
         type: RuntimeDefault
       sysctls:
         - name: kernel.shm_rmid_forced
           value: "0"
         - name: net.core.somaxconn
           value: "1024"
         - name: kernel.msgmax
           value: "65536"
   ```

2. Create the pod using the following command:
Verify that the pod is scheduled but does not deploy because unsafe sysctls are not allowed for the node using the following command:

```
$ oc get pod
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysctl-example-unsafe</td>
<td>0/1</td>
<td>SysctlForbidden</td>
<td>0</td>
<td>14s</td>
</tr>
</tbody>
</table>

### 6.9.6. Enabling unsafe sysctls

A cluster administrator can allow certain unsafe sysctls for very special situations such as high performance or real-time application tuning.

If you want to use unsafe sysctls, a cluster administrator must enable them individually for a specific type of node. The sysctls must be namespaced.

You can further control which sysctls can be set in pods by specifying lists of sysctls or sysctl patterns in the `forbiddenSysctls` and `allowedUnsafeSysctls` fields of the Security Context Constraints.

- The `forbiddenSysctls` option excludes specific sysctls.
- The `allowedUnsafeSysctls` option controls specific needs such as high performance or real-time application tuning.

**WARNING**

Due to their nature of being unsafe, the use of unsafe sysctls is at-your-own-risk and can lead to severe problems, such as improper behavior of containers, resource shortage, or breaking a node.

### Procedure

1. List existing MachineConfig objects for your OpenShift Container Platform cluster to decide how to label your machine config by running the following command:

```
$ oc get machineconfigpool
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>CONFIG</th>
<th>UPDATED</th>
<th>UPDATING</th>
<th>DEGRADED</th>
<th>MACHINECOUNT</th>
<th>READYMACHINECOUNT</th>
<th>UPDATEDMACHINECOUNT</th>
<th>DEGRADEDMACHINECOUNT</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>rendered-master-bfb92f0cd1684e54d8e234ab7423cc96</td>
<td>True</td>
<td>False</td>
<td>False</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Add a label to the machine config pool where the containers with the unsafe sysctls will run by running the following command:

```bash
$ oc label machineconfigpool worker custom-kubelet=sysctl
```

3. Create a YAML file `set-sysctl-worker.yaml` that defines a `KubeletConfig` custom resource (CR):

```yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: custom-kubelet
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: sysctl
  kubeletConfig:
    allowedUnsafeSysctls:
      - "kernel.msg*"
      - "net.core.somaxconn"
```

1. Specify the label from the machine config pool.
2. List the unsafe sysctls you want to allow.

4. Create the object by running the following command:

```bash
$ oc apply -f set-sysctl-worker.yaml
```

5. Wait for the Machine Config Operator to generate the new rendered configuration and apply it to the machines by running the following command:

```bash
$ oc get machineconfigpool worker -w
```

After some minutes the **UPDATING** status changes from True to False:

<table>
<thead>
<tr>
<th>NAME</th>
<th>CONFIG</th>
<th>UPDATED</th>
<th>UPDATING</th>
<th>DEGRADED</th>
</tr>
</thead>
<tbody>
<tr>
<td>worker</td>
<td>rendered-worker-21b6cb9a0f8919c88caf39db80ac1f7e</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td></td>
<td>True 3rd party</td>
<td>42m</td>
<td></td>
<td></td>
</tr>
<tr>
<td>worker</td>
<td>rendered-worker-f1704a00fc6f30d3a7e9a15fd68a800</td>
<td>False</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td></td>
<td>True 3rd party</td>
<td>71m</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. Create a YAML file `sysctl-example-safe-unsafe.yaml` that defines an example pod and add the **securityContext** spec, as shown in the following example:
Create the pod by running the following command:

```
$ oc apply -f sysctl-example-safe-unsafe.yaml
```

**Expected output**

Warning: would violate PodSecurity "restricted:latest": forbidden sysctls (net.core.somaxconn, kernel.msgmax)

```
pod/sysctl-example-safe-unsafe created
```

Verify that the pod is created by running the following command:

```
$ oc get pod
```

**Example output**

```
NAME                         READY   STATUS    RESTARTS   AGE
sysctl-example-safe-unsafe   1/1     Running   0          19s
```

Log in to the pod by running the following command:

```
$ oc rsh sysctl-example-safe-unsafe
```

Verify the values of the configured sysctl flags. For example, find the value `net.core.somaxconn` by running the following command:
sh-4.4# sysctl net.core.somaxconn

Expected output

net.core.somaxconn = 1024

The unsafe sysctl is now allowed and the value is set as defined in the `securityContext` spec of the updated pod specification.

6.9.7. Additional resources

- Setting interface-level network sysctls
CHAPTER 7. WORKING WITH CLUSTERS

7.1. VIEWING SYSTEM EVENT INFORMATION IN AN OPENSHIFT CONTAINER PLATFORM CLUSTER

Events in OpenShift Container Platform are modeled based on events that happen to API objects in an OpenShift Container Platform cluster.

7.1.1. Understanding events

Events allow OpenShift Container Platform to record information about real-world events in a resource-agnostic manner. They also allow developers and administrators to consume information about system components in a unified way.

7.1.2. Viewing events using the CLI

You can get a list of events in a given project using the CLI.

Procedure

- To view events in a project use the following command:

  ```bash
  $ oc get events [-n <project>]
  ```
  
  The name of the project.

  For example:

  ```bash
  $ oc get events -n openshift-config
  ```

Example output

<table>
<thead>
<tr>
<th>LAST SEEN</th>
<th>TYPE</th>
<th>REASON</th>
<th>OBJECT</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>97m</td>
<td>Normal</td>
<td>Scheduled</td>
<td>pod/dapi-env-test-pod</td>
<td>Successfully assigned openshift-config/dapi-env-test-pod to ip-10-0-171-202.ec2.internal</td>
</tr>
<tr>
<td>97m</td>
<td>Normal</td>
<td>Pulling</td>
<td>pod/dapi-env-test-pod</td>
<td>pulling image &quot;gcr.io/google_containers/busybox&quot;</td>
</tr>
<tr>
<td>97m</td>
<td>Normal</td>
<td>Pulled</td>
<td>pod/dapi-env-test-pod</td>
<td>Successfully pulled image &quot;gcr.io/google_containers/busybox&quot;</td>
</tr>
<tr>
<td>97m</td>
<td>Normal</td>
<td>Created</td>
<td>pod/dapi-env-test-pod</td>
<td>Created container</td>
</tr>
<tr>
<td>9m5s</td>
<td>Warning</td>
<td>FailedCreatePodSandBox</td>
<td>pod/dapi-volume-test-pod</td>
<td>Failed create pod sandbox: rpc error: code = Unknown desc = failed to create pod network sandbox k8s_dapi-volume-test-pod_openshift-config_6bc60c1f-452e-11e9-9140-0eecc59c2366_0(748c7a40db3d08c07f4f9ea774bd5eefe5f0d5090a242432a733ee66ba9e22): Multus: Err adding pod to network &quot;openshift-sdn&quot;: cannot set &quot;openshift-sdn&quot; ifname to &quot;eth0&quot;: no nets: failed to Stats &quot;/proc/33366/ns/net&quot;: no such file or directory</td>
</tr>
<tr>
<td>8m31s</td>
<td>Normal</td>
<td>Scheduled</td>
<td>pod/dapi-volume-test-pod</td>
<td>Successfully assigned openshift-config/dapi-volume-test-pod to ip-10-0-171-202.ec2.internal</td>
</tr>
</tbody>
</table>

- To view events in your project from the OpenShift Container Platform console.

  1. Launch the OpenShift Container Platform console.
2. Click Home → Events and select your project.

3. Move to resource that you want to see events. For example: Home → Projects → <project-name> → <resource-name>. Many objects, such as pods and deployments, have their own Events tab as well, which shows events related to that object.

### 7.1.3. List of events

This section describes the events of OpenShift Container Platform.

#### Table 7.1. Configuration events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FailedValidation</td>
<td>Failed pod configuration validation.</td>
</tr>
</tbody>
</table>

#### Table 7.2. Container events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackOff</td>
<td>Back-off restarting failed the container.</td>
</tr>
<tr>
<td>Created</td>
<td>Container created.</td>
</tr>
<tr>
<td>Failed</td>
<td>Pull/Create/Start failed.</td>
</tr>
<tr>
<td>Killing</td>
<td>Killing the container.</td>
</tr>
<tr>
<td>Started</td>
<td>Container started.</td>
</tr>
<tr>
<td>Preempting</td>
<td>Preempting other pods.</td>
</tr>
<tr>
<td>ExceededGrace Period</td>
<td>Container runtime did not stop the pod within specified grace period.</td>
</tr>
</tbody>
</table>

#### Table 7.3. Health events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unhealthy</td>
<td>Container is unhealthy.</td>
</tr>
</tbody>
</table>

#### Table 7.4. Image events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackOff</td>
<td>Back off Ctr Start, image pull.</td>
</tr>
</tbody>
</table>
## Table 7.5. Image Manager events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ErrImageNeverPull</strong></td>
<td>The image’s NeverPull Policy is violated.</td>
</tr>
<tr>
<td><strong>Failed</strong></td>
<td>Failed to pull the image.</td>
</tr>
<tr>
<td><strong>InspectFailed</strong></td>
<td>Failed to inspect the image.</td>
</tr>
<tr>
<td><strong>Pulled</strong></td>
<td>Successfully pulled the image or the container image is already present on the machine.</td>
</tr>
<tr>
<td><strong>Pulling</strong></td>
<td>Pulling the image.</td>
</tr>
</tbody>
</table>

## Table 7.6. Node events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FreeDiskSpaceFailed</strong></td>
<td>Free disk space failed.</td>
</tr>
<tr>
<td><strong>InvalidDiskCapacity</strong></td>
<td>Invalid disk capacity.</td>
</tr>
<tr>
<td><strong>FailedMount</strong></td>
<td>Volume mount failed.</td>
</tr>
<tr>
<td><strong>HostNetworkNotSupported</strong></td>
<td>Host network not supported.</td>
</tr>
<tr>
<td><strong>HostPortConflict</strong></td>
<td>Host/port conflict.</td>
</tr>
<tr>
<td><strong>KubeletSetupFailed</strong></td>
<td>Kubelet setup failed.</td>
</tr>
<tr>
<td><strong>NilShaper</strong></td>
<td>Undefined shaper.</td>
</tr>
<tr>
<td><strong>NodeNotReady</strong></td>
<td>Node is not ready.</td>
</tr>
<tr>
<td><strong>NodeNotSchedulable</strong></td>
<td>Node is not schedulable.</td>
</tr>
<tr>
<td><strong>NodeReady</strong></td>
<td>Node is ready.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>NodeSchedulable</td>
<td>Node is schedulable.</td>
</tr>
<tr>
<td>NodeSelectorMismatching</td>
<td>Node selector mismatch.</td>
</tr>
<tr>
<td>OutOfDisk</td>
<td>Out of disk.</td>
</tr>
<tr>
<td>Rebooted</td>
<td>Node rebooted.</td>
</tr>
<tr>
<td>Starting</td>
<td>Starting kubelet.</td>
</tr>
<tr>
<td>FailedAttachVolume</td>
<td>Failed to attach volume.</td>
</tr>
<tr>
<td>FailedDetachVolume</td>
<td>Failed to detach volume.</td>
</tr>
<tr>
<td>VolumeResizeFailed</td>
<td>Failed to expand/reduce volume.</td>
</tr>
<tr>
<td>VolumeResizeSuccessful</td>
<td>Successfully expanded/reduced volume.</td>
</tr>
<tr>
<td>FileSystemResizeFailed</td>
<td>Failed to expand/reduce file system.</td>
</tr>
<tr>
<td>FileSystemResizeSuccessful</td>
<td>Successfully expanded/reduced file system.</td>
</tr>
<tr>
<td>FailedUnmount</td>
<td>Failed to unmount volume.</td>
</tr>
<tr>
<td>FailedMapVolume</td>
<td>Failed to map a volume.</td>
</tr>
<tr>
<td>FailedUnmapDevice</td>
<td>Failed unmaped device.</td>
</tr>
<tr>
<td>AlreadyMountedVolume</td>
<td>Volume is already mounted.</td>
</tr>
<tr>
<td>SuccessfulDetachVolume</td>
<td>Volume is successfully detached.</td>
</tr>
<tr>
<td>SuccessfulMountVolume</td>
<td>Volume is successfully mounted.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>SuccessfulUnmountVolume</td>
<td>Volume is successfully unmounted.</td>
</tr>
<tr>
<td>ContainerGCFailed</td>
<td>Container garbage collection failed.</td>
</tr>
<tr>
<td>ImageGCFailed</td>
<td>Image garbage collection failed.</td>
</tr>
<tr>
<td>FailedNodeAllocatableEnforcement</td>
<td>Failed to enforce System Reserved Cgroup limit.</td>
</tr>
<tr>
<td>NodeAllocatableEnforced</td>
<td>Enforced System Reserved Cgroup limit.</td>
</tr>
<tr>
<td>UnsupportedMountOption</td>
<td>Unsupported mount option.</td>
</tr>
<tr>
<td>SandboxChanged</td>
<td>Pod sandbox changed.</td>
</tr>
<tr>
<td>FailedCreatePodSandBox</td>
<td>Failed to create pod sandbox.</td>
</tr>
<tr>
<td>FailedPodSandboxStatus</td>
<td>Failed pod sandbox status.</td>
</tr>
</tbody>
</table>

Table 7.7. Pod worker events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FailedSync</td>
<td>Pod sync failed.</td>
</tr>
</tbody>
</table>

Table 7.8. System Events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SystemOOM</td>
<td>There is an OOM (out of memory) situation on the cluster.</td>
</tr>
</tbody>
</table>

Table 7.9. Pod events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FailedKillPod</td>
<td>Failed to stop a pod.</td>
</tr>
</tbody>
</table>
Failed to create a pod container.

Failed to make pod data directories.

Network is not ready.

Error creating: <error-msg>.

Created pod: <pod-name>.

Error deleting: <error-msg>.

Deleted pod: <pod-id>.

Table 7.10. Horizontal Pod AutoScaler events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FailedCreatePodContainer</td>
<td>Failed to create a pod container.</td>
</tr>
<tr>
<td>Failed</td>
<td>Failed to make pod data directories.</td>
</tr>
<tr>
<td>NetworkNotReady</td>
<td>Network is not ready.</td>
</tr>
<tr>
<td>FailedCreate</td>
<td>Error creating: &lt;error-msg&gt;.</td>
</tr>
<tr>
<td>SuccessfulCreate</td>
<td>Created pod: &lt;pod-name&gt;.</td>
</tr>
<tr>
<td>FailedDelete</td>
<td>Error deleting: &lt;error-msg&gt;.</td>
</tr>
<tr>
<td>SuccessfulDelete</td>
<td>Deleted pod: &lt;pod-id&gt;.</td>
</tr>
</tbody>
</table>

Table: | Name | Description |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SelectorRequired</td>
<td>Selector is required.</td>
<td></td>
</tr>
<tr>
<td>InvalidSelector</td>
<td>Could not convert selector into a corresponding internal selector object.</td>
<td></td>
</tr>
<tr>
<td>FailedGetObjectMetric</td>
<td>HPA was unable to compute the replica count.</td>
<td></td>
</tr>
<tr>
<td>InvalidMetricSourceType</td>
<td>Unknown metric source type.</td>
<td></td>
</tr>
<tr>
<td>ValidMetricFound</td>
<td>HPA was able to successfully calculate a replica count.</td>
<td></td>
</tr>
<tr>
<td>FailedConvertHPA</td>
<td>Failed to convert the given HPA.</td>
<td></td>
</tr>
<tr>
<td>FailedGetScale</td>
<td>HPA controller was unable to get the target’s current scale.</td>
<td></td>
</tr>
<tr>
<td>SucceededGetScale</td>
<td>HPA controller was able to get the target’s current scale.</td>
<td></td>
</tr>
<tr>
<td>FailedComputeMetricsReplicas</td>
<td>Failed to compute desired number of replicas based on listed metrics.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>FailedRescale</td>
<td>New size: <code>&lt;size&gt;</code>; reason: <code>&lt;msg&gt;</code>; error: <code>&lt;error-msg&gt;</code>.</td>
<td></td>
</tr>
<tr>
<td>SuccessfulRescale</td>
<td>New size: <code>&lt;size&gt;</code>; reason: <code>&lt;msg&gt;</code>.</td>
<td></td>
</tr>
<tr>
<td>FailedUpdateStatus</td>
<td>Failed to update status.</td>
<td></td>
</tr>
</tbody>
</table>

Table 7.11. Network events (openshift-sdn)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting</td>
<td>Starting OpenShift SDN.</td>
</tr>
<tr>
<td>NetworkFailed</td>
<td>The pod’s network interface has been lost and the pod will be stopped.</td>
</tr>
</tbody>
</table>

Table 7.12. Network events (kube-proxy)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NeedPods</td>
<td>The service-port <code>&lt;serviceName&gt;:&lt;port&gt;</code> needs pods.</td>
</tr>
</tbody>
</table>

Table 7.13. Volume events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FailedBinding</td>
<td>There are no persistent volumes available and no storage class is set.</td>
</tr>
<tr>
<td>VolumeMismatch</td>
<td>Volume size or class is different from what is requested in claim.</td>
</tr>
<tr>
<td>VolumeFailedRecycle</td>
<td>Error creating recycler pod.</td>
</tr>
<tr>
<td>VolumeRecycled</td>
<td>Occurs when volume is recycled.</td>
</tr>
<tr>
<td>RecyclerPod</td>
<td>Occurs when pod is recycled.</td>
</tr>
<tr>
<td>VolumeDelete</td>
<td>Occurs when volume is deleted.</td>
</tr>
<tr>
<td>VolumeFailedDelete</td>
<td>Error when deleting the volume.</td>
</tr>
</tbody>
</table>
ExternalProvisioning Occurs when volume for the claim is provisioned either manually or via external software.

ProvisioningFailed Failed to provision volume.

ProvisioningCleanupFailed Error cleaning provisioned volume.

ProvisioningSucceeded Occurs when the volume is provisioned successfully.

WaitForFirstConsumer Delay binding until pod scheduling.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FailedPostStartHook Handler failed for pod start.</td>
<td></td>
</tr>
<tr>
<td>FailedPreStopHook  Handler failed for pre-stop.</td>
<td></td>
</tr>
<tr>
<td>UnfinishedPreStopHook Pre-stop hook unfinished.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeploymentCancellationFailed Failed to cancel deployment.</td>
<td></td>
</tr>
<tr>
<td>DeploymentCancelled Canceled deployment.</td>
<td></td>
</tr>
<tr>
<td>DeploymentCreated Created new replication controller.</td>
<td></td>
</tr>
<tr>
<td>IngressIPRangeFull No available Ingress IP to allocate to service.</td>
<td></td>
</tr>
</tbody>
</table>
Table 7.16. Scheduler events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FailedScheduling</td>
<td>Failed to schedule pod: <code>&lt;pod-namespace&gt;/&lt;pod-name&gt;</code>. This event is raised for multiple reasons, for example: <code>AssumePodVolumes</code> failed, Binding rejected etc.</td>
</tr>
<tr>
<td>Preempted</td>
<td>By <code>&lt;preemptor-namespace&gt;/&lt;preemptor-name&gt;</code> on node <code>&lt;node-name&gt;</code>.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>Successfully assigned <code>&lt;pod-name&gt;</code> to <code>&lt;node-name&gt;</code>.</td>
</tr>
</tbody>
</table>

Table 7.17. Daemon set events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SelectingAll</td>
<td>This daemon set is selecting all pods. A non-empty selector is required.</td>
</tr>
<tr>
<td>FailedPlacement</td>
<td>Failed to place pod on <code>&lt;node-name&gt;</code>.</td>
</tr>
<tr>
<td>FailedDaemonPod</td>
<td>Found failed daemon pod <code>&lt;pod-name&gt;</code> on node <code>&lt;node-name&gt;</code>, will try to kill it.</td>
</tr>
</tbody>
</table>

Table 7.18. LoadBalancer service events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreatingLoadBalancerFailed</td>
<td>Error creating load balancer.</td>
</tr>
<tr>
<td>DeletingLoadBalancer</td>
<td>Deleting load balancer.</td>
</tr>
<tr>
<td>EnsuringLoadBalancer</td>
<td>Ensuring load balancer.</td>
</tr>
<tr>
<td>EnsuredLoadBalancer</td>
<td>Ensured load balancer.</td>
</tr>
<tr>
<td>UnAvailableLoadBalancer</td>
<td>There are no available nodes for <code>LoadBalancer</code> service.</td>
</tr>
<tr>
<td>LoadBalancerSourceRanges</td>
<td>Lists the new <code>LoadBalancerSourceRanges</code>. For example, <code>&lt;old-source-range&gt; → &lt;new-source-range&gt;</code>.</td>
</tr>
<tr>
<td>LoadbalancerIP</td>
<td>Lists the new IP address. For example, <code>&lt;old-ip&gt; → &lt;new-ip&gt;</code>.</td>
</tr>
<tr>
<td>ExternalIP</td>
<td>Lists external IP address. For example, <code>Added: &lt;external-ip&gt;</code>.</td>
</tr>
</tbody>
</table>
### 7.2. ESTIMATING THE NUMBER OF PODS YOUR OPENSIFT CONTAINER PLATFORM NODES CAN HOLD

As a cluster administrator, you can use the cluster capacity tool to view the number of pods that can be scheduled to increase the current resources before they become exhausted, and to ensure any future pods can be scheduled. This capacity comes from an individual node host in a cluster, and includes CPU, memory, disk space, and others.

#### 7.2.1. Understanding the OpenShift Container Platform cluster capacity tool

The cluster capacity tool simulates a sequence of scheduling decisions to determine how many instances of an input pod can be scheduled on the cluster before it is exhausted of resources to provide a more accurate estimation.

**NOTE**

The remaining allocatable capacity is a rough estimation, because it does not count all of the resources being distributed among nodes. It analyzes only the remaining resources and estimates the available capacity that is still consumable in terms of a number of instances of a pod with given requirements that can be scheduled in a cluster.

Also, pods might only have scheduling support on particular sets of nodes based on its selection and affinity criteria. As a result, the estimation of which remaining pods a cluster can schedule can be difficult.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
<td>Lists the new UID. For example, <code>&lt;old-service-uid&gt; → &lt;new-service-uid&gt;</code>.</td>
</tr>
<tr>
<td>ExternalTrafficPolicy</td>
<td>Lists the new ExternalTrafficPolicy. For example, <code>&lt;old-policy&gt; → &lt;new-policy&gt;</code>.</td>
</tr>
<tr>
<td>HealthCheckNodePort</td>
<td>Lists the new HealthCheckNodePort. For example, <code>&lt;old-node-port&gt; → new-node-port&gt;</code>.</td>
</tr>
<tr>
<td>UpdatedLoadBalancer</td>
<td>Updated load balancer with new hosts.</td>
</tr>
<tr>
<td>LoadBalancerUpdateFailed</td>
<td>Error updating load balancer with new hosts.</td>
</tr>
<tr>
<td>DeletingLoadBalancer</td>
<td>Deleting load balancer.</td>
</tr>
<tr>
<td>DeletingLoadBalancerFailed</td>
<td>Error deleting load balancer.</td>
</tr>
<tr>
<td>DeletedLoadBalancer</td>
<td>Deleted load balancer.</td>
</tr>
</tbody>
</table>
You can run the cluster capacity analysis tool as a stand-alone utility from the command line, or as a job in a pod inside an OpenShift Container Platform cluster. Running it as job inside of a pod enables you to run it multiple times without intervention.

### 7.2.2. Running the cluster capacity tool on the command line

You can run the OpenShift Container Platform cluster capacity tool from the command line to estimate the number of pods that can be scheduled onto your cluster.

**Prerequisites**

- Run the OpenShift Cluster Capacity Tool, which is available as a container image from the Red Hat Ecosystem Catalog.
- Create a sample Pod spec file, which the tool uses for estimating resource usage. The podspec specifies its resource requirements as limits or requests. The cluster capacity tool takes the pod’s resource requirements into account for its estimation analysis.

An example of the Pod spec input is:

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: small-pod
labels:
  app: guestbook
tier: frontend
spec:
  containers:
  - name: php-redis
    image: gcr.io/google-samples/gb-frontend:v4
    imagePullPolicy: Always
    resources:
      limits:
        cpu: 150m
        memory: 100Mi
      requests:
        cpu: 150m
        memory: 100Mi
```

