



OpenShift Container Platform 4.9

Scalability and performance

Scaling your OpenShift Container Platform cluster and tuning performance in production environments

OpenShift Container Platform 4.9 Scalability and performance

Scaling your OpenShift Container Platform cluster and tuning performance in production environments

Legal Notice

Copyright © 2022 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

This document provides instructions for scaling your cluster and optimizing the performance of your OpenShift Container Platform environment.

Table of Contents

CHAPTER 1. RECOMMENDED PRACTICES FOR INSTALLING LARGE CLUSTERS	8
1.1. RECOMMENDED PRACTICES FOR INSTALLING LARGE SCALE CLUSTERS	8
CHAPTER 2. RECOMMENDED HOST PRACTICES	9
2.1. RECOMMENDED NODE HOST PRACTICES	9
2.2. CREATING A KUBELETCONFIG CRD TO EDIT KUBELET PARAMETERS	10
2.3. MODIFYING THE NUMBER OF UNAVAILABLE WORKER NODES	14
2.4. CONTROL PLANE NODE SIZING	14
2.4.1. Increasing the flavor size of the Amazon Web Services (AWS) master instances	16
2.5. RECOMMENDED ETCD PRACTICES	17
2.6. DEFRAGMENTING ETCD DATA	18
2.6.1. Automatic defragmentation	18
2.6.2. Manual defragmentation	18
2.7. OPENSIFT CONTAINER PLATFORM INFRASTRUCTURE COMPONENTS	21
2.8. MOVING THE MONITORING SOLUTION	22
2.9. MOVING THE DEFAULT REGISTRY	23
2.10. MOVING THE ROUTER	24
2.11. INFRASTRUCTURE NODE SIZING	26
2.12. ADDITIONAL RESOURCES	27
CHAPTER 3. RECOMMENDED HOST PRACTICES FOR IBM Z & LINUXONE ENVIRONMENTS	28
3.1. MANAGING CPU OVERCOMMITMENT	28
3.2. HOW TO DISABLE TRANSPARENT HUGE PAGES	28
3.2.1. Disable THP with a Node Tuning Operator (NTO) profile	29
3.3. BOOST NETWORKING PERFORMANCE WITH RECEIVE FLOW STEERING	30
3.3.1. Use the Machine Config Operator (MCO) to activate RFS	30
3.4. CHOOSE YOUR NETWORKING SETUP	31
3.5. ENSURE HIGH DISK PERFORMANCE WITH HYPERPAV ON Z/VM	31
3.5.1. Use the Machine Config Operator (MCO) to activate HyperPAV aliases in nodes using z/VM full-pack minidisks	32
3.6. RHEL KVM ON IBM Z HOST RECOMMENDATIONS	33
3.6.1. Use multiple queues for your VirtIO network interfaces	33
3.6.2. Use I/O threads for your virtual block devices	33
3.6.3. Avoid virtual SCSI devices	34
3.6.4. Configure guest caching for disk	34
3.6.5. Exclude the memory balloon device	34
3.6.6. Tune the CPU migration algorithm of the host scheduler	35
3.6.7. Disable the cpuset cgroup controller	35
3.6.8. Tune the polling period for idle virtual CPUs	36
CHAPTER 4. RECOMMENDED CLUSTER SCALING PRACTICES	37
4.1. RECOMMENDED PRACTICES FOR SCALING THE CLUSTER	37
4.2. MODIFYING A MACHINE SET	37
4.3. ABOUT MACHINE HEALTH CHECKS	39
4.3.1. Limitations when deploying machine health checks	39
4.4. SAMPLE MACHINEHEALTHCHECK RESOURCE	40
4.4.1. Short-circuiting machine health check remediation	41
4.4.1.1. Setting maxUnhealthy by using an absolute value	41
4.4.1.2. Setting maxUnhealthy by using percentages	41
4.5. CREATING A MACHINEHEALTHCHECK RESOURCE	42
CHAPTER 5. USING THE NODE TUNING OPERATOR	43

5.1. ABOUT THE NODE TUNING OPERATOR	43
5.2. ACCESSING AN EXAMPLE NODE TUNING OPERATOR SPECIFICATION	43
5.3. DEFAULT PROFILES SET ON A CLUSTER	44
5.4. VERIFYING THAT THE TUNED PROFILES ARE APPLIED	44
5.5. CUSTOM TUNING SPECIFICATION	44
5.6. CUSTOM TUNING EXAMPLES	48
5.7. SUPPORTED TUNED DAEMON PLUG-INS	50
CHAPTER 6. USING CLUSTER LOADER	52
6.1. INSTALLING CLUSTER LOADER	52
6.2. RUNNING CLUSTER LOADER	52
6.3. CONFIGURING CLUSTER LOADER	53
6.3.1. Example Cluster Loader configuration file	53
6.3.2. Configuration fields	54
6.4. KNOWN ISSUES	57
CHAPTER 7. USING CPU MANAGER	58
7.1. SETTING UP CPU MANAGER	58
CHAPTER 8. USING TOPOLOGY MANAGER	63
8.1. TOPOLOGY MANAGER POLICIES	63
8.2. SETTING UP TOPOLOGY MANAGER	64
8.3. POD INTERACTIONS WITH TOPOLOGY MANAGER POLICIES	64
CHAPTER 9. SCALING THE CLUSTER MONITORING OPERATOR	66
9.1. PROMETHEUS DATABASE STORAGE REQUIREMENTS	66
9.2. CONFIGURING CLUSTER MONITORING	67
CHAPTER 10. PLANNING YOUR ENVIRONMENT ACCORDING TO OBJECT MAXIMUMS	69
10.1. OPENSIFT CONTAINER PLATFORM TESTED CLUSTER MAXIMUMS FOR MAJOR RELEASES	69
10.2. OPENSIFT CONTAINER PLATFORM ENVIRONMENT AND CONFIGURATION ON WHICH THE CLUSTER MAXIMUMS ARE TESTED	70
10.3. HOW TO PLAN YOUR ENVIRONMENT ACCORDING TO TESTED CLUSTER MAXIMUMS	72
10.4. HOW TO PLAN YOUR ENVIRONMENT ACCORDING TO APPLICATION REQUIREMENTS	72
CHAPTER 11. OPTIMIZING STORAGE	76
11.1. AVAILABLE PERSISTENT STORAGE OPTIONS	76
11.2. RECOMMENDED CONFIGURABLE STORAGE TECHNOLOGY	77
11.2.1. Specific application storage recommendations	77
11.2.1.1. Registry	78
11.2.1.2. Scaled registry	78
11.2.1.3. Metrics	78
11.2.1.4. Logging	79
11.2.1.5. Applications	79
11.2.2. Other specific application storage recommendations	79
11.3. DATA STORAGE MANAGEMENT	79
CHAPTER 12. OPTIMIZING ROUTING	81
12.1. BASELINE INGRESS CONTROLLER (ROUTER) PERFORMANCE	81
12.2. INGRESS CONTROLLER (ROUTER) PERFORMANCE OPTIMIZATIONS	82
CHAPTER 13. OPTIMIZING NETWORKING	83
13.1. OPTIMIZING THE MTU FOR YOUR NETWORK	83
13.2. RECOMMENDED PRACTICES FOR INSTALLING LARGE SCALE CLUSTERS	84
13.3. IMPACT OF IPSEC	84

CHAPTER 14. MANAGING BARE METAL HOSTS	85
14.1. ABOUT BARE METAL HOSTS AND NODES	85
14.2. MAINTAINING BARE METAL HOSTS	85
14.2.1. Adding a bare metal host to the cluster using the web console	85
14.2.2. Adding a bare metal host to the cluster using YAML in the web console	86
14.2.3. Automatically scaling machines to the number of available bare metal hosts	87
CHAPTER 15. WHAT HUGE PAGES DO AND HOW THEY ARE CONSUMED BY APPLICATIONS	89
15.1. WHAT HUGE PAGES DO	89
15.2. HOW HUGE PAGES ARE CONSUMED BY APPS	89
15.3. CONSUMING HUGE PAGES RESOURCES USING THE DOWNWARD API	90
15.4. CONFIGURING HUGE PAGES	92
15.4.1. At boot time	92
CHAPTER 16. PERFORMANCE ADDON OPERATOR FOR LOW LATENCY NODES	95
16.1. UNDERSTANDING LOW LATENCY	95
16.1.1. About hyperthreading for low latency and real-time applications	95
16.2. INSTALLING THE PERFORMANCE ADDON OPERATOR	96
16.2.1. Installing the Operator using the CLI	96
16.2.2. Installing the Performance Addon Operator using the web console	97
16.3. UPGRADING PERFORMANCE ADDON OPERATOR	98
16.3.1. About upgrading Performance Addon Operator	98
16.3.1.1. How Performance Addon Operator upgrades affect your cluster	99
16.3.1.2. Upgrading Performance Addon Operator to the next minor version	99
16.3.1.3. Upgrading Performance Addon Operator when previously installed to a specific namespace	99
16.3.2. Monitoring upgrade status	100
16.4. PROVISIONING REAL-TIME AND LOW LATENCY WORKLOADS	101
16.4.1. Known limitations for real-time	101
16.4.2. Provisioning a worker with real-time capabilities	102
16.4.3. Verifying the real-time kernel installation	103
16.4.4. Creating a workload that works in real-time	103
16.4.5. Creating a pod with a QoS class of Guaranteed	104
16.4.6. Optional: Disabling CPU load balancing for DPDK	105
16.4.7. Assigning a proper node selector	105
16.4.8. Scheduling a workload onto a worker with real-time capabilities	106
16.4.9. Managing device interrupt processing for guaranteed pod isolated CPUs	106
16.4.9.1. Disabling global device interrupts handling in Performance Addon Operator	106
16.4.9.2. Disabling interrupt processing for individual pods	107
16.4.10. Upgrading the performance profile to use device interrupt processing	107
16.4.10.1. Supported API Versions	107
16.4.10.1.1. Upgrading Performance Addon Operator API from v1alpha1 to v1	107
16.4.10.1.2. Upgrading Performance Addon Operator API from v1alpha1 or v1 to v2	107
16.4.11. Configuring a node for IRQ dynamic load balancing	107
16.4.12. Configuring hyperthreading for a cluster	110
16.4.12.1. Disabling hyperthreading for low latency applications	112
16.5. TUNING NODES FOR LOW LATENCY WITH THE PERFORMANCE PROFILE	113
16.5.1. Configuring huge pages	114
16.5.2. Allocating multiple huge page sizes	115
16.5.3. Restricting CPUs for infra and application containers	115
16.6. REDUCING NIC QUEUES USING THE PERFORMANCE ADDON OPERATOR	117
16.6.1. Adjusting the NIC queues with the performance profile	117
16.6.2. Verifying the queue status	121
16.6.3. Logging associated with adjusting NIC queues	124

16.7. PERFORMING END-TO-END TESTS FOR PLATFORM VERIFICATION	124
16.7.1. Prerequisites	125
16.7.2. Dry run	126
16.7.3. Disconnected mode	126
16.7.3.1. Mirroring the images to a custom registry accessible from the cluster	126
16.7.3.2. Instruct the tests to consume those images from a custom registry	126
16.7.3.3. Mirroring to the cluster internal registry	127
16.7.3.4. Mirroring a different set of images	128
16.7.4. Running in a single node cluster	129
Required parameters	129
16.7.5. Impact of tests on the cluster	129
16.7.5.1. SCTP	129
16.7.5.2. XT_U32	129
16.7.5.3. SR-IOV	130
16.7.5.4. PTP	130
16.7.5.5. Performance	130
16.7.5.6. DPDK	130
16.7.5.7. Container-mount-namespace	130
16.7.5.8. Cleaning up	130
16.7.6. Override test image parameters	130
16.7.6.1. Ginkgo parameters	130
16.7.6.2. Available features	131
16.7.7. Discovery mode	131
16.7.7.1. Required environment configuration prerequisites	132
16.7.7.2. Limiting the nodes used during tests	133
16.7.7.3. Using a single performance profile	133
16.7.7.4. Disabling the performance profile cleanup	134
16.7.8. Running the latency tests	134
16.7.8.1. Running hwlatdetect	135
16.7.8.2. Running cyclicttest	137
16.7.8.3. Running oslat	139
16.7.9. Troubleshooting	141
16.7.10. Test reports	142
16.7.10.1. JUnit test output	142
16.7.10.2. Test failure report	142
16.7.10.3. A note on podman	142
16.7.10.4. Running on OpenShift Container Platform 4.4	142
16.7.10.5. Using a single performance profile	142
16.8. DEBUGGING LOW LATENCY CNF TUNING STATUS	143
16.8.1. Machine config pools	144
16.9. COLLECTING LOW LATENCY TUNING DEBUGGING DATA FOR RED HAT SUPPORT	146
16.9.1. About the must-gather tool	146
16.9.2. About collecting low latency tuning data	146
16.9.3. Gathering data about specific features	146
CHAPTER 17. CREATING A PERFORMANCE PROFILE	148
17.1. ABOUT THE PERFORMANCE PROFILE CREATOR	148
17.1.1. Gathering data about your cluster using must-gather	148
17.1.2. Running the Performance Profile Creator using podman	149
17.1.2.1. How to run podman to create a performance profile	152
17.1.3. Running the Performance Profile Creator wrapper script	152
17.1.4. Performance Profile Creator arguments	157
17.2. ADDITIONAL RESOURCES	159

CHAPTER 18. DEPLOYING DISTRIBUTED UNITS AT SCALE IN A DISCONNECTED ENVIRONMENT	160
18.1. PROVISIONING EDGE SITES AT SCALE	160
18.2. THE GITOPS APPROACH	161
18.3. ABOUT ZTP AND DISTRIBUTED UNITS ON SINGLE NODES	161
18.4. ZERO TOUCH PROVISIONING BUILDING BLOCKS	162
18.5. SINGLE NODE CLUSTERS	163
18.6. SITE PLANNING CONSIDERATIONS FOR DISTRIBUTED UNIT DEPLOYMENTS	163
18.7. LOW LATENCY FOR DISTRIBUTED UNITS (DUS)	164
18.8. CONFIGURING BIOS FOR DISTRIBUTED UNIT BARE-METAL HOSTS	165
18.9. PREPARING THE DISCONNECTED ENVIRONMENT	166
18.9.1. Disconnected environment prerequisites	166
18.9.2. About the mirror registry	167
18.9.3. Preparing your mirror host	167
18.9.3.1. Installing the OpenShift CLI by downloading the binary	167
Installing the OpenShift CLI on Linux	168
Installing the OpenShift CLI on Windows	168
Installing the OpenShift CLI on macOS	169
18.9.3.2. Configuring credentials that allow images to be mirrored	169
18.9.3.3. Mirroring the OpenShift Container Platform image repository	171
18.9.3.4. Adding RHCOS ISO and RootFS images to a disconnected mirror host	174
18.10. INSTALLING RED HAT ADVANCED CLUSTER MANAGEMENT IN A DISCONNECTED ENVIRONMENT	175
18.11. ENABLING ASSISTED INSTALLER SERVICE ON BARE METAL	176
18.12. ZTP CUSTOM RESOURCES	177
18.13. CREATING CUSTOM RESOURCES TO INSTALL A SINGLE MANAGED CLUSTER	179
18.13.1. Configuring static IP addresses for managed clusters	184
18.13.2. Automated Discovery image ISO process for provisioning clusters	186
18.13.3. Checking the managed cluster status	186
18.13.4. Configuring a managed cluster for a disconnected environment	187
18.13.5. Configuring IPv6 addresses for a disconnected environment	189
18.13.6. Troubleshooting the managed cluster	190
18.14. APPLYING THE RAN POLICIES FOR MONITORING CLUSTER ACTIVITY	191
18.14.1. Applying source custom resource policies	192
18.14.2. The PolicyGenTemplate	195
18.14.3. Considerations when creating custom resource policies	196
18.14.4. Generating RAN policies	197
18.15. CLUSTER PROVISIONING	198
18.15.1. Machine Config Operator	199
18.15.2. Performance Addon Operator	199
18.15.3. SR-IOV Operator	200
18.15.4. Precision Time Protocol Operator	200
18.16. CREATING ZTP CUSTOM RESOURCES FOR MULTIPLE MANAGED CLUSTERS	200
18.16.1. Prerequisites for deploying the ZTP pipeline	201
18.16.2. Installing the GitOps ZTP pipeline	202
18.16.2.1. Preparing the ZTP Git repository	202
18.16.2.2. Preparing the hub cluster for ZTP	202
18.16.3. Creating the site secrets	204
18.16.4. Creating the SiteConfig custom resources	205
18.16.5. Creating the PolicyGenTemplates	207
18.16.6. Checking the installation status	208
18.16.7. Site cleanup	208
18.16.7.1. Removing the ArgoCD pipeline	208
18.17. TROUBLESHOOTING GITOPS ZTP	209

18.17.1. Validating the generation of installation CRs	209
18.17.2. Validating the generation of policy CRs	210

CHAPTER 1. RECOMMENDED PRACTICES FOR INSTALLING LARGE CLUSTERS

Apply the following practices when installing large clusters or scaling clusters to larger node counts.

1.1. RECOMMENDED PRACTICES FOR INSTALLING LARGE SCALE CLUSTERS

When installing large clusters or scaling the cluster to larger node counts, set the cluster network **cidr** accordingly in your **install-config.yaml** file before you install the cluster:

```
networking:
  clusterNetwork:
    - cidr: 10.128.0.0/14
      hostPrefix: 23
  machineNetwork:
    - cidr: 10.0.0.0/16
  networkType: OpenShiftSDN
  serviceNetwork:
    - 172.30.0.0/16
```

The default cluster network **cidr 10.128.0.0/14** cannot be used if the cluster size is more than 500 nodes. It must be set to **10.128.0.0/12** or **10.128.0.0/10** to get to larger node counts beyond 500 nodes.

CHAPTER 2. RECOMMENDED HOST PRACTICES

This topic provides recommended host practices for OpenShift Container Platform.



IMPORTANT

These guidelines apply to OpenShift Container Platform with software-defined networking (SDN), not Open Virtual Network (OVN).

2.1. RECOMMENDED NODE HOST PRACTICES

The OpenShift Container Platform node configuration file contains important options. For example, two parameters control the maximum number of pods that can be scheduled to a node: **podsPerCore** and **maxPods**.

When both options are in use, the lower of the two values limits the number of pods on a node. Exceeding these values can result in:

- Increased CPU utilization.
- Slow pod scheduling.
- Potential out-of-memory scenarios, depending on the amount of memory in the node.
- Exhausting the pool of IP addresses.
- Resource overcommitting, leading to poor user application performance.



IMPORTANT

In Kubernetes, a pod that is holding a single container actually uses two containers. The second container is used to set up networking prior to the actual container starting. Therefore, a system running 10 pods will actually have 20 containers running.



NOTE

Disk IOPS throttling from the cloud provider might have an impact on CRI-O and kubelet. They might get overloaded when there are large number of I/O intensive pods running on the nodes. It is recommended that you monitor the disk I/O on the nodes and use volumes with sufficient throughput for the workload.

podsPerCore sets 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 will be **40**.

```
kubeletConfig:
  podsPerCore: 10
```

Setting **podsPerCore** to **0** disables this limit. The default is **0**. **podsPerCore** cannot exceed **maxPods**.

maxPods sets the number of pods the node can run to a fixed value, regardless of the properties of the node.

kubeletConfig:
maxPods: 250

2.2. CREATING A KUBELETCONFIG CRD TO EDIT KUBELET PARAMETERS

The kubelet configuration is currently serialized as an Ignition configuration, so it can be directly edited. However, there is also a new **kubelet-config-controller** added to the Machine Config Controller (MCC). This lets you use a **KubeletConfig** custom resource (CR) to edit the kubelet parameters.



NOTE

As the fields in the **kubeletConfig** object are passed directly to the kubelet from upstream Kubernetes, the kubelet validates those values directly. Invalid values in the **kubeletConfig** object might cause cluster nodes to become unavailable. For valid values, see the [Kubernetes documentation](#).

Consider the following guidance:

- Create one **KubeletConfig** CR for each machine config pool with all the config changes you want for that pool. If you are applying the same content to all of the pools, you need only one **KubeletConfig** CR for all of the pools.
- Edit an existing **KubeletConfig** CR to modify existing settings or add new settings, instead of creating a CR for each change. It is recommended that you create a CR only to modify a different machine config pool, or for changes that are intended to be temporary, so that you can revert the changes.
- As needed, create multiple **KubeletConfig** CRs with a limit of 10 per cluster. For the first **KubeletConfig** CR, the Machine Config Operator (MCO) creates a machine config appended with **kubelet**. With each subsequent CR, the controller creates another **kubelet** machine config with a numeric suffix. For example, if you have a **kubelet** machine config with a **-2** suffix, the next **kubelet** machine config is appended with **-3**.

If you want to delete the machine configs, delete them in reverse order to avoid exceeding the limit. For example, you delete the **kubelet-3** machine config before deleting the **kubelet-2** machine config.



NOTE

If you have a machine config with a **kubelet-9** suffix, and you create another **KubeletConfig** CR, a new machine config is not created, even if there are fewer than 10 **kubelet** machine configs.

Example KubeletConfig CR

```
$ oc get kubeletconfig
```

NAME	AGE
set-max-pods	15m

Example showing a KubeletConfig machine config



```
$ oc get mc | grep kubelet
```

```
...
99-worker-generated-kubelet-1      b5c5119de007945b6fe6fb215db3b8e2ceb12511  3.2.0
26m
...
```

The following procedure is an example to show how to configure the maximum number of pods per node on the worker nodes.

Prerequisites

1. Obtain the label associated with the static **MachineConfigPool** CR 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: set-max-pods 1
```

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=set-max-pods
```

Procedure

1. View the available machine configuration objects that you can select:

```
$ oc get machineconfig
```

By default, the two kubelet-related configs are **01-master-kubelet** and **01-worker-kubelet**.

2. Check the current value for the maximum pods per node:

```
$ oc describe node <node_name>
```

For example:

```
$ oc describe node ci-ln-5grqprb-f76d1-ncnqq-worker-a-mdv94
```

Look for **value: pods: <value>** in the **Allocatable** stanza:

Example output

```
Allocatable:
attachable-volumes-aws-ebs: 25
cpu:                        3500m
hugepages-1Gi:             0
hugepages-2Mi:             0
memory:                    15341844Ki
pods:                      250
```

- Set the maximum pods per node on the worker nodes by creating a custom resource file that contains the kubelet configuration:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: set-max-pods
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: set-max-pods ❶
  kubeletConfig:
    maxPods: 500 ❷
```

- ❶ Enter the label from the machine config pool.
- ❷ Add the kubelet configuration. In this example, use **maxPods** to set the maximum pods per node.



NOTE

The rate at which the kubelet talks to the API server depends on queries per second (QPS) and burst values. The default values, **50** for **kubeAPIQPS** and **100** for **kubeAPIBurst**, are sufficient if there are limited pods running on each node. It is recommended to update the kubelet QPS and burst rates if there are enough CPU and memory resources on the node.