**Procedure**

To use the cluster capacity tool on the command line:

1. From the terminal, log in to the Red Hat Registry:

   ```
   $ podman login registry.redhat.io
   ```

2. Pull the cluster capacity tool image:

   ```
   $ podman pull registry.redhat.io/openshift4/ose-cluster-capacity
   ```

3. Run the cluster capacity tool:
You can also add the --verbose option to output a detailed description of how many pods can be scheduled on each node in the cluster.

Example output

small-pod pod requirements:
- CPU: 150m
- Memory: 100Mi

The cluster can schedule 88 instance(s) of the pod small-pod.

Termination reason: Unschedulable: 0/5 nodes are available: 2 Insufficient cpu, 3 node(s) had taint {node-role.kubernetes.io/master: }, that the pod didn’t tolerate.

Pod distribution among nodes:
small-pod
- 192.168.124.214: 45 instance(s)
- 192.168.124.120: 43 instance(s)

In the above example, the number of estimated pods that can be scheduled onto the cluster is 88.

7.2.3. Running the cluster capacity tool as a job inside a pod

Running the cluster capacity tool as a job inside of a pod has the advantage of being able to be run multiple times without needing user intervention. Running the cluster capacity tool as a job involves using a ConfigMap object.

Prerequisites

Download and install the cluster capacity tool.

Procedure

To run the cluster capacity tool:

1. Create the cluster role:

   $ cat << EOF| oc create -f -

Example output

kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: cluster-capacity-role
rules:
- apiGroups: [""]
  resources: ["pods", "nodes", "persistentvolumeclaims", "persistentvolumes", "services",]
2. Create the service account:

```
$ oc create sa cluster-capacity-sa
```

3. Add the role to the service account:

```
$ oc adm policy add-cluster-role-to-user cluster-capacity-role \
  system:serviceaccount:default:cluster-capacity-sa
```

4. Define and create the **Pod** spec:

```
apiVersion: v1
kind: Pod
metadata:
  name: small-pod
labels:
  app: guestbook
tier: frontend
spec:
  containers:
    - name: php-redis
      image: gcr.io/google-samples/gb-frontend:v4
      imagePullPolicy: Always
      resources:
        limits:
          cpu: 150m
          memory: 100Mi
        requests:
          cpu: 150m
          memory: 100Mi
EOF
```

5. The cluster capacity analysis is mounted in a volume using a **ConfigMap** object named `cluster-capacity-configmap` to mount input pod spec file `pod.yaml` into a volume `test-volume` at the path `/test-pod`.

   If you haven’t created a **ConfigMap** object, create one before creating the job:

```
$ oc create configmap cluster-capacity-configmap \
  --from-file=pod.yaml=pod.yaml
```

6. Create the job using the below example of a job specification file:
A required environment variable letting the cluster capacity tool know that it is running inside a cluster as a pod.

The pod.yaml key of the ConfigMap object is the same as the Pod spec file name, though it is not required. By doing this, the input pod spec file can be accessed inside the pod as /test-pod/pod.yaml.

7. Run the cluster capacity image as a job in a pod:

   $ oc create -f cluster-capacity-job.yaml

8. Check the job logs to find the number of pods that can be scheduled in the cluster:

   $ oc logs jobs/cluster-capacity-job

Example output

small-pod pod requirements:
   - CPU: 150m
   - Memory: 100Mi
7.3. RESTRICT RESOURCE CONSUMPTION WITH LIMIT RANGES

By default, containers run with unbounded compute resources on an OpenShift Container Platform cluster. With limit ranges, you can restrict resource consumption for specific objects in a project:

- pods and containers: You can set minimum and maximum requirements for CPU and memory for pods and their containers.
- Image streams: You can set limits on the number of images and tags in an ImageStream object.
- Images: You can limit the size of images that can be pushed to an internal registry.
- Persistent volume claims (PVC): You can restrict the size of the PVCs that can be requested.

If a pod does not meet the constraints imposed by the limit range, the pod cannot be created in the namespace.

7.3.1. About limit ranges

A limit range, defined by a LimitRange object, restricts resource consumption in a project. In the project you can set specific resource limits for a pod, container, image, image stream, or persistent volume claim (PVC).

All requests to create and modify resources are evaluated against each LimitRange object in the project. If the resource violates any of the enumerated constraints, the resource is rejected.

The following shows a limit range object for all components: pod, container, image, image stream, or PVC. You can configure limits for any or all of these components in the same object. You create a different limit range object for each project where you want to control resources.

Sample limit range object for a container

```yaml
apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "resource-limits"
spec:
  limits:
    - type: "Container"
      max:
        cpu: "2"
        memory: "1Gi"
      min:
        cpu: "100m"
        memory: "4Mi"
```
7.3.1.1. About component limits

The following examples show limit range parameters for each component. The examples are broken out for clarity. You can create a single `LimitRange` object for any or all components as necessary.

7.3.1.1.1. Container limits

A limit range allows you to specify the minimum and maximum CPU and memory that each container in a pod can request for a specific project. If a container is created in the project, the container CPU and memory requests in the `Pod` spec must comply with the values set in the `LimitRange` object. If not, the pod does not get created.

- The container CPU or memory request and limit must be greater than or equal to the `min` resource constraint for containers that are specified in the `LimitRange` object.

- The container CPU or memory request and limit must be less than or equal to the `max` resource constraint for containers that are specified in the `LimitRange` object. If the `LimitRange` object defines a `max` CPU, you do not need to define a CPU `request` value in the `Pod` spec. But you must specify a CPU `limit` value that satisfies the maximum CPU constraint specified in the limit range.

- The ratio of the container limits to requests must be less than or equal to the `maxLimitRequestRatio` value for containers that is specified in the `LimitRange` object. If the `LimitRange` object defines a `maxLimitRequestRatio` constraint, any new containers must have both a `request` and a `limit` value. OpenShift Container Platform calculates the limit-to-request ratio by dividing the `limit` by the `request`. This value should be a non-negative integer greater than 1.

For example, if a container has `cpu: 500` in the `limit` value, and `cpu: 100` in the `request` value, the limit-to-request ratio for `cpu` is 5. This ratio must be less than or equal to the `maxLimitRequestRatio`.

If the `Pod` spec does not specify a container resource memory or limit, the `default` or `defaultRequest` CPU and memory values for containers specified in the limit range object are assigned to the container.

Container LimitRange object definition

```yaml
apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "resource-limits"
spec:
  limits:
  - type: "Container"
    max:
      cpu: "2"
```
The name of the LimitRange object.

The maximum amount of CPU that a single container in a pod can request.

The maximum amount of memory that a single container in a pod can request.

The minimum amount of CPU that a single container in a pod can request.

The minimum amount of memory that a single container in a pod can request.

The default amount of CPU that a container can use if not specified in the Pod spec.

The default amount of memory that a container can use if not specified in the Pod spec.

The default amount of CPU that a container can request if not specified in the Pod spec.

The default amount of memory that a container can request if not specified in the Pod spec.

The maximum limit-to-request ratio for a container.

### 7.3.1.1.2. Pod limits

A limit range allows you to specify the minimum and maximum CPU and memory limits for all containers across a pod in a given project. To create a container in the project, the container CPU and memory requests in the Pod spec must comply with the values set in the LimitRange object. If not, the pod does not get created.

If the Pod spec does not specify a container resource memory or limit, the default or defaultRequest CPU and memory values for containers specified in the limit range object are assigned to the container.

Across all containers in a pod, the following must hold true:

- The container CPU or memory request and limit must be greater than or equal to the min resource constraints for pods that are specified in the LimitRange object.

- The container CPU or memory request and limit must be less than or equal to the max resource constraints for pods that are specified in the LimitRange object.

- The ratio of the container limits to requests must be less than or equal to the maxLimitRequestRatio constraint specified in the LimitRange object.

**Pod LimitRange object definition**
The name of the limit range object.

The maximum amount of CPU that a pod can request across all containers.

The maximum amount of memory that a pod can request across all containers.

The minimum amount of CPU that a pod can request across all containers.

The minimum amount of memory that a pod can request across all containers.

The maximum limit-to-request ratio for a container.