```
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: set-max-pods
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: set-max-pods
  kubeletConfig:
    maxPods: <pod_count>
    kubeAPIBurst: <burst_rate>
    kubeAPIQPS: <QPS>
```


- a. Update the machine config pool for workers with the label:

```
$ oc label machineconfigpool worker custom-kubelet=large-pods
```

- b. Create the **KubeletConfig** object:

```
$ oc create -f change-maxPods-cr.yaml
```

- c. Verify that the **KubeletConfig** object is created:

```
$ oc get kubeletconfig
```

Example output

```
NAME          AGE
set-max-pods  15m
```

Depending on the number of worker nodes in the cluster, wait for the worker nodes to be rebooted one by one. For a cluster with 3 worker nodes, this could take about 10 to 15 minutes.

4. Verify that the changes are applied to the node:

- a. Check on a worker node that the **maxPods** value changed:

```
$ oc describe node <node_name>
```

- b. Locate the **Allocatable** stanza:

```
...
Allocatable:
attachable-volumes-gce-pd: 127
cpu:                        3500m
ephemeral-storage:         123201474766
hugepages-1Gi:             0
hugepages-2Mi:             0
memory:                    14225400Ki
pods:                      500 1
...
```

1 In this example, the **pods** parameter should report the value you set in the **KubeletConfig** object.

5. Verify the change in the **KubeletConfig** object:

```
$ oc get kubeletconfigs set-max-pods -o yaml
```

This should show a status of **True** and **type:Success**, as shown in the following example:

```
spec:
  kubeletConfig:
    maxPods: 500
```

```

machineConfigPoolSelector:
  matchLabels:
    custom-kubelet: set-max-pods
status:
  conditions:
  - lastTransitionTime: "2021-06-30T17:04:07Z"
    message: Success
    status: "True"
    type: Success

```

2.3. MODIFYING THE NUMBER OF UNAVAILABLE WORKER NODES

By default, only one machine is allowed to be unavailable when applying the kubelet-related configuration to the available worker nodes. For a large cluster, it can take a long time for the configuration change to be reflected. At any time, you can adjust the number of machines that are updating to speed up the process.

Procedure

1. Edit the **worker** machine config pool:

```
$ oc edit machineconfigpool worker
```

2. Set **maxUnavailable** to the value that you want:

```

spec:
  maxUnavailable: <node_count>

```



IMPORTANT

When setting the value, consider the number of worker nodes that can be unavailable without affecting the applications running on the cluster.

2.4. CONTROL PLANE NODE SIZING

The control plane node resource requirements depend on the number of nodes in the cluster. The following control plane node size recommendations are based on the results of control plane density focused testing. The control plane tests create the following objects across the cluster in each of the namespaces depending on the node counts:

- 12 image streams
- 3 build configurations
- 6 builds
- 1 deployment with 2 pod replicas mounting two secrets each
- 2 deployments with 1 pod replica mounting two secrets
- 3 services pointing to the previous deployments
- 3 routes pointing to the previous deployments

- 10 secrets, 2 of which are mounted by the previous deployments
- 10 config maps, 2 of which are mounted by the previous deployments

Number of worker nodes	Cluster load (namespaces)	CPU cores	Memory (GB)
25	500	4	16
100	1000	8	32
250	4000	16	96

On a large and dense cluster with three masters or control plane nodes, the CPU and memory usage will spike up when one of the nodes is stopped, rebooted or fails. The failures can be due to unexpected issues with power, network or underlying infrastructure in addition to intentional cases where the cluster is restarted after shutting it down to save costs. The remaining two control plane nodes must handle the load in order to be highly available which leads to increase in the resource usage. This is also expected during upgrades because the masters are cordoned, drained, and rebooted serially to apply the operating system updates, as well as the control plane Operators update. To avoid cascading failures, keep the overall CPU and memory resource usage on the control plane nodes to at most half of all available capacity to handle the resource usage spikes. Increase the CPU and memory on the control plane nodes accordingly to avoid potential downtime due to lack of resources.



IMPORTANT

The node sizing varies depending on the number of nodes and object counts in the cluster. It also depends on whether the objects are actively being created on the cluster. During object creation, the control plane is more active in terms of resource usage compared to when the objects are in the **running** phase.

Operator Lifecycle Manager (OLM) runs on the control plane nodes and it's memory footprint depends on the number of namespaces and user installed operators that OLM needs to manage on the cluster. Control plane nodes need to be sized accordingly to avoid OOM kills. Following data points are based on the results from cluster maximums testing.

Number of namespaces	OLM memory at idle state (GB)	OLM memory with 5 user operators installed (GB)
500	0.823	1.7
1000	1.2	2.5
1500	1.7	3.2
2000	2	4.4
3000	2.7	5.6

Number of namespaces	OLM memory at idle state (GB)	OLM memory with 5 user operators installed (GB)
4000	3.8	7.6
5000	4.2	9.02
6000	5.8	11.3
7000	6.6	12.9
8000	6.9	14.8
9000	8	17.7
10,000	9.9	21.6

**IMPORTANT**

If you used an installer-provisioned infrastructure installation method, you cannot modify the control plane node size in a running OpenShift Container Platform 4.9 cluster. Instead, you must estimate your total node count and use the suggested control plane node size during installation.

**IMPORTANT**

The recommendations are based on the data points captured on OpenShift Container Platform clusters with OpenShift SDN as the network plug-in.

**NOTE**

In OpenShift Container Platform 4.9, half of a CPU core (500 millicore) is now reserved by the system by default compared to OpenShift Container Platform 3.11 and previous versions. The sizes are determined taking that into consideration.

2.4.1. Increasing the flavor size of the Amazon Web Services (AWS) master instances

When you have overloaded AWS master nodes in a cluster and the master nodes require more resources, you can increase the flavor size of the master instances.

**NOTE**

It is recommended to backup etcd before increasing the flavor size of the AWS master instances.

Prerequisites

- You have an IPI (installer-provisioned infrastructure) or UPI (user-provisioned infrastructure) cluster on AWS.

Procedure

1. Open the AWS console, fetch the master instances.
2. Stop one master instance.
3. Select the stopped instance, and click **Actions** → **Instance Settings** → **Change instance type**
4. Change the instance to a larger type, ensuring that the type is the same base as the previous selection, and apply changes. For example, you can change **m5.xlarge** to **m5.2xlarge** or **m5.4xlarge**.
5. Backup the instance, and repeat the steps for the next master instance.

Additional resources

- [Backing up etcd](#)

2.5. RECOMMENDED ETCD PRACTICES

For large and dense clusters, etcd can suffer from poor performance if the keyspace grows excessively large and exceeds the space quota. Periodic maintenance of etcd, including defragmentation, must be performed to free up space in the data store. It is highly recommended that you monitor Prometheus for etcd metrics and defragment it when required before etcd raises a cluster-wide alarm that puts the cluster into a maintenance mode, which only accepts key reads and deletes. Some of the key metrics to monitor are **etcd_server_quota_backend_bytes** which is the current quota limit, **etcd_mvcc_db_total_size_in_use_in_bytes** which indicates the actual database usage after a history compaction, and **etcd_debugging_mvcc_db_total_size_in_bytes** which shows the database size including free space waiting for defragmentation. Instructions on defragging etcd can be found in the **Defragmenting etcd data** section.

Etcd writes data to disk, so its performance strongly depends on disk performance. Etcd persists proposals on disk. Slow disks and disk activity from other processes might cause long fsync latencies, causing etcd to miss heartbeats, inability to commit new proposals to the disk on time, which can cause request timeouts and temporary leader loss. It is highly recommended to run etcd on machines backed by SSD/NVMe disks with low latency and high throughput.

Some of the key metrics to monitor on a deployed OpenShift Container Platform cluster are p99 of etcd disk write ahead log duration and the number of etcd leader changes. Use Prometheus to track these metrics. **etcd_disk_wal_fsync_duration_seconds_bucket** reports the etcd disk fsync duration, **etcd_server_leader_changes_seen_total** reports the leader changes. To rule out a slow disk and confirm that the disk is reasonably fast, 99th percentile of the **etcd_disk_wal_fsync_duration_seconds_bucket** should be less than 10ms.

Fio, a I/O benchmarking tool can be used to validate the hardware for etcd before or after creating the OpenShift Container Platform cluster. Run fio and analyze the results:

Assuming container runtimes like podman or docker are installed on the machine under test and the path etcd writes the data exists - /var/lib/etcd, run:

Procedure

Run the following if using podman:

```
$ sudo podman run --volume /var/lib/etcd:/var/lib/etcd:Z quay.io/openshift-scale/etcd-perf
```

Alternatively, run the following if using docker:

```
$ sudo docker run --volume /var/lib/etcd:/var/lib/etcd:Z quay.io/openshift-scale/etcd-perf
```

The output reports whether the disk is fast enough to host etcd by comparing the 99th percentile of the fsync metric captured from the run to see if it is less than 10ms.

Etcd replicates the requests among all the members, so its performance strongly depends on network input/output (IO) latency. High network latencies result in etcd heartbeats taking longer than the election timeout, which leads to leader elections that are disruptive to the cluster. A key metric to monitor on a deployed OpenShift Container Platform cluster is the 99th percentile of etcd network peer latency on each etcd cluster member. Use Prometheus to track the metric. **histogram_quantile(0.99, rate(etcd_network_peer_round_trip_time_seconds_bucket[2m]))** reports the round trip time for etcd to finish replicating the client requests between the members; it should be less than 50 ms.

2.6. DEFRAAGMENTING ETCD DATA

Defragment etcd data to reclaim disk space after events that cause disk fragmentation, such as etcd history compaction.

History compaction is performed automatically every five minutes and leaves gaps in the back-end database. This fragmented space is available for use by etcd, but is not available to the host file system. You must defragment etcd to make this space available to the host file system.

Defragmentation occurs automatically, but you can also trigger it manually.



NOTE

Automatic defragmentation is good for most cases, because the etcd operator uses cluster information to determine the most efficient operation for the user.

2.6.1. Automatic defragmentation

The etcd Operator automatically defragments disks. No manual intervention is needed.

Verify that the defragmentation process is successful by viewing one of these logs:

- etcd logs
- cluster-etcd-operator pod
- operator status error log

Example log output

```
I0907 08:43:12.171919    1
defragcontroller.go:198] etcd member "ip-
10-0-191-150.us-west-2.compute.internal"
backend store fragmented: 39.33 %, dbSize:
349138944
```

2.6.2. Manual defragmentation

You can monitor the **etcd_db_total_size_in_bytes** metric to determine whether manual defragmentation is necessary.



WARNING

Defragmenting etcd is a blocking action. The etcd member will not response until defragmentation is complete. For this reason, wait at least one minute between defragmentation actions on each of the pods to allow the cluster to recover.

Follow this procedure to defragment etcd data on each etcd member.

Prerequisites

- You have access to the cluster as a user with the **cluster-admin** role.

Procedure

- Determine which etcd member is the leader, because the leader should be defragmented last.
 - Get the list of etcd pods:

```
$ oc get pods -n openshift-etcd -o wide | grep -v quorum-guard | grep etcd
```

Example output

```
etcd-ip-10-0-159-225.example.redhat.com      3/3   Running   0       175m
10.0.159.225 ip-10-0-159-225.example.redhat.com <none>   <none>
etcd-ip-10-0-191-37.example.redhat.com      3/3   Running   0       173m
10.0.191.37 ip-10-0-191-37.example.redhat.com <none>   <none>
etcd-ip-10-0-199-170.example.redhat.com     3/3   Running   0       176m
10.0.199.170 ip-10-0-199-170.example.redhat.com <none>   <none>
```

- Choose a pod and run the following command to determine which etcd member is the leader:

```
$ oc rsh -n openshift-etcd etcd-ip-10-0-159-225.us-west-1.compute.internal etcdctl
endpoint status --cluster -w table
```

Example output

```
Defaulting container name to etcdctl.
Use 'oc describe pod/etcd-ip-10-0-159-225.example.redhat.com -n openshift-etcd' to see
all of the containers in this pod.
```

```
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
|   ENDPOINT   |   ID   | VERSION | DB SIZE | IS LEADER | IS LEARNER |
| RAFT TERM | RAFT INDEX | RAFT APPLIED INDEX | ERRORS |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
```

```
| https://10.0.191.37:2379 | 251cd44483d811c3 | 3.4.9 | 104 MB | false | false |
7 | 91624 | 91624 |
| https://10.0.159.225:2379 | 264c7c58ecbdabee | 3.4.9 | 104 MB | false | false |
7 | 91624 | 91624 |
| https://10.0.199.170:2379 | 9ac311f93915cc79 | 3.4.9 | 104 MB | true | false |
7 | 91624 | 91624 |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
```

Based on the **IS LEADER** column of this output, the **https://10.0.199.170:2379** endpoint is the leader. Matching this endpoint with the output of the previous step, the pod name of the leader is **etcd-ip-10-0-199-170.example.redhat.com**.

2. Defragment an etcd member.

- a. Connect to the running etcd container, passing in the name of a pod that is *not* the leader:

```
$ oc rsh -n openshift-etcd etcd-ip-10-0-159-225.example.redhat.com
```

- b. Unset the **ETCDCTL_ENDPOINTS** environment variable:

```
sh-4.4# unset ETCDCTL_ENDPOINTS
```

- c. Defragment the etcd member:

```
sh-4.4# etcdctl --command-timeout=30s --endpoints=https://localhost:2379 defrag
```

Example output

```
Finished defragmenting etcd member[https://localhost:2379]
```

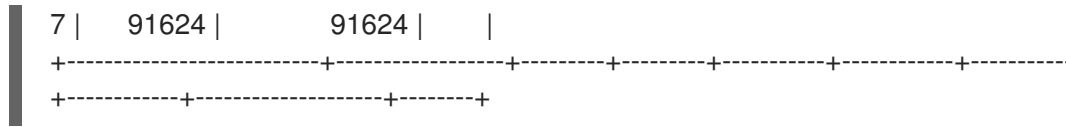
If a timeout error occurs, increase the value for **--command-timeout** until the command succeeds.

- d. Verify that the database size was reduced:

```
sh-4.4# etcdctl endpoint status -w table --cluster
```

Example output

```
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
|   ENDPOINT   |   ID   | VERSION | DB SIZE | IS LEADER | IS LEARNER |
| RAFT TERM | RAFT INDEX | RAFT APPLIED INDEX | ERRORS |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
| https://10.0.191.37:2379 | 251cd44483d811c3 | 3.4.9 | 104 MB | false | false |
7 | 91624 | 91624 |
| https://10.0.159.225:2379 | 264c7c58ecbdabee | 3.4.9 | 41 MB | false | false |
7 | 91624 | 91624 |
| https://10.0.199.170:2379 | 9ac311f93915cc79 | 3.4.9 | 104 MB | true | false |
```

This example shows that the database size for this etcd member is now 41 MB as opposed to the starting size of 104 MB.

- e. Repeat these steps to connect to each of the other etcd members and defragment them. Always defragment the leader last.
Wait at least one minute between defragmentation actions to allow the etcd pod to recover. Until the etcd pod recovers, the etcd member will not respond.
3. If any **NOSPACE** alarms were triggered due to the space quota being exceeded, clear them.
 - a. Check if there are any **NOSPACE** alarms:

```
sh-4.4# etcdctl alarm list
```

Example output

```
memberID:12345678912345678912 alarm:NOSPACE
```

- b. Clear the alarms:

```
sh-4.4# etcdctl alarm disarm
```

2.7. OPENSIFT CONTAINER PLATFORM INFRASTRUCTURE COMPONENTS

The following infrastructure workloads do not incur OpenShift Container Platform worker subscriptions:

- Kubernetes and OpenShift Container Platform control plane services that run on masters
- The default router
- The integrated container image registry
- The HAProxy-based Ingress Controller
- The cluster metrics collection, or monitoring service, including components for monitoring user-defined projects
- Cluster aggregated logging
- Service brokers
- Red Hat Quay
- Red Hat OpenShift Container Storage
- Red Hat Advanced Cluster Manager
- Red Hat Advanced Cluster Security for Kubernetes
- Red Hat OpenShift GitOps

- Red Hat OpenShift Pipelines

Any node that runs any other container, pod, or component is a worker node that your subscription must cover.

For information on infrastructure nodes and which components can run on infrastructure nodes, see the "Red Hat OpenShift control plane and infrastructure nodes" section in the [OpenShift sizing and subscription guide for enterprise Kubernetes](#) document.

2.8. MOVING THE MONITORING SOLUTION

By default, the Prometheus Cluster Monitoring stack, which contains Prometheus, Grafana, and AlertManager, is deployed to provide cluster monitoring. It is managed by the Cluster Monitoring Operator. To move its components to different machines, you create and apply a custom config map.

Procedure

1. Save the following **ConfigMap** definition as the **cluster-monitoring-configmap.yaml** file:

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml: |+
    alertmanagerMain:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
    prometheusK8s:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
    prometheusOperator:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
    grafana:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
    k8sPrometheusAdapter:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
    kubeStateMetrics:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
    telemeterClient:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
    openshiftStateMetrics:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
    thanosQuerier:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
```

Running this config map forces the components of the monitoring stack to redeploy to infrastructure nodes.

2. Apply the new config map:

```
$ oc create -f cluster-monitoring-configmap.yaml
```

3. Watch the monitoring pods move to the new machines:

```
$ watch 'oc get pod -n openshift-monitoring -o wide'
```

4. If a component has not moved to the **infra** node, delete the pod with this component:

```
$ oc delete pod -n openshift-monitoring <pod>
```

The component from the deleted pod is re-created on the **infra** node.

2.9. MOVING THE DEFAULT REGISTRY

You configure the registry Operator to deploy its pods to different nodes.

Prerequisites

- Configure additional machine sets in your OpenShift Container Platform cluster.

Procedure

1. View the **config/instance** object:

```
$ oc get configs.imageregistry.operator.openshift.io/cluster -o yaml
```

Example output

```
apiVersion: imageregistry.operator.openshift.io/v1
kind: Config
metadata:
  creationTimestamp: 2019-02-05T13:52:05Z
  finalizers:
  - imageregistry.operator.openshift.io/finalizer
  generation: 1
  name: cluster
  resourceVersion: "56174"
  selfLink: /apis/imageregistry.operator.openshift.io/v1/configs/cluster
  uid: 36fd3724-294d-11e9-a524-12fdee2931b
spec:
  httpSecret: d9a012ccd117b1e6616ceccb2c3bb66a5fed1b5e481623
  logging: 2
  managementState: Managed
  proxy: {}
  replicas: 1
  requests:
    read: {}
    write: {}
```

```

storage:
  s3:
    bucket: image-registry-us-east-1-c92e88cad85b48ec8b312344dff03c82-392c
    region: us-east-1
status:
...

```

2. Edit the **config/instance** object:

```
$ oc edit configs.imageregistry.operator.openshift.io/cluster
```

3. Modify the **spec** section of the object to resemble the following YAML:

```

spec:
  affinity:
    podAntiAffinity:
      preferredDuringSchedulingIgnoredDuringExecution:
        - podAffinityTerm:
            namespaces:
              - openshift-image-registry
            topologyKey: kubernetes.io/hostname
            weight: 100
  logLevel: Normal
  managementState: Managed
  nodeSelector:
    node-role.kubernetes.io/infra: ""

```

4. Verify the registry pod has been moved to the infrastructure node.
 - a. Run the following command to identify the node where the registry pod is located:

```
$ oc get pods -o wide -n openshift-image-registry
```

- b. Confirm the node has the label you specified:

```
$ oc describe node <node_name>
```

Review the command output and confirm that **node-role.kubernetes.io/infra** is in the **LABELS** list.

2.10. MOVING THE ROUTER

You can deploy the router pod to a different machine set. By default, the pod is deployed to a worker node.

Prerequisites

- Configure additional machine sets in your OpenShift Container Platform cluster.

Procedure

1. View the **IngressController** custom resource for the router Operator:

```
$ oc get ingresscontroller default -n openshift-ingress-operator -o yaml
```

The command output resembles the following text:

```
apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  creationTimestamp: 2019-04-18T12:35:39Z
  finalizers:
    - ingresscontroller.operator.openshift.io/finalizer-ingresscontroller
  generation: 1
  name: default
  namespace: openshift-ingress-operator
  resourceVersion: "11341"
  selfLink: /apis/operator.openshift.io/v1/namespaces/openshift-ingress-
operator/ingresscontrollers/default
  uid: 79509e05-61d6-11e9-bc55-02ce4781844a
spec: {}
status:
  availableReplicas: 2
  conditions:
    - lastTransitionTime: 2019-04-18T12:36:15Z
      status: "True"
      type: Available
  domain: apps.<cluster>.example.com
  endpointPublishingStrategy:
    type: LoadBalancerService
  selector: ingresscontroller.operator.openshift.io/deployment-ingresscontroller=default
```

2. Edit the **ingresscontroller** resource and change the **nodeSelector** to use the **infra** label:

```
$ oc edit ingresscontroller default -n openshift-ingress-operator
```

Add the **nodeSelector** stanza that references the **infra** label to the **spec** section, as shown:

```
spec:
  nodePlacement:
    nodeSelector:
      matchLabels:
        node-role.kubernetes.io/infra: ""
```

3. Confirm that the router pod is running on the **infra** node.
 - a. View the list of router pods and note the node name of the running pod:

```
$ oc get pod -n openshift-ingress -o wide
```

Example output

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE
NOMINATED NODE	READINESS	GATES				
router-default-86798b4b5d-bdlvd	1/1	Running	0	28s	10.130.2.4	ip-10-

```
0-217-226.ec2.internal <none> <none>
router-default-955d875f4-255g8 0/1 Terminating 0 19h 10.129.2.4 ip-10-
0-148-172.ec2.internal <none> <none>
```

In this example, the running pod is on the **ip-10-0-217-226.ec2.internal** node.

- b. View the node status of the running pod:

```
$ oc get node <node_name> 1
```

1 **1** Specify the **<node_name>** that you obtained from the pod list.

Example output

```
NAME                                STATUS ROLES    AGE  VERSION
ip-10-0-217-226.ec2.internal Ready  infra,worker  17h  v1.22.1
```

Because the role list includes **infra**, the pod is running on the correct node.

2.11. INFRASTRUCTURE NODE SIZING

Infrastructure nodes are nodes that are labeled to run pieces of the OpenShift Container Platform environment. The infrastructure node resource requirements depend on the cluster age, nodes, and objects in the cluster, as these factors can lead to an increase in the number of metrics or time series in Prometheus. The following infrastructure node size recommendations are based on the results of cluster maximums and control plane density focused testing.

Number of worker nodes	CPU cores	Memory (GB)
25	4	16
100	8	32
250	16	128
500	32	128

In general, three infrastructure nodes are recommended per cluster.



IMPORTANT

These sizing recommendations are based on scale tests, which create a large number of objects across the cluster. These tests include reaching some of the cluster maximums. In the case of 250 and 500 node counts on an OpenShift Container Platform 4.9 cluster, these maximums are 10000 namespaces with 61000 pods, 10000 deployments, 181000 secrets, 400 config maps, and so on. Prometheus is a highly memory intensive application; the resource usage depends on various factors including the number of nodes, objects, the Prometheus metrics scraping interval, metrics or time series, and the age of the cluster. The disk size also depends on the retention period. You must take these factors into consideration and size them accordingly.

These sizing recommendations are only applicable for the Prometheus, Router, and Registry infrastructure components, which are installed during cluster installation. Logging is a day-two operation and is not included in these recommendations.



NOTE

In OpenShift Container Platform 4.9, half of a CPU core (500 millicore) is now reserved by the system by default compared to OpenShift Container Platform 3.11 and previous versions. This influences the stated sizing recommendations.

2.12. ADDITIONAL RESOURCES

- [OpenShift Container Platform cluster maximums](#)
- [Creating infrastructure machine sets](#)

CHAPTER 3. RECOMMENDED HOST PRACTICES FOR IBM Z & LINUXONE ENVIRONMENTS

This topic provides recommended host practices for OpenShift Container Platform on IBM Z and LinuxONE.



NOTE

The s390x architecture is unique in many aspects. Therefore, some recommendations made here might not apply to other platforms.



NOTE

Unless stated otherwise, these practices apply to both z/VM and Red Hat Enterprise Linux (RHEL) KVM installations on IBM Z and LinuxONE.

3.1. MANAGING CPU OVERCOMMITMENT

In a highly virtualized IBM Z environment, you must carefully plan the infrastructure setup and sizing. One of the most important features of virtualization is the capability to do resource overcommitment, allocating more resources to the virtual machines than actually available at the hypervisor level. This is very workload dependent and there is no golden rule that can be applied to all setups.

Depending on your setup, consider these best practices regarding CPU overcommitment:

- At LPAR level (PR/SM hypervisor), avoid assigning all available physical cores (IFLs) to each LPAR. For example, with four physical IFLs available, you should not define three LPARs with four logical IFLs each.
- Check and understand LPAR shares and weights.
- An excessive number of virtual CPUs can adversely affect performance. Do not define more virtual processors to a guest than logical processors are defined to the LPAR.
- Configure the number of virtual processors per guest for peak workload, not more.
- Start small and monitor the workload. Increase the vCPU number incrementally if necessary.
- Not all workloads are suitable for high overcommitment ratios. If the workload is CPU intensive, you will probably not be able to achieve high ratios without performance problems. Workloads that are more I/O intensive can keep consistent performance even with high overcommitment ratios.

Additional resources

- [z/VM Common Performance Problems and Solutions](#)
- [z/VM overcommitment considerations](#)
- [LPAR CPU management](#)

3.2. HOW TO DISABLE TRANSPARENT HUGE PAGES

Transparent Huge Pages (THP) attempt to automate most aspects of creating, managing, and using

huge pages. Since THP automatically manages the huge pages, this is not always handled optimally for all types of workloads. THP can lead to performance regressions, since many applications handle huge pages on their own. Therefore, consider disabling THP. The following steps describe how to disable THP using a Node Tuning Operator (NTO) profile.

3.2.1. Disable THP with a Node Tuning Operator (NTO) profile

Procedure

1. Copy the following NTO sample profile into a YAML file. For example, **thp-s390-tuned.yaml**:

```
apiVersion: tuned.openshift.io/v1
kind: Tuned
metadata:
  name: thp-workers-profile
  namespace: openshift-cluster-node-tuning-operator
spec:
  profile:
    - data: |
        [main]
        summary=Custom tuned profile for OpenShift on IBM Z to turn off THP on worker nodes
        include=openshift-node

        [vm]
        transparent_hugepages=never
        name: openshift-thp-never-worker

    recommend:
      - match:
          - label: node-role.kubernetes.io/worker
          priority: 35
          profile: openshift-thp-never-worker
```

2. Create the NTO profile:

```
$ oc create -f thp-s390-tuned.yaml
```

3. Check the list of active profiles:

```
$ oc get tuned -n openshift-cluster-node-tuning-operator
```

4. Remove the profile:

```
$ oc delete -f thp-s390-tuned.yaml
```

Verification

- Log in to one of the nodes and do a regular THP check to verify if the nodes applied the profile successfully:

```
$ cat /sys/kernel/mm/transparent_hugepage/enabled
always madvise [never]
```

3.3. BOOST NETWORKING PERFORMANCE WITH RECEIVE FLOW STEERING

Receive Flow Steering (RFS) extends Receive Packet Steering (RPS) by further reducing network latency. RFS is technically based on RPS, and improves the efficiency of packet processing by increasing the CPU cache hit rate. RFS achieves this, and in addition considers queue length, by determining the most convenient CPU for computation so that cache hits are more likely to occur within the CPU. Thus, the CPU cache is invalidated less and requires fewer cycles to rebuild the cache. This can help reduce packet processing run time.

3.3.1. Use the Machine Config Operator (MCO) to activate RFS

Procedure

1. Copy the following MCO sample profile into a YAML file. For example, **enable-rfs.yaml**:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: 50-enable-rfs
spec:
  config:
    ignition:
      version: 2.2.0
    storage:
      files:
        - contents:
            source: data:text/plain;charset=US-
            ASCII,%23%20turn%20on%20Receive%20Flow%20Steering%20%28RFS%29%20for%20all%20network%20interfaces%0ASUBSYSTEM%3D%3D%22net%22%2C%20ACTION%3D%3D%22add%22%2C%20RUN%7Bprogram%7D%2B%3D%22/bin/bash%20-
            c%20%27for%20x%20in%20/sys/%24DEVPATH/queues/rx-
            %2A%3B%20do%20echo%208192%20%3E%20%24x/rps_flow_cnt%3B%20%20done%27
            %22%0A
            filesystem: root
            mode: 0644
            path: /etc/udev/rules.d/70-persistent-net.rules
          - contents:
              source: data:text/plain;charset=US-
              ASCII,%23%20define%20sock%20flow%20enbtried%20for%20%20Receive%20Flow%20Ste
              ering%20%28RFS%29%0Anet.core.rps_sock_flow_entries%3D8192%0A
              filesystem: root
              mode: 0644
              path: /etc/sysctl.d/95-enable-rps.conf
```

2. Create the MCO profile:

```
$ oc create -f enable-rfs.yaml
```

3. Verify that an entry named **50-enable-rfs** is listed:

```
$ oc get mc
```

4. To deactivate, enter:

```
$ oc delete mc 50-enable-rfs
```

Additional resources

- [OpenShift Container Platform on IBM Z: Tune your network performance with RFS](#)
- [Configuring Receive Flow Steering \(RFS\)](#)
- [Scaling in the Linux Networking Stack](#)

3.4. CHOOSE YOUR NETWORKING SETUP

The networking stack is one of the most important components for a Kubernetes-based product like OpenShift Container Platform. For IBM Z setups, the networking setup depends on the hypervisor of your choice. Depending on the workload and the application, the best fit usually changes with the use case and the traffic pattern.

Depending on your setup, consider these best practices:

- Consider all options regarding networking devices to optimize your traffic pattern. Explore the advantages of OSA-Express, RoCE Express, HiperSockets, z/VM VSwitch, Linux Bridge (KVM), and others to decide which option leads to the greatest benefit for your setup.
- Always use the latest available NIC version. For example, OSA Express 7S 10 GbE shows great improvement compared to OSA Express 6S 10 GbE with transactional workload types, although both are 10 GbE adapters.
- Each virtual switch adds an additional layer of latency.
- The load balancer plays an important role for network communication outside the cluster. Consider using a production-grade hardware load balancer if this is critical for your application.
- OpenShift Container Platform SDN introduces flows and rules, which impact the networking performance. Make sure to consider pod affinities and placements, to benefit from the locality of services where communication is critical.
- Balance the trade-off between performance and functionality.

Additional resources

- [OpenShift Container Platform on IBM Z - Performance Experiences, Hints and Tips](#)
- [OpenShift Container Platform on IBM Z Networking Performance](#)
- [Controlling pod placement on nodes using node affinity rules](#)

3.5. ENSURE HIGH DISK PERFORMANCE WITH HYPERPAV ON Z/VM

DASD and ECKD devices are commonly used disk types in IBM Z environments. In a typical OpenShift Container Platform setup in z/VM environments, DASD disks are commonly used to support the local storage for the nodes. You can set up HyperPAV alias devices to provide more throughput and overall better I/O performance for the DASD disks that support the z/VM guests.

Using HyperPAV for the local storage devices leads to a significant performance benefit. However, you must be aware that there is a trade-off between throughput and CPU costs.

3.5.1. Use the Machine Config Operator (MCO) to activate HyperPAV aliases in nodes using z/VM full-pack minidisks

For z/VM-based OpenShift Container Platform setups that use full-pack minidisks, you can leverage the advantage of MCO profiles by activating HyperPAV aliases in all of the nodes. You must add YAML configurations for both control plane and compute nodes.

Procedure

1. Copy the following MCO sample profile into a YAML file for the control plane node. For example, **05-master-kernelarg-hpav.yaml**:

```
$ cat 05-master-kernelarg-hpav.yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: master
  name: 05-master-kernelarg-hpav
spec:
  config:
    ignition:
      version: 3.1.0
    kernelArguments:
      - rd.dasd=800-805
```

2. Copy the following MCO sample profile into a YAML file for the compute node. For example, **05-worker-kernelarg-hpav.yaml**:

```
$ cat 05-worker-kernelarg-hpav.yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: 05-worker-kernelarg-hpav
spec:
  config:
    ignition:
      version: 3.1.0
    kernelArguments:
      - rd.dasd=800-805
```



NOTE

You must modify the **rd.dasd** arguments to fit the device IDs.

3. Create the MCO profiles:

```
$ oc create -f 05-master-kernelarg-hpav.yaml
```

```
$ oc create -f 05-worker-kernelarg-hpav.yaml
```

4. To deactivate, enter:

```
$ oc delete -f 05-master-kernelarg-hpav.yaml
```

```
$ oc delete -f 05-worker-kernelarg-hpav.yaml
```

Additional resources

- [Using HyperPAV for ECKD DASD](#)
- [Scaling HyperPAV alias devices on Linux guests on z/VM](#)

3.6. RHEL KVM ON IBM Z HOST RECOMMENDATIONS

Optimizing a KVM virtual server environment strongly depends on the workloads of the virtual servers and on the available resources. The same action that enhances performance in one environment can have adverse effects in another. Finding the best balance for a particular setting can be a challenge and often involves experimentation.

The following section introduces some best practices when using OpenShift Container Platform with RHEL KVM on IBM Z and LinuxONE environments.

3.6.1. Use multiple queues for your VirtIO network interfaces

With multiple virtual CPUs, you can transfer packages in parallel if you provide multiple queues for incoming and outgoing packets. Use the **queues** attribute of the **driver** element to configure multiple queues. Specify an integer of at least 2 that does not exceed the number of virtual CPUs of the virtual server.

The following example specification configures two input and output queues for a network interface:

```
<interface type="direct">
  <source network="net01"/>
  <model type="virtio"/>
  <driver ... queues="2"/>
</interface>
```

Multiple queues are designed to provide enhanced performance for a network interface, but they also use memory and CPU resources. Start with defining two queues for busy interfaces. Next, try two queues for interfaces with less traffic or more than two queues for busy interfaces.

3.6.2. Use I/O threads for your virtual block devices

To make virtual block devices use I/O threads, you must configure one or more I/O threads for the virtual server and each virtual block device to use one of these I/O threads.

The following example specifies **<iouthreads>3</iouthreads>** to configure three I/O threads, with consecutive decimal thread IDs 1, 2, and 3. The **iothread="2"** parameter specifies the driver element of the disk device to use the I/O thread with ID 2.

Sample I/O thread specification

```

...
<domain>
  <iotreads>3</iotreads> 1
  ...
  <devices>
    ...
    <disk type="block" device="disk"> 2
  <driver ... iotread="2"/>
  </disk>
  ...
  </devices>
  ...
</domain>

```

- 1** The number of I/O threads.
- 2** The driver element of the disk device.

Threads can increase the performance of I/O operations for disk devices, but they also use memory and CPU resources. You can configure multiple devices to use the same thread. The best mapping of threads to devices depends on the available resources and the workload.

Start with a small number of I/O threads. Often, a single I/O thread for all disk devices is sufficient. Do not configure more threads than the number of virtual CPUs, and do not configure idle threads.

You can use the **virsh iotreadadd** command to add I/O threads with specific thread IDs to a running virtual server.

3.6.3. Avoid virtual SCSI devices

Configure virtual SCSI devices only if you need to address the device through SCSI-specific interfaces. Configure disk space as virtual block devices rather than virtual SCSI devices, regardless of the backing on the host.

However, you might need SCSI-specific interfaces for:

- A LUN for a SCSI-attached tape drive on the host.
- A DVD ISO file on the host file system that is mounted on a virtual DVD drive.

3.6.4. Configure guest caching for disk

Configure your disk devices to do caching by the guest and not by the host.

Ensure that the driver element of the disk device includes the **cache="none"** and **io="native"** parameters.

```

<disk type="block" device="disk">
  <driver name="qemu" type="raw" cache="none" io="native" iotread="1"/>
  ...
</disk>

```

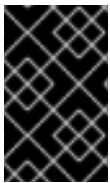
3.6.5. Exclude the memory balloon device

Unless you need a dynamic memory size, do not define a memory balloon device and ensure that libvirt does not create one for you. Include the **memballoon** parameter as a child of the devices element in your domain configuration XML file.

- Check the list of active profiles:

```
<memballoon model="none"/>
```

3.6.6. Tune the CPU migration algorithm of the host scheduler



IMPORTANT

Do not change the scheduler settings unless you are an expert who understands the implications. Do not apply changes to production systems without testing them and confirming that they have the intended effect.

The **kernel.sched_migration_cost_ns** parameter specifies a time interval in nanoseconds. After the last execution of a task, the CPU cache is considered to have useful content until this interval expires. Increasing this interval results in fewer task migrations. The default value is 500000 ns.

If the CPU idle time is higher than expected when there are runnable processes, try reducing this interval. If tasks bounce between CPUs or nodes too often, try increasing it.

To dynamically set the interval to 60000 ns, enter the following command:

```
# sysctl kernel.sched_migration_cost_ns=60000
```

To persistently change the value to 60000 ns, add the following entry to **/etc/sysctl.conf**:

```
kernel.sched_migration_cost_ns=60000
```

3.6.7. Disable the cpuset cgroup controller



NOTE

This setting applies only to KVM hosts with cgroups version 1. To enable CPU hotplug on the host, disable the cgroup controller.

Procedure

1. Open **/etc/libvirt/qemu.conf** with an editor of your choice.
2. Go to the **cgroup_controllers** line.
3. Duplicate the entire line and remove the leading number sign (#) from the copy.
4. Remove the **cpuset** entry, as follows:

```
cgroup_controllers = [ "cpu", "devices", "memory", "blkio", "cpuacct" ]
```

5. For the new setting to take effect, you must restart the libvirtd daemon:

- a. Stop all virtual machines.
- b. Run the following command:

```
# systemctl restart libvirtd
```

- c. Restart the virtual machines.

This setting persists across host reboots.

3.6.8. Tune the polling period for idle virtual CPUs

When a virtual CPU becomes idle, KVM polls for wakeup conditions for the virtual CPU before allocating the host resource. You can specify the time interval, during which polling takes place in sysfs at **/sys/module/kvm/parameters/halt_poll_ns**. During the specified time, polling reduces the wakeup latency for the virtual CPU at the expense of resource usage. Depending on the workload, a longer or shorter time for polling can be beneficial. The time interval is specified in nanoseconds. The default is 50000 ns.

- To optimize for low CPU consumption, enter a small value or write 0 to disable polling:

```
# echo 0 > /sys/module/kvm/parameters/halt_poll_ns
```

- To optimize for low latency, for example for transactional workloads, enter a large value:

```
# echo 80000 > /sys/module/kvm/parameters/halt_poll_ns
```

Additional resources

- [Linux on IBM Z Performance Tuning for KVM](#)
- [Getting started with virtualization on IBM Z](#)

CHAPTER 4. RECOMMENDED CLUSTER SCALING PRACTICES



IMPORTANT

The guidance in this section is only relevant for installations with cloud provider integration.

These guidelines apply to OpenShift Container Platform with software-defined networking (SDN), not Open Virtual Network (OVN).

Apply the following best practices to scale the number of worker machines in your OpenShift Container Platform cluster. You scale the worker machines by increasing or decreasing the number of replicas that are defined in the worker machine set.

4.1. RECOMMENDED PRACTICES FOR SCALING THE CLUSTER

When scaling up the cluster to higher node counts:

- Spread nodes across all of the available zones for higher availability.
- Scale up by no more than 25 to 50 machines at once.
- Consider creating new machine sets in each available zone with alternative instance types of similar size to help mitigate any periodic provider capacity constraints. For example, on AWS, use m5.large and m5d.large.



NOTE

Cloud providers might implement a quota for API services. Therefore, gradually scale the cluster.

The controller might not be able to create the machines if the replicas in the machine sets are set to higher numbers all at one time. The number of requests the cloud platform, which OpenShift Container Platform is deployed on top of, is able to handle impacts the process. The controller will start to query more while trying to create, check, and update the machines with the status. The cloud platform on which OpenShift Container Platform is deployed has API request limits and excessive queries might lead to machine creation failures due to cloud platform limitations.

Enable machine health checks when scaling to large node counts. In case of failures, the health checks monitor the condition and automatically repair unhealthy machines.



NOTE

When scaling large and dense clusters to lower node counts, it might take large amounts of time as the process involves draining or evicting the objects running on the nodes being terminated in parallel. Also, the client might start to throttle the requests if there are too many objects to evict. The default client QPS and burst rates are currently set to **5** and **10** respectively and they cannot be modified in OpenShift Container Platform.

4.2. MODIFYING A MACHINE SET

To make changes to a machine set, edit the **MachineSet** YAML. Then, remove all machines associated with the machine set by deleting each machine or scaling down the machine set to **0** replicas. Then, scale

the replicas back to the desired number. Changes you make to a machine set do not affect existing machines.

If you need to scale a machine set without making other changes, you do not need to delete the machines.



NOTE

By default, the OpenShift Container Platform router pods are deployed on workers. Because the router is required to access some cluster resources, including the web console, do not scale the worker machine set to **0** unless you first relocate the router pods.

Prerequisites

- Install an OpenShift Container Platform cluster and the **oc** command line.
- Log in to **oc** as a user with **cluster-admin** permission.

Procedure

1. Edit the machine set:

```
$ oc edit machineset <machineset> -n openshift-machine-api
```

2. Scale down the machine set to **0**:

```
$ oc scale --replicas=0 machineset <machineset> -n openshift-machine-api
```

Or:

```
$ oc edit machineset <machineset> -n openshift-machine-api
```

TIP

You can alternatively apply the following YAML to scale the machine set:

```
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. Scale up the machine set as needed:

```
$ oc scale --replicas=2 machineset <machineset> -n openshift-machine-api
```

Or:

-

```
$ oc edit machineset <machineset> -n openshift-machine-api
```

TIP

You can alternatively apply the following YAML to scale the machine set:

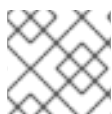
```
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  name: <machineset>
  namespace: openshift-machine-api
spec:
  replicas: 2
```

Wait for the machines to start. The new machines contain changes you made to the machine set.

4.3. ABOUT MACHINE HEALTH CHECKS

Machine health checks automatically repair unhealthy machines in a particular machine pool.

To monitor machine health, create a resource to define the configuration for a controller. Set a condition to check, such as staying in the **NotReady** status for five minutes or displaying a permanent condition in the node-problem-detector, and a label for the set of machines to monitor.



NOTE

You cannot apply a machine health check to a machine with the master role.

The controller that observes a **MachineHealthCheck** resource checks for the defined condition. If a machine fails the health check, the machine is automatically deleted and one is created to take its place. When a machine is deleted, you see a **machine deleted** event.

To limit disruptive impact of the machine deletion, the controller drains and deletes only one node at a time. If there are more unhealthy machines than the **maxUnhealthy** threshold allows for in the targeted pool of machines, remediation stops and therefore enables manual intervention.



NOTE

Consider the timeouts carefully, accounting for workloads and requirements.

- Long timeouts can result in long periods of downtime for the workload on the unhealthy machine.
- Too short timeouts can result in a remediation loop. For example, the timeout for checking the **NotReady** status must be long enough to allow the machine to complete the startup process.

To stop the check, remove the resource.

4.3.1. Limitations when deploying machine health checks

There are limitations to consider before deploying a machine health check:

- Only machines owned by a machine set are remediated by a machine health check.
- Control plane machines are not currently supported and are not remediated if they are unhealthy.
- If the node for a machine is removed from the cluster, a machine health check considers the machine to be unhealthy and remediates it immediately.
- If the corresponding node for a machine does not join the cluster after the **nodeStartupTimeout**, the machine is remediated.
- A machine is remediated immediately if the **Machine** resource phase is **Failed**.

4.4. SAMPLE MACHINEHEALTHCHECK RESOURCE

The **MachineHealthCheck** resource for all cloud-based installation types, and other than bare metal, resembles the following YAML file:

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineHealthCheck
metadata:
  name: example 1
  namespace: openshift-machine-api
spec:
  selector:
    matchLabels:
      machine.openshift.io/cluster-api-machine-role: <role> 2
      machine.openshift.io/cluster-api-machine-type: <role> 3
      machine.openshift.io/cluster-api-machineset: <cluster_name>-<label>-<zone> 4
  unhealthyConditions:
    - type: "Ready"
      timeout: "300s" 5
      status: "False"
    - type: "Ready"
      timeout: "300s" 6
      status: "Unknown"
  maxUnhealthy: "40%" 7
  nodeStartupTimeout: "10m" 8
```

1 Specify the name of the machine health check to deploy.

2 3 Specify a label for the machine pool that you want to check.

4 Specify the machine set to track in **<cluster_name>-<label>-<zone>** format. For example, **prod-node-us-east-1a**.

5 6 Specify the timeout duration for a node condition. If a condition is met for the duration of the timeout, the machine will be remediated. Long timeouts can result in long periods of downtime for a workload on an unhealthy machine.

7 Specify the amount of machines allowed to be concurrently remediated in the targeted pool. This can be set as a percentage or an integer. If the number of unhealthy machines exceeds the limit set

- 8 Specify the timeout duration that a machine health check must wait for a node to join the cluster before a machine is determined to be unhealthy.



NOTE

The **matchLabels** are examples only; you must map your machine groups based on your specific needs.

4.4.1. Short-circuiting machine health check remediation

Short circuiting ensures that machine health checks remediate machines only when the cluster is healthy. Short-circuiting is configured through the **maxUnhealthy** field in the **MachineHealthCheck** resource.

If the user defines a value for the **maxUnhealthy** field, before remediating any machines, the **MachineHealthCheck** compares the value of **maxUnhealthy** with the number of machines within its target pool that it has determined to be unhealthy. Remediation is not performed if the number of unhealthy machines exceeds the **maxUnhealthy** limit.



IMPORTANT

If **maxUnhealthy** is not set, the value defaults to **100%** and the machines are remediated regardless of the state of the cluster.

The appropriate **maxUnhealthy** value depends on the scale of the cluster you deploy and how many machines the **MachineHealthCheck** covers. For example, you can use the **maxUnhealthy** value to cover multiple machine sets across multiple availability zones so that if you lose an entire zone, your **maxUnhealthy** setting prevents further remediation within the cluster.

The **maxUnhealthy** field can be set as either an integer or percentage. There are different remediation implementations depending on the **maxUnhealthy** value.

4.4.1.1. Setting maxUnhealthy by using an absolute value

If **maxUnhealthy** is set to **2**:

- Remediation will be performed if 2 or fewer nodes are unhealthy
- Remediation will not be performed if 3 or more nodes are unhealthy

These values are independent of how many machines are being checked by the machine health check.

4.4.1.2. Setting maxUnhealthy by using percentages

If **maxUnhealthy** is set to **40%** and there are 25 machines being checked:

- Remediation will be performed if 10 or fewer nodes are unhealthy
- Remediation will not be performed if 11 or more nodes are unhealthy

If **maxUnhealthy** is set to **40%** and there are 6 machines being checked:

- Remediation will be performed if 2 or fewer nodes are unhealthy

- Remediation will not be performed if 3 or more nodes are unhealthy

**NOTE**

The allowed number of machines is rounded down when the percentage of **maxUnhealthy** machines that are checked is not a whole number.

4.5. CREATING A MACHINEHEALTHCHECK RESOURCE

You can create a **MachineHealthCheck** resource for all **MachineSets** in your cluster. You should not create a **MachineHealthCheck** resource that targets control plane machines.

Prerequisites

- Install the **oc** command line interface.

Procedure

1. Create a **healthcheck.yml** file that contains the definition of your machine health check.
2. Apply the **healthcheck.yml** file to your cluster:

```
$ oc apply -f healthcheck.yml
```

CHAPTER 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.

5.1. ABOUT THE NODE TUNING OPERATOR

The Node Tuning Operator helps you manage node-level tuning by orchestrating the TuneD daemon. 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 is part of a standard OpenShift Container Platform installation in version 4.1 and later.

5.2. ACCESSING AN EXAMPLE NODE TUNING OPERATOR SPECIFICATION

Use this process to access an example Node Tuning Operator specification.

Procedure

1. Run:

```
$ 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 might be deprecated in future versions of the Node Tuning Operator.