7.3.1.1.3. Image limits

A LimitRange object allows you to specify the maximum size of an image that can be pushed to an internal registry.

When pushing images to an internal registry, the following must hold true:

- The size of the image must be less than or equal to the \texttt{max} size for images that is specified in the LimitRange object.

Image LimitRange object definition

```
apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "resource-limits"
spec:
  limits:
    - type: "Pod"
      max:
        cpu: "2"  
        memory: "1Gi"
      min:
        cpu: "200m"
        memory: "6Mi"
      maxLimitRequestRatio:
        cpu: "10"

apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "resource-limits"
spec:
  limits:
    - type: openshift.io/Image
      max:
        storage: 1Gi
```

1 The name of the LimitRange object.

2 The maximum size of an image that can be pushed to an internal registry.
NOTE

To prevent blobs that exceed the limit from being uploaded to the registry, the registry must be configured to enforce quotas.

WARNING

The image size is not always available in the manifest of an uploaded image. This is especially the case for images built with Docker 1.10 or higher and pushed to a v2 registry. If such an image is pulled with an older Docker daemon, the image manifest is converted by the registry to schema v1 lacking all the size information. No storage limit set on images prevent it from being uploaded.

The issue is being addressed.

7.3.1.4. Image stream limits

A LimitRange object allows you to specify limits for image streams.

For each image stream, the following must hold true:

- The number of image tags in an ImageStream specification must be less than or equal to the openshift.io/image-tags constraint in the LimitRange object.
- The number of unique references to images in an ImageStream specification must be less than or equal to the openshift.io/images constraint in the limit range object.

Imagestream LimitRange object definition

```yaml
apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "resource-limits"
spec:
  limits:
    - type: openshift.io/ImageStream
      max:
        openshift.io/image-tags: 20
        openshift.io/images: 30

1 The name of the LimitRange object.
2 The maximum number of unique image tags in the imagestream.spec.tags parameter in imagestream spec.
3 The maximum number of unique image references in the imagestream.status.tags parameter in the imagestream spec.

The openshift.io/image-tags resource represents unique image references. Possible references are an ImageStreamTag, an ImageStreamImage and a DockerImage. Tags can be created using the oc tag.
and `oc import-image` commands. No distinction is made between internal and external references. However, each unique reference tagged in an ImageStream specification is counted just once. It does not restrict pushes to an internal container image registry in any way, but is useful for tag restriction.

The `openshift.io/images` resource represents unique image names recorded in image stream status. It allows for restriction of a number of images that can be pushed to the internal registry. Internal and external references are not distinguished.

### 7.3.1.1.5. Persistent volume claim limits

A LimitRange object allows you to restrict the storage requested in a persistent volume claim (PVC).

Across all persistent volume claims in a project, the following must hold true:

- The resource request in a persistent volume claim (PVC) must be greater than or equal the min constraint for PVCs that is specified in the LimitRange object.
- The resource request in a persistent volume claim (PVC) must be less than or equal the max constraint for PVCs that is specified in the LimitRange object.

#### PVC LimitRange object definition

```yaml
apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "resource-limits" 1
spec:
limits:
  - type: "PersistentVolumeClaim"
    min:
      storage: "2Gi" 2
    max:
      storage: "50Gi" 3

1 The name of the LimitRange object.
2 The minimum amount of storage that can be requested in a persistent volume claim.
3 The maximum amount of storage that can be requested in a persistent volume claim.
```

### 7.3.2. Creating a Limit Range

To apply a limit range to a project:

1. Create a LimitRange object with your required specifications:

```yaml
apiVersion: "v1"
kind: "LimitRange"
metadata:
  name: "resource-limits" 1
spec:
limits:
  - type: "Pod" 2
    max:
```

1 Create a LimitRange object with your required specifications.
2 Specify the type of resource to limit.
Specify a name for the LimitRange object.

1 To set limits for a pod, specify the minimum and maximum CPU and memory requests as needed.

2 To set limits for a container, specify the minimum and maximum CPU and memory requests as needed.

3 Optional. For a container, specify the default amount of CPU or memory that a container can use, if not specified in the Pod spec.

4 Optional. For a container, specify the default amount of CPU or memory that a container can request, if not specified in the Pod spec.

5 Optional. For a container, specify the maximum limit-to-request ratio that can be specified in the Pod spec.

6 To set limits for an Image object, set the maximum size of an image that can be pushed to an internal registry.

7 To set limits for an image stream, set the maximum number of image tags and references that can be in the ImageStream object file, as needed.

8
To set limits for a persistent volume claim, set the minimum and maximum amount of storage that can be requested.

2. Create the object:

   ```bash
   $ oc create -f <limit_range_file> -n <project>
   ```

   Specify the name of the YAML file you created and the project where you want the limits to apply.

7.3.3. Viewing a limit

You can view any limits defined in a project by navigating in the web console to the project’s Quota page.

You can also use the CLI to view limit range details:

1. Get the list of LimitRange object defined in the project. For example, for a project called demoproject:

   ```bash
   $ oc get limits -n demoproject
   ```

<table>
<thead>
<tr>
<th>NAME</th>
<th>CREATED AT</th>
</tr>
</thead>
<tbody>
<tr>
<td>resource-limits</td>
<td>2020-07-15T17:14:23Z</td>
</tr>
</tbody>
</table>

2. Describe the LimitRange object you are interested in, for example the resource-limits limit range:

   ```bash
   $ oc describe limits resource-limits -n demoproject
   ```

   Name: resource-limits
   Namespace: demoproject
   Type: Resource

   Limit/Request Ratio

   Pod
   ---                            --------  ----     ---     -----------  -------------  -----------------------
   cpu    200m                 2       -               -               -
   memory 6Mi       1Gi     1Gi     -               -               -
   Container
   ---                            --------  ----     ---     -----------  -------------  -----------------------
   cpu    100m                 2       200m           300m           10
   memory 4Mi       1Gi     100Mi      200Mi         -
   openshift.io/image storage  -       1Gi     -               -               -
   openshift.io/imageStream openshift.io/image -       12           -               -               -
   openshift.io/imageStream openshift.io/image-tags -       10           -               -               -
   PersistentVolumeClaim storage -       50Gi    -               -               -

7.3.4. Deleting a Limit Range

To remove any active LimitRange object to no longer enforce the limits in a project:

1. Run the following command:

   ```bash
   $ oc delete limits <limit_name>
   ```
7.4. CONFIGURING CLUSTER MEMORY TO MEET CONTAINER MEMORY AND RISK REQUIREMENTS

As a cluster administrator, you can help your clusters operate efficiently through managing application memory by:

- Determining the memory and risk requirements of a containerized application component and configuring the container memory parameters to suit those requirements.
- Configuring containerized application runtimes (for example, OpenJDK) to adhere optimally to the configured container memory parameters.
- Diagnosing and resolving memory-related error conditions associated with running in a container.

7.4.1. Understanding managing application memory

It is recommended to fully read the overview of how OpenShift Container Platform manages Compute Resources before proceeding.

For each kind of resource (memory, CPU, storage), OpenShift Container Platform allows optional request and limit values to be placed on each container in a pod.

Note the following about memory requests and memory limits:

- **Memory request**
  - The memory request value, if specified, influences the OpenShift Container Platform scheduler. The scheduler considers the memory request when scheduling a container to a node, then fences off the requested memory on the chosen node for the use of the container.
  - If a node’s memory is exhausted, OpenShift Container Platform prioritizes evicting its containers whose memory usage most exceeds their memory request. In serious cases of memory exhaustion, the node OOM killer may select and kill a process in a container based on a similar metric.
  - The cluster administrator can assign quota or assign default values for the memory request value.
  - The cluster administrator can override the memory request values that a developer specifies, to manage cluster overcommit.

- **Memory limit**
  - The memory limit value, if specified, provides a hard limit on the memory that can be allocated across all the processes in a container.
  - If the memory allocated by all of the processes in a container exceeds the memory limit, the node Out of Memory (OOM) killer will immediately select and kill a process in the container.
  - If both memory request and limit are specified, the memory limit value must be greater than or equal to the memory request.
  - The cluster administrator can assign quota or assign default values for the memory limit value.
The minimum memory limit is 12 MB. If a container fails to start due to a Cannot allocate memory pod event, the memory limit is too low. Either increase or remove the memory limit. Removing the limit allows pods to consume unbounded node resources.

### 7.4.1.1. Managing application memory strategy

The steps for sizing application memory on OpenShift Container Platform are as follows:

1. **Determine expected container memory usage**
   Determine expected mean and peak container memory usage, empirically if necessary (for example, by separate load testing). Remember to consider all the processes that may potentially run in parallel in the container: for example, does the main application spawn any ancillary scripts?

2. **Determine risk appetite**
   Determine risk appetite for eviction. If the risk appetite is low, the container should request memory according to the expected peak usage plus a percentage safety margin. If the risk appetite is higher, it may be more appropriate to request memory according to the expected mean usage.

3. **Set container memory request**
   Set container memory request based on the above. The more accurately the request represents the application memory usage, the better. If the request is too high, cluster and quota usage will be inefficient. If the request is too low, the chances of application eviction increase.

4. **Set container memory limit, if required**
   Set container memory limit, if required. Setting a limit has the effect of immediately killing a container process if the combined memory usage of all processes in the container exceeds the limit, and is therefore a mixed blessing. On the one hand, it may make unanticipated excess memory usage obvious early ("fail fast"); on the other hand it also terminates processes abruptly.

   Note that some OpenShift Container Platform clusters may require a limit value to be set; some may override the request based on the limit; and some application images rely on a limit value being set as this is easier to detect than a request value.

   If the memory limit is set, it should not be set to less than the expected peak container memory usage plus a percentage safety margin.

5. **Ensure application is tuned**
   Ensure application is tuned with respect to configured request and limit values, if appropriate. This step is particularly relevant to applications which pool memory, such as the JVM. The rest of this page discusses this.

**Additional resources**

- Understanding compute resources and containers

### 7.4.2. Understanding OpenJDK settings for OpenShift Container Platform

The default OpenJDK settings do not work well with containerized environments. As a result, some additional Java memory settings must always be provided whenever running the OpenJDK in a container.
The JVM memory layout is complex, version dependent, and describing it in detail is beyond the scope of this documentation. However, as a starting point for running OpenJDK in a container, at least the following three memory-related tasks are key:

1. Overriding the JVM maximum heap size.
2. Encouraging the JVM to release unused memory to the operating system, if appropriate.
3. Ensuring all JVM processes within a container are appropriately configured.

Optimally tuning JVM workloads for running in a container is beyond the scope of this documentation, and may involve setting multiple additional JVM options.

7.4.2.1. Understanding how to override the JVM maximum heap size

For many Java workloads, the JVM heap is the largest single consumer of memory. Currently, the OpenJDK defaults to allowing up to 1/4 (1/\(-XX:MaxRAMFraction\)) of the compute node’s memory to be used for the heap, regardless of whether the OpenJDK is running in a container or not. It is therefore essential to override this behavior, especially if a container memory limit is also set.

There are at least two ways the above can be achieved:

1. If the container memory limit is set and the experimental options are supported by the JVM, set 
   -XX:+UnlockExperimentalVMOptions -XX:+UseCGroupMemoryLimitForHeap.

   **NOTE**

   The UseCGroupMemoryLimitForHeap option has been removed in JDK 11. Use -XX:+UseContainerSupport instead.

   This sets \(-XX:MaxRAM\) to the container memory limit, and the maximum heap size (\(-XX:MaxHeapSize / -Xmx\)) to 1/\(-XX:MaxRAMFraction\) (1/4 by default).

2. Directly override one of \(-XX:MaxRAM, -XX:MaxHeapSize or -Xmx\).

   This option involves hard-coding a value, but has the advantage of allowing a safety margin to be calculated.

7.4.2.2. Understanding how to encourage the JVM to release unused memory to the operating system

By default, the OpenJDK does not aggressively return unused memory to the operating system. This may be appropriate for many containerized Java workloads, but notable exceptions include workloads where additional active processes co-exist with a JVM within a container, whether those additional processes are native, additional JVMs, or a combination of the two.

The OpenShift Container Platform Jenkins maven slave image uses the following JVM arguments to encourage the JVM to release unused memory to the operating system:

-XX:+UseParallelGC
-XX:MinHeapFreeRatio=5 -XX:MaxHeapFreeRatio=10 -XX:GCTimeRatio=4
-XX:AdaptiveSizePolicyWeight=90.

These arguments are intended to return heap memory to the operating system whenever allocated memory exceeds 110% of in-use memory (\(-XX:MaxHeapFreeRatio\)), spending up to 20% of CPU time in the garbage collector (\(-XX:GCTimeRatio\)). At no time will the application heap allocation be less than
the initial heap allocation (overridden by `-XX:InitialHeapSize / -Xms`). Detailed additional information is available Tuning Java’s footprint in OpenShift (Part 1), Tuning Java’s footprint in OpenShift (Part 2), and at OpenJDK and Containers.

### 7.4.2.3. Understanding how to ensure all JVM processes within a container are appropriately configured

In the case that multiple JVMs run in the same container, it is essential to ensure that they are all configured appropriately. For many workloads it will be necessary to grant each JVM a percentage memory budget, leaving a perhaps substantial additional safety margin.

Many Java tools use different environment variables (`JAVA_OPTS`, `GRADLE_OPTS`, `MAVEN_OPTS`, and so on) to configure their JVMs and it can be challenging to ensure that the right settings are being passed to the right JVM.

The `JAVA_TOOL_OPTIONS` environment variable is always respected by the OpenJDK, and values specified in `JAVA_TOOL_OPTIONS` will be overridden by other options specified on the JVM command line. By default, to ensure that these options are used by default for all JVM workloads run in the slave image, the OpenShift Container Platform Jenkins maven slave image sets:

```bash
JAVA_TOOL_OPTIONS="-XX:+UnlockExperimentalVMOptions -XX:+UseCGroupMemoryLimitForHeap -Dsun.zip.disableMemoryMapping=true"
```

---

**NOTE**

The `UseCGroupMemoryLimitForHeap` option has been removed in JDK 11. Use `-XX:+UseContainerSupport` instead.

This does not guarantee that additional options are not required, but is intended to be a helpful starting point.

### 7.4.3. Finding the memory request and limit from within a pod

An application wishing to dynamically discover its memory request and limit from within a pod should use the Downward API.

**Procedure**

1. Configure the pod to add the `MEMORY_REQUEST` and `MEMORY_LIMIT` stanzas:

```yaml
apiVersion: v1
customKind: Pod
metadata:
  name: test
spec:
  containers:
    - name: test
      image: fedora:latest
      command:
        - sleep
        - "3600"
      env:
        - name: MEMORY_REQUEST
          valueFrom:
```
Add this stanza to discover the application memory request value.

Add this stanza to discover the application memory limit value.

2. Create the pod:

```bash
$ oc create -f <file-name>.yaml
```

3. Access the pod using a remote shell:

```bash
$ oc rsh test
```

4. Check that the requested values were applied:

```bash
$ env | grep MEMORY | sort
```

**Example output**

```
MEMORY_LIMIT=536870912
MEMORY_REQUEST=402653184
```

**NOTE**

The memory limit value can also be read from inside the container by the `/sys/fs/cgroup/memory/memory.limit_in_bytes` file.

### 7.4.4. Understanding OOM kill policy

OpenShift Container Platform can kill a process in a container if the total memory usage of all the processes in the container exceeds the memory limit, or in serious cases of node memory exhaustion.

When a process is Out of Memory (OOM) killed, this might result in the container exiting immediately. If the container PID 1 process receives the `SIGKILL`, the container will exit immediately. Otherwise, the container behavior is dependent on the behavior of the other processes.

For example, a container process exited with code 137, indicating it received a SIGKILL signal.

If the container does not exit immediately, an OOM kill is detectable as follows:
1. Access the pod using a remote shell:
   
   ```
   # oc rsh test
   ```

2. Run the following command to see the current OOM kill count in
   `/sys/fs/cgroup/memory/memory.oom_control`:

   ```
   $ grep '^oom_kill ' /sys/fs/cgroup/memory/memory.oom_control
   oom_kill 0
   ```

3. Run the following command to provoke an OOM kill:

   ```
   $ sed -e " </dev/zero
   ```

   **Example output**

   ```
   Killed
   ```

4. Run the following command to view the exit status of the `sed` command:

   ```
   $ echo $?
   ```

   **Example output**

   ```
   137
   ```

   The **137** code indicates the container process exited with code 137, indicating it received a
   `SIGKILL` signal.

5. Run the following command to see that the OOM kill counter in
   `/sys/fs/cgroup/memory/memory.oom_control` incremented:

   ```
   $ grep '^oom_kill ' /sys/fs/cgroup/memory/memory.oom_control
   oom_kill 1
   ```

   If one or more processes in a pod are OOM killed, when the pod subsequently exits, whether
   immediately or not, it will have phase **Failed** and reason **OOMKilled**. An OOM-killed pod might
   be restarted depending on the value of **restartPolicy**. If not restarted, controllers such as the
   replication controller will notice the pod’s failed status and create a new pod to replace the old
   one.

   Use the following command to get the pod status:

   ```
   $ oc get pod test
   ```

   **Example output**

   ```
   NAME     READY   STATUS      RESTARTS   AGE
   test     0/1     OOMKilled   0          1m
   ```

   - If the pod has not restarted, run the following command to view the pod:
7.4.5. Understanding pod eviction

OpenShift Container Platform may evict a pod from its node when the node's memory is exhausted. Depending on the extent of memory exhaustion, the eviction may or may not be graceful. Graceful eviction implies the main process (PID 1) of each container receiving a SIGTERM signal, then some time later a SIGKILL signal if the process has not exited already. Non-graceful eviction implies the main process of each container immediately receiving a SIGKILL signal.

An evicted pod has phase Failed and reason Evicted. It will not be restarted, regardless of the value of restartPolicy. However, controllers such as the replication controller will notice the pod’s failed status and create a new pod to replace the old one.
7.5. CONFIGURING YOUR CLUSTER TO PLACE PODS ON OVERCOMMITTED NODES

In an overcommitted state, the sum of the container compute resource requests and limits exceeds the resources available on the system. For example, you might want to use overcommitment in development environments where a trade-off of guaranteed performance for capacity is acceptable.

Containers can specify compute resource requests and limits. Requests are used for scheduling your container and provide a minimum service guarantee. Limits constrain the amount of compute resource that can be consumed on your node.

The scheduler attempts to optimize the compute resource use across all nodes in your cluster. It places pods onto specific nodes, taking the pods’ compute resource requests and nodes’ available capacity into consideration.

OpenShift Container Platform administrators can control the level of overcommit and manage container density on nodes. You can configure cluster-level overcommit using the `ClusterResourceOverride Operator` to override the ratio between requests and limits set on developer containers. In conjunction with node overcommit and project memory and CPU limits and defaults, you can adjust the resource limit and request to achieve the desired level of overcommit.

**NOTE**

In OpenShift Container Platform, you must enable cluster-level overcommit. Node overcommitment is enabled by default. See [Disabling overcommitment for a node](#).

### 7.5.1. Resource requests and overcommitment

For each compute resource, a container may specify a resource request and limit. Scheduling decisions are made based on the request to ensure that a node has enough capacity available to meet the requested value. If a container specifies limits, but omits requests, the requests are defaulted to the limits. A container is not able to exceed the specified limit on the node.

The enforcement of limits is dependent upon the compute resource type. If a container makes no request or limit, the container is scheduled to a node with no resource guarantees. In practice, the container is able to consume as much of the specified resource as is available with the lowest local priority. In low resource situations, containers that specify no resource requests are given the lowest quality of service.

Scheduling is based on resources requested, while quota and hard limits refer to resource limits, which
can be set higher than requested resources. The difference between request and limit determines the level of overcommit; for instance, if a container is given a memory request of 1Gi and a memory limit of 2Gi, it is scheduled based on the 1Gi request being available on the node, but could use up to 2Gi; so it is 200% overcommitted.

### 7.5.2. Cluster-level overcommit using the Cluster Resource Override Operator

The Cluster Resource Override Operator is an admission webhook that allows you to control the level of overcommit and manage container density across all the nodes in your cluster. The Operator controls how nodes in specific projects can exceed defined memory and CPU limits.

You must install the Cluster Resource Override Operator using the OpenShift Container Platform console or CLI as shown in the following sections. During the installation, you create a `ClusterResourceOverride` custom resource (CR), where you set the level of overcommit, as shown in the following example:

```yaml
apiVersion: operator.autoscaling.openshift.io/v1
kind: ClusterResourceOverride
metadata:
  name: cluster
spec:
  podResourceOverride:
    spec:
      memoryRequestToLimitPercent: 50
      cpuRequestToLimitPercent: 25
      limitCPUToMemoryPercent: 200
```

1. The name must be `cluster`.
2. Optional. If a container memory limit has been specified or defaulted, the memory request is overridden to this percentage of the limit, between 1-100. The default is 50.
3. Optional. If a container CPU limit has been specified or defaulted, the CPU request is overridden to this percentage of the limit, between 1-100. The default is 25.
4. Optional. If a container memory limit has been specified or defaulted, the CPU limit is overridden to a percentage of the memory limit, if specified. Scaling 1Gi of RAM at 100 percent is equal to 1 CPU core. This is processed prior to overriding the CPU request (if configured). The default is 200.

**NOTE**

The Cluster Resource Override Operator overrides have no effect if limits have not been set on containers. Create a `LimitRange` object with default limits per individual project or configure limits in `Pod` specs for the overrides to apply.

When configured, overrides can be enabled per-project by applying the following label to the Namespace object for each project:

```yaml
apiVersion: v1
kind: Namespace
metadata:
  ....
```
The Operator watches for the `ClusterResourceOverride` CR and ensures that the `ClusterResourceOverride` admission webhook is installed into the same namespace as the operator.

7.5.2.1. Installing the Cluster Resource Override Operator using the web console

You can use the OpenShift Container Platform web console to install the Cluster Resource Override Operator to help control overcommit in your cluster.

Prerequisites

- The Cluster Resource Override Operator has no effect if limits have not been set on containers. You must specify default limits for a project using a `LimitRange` object or configure limits in `Pod` specs for the overrides to apply.

Procedure

To install the Cluster Resource Override Operator using the OpenShift Container Platform web console:

1. In the OpenShift Container Platform web console, navigate to `Home → Projects`
   a. Click `Create Project`
   b. Specify `clusterresourceoverride-operator` as the name of the project.
   c. Click `Create`.

   a. Choose `ClusterResourceOverride Operator` from the list of available Operators and click `Install`.
   b. On the `Install Operator` page, make sure `A specific Namespace on the cluster` is selected for `Installation Mode`.
   c. Make sure `clusterresourceoverride-operator` is selected for `Installed Namespace`.
   d. Select an `Update Channel` and `Approval Strategy`.
   e. Click `Install`.

   b. On the `Create ClusterResourceOverride` page, edit the YAML template to set the overcommit values as needed:

```yaml
apiVersion: operator.autoscaling.openshift.io/v1
kind: ClusterResourceOverride
metadata:
  name: cluster
```

...
The name must be `cluster`.

Optional. Specify the percentage to override the container memory limit, if used, between 1-100. The default is 50.

Optional. Specify the percentage to override the container CPU limit, if used, between 1-100. The default is 25.

Optional. Specify the percentage to override the container memory limit, if used. Scaling 1Gi of RAM at 100 percent is equal to 1 CPU core. This is processed prior to overriding the CPU request, if configured. The default is 200.

c. Click **Create**.

d. Check the current state of the admission webhook by checking the status of the cluster custom resource:

   a. On the **ClusterResourceOverride Operator** page, click **cluster**.

   b. On the **ClusterResourceOverride Details** page, click **YAML**. The `mutatingWebhookConfigurationRef` section appears when the webhook is called.

```yaml
apiVersion: operator.autoscaling.openshift.io/v1
kind: ClusterResourceOverride
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

  
  {"apiVersion":"operator.autoscaling.openshift.io/v1","kind":"ClusterResourceOverride","metadata":{"annotations":{"name":"cluster"},"spec":{"podResourceOverride":{"spec":{"cpuRequestToLimitPercent":25,\"limitCPUToMemoryPercent\":200,\"memoryRequestToLimitPercent\":50}}}}}

creationTimestamp: "2019-12-18T22:35:02Z"

name: cluster

resourceVersion: "127622"

selfLink: /apis/operator.autoscaling.openshift.io/v1/clusterresourceoverrides/cluster

uid: 978fc959-1717-4bd1-97d0-ae00ee11e8d

spec:
  podResourceOverride:
    spec:
      cpuRequestToLimitPercent: 25
      limitCPUToMemoryPercent: 200
      memoryRequestToLimitPercent: 50

status:

....
```
7.5.2.2. Installing the Cluster Resource Override Operator using the CLI

You can use the OpenShift Container Platform CLI to install the Cluster Resource Override Operator to help control overcommit in your cluster.

Prerequisites

- The Cluster Resource Override Operator has no effect if limits have not been set on containers. You must specify default limits for a project using a LimitRange object or configure limits in Pod specs for the overrides to apply.

Procedure

To install the Cluster Resource Override Operator using the CLI:

1. Create a namespace for the Cluster Resource Override Operator:
   a. Create a Namespace object YAML file (for example, cro-namespace.yaml) for the Cluster Resource Override Operator:

   ```yaml
   apiVersion: v1
   kind: Namespace
   metadata:
     name: clusterresourceoverride-operator
   ```

   b. Create the namespace:

   ```bash
   $ oc create -f <file-name>.yaml
   ```

   For example:

   ```bash
   $ oc create -f cro-namespace.yaml
   ```

2. Create an Operator group:
   a. Create an OperatorGroup object YAML file (for example, cro-og.yaml) for the Cluster Resource Override Operator:

   ```yaml
   apiVersion: operators.coreos.com/v1
   kind: OperatorGroup
   metadata:
     name: clusterresourceoverride-operator
   namespace: clusterresourceoverride-operator
   ```
Create the Operator Group:

For example:

$ oc create -f cro-og.yaml

3. Create a subscription:

a. Create a **Subscription** object YAML file (for example, cro-sub.yaml) for the Cluster Resource Override Operator:

```yaml
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: clusterresourceoverride
  namespace: clusterresourceoverride-operator
spec:
  channel: "4.11"
  name: clusterresourceoverride
  source: redhat-operators
  sourceNamespace: openshift-marketplace
```

b. Create the subscription:

$ oc create -f cro-sub.yaml

4. Create a **ClusterResourceOverride** custom resource (CR) object in the `clusterresourceoverride-operator` namespace:

a. Change to the `clusterresourceoverride-operator` namespace.

$ oc project clusterresourceoverride-operator

b. Create a **ClusterResourceOverride** object YAML file (for example, cro-cr.yaml) for the Cluster Resource Override Operator:

```yaml
apiVersion: operator.autoscaling.openshift.io/v1
kind: ClusterResourceOverride
metadata:
  name: cluster
spec:
  podResourceOverride:
    spec:
```
The name must be `cluster`.

Optional. Specify the percentage to override the container memory limit, if used, between 1-100. The default is 50.

Optional. Specify the percentage to override the container CPU limit, if used, between 1-100. The default is 25.

Optional. Specify the percentage to override the container memory limit, if used. Scaling 1Gi of RAM at 100 percent is equal to 1 CPU core. This is processed prior to overriding the CPU request, if configured. The default is 200.

c. Create the `ClusterResourceOverride` object:

```
$ oc create -f <file-name>.yaml
```

For example:

```
$ oc create -f cro-cr.yaml
```

5. Verify the current state of the admission webhook by checking the status of the cluster custom resource.

```
$ oc get clusterresourceoverride cluster -n clusterresourceoverride-operator -o yaml
```

The `mutatingWebhookConfigurationRef` section appears when the webhook is called.

**Example output**

```yaml
apiVersion: operator.autoscaling.openshift.io/v1
kind: ClusterResourceOverride
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration:
      value: |
        {"apiVersion":"operator.autoscaling.openshift.io/v1","kind":"ClusterResourceOverride","metadata":{"annotations":{},"name":"cluster"},"spec":{"podResourceOverride":{"spec":{"cpuRequestToLimitPercent":25,"limitCPUToMemoryPercent":200,"memoryRequestToLimitPercent":50}}}]

creationTimestamp: "2019-12-18T22:35:02Z"

generation: 1

name: cluster

resourceVersion: "127622"

selfLink: /apis/operator.autoscaling.openshift.io/v1/clusterresourceoverrides/cluster

uid: 978fc959-1717-4bd1-97d0-ae00ee111e8d

spec:

  podResourceOverride:
    spec:
      cpuRequestToLimitPercent: 25
      limitCPUToMemoryPercent: 200
```
7.5.2.3. Configuring cluster-level overcommit

The Cluster Resource Override Operator requires a `ClusterResourceOverride` custom resource (CR) and a label for each project where you want the Operator to control overcommit.

**Prerequisites**

- The Cluster Resource Override Operator has no effect if limits have not been set on containers. You must specify default limits for a project using a `LimitRange` object or configure limits in `Pod` specs for the overrides to apply.

**Procedure**

To modify cluster-level overcommit:

1. Edit the `ClusterResourceOverride` CR:

   ```yaml
   apiVersion: operator.autoscaling.openshift.io/v1
   kind: ClusterResourceOverride
   metadata:
     name: cluster
   spec:
     podResourceOverride:
       spec:
         memoryRequestToLimitPercent: 50
         cpuRequestToLimitPercent: 25
         limitCPUToMemoryPercent: 200
   
   1 Optional. Specify the percentage to override the container memory limit, if used, between 1-100. The default is 50.
   
   2 Optional. Specify the percentage to override the container CPU limit, if used, between 1-100. The default is 25.
   
   3 Optional. Specify the percentage to override the container memory limit, if used. Scaling 1Gi of RAM at 100 percent is equal to 1 CPU core. This is processed prior to overriding the CPU request, if configured. The default is 200.
   ```
2. Ensure the following label has been added to the Namespace object for each project where you want the Cluster Resource Override Operator to control overcommit:

```yaml
apiVersion: v1
kind: Namespace
metadata:
  ...
labels:
  clusterresourceoverrides.admission.autoscaling.openshift.io/enabled: "true" 1
  ...
```

1. Add this label to each project.

7.5.3. Node-level overcommit

You can use various ways to control overcommit on specific nodes, such as quality of service (QOS) guarantees, CPU limits, or reserve resources. You can also disable overcommit for specific nodes and specific projects.

7.5.3.1. Understanding compute resources and containers

The node-enforced behavior for compute resources is specific to the resource type.

7.5.3.1.1. Understanding container CPU requests

A container is guaranteed the amount of CPU it requests and is additionally able to consume excess CPU available on the node, up to any limit specified by the container. If multiple containers are attempting to use excess CPU, CPU time is distributed based on the amount of CPU requested by each container.

For example, if one container requested 500m of CPU time and another container requested 250m of CPU time, then any extra CPU time available on the node is distributed among the containers in a 2:1 ratio. If a container specified a limit, it will be throttled not to use more CPU than the specified limit. CPU requests are enforced using the CFS shares support in the Linux kernel. By default, CPU limits are enforced using the CFS quota support in the Linux kernel over a 100ms measuring interval, though this can be disabled.

7.5.3.1.2. Understanding container memory requests

A container is guaranteed the amount of memory it requests. A container can use more memory than requested, but once it exceeds its requested amount, it could be terminated in a low memory situation on the node. If a container uses less memory than requested, it will not be terminated unless system tasks or daemons need more memory than was accounted for in the node’s resource reservation. If a container specifies a limit on memory, it is immediately terminated if it exceeds the limit amount.

7.5.3.2. Understanding overcommitment and quality of service classes

A node is overcommitted when it has a pod scheduled that makes no request, or when the sum of limits across all pods on that node exceeds available machine capacity.

In an overcommitted environment, it is possible that the pods on the node will attempt to use more
compute resource than is available at any given point in time. When this occurs, the node must give priority to one pod over another. The facility used to make this decision is referred to as a Quality of Service (QoS) Class.

For each compute resource, a container is divided into one of three QoS classes with decreasing order of priority:

### Table 7.19. Quality of Service Classes

<table>
<thead>
<tr>
<th>Priority</th>
<th>Class Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (highest)</td>
<td>Guaranteed</td>
<td>If limits and optionally requests are set (not equal to 0) for all resources and they are equal, then the container is classified as Guaranteed.</td>
</tr>
<tr>
<td>2</td>
<td>Burstable</td>
<td>If requests and optionally limits are set (not equal to 0) for all resources, and they are not equal, then the container is classified as Burstable.</td>
</tr>
<tr>
<td>3 (lowest)</td>
<td>BestEffort</td>
<td>If requests and limits are not set for any of the resources, then the container is classified as BestEffort.</td>
</tr>
</tbody>
</table>

Memory is an incompressible resource, so in low memory situations, containers that have the lowest priority are terminated first:

- **Guaranteed** containers are considered top priority, and are guaranteed to only be terminated if they exceed their limits, or if the system is under memory pressure and there are no lower priority containers that can be evicted.
- **Burstable** containers under system memory pressure are more likely to be terminated once they exceed their requests and no other **BestEffort** containers exist.
- **BestEffort** containers are treated with the lowest priority. Processes in these containers are first to be terminated if the system runs out of memory.

#### 7.5.3.2.1. Understanding how to reserve memory across quality of service tiers

You can use the `qos-reserved` parameter to specify a percentage of memory to be reserved by a pod in a particular QoS level. This feature attempts to reserve requested resources to exclude pods from lower QoS classes from using resources requested by pods in higher QoS classes.

OpenShift Container Platform uses the `qos-reserved` parameter as follows:

- A value of `qos-reserved=memory=100%` will prevent the **Burstable** and **BestEffort** QoS classes from consuming memory that was requested by a higher QoS class. This increases the risk of inducing OOM on **BestEffort** and **Burstable** workloads in favor of increasing memory resource guarantees for **Guaranteed** and **Burstable** workloads.

- A value of `qos-reserved=memory=50%` will allow the **Burstable** and **BestEffort** QoS classes to consume half of the memory requested by a higher QoS class.

- A value of `qos-reserved=memory=0%` will allow a **Burstable** and **BestEffort** QoS classes to consume up to the full node allocatable amount if available, but increases the risk that a **Guaranteed** workload will not have access to requested memory. This condition effectively disables this feature.
7.5.3.3. Understanding swap memory and QOS

You can disable swap by default on your nodes to preserve quality of service (QOS) guarantees. Otherwise, physical resources on a node can oversubscribe, affecting the resource guarantees the Kubernetes scheduler makes during pod placement.

For example, if two guaranteed pods have reached their memory limit, each container could start using swap memory. Eventually, if there is not enough swap space, processes in the pods can be terminated due to the system being oversubscribed.

Failing to disable swap results in nodes not recognizing that they are experiencing MemoryPressure, resulting in pods not receiving the memory they made in their scheduling request. As a result, additional pods are placed on the node to further increase memory pressure, ultimately increasing your risk of experiencing a system out of memory (OOM) event.

**IMPORTANT**

If swap is enabled, any out-of-resource handling eviction thresholds for available memory will not work as expected. Take advantage of out-of-resource handling to allow pods to be evicted from a node when it is under memory pressure, and rescheduled on an alternative node that has no such pressure.

7.5.3.4. Understanding nodes overcommitment

In an overcommitted environment, it is important to properly configure your node to provide best system behavior.

When the node starts, it ensures that the kernel tunable flags for memory management are set properly. The kernel should never fail memory allocations unless it runs out of physical memory.

To ensure this behavior, OpenShift Container Platform configures the kernel to always overcommit memory by setting the `vm.overcommit_memory` parameter to 1, overriding the default operating system setting.

OpenShift Container Platform also configures the kernel not to panic when it runs out of memory by setting the `vm.panic_on_oom` parameter to 0. A setting of 0 instructs the kernel to call oom_killer in an Out of Memory (OOM) condition, which kills processes based on priority.

You can view the current setting by running the following commands on your nodes:

```
$ sysctl -a | grep commit

Example output

vm.overcommit_memory = 1

$ sysctl -a | grep panic

Example output

vm.panic_on_oom = 0
```
NOTE

The above flags should already be set on nodes, and no further action is required.

You can also perform the following configurations for each node:

- Disable or enforce CPU limits using CPU CFS quotas
- Reserve resources for system processes
- Reserve memory across quality of service tiers

7.5.3.5. Disabling or enforcing CPU limits using CPU CFS quotas

Nodes by default enforce specified CPU limits using the Completely Fair Scheduler (CFS) quota support in the Linux kernel.

If you disable CPU limit enforcement, it is important to understand the impact on your node:

- If a container has a CPU request, the request continues to be enforced by CFS shares in the Linux kernel.
- If a container does not have a CPU request, but does have a CPU limit, the CPU request defaults to the specified CPU limit, and is enforced by CFS shares in the Linux kernel.
- If a container has both a CPU request and limit, the CPU request is enforced by CFS shares in the Linux kernel, and the CPU limit has no impact on the node.

Prerequisites

1. Obtain the label associated with the static MachineConfigPool CRD for the type of node you want to configure. Perform one of the following steps:

   a. View the machine config pool:

   ```
   $ oc describe machineconfigpool <name>
   ```

   For example:

   ```
   $ oc describe machineconfigpool worker
   ```

   Example output

   ```
   apiVersion: machineconfiguration.openshift.io/v1
   kind: MachineConfigPool
   metadata:
     creationTimestamp: 2019-02-08T14:52:39Z
     generation: 1
     labels:
       custom-kubelet: small-pods
   ```

   If a label has been added it appears under `labels`.

   b. If the label is not present, add a key/value pair:
You can alternatively apply the following YAML to add the label:

```yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
metadata:
  labels:
    custom-kubelet: small-pods
name: worker
```

**Procedure**

1. Create a custom resource (CR) for your configuration change.

**Sample configuration for a disabling CPU limits**

```yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: disable-cpu-units
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: small-pods
  kubeletConfig:
    cpuCfsQuota:
      - "false"
```

1. Assign a name to CR.
2. Specify the label to apply the configuration change.
3. Set the `cpuCfsQuota` parameter to `false`.

### 7.5.3.6. Reserving resources for system processes

To provide more reliable scheduling and minimize node resource overcommitment, each node can reserve a portion of its resources for use by system daemons that are required to run on your node for your cluster to function. In particular, it is recommended that you reserve resources for incompressible resources such as memory.

**Procedure**

To explicitly reserve resources for non-pod processes, allocate node resources by specifying resources available for scheduling. For more details, see Allocating Resources for Nodes.

### 7.5.3.7. Disabling overcommitment for a node

When enabled, overcommitment can be disabled on each node.
Procedure
To disable overcommitment in a node run the following command on that node:

```
$ sysctl -w vm.overcommit_memory=0
```

7.5.4. Project-level limits
To help control overcommit, you can set per-project resource limit ranges, specifying memory and CPU limits and defaults for a project that overcommit cannot exceed.

For information on project-level resource limits, see Additional resources.

Alternatively, you can disable overcommitment for specific projects.

7.5.4.1. Disabling overcommitment for a project
When enabled, overcommitment can be disabled per-project. For example, you can allow infrastructure components to be configured independently of overcommitment.

Procedure
To disable overcommitment in a project:

1. Edit the project object file
2. Add the following annotation:

```
quota.openshift.io/cluster-resource-override-enabled: "false"
```
3. Create the project object:

```
$ oc create -f <file-name>.yaml
```

7.5.5. Additional resources
- Setting deployment resources.
- Allocating resources for nodes.

7.6. ENABLING OPENSIFT CONTAINER PLATFORM FEATURES USING FEATUREGATES
As an administrator, you can use feature gates to enable features that are not part of the default set of features.

7.6.1. Understanding feature gates
You can use the FeatureGate custom resource (CR) to enable specific feature sets in your cluster. A feature set is a collection of OpenShift Container Platform features that are not enabled by default.

You can activate the following feature set by using the FeatureGate CR:

- TechPreviewNoUpgrade. This feature set is a subset of the current Technology Preview
features. This feature set allows you to enable these tech preview features on test clusters, where you can fully test them, while leaving the features disabled on production clusters. Enabling this feature set cannot be undone and prevents minor version updates. This feature set is not recommended on production clusters.

The following Technology Preview features are enabled by this feature set:

- Microsoft Azure File CSI Driver Operator. Enables the provisioning of persistent volumes (PVs) by using the Container Storage Interface (CSI) driver for Microsoft Azure File Storage.

- CSI automatic migration. Enables automatic migration for supported in-tree volume plugins to their equivalent Container Storage Interface (CSI) drivers. Supported for:
  - Amazon Web Services (AWS) Elastic Block Storage (EBS)
  - OpenStack Cinder
  - Azure Disk
  - Azure File
  - Google Cloud Platform Persistent Disk (CSI)
  - VMware vSphere

- Cluster Cloud Controller Manager Operator. Enables the Cluster Cloud Controller Manager Operator rather than the in-tree cloud controller. Available as a Technology Preview for:
  - Alibaba Cloud
  - Amazon Web Services (AWS)
  - Google Cloud Platform (GCP)
  - IBM Cloud
  - Microsoft Azure
  - Red Hat OpenStack Platform (RHOSP)
  - VMware vSphere

- Shared resource CSI driver

- CSI volume support for the OpenShift Container Platform build system

- Swap memory on nodes

- Cluster API. Enables the integrated upstream Cluster API in OpenShift Container Platform with the `ClusterAPIEnabled` feature gate. Available as a Technology Preview for:
  - Amazon Web Services (AWS)
  - Google Cloud Platform (GCP)

Additional resources
For more information on the features activated by the TechPreviewNoUpgrade feature gate, see the following topics:

- Azure File CSI Driver Operator
- CSI automatic migration
- Cluster Cloud Controller Manager Operator
- Source-to-image (S2I) build volumes and Docker build volumes
- Swap memory on nodes

### 7.6.2. Enabling feature sets using the web console

You can use the OpenShift Container Platform web console to enable feature sets for all of the nodes in a cluster by editing the FeatureGate custom resource (CR).

**Procedure**

To enable feature sets:

1. In the OpenShift Container Platform web console, switch to the Administration → Custom Resource Definitions page.
2. On the Custom Resource Definitions page, click FeatureGate.
3. On the Custom Resource Definition Details page, click the Instances tab.
4. Click the cluster feature gate, then click the YAML tab.
5. Edit the cluster instance to add specific feature sets:

**Sample Feature Gate custom resource**

```yaml
apiversion: config.openshift.io/v1
kind: FeatureGate
metadata:
  name: cluster

spec:
  featureSet: TechPreviewNoUpgrade
```

1. The name of the FeatureGate CR must be cluster.
2. Add the feature set that you want to enable:
   - TechPreviewNoUpgrade enables specific Technology Preview features.

After you save the changes, new machine configs are created, the machine config pools are updated, and scheduling on each node is disabled while the change is being applied.
Enabling the **TechPreviewNoUpgrade** feature set cannot be undone and prevents minor version updates. These feature sets are not recommended on production clusters.

### Verification

You can verify that the feature gates are enabled by looking at the **kubelet.conf** file on a node after the nodes return to the ready state.

1. From the Administrator perspective in the web console, navigate to **Compute → Nodes**.
2. Select a node.
3. In the **Node details** page, click **Terminal**.
4. In the terminal window, change your root directory to the host:
   ```
   sh-4.2# chroot /host
   ```
5. View the **kubelet.conf** file:
   ```
   sh-4.2# cat /etc/kubernetes/kubelet.conf
   ```

**Sample output**

```
... 
featureGates:
  InsightsOperatorPullingSCA: true,
  LegacyNodeRoleBehavior: false
...
```

The features that are listed as **true** are enabled on your cluster.

**NOTE**

The features listed vary depending upon the OpenShift Container Platform version.

### 7.6.3. Enabling feature sets using the CLI

You can use the OpenShift CLI (**oc**) to enable feature sets for all of the nodes in a cluster by editing the **FeatureGate** custom resource (CR).

**Prerequisites**

- You have installed the OpenShift CLI (**oc**).

**Procedure**

To enable feature sets:

1. Edit the **FeatureGate** CR named **cluster**.
Sample FeatureGate custom resource

```yaml
apiVersion: config.openshift.io/v1
kind: FeatureGate
metadata:
  name: cluster
spec:
  featureSet: TechPreviewNoUpgrade
```

1. The name of the `FeatureGate` CR must be `cluster`.
2. Add the feature set that you want to enable:
   - `TechPreviewNoUpgrade` enables specific Technology Preview features.

After you save the changes, new machine configs are created, the machine config pools are updated, and scheduling on each node is disabled while the change is being applied.

**NOTE**

Enabling the `TechPreviewNoUpgrade` feature set cannot be undone and prevents minor version updates. These feature sets are not recommended on production clusters.

**Verification**

You can verify that the feature gates are enabled by looking at the `kubelet.conf` file on a node after the nodes return to the ready state.

1. Start a debug session for a node:

   ```bash
   $ oc debug node/<node_name>
   ``

2. Change your root directory to the host:

   ```bash
   sh-4.2# chroot /host
   ``

3. View the `kubelet.conf` file:

   ```bash
   sh-4.2# cat /etc/kubernetes/kubelet.conf
   ``

**Sample output**

```
... featureGates:
  InsightsOperatorPullingSCA: true,
  LegacyNodeRoleBehavior: false
...`

The features that are listed as `true` are enabled on your cluster.
The features listed vary depending upon the OpenShift Container Platform version.

7.7. IMPROVING CLUSTER STABILITY IN HIGH LATENCY ENVIRONMENTS USING WORKER LATENCY PROFILES

All nodes send heartbeats to the Kubernetes Controller Manager Operator (kube controller) in the OpenShift Container Platform cluster every 10 seconds, by default. If the cluster does not receive heartbeats from a node, OpenShift Container Platform responds using several default mechanisms.

For example, if the Kubernetes Controller Manager Operator loses contact with a node after a configured period:

1. The node controller on the control plane updates the node health to Unhealthy and marks the node Ready condition as Unknown.
2. In response, the scheduler stops scheduling pods to that node.
3. The on-premise node controller adds a node.kubernetes.io/unreachable taint with a NoExecute effect to the node and schedules any pods on the node for eviction after five minutes, by default.

This behavior can cause problems if your network is prone to latency issues, especially if you have nodes at the network edge. In some cases, the Kubernetes Controller Manager Operator might not receive an update from a healthy node due to network latency. The Kubernetes Controller Manager Operator would then evict pods from the node even though the node is healthy. To avoid this problem, you can use worker latency profiles to adjust the frequency that the kubelet and the Kubernetes Controller Manager Operator wait for status updates before taking action. These adjustments help to ensure that your cluster runs properly in the event that network latency between the control plane and the worker nodes is not optimal.

These worker latency profiles are three sets of carefully-tuned values that control the reaction of the cluster to latency issues without needing to determine the best values manually.

You can configure worker latency profiles when installing a cluster or at any time you notice increased latency in your cluster network.

7.7.1. Understanding worker latency profiles

Worker latency profiles are multiple sets of carefully-tuned values for the node-status-update-frequency, node-monitor-grace-period, default-not-ready-toleration-seconds and default-unreachable-toleration-seconds parameters. These parameters let you control the reaction of the cluster to latency issues without needing to determine the best values manually.

All worker latency profiles configure the following parameters:

- node-status-update-frequency. Specifies the amount of time in seconds that a kubelet updates its status to the Kubernetes Controller Manager Operator.
- **node-monitor-grace-period.** Specifies the amount of time in seconds that the Kubernetes Controller Manager Operator waits for an update from a kubelet before marking the node unhealthy and adding the `node.kubernetes.io/not-ready` or `node.kubernetes.io/unreachable` taint to the node.

- **default-not-ready-toleration-seconds.** Specifies the amount of time in seconds after marking a node unhealthy that the Kubernetes Controller Manager Operator waits before evicting pods from that node.

- **default-unreachable-toleration-seconds.** Specifies the amount of time in seconds after marking a node unreachable that the Kubernetes Controller Manager Operator waits before evicting pods from that node.

**IMPORTANT**

Manually modifying the **node-monitor-grace-period** parameter is not supported.

While the default configuration works in most cases, OpenShift Container Platform offers two other worker latency profiles for situations where the network is experiencing higher latency than usual. The three worker latency profiles are described in the following sections:

### Default worker latency profile

With the Default profile, each kubelet reports its node status to the Kubelet Controller Manager Operator (kube controller) every 10 seconds. The Kubelet Controller Manager Operator checks the kubelet for a status every 5 seconds.

The Kubernetes Controller Manager Operator waits 40 seconds for a status update before considering that node unhealthy. It marks the node with the `node.kubernetes.io/not-ready` or `node.kubernetes.io/unreachable` taint and evicts the pods on that node. If a pod on that node has the NoExecute toleration, the pod gets evicted in 300 seconds. If the pod has the tolerationSeconds parameter, the eviction waits for the period specified by that parameter.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Component</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>kubelet</td>
<td>node-status-update-frequency</td>
<td>10s</td>
</tr>
<tr>
<td></td>
<td>Kubelet Controller Manager</td>
<td>node-monitor-grace-period</td>
<td>40s</td>
</tr>
<tr>
<td></td>
<td>Kubernetes API Server</td>
<td>default-not-ready-toleration-seconds</td>
<td>300s</td>
</tr>
<tr>
<td></td>
<td>Kubernetes API Server</td>
<td>default-unreachable-toleration-seconds</td>
<td>300s</td>
</tr>
</tbody>
</table>

### Medium worker latency profile

Use the **MediumUpdateAverageReaction** profile if the network latency is slightly higher than usual. The **MediumUpdateAverageReaction** profile reduces the frequency of kubelet updates to 20 seconds and changes the period that the Kubernetes Controller Manager Operator waits for those updates to 2 minutes. The pod eviction period for a pod on that node is reduced to 60 seconds. If
the pod has the `tolerationSeconds` parameter, the eviction waits for the period specified by that parameter.

The Kubernetes Controller Manager Operator waits for 2 minutes to consider a node unhealthy. In another minute, the eviction process starts.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Component</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MediumUpdateAverageReaction</td>
<td>kubelet</td>
<td>node-status-update-frequency</td>
<td>20s</td>
</tr>
<tr>
<td>Kubelet Controller Manager</td>
<td></td>
<td>node-monitor-grace-period</td>
<td>2m</td>
</tr>
<tr>
<td>Kubernetes API Server</td>
<td></td>
<td>default-not-ready-toleration-seconds</td>
<td>60s</td>
</tr>
<tr>
<td>Kubernetes API Server</td>
<td></td>
<td>default-unreachable-toleration-seconds</td>
<td>60s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profile</th>
<th>Component</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LowUpdateSlowReaction</td>
<td>kubelet</td>
<td>node-status-update-frequency</td>
<td>1m</td>
</tr>
<tr>
<td>Kubelet Controller Manager</td>
<td></td>
<td>node-monitor-grace-period</td>
<td>5m</td>
</tr>
<tr>
<td>Kubernetes API Server</td>
<td></td>
<td>default-not-ready-toleration-seconds</td>
<td>60s</td>
</tr>
<tr>
<td>Kubernetes API Server</td>
<td></td>
<td>default-unreachable-toleration-seconds</td>
<td>60s</td>
</tr>
</tbody>
</table>

7.7.2. Using worker latency profiles
To implement a worker latency profile to deal with network latency, edit the `node.config` object to add the name of the profile. You can change the profile at any time as latency increases or decreases.

You must move one worker latency profile at a time. For example, you cannot move directly from the `Default` profile to the `LowUpdateSlowReaction` worker latency profile. You must move from the `default` worker latency profile to the `MediumUpdateAverageReaction` profile first, then to `LowUpdateSlowReaction`. Similarly, when returning to the default profile, you must move from the low profile to the medium profile first, then to the default.

**NOTE**

You can also configure worker latency profiles upon installing an OpenShift Container Platform cluster.

**Procedure**

To move from the default worker latency profile:

1. Move to the medium worker latency profile:
   
   a. Edit the `node.config` object:
      
      ```
      $ oc edit nodes.config/cluster
      ```
   
   b. Add `spec.workerLatencyProfile: MediumUpdateAverageReaction`:

   **Example node.config object**

   ```yaml
   apiVersion: config.openshift.io/v1
   kind: Node
   metadata:
   annotations:
     include.release.openshift.io/ibm-cloud-managed: "true"
     include.release.openshift.io/self-managed-high-availability: "true"
     include.release.openshift.io/single-node-developer: "true"
     release.openshift.io/create-only: "true"
   creationTimestamp: "2022-07-08T16:02:51Z"
   generation: 1
   name: cluster
   ownerReferences:
   - apiVersion: config.openshift.io/v1
     kind: ClusterVersion
     name: version
     uid: 36282574-bf9f-409e-a6cd-3032939293eb
     resourceVersion: "1865"
     uid: 0c0f7a4c-4307-4187-b591-6155695ac85b
     spec:
       workerLatencyProfile: MediumUpdateAverageReaction
   ...
   ```

   1. Specifies the medium worker latency policy.

   Scheduling on each worker node is disabled as the change is being applied.
When all nodes return to the **Ready** condition, you can use the following command to look in the Kubernetes Controller Manager to ensure it was applied:

```
$ oc get KubeControllerManager -o yaml | grep -i workerlatency -A 5 -B 5
```

**Example output**

```yaml
...  
- lastTransitionTime: "2022-07-11T19:47:10Z"
  reason: ProfileUpdated
  status: "False"
  type: WorkerLatencyProfileProgressing
- lastTransitionTime: "2022-07-11T19:47:10Z"
  message: all static pod revision(s) have updated latency profile
  reason: ProfileUpdated
  status: "True"
  type: WorkerLatencyProfileComplete
- lastTransitionTime: "2022-07-11T19:20:11Z"
  reason: AsExpected
  status: "False"
  type: WorkerLatencyProfileDegraded
- lastTransitionTime: "2022-07-11T19:20:36Z"
  status: "False"
...
```

1. Specifies that the profile is applied and active.

2. Optional: Move to the low worker latency profile:
   
a. Edit the **node.config** object:

```
$ oc edit nodes.config/cluster
```

b. Change the **spec.workerLatencyProfile** value to **LowUpdateSlowReaction**:

**Example node.config object**

```yaml
apiVersion: config.openshift.io/v1
kind: Node
metadata:
  annotations:
    include.release.openshift.io/ibm-cloud-managed: "true"
    include.release.openshift.io/self-managed-high-availability: "true"
    include.release.openshift.io/single-node-developer: "true"
    release.openshift.io/create-only: "true"
  creationTimestamp: "2022-07-08T16:02:51Z"
  generation: 1
  name: cluster
  ownerReferences:
    - apiVersion: config.openshift.io/v1
      kind: ClusterVersion
      name: version
      uid: 36282574-bf9f-409e-a6cd-3032939293eb
```
resourceVersion: "1865"
uid: 0c0f7a4c-4307-4187-b591-6155695ac85b
spec:
  workerLatencyProfile: LowUpdateSlowReaction

Scheduling on each worker node is disabled as the change is being applied.

To change the low profile to medium or change the medium to low, edit the `node.config` object and set the `spec.workerLatencyProfile` parameter to the appropriate value.

1 Specifies to use the low worker latency policy.
You can configure OpenShift Container Platform clusters with nodes located at your network edge. In this topic, they are called remote worker nodes. A typical cluster with remote worker nodes combines on-premise master and worker nodes with worker nodes in other locations that connect to the cluster. This topic is intended to provide guidance on best practices for using remote worker nodes and does not contain specific configuration details.

There are multiple use cases across different industries, such as telecommunications, retail, manufacturing, and government, for using a deployment pattern with remote worker nodes. For example, you can separate and isolate your projects and workloads by combining the remote worker nodes into Kubernetes zones.

However, having remote worker nodes can introduce higher latency, intermittent loss of network connectivity, and other issues. Among the challenges in a cluster with remote worker node are:

- **Network separation**: The OpenShift Container Platform control plane and the remote worker nodes must be able to communicate with each other. Because of the distance between the control plane and the remote worker nodes, network issues could prevent this communication. See Network separation with remote worker nodes for information on how OpenShift Container Platform responds to network separation and for methods to diminish the impact to your cluster.

- **Power outage**: Because the control plane and remote worker nodes are in separate locations, a power outage at the remote location or at any point between the two can negatively impact your cluster. See Power loss on remote worker nodes for information on how OpenShift Container Platform responds to a node losing power and for methods to diminish the impact to your cluster.

- **Latency spikes or temporary reduction in throughput**: As with any network, any changes in network conditions between your cluster and the remote worker nodes can negatively impact your cluster. OpenShift Container Platform offers multiple worker latency profiles that let you control the reaction of the cluster to latency issues.

Note the following limitations when planning a cluster with remote worker nodes:

- OpenShift Container Platform does not support remote worker nodes that use a different cloud provider than the on-premise cluster uses.

- Moving workloads from one Kubernetes zone to a different Kubernetes zone can be problematic due to system and environment issues, such as a specific type of memory not being available in a different zone.

- Proxies and firewalls can present additional limitations that are beyond the scope of this document. See the relevant OpenShift Container Platform documentation for how to address such limitations, such as Configuring your firewall.

- You are responsible for configuring and maintaining L2/L3-level network connectivity between the control plane and the network-edge nodes.

### 8.1.1. Network separation with remote worker nodes
All nodes send heartbeats to the Kubernetes Controller Manager Operator (kube controller) in the OpenShift Container Platform cluster every 10 seconds. If the cluster does not receive heartbeats from a node, OpenShift Container Platform responds using several default mechanisms.

OpenShift Container Platform is designed to be resilient to network partitions and other disruptions. You can mitigate some of the more common disruptions, such as interruptions from software upgrades, network splits, and routing issues. Mitigation strategies include ensuring that pods on remote worker nodes request the correct amount of CPU and memory resources, configuring an appropriate replication policy, using redundancy across zones, and using Pod Disruption Budgets on workloads.

If the kube controller loses contact with a node after a configured period, the node controller on the control plane updates the node health to **Unhealthy** and marks the node **Ready** condition as **Unknown**. In response, the scheduler stops scheduling pods to that node. The on-premise node controller adds a `node.kubernetes.io/unreachable` taint with a `NoExecute` effect to the node and schedules pods on the node for eviction after five minutes, by default.

If a workload controller, such as a **Deployment** object or **StatefulSet** object, is directing traffic to pods on the unhealthy node and other nodes can reach the cluster, OpenShift Container Platform routes the traffic away from the pods on the node. Nodes that cannot reach the cluster do not get updated with the new traffic routing. As a result, the workloads on those nodes might continue to attempt to reach the unhealthy node.

You can mitigate the effects of connection loss by:

- using daemon sets to create pods that tolerate the taints
- using static pods that automatically restart if a node goes down
- using Kubernetes zones to control pod eviction
- configuring pod tolerations to delay or avoid pod eviction
- configuring the kubelet to control the timing of when it marks nodes as unhealthy.

For more information on using these objects in a cluster with remote worker nodes, see About remote worker node strategies.

### 8.1.2. Power loss on remote worker nodes

If a remote worker node loses power or restarts ungracefully, OpenShift Container Platform responds using several default mechanisms.

If the Kubernetes Controller Manager Operator (kube controller) loses contact with a node after a configured period, the control plane updates the node health to **Unhealthy** and marks the node **Ready** condition as **Unknown**. In response, the scheduler stops scheduling pods to that node. The on-premise node controller adds a `node.kubernetes.io/unreachable` taint with a `NoExecute` effect to the node and schedules pods on the node for eviction after five minutes, by default.

On the node, the pods must be restarted when the node recovers power and reconnects with the control plane.

**NOTE**

If you want the pods to restart immediately upon restart, use static pods.

After the node restarts, the kubelet also restarts and attempts to restart the pods that were scheduled.
on the node. If the connection to the control plane takes longer than the default five minutes, the control plane cannot update the node health and remove the `node.kubernetes.io/unreachable` taint. On the node, the kubelet terminates any running pods. When these conditions are cleared, the scheduler can start scheduling pods to that node.

You can mitigate the effects of power loss by:

- using daemon sets to create pods that tolerate the taints
- using static pods that automatically restart with a node
- configuring pods tolerations to delay or avoid pod eviction
- configuring the kubelet to control the timing of when the node controller marks nodes as unhealthy.

For more information on using these objects in a cluster with remote worker nodes, see About remote worker node strategies.

### 8.1.3. Latency spikes or temporary reduction in throughput to remote workers

All nodes send heartbeats to the Kubernetes Controller Manager Operator (kube controller) in the OpenShift Container Platform cluster every 10 seconds, by default. If the cluster does not receive heartbeats from a node, OpenShift Container Platform responds using several default mechanisms.

For example, if the Kubernetes Controller Manager Operator loses contact with a node after a configured period:

1. The node controller on the control plane updates the node health to **Unhealthy** and marks the node **Ready** condition as **Unknown**.
2. In response, the scheduler stops scheduling pods to that node.
3. The on-premise node controller adds a `node.kubernetes.io/unreachable` taint with a **NoExecute** effect to the node and schedules any pods on the node for eviction after five minutes, by default.

This behavior can cause problems if your network is prone to latency issues, especially if you have nodes at the network edge. In some cases, the Kubernetes Controller Manager Operator might not receive an update from a healthy node due to network latency. The Kubernetes Controller Manager Operator would then evict pods from the node even though the node is healthy. To avoid this problem, you can use **worker latency profiles** to adjust the frequency that the kubelet and the Kubernetes Controller Manager Operator wait for status updates before taking action. These adjustments help to ensure that your cluster runs properly in the event that network latency between the control plane and the worker nodes is not optimal.

These worker latency profiles are three sets of parameters that are pre-defined with carefully tuned values that let you control the reaction of the cluster to latency issues without needing to determine the best values manually.

**Additional resources**

- Improving cluster stability in high latency environments using worker latency profiles

### 8.1.4. Remote worker node strategies
If you use remote worker nodes, consider which objects to use to run your applications.

It is recommended to use daemon sets or static pods based on the behavior you want in the event of network issues or power loss. In addition, you can use Kubernetes zones and tolerations to control or avoid pod evictions if the control plane cannot reach remote worker nodes.

**Daemon sets**

Daemon sets are the best approach to managing pods on remote worker nodes for the following reasons:

- Daemon sets do not typically need rescheduling behavior. If a node disconnects from the cluster, pods on the node can continue to run. OpenShift Container Platform does not change the state of daemon set pods, and leaves the pods in the state they last reported. For example, if a daemon set pod is in the **Running** state, when a node stops communicating, the pod keeps running and is assumed to be running by OpenShift Container Platform.

- Daemon set pods, by default, are created with **NoExecute** tolerations for the `node.kubernetes.io/unreachable` and `node.kubernetes.io/not-ready` taints with no `tolerationSeconds` value. These default values ensure that daemon set pods are never evicted if the control plane cannot reach a node. For example:

  **Tolerations added to daemon set pods by default**

  ```yaml
  tolerations:
  - key: node.kubernetes.io/not-ready
    operator: Exists
    effect: NoExecute
  - key: node.kubernetes.io/unreachable
    operator: Exists
    effect: NoExecute
  - key: node.kubernetes.io/disk-pressure
    operator: Exists
    effect: NoSchedule
  - key: node.kubernetes.io/memory-pressure
    operator: Exists
    effect: NoSchedule
  - key: node.kubernetes.io/pid-pressure
    operator: Exists
    effect: NoSchedule
  - key: node.kubernetes.io/unschedulable
    operator: Exists
    effect: NoSchedule
  ```

- Daemon sets can use labels to ensure that a workload runs on a matching worker node.

- You can use an OpenShift Container Platform service endpoint to load balance daemon set pods.

**NOTE**

Daemon sets do not schedule pods after a reboot of the node if OpenShift Container Platform cannot reach the node.

**Static pods**

- **tolerations:**
  - key: node.kubernetes.io/not-ready
    operator: Exists
    effect: NoExecute
  - key: node.kubernetes.io/unreachable
    operator: Exists
    effect: NoExecute
  - key: node.kubernetes.io/disk-pressure
    operator: Exists
    effect: NoSchedule
  - key: node.kubernetes.io/memory-pressure
    operator: Exists
    effect: NoSchedule
  - key: node.kubernetes.io/pid-pressure
    operator: Exists
    effect: NoSchedule
  - key: node.kubernetes.io/unschedulable
    operator: Exists
    effect: NoSchedule

- **NOTE**

  Daemon sets do not schedule pods after a reboot of the node if OpenShift Container Platform cannot reach the node.
If you want pods restart if a node reboots, after a power loss for example, consider static pods. The kubelet on a node automatically restarts static pods as node restarts.

**NOTE**

Static pods cannot use secrets and config maps.

**Kubernetes zones**

Kubernetes zones can slow down the rate or, in some cases, completely stop pod evictions.

When the control plane cannot reach a node, the node controller, by default, applies `node.kubernetes.io/unreachable` taints and evicts pods at a rate of 0.1 nodes per second. However, in a cluster that uses Kubernetes zones, pod eviction behavior is altered.

If a zone is fully disrupted, where all nodes in the zone have a `Ready` condition that is `False` or `Unknown`, the control plane does not apply the `node.kubernetes.io/unreachable` taint to the nodes in that zone.

For partially disrupted zones, where more than 55% of the nodes have a `False` or `Unknown` condition, the pod eviction rate is reduced to 0.01 nodes per second. Nodes in smaller clusters, with fewer than 50 nodes, are not tainted. Your cluster must have more than three zones for these behavior to take effect.

You assign a node to a specific zone by applying the `topology.kubernetes.io/region` label in the node specification.

**Sample node labels for Kubernetes zones**