5.3. DEFAULT PROFILES SET ON A CLUSTER

The following are the default profiles set on a cluster.

```
apiVersion: tuned.openshift.io/v1
kind: Tuned
metadata:
  name: default
  namespace: openshift-cluster-node-tuning-operator
spec:
  recommend:
  - profile: "openshift-control-plane"
    priority: 30
    match:
    - label: "node-role.kubernetes.io/master"
    - label: "node-role.kubernetes.io/infra"

  - profile: "openshift-node"
    priority: 40
```

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 ^ {} \;
```

5.4. VERIFYING THAT THE TUNED PROFILES ARE APPLIED

Verify the TuneD profiles that are applied to your cluster node.

```
$ oc get profile -n openshift-cluster-node-tuning-operator
```

Example output

NAME	TUNED	APPLIED	DEGRADED	AGE
master-0	openshift-control-plane	True	False	6h33m
master-1	openshift-control-plane	True	False	6h33m
master-2	openshift-control-plane	True	False	6h33m
worker-a	openshift-node	True	False	6h28m
worker-b	openshift-node	True	False	6h28m

- **NAME:** Name of the Profile object. There is one Profile object per node and their names match.
- **TUNED:** Name of the desired TuneD profile to apply.
- **APPLIED:** **True** if the TuneD daemon applied the desired profile. (**True/False/Unknown**).
- **DEGRADED:** **True** if any errors were reported during application of the TuneD profile (**True/False/Unknown**).
- **AGE:** Time elapsed since the creation of Profile object.

5.5. 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]
    summary=Description of tuned_profile_n profile

    # tuned_profile_n profile settings
```

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.

```
recommend:
<recommend-item-1>
# ...
<recommend-item-n>
```

The individual items of the list:

```

- machineConfigLabels: ❶
  <mcLabels> ❷
  match: ❸
    <match> ❹
  priority: <priority> ❺
  profile: <tuned_profile_name> ❻

```

- ❶ Optional.
- ❷ A dictionary of key/value **MachineConfig** labels. The keys must be unique.
- ❸ If omitted, profile match is assumed unless a profile with a higher priority matches first or **machineConfigLabels** is set.
- ❹ An optional list.
- ❺ Profile ordering priority. Lower numbers mean higher priority (**0** is the highest priority).
- ❻ A TuneD profile to apply on a match. For example **tuned_profile_1**.

<match> is an optional list recursively defined as follows:

```

- label: <label_name> ❶
  value: <label_value> ❷
  type: <label_type> ❸
  <match> ❹

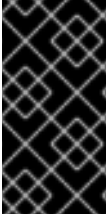
```

- ❶ Node or pod label name.
- ❷ Optional node or pod label value. If omitted, the presence of **<label_name>** is enough to match.
- ❸ Optional object type (**node** or **pod**). If omitted, **node** is assumed.
- ❹ 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.

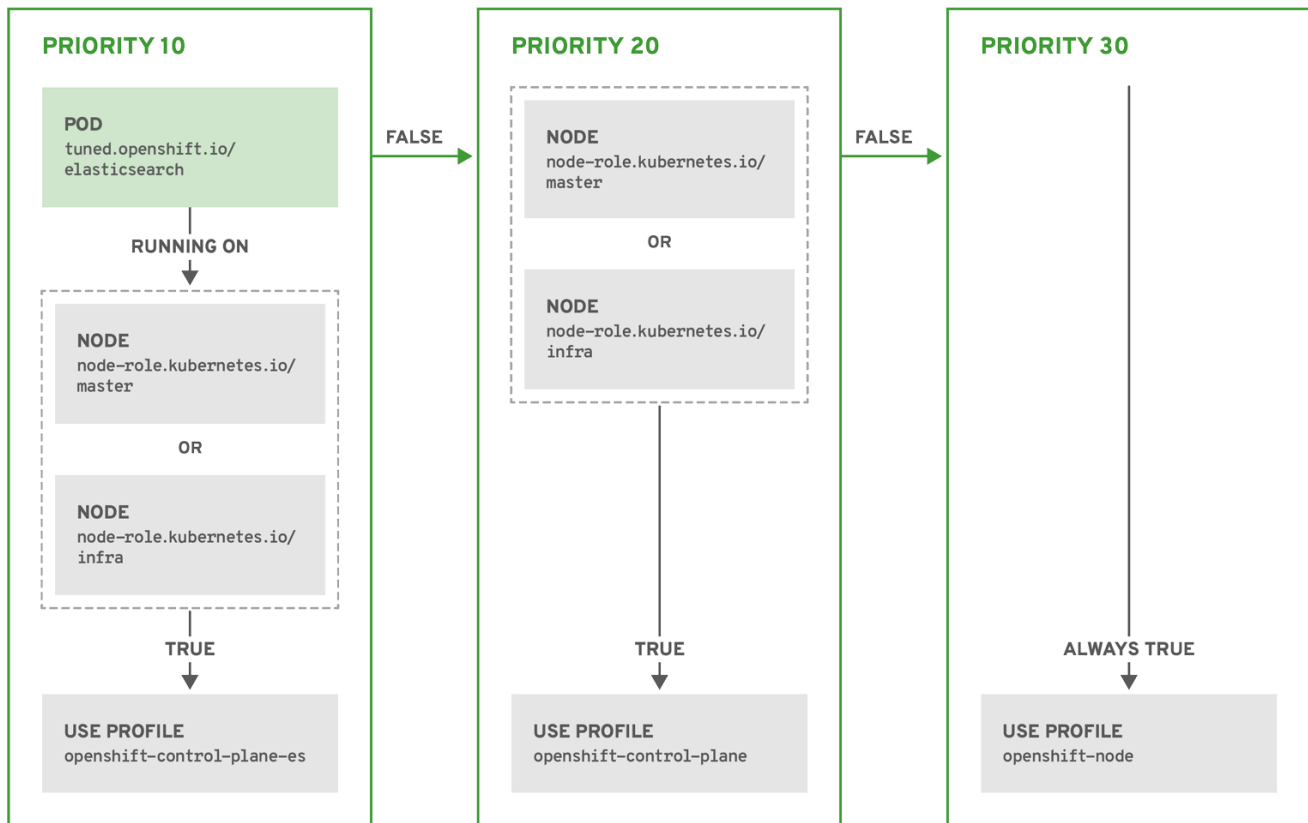
Example: node or pod label based matching

```
- 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.



OPENSIFT_10_0319

Example: machine config pool based matching

```

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
        include=openshift-node
        [bootloader]
        cmdline_openshift_node_custom=+skew_tick=1
        name: openshift-node-custom

  recommend:
    - machineConfigLabels:
        machineconfiguration.openshift.io/role: "worker-custom"
      priority: 20
      profile: openshift-node-custom
  
```

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.

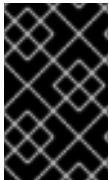
5.6. CUSTOM TUNING EXAMPLES

Using TuneD profiles from the default CR

The following CR applies custom node-level tuning for OpenShift Container Platform nodes with label **tuned.openshift.io/ingress-node-label** set to any value.

Example: custom tuning using the openshift-control-plane TuneD profile

```
apiVersion: tuned.openshift.io/v1
kind: Tuned
metadata:
  name: ingress
  namespace: openshift-cluster-node-tuning-operator
spec:
  profile:
    - data: |
        [main]
        summary=A custom OpenShift ingress profile
        include=openshift-control-plane
        [sysctl]
        net.ipv4.ip_local_port_range="1024 65535"
        net.ipv4.tcp_tw_reuse=1
        name: openshift-ingress
  recommend:
    - match:
        - label: tuned.openshift.io/ingress-node-label
        priority: 10
        profile: openshift-ingress
```



IMPORTANT

Custom profile writers are strongly encouraged to include the default TuneD daemon profiles shipped within the default Tuned CR. The example above uses the default **openshift-control-plane** profile to accomplish this.

Using built-in TuneD profiles

Given the successful rollout of the NTO-managed daemon set, the TuneD operands all manage the same version of the TuneD daemon. To list the built-in TuneD profiles supported by the daemon, query any TuneD pod in the following way:

```
$ oc exec $tuned_pod -n openshift-cluster-node-tuning-operator -- find /usr/lib/tuned/ -name
tuned.conf -printf '%h\n' | sed 's|^.*|/'
```

You can use the profile names retrieved by this in your custom tuning specification.

Example: using built-in hpc-compute TuneD profile

```
apiVersion: tuned.openshift.io/v1
kind: Tuned
metadata:
  name: openshift-node-hpc-compute
  namespace: openshift-cluster-node-tuning-operator
spec:
  profile:
```

```
- data: |
  [main]
  summary=Custom OpenShift node profile for HPC compute workloads
  include=openshift-node,hpc-compute
  name: openshift-node-hpc-compute

recommend:
- match:
  - label: tuned.openshift.io/openshift-node-hpc-compute
  priority: 20
  profile: openshift-node-hpc-compute
```

In addition to the built-in **hpc-compute** profile, the example above includes the **openshift-node** TuneD daemon profile shipped within the default Tuned CR to use OpenShift-specific tuning for compute nodes.

5.7. 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:

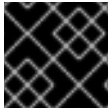
- bootloader
- script

- `systemd`

See [Available TuneD Plug-ins](#) and [Getting Started with TuneD](#) for more information.

CHAPTER 6. USING CLUSTER LOADER

Cluster Loader is a tool that deploys large numbers of various objects to a cluster, which creates user-defined cluster objects. Build, configure, and run Cluster Loader to measure performance metrics of your OpenShift Container Platform deployment at various cluster states.



IMPORTANT

Cluster Loader is now deprecated and will be removed in a future release.

6.1. INSTALLING CLUSTER LOADER

Procedure

1. To pull the container image, run:

```
$ podman pull quay.io/openshift/origin-tests:4.9
```

6.2. RUNNING CLUSTER LOADER

Prerequisites

- The repository will prompt you to authenticate. The registry credentials allow you to access the image, which is not publicly available. Use your existing authentication credentials from installation.

Procedure

1. Execute Cluster Loader using the built-in test configuration, which deploys five template builds and waits for them to complete:

```
$ podman run -v ${LOCAL_KUBECONFIG}:/root/.kube/config:z -i \
quay.io/openshift/origin-tests:4.9 /bin/bash -c 'export KUBECONFIG=/root/.kube/config && \
openshift-tests run-test "[sig-scalability][Feature:Performance] Load cluster \
should populate the cluster [Slow][Serial] [Suite:openshift]'"
```

Alternatively, execute Cluster Loader with a user-defined configuration by setting the environment variable for **VIPERCONFIG**:

```
$ podman run -v ${LOCAL_KUBECONFIG}:/root/.kube/config:z \
-v ${LOCAL_CONFIG_FILE_PATH}:/root/configs:z \
-i quay.io/openshift/origin-tests:4.9 \
/bin/bash -c 'KUBECONFIG=/root/.kube/config VIPERCONFIG=/root/configs/test.yaml \
openshift-tests run-test "[sig-scalability][Feature:Performance] Load cluster \
should populate the cluster [Slow][Serial] [Suite:openshift]'"
```

In this example, **\${LOCAL_KUBECONFIG}** refers to the path to the **kubeconfig** on your local file system. Also, there is a directory called **\${LOCAL_CONFIG_FILE_PATH}**, which is mounted into the container that contains a configuration file called **test.yaml**. Additionally, if the **test.yaml** references any external template files or podspec files, they should also be mounted into the container.

6.3. CONFIGURING CLUSTER LOADER

The tool creates multiple namespaces (projects), which contain multiple templates or pods.

6.3.1. Example Cluster Loader configuration file

Cluster Loader's configuration file is a basic YAML file:

```
provider: local ❶
ClusterLoader:
  cleanup: true
  projects:
    - num: 1
      basename: clusterloader-cakephp-mysql
      tuning: default
      ifexists: reuse
      templates:
        - num: 1
          file: cakephp-mysql.json

    - num: 1
      basename: clusterloader-dancer-mysql
      tuning: default
      ifexists: reuse
      templates:
        - num: 1
          file: dancer-mysql.json

    - num: 1
      basename: clusterloader-django-postgresql
      tuning: default
      ifexists: reuse
      templates:
        - num: 1
          file: django-postgresql.json

    - num: 1
      basename: clusterloader-nodejs-mongodb
      tuning: default
      ifexists: reuse
      templates:
        - num: 1
          file: quickstarts/nodejs-mongodb.json

    - num: 1
      basename: clusterloader-rails-postgresql
      tuning: default
      templates:
        - num: 1
          file: rails-postgresql.json

  tuningsets: ❷
    - name: default
      pods:
        stepping: ❸
```

```

stepsize: 5
pause: 0 s
rate_limit: 4
delay: 0 ms

```

- 1 Optional setting for end-to-end tests. Set to **local** to avoid extra log messages.
- 2 The tuning sets allow rate limiting and stepping, the ability to create several batches of pods while pausing in between sets. Cluster Loader monitors completion of the previous step before continuing.
- 3 Stepping will pause for **M** seconds after each **N** objects are created.
- 4 Rate limiting will wait **M** milliseconds between the creation of objects.

This example assumes that references to any external template files or pod spec files are also mounted into the container.



IMPORTANT

If you are running Cluster Loader on Microsoft Azure, then you must set the **AZURE_AUTH_LOCATION** variable to a file that contains the output of **terraform.azure.auto.tfvars.json**, which is present in the installer directory.

6.3.2. Configuration fields

Table 6.1. Top-level Cluster Loader Fields

Field	Description
cleanup	Set to true or false . One definition per configuration. If set to true , cleanup deletes all namespaces (projects) created by Cluster Loader at the end of the test.
projects	A sub-object with one or many definition(s). Under projects , each namespace to create is defined and projects has several mandatory subheadings.
tuningsets	A sub-object with one definition per configuration. tuningsets allows the user to define a tuning set to add configurable timing to project or object creation (pods, templates, and so on).
sync	An optional sub-object with one definition per configuration. Adds synchronization possibilities during object creation.

Table 6.2. Fields under **projects**

Field	Description
num	An integer. One definition of the count of how many projects to create.
basename	A string. One definition of the base name for the project. The count of identical namespaces will be appended to Basename to prevent collisions.
tuning	A string. One definition of what tuning set you want to apply to the objects, which you deploy inside this namespace.
ifexists	A string containing either reuse or delete . Defines what the tool does if it finds a project or namespace that has the same name of the project or namespace it creates during execution.
configmaps	A list of key-value pairs. The key is the config map name and the value is a path to a file from which you create the config map.
secrets	A list of key-value pairs. The key is the secret name and the value is a path to a file from which you create the secret.
Pods	A sub-object with one or many definition(s) of pods to deploy.
templates	A sub-object with one or many definition(s) of templates to deploy.

Table 6.3. Fields under **pods** and **templates**

Field	Description
num	An integer. The number of pods or templates to deploy.
image	A string. The docker image URL to a repository where it can be pulled.
basename	A string. One definition of the base name for the template (or pod) that you want to create.
file	A string. The path to a local file, which is either a pod spec or template to be created.

Field	Description
parameters	Key-value pairs. Under parameters , you can specify a list of values to override in the pod or template.

Table 6.4. Fields under **tuningsets**

Field	Description
name	A string. The name of the tuning set which will match the name specified when defining a tuning in a project.
pods	A sub-object identifying the tuningsets that will apply to pods.
templates	A sub-object identifying the tuningsets that will apply to templates.

Table 6.5. Fields under **tuningsets pods** or **tuningsets templates**

Field	Description
stepping	A sub-object. A stepping configuration used if you want to create an object in a step creation pattern.
rate_limit	A sub-object. A rate-limiting tuning set configuration to limit the object creation rate.

Table 6.6. Fields under **tuningsets pods** or **tuningsets templates, stepping**

Field	Description
stepsize	An integer. How many objects to create before pausing object creation.
pause	An integer. How many seconds to pause after creating the number of objects defined in stepsize .
timeout	An integer. How many seconds to wait before failure if the object creation is not successful.
delay	An integer. How many milliseconds (ms) to wait between creation requests.

Table 6.7. Fields under **sync**

Field	Description
server	A sub-object with enabled and port fields. The boolean enabled defines whether to start an HTTP server for pod synchronization. The integer port defines the HTTP server port to listen on (9090 by default).
running	A boolean. Wait for pods with labels matching selectors to go into Running state.
succeeded	A boolean. Wait for pods with labels matching selectors to go into Completed state.
selectors	A list of selectors to match pods in Running or Completed states.
timeout	A string. The synchronization timeout period to wait for pods in Running or Completed states. For values that are not 0 , use units: [ns us ms s m h].

6.4. KNOWN ISSUES

- Cluster Loader fails when called without configuration. ([BZ#1761925](#))
- If the **IDENTIFIER** parameter is not defined in user templates, template creation fails with **error: unknown parameter name "IDENTIFIER"**. If you deploy templates, add this parameter to your template to avoid this error:

```
{
  "name": "IDENTIFIER",
  "description": "Number to append to the name of resources",
  "value": "1"
}
```

If you deploy pods, adding the parameter is unnecessary.

CHAPTER 7. USING CPU MANAGER

CPU Manager manages groups of CPUs and constrains workloads to specific CPUs.

CPU Manager is useful for workloads that have some of these attributes:

- Require as much CPU time as possible.
- Are sensitive to processor cache misses.
- Are low-latency network applications.
- Coordinate with other processes and benefit from sharing a single processor cache.

7.1. SETTING UP CPU MANAGER

Procedure

1. Optional: Label a node:

```
# oc label node perf-node.example.com cpumanager=true
```

2. Edit the **MachineConfigPool** of the nodes where CPU Manager should be enabled. In this example, all workers have CPU Manager enabled:

```
# oc edit machineconfigpool worker
```

3. Add a label to the worker machine config pool:

```
metadata:
  creationTimestamp: 2020-xx-xxx
  generation: 3
  labels:
    custom-kubelet: cpumanager-enabled
```

4. Create a **KubeletConfig**, **cpumanager-kubeletconfig.yaml**, custom resource (CR). Refer to the label created in the previous step to have the correct nodes updated with the new kubelet config. See the **machineConfigPoolSelector** section:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: cpumanager-enabled
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: cpumanager-enabled
  kubeletConfig:
    cpuManagerPolicy: static ❶
    cpuManagerReconcilePeriod: 5s ❷
```

- ❶ Specify a policy:

- **none.** This policy explicitly enables the existing default CPU affinity scheme, providing no affinity beyond what the scheduler does automatically.
- **static.** This policy allows pods with certain resource characteristics to be granted increased CPU affinity and exclusivity on the node.

2 Optional. Specify the CPU Manager reconcile frequency. The default is **5s**.

5. Create the dynamic kubelet config:

```
# oc create -f cpumanager-kubeletconfig.yaml
```

This adds the CPU Manager feature to the kubelet config and, if needed, the Machine Config Operator (MCO) reboots the node. To enable CPU Manager, a reboot is not needed.

6. Check for the merged kubelet config:

```
# oc get machineconfig 99-worker-XXXXXX-XXXXX-XXXX-XXXXX-kubelet -o json | grep
ownerReference -A7
```

Example output

```
"ownerReferences": [
  {
    "apiVersion": "machineconfiguration.openshift.io/v1",
    "kind": "KubeletConfig",
    "name": "cpumanager-enabled",
    "uid": "7ed5616d-6b72-11e9-aae1-021e1ce18878"
  }
]
```

7. Check the worker for the updated **kubelet.conf**:

```
# oc debug node/perf-node.example.com
sh-4.2# cat /host/etc/kubernetes/kubelet.conf | grep cpuManager
```

Example output

```
cpuManagerPolicy: static 1
cpuManagerReconcilePeriod: 5s 2
```

1 2 These settings were defined when you created the **KubeletConfig** CR.

8. Create a pod that requests a core or multiple cores. Both limits and requests must have their CPU value set to a whole integer. That is the number of cores that will be dedicated to this pod:

```
# cat cpumanager-pod.yaml
```

Example output

```
apiVersion: v1
```

```

kind: Pod
metadata:
  generateName: cpumanager-
spec:
  containers:
  - name: cpumanager
    image: gcr.io/google_containers/pause-amd64:3.0
    resources:
      requests:
        cpu: 1
        memory: "1G"
      limits:
        cpu: 1
        memory: "1G"
  nodeSelector:
    cpumanager: "true"

```

9. Create the pod:

```
# oc create -f cpumanager-pod.yaml
```

10. Verify that the pod is scheduled to the node that you labeled:

```
# oc describe pod cpumanager
```

Example output

```

Name:          cpumanager-6cqz7
Namespace:     default
Priority:       0
PriorityClassName: <none>
Node: perf-node.example.com/xxx.xx.xx.xxx
...
Limits:
  cpu: 1
  memory: 1G
Requests:
  cpu: 1
  memory: 1G
...
QoS Class:     Guaranteed
Node-Selectors: cpumanager=true

```

11. Verify that the **cgroups** are set up correctly. Get the process ID (PID) of the **pause** process:

```

# └─init.scope
|   └─1 /usr/lib/systemd/systemd --switched-root --system --deserialize 17
└─kubepods.slice
    └─kubepods-pod69c01f8e_6b74_11e9_ac0f_0a2b62178a22.slice
        └─crio-b5437308f1a574c542bdf08563b865c0345c8f8c0b0a655612c.scope
            └─32706 /pause

```

Pods of quality of service (QoS) tier **Guaranteed** are placed within the **kubepods.slice**. Pods of other QoS tiers end up in child **cgroups** of **kubepods**:


```
# cd /sys/fs/cgroup/cpuset/kubepods.slice/kubepods-
pod69c01f8e_6b74_11e9_ac0f_0a2b62178a22.slice/crio-
b5437308f1ad1a7db0574c542bdf08563b865c0345c86e9585f8c0b0a655612c.scope
# for i in `ls cpuset.cpus tasks` ; do echo -n "$i "; cat $i ; done
```

Example output

```
cpuset.cpus 1
tasks 32706
```

12. Check the allowed CPU list for the task:

```
# grep ^Cpus_allowed_list /proc/32706/status
```

Example output

```
Cpus_allowed_list: 1
```

13. Verify that another pod (in this case, the pod in the **burstable** QoS tier) on the system cannot run on the core allocated for the **Guaranteed** pod:

```
# cat /sys/fs/cgroup/cpuset/kubepods.slice/kubepods-besteffort.slice/kubepods-besteffort-
podc494a073_6b77_11e9_98c0_06bba5c387ea.slice/crio-
c56982f57b75a2420947f0afc6cafe7534c5734efc34157525fa9abbf99e3849.scope/cpuset.cpus

0
# oc describe node perf-node.example.com
```

Example output

```
...
Capacity:
attachable-volumes-aws-ebs: 39
cpu: 2
ephemeral-storage: 124768236Ki
hugepages-1Gi: 0
hugepages-2Mi: 0
memory: 8162900Ki
pods: 250
Allocatable:
attachable-volumes-aws-ebs: 39
cpu: 1500m
ephemeral-storage: 124768236Ki
hugepages-1Gi: 0
hugepages-2Mi: 0
memory: 7548500Ki
pods: 250
-----
-
  default          cpumanager-6cqz7      1 (66%)    1 (66%)    1G (12%)
1G (12%)    29m

Allocated resources:
```

(Total limits may be over 100 percent, i.e., overcommitted.)

Resource	Requests	Limits
-----	-----	-----
cpu	1440m (96%)	1 (66%)

This VM has two CPU cores. The **system-reserved** setting reserves 500 millicores, meaning that half of one core is subtracted from the total capacity of the node to arrive at the **Node Allocatable** amount. You can see that **Allocatable CPU** is 1500 millicores. This means you can run one of the CPU Manager pods since each will take one whole core. A whole core is equivalent to 1000 millicores. If you try to schedule a second pod, the system will accept the pod, but it will never be scheduled:

NAME	READY	STATUS	RESTARTS	AGE
cpumanager-6cqz7	1/1	Running	0	33m
cpumanager-7qc2t	0/1	Pending	0	11s

CHAPTER 8. USING TOPOLOGY MANAGER

Topology Manager collects hints from the CPU Manager, Device Manager, and other Hint Providers to align pod resources, such as CPU, SR-IOV VFs, and other device resources, for all Quality of Service (QoS) classes on the same non-uniform memory access (NUMA) node.

Topology Manager uses topology information from collected hints to decide if a pod can be accepted or rejected on a node, based on the configured Topology Manager policy and Pod resources requested.

Topology Manager is useful for workloads that use hardware accelerators to support latency-critical execution and high throughput parallel computation.



NOTE

To use Topology Manager you must use the CPU Manager with the **static** policy. For more information on CPU Manager, see [Using CPU Manager](#).

8.1. TOPOLOGY MANAGER POLICIES

Topology Manager aligns **Pod** resources of all Quality of Service (QoS) classes by collecting topology hints from Hint Providers, such as CPU Manager and Device Manager, and using the collected hints to align the **Pod** resources.



NOTE

To align CPU resources with other requested resources in a **Pod** spec, the CPU Manager must be enabled with the **static** CPU Manager policy.

Topology Manager supports four allocation policies, which you assign in the **cpumanager-enabled** custom resource (CR):

none policy

This is the default policy and does not perform any topology alignment.

best-effort policy

For each container in a pod with the **best-effort** topology management policy, kubelet calls each Hint Provider to discover their resource availability. Using this information, the Topology Manager stores the preferred NUMA Node affinity for that container. If the affinity is not preferred, Topology Manager stores this and admits the pod to the node.

restricted policy

For each container in a pod with the **restricted** topology management policy, kubelet calls each Hint Provider to discover their resource availability. Using this information, the Topology Manager stores the preferred NUMA Node affinity for that container. If the affinity is not preferred, Topology Manager rejects this pod from the node, resulting in a pod in a **Terminated** state with a pod admission failure.

single-numa-node policy

For each container in a pod with the **single-numa-node** topology management policy, kubelet calls each Hint Provider to discover their resource availability. Using this information, the Topology Manager determines if a single NUMA Node affinity is possible. If it is, the pod is admitted to the node. If a single NUMA Node affinity is not possible, the Topology Manager rejects the pod from the node. This results in a pod in a Terminated state with a pod admission failure.

8.2. SETTING UP TOPOLOGY MANAGER

To use Topology Manager, you must configure an allocation policy in the **cpumanager-enabled** custom resource (CR). This file might exist if you have set up CPU Manager. If the file does not exist, you can create the file.

Prerequisites

- Configure the CPU Manager policy to be **static**. See the Using CPU Manager in the Scalability and Performance section.

Procedure

To activate Topology Manager:

1. Configure the Topology Manager allocation policy in the **cpumanager-enabled** custom resource (CR).

```
$ oc edit KubeletConfig cpumanager-enabled

apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: cpumanager-enabled
spec:
  machineConfigPoolSelector:
    matchLabels:
      custom-kubelet: cpumanager-enabled
  kubeletConfig:
    cpuManagerPolicy: static 1
    cpuManagerReconcilePeriod: 5s
    topologyManagerPolicy: single-numa-node 2
```

- 1** This parameter must be **static**.
- 2** Specify your selected Topology Manager allocation policy. Here, the policy is **single-numa-node**. Acceptable values are: **default**, **best-effort**, **restricted**, **single-numa-node**.

Additional resources

For more information on CPU Manager, see [Using CPU Manager](#).

8.3. POD INTERACTIONS WITH TOPOLOGY MANAGER POLICIES

The example **Pod** specs below help illustrate pod interactions with Topology Manager.

The following pod runs in the **BestEffort** QoS class because no resource requests or limits are specified.

```
spec:
  containers:
  - name: nginx
    image: nginx
```

The next pod runs in the **Burstable** QoS class because requests are less than limits.

```
spec:
  containers:
  - name: nginx
    image: nginx
    resources:
      limits:
        memory: "200Mi"
      requests:
        memory: "100Mi"
```

If the selected policy is anything other than **none**, Topology Manager would not consider either of these **Pod** specifications.

The last example pod below runs in the Guaranteed QoS class because requests are equal to limits.

```
spec:
  containers:
  - name: nginx
    image: nginx
    resources:
      limits:
        memory: "200Mi"
        cpu: "2"
        example.com/device: "1"
      requests:
        memory: "200Mi"
        cpu: "2"
        example.com/device: "1"
```

Topology Manager would consider this pod. The Topology Manager consults the CPU Manager static policy, which returns the topology of available CPUs. Topology Manager also consults Device Manager to discover the topology of available devices for example.com/device.

Topology Manager will use this information to store the best Topology for this container. In the case of this pod, CPU Manager and Device Manager will use this stored information at the resource allocation stage.

CHAPTER 9. SCALING THE CLUSTER MONITORING OPERATOR

OpenShift Container Platform exposes metrics that the Cluster Monitoring Operator collects and stores in the Prometheus-based monitoring stack. As an administrator, you can view system resources, containers and components metrics in one dashboard interface, Grafana.



IMPORTANT

If you are running cluster monitoring with an attached PVC for Prometheus, you might experience OOM kills during cluster upgrade. When persistent storage is in use for Prometheus, Prometheus memory usage doubles during cluster upgrade and for several hours after upgrade is complete. To avoid the OOM kill issue, allow worker nodes with double the size of memory that was available prior to the upgrade. For example, if you are running monitoring on the minimum recommended nodes, which is 2 cores with 8 GB of RAM, increase memory to 16 GB. For more information, see [BZ#1925061](#).

9.1. PROMETHEUS DATABASE STORAGE REQUIREMENTS

Red Hat performed various tests for different scale sizes.



NOTE

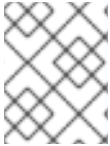
The Prometheus storage requirements below are not prescriptive. Higher resource consumption might be observed in your cluster depending on workload activity and resource use.

Table 9.1. Prometheus Database storage requirements based on number of nodes/pods in the cluster

Number of Nodes	Number of pods	Prometheus storage growth per day	Prometheus storage growth per 15 days	RAM Space (per scale size)	Network (per tsdb chunk)
50	1800	6.3 GB	94 GB	6 GB	16 MB
100	3600	13 GB	195 GB	10 GB	26 MB
150	5400	19 GB	283 GB	12 GB	36 MB
200	7200	25 GB	375 GB	14 GB	46 MB

Approximately 20 percent of the expected size was added as overhead to ensure that the storage requirements do not exceed the calculated value.

The above calculation is for the default OpenShift Container Platform Cluster Monitoring Operator.

**NOTE**

CPU utilization has minor impact. The ratio is approximately 1 core out of 40 per 50 nodes and 1800 pods.

Recommendations for OpenShift Container Platform

- Use at least three infrastructure (infra) nodes.
- Use at least three **openshift-container-storage** nodes with non-volatile memory express (NVMe) drives.

9.2. CONFIGURING CLUSTER MONITORING**Procedure**

To increase the storage capacity for Prometheus:

1. Create a YAML configuration file, **cluster-monitoring-config.yml**. For example:

```
apiVersion: v1
kind: ConfigMap
data:
  config.yaml: |
    prometheusOperator:
      baseImage: quay.io/coreos/prometheus-operator
      prometheusConfigReloaderBaseImage: quay.io/coreos/prometheus-config-reloader
      configReloaderBaseImage: quay.io/coreos/configmap-reload
      nodeSelector:
        node-role.kubernetes.io/infra: ""
    prometheusK8s:
      retention: {{PROMETHEUS_RETENTION_PERIOD}} ❶
      baseImage: openshift/prometheus
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      volumeClaimTemplate:
        spec:
          storageClassName: gp2
          resources:
            requests:
              storage: {{PROMETHEUS_STORAGE_SIZE}} ❷
    alertmanagerMain:
      baseImage: openshift/prometheus-alertmanager
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      volumeClaimTemplate:
        spec:
          storageClassName: gp2
          resources:
            requests:
              storage: {{ALERTMANAGER_STORAGE_SIZE}} ❸
    nodeExporter:
      baseImage: openshift/prometheus-node-exporter
    kubeRbacProxy:
      baseImage: quay.io/coreos/kube-rbac-proxy
```

```

kubeStateMetrics:
  baseImage: quay.io/coreos/kube-state-metrics
  nodeSelector:
    node-role.kubernetes.io/infra: ""
grafana:
  baseImage: grafana/grafana
  nodeSelector:
    node-role.kubernetes.io/infra: ""
auth:
  baseImage: openshift/oauth-proxy
k8sPrometheusAdapter:
  nodeSelector:
    node-role.kubernetes.io/infra: ""
metadata:
  name: cluster-monitoring-config
namespace: openshift-monitoring

```

- 1 A typical value is **PROMETHEUS_RETENTION_PERIOD=15d**. Units are measured in time using one of these suffixes: s, m, h, d.
- 2 A typical value is **PROMETHEUS_STORAGE_SIZE=2000Gi**. Storage values can be a plain integer or as a fixed-point integer using one of these suffixes: E, P, T, G, M, K. You can also use the power-of-two equivalents: Ei, Pi, Ti, Gi, Mi, Ki.
- 3 A typical value is **ALERTMANAGER_STORAGE_SIZE=20Gi**. Storage values can be a plain integer or as a fixed-point integer using one of these suffixes: E, P, T, G, M, K. You can also use the power-of-two equivalents: Ei, Pi, Ti, Gi, Mi, Ki.

2. Set the values like the retention period and storage sizes.
3. Apply the changes by running:

```
$ oc create -f cluster-monitoring-config.yml
```


CHAPTER 10. PLANNING YOUR ENVIRONMENT ACCORDING TO OBJECT MAXIMUMS

Consider the following tested object maximums when you plan your OpenShift Container Platform cluster.

These guidelines are based on the largest possible cluster. For smaller clusters, the maximums are lower. There are many factors that influence the stated thresholds, including the etcd version or storage data format.



IMPORTANT

These guidelines apply to OpenShift Container Platform with software-defined networking (SDN), not Open Virtual Network (OVN).

In most cases, exceeding these numbers results in lower overall performance. It does not necessarily mean that the cluster will fail.

10.1. OPENSIFT CONTAINER PLATFORM TESTED CLUSTER MAXIMUMS FOR MAJOR RELEASES

Tested Cloud Platforms for OpenShift Container Platform 3.x: Red Hat OpenStack Platform (RHOSP), Amazon Web Services and Microsoft Azure. Tested Cloud Platforms for OpenShift Container Platform 4.x: Amazon Web Services, Microsoft Azure and Google Cloud Platform.

Maximum type	3.x tested maximum	4.x tested maximum
Number of nodes	2,000	2,000 ^[1]
Number of pods ^[2]	150,000	150,000
Number of pods per node	250	500 ^[3]
Number of pods per core	There is no default value.	There is no default value.
Number of namespaces ^[4]	10,000	10,000
Number of builds	10,000 (Default pod RAM 512 Mi) - Pipeline Strategy	10,000 (Default pod RAM 512 Mi) - Source-to-Image (S2I) build strategy
Number of pods per namespace ^[5]	25,000	25,000
Number of services ^[6]	10,000	10,000
Number of services per namespace	5,000	5,000

Maximum type	3.x tested maximum	4.x tested maximum
Number of back-ends per service	5,000	5,000
Number of deployments per namespace ^[5]	2,000	2,000
Number of build configs	12,000	12,000
Number of secrets	40,000	40,000

1. Pause pods were deployed to stress the control plane components of OpenShift at 2000 node scale.
2. The pod count displayed here is the number of test pods. The actual number of pods depends on the application's memory, CPU, and storage requirements.
3. This was tested on a cluster with 100 worker nodes with 500 pods per worker node. The default **maxPods** is still 250. To get to 500 **maxPods**, the cluster must be created with a **maxPods** set to **500** using a custom kubelet config. If you need 500 user pods, you need a **hostPrefix** of **22** because there are 10-15 system pods already running on the node. The maximum number of pods with attached persistent volume claims (PVC) depends on storage backend from where PVC are allocated. In our tests, only OpenShift Container Storage v4 (OCS v4) was able to satisfy the number of pods per node discussed in this document.
4. When there are a large number of active projects, etcd might suffer from poor performance if the keypace grows excessively large and exceeds the space quota. Periodic maintenance of etcd, including defragmentation, is highly recommended to free etcd storage.
5. There are a number of control loops in the system that must iterate over all objects in a given namespace as a reaction to some changes in state. Having a large number of objects of a given type in a single namespace can make those loops expensive and slow down processing given state changes. The limit assumes that the system has enough CPU, memory, and disk to satisfy the application requirements.
6. Each service port and each service back-end has a corresponding entry in iptables. The number of back-ends of a given service impact the size of the endpoints objects, which impacts the size of data that is being sent all over the system.



NOTE

Red Hat does not provide direct guidance on sizing your OpenShift Container Platform cluster. This is because determining whether your cluster is within the supported bounds of OpenShift Container Platform requires careful consideration of all the multidimensional factors that limit the cluster scale.

10.2. OPENSIFT CONTAINER PLATFORM ENVIRONMENT AND CONFIGURATION ON WHICH THE CLUSTER MAXIMUMS ARE TESTED

AWS cloud platform:

Node	Flavor	vCPU	RAM(GiB)	Disk type	Disk size(GiB) /IOS	Count	Region
Master/etcd ^[1]	r5.4xlarge	16	128	io1	220 / 3000	3	us-west-2
Infra ^[2]	m5.12xlarge	48	192	gp2	100	3	us-west-2
Workload ^[3]	m5.4xlarge	16	64	gp2	500 ^[4]	1	us-west-2
Worker	m5.2xlarge	8	32	gp2	100	3/25/250 /500 ^[5]	us-west-2

1. io1 disks with 3000 IOPS are used for master/etcd nodes as etcd is I/O intensive and latency sensitive.
2. Infra nodes are used to host Monitoring, Ingress, and Registry components to ensure they have enough resources to run at large scale.
3. Workload node is dedicated to run performance and scalability workload generators.
4. Larger disk size is used so that there is enough space to store the large amounts of data that is collected during the performance and scalability test run.
5. Cluster is scaled in iterations and performance and scalability tests are executed at the specified node counts.

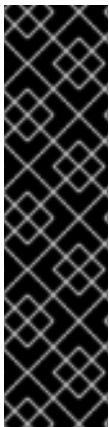
IBM Power Systems platform:

Node	vCPU	RAM(GiB)	Disk type	Disk size(GiB)/IOS	Count
Master/etcd ^[1]	16	32	io1	120 / 3 IOPS per GB	3
Infra ^[2]	16	64	gp2	120	2
Workload ^[3]	16	256	gp2	120 ^[4]	1
Worker	16	64	gp2	120	3/25/250/500 ^[5]

1. io1 disks with 120 / 3 IOPS per GB are used for master/etcd nodes as etcd is I/O intensive and latency sensitive.

2. Infra nodes are used to host Monitoring, Ingress, and Registry components to ensure they have enough resources to run at large scale.
3. Workload node is dedicated to run performance and scalability workload generators.
4. Larger disk size is used so that there is enough space to store the large amounts of data that is collected during the performance and scalability test run.
5. Cluster is scaled in iterations and performance and scalability tests are executed at the specified node counts.

10.3. HOW TO PLAN YOUR ENVIRONMENT ACCORDING TO TESTED CLUSTER MAXIMUMS



IMPORTANT

Oversubscribing the physical resources on a node affects resource guarantees the Kubernetes scheduler makes during pod placement. Learn what measures you can take to avoid memory swapping.

Some of the tested maximums are stretched only in a single dimension. They will vary when many objects are running on the cluster.

The numbers noted in this documentation are based on Red Hat's test methodology, setup, configuration, and tunings. These numbers can vary based on your own individual setup and environments.

While planning your environment, determine how many pods are expected to fit per node:

$$\text{required pods per cluster} / \text{pods per node} = \text{total number of nodes needed}$$

The current maximum number of pods per node is 250. However, the number of pods that fit on a node is dependent on the application itself. Consider the application's memory, CPU, and storage requirements, as described in *How to plan your environment according to application requirements*.

Example scenario

If you want to scope your cluster for 2200 pods per cluster, you would need at least five nodes, assuming that there are 500 maximum pods per node:

$$2200 / 500 = 4.4$$

If you increase the number of nodes to 20, then the pod distribution changes to 110 pods per node:

$$2200 / 20 = 110$$

Where:

$$\text{required pods per cluster} / \text{total number of nodes} = \text{expected pods per node}$$

10.4. HOW TO PLAN YOUR ENVIRONMENT ACCORDING TO APPLICATION REQUIREMENTS

Consider an example application environment:

Pod type	Pod quantity	Max memory	CPU cores	Persistent storage
apache	100	500 MB	0.5	1 GB
node.js	200	1 GB	1	1 GB
postgresql	100	1 GB	2	10 GB
JBoss EAP	100	1 GB	1	1 GB

Extrapolated requirements: 550 CPU cores, 450GB RAM, and 1.4TB storage.

Instance size for nodes can be modulated up or down, depending on your preference. Nodes are often resource overcommitted. In this deployment scenario, you can choose to run additional smaller nodes or fewer larger nodes to provide the same amount of resources. Factors such as operational agility and cost-per-instance should be considered.

Node type	Quantity	CPUs	RAM (GB)
Nodes (option 1)	100	4	16
Nodes (option 2)	50	8	32
Nodes (option 3)	25	16	64

Some applications lend themselves well to overcommitted environments, and some do not. Most Java applications and applications that use huge pages are examples of applications that would not allow for overcommitment. That memory can not be used for other applications. In the example above, the environment would be roughly 30 percent overcommitted, a common ratio.

The application pods can access a service either by using environment variables or DNS. If using environment variables, for each active service the variables are injected by the kubelet when a pod is run on a node. A cluster-aware DNS server watches the Kubernetes API for new services and creates a set of DNS records for each one. If DNS is enabled throughout your cluster, then all pods should automatically be able to resolve services by their DNS name. Service discovery using DNS can be used in case you must go beyond 5000 services. When using environment variables for service discovery, the argument list exceeds the allowed length after 5000 services in a namespace, then the pods and deployments will start failing. Disable the service links in the deployment's service specification file to overcome this:

```
---
apiVersion: v1
kind: Template
metadata:
  name: deployment-config-template
  creationTimestamp:
  annotations:
```

```

description: This template will create a deploymentConfig with 1 replica, 4 env vars and a service.
tags: "
objects:
- apiVersion: v1
  kind: DeploymentConfig
  metadata:
    name: deploymentconfig${IDENTIFIER}
  spec:
    template:
      metadata:
        labels:
          name: replicationcontroller${IDENTIFIER}
      spec:
        enableServiceLinks: false
        containers:
        - name: pause${IDENTIFIER}
          image: "${IMAGE}"
          ports:
          - containerPort: 8080
            protocol: TCP
          env:
          - name: ENVVAR1_${IDENTIFIER}
            value: "${ENV_VALUE}"
          - name: ENVVAR2_${IDENTIFIER}
            value: "${ENV_VALUE}"
          - name: ENVVAR3_${IDENTIFIER}
            value: "${ENV_VALUE}"
          - name: ENVVAR4_${IDENTIFIER}
            value: "${ENV_VALUE}"
          resources: {}
          imagePullPolicy: IfNotPresent
          capabilities: {}
          securityContext:
            capabilities: {}
            privileged: false
          restartPolicy: Always
          serviceAccount: "
        replicas: 1
        selector:
          name: replicationcontroller${IDENTIFIER}
        triggers:
        - type: ConfigChange
        strategy:
          type: Rolling
- apiVersion: v1
  kind: Service
  metadata:
    name: service${IDENTIFIER}
  spec:
    selector:
      name: replicationcontroller${IDENTIFIER}
    ports:
    - name: serviceport${IDENTIFIER}
      protocol: TCP
      port: 80
      targetPort: 8080

```

```

portalIP: "
type: ClusterIP
sessionAffinity: None
status:
  loadBalancer: {}
parameters:
- name: IDENTIFIER
  description: Number to append to the name of resources
  value: '1'
  required: true
- name: IMAGE
  description: Image to use for deploymentConfig
  value: gcr.io/google-containers/pause-amd64:3.0
  required: false
- name: ENV_VALUE
  description: Value to use for environment variables
  generate: expression
  from: "[A-Za-z0-9]{255}"
  required: false
labels:
  template: deployment-config-template

```

The number of application pods that can run in a namespace is dependent on the number of services and the length of the service name when the environment variables are used for service discovery.

ARG_MAX on the system defines the maximum argument length for a new process and it is set to **2097152 KiB** by default. The Kubelet injects environment variables in to each pod scheduled to run in the namespace including:

- **<SERVICE_NAME>_SERVICE_HOST=<IP>**
- **<SERVICE_NAME>_SERVICE_PORT=<PORT>**
- **<SERVICE_NAME>_PORT=tcp://<IP>:<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP=tcp://<IP>:<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_PROTO=tcp**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_PORT=<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_ADDR=<ADDR>**

The pods in the namespace will start to fail if the argument length exceeds the allowed value and the number of characters in a service name impacts it. For example, in a namespace with 5000 services, the limit on the service name is 33 characters, which enables you to run 5000 pods in the namespace.

CHAPTER 11. OPTIMIZING STORAGE

Optimizing storage helps to minimize storage use across all resources. By optimizing storage, administrators help ensure that existing storage resources are working in an efficient manner.

11.1. AVAILABLE PERSISTENT STORAGE OPTIONS

Understand your persistent storage options so that you can optimize your OpenShift Container Platform environment.

Table 11.1. Available storage options

Storage type	Description	Examples
Block	<ul style="list-style-type: none">● Presented to the operating system (OS) as a block device● Suitable for applications that need full control of storage and operate at a low level on files bypassing the file system● Also referred to as a Storage Area Network (SAN)● Non-shareable, which means that only one client at a time can mount an endpoint of this type	AWS EBS and VMware vSphere support dynamic persistent volume (PV) provisioning natively in OpenShift Container Platform.
File	<ul style="list-style-type: none">● Presented to the OS as a file system export to be mounted● Also referred to as Network Attached Storage (NAS)● Concurrency, latency, file locking mechanisms, and other capabilities vary widely between protocols, implementations, vendors, and scales.	RHEL NFS, NetApp NFS ^[1] , and Vendor NFS
Object	<ul style="list-style-type: none">● Accessible through a REST API endpoint● Configurable for use in the OpenShift Container Platform Registry● Applications must build their drivers into the application and/or container.	AWS S3

1. NetApp NFS supports dynamic PV provisioning when using the Trident plug-in.

**IMPORTANT**

Currently, CNS is not supported in OpenShift Container Platform 4.9.

11.2. RECOMMENDED CONFIGURABLE STORAGE TECHNOLOGY

The following table summarizes the recommended and configurable storage technologies for the given OpenShift Container Platform cluster application.

Table 11.2. Recommended and configurable storage technology

Storage type	ROX ¹	RWX ²	Registry	Scaled registry	Metrics ³	Logging	Apps
Block	Yes ⁴	No	Configurable	Not configurable	Recommended	Recommended	Recommended
File	Yes ⁴	Yes	Configurable	Configurable	Configurable ⁵	Configurable ⁶	Recommended
Object	Yes	Yes	Recommended	Recommended	Not configurable	Not configurable	Not configurable ⁷

¹ **ReadOnlyMany**

² **ReadWriteMany**

³ Prometheus is the underlying technology used for metrics.

⁴ This does not apply to physical disk, VM physical disk, VMDK, loopback over NFS, AWS EBS, and Azure Disk.

⁵ For metrics, using file storage with the **ReadWriteMany** (RWX) access mode is unreliable. If you use file storage, do not configure the RWX access mode on any persistent volume claims (PVCs) that are configured for use with metrics.

⁶ For logging, using any shared storage would be an anti-pattern. One volume per elasticsearch is required.

⁷ Object storage is not consumed through OpenShift Container Platform's PVs or PVCs. Apps must integrate with the object storage REST API.

**NOTE**

A scaled registry is an OpenShift Container Platform registry where two or more pod replicas are running.

11.2.1. Specific application storage recommendations

**IMPORTANT**

Testing shows issues with using the NFS server on Red Hat Enterprise Linux (RHEL) as storage backend for core services. This includes the OpenShift Container Registry and Quay, Prometheus for monitoring storage, and Elasticsearch for logging storage. Therefore, using RHEL NFS to back PVs used by core services is not recommended.