```yaml
kind: Node
apiVersion: v1
metadata:
  labels:
    topology.kubernetes.io/region=east
```

**KubeletConfig objects**

You can adjust the amount of time that the kubelet checks the state of each node.

To set the interval that affects the timing of when the on-premise node controller marks nodes with the Unhealthy or Unreachable condition, create a KubeletConfig object that contains the `node-status-update-frequency` and `node-status-report-frequency` parameters.

The kubelet on each node determines the node status as defined by the `node-status-update-frequency` setting and reports that status to the cluster based on the `node-status-report-frequency` setting. By default, the kubelet determines the pod status every 10 seconds and reports the status every minute. However, if the node state changes, the kubelet reports the change to the cluster immediately. OpenShift Container Platform uses the `node-status-report-frequency` setting only when the Node Lease feature gate is enabled, which is the default state in OpenShift Container Platform clusters. If the Node Lease feature gate is disabled, the node reports its status based on the `node-status-update-frequency` setting.

**Example kubelet config**

```yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
```
Specify the type of node type to which this KubeletConfig object applies using the label from the MachineConfig object.

Specify the frequency that the kubelet checks the status of a node associated with this MachineConfig object. The default value is 10s. If you change this default, the node-status-report-frequency value is changed to the same value.

Specify the frequency that the kubelet reports the status of a node associated with this MachineConfig object. The default value is 1m.

The node-status-update-frequency parameter works with the node-monitor-grace-period and pod-eviction-timeout parameters.

- The node-monitor-grace-period parameter specifies how long OpenShift Container Platform waits after a node associated with a MachineConfig object is marked Unhealthy if the controller manager does not receive the node heartbeat. Workloads on the node continue to run after this time. If the remote worker node rejoins the cluster after node-monitor-grace-period expires, pods continue to run. New pods can be scheduled to that node. The node-monitor-grace-period interval is 40s. The node-status-update-frequency value must be lower than the node-monitor-grace-period value.

- The pod-eviction-timeout parameter specifies the amount of time OpenShift Container Platform waits after marking a node that is associated with a MachineConfig object as Unreachable to start marking pods for eviction. Evicted pods are rescheduled on other nodes. If the remote worker node rejoins the cluster after pod-eviction-timeout expires, the pods running on the remote worker node are terminated because the node controller has evicted the pods on-premise. Pods can then be rescheduled to that node. The pod-eviction-timeout interval is 5m0s.

NOTE

Modifying the node-monitor-grace-period and pod-eviction-timeout parameters is not supported.

Tolerations

You can use pod tolerations to mitigate the effects if the on-premise node controller adds a node.kubernetes.io/unreachable taint with a NoExecute effect to a node it cannot reach.

A taint with the NoExecute effect affects pods that are running on the node in the following ways:

- Pods that do not tolerate the taint are queued for eviction.
Pods that tolerate the taint without specifying a `tolerationSeconds` value in their toleration specification remain bound forever.

Pods that tolerate the taint with a specified `tolerationSeconds` value remain bound for the specified amount of time. After the time elapses, the pods are queued for eviction.

You can delay or avoid pod eviction by configuring pods tolerations with the `NoExecute` effect for the `node.kubernetes.io/unreachable` and `node.kubernetes.io/not-ready` taints.

**Example toleration in a pod spec**

```yaml
... 
  tolerations:
    - key: "node.kubernetes.io/unreachable"
      operator: "Exists"
      effect: "NoExecute" ①
    - key: "node.kubernetes.io/not-ready"
      operator: "Exists"
      effect: "NoExecute" ②
      tolerationSeconds: 600
... 
```

① The `NoExecute` effect without `tolerationSeconds` lets pods remain forever if the control plane cannot reach the node.

② The `NoExecute` effect with `tolerationSeconds`: 600 lets pods remain for 10 minutes if the control plane marks the node as Unhealthy.

OpenShift Container Platform uses the `tolerationSeconds` value after the `pod-eviction-timeout` value elapses.

**Other types of OpenShift Container Platform objects**

You can use replica sets, deployments, and replication controllers. The scheduler can reschedule these pods onto other nodes after the node is disconnected for five minutes. Rescheduling onto other nodes can be beneficial for some workloads, such as REST APIs, where an administrator can guarantee a specific number of pods are running and accessible.

**NOTE**

When working with remote worker nodes, rescheduling pods on different nodes might not be acceptable if remote worker nodes are intended to be reserved for specific functions.

Stateful sets do not get restarted when there is an outage. The pods remain in the *terminating* state until the control plane can acknowledge that the pods are terminated.

To avoid scheduling a to a node that does not have access to the same type of persistent storage, OpenShift Container Platform cannot migrate pods that require persistent volumes to other zones in the case of network separation.

**Additional resources**

- For more information on Daemonesets, see DaemonSets.
- For more information on taints and tolerations, see *Controlling pod placement using node taints*.

- For more information on configuring *KubeletConfig* objects, see *Creating a KubeletConfig CRD*.

- For more information on replica sets, see *ReplicaSets*.

- For more information on deployments, see *Deployments*.

- For more information on replication controllers, see *Replication controllers*.

- For more information on the controller manager, see *Kubernetes Controller Manager Operator*.
CHAPTER 9. WORKER NODES FOR SINGLE-NODE OPENSHIFT CLUSTERS

9.1. ADDING WORKER NODES TO SINGLE-NODE OPENSHIFT CLUSTERS

Single-node OpenShift clusters reduce the host prerequisites for deployment to a single host. This is useful for deployments in constrained environments or at the network edge. However, sometimes you need to add additional capacity to your cluster, for example, in telecommunications and network edge scenarios. In these scenarios, you can add worker nodes to the single-node cluster.

There are several ways that you can add worker nodes to a single-node cluster. You can add worker nodes to a cluster manually, using Red Hat OpenShift Cluster Manager, or by using the Assisted Installer REST API directly.

**IMPORTANT**

Adding worker nodes does not expand the cluster control plane, and it does not provide high availability to your cluster. For single-node OpenShift clusters, high availability is handled by failing over to another site. It is not recommended to add a large number of worker nodes to a single-node cluster.

**NOTE**

Unlike multi-node clusters, by default all ingress traffic is routed to the single control-plane node, even after adding additional worker nodes.

9.1.1. Requirements for installing single-node OpenShift worker nodes

To install a single-node OpenShift worker node, you must address the following requirements:

- **Administration host**: You must have a computer to prepare the ISO and to monitor the installation.

- **Production-grade server**: Installing single-node OpenShift worker nodes requires a server with sufficient resources to run OpenShift Container Platform services and a production workload.

Table 9.1. Minimum resource requirements

<table>
<thead>
<tr>
<th>Profile</th>
<th>vCPU</th>
<th>Memory</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>2 vCPU cores</td>
<td>8GB of RAM</td>
<td>100GB</td>
</tr>
</tbody>
</table>

**NOTE**

One vCPU is equivalent to one physical core when simultaneous multithreading (SMT), or hyperthreading, is not enabled. When enabled, use the following formula to calculate the corresponding ratio:

\[(\text{threads per core} \times \text{cores}) \times \text{sockets} = \text{vCPUs}\]
The server must have a Baseboard Management Controller (BMC) when booting with virtual media.

- **Networking**: The worker node server must have access to the internet or access to a local registry if it is not connected to a routable network. The worker node server must have a DHCP reservation or a static IP address and be able to access the single-node OpenShift cluster Kubernetes API, ingress route, and cluster node domain names. You must configure the DNS to resolve the IP address to each of the following fully qualified domain names (FQDN) for the single-node OpenShift cluster:

<table>
<thead>
<tr>
<th>Usage</th>
<th>FQDN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kubernetes API</td>
<td>api.&lt;cluster_name&gt;.&lt;base_domain&gt;</td>
<td>Add a DNS A/AAAA or CNAME record. This record must be resolvable by clients external to the cluster.</td>
</tr>
<tr>
<td>Internal API</td>
<td>api-int.&lt;cluster_name&gt;.&lt;base_domain&gt;</td>
<td>Add a DNS A/AAAA or CNAME record when creating the ISO manually. This record must be resolvable by nodes within the cluster.</td>
</tr>
<tr>
<td>Ingress route</td>
<td>*.apps.&lt;cluster_name&gt;.&lt;base_domain&gt;</td>
<td>Add a wildcard DNS A/AAAA or CNAME record that targets the node. This record must be resolvable by clients external to the cluster.</td>
</tr>
</tbody>
</table>

Without persistent IP addresses, communications between the **apiserver** and **etcd** might fail.

**Additional resources**

- Minimum resource requirements for cluster installation
- Recommended practices for scaling the cluster
- User-provisioned DNS requirements
- Creating a bootable ISO image on a USB drive
- Booting from an ISO image served over HTTP using the Redfish API
- Deleting nodes from a cluster

**9.1.2. Adding worker nodes using the Assisted Installer and OpenShift Cluster Manager**

You can add worker nodes to single-node OpenShift clusters that were created on Red Hat OpenShift Cluster Manager using the **Assisted Installer**.
**IMPORTANT**

Adding worker nodes to single-node OpenShift clusters is only supported for clusters running OpenShift Container Platform version 4.11 and up.

**Prerequisites**

- Have access to a single-node OpenShift cluster installed using Assisted Installer.
- Install the OpenShift CLI (oc).
- Log in as a user with `cluster-admin` privileges.
- Ensure that all the required DNS records exist for the cluster that you are adding the worker node to.

**Procedure**

1. Log in to OpenShift Cluster Manager and click the single-node cluster that you want to add a worker node to.
2. Click **Add hosts**, and download the discovery ISO for the new worker node, adding SSH public key and configuring cluster-wide proxy settings as required.
3. Boot the target host using the discovery ISO, and wait for the host to be discovered in the console. After the host is discovered, start the installation.
4. As the installation proceeds, the installation generates pending certificate signing requests (CSRs) for the worker node. When prompted, approve the pending CSRs to complete the installation.
   
   When the worker node is successfully installed, it is listed as a worker node in the cluster web console.

**Additional resources**

- User-provisioned DNS requirements
- Approving the certificate signing requests for your machines

**9.1.3. Adding worker nodes using the Assisted Installer API**

You can add worker nodes to single-node OpenShift clusters using the Assisted Installer REST API. Before you add worker nodes, you must log in to OpenShift Cluster Manager and authenticate against the API.

**9.1.3.1. Authenticating against the Assisted Installer REST API**

Before you can use the Assisted Installer REST API, you must authenticate against the API using a JSON web token (JWT) that you generate.

**Prerequisites**

- Log in to OpenShift Cluster Manager as a user with cluster creation privileges.
- Install `jq`. 
Procedure

1. Log in to OpenShift Cluster Manager and copy your API token.

2. Set the `$OFFLINE_TOKEN` variable using the copied API token by running the following command:

   ```bash
   $ export OFFLINE_TOKEN=<copied_api_token>
   ```

3. Set the `$JWT_TOKEN` variable using the previously set `$OFFLINE_TOKEN` variable:

   ```bash
   $ export JWT_TOKEN=$(curl \
   --silent \
   --header "Accept: application/json" \
   --header "Content-Type: application/x-www-form-urlencoded" \
   --data-urlencode "grant_type=refresh_token" \
   --data-urlencode "client_id=cloud-services" \
   --data-urlencoded "refresh_token=${OFFLINE_TOKEN}" \
   "https://sso.redhat.com/auth/realms/redhat-external/protocol/openid-connect/token" \
   | jq --raw-output ".access_token"
   )
   ```

   **NOTE**

   The JWT token is valid for 15 minutes only.

Verification

- Optional: Check that you can access the API by running the following command:

  ```bash
  ```

Example output

```json
{
   "release_tag": "v2.5.1",
   "versions":
   {
      "assisted-installer": "registry.redhat.io/rhai-tech-preview/assisted-installer-rhel8:v1.0.0-175",
      "assisted-installer-controller": "registry.redhat.io/rhai-tech-preview/assisted-installer-reporter-rhel8:v1.0.0-223",
      "assisted-installer-service": "quay.io/app-sre/assisted-service:ac87f93",
      "discovery-agent": "registry.redhat.io/rhai-tech-preview/assisted-installer-agent-rhel8:v1.0.0-156"
   }
}
```

9.1.3.2. Adding worker nodes using the Assisted Installer REST API

You can add worker nodes to clusters using the Assisted Installer REST API.
Prerequisites

- Install the OpenShift Cluster Manager CLI (ocm).
- Log in to OpenShift Cluster Manager as a user with cluster creation privileges.
- Install jq.
- Ensure that all the required DNS records exist for the cluster that you are adding the worker node to.

Procedure

1. Authenticate against the Assisted Installer REST API and generate a JSON web token (JWT) for your session. The generated JWT token is valid for 15 minutes only.

   ```
   $ export API_URL=<api_url>  
   1 Replace <api_url> with the Assisted Installer API URL, for example, https://api.openshift.com
   ```

2. Set the $API_URL variable by running the following command:

   ```
   $ export API_URL=<api_url>  
   1 Replace <api_url> with the Assisted Installer API URL, for example, https://api.openshift.com
   ```

3. Import the single-node OpenShift cluster by running the following commands:

   a. Set the $OPENSHIFT_CLUSTER_ID variable. Log in to the cluster and run the following command:

      ```
      $ export OPENSHIFT_CLUSTER_ID=$(oc get clusterversion -o jsonpath='{.items[].spec.clusterID}')
      ```

   b. Set the $CLUSTER_REQUEST variable that is used to import the cluster:

      ```
      $ export CLUSTER_REQUEST=$(jq --null-input --arg openshift_cluster_id "$OPENSHIFT_CLUSTER_ID" '{
      "api_vip_dnsname": "<api_vip>", 1
      "openshift_cluster_id": $openshift_cluster_id,
      "name": "<openshift_cluster_name>" 2
      }')
      ```

      1 Replace <api_vip> with the hostname for the cluster’s API server. This can be the DNS domain for the API server or the IP address of the single node which the worker node can reach. For example, api.compute-1.example.com.

      2 Replace <openshift_cluster_name> with the plain text name for the cluster. The cluster name should match the cluster name that was set during the Day 1 cluster installation.

   c. Import the cluster and set the $CLUSTER_ID variable. Run the following command:

      ```
      $ CLUSTER_ID=$(curl "$API_URL/api/assisted-install/v2/clusters/import" -H "Authorization: Bearer ${JWT_TOKEN}" -H 'accept: application/json' -H 'Content-Type: application/json' \
      ```
4. Generate the InfraEnv resource for the cluster and set the $INFRA_ENV_ID variable by running the following commands:
   
a. Download the pull secret file from Red Hat OpenShift Cluster Manager at console.redhat.com.

b. Set the $INFRA_ENV_REQUEST variable:

   ```bash
   export INFRA_ENV_REQUEST=$(jq --null-input \
   --slurpfile pull_secret <path_to_pull_secret_file> \n   --arg ssh_pub_key "$(cat <path_to_ssh_pub_key>)" \n   --arg cluster_id "$CLUSTER_ID" '{\n   "name": "<infraenv_name>", \n   "pull_secret": $pull_secret[0] | tojson, \n   "cluster_id": $cluster_id, \n   "ssh_authorized_key": $ssh_pub_key, \n   "image_type": "<iso_image_type>" \n   }')
   ```

   1 Replace `<path_to_pull_secret_file>` with the path to the local file containing the downloaded pull secret from Red Hat OpenShift Cluster Manager at console.redhat.com.

   2 Replace `<path_to_ssh_pub_key>` with the path to the public SSH key required to access the host. If you do not set this value, you cannot access the host while in discovery mode.

   3 Replace `<infraenv_name>` with the plain text name for the InfraEnv resource.

   4 Replace `<iso_image_type>` with the ISO image type, either full-iso or minimal-iso.

c. Post the $INFRA_ENV_REQUEST to the /v2/infra-envs API and set the $INFRA_ENV_ID variable:

   ```bash
   $ INFRA_ENV_ID=$(curl -s "$API_URL/api/assisted-install/v2/infra-envs" -H "Authorization: Bearer $[JWT_TOKEN]" -H 'accept: application/json' -H 'Content-Type: application/json' -d "$INFRA_ENV_REQUEST" | tee /dev/stderr | jq -r '.id')
   ```

5. Get the URL of the discovery ISO for the cluster worker node by running the following command:

   ```bash
   $ curl -s "$API_URL/api/assisted-install/v2/infra-envs/$INFRA_ENV_ID" -H "Authorization: Bearer $[JWT_TOKEN]" | jq -r '.download_url'
   ```

Example output

https://api.openshift.com/api/assisted-images/images/41b91e72-c33e-42ee-b80f-b5c55bb6431a?arch=x86_64&image_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2NTYwMjYzNzEsInN1YiI6IjQxYjkxZTcyLWMzM2UtNDJiZS1iODBmLWI1YzViYmY2NDMxYSJ9.1EX_VGaMNeJmhrAvVRBS7PDIQtb00c8ltg8OukE1a4&type=minimal-iso&version=4.11
6. Download the ISO:

```bash
$ curl -L -s '<iso_url>' --output rhcos-live-minimal.iso
```

1. Replace `<iso_url>` with the URL for the ISO from the previous step.

7. Boot the new worker host from the downloaded `rhcos-live-minimal.iso`.

8. Get the list of hosts in the cluster that are not installed. Keep running the following command until the new host shows up:

```bash
$ curl -s "$API_URL/api/assisted-install/v2/clusters/$CLUSTER_ID" -H "Authorization: Bearer ${JWT_TOKEN}" | jq -r '.hosts[] | select(.status != "installed").id'
```

**Example output**

```
2294ba03-c264-4f11-ac08-2f1bb2f8c296
```

9. Set the `$HOST_ID` variable for the new worker node, for example:

```bash
$ HOST_ID=<host_id>
```

1. Replace `<host_id>` with the host ID from the previous step.

10. Check that the host is ready to install by running the following command:

```bash
$ curl -s $API_URL/api/assisted-install/v2/clusters/$CLUSTER_ID -H "Authorization: Bearer ${JWT_TOKEN}" | jq 'def host_name($host):
if (.suggested_hostname // "") == "" then
  if (.inventory // "") == "" then
    "Unknown hostname, please wait"
  else
    .inventory | fromjson | .hostname
  end
else
  .suggested_hostname
end;

def is_notable($validation):
  ["failure", "pending", "error"] | any(. == $validation.status);

def notable_validations($validations_info):
[  $validations_info // "{"[
    | fromjson
  | to_entries[]].value
```
"Hosts validations": {
  "Hosts": [
    .hosts[
      | select(.status != "installed")
    ]
    | {
      "id": .id,
      "name": host_name(.),
      "status": .status,
      "notable_validations": notable_validations(.validations_info)
    }
  ],
  "Cluster validations info": {
    "notable_validations": notable_validations(.validations_info)
  }
}

Example output

{ "Hosts validations": {
  "Hosts": [
    {
      "id": "97ec378c-3568-460c-bc22-df54534ff08f",
      "name": "localhost.localdomain",
      "status": "insufficient",
      "notable_validations": [
        {
          "id": "ntp-synced",
          "status": "failure",
          "message": "Host couldn't synchronize with any NTP server"
        },
        {
          "id": "api-domain-name-resolved-correctly",
          "status": "error",
          "message": "Parse error for domain name resolutions result"
        },
        {
          "id": "api-int-domain-name-resolved-correctly",
          "status": "error",
          "message": "Parse error for domain name resolutions result"
        },
        {
          "id": "apps-domain-name-resolved-correctly",
          "status": "error",
          "message": "Parse error for domain name resolutions result"
        }
      ]
    }
    ]
  }
}
When the previous command shows that the host is ready, start the installation using the `/v2/infra-envs/{infra_env_id}/hosts/{host_id}/actions/install` API by running the following command:

```
$ curl -X POST -s "$API_URL/api/assisted-install/v2/infra-envs/{INFRA_ENV_ID}/hosts/{HOST_ID}/actions/install" -H "Authorization: Bearer ${JWT_TOKEN}"
```

As the installation proceeds, the installation generates pending certificate signing requests (CSRs) for the worker node.

**IMPORTANT**

You must approve the CSRs to complete the installation.

Keep running the following API call to monitor the cluster installation:

```
$ curl -s "$API_URL/api/assisted-install/v2/clusters/$CLUSTER_ID" -H "Authorization: Bearer ${JWT_TOKEN}" | jq '{
  "Cluster day-2 hosts": [
    .hosts[]
    | select(.status != "installed")
    | {id, requested_hostname, status, status_info, progress, status_updated_at, updated_at, infra_env_id, cluster_id, created_at}
  ]
}'
```

**Example output**

```
{
  "Cluster day-2 hosts": [
    {
      "id": "a1c52dde-3432-4f59-b2ae-0a530c851480",
      "requested_hostname": "control-plane-1",
      "status": "added-to-existing-cluster",
      "status_info": "Host has rebooted and no further updates will be posted. Please check console for progress and to possibly approve pending CSRs",
      "progress": {
        "current_stage": "Done",
        "installation_percentage": 100,
        "stage_started_at": "2022-07-08T10:56:20.476Z",
        "stage_updated_at": "2022-07-08T10:56:20.476Z"
      },
      "status_updated_at": "2022-07-08T10:56:20.476Z",
      "updated_at": "2022-07-08T10:57:15.306369Z",
      "infra_env_id": "b74ec0c3-d5b5-4717-a866-5b6854791bd3",
      "cluster_id": "8f721322-419d-4eed-aa5b-61b50ea586ae",
      "created_at": "2022-07-06T22:54:57.161614Z"
    }
  ]
}```
13. Optional: Run the following command to see all the events for the cluster:

```
$ curl -s "$API_URL/api/assisted-install/v2/events?cluster_id=$CLUSTER_ID" -H "Authorization: Bearer ${JWT_TOKEN}" | jq -c '.[] | {severity, message, event_time, host_id}'
```

**Example output**

```json
{"severity":"info","message":"Host compute-0: updated status from insufficient to known (Host is ready to be installed)","event_time":"2022-07-08T11:21:46.346Z","host_id":"9d7b3b44-1125-4ad0-9b14-76550087b445"}
{"severity":"info","message":"Host compute-0: updated status from known to installing (Installation is in progress)","event_time":"2022-07-08T11:28:28.647Z","host_id":"9d7b3b44-1125-4ad0-9b14-76550087b445"}
{"severity":"info","message":"Host compute-0: updated status from installing to installing-in-progress (Starting installation)","event_time":"2022-07-08T11:28:52.068Z","host_id":"9d7b3b44-1125-4ad0-9b14-76550087b445"}
{"severity":"info","message":"Uploaded logs for host compute-0 cluster 8f721322-419d-4eed-aa5b-61b50ea586ae","event_time":"2022-07-08T11:29:47.802Z","host_id":"9d7b3b44-1125-4ad0-9b14-76550087b445"}
{"severity":"info","message":"Host compute-0: updated status from installing-in-progress to added-to-existing-cluster (Host has rebooted and no further updates will be posted. Please check console for progress and to possibly approve pending CSRs)","event_time":"2022-07-08T11:29:48.259Z","host_id":"9d7b3b44-1125-4ad0-9b14-76550087b445"}
{"severity":"info","message":"Host: compute-0, reached installation stage Rebooting","event_time":"2022-07-08T11:29:48.261Z","host_id":"9d7b3b44-1125-4ad0-9b14-76550087b445"}
```

14. Log in to the cluster and approve the pending CSRs to complete the installation.

**Verification**

- Check that the new worker node was successfully added to the cluster with a status of **Ready**:

  `$ oc get nodes`

**Example output**

```
NAME                           STATUS   ROLES           AGE   VERSION
control-plane-1.example.com    Ready    master,worker   56m   v1.24.0+beaaed6
compute-1.example.com          Ready    worker          11m   v1.24.0+beaaed6
```

**Additional resources**

- User-provisioned DNS requirements
- Approving the certificate signing requests for your machines

**9.1.4. Adding worker nodes to single-node OpenShift clusters manually**
You can add a worker node to a single-node OpenShift cluster manually by booting the worker node from Red Hat Enterprise Linux CoreOS (RHCOS) ISO and using the cluster `worker.ign` file to join the new worker node to the cluster.

**Prerequisites**

- Install a single-node OpenShift cluster on bare metal.
- Install the OpenShift CLI (`oc`).
- Log in as a user with `cluster-admin` privileges.
- Ensure that all the required DNS records exist for the cluster that you are adding the worker node to.

**Procedure**

1. Set the OpenShift Container Platform version:

   ```bash
   $ OCP_VERSION=<ocp_version>
   ```

   Replace `<ocp_version>` with the current version, for example, `latest-4.11`

2. Set the host architecture:

   ```bash
   $ ARCH=<architecture>
   ```

   Replace `<architecture>` with the target host architecture, for example, `aarch64` or `x86_64`.

3. Get the `worker.ign` data from the running single-node cluster by running the following command:

   ```bash
   $ oc extract -n openshift-machine-api secret/worker-user-data --keys=userData --to=- > worker.ign
   ```

4. Host the `worker.ign` file on a web server accessible from your network.

5. Download the OpenShift Container Platform installer and make it available for use by running the following commands:

   ```bash
   
   $ tar zxvf openshift-install-linux.tar.gz
   
   $ chmod +x openshift-install
   ```

6. Retrieve the RHCOS ISO URL:
Use the RHCOS ISO and the hosted worker.ign file to install the worker node:

a. Boot the target host using the RHCOS ISO and your preferred method of installation.

b. When the target host has booted from the RHCOS ISO, open a console on the target host, and run the following coreos-installer command to install the system:

```
$ coreos-installer install --ignition-url=<hosted_worker_ign_file> <hard_disk>
```

where:

- `<hosted_worker_ign_file>` is the locally accessible URL for the hosted worker.ign file, for example, http://webserver.example.com/worker.ign
- `<hard_disk>` is hard disk where you install RHCOS, for example, /dev/sda.

8. As the installation proceeds, the installation generates pending certificate signing requests (CSRs) for the worker node. When prompted, approve the pending CSRs to complete the installation.

9. When the install is complete, reboot the host. The host joins the cluster as a new worker node.

**Verification**

- Check that the new worker node was successfully added to the cluster with a status of Ready:

```
$ oc get nodes
```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>ROLES</th>
<th>AGE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>control-plane-1.example.com</td>
<td>Ready</td>
<td>master, worker</td>
<td>56m</td>
<td>v1.24.0+beaaed6</td>
</tr>
<tr>
<td>compute-1.example.com</td>
<td>Ready</td>
<td>worker</td>
<td>11m</td>
<td>v1.24.0+beaaed6</td>
</tr>
</tbody>
</table>

**Additional resources**

- User-provisioned DNS requirements
- Approving the certificate signing requests for your machines

**9.1.5. Approving the certificate signing requests for your machines**

When you add machines to a cluster, two pending certificate signing requests (CSRs) are generated for each machine that you added. You must confirm that these CSRs are approved or, if necessary, approve them yourself. The client requests must be approved first, followed by the server requests.

**Prerequisites**

- You added machines to your cluster.
Procedure

1. Confirm that the cluster recognizes the machines:

   $ oc get nodes

   **Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>ROLES</th>
<th>AGE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>master-0</td>
<td>Ready</td>
<td>master</td>
<td>63m</td>
<td>v1.24.0</td>
</tr>
<tr>
<td>master-1</td>
<td>Ready</td>
<td>master</td>
<td>63m</td>
<td>v1.24.0</td>
</tr>
<tr>
<td>master-2</td>
<td>Ready</td>
<td>master</td>
<td>64m</td>
<td>v1.24.0</td>
</tr>
</tbody>
</table>

   The output lists all of the machines that you created.

   **NOTE**

   The preceding output might not include the compute nodes, also known as worker nodes, until some CSRs are approved.

2. Review the pending CSRs and ensure that you see the client requests with the **Pending** or **Approved** status for each machine that you added to the cluster:

   $ oc get csr

   **Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>AGE</th>
<th>REQUESTOR</th>
<th>CONDITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>csr-8b2br</td>
<td>15m</td>
<td>system:serviceaccount:openshift-machine-config-operator:node-bootstrapper</td>
<td>Pending</td>
</tr>
<tr>
<td>csr-8vnps</td>
<td>15m</td>
<td>system:serviceaccount:openshift-machine-config-operator:node-bootstrapper</td>
<td>Pending</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

   In this example, two machines are joining the cluster. You might see more approved CSRs in the list.

3. If the CSRs were not approved, after all of the pending CSRs for the machines you added are in **Pending** status, approve the CSRs for your cluster machines:

   **NOTE**

   Because the CSRs rotate automatically, approve your CSRs within an hour of adding the machines to the cluster. If you do not approve them within an hour, the certificates will rotate, and more than two certificates will be present for each node. You must approve all of these certificates. After the client CSR is approved, the Kubelet creates a secondary CSR for the serving certificate, which requires manual approval. Then, subsequent serving certificate renewal requests are automatically approved by the **machine-approver** if the Kubelet requests a new certificate with identical parameters.
NOTE
For clusters running on platforms that are not machine API enabled, such as bare metal and other user-provisioned infrastructure, you must implement a method of automatically approving the kubelet serving certificate requests (CSRs). If a request is not approved, then the `oc exec`, `oc rsh`, and `oc logs` commands cannot succeed, because a serving certificate is required when the API server connects to the kubelet. Any operation that contacts the Kubelet endpoint requires this certificate approval to be in place. The method must watch for new CSRs, confirm that the CSR was submitted by the `node-bootstrapper` service account in the `system:node` or `system:admin` groups, and confirm the identity of the node.

- To approve them individually, run the following command for each valid CSR:

  ```
  $ oc adm certificate approve <csr_name>
  ```

  `<csr_name>` is the name of a CSR from the list of current CSRs.

- To approve all pending CSRs, run the following command:

  ```
  $ oc get csr -o go-template="{{range .items}}{{if not .status}}{{.metadata.name}}{{"\n"}}{{end}}{{end}}\t| xargs --no-run-if-empty oc adm certificate approve
  ```

NOTE
Some Operators might not become available until some CSRs are approved.

4. Now that your client requests are approved, you must review the server requests for each machine that you added to the cluster:

  ```
  $ oc get csr
  ```

**Example output**

<table>
<thead>
<tr>
<th>NAME</th>
<th>AGE</th>
<th>REQUESTOR</th>
<th>CONDITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>csr-bfd72</td>
<td>5m26s</td>
<td>system:node:ip-10-0-50-126.us-east-2.compute.internal</td>
<td>Pending</td>
</tr>
<tr>
<td>csr-c57lv</td>
<td>5m26s</td>
<td>system:node:ip-10-0-95-157.us-east-2.compute.internal</td>
<td>Pending</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. If the remaining CSRs are not approved, and are in the **Pending** status, approve the CSRs for your cluster machines:

- To approve them individually, run the following command for each valid CSR:

  ```
  $ oc adm certificate approve <csr_name>
  ```

  `<csr_name>` is the name of a CSR from the list of current CSRs.
To approve all pending CSRs, run the following command:

```bash
$ oc get csr -o go-template="{{range .items}}{{if not .status}}{{.metadata.name}}{{"\n"}}{{end}}{{end}}' | xargs oc adm certificate approve
```

6. After all client and server CSRs have been approved, the machines have the **Ready** status. Verify this by running the following command:

```bash
$ oc get nodes
```

**Example output**

```
NAME      STATUS    ROLES   AGE  VERSION
master-0  Ready     master  73m  v1.24.0
master-1  Ready     master  73m  v1.24.0
master-2  Ready     master  74m  v1.24.0
worker-0  Ready     worker  11m  v1.24.0
worker-1  Ready     worker  11m  v1.24.0
```

**NOTE**

It can take a few minutes after approval of the server CSRs for the machines to transition to the **Ready** status.

**Additional information**

- For more information on CSRs, see Certificate Signing Requests.