Other NFS implementations on the marketplace might not have these issues. Contact the individual NFS implementation vendor for more information on any testing that was possibly completed against these OpenShift Container Platform core components.

11.2.1.1. Registry

In a non-scaled/high-availability (HA) OpenShift Container Platform registry cluster deployment:

- The storage technology does not have to support RWX access mode.
- The storage technology must ensure read-after-write consistency.
- The preferred storage technology is object storage followed by block storage.
- File storage is not recommended for OpenShift Container Platform registry cluster deployment with production workloads.

11.2.1.2. Scaled registry

In a scaled/HA OpenShift Container Platform registry cluster deployment:

- The storage technology must support RWX access mode.
- The storage technology must ensure read-after-write consistency.
- The preferred storage technology is object storage.
- Amazon Simple Storage Service (Amazon S3), Google Cloud Storage (GCS), Microsoft Azure Blob Storage, and OpenStack Swift are supported.
- Object storage should be S3 or Swift compliant.
- For non-cloud platforms, such as vSphere and bare metal installations, the only configurable technology is file storage.
- Block storage is not configurable.

11.2.1.3. Metrics

In an OpenShift Container Platform hosted metrics cluster deployment:

- The preferred storage technology is block storage.
- Object storage is not configurable.

**IMPORTANT**

It is not recommended to use file storage for a hosted metrics cluster deployment with production workloads.

11.2.1.4. Logging

In an OpenShift Container Platform hosted logging cluster deployment:

- The preferred storage technology is block storage.
- Object storage is not configurable.

11.2.1.5. Applications

Application use cases vary from application to application, as described in the following examples:

- Storage technologies that support dynamic PV provisioning have low mount time latencies, and are not tied to nodes to support a healthy cluster.
- Application developers are responsible for knowing and understanding the storage requirements for their application, and how it works with the provided storage to ensure that issues do not occur when an application scales or interacts with the storage layer.

11.2.2. Other specific application storage recommendations

- OpenShift Container Platform Internal **etcd**: For the best **etcd** reliability, the lowest consistent latency storage technology is preferable.
- It is highly recommended that you use **etcd** with storage that handles serial writes (fsync) quickly, such as NVMe or SSD. Ceph, NFS, and spinning disks are not recommended.
- Red Hat OpenStack Platform (RHOSP) Cinder: RHOSP Cinder tends to be adept in ROX access mode use cases.
- Databases: Databases (RDBMSs, NoSQL DBs, etc.) tend to perform best with dedicated block storage.

11.3. DATA STORAGE MANAGEMENT

The following table summarizes the main directories that OpenShift Container Platform components write data to.

Table 11.3. Main directories for storing OpenShift Container Platform data

Directory	Notes	Sizing	Expected growth
<i>/var/log</i>	Log files for all components.	10 to 30 GB.	Log files can grow quickly; size can be managed by growing disks or by using log rotate.

Directory	Notes	Sizing	Expected growth
<i>/var/lib/etcd</i>	Used for etcd storage when storing the database.	Less than 20 GB. Database can grow up to 8 GB.	Will grow slowly with the environment. Only storing metadata. Additional 20-25 GB for every additional 8 GB of memory.
<i>/var/lib/containers</i>	This is the mount point for the CRI-O runtime. Storage used for active container runtimes, including pods, and storage of local images. Not used for registry storage.	50 GB for a node with 16 GB memory. Note that this sizing should not be used to determine minimum cluster requirements. Additional 20-25 GB for every additional 8 GB of memory.	Growth is limited by capacity for running containers.
<i>/var/lib/kubelet</i>	Ephemeral volume storage for pods. This includes anything external that is mounted into a container at runtime. Includes environment variables, kube secrets, and data volumes not backed by persistent volumes.	Varies	Minimal if pods requiring storage are using persistent volumes. If using ephemeral storage, this can grow quickly.
<i>/var/log</i>	Log files for all components.	10 to 30 GB.	Log files can grow quickly; size can be managed by growing disks or by using log rotate.

CHAPTER 12. OPTIMIZING ROUTING

The OpenShift Container Platform HAProxy router scales to optimize performance.

12.1. BASELINE INGRESS CONTROLLER (ROUTER) PERFORMANCE

The OpenShift Container Platform Ingress Controller, or router, is the Ingress point for all external traffic destined for OpenShift Container Platform services.

When evaluating a single HAProxy router performance in terms of HTTP requests handled per second, the performance varies depending on many factors. In particular:

- HTTP keep-alive/close mode
- Route type
- TLS session resumption client support
- Number of concurrent connections per target route
- Number of target routes
- Back end server page size
- Underlying infrastructure (network/SDN solution, CPU, and so on)

While performance in your specific environment will vary, Red Hat lab tests on a public cloud instance of size 4 vCPU/16GB RAM. A single HAProxy router handling 100 routes terminated by backends serving 1kB static pages is able to handle the following number of transactions per second.

In HTTP keep-alive mode scenarios:

Encryption	LoadBalancerService	HostNetwork
none	21515	29622
edge	16743	22913
passthrough	36786	53295
re-encrypt	21583	25198

In HTTP close (no keep-alive) scenarios:

Encryption	LoadBalancerService	HostNetwork
none	5719	8273
edge	2729	4069
passthrough	4121	5344

Encryption	LoadBalancerService	HostNetwork
re-encrypt	2320	2941

Default Ingress Controller configuration with **ROUTER_THREADS=4** was used and two different endpoint publishing strategies (LoadBalancerService/HostNetwork) were tested. TLS session resumption was used for encrypted routes. With HTTP keep-alive, a single HAProxy router is capable of saturating 1 Gbit NIC at page sizes as small as 8 kB.

When running on bare metal with modern processors, you can expect roughly twice the performance of the public cloud instance above. This overhead is introduced by the virtualization layer in place on public clouds and holds mostly true for private cloud-based virtualization as well. The following table is a guide to how many applications to use behind the router:

Number of applications	Application type
5-10	static file/web server or caching proxy
100-1000	applications generating dynamic content

In general, HAProxy can support routes for 5 to 1000 applications, depending on the technology in use. Ingress Controller performance might be limited by the capabilities and performance of the applications behind it, such as language or static versus dynamic content.

Ingress, or router, sharding should be used to serve more routes towards applications and help horizontally scale the routing tier.

For more information on Ingress sharding, see [Configuring Ingress Controller sharding by using route labels](#) and [Configuring Ingress Controller sharding by using namespace labels](#).

12.2. INGRESS CONTROLLER (ROUTER) PERFORMANCE OPTIMIZATIONS

OpenShift Container Platform no longer supports modifying Ingress Controller deployments by setting environment variables such as **ROUTER_THREADS**, **ROUTER_DEFAULT_TUNNEL_TIMEOUT**, **ROUTER_DEFAULT_CLIENT_TIMEOUT**, **ROUTER_DEFAULT_SERVER_TIMEOUT**, and **RELOAD_INTERVAL**.

You can modify the Ingress Controller deployment, but if the Ingress Operator is enabled, the configuration is overwritten.

CHAPTER 13. OPTIMIZING NETWORKING

The [OpenShift SDN](#) uses OpenvSwitch, virtual extensible LAN (VXLAN) tunnels, OpenFlow rules, and iptables. This network can be tuned by using jumbo frames, network interface controllers (NIC) offloads, multi-queue, and ethtool settings.

[OVN-Kubernetes](#) uses Geneve (Generic Network Virtualization Encapsulation) instead of VXLAN as the tunnel protocol.

VXLAN provides benefits over VLANs, such as an increase in networks from 4096 to over 16 million, and layer 2 connectivity across physical networks. This allows for all pods behind a service to communicate with each other, even if they are running on different systems.

VXLAN encapsulates all tunneled traffic in user datagram protocol (UDP) packets. However, this leads to increased CPU utilization. Both these outer- and inner-packets are subject to normal checksumming rules to guarantee data is not corrupted during transit. Depending on CPU performance, this additional processing overhead can cause a reduction in throughput and increased latency when compared to traditional, non-overlay networks.

Cloud, VM, and bare metal CPU performance can be capable of handling much more than one Gbps network throughput. When using higher bandwidth links such as 10 or 40 Gbps, reduced performance can occur. This is a known issue in VXLAN-based environments and is not specific to containers or OpenShift Container Platform. Any network that relies on VXLAN tunnels will perform similarly because of the VXLAN implementation.

If you are looking to push beyond one Gbps, you can:

- Evaluate network plug-ins that implement different routing techniques, such as border gateway protocol (BGP).
- Use VXLAN-offload capable network adapters. VXLAN-offload moves the packet checksum calculation and associated CPU overhead off of the system CPU and onto dedicated hardware on the network adapter. This frees up CPU cycles for use by pods and applications, and allows users to utilize the full bandwidth of their network infrastructure.

VXLAN-offload does not reduce latency. However, CPU utilization is reduced even in latency tests.

13.1. OPTIMIZING THE MTU FOR YOUR NETWORK

There are two important maximum transmission units (MTUs): the network interface controller (NIC) MTU and the cluster network MTU.

The NIC MTU is only configured at the time of OpenShift Container Platform installation. The MTU must be less than or equal to the maximum supported value of the NIC of your network. If you are optimizing for throughput, choose the largest possible value. If you are optimizing for lowest latency, choose a lower value.

The SDN overlay's MTU must be less than the NIC MTU by 50 bytes at a minimum. This accounts for the SDN overlay header. So, on a normal ethernet network, set this to **1450**. On a jumbo frame ethernet network, set this to **8950**.

For OVN and Geneve, the MTU must be less than the NIC MTU by 100 bytes at a minimum.

**NOTE**

This 50 byte overlay header is relevant to the OpenShift SDN. Other SDN solutions might require the value to be more or less.

13.2. RECOMMENDED PRACTICES FOR INSTALLING LARGE SCALE CLUSTERS

When installing large clusters or scaling the cluster to larger node counts, set the cluster network **cidr** accordingly in your **install-config.yaml** file before you install the cluster:

```
networking:
  clusterNetwork:
    - cidr: 10.128.0.0/14
      hostPrefix: 23
  machineNetwork:
    - cidr: 10.0.0.0/16
  networkType: OpenShiftSDN
  serviceNetwork:
    - 172.30.0.0/16
```

The default cluster network **cidr 10.128.0.0/14** cannot be used if the cluster size is more than 500 nodes. It must be set to **10.128.0.0/12** or **10.128.0.0/10** to get to larger node counts beyond 500 nodes.

13.3. IMPACT OF IPSEC

Because encrypting and decrypting node hosts uses CPU power, performance is affected both in throughput and CPU usage on the nodes when encryption is enabled, regardless of the IP security system being used.

IPSec encrypts traffic at the IP payload level, before it hits the NIC, protecting fields that would otherwise be used for NIC offloading. This means that some NIC acceleration features might not be usable when IPSec is enabled and will lead to decreased throughput and increased CPU usage.

Additional resources

- [Modifying advanced network configuration parameters](#)
- [Configuration parameters for the OVN-Kubernetes default CNI network provider](#)
- [Configuration parameters for the OpenShift SDN default CNI network provider](#)

CHAPTER 14. MANAGING BARE METAL HOSTS

When you install OpenShift Container Platform on a bare metal cluster, you can provision and manage bare metal nodes using **machine** and **machineset** custom resources (CRs) for bare metal hosts that exist in the cluster.

14.1. ABOUT BARE METAL HOSTS AND NODES

To provision a Red Hat Enterprise Linux CoreOS (RHCOS) bare metal host as a node in your cluster, first create a **MachineSet** custom resource (CR) object that corresponds to the bare metal host hardware. Bare metal host machine sets describe infrastructure components specific to your configuration. You apply specific Kubernetes labels to these machine sets and then update the infrastructure components to run on only those machines.

Machine CR's are created automatically when you scale up the relevant **MachineSet** containing a **metal3.io/autoscale-to-hosts** annotation. OpenShift Container Platform uses **Machine** CR's to provision the bare metal node that corresponds to the host as specified in the **MachineSet** CR.

14.2. MAINTAINING BARE METAL HOSTS

You can maintain the details of the bare metal hosts in your cluster from the OpenShift Container Platform web console. Navigate to **Compute → Bare Metal Hosts**, and select a task from the **Actions** drop down menu. Here you can manage items such as BMC details, boot MAC address for the host, enable power management, and so on. You can also review the details of the network interfaces and drives for the host.

You can move a bare metal host into maintenance mode. When you move a host into maintenance mode, the scheduler moves all managed workloads off the corresponding bare metal node. No new workloads are scheduled while in maintenance mode.

You can deprovision a bare metal host in the web console. Deprovisioning a host does the following actions:

1. Annotates the bare metal host CR with **cluster.k8s.io/delete-machine: true**
2. Scales down the related machine set



NOTE

Powering off the host without first moving the daemon set and unmanaged static pods to another node can cause service disruption and loss of data.

Additional Resources

- [Adding compute machines to bare metal](#)

14.2.1. Adding a bare metal host to the cluster using the web console

You can add bare metal hosts to the cluster in the web console.

Prerequisites

- Install an RHCOS cluster on bare metal.

- Log in as a user with **cluster-admin** privileges.

Procedure

1. In the web console, navigate to **Compute → Bare Metal Hosts**.
2. Select **Add Host → New with Dialog**.
3. Specify a unique name for the new bare metal host.
4. Set the **Boot MAC address**.
5. Set the **Baseboard Management Console (BMC) Address**.
6. Optional: Enable power management for the host. This allows OpenShift Container Platform to control the power state of the host.
7. Enter the user credentials for the host's baseboard management controller (BMC).
8. Select to power on the host after creation, and select **Create**.
9. Scale up the number of replicas to match the number of available bare metal hosts. Navigate to **Compute → MachineSets**, and increase the number of machine replicas in the cluster by selecting **Edit Machine count** from the **Actions** drop-down menu.



NOTE

You can also manage the number of bare metal nodes using the **oc scale** command and the appropriate bare metal machine set.

14.2.2. Adding a bare metal host to the cluster using YAML in the web console

You can add bare metal hosts to the cluster in the web console using a YAML file that describes the bare metal host.

Prerequisites

- Install a RHCOS compute machine on bare metal infrastructure for use in the cluster.
- Log in as a user with **cluster-admin** privileges.
- Create a **Secret** CR for the bare metal host.

Procedure

1. In the web console, navigate to **Compute → Bare Metal Hosts**.
2. Select **Add Host → New from YAML**.
3. Copy and paste the below YAML, modifying the relevant fields with the details of your host:

```
apiVersion: metal3.io/v1alpha1
kind: BareMetalHost
metadata:
  name: <bare_metal_host_name>
```

```
spec:
  online: true
  bmc:
    address: <bmc_address>
    credentialsName: <secret_credentials_name>
    disableCertificateVerification: True
  bootMACAddress: <host_boot_mac_address>
  hardwareProfile: unknown
```

- 1** **credentialsName** must reference a valid **Secret** CR. The **baremetal-operator** cannot manage the bare metal host without a valid **Secret** referenced in the **credentialsName**. For more information about secrets and how to create them, see [Understanding secrets](#).

4. Select **Create** to save the YAML and create the new bare metal host.
5. Scale up the number of replicas to match the number of available bare metal hosts. Navigate to **Compute** → **MachineSets**, and increase the number of machines in the cluster by selecting **Edit Machine count** from the **Actions** drop-down menu.



NOTE

You can also manage the number of bare metal nodes using the **oc scale** command and the appropriate bare metal machine set.

14.2.3. Automatically scaling machines to the number of available bare metal hosts

To automatically create the number of **Machine** objects that matches the number of available **BareMetalHost** objects, add a **metal3.io/autoscale-to-hosts** annotation to the **MachineSet** object.

Prerequisites

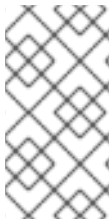
- Install RHCOS bare metal compute machines for use in the cluster, and create corresponding **BareMetalHost** objects.
- Install the OpenShift Container Platform CLI (**oc**).
- Log in as a user with **cluster-admin** privileges.

Procedure

1. Annotate the machine set that you want to configure for automatic scaling by adding the **metal3.io/autoscale-to-hosts** annotation. Replace **<machineset>** with the name of the machine set.

```
$ oc annotate machineset <machineset> -n openshift-machine-api 'metal3.io/autoscale-to-hosts=<any_value>'
```

Wait for the new scaled machines to start.



NOTE

When you use a **BareMetalHost** object to create a machine in the cluster and labels or selectors are subsequently changed on the **BareMetalHost**, the **BareMetalHost** object continues to be counted against the **MachineSet** that the **Machine** object was created from.

Additional resources

- [Expanding the cluster](#)
- [MachineHealthChecks on bare metal](#)

CHAPTER 15. WHAT HUGE PAGES DO AND HOW THEY ARE CONSUMED BY APPLICATIONS

15.1. WHAT HUGE PAGES DO

Memory is managed in blocks known as pages. On most systems, a page is 4Ki. 1Mi of memory is equal to 256 pages; 1Gi of memory is 256,000 pages, and so on. CPUs have a built-in memory management unit that manages a list of these pages in hardware. The Translation Lookaside Buffer (TLB) is a small hardware cache of virtual-to-physical page mappings. If the virtual address passed in a hardware instruction can be found in the TLB, the mapping can be determined quickly. If not, a TLB miss occurs, and the system falls back to slower, software-based address translation, resulting in performance issues. Since the size of the TLB is fixed, the only way to reduce the chance of a TLB miss is to increase the page size.

A huge page is a memory page that is larger than 4Ki. On x86_64 architectures, there are two common huge page sizes: 2Mi and 1Gi. Sizes vary on other architectures. To use huge pages, code must be written so that applications are aware of them. Transparent Huge Pages (THP) attempt to automate the management of huge pages without application knowledge, but they have limitations. In particular, they are limited to 2Mi page sizes. THP can lead to performance degradation on nodes with high memory utilization or fragmentation due to defragmenting efforts of THP, which can lock memory pages. For this reason, some applications may be designed to (or recommend) usage of pre-allocated huge pages instead of THP.

In OpenShift Container Platform, applications in a pod can allocate and consume pre-allocated huge pages.

15.2. HOW HUGE PAGES ARE CONSUMED BY APPS

Nodes must pre-allocate huge pages in order for the node to report its huge page capacity. A node can only pre-allocate huge pages for a single size.

Huge pages can be consumed through container-level resource requirements using the resource name **hugepages-<size>**, where size is the most compact binary notation using integer values supported on a particular node. For example, if a node supports 2048KiB page sizes, it exposes a schedulable resource **hugepages-2Mi**. Unlike CPU or memory, huge pages do not support over-commitment.

```
apiVersion: v1
kind: Pod
metadata:
  generateName: hugepages-volume-
spec:
  containers:
  - securityContext:
    privileged: true
    image: rhel7:latest
    command:
    - sleep
    - inf
    name: example
    volumeMounts:
    - mountPath: /dev/hugepages
      name: hugepage
  resources:
    limits:
```

```

hugepages-2Mi: 100Mi 1
memory: "1Gi"
cpu: "1"
volumes:
- name: hugepage
  emptyDir:
    medium: HugePages

```

- 1 Specify the amount of memory for **hugepages** as the exact amount to be allocated. Do not specify this value as the amount of memory for **hugepages** multiplied by the size of the page. For example, given a huge page size of 2MB, if you want to use 100MB of huge-page-backed RAM for your application, then you would allocate 50 huge pages. OpenShift Container Platform handles the math for you. As in the above example, you can specify **100MB** directly.

Allocating huge pages of a specific size

Some platforms support multiple huge page sizes. To allocate huge pages of a specific size, precede the huge pages boot command parameters with a huge page size selection parameter **hugepagesz=<size>**. The **<size>** value must be specified in bytes with an optional scale suffix [**kKmMgG**]. The default huge page size can be defined with the **default_hugepagesz=<size>** boot parameter.

Huge page requirements

- Huge page requests must equal the limits. This is the default if limits are specified, but requests are not.
- Huge pages are isolated at a pod scope. Container isolation is planned in a future iteration.
- **EmptyDir** volumes backed by huge pages must not consume more huge page memory than the pod request.
- Applications that consume huge pages via **shmget()** with **SHM_HUGETLB** must run with a supplemental group that matches *proc/sys/vm/hugetlb_shm_group*.

Additional resources

- [Configuring Transparent Huge Pages](#)

15.3. CONSUMING HUGE PAGES RESOURCES USING THE DOWNWARD API

You can use the Downward API to inject information about the huge pages resources that are consumed by a container.

You can inject the resource allocation as environment variables, a volume plug-in, or both. Applications that you develop and run in the container can determine the resources that are available by reading the environment variables or files in the specified volumes.

Procedure

1. Create a **hugepages-volume-pod.yaml** file that is similar to the following example:

```

apiVersion: v1
kind: Pod

```

```

metadata:
  generateName: hugepages-volume-
  labels:
    app: hugepages-example
spec:
  containers:
  - securityContext:
      capabilities:
        add: [ "IPC_LOCK" ]
    image: rhel7:latest
    command:
      - sleep
      - inf
    name: example
    volumeMounts:
      - mountPath: /dev/hugepages
        name: hugepage
      - mountPath: /etc/podinfo
        name: podinfo
    resources:
      limits:
        hugepages-1Gi: 2Gi
        memory: "1Gi"
        cpu: "1"
      requests:
        hugepages-1Gi: 2Gi
    env:
      - name: REQUESTS_HUGEPAGES_1Gi <.>
        valueFrom:
          resourceFieldRef:
            containerName: example
            resource: requests.hugepages-1Gi
  volumes:
  - name: hugepage
    emptyDir:
      medium: HugePages
  - name: podinfo
  downwardAPI:
    items:
      - path: "hugepages_1G_request" <.>
        resourceFieldRef:
          containerName: example
          resource: requests.hugepages-1Gi
        divisor: 1Gi

```

<.> Specifies to read the resource use from **requests.hugepages-1Gi** and expose the value as the **REQUESTS_HUGEPAGES_1GI** environment variable. <.> Specifies to read the resource use from **requests.hugepages-1Gi** and expose the value as the file **/etc/podinfo/hugepages_1G_request**.

2. Create the pod from the **hugepages-volume-pod.yaml** file:

```
$ oc create -f hugepages-volume-pod.yaml
```

Verification

1. Check the value of the **REQUESTS_HUGEPAGES_1GI** environment variable:

```
$ oc exec -it $(oc get pods -l app=hugepages-example -o
jsonpath='{.items[0].metadata.name}') \
-- env | grep REQUESTS_HUGEPAGES_1GI
```

Example output

```
REQUESTS_HUGEPAGES_1GI=2147483648
```

2. Check the value of the **/etc/podinfo/hugepages_1G_request** file:

```
$ oc exec -it $(oc get pods -l app=hugepages-example -o
jsonpath='{.items[0].metadata.name}') \
-- cat /etc/podinfo/hugepages_1G_request
```

Example output

```
2
```

Additional resources

- [Allowing containers to consume Downward API objects](#)

15.4. CONFIGURING HUGE PAGES

Nodes must pre-allocate huge pages used in an OpenShift Container Platform cluster. There are two ways of reserving huge pages: at boot time and at run time. Reserving at boot time increases the possibility of success because the memory has not yet been significantly fragmented. The Node Tuning Operator currently supports boot time allocation of huge pages on specific nodes.

15.4.1. At boot time

Procedure

To minimize node reboots, the order of the steps below needs to be followed:

1. Label all nodes that need the same huge pages setting by a label.

```
$ oc label node <node_using_hugepages> node-role.kubernetes.io/worker-hp=
```

2. Create a file with the following content and name it **hugepages-tuned-boottime.yaml**:

```
apiVersion: tuned.openshift.io/v1
kind: Tuned
metadata:
  name: hugepages 1
  namespace: openshift-cluster-node-tuning-operator
spec:
  profile: 2
  - data: |
    [main]
```



```
summary=Boot time configuration for hugepages
include=openshift-node
[bootloader]
cmdline_openshift_node_hugepages=hugepagesz=2M hugepages=50 3
name: openshift-node-hugepages

recommend:
- machineConfigLabels: 4
  machineconfiguration.openshift.io/role: "worker-hp"
  priority: 30
  profile: openshift-node-hugepages
```

- 1 Set the **name** of the Tuned resource to **hugepages**.
- 2 Set the **profile** section to allocate huge pages.
- 3 Note the order of parameters is important as some platforms support huge pages of various sizes.
- 4 Enable machine config pool based matching.

3. Create the Tuned **hugepages** object

```
$ oc create -f hugepages-tuned-boottime.yaml
```

4. Create a file with the following content and name it **hugepages-mcp.yaml**:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
metadata:
  name: worker-hp
  labels:
    worker-hp: ""
spec:
  machineConfigSelector:
    matchExpressions:
      - {key: machineconfiguration.openshift.io/role, operator: In, values: [worker,worker-hp]}
  nodeSelector:
    matchLabels:
      node-role.kubernetes.io/worker-hp: ""
```

5. Create the machine config pool:

```
$ oc create -f hugepages-mcp.yaml
```

Given enough non-fragmented memory, all the nodes in the **worker-hp** machine config pool should now have 50 2Mi huge pages allocated.

```
$ oc get node <node_using_hugepages> -o jsonpath="{.status.allocatable.hugepages-2Mi}"
100Mi
```

**WARNING**

This functionality is currently only supported on Red Hat Enterprise Linux CoreOS (RHCOS) 8.x worker nodes. On Red Hat Enterprise Linux (RHEL) 7.x worker nodes the TunedD **[bootloader]** plug-in is currently not supported.

CHAPTER 16. PERFORMANCE ADDON OPERATOR FOR LOW LATENCY NODES

16.1. UNDERSTANDING LOW LATENCY

The emergence of Edge computing in the area of Telco / 5G plays a key role in reducing latency and congestion problems and improving application performance.

Simply put, latency determines how fast data (packets) moves from the sender to receiver and returns to the sender after processing by the receiver. Obviously, maintaining a network architecture with the lowest possible delay of latency speeds is key for meeting the network performance requirements of 5G. Compared to 4G technology, with an average latency of 50ms, 5G is targeted to reach latency numbers of 1ms or less. This reduction in latency boosts wireless throughput by a factor of 10.

Many of the deployed applications in the Telco space require low latency that can only tolerate zero packet loss. Tuning for zero packet loss helps mitigate the inherent issues that degrade network performance. For more information, see [Tuning for Zero Packet Loss in Red Hat OpenStack Platform \(RHOSP\)](#).

The Edge computing initiative also comes in to play for reducing latency rates. Think of it as literally being on the edge of the cloud and closer to the user. This greatly reduces the distance between the user and distant data centers, resulting in reduced application response times and performance latency.

Administrators must be able to manage their many Edge sites and local services in a centralized way so that all of the deployments can run at the lowest possible management cost. They also need an easy way to deploy and configure certain nodes of their cluster for real-time low latency and high-performance purposes. Low latency nodes are useful for applications such as Cloud-native Network Functions (CNF) and Data Plane Development Kit (DPDK).

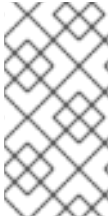
OpenShift Container Platform currently provides mechanisms to tune software on an OpenShift Container Platform cluster for real-time running and low latency (around <20 microseconds reaction time). This includes tuning the kernel and OpenShift Container Platform set values, installing a kernel, and reconfiguring the machine. But this method requires setting up four different Operators and performing many configurations that, when done manually, is complex and could be prone to mistakes.

OpenShift Container Platform provides a Performance Addon Operator to implement automatic tuning to achieve low latency performance for OpenShift applications. The cluster administrator uses this performance profile configuration that makes it easier to make these changes in a more reliable way. The administrator can specify whether to update the kernel to kernel-rt, reserve CPUs for cluster and operating system housekeeping duties, including pod infra containers, and isolate CPUs for application containers to run the workloads.

16.1.1. About hyperthreading for low latency and real-time applications

Hyperthreading is an Intel processor technology that allows a physical CPU processor core to function as two logical cores, executing two independent threads simultaneously. Hyperthreading allows for better system throughput for certain workload types where parallel processing is beneficial. The default OpenShift Container Platform configuration expects hyperthreading to be enabled by default.

For telecommunications applications, it is important to design your application infrastructure to minimize latency as much as possible. Hyperthreading can slow performance times and negatively affect throughput for compute intensive workloads that require low latency. Disabling hyperthreading ensures predictable performance and can decrease processing times for these workloads.

**NOTE**

Hyperthreading implementation and configuration differs depending on the hardware you are running OpenShift Container Platform on. Consult the relevant host hardware tuning information for more details of the hyperthreading implementation specific to that hardware. Disabling hyperthreading can increase the cost per core of the cluster.

Additional resources

- [Configuring hyperthreading for a cluster](#)

16.2. INSTALLING THE PERFORMANCE ADDON OPERATOR

Performance Addon Operator provides the ability to enable advanced node performance tunings on a set of nodes. As a cluster administrator, you can install Performance Addon Operator using the OpenShift Container Platform CLI or the web console.

16.2.1. Installing the Operator using the CLI

As a cluster administrator, you can install the Operator using the CLI.

Prerequisites

- A cluster installed on bare-metal hardware.
- Install the OpenShift CLI (**oc**).
- Log in as a user with **cluster-admin** privileges.

Procedure

1. Create a namespace for the Performance Addon Operator by completing the following actions:
 - a. Create the following Namespace Custom Resource (CR) that defines the **openshift-performance-addon-operator** namespace, and then save the YAML in the **pao-namespace.yaml** file:

```
apiVersion: v1
kind: Namespace
metadata:
  name: openshift-performance-addon-operator
  annotations:
    workload.openshift.io/allowed: management
```

- b. Create the namespace by running the following command:

```
$ oc create -f pao-namespace.yaml
```

2. Install the Performance Addon Operator in the namespace you created in the previous step by creating the following objects:
 - a. Create the following **OperatorGroup** CR and save the YAML in the **pao-operatorgroup.yaml** file:

```
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: openshift-performance-addon-operator
  namespace: openshift-performance-addon-operator
```

- b. Create the **OperatorGroup** CR by running the following command:

```
$ oc create -f pao-operatorgroup.yaml
```

- c. Run the following command to get the **channel** value required for the next step.

```
$ oc get packagemanifest performance-addon-operator -n openshift-marketplace -o
jsonpath='{.status.defaultChannel}'
```

Example output

```
4.9
```

- d. Create the following Subscription CR and save the YAML in the **pao-sub.yaml** file:

Example Subscription

```
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: openshift-performance-addon-operator-subscription
  namespace: openshift-performance-addon-operator
spec:
  channel: "<channel>" ❶
  name: performance-addon-operator
  source: redhat-operators ❷
  sourceNamespace: openshift-marketplace
```

- ❶ Specify the value from you obtained in the previous step for the **.status.defaultChannel** parameter.

- ❷ You must specify the **redhat-operators** value.

- e. Create the Subscription object by running the following command:

```
$ oc create -f pao-sub.yaml
```

- f. Change to the **openshift-performance-addon-operator** project:

```
$ oc project openshift-performance-addon-operator
```

16.2.2. Installing the Performance Addon Operator using the web console

As a cluster administrator, you can install the Performance Addon Operator using the web console.

**NOTE**

You must create the **Namespace** CR and **OperatorGroup** CR as mentioned in the previous section.

Procedure

1. Install the Performance Addon Operator using the OpenShift Container Platform web console:
 - a. In the OpenShift Container Platform web console, click **Operators** → **OperatorHub**.
 - b. Choose **Performance Addon Operator** from the list of available Operators, and then click **Install**.
 - c. On the **Install Operator** page, select **All namespaces on the cluster**. Then, click **Install**.
2. Optional: Verify that the performance-addon-operator installed successfully:
 - a. Switch to the **Operators** → **Installed Operators** page.
 - b. Ensure that **Performance Addon Operator** is listed in the **openshift-performance-addon-operator** project with a **Status** of **InstallSucceeded**.

**NOTE**

During installation an Operator might display a **Failed** status. If the installation later succeeds with an **InstallSucceeded** message, you can ignore the **Failed** message.

If the Operator does not appear as installed, to troubleshoot further:

- Go to the **Operators** → **Installed Operators** page and inspect the **Operator Subscriptions** and **Install Plans** tabs for any failure or errors under **Status**.
- Go to the **Workloads** → **Pods** page and check the logs for pods in the **performance-addon-operator** project.

16.3. UPGRADING PERFORMANCE ADDON OPERATOR

You can manually upgrade to the next minor version of Performance Addon Operator and monitor the status of an update by using the web console.

16.3.1. About upgrading Performance Addon Operator

- You can upgrade to the next minor version of Performance Addon Operator by using the OpenShift Container Platform web console to change the channel of your Operator subscription.
- You can enable automatic z-stream updates during Performance Addon Operator installation.
- Updates are delivered via the Marketplace Operator, which is deployed during OpenShift Container Platform installation. The Marketplace Operator makes external Operators available to your cluster.

- The amount of time an update takes to complete depends on your network connection. Most automatic updates complete within fifteen minutes.

16.3.1.1. How Performance Addon Operator upgrades affect your cluster

- Neither the low latency tuning nor huge pages are affected.
- Updating the Operator should not cause any unexpected reboots.

16.3.1.2. Upgrading Performance Addon Operator to the next minor version

You can manually upgrade Performance Addon Operator to the next minor version by using the OpenShift Container Platform web console to change the channel of your Operator subscription.

Prerequisites

- Access to the cluster as a user with the cluster-admin role.

Procedure

1. Access the web console and navigate to **Operators → Installed Operators**.
2. Click **Performance Addon Operator** to open the **Operator details** page.
3. Click the **Subscription** tab to open the **Subscription details** page.
4. In the **Update channel** pane, click the pencil icon on the right side of the version number to open the **Change Subscription update channel** window.
5. Select the next minor version. For example, if you want to upgrade to Performance Addon Operator 4.9, select **4.9**.
6. Click **Save**.
7. Check the status of the upgrade by navigating to **Operators → Installed Operators**. You can also check the status by running the following **oc** command:

```
$ oc get csv -n openshift-performance-addon-operator
```

16.3.1.3. Upgrading Performance Addon Operator when previously installed to a specific namespace

If you previously installed the Performance Addon Operator to a specific namespace on the cluster, for example **openshift-performance-addon-operator**, modify the **OperatorGroup** object to remove the **targetNamespaces** entry before upgrading.

Prerequisites

- Install the OpenShift Container Platform CLI (oc).
- Log in to the OpenShift cluster as a user with cluster-admin privileges.

Procedure

1. Edit the Performance Addon Operator **OperatorGroup** CR and remove the **spec** element that contains the **targetNamespaces** entry by running the following command:

```
$ oc patch operatorgroup -n openshift-performance-addon-operator openshift-performance-addon-operator --type json -p '[{"op": "remove", "path": "/spec"}]'
```

2. Wait until the Operator Lifecycle Manager (OLM) processes the change.
3. Verify that the OperatorGroup CR change has been successfully applied. Check that the **OperatorGroup** CR **spec** element has been removed:

```
$ oc describe -n openshift-performance-addon-operator og openshift-performance-addon-operator
```

4. Proceed with the Performance Addon Operator upgrade.

16.3.2. Monitoring upgrade status

The best way to monitor Performance Addon Operator upgrade status is to watch the **ClusterServiceVersion** (CSV) **PHASE**. You can also monitor the CSV conditions in the web console or by running the **oc get csv** command.



NOTE

The **PHASE** and conditions values are approximations that are based on available information.

Prerequisites

- Access to the cluster as a user with the **cluster-admin** role.
- Install the OpenShift CLI (**oc**).

Procedure

1. Run the following command:

```
$ oc get csv
```

2. Review the output, checking the **PHASE** field. For example:

VERSION	REPLACES	PHASE
4.9.0	performance-addon-operator.v4.9.0	Installing
4.8.0		Replacing

3. Run **get csv** again to verify the output:

```
# oc get csv
```

Example output

NAME	DISPLAY	VERSION	REPLACES
PHASE			

performance-addon-operator.v4.9.0 Performance Addon Operator 4.9.0 performance-addon-operator.v4.8.0 Succeeded

16.4. PROVISIONING REAL-TIME AND LOW LATENCY WORKLOADS

Many industries and organizations need extremely high performance computing and might require low and predictable latency, especially in the financial and telecommunications industries. For these industries, with their unique requirements, OpenShift Container Platform provides a Performance Addon Operator to implement automatic tuning to achieve low latency performance and consistent response time for OpenShift Container Platform applications.

The cluster administrator can use this performance profile configuration to make these changes in a more reliable way. The administrator can specify whether to update the kernel to kernel-rt (real-time), reserve CPUs for cluster and operating system housekeeping duties, including pod infra containers, and isolate CPUs for application containers to run the workloads.



WARNING

The usage of execution probes in conjunction with applications that require guaranteed CPUs can cause latency spikes. It is recommended to use other probes, such as a properly configured set of network probes, as an alternative.

16.4.1. Known limitations for real-time



NOTE

In most deployments, kernel-rt is supported only on worker nodes when you use a standard cluster with three control plane nodes and three worker nodes. There are exceptions for compact and single nodes on OpenShift Container Platform deployments. For installations on a single node, kernel-rt is supported on the single control plane node.

To fully utilize the real-time mode, the containers must run with elevated privileges. See [Set capabilities for a Container](#) for information on granting privileges.

OpenShift Container Platform restricts the allowed capabilities, so you might need to create a **SecurityContext** as well.



NOTE

This procedure is fully supported with bare metal installations using Red Hat Enterprise Linux CoreOS (RHCOS) systems.

Establishing the right performance expectations refers to the fact that the real-time kernel is not a panacea. Its objective is consistent, low-latency determinism offering predictable response times. There is some additional kernel overhead associated with the real-time kernel. This is due primarily to handling hardware interruptions in separately scheduled threads. The increased overhead in some workloads results in some degradation in overall throughput. The exact amount of degradation is very workload dependent, ranging from 0% to 30%. However, it is the cost of determinism.

16.4.2. Provisioning a worker with real-time capabilities

1. Install Performance Addon Operator to the cluster.
2. Optional: Add a node to the OpenShift Container Platform cluster. See [Setting BIOS parameters](#).
3. Add the label **worker-rt** to the worker nodes that require the real-time capability by using the **oc** command.
4. Create a new machine config pool for real-time nodes:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
metadata:
  name: worker-rt
labels:
  machineconfiguration.openshift.io/role: worker-rt
spec:
  machineConfigSelector:
    matchExpressions:
      - {
        key: machineconfiguration.openshift.io/role,
        operator: In,
        values: [worker, worker-rt],
      }
  paused: false
  nodeSelector:
    matchLabels:
      node-role.kubernetes.io/worker-rt: ""
```

Note that a machine config pool **worker-rt** is created for group of nodes that have the label **worker-rt**.

5. Add the node to the proper machine config pool by using node role labels.



NOTE

You must decide which nodes are configured with real-time workloads. You could configure all of the nodes in the cluster, or a subset of the nodes. The Performance Addon Operator expects all of the nodes are part of a dedicated machine config pool. If you use all of the nodes, you must point the Performance Addon Operator to the worker node role label. If you use a subset, you must group the nodes into a new machine config pool.

6. Create the **PerformanceProfile** with the proper set of housekeeping cores and **realTimeKernel: enabled: true**.
7. You must set **machineConfigPoolSelector** in **PerformanceProfile**:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: example-performanceprofile
spec:
```

```
...
realTimeKernel:
  enabled: true
nodeSelector:
  node-role.kubernetes.io/worker-rt: ""
machineConfigPoolSelector:
  machineconfiguration.openshift.io/role: worker-rt
```

8. Verify that a matching machine config pool exists with a label:

```
$ oc describe mcp/worker-rt
```

Example output

```
Name:      worker-rt
Namespace:
Labels:    machineconfiguration.openshift.io/role=worker-rt
```

9. OpenShift Container Platform will start configuring the nodes, which might involve multiple reboots. Wait for the nodes to settle. This can take a long time depending on the specific hardware you use, but 20 minutes per node is expected.
10. Verify everything is working as expected.

16.4.3. Verifying the real-time kernel installation

Use this command to verify that the real-time kernel is installed:

```
$ oc get node -o wide
```

Note the worker with the role **worker-rt** that contains the string **4.18.0-211.rt5.23.el8.x86_64**:

NAME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP
EXTERNAL-IP	OS-IMAGE			KERNEL-VERSION	
CONTAINER-RUNTIME					
rt-worker-0.example.com	Ready	worker,worker-rt	5d17h	v1.22.1	
128.66.135.107	<none>	Red Hat Enterprise Linux CoreOS	46.82.202008252340-0	(Ootpa)	
4.18.0-211.rt5.23.el8.x86_64	cri-o://1.22.1-90.rhaos4.9.git4a0ac05.el8-rc.1				
[...]					

16.4.4. Creating a workload that works in real-time

Use the following procedures for preparing a workload that will use real-time capabilities.

Procedure

1. Create a pod with a QoS class of **Guaranteed**.
2. Optional: Disable CPU load balancing for DPDK.
3. Assign a proper node selector.

When writing your applications, follow the general recommendations described in [Application tuning and deployment](#).

16.4.5. Creating a pod with a QoS class of **Guaranteed**

Keep the following in mind when you create a pod that is given a QoS class of **Guaranteed**:

- Every container in the pod must have a memory limit and a memory request, and they must be the same.
- Every container in the pod must have a CPU limit and a CPU request, and they must be the same.

The following example shows the configuration file for a pod that has one container. The container has a memory limit and a memory request, both equal to 200 MiB. The container has a CPU limit and a CPU request, both equal to 1 CPU.

```
apiVersion: v1
kind: Pod
metadata:
  name: qos-demo
  namespace: qos-example
spec:
  containers:
  - name: qos-demo-ctr
    image: <image-pull-spec>
    resources:
      limits:
        memory: "200Mi"
        cpu: "1"
      requests:
        memory: "200Mi"
        cpu: "1"
```

1. Create the pod:

```
$ oc apply -f qos-pod.yaml --namespace=qos-example
```

2. View detailed information about the pod:

```
$ oc get pod qos-demo --namespace=qos-example --output=yaml
```

Example output

```
spec:
  containers:
  ...
status:
  qosClass: Guaranteed
```

**NOTE**

If a container specifies its own memory limit, but does not specify a memory request, OpenShift Container Platform automatically assigns a memory request that matches the limit. Similarly, if a container specifies its own CPU limit, but does not specify a CPU request, OpenShift Container Platform automatically assigns a CPU request that matches the limit.

16.4.6. Optional: Disabling CPU load balancing for DPDK

Functionality to disable or enable CPU load balancing is implemented on the CRI-O level. The code under the CRI-O disables or enables CPU load balancing only when the following requirements are met.

- The pod must use the **performance-<profile-name>** runtime class. You can get the proper name by looking at the status of the performance profile, as shown here:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
...
status:
...
runtimeClass: performance-manual
```

- The pod must have the **cpu-load-balancing.crio.io: true** annotation.

The Performance Addon Operator is responsible for the creation of the high-performance runtime handler config snippet under relevant nodes and for creation of the high-performance runtime class under the cluster. It will have the same content as default runtime handler except it enables the CPU load balancing configuration functionality.

To disable the CPU load balancing for the pod, the **Pod** specification must include the following fields:

```
apiVersion: v1
kind: Pod
metadata:
...
annotations:
...
  cpu-load-balancing.crio.io: "disable"
...
spec:
...
  runtimeClassName: performance-<profile_name>
...
```

**NOTE**

Only disable CPU load balancing when the CPU manager static policy is enabled and for pods with guaranteed QoS that use whole CPUs. Otherwise, disabling CPU load balancing can affect the performance of other containers in the cluster.

16.4.7. Assigning a proper node selector

The preferred way to assign a pod to nodes is to use the same node selector the performance profile used, as shown here:

```
apiVersion: v1
kind: Pod
metadata:
  name: example
spec:
  # ...
  nodeSelector:
    node-role.kubernetes.io/worker-rt: ""
```

For more information, see [Placing pods on specific nodes using node selectors](#).

16.4.8. Scheduling a workload onto a worker with real-time capabilities

Use label selectors that match the nodes attached to the machine config pool that was configured for low latency by the Performance Addon Operator. For more information, see [Assigning pods to nodes](#).

16.4.9. Managing device interrupt processing for guaranteed pod isolated CPUs

The Performance Addon Operator can manage host CPUs by dividing them into reserved CPUs for cluster and operating system housekeeping duties, including pod infra containers, and isolated CPUs for application containers to run the workloads. This allows you to set CPUs for low latency workloads as isolated.

Device interrupts are load balanced between all isolated and reserved CPUs to avoid CPUs being overloaded, with the exception of CPUs where there is a guaranteed pod running. Guaranteed pod CPUs are prevented from processing device interrupts when the relevant annotations are set for the pod.

In the performance profile, **globallyDisableIrqLoadBalancing** is used to manage whether device interrupts are processed or not. For certain workloads the reserved CPUs are not always sufficient for dealing with device interrupts, and for this reason, device interrupts are not globally disabled on the isolated CPUs. By default, Performance Addon Operator does not disable device interrupts on isolated CPUs.

To achieve low latency for workloads, some (but not all) pods require the CPUs they are running on to not process device interrupts. A pod annotation, **irq-load-balancing.crio.io**, is used to define whether device interrupts are processed or not. When configured, CRI-O disables device interrupts only as long as the pod is running.

16.4.9.1. Disabling global device interrupts handling in Performance Addon Operator

To configure Performance Addon Operator to disable global device interrupts for the isolated CPU set, set the **globallyDisableIrqLoadBalancing** field in the performance profile to **true**. When **true**, conflicting pod annotations are ignored. When **false**, IRQ loads are balanced across all CPUs.

A performance profile snippet illustrates this setting:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: manual
```

```
spec:
  globallyDisableIrqLoadBalancing: true
...
```

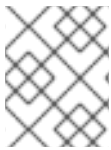
16.4.9.2. Disabling interrupt processing for individual pods

To disable interrupt processing for individual pods, ensure that **globallyDisableIrqLoadBalancing** is set to **false** in the performance profile. Then, in the pod specification, set the **irq-load-balancing.crio.io** and **cpu-load-balancing.crio.io** pod annotations to **disable**. An example pod specification snippet that illustrates this is below:

```
apiVersion: performance.openshift.io/v2
kind: Pod
metadata:
  annotations:
    irq-load-balancing.crio.io: "disable"
    cpu-load-balancing.crio.io: "disable"
spec:
  runtimeClassName: performance-<profile_name>
...
```

16.4.10. Upgrading the performance profile to use device interrupt processing

When you upgrade the Performance Addon Operator performance profile custom resource definition (CRD) from v1 or v1alpha1 to v2, **globallyDisableIrqLoadBalancing** is set to **true** on existing profiles.



NOTE

When **globallyDisableIrqLoadBalancing** is set to **true**, device interrupts are processed across all CPUs as long as they don't belong to a guaranteed pod.

16.4.10.1. Supported API Versions

The Performance Addon Operator supports **v2**, **v1**, and **v1alpha1** for the performance profile **apiVersion** field. The v1 and v1alpha1 APIs are identical. The v2 API includes an optional boolean field **globallyDisableIrqLoadBalancing** with a default value of **false**.

16.4.10.1.1. Upgrading Performance Addon Operator API from v1alpha1 to v1

When upgrading Performance Addon Operator API version from v1alpha1 to v1, the v1alpha1 performance profiles are converted on-the-fly using a "None" Conversion strategy and served to the Performance Addon Operator with API version v1.

16.4.10.1.2. Upgrading Performance Addon Operator API from v1alpha1 or v1 to v2

When upgrading from an older Performance Addon Operator API version, the existing v1 and v1alpha1 performance profiles are converted using a conversion webhook that injects the **globallyDisableIrqLoadBalancing** field with a value of **true**.

16.4.11. Configuring a node for IRQ dynamic load balancing

To configure a cluster node to handle IRQ dynamic load balancing, do the following:

1. Log in to the OpenShift Container Platform cluster as a user with cluster-admin privileges.
2. Set the performance profile **apiVersion** to use **performance.openshift.io/v2**.
3. Remove the **globallyDisableIrqLoadBalancing** field or set it to **false**.
4. Set the appropriate isolated and reserved CPUs. The following snippet illustrates a profile that reserves 2 CPUs. IRQ load-balancing is enabled for pods running on the **isolated** CPU set:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: dynamic-irq-profile
spec:
  cpu:
    isolated: 2-5
    reserved: 0-1
  ...
```

**NOTE**

When you configure reserved and isolated CPUs, the infra containers in pods use the reserved CPUs and the application containers use the isolated CPUs.

5. Create the pod that uses exclusive CPUs, and set **irq-load-balancing.crio.io** and **cpu-quota.crio.io** annotations to **disable**. For example:

```
apiVersion: v1
kind: Pod
metadata:
  name: dynamic-irq-pod
  annotations:
    irq-load-balancing.crio.io: "disable"
    cpu-quota.crio.io: "disable"
spec:
  containers:
  - name: dynamic-irq-pod
    image: "quay.io/openshift-kni/cnf-tests:4.9"
    command: ["sleep", "10h"]
    resources:
      requests:
        cpu: 2
        memory: "200M"
      limits:
        cpu: 2
        memory: "200M"
    nodeSelector:
      node-role.kubernetes.io/worker-cnf: ""
    runtimeClassName: performance-dynamic-irq-profile
  ...
```

6. Enter the pod **runtimeClassName** in the form **performance-<profile_name>**, where **<profile_name>** is the **name** from the **PerformanceProfile** YAML, in this example, **performance-dynamic-irq-profile**.

7. Set the node selector to target a cnf-worker.
8. Ensure the pod is running correctly. Status should be **running**, and the correct cnf-worker node should be set:

```
$ oc get pod -o wide
```

Expected output

```
NAME          READY STATUS  RESTARTS  AGE   IP           NODE
NOMINATED NODE READINESS GATES
dynamic-irq-pod 1/1   Running  0         5h33m <ip-address> <node-name> <none>
<none>
```

9. Get the CPUs that the pod configured for IRQ dynamic load balancing runs on:

```
$ oc exec -it dynamic-irq-pod -- /bin/bash -c "grep Cpus_allowed_list /proc/self/status | awk '{print $2}'"
```

Expected output

```
Cpus_allowed_list: 2-3
```

10. Ensure the node configuration is applied correctly. SSH into the node to verify the configuration.

```
$ oc debug node/<node-name>
```

Expected output

```
Starting pod/<node-name>-debug ...
To use host binaries, run `chroot /host`

Pod IP: <ip-address>
If you don't see a command prompt, try pressing enter.

sh-4.4#
```

11. Verify that you can use the node file system:

```
sh-4.4# chroot /host
```

Expected output

```
sh-4.4#
```

12. Ensure the default system CPU affinity mask does not include the **dynamic-irq-pod** CPUs, for example, CPUs 2 and 3.

```
$ cat /proc/irq/default_smp_affinity
```

Example output

33

13. Ensure the system IRQs are not configured to run on the **dynamic-irq-pod** CPUs:

```
find /proc/irq/ -name smp_affinity_list -exec sh -c 'i="$1"; mask=$(cat $i); file=$(echo $i); echo $file: $mask' _ {} \;
```

Example output

```
/proc/irq/0/smp_affinity_list: 0-5
/proc/irq/1/smp_affinity_list: 5
/proc/irq/2/smp_affinity_list: 0-5
/proc/irq/3/smp_affinity_list: 0-5
/proc/irq/4/smp_affinity_list: 0
/proc/irq/5/smp_affinity_list: 0-5
/proc/irq/6/smp_affinity_list: 0-5
/proc/irq/7/smp_affinity_list: 0-5
/proc/irq/8/smp_affinity_list: 4
/proc/irq/9/smp_affinity_list: 4
/proc/irq/10/smp_affinity_list: 0-5
/proc/irq/11/smp_affinity_list: 0
/proc/irq/12/smp_affinity_list: 1
/proc/irq/13/smp_affinity_list: 0-5
/proc/irq/14/smp_affinity_list: 1
/proc/irq/15/smp_affinity_list: 0
/proc/irq/24/smp_affinity_list: 1
/proc/irq/25/smp_affinity_list: 1
/proc/irq/26/smp_affinity_list: 1
/proc/irq/27/smp_affinity_list: 5
/proc/irq/28/smp_affinity_list: 1
/proc/irq/29/smp_affinity_list: 0
/proc/irq/30/smp_affinity_list: 0-5
```

Some IRQ controllers do not support IRQ re-balancing and will always expose all online CPUs as the IRQ mask. These IRQ controllers effectively run on CPU 0. For more information on the host configuration, SSH into the host and run the following, replacing **<irq-num>** with the CPU number that you want to query:

```
$ cat /proc/irq/<irq-num>/effective_affinity
```

16.4.12. Configuring hyperthreading for a cluster

To configure hyperthreading for an OpenShift Container Platform cluster, set the CPU threads in the performance profile to the same cores that are configured for the reserved or isolated CPU pools.



NOTE

If you configure a performance profile, and subsequently change the hyperthreading configuration for the host, ensure that you update the CPU **isolated** and **reserved** fields in the **PerformanceProfile** YAML to match the new configuration.



WARNING

Disabling a previously enabled host hyperthreading configuration can cause the CPU core IDs listed in the **PerformanceProfile** YAML to be incorrect. This incorrect configuration can cause the node to become unavailable because the listed CPUs can no longer be found.

Prerequisites

- Access to the cluster as a user with the **cluster-admin** role.
- Install the OpenShift CLI (oc).

Procedure

1. Ascertain which threads are running on what CPUs for the host you want to configure. You can view which threads are running on the host CPUs by logging in to the cluster and running the following command:

```
$ lscpu --all --extended
```

Example output

```
CPU NODE SOCKET CORE L1d:L1i:L2:L3 ONLINE MAXMHZ  MINMHZ
0  0  0    0  0:0:0:0   yes  4800.0000 400.0000
1  0  0    1  1:1:1:0   yes  4800.0000 400.0000
2  0  0    2  2:2:2:0   yes  4800.0000 400.0000
3  0  0    3  3:3:3:0   yes  4800.0000 400.0000
4  0  0    0  0:0:0:0   yes  4800.0000 400.0000
5  0  0    1  1:1:1:0   yes  4800.0000 400.0000
6  0  0    2  2:2:2:0   yes  4800.0000 400.0000
7  0  0    3  3:3:3:0   yes  4800.0000 400.0000
```

In this example, there are eight logical CPU cores running on four physical CPU cores. CPU0 and CPU4 are running on physical Core0, CPU1 and CPU5 are running on physical Core 1, and so on.

Alternatively, to view the threads that are set for a particular physical CPU core (**cpu0** in the example below), open a command prompt and run the following:

```
$ cat /sys/devices/system/cpu/cpu0/topology/thread_siblings_list
```

Example output

```
0-4
```

2. Apply the isolated and reserved CPUs in the **PerformanceProfile** YAML. For example, you can set logical cores CPU0 and CPU4 as **isolated**, and logical cores CPU1 to CPU3 and CPU5 to CPU7 as **reserved**. When you configure reserved and isolated CPUs, the infra containers in

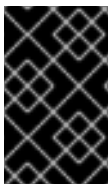
pods use the reserved CPUs and the application containers use the isolated CPUs.

```
...
cpu:
  isolated: 0,4
  reserved: 1-3,5-7
...
```



NOTE

The reserved and isolated CPU pools must not overlap and together must span all available cores in the worker node.



IMPORTANT

Hyperthreading is enabled by default on most Intel processors. If you enable hyperthreading, all threads processed by a particular core must be isolated or processed on the same core.

16.4.12.1. Disabling hyperthreading for low latency applications

When configuring clusters for low latency processing, consider whether you want to disable hyperthreading before you deploy the cluster. To disable hyperthreading, do the following:

1. Create a performance profile that is appropriate for your hardware and topology.
2. Set **`nosmt`** as an additional kernel argument. The following example performance profile illustrates this setting:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: example-performanceprofile
spec:
  additionalKernelArgs:
    - nmi_watchdog=0
    - audit=0
    - mce=off
    - processor.max_cstate=1
    - idle=poll
    - intel_idle.max_cstate=0
    - nosmt
  cpu:
    isolated: 2-3
    reserved: 0-1
  hugepages:
    defaultHugepagesSize: 1G
  pages:
    - count: 2
      node: 0
      size: 1G
  nodeSelector:
    node-role.kubernetes.io/performance: "
  realTimeKernel:
    enabled: true
```

**NOTE**

When you configure reserved and isolated CPUs, the infra containers in pods use the reserved CPUs and the application containers use the isolated CPUs.

16.5. TUNING NODES FOR LOW LATENCY WITH THE PERFORMANCE PROFILE

The performance profile lets you control latency tuning aspects of nodes that belong to a certain machine config pool. After you specify your settings, the **PerformanceProfile** object is compiled into multiple objects that perform the actual node level tuning:

- A **MachineConfig** file that manipulates the nodes.
- A **KubeletConfig** file that configures the Topology Manager, the CPU Manager, and the OpenShift Container Platform nodes.
- The Tuned profile that configures the Node Tuning Operator.

You can use a performance profile to specify whether to update the kernel to kernel-rt, to allocate huge pages, and to partition the CPUs for performing housekeeping duties or running workloads.

**NOTE**

You can manually create the **PerformanceProfile** object or use the Performance Profile Creator (PPC) to generate a performance profile. See the additional resources below for more information on the PPC.

Sample performance profile

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: performance
spec:
  cpu:
    isolated: "5-15" 1
    reserved: "0-4" 2
  hugepages:
    defaultHugepagesSize: "1G"
  pages:
    - size: "1G"
      count: 16
      node: 0
  realTimeKernel:
    enabled: true 3
  numa: 4
    topologyPolicy: "best-effort"
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: "" 5
```

- 1** Use this field to isolate specific CPUs to use with application containers for workloads.

- 2 Use this field to reserve specific CPUs to use with infra containers for housekeeping.
- 3 Use this field to install the real-time kernel on the node. Valid values are **true** or **false**. Setting the **true** value installs the real-time kernel.
- 4 Use this field to configure the topology manager policy. Valid values are **none** (default), **best-effort**, **restricted**, and **single-numa-node**. For more information, see [Topology Manager Policies](#).
- 5 Use this field to specify a node selector to apply the performance profile to specific nodes.

Additional resources

For information on using the Performance Profile Creator (PPC) to generate a performance profile, see [Creating a performance profile](#).

16.5.1. Configuring huge pages

Nodes must pre-allocate huge pages used in an OpenShift Container Platform cluster. Use the Performance Addon Operator to allocate huge pages on a specific node.

OpenShift Container Platform provides a method for creating and allocating huge pages. Performance Addon Operator provides an easier method for doing this using the performance profile.

For example, in the **hugepages pages** section of the performance profile, you can specify multiple blocks of **size**, **count**, and, optionally, **node**:

```
hugepages:
  defaultHugepagesSize: "1G"
  pages:
    - size: "1G"
      count: 4
      node: 0 1
```

- 1 **node** is the NUMA node in which the huge pages are allocated. If you omit **node**, the pages are evenly spread across all NUMA nodes.



NOTE

Wait for the relevant machine config pool status that indicates the update is finished.

These are the only configuration steps you need to do to allocate huge pages.

Verification

- To verify the configuration, see the **/proc/meminfo** file on the node:

```
$ oc debug node/ip-10-0-141-105.ec2.internal
```

```
# grep -i huge /proc/meminfo
```

Example output

```
AnonHugePages: ##### ##
ShmemHugePages: 0 kB
HugePages_Total: 2
HugePages_Free: 2
HugePages_Rsvd: 0
HugePages_Surp: 0
Hugepagesize: ##### ##
Hugetlb: ##### ##
```

- Use **oc describe** to report the new size:

```
$ oc describe node worker-0.ocp4poc.example.com | grep -i huge
```

Example output

```
hugepages-1g=true
hugepages-###: ###
hugepages-###: ###
```

16.5.2. Allocating multiple huge page sizes

You can request huge pages with different sizes under the same container. This allows you to define more complicated pods consisting of containers with different huge page size needs.

For example, you can define sizes **1G** and **2M** and the Performance Addon Operator will configure both sizes on the node, as shown here:

```
spec:
  hugepages:
    defaultHugepagesSize: 1G
  pages:
    - count: 1024
      node: 0
      size: 2M
    - count: 4
      node: 1
      size: 1G
```

16.5.3. Restricting CPUs for infra and application containers

Generic housekeeping and workload tasks use CPUs in a way that may impact latency-sensitive processes. By default, the container runtime uses all online CPUs to run all containers together, which can result in context switches and spikes in latency. Partitioning the CPUs prevents noisy processes from interfering with latency-sensitive processes by separating them from each other. The following table describes how processes run on a CPU after you have tuned the node using the Performance Add-On Operator:

Table 16.1. Process' CPU assignments

Process type	Details
--------------	---------

Process type	Details
Burstable and best-effort pods	Runs on any CPU except where low latency workload is running
Infrastructure pods	Runs on any CPU except where low latency workload is running
Interrupts	Redirects to reserved CPUs (optional in OpenShift Container Platform 4.9 and later)
Kernel processes	Pins to reserved CPUs
Latency-sensitive workload pods	Pins to a specific set of exclusive CPUs from the isolated pool
OS processes/systemd services	Pins to reserved CPUs

The exact partitioning pattern to use depends on many factors like hardware, workload characteristics and the expected system load. Some sample use cases are as follows:

- If the latency-sensitive workload uses specific hardware, such as a network interface controller (NIC), ensure that the CPUs in the isolated pool are as close as possible to this hardware. At a minimum, you should place the workload in the same Non-Uniform Memory Access (NUMA) node.
- The reserved pool is used for handling all interrupts. When depending on system networking, allocate a sufficiently-sized reserve pool to handle all the incoming packet interrupts. In 4.9 and later versions, workloads can optionally be labeled as sensitive.

The decision regarding which specific CPUs should be used for reserved and isolated partitions requires detailed analysis and measurements. Factors like NUMA affinity of devices and memory play a role. The selection also depends on the workload architecture and the specific use case.



IMPORTANT

The reserved and isolated CPU pools must not overlap and together must span all available cores in the worker node.

To ensure that housekeeping tasks and workloads do not interfere with each other, specify two groups of CPUs in the **spec** section of the performance profile.

- **isolated** - Specifies the CPUs for the application container workloads. These CPUs have the lowest latency. Processes in this group have no interruptions and can, for example, reach much higher DPDK zero packet loss bandwidth.
- **reserved** - Specifies the CPUs for the cluster and operating system housekeeping duties. Threads in the **reserved** group are often busy. Do not run latency-sensitive applications in the **reserved** group. Latency-sensitive applications run in the **isolated** group.

Procedure

1. Create a performance profile appropriate for the environment's hardware and topology.
2. Add the **reserved** and **isolated** parameters with the CPUs you want reserved and isolated for the infra and application containers:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: infra-cpus
spec:
  cpu:
    reserved: "0-4,9" 1
    isolated: "5-8" 2
  nodeSelector: 3
    node-role.kubernetes.io/worker: ""
```

- 1 Specify which CPUs are for infra containers to perform cluster and operating system housekeeping duties.
- 2 Specify which CPUs are for application containers to run workloads.
- 3 Optional: Specify a node selector to apply the performance profile to specific nodes.

Additional resources

- [Managing device interrupt processing for guaranteed pod isolated CPUs](#)
- [Create a pod that gets assigned a QoS class of Guaranteed](#)

16.6. REDUCING NIC QUEUES USING THE PERFORMANCE ADDON OPERATOR

The Performance Addon Operator allows you to adjust the network interface controller (NIC) queue count for each network device by configuring the performance profile. Device network queues allows the distribution of packets among different physical queues and each queue gets a separate thread for packet processing.

In real-time or low latency systems, all the unnecessary interrupt request lines (IRQs) pinned to the isolated CPUs must be moved to reserved or housekeeping CPUs.

In deployments with applications that require system, OpenShift Container Platform networking or in mixed deployments with Data Plane Development Kit (DPDK) workloads, multiple queues are needed to achieve good throughput and the number of NIC queues should be adjusted or remain unchanged. For example, to achieve low latency the number of NIC queues for DPDK based workloads should be reduced to just the number of reserved or housekeeping CPUs.

Too many queues are created by default for each CPU and these do not fit into the interrupt tables for housekeeping CPUs when tuning for low latency. Reducing the number of queues makes proper tuning possible. Smaller number of queues means a smaller number of interrupts that then fit in the IRQ table.

16.6.1. Adjusting the NIC queues with the performance profile

The performance profile lets you adjust the queue count for each network device.

Supported network devices:

- Non-virtual network devices
- Network devices that support multiple queues (channels)

Unsupported network devices:

- Pure software network interfaces
- Block devices
- Intel DPDK virtual functions

Prerequisites

- Access to the cluster as a user with the **cluster-admin** role.
- Install the OpenShift CLI (**oc**).

Procedure

1. Log in to the OpenShift Container Platform cluster running the Performance Addon Operator as a user with **cluster-admin** privileges.
2. Create and apply a performance profile appropriate for your hardware and topology. For guidance on creating a profile, see the "Creating a performance profile" section.
3. Edit this created performance profile:

```
$ oc edit -f <your_profile_name>.yaml
```

4. Populate the **spec** field with the **net** object. The object list can contain two fields:
 - **userLevelNetworking** is a required field specified as a boolean flag. If **userLevelNetworking** is **true**, the queue count is set to the reserved CPU count for all supported devices. The default is **false**.
 - **devices** is an optional field specifying a list of devices that will have the queues set to the reserved CPU count. If the device list is empty, the configuration applies to all network devices. The configuration is as follows:
 - **interfaceName**: This field specifies the interface name, and it supports shell-style wildcards, which can be positive or negative.
 - Example wildcard syntax is as follows: **<string>.***
 - Negative rules are prefixed with an exclamation mark. To apply the net queue changes to all devices other than the excluded list, use **!<device>**, for example, **!eno1**.
 - **vendorID**: The network device vendor ID represented as a 16-bit hexadecimal number with a **0x** prefix.
 - **deviceID**: The network device ID (model) represented as a 16-bit hexadecimal number with a **0x** prefix.

**NOTE**

When a **deviceID** is specified, the **vendorID** must also be defined. A device that matches all of the device identifiers specified in a device entry **interfaceName**, **vendorID**, or a pair of **vendorID** plus **deviceID** qualifies as a network device. This network device then has its net queues count set to the reserved CPU count.

When two or more devices are specified, the net queues count is set to any net device that matches one of them.

- Set the queue count to the reserved CPU count for all devices by using this example performance profile:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: manual
spec:
  cpu:
    isolated: 3-51,54-103
    reserved: 0-2,52-54
  net:
    userLevelNetworking: true
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: ""
```

- Set the queue count to the reserved CPU count for all devices matching any of the defined device identifiers by using this example performance profile:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: manual
spec:
  cpu:
    isolated: 3-51,54-103
    reserved: 0-2,52-54
  net:
    userLevelNetworking: true
  devices:
    - interfaceName: "eth0"
    - interfaceName: "eth1"
    - vendorID: "0x1af4"
    deviceID: "0x1000"
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: ""
```

- Set the queue count to the reserved CPU count for all devices starting with the interface name **eth** by using this example performance profile:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: manual
```

```
spec:
  cpu:
    isolated: 3-51,54-103
    reserved: 0-2,52-54
  net:
    userLevelNetworking: true
  devices:
    - interfaceName: "eth*"
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: ""
```

8. Set the queue count to the reserved CPU count for all devices with an interface named anything other than **eno1** by using this example performance profile:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: manual
spec:
  cpu:
    isolated: 3-51,54-103
    reserved: 0-2,52-54
  net:
    userLevelNetworking: true
  devices:
    - interfaceName: "!eno1"
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: ""
```

9. Set the queue count to the reserved CPU count for all devices that have an interface name **eth0**, **vendorID** of **0x1af4**, and **deviceID** of **0x1000** by using this example performance profile:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: manual
spec:
  cpu:
    isolated: 3-51,54-103
    reserved: 0-2,52-54
  net:
    userLevelNetworking: true
  devices:
    - interfaceName: "eth0"
      vendorID: "0x1af4"
      deviceID: "0x1000"
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: ""
```

10. Apply the updated performance profile:

```
$ oc apply -f <your_profile_name>.yaml
```

Additional resources

- [Creating a performance profile](#) .

16.6.2. Verifying the queue status

In this section, a number of examples illustrate different performance profiles and how to verify the changes are applied.

Example 1

In this example, the net queue count is set to the reserved CPU count (2) for *all* supported devices.

The relevant section from the performance profile is:

```
apiVersion: performance.openshift.io/v2
metadata:
  name: performance
spec:
  kind: PerformanceProfile
  spec:
    cpu:
      reserved: 0-1 #total = 2
      isolated: 2-8
    net:
      userLevelNetworking: true
# ...
```

- Display the status of the queues associated with a device using the following command:



NOTE

Run this command on the node where the performance profile was applied.

```
$ ethtool -l <device>
```

- Verify the queue status before the profile is applied:

```
$ ethtool -l ens4
```

Example output

```
Channel parameters for ens4:
Pre-set maximums:
RX:      0
TX:      0
Other:    0
Combined: 4
Current hardware settings:
RX:      0
TX:      0
Other:    0
Combined: 4
```

- Verify the queue status after the profile is applied:

–

```
$ ethtool -l ens4
```

Example output

```
Channel parameters for ens4:
Pre-set maximums:
RX:      0
TX:      0
Other:    0
Combined: 4
Current hardware settings:
RX:      0
TX:      0
Other:    0
Combined: 2 1
```

- 1** The combined channel shows that the total count of reserved CPUs for *all* supported devices is 2. This matches what is configured in the performance profile.

Example 2

In this example, the net queue count is set to the reserved CPU count (2) for *all* supported network devices with a specific **vendorID**.

The relevant section from the performance profile is:

```
apiVersion: performance.openshift.io/v2
metadata:
  name: performance
spec:
  kind: PerformanceProfile
  spec:
    cpu:
      reserved: 0-1 #total = 2
      isolated: 2-8
    net:
      userLevelNetworking: true
      devices:
        - vendorID = 0x1af4
# ...
```

- Display the status of the queues associated with a device using the following command:



NOTE

Run this command on the node where the performance profile was applied.

```
$ ethtool -l <device>
```

- Verify the queue status after the profile is applied:

```
$ ethtool -l ens4
```

Example output

```

Channel parameters for ens4:
Pre-set maximums:
RX:      0
TX:      0
Other:   0
Combined: 4
Current hardware settings:
RX:      0
TX:      0
Other:   0
Combined: 2 1

```

- 1** The total count of reserved CPUs for all supported devices with **vendorID=0x1af4** is 2. For example, if there is another network device **ens2** with **vendorID=0x1af4** it will also have total net queues of 2. This matches what is configured in the performance profile.

Example 3

In this example, the net queue count is set to the reserved CPU count (2) for *all* supported network devices that match any of the defined device identifiers.

The command **udevadm info** provides a detailed report on a device. In this example the devices are:

```

# udevadm info -p /sys/class/net/ens4
...
E: ID_MODEL_ID=0x1000
E: ID_VENDOR_ID=0x1af4
E: INTERFACE=ens4
...

```

```

# udevadm info -p /sys/class/net/eth0
...
E: ID_MODEL_ID=0x1002
E: ID_VENDOR_ID=0x1001
E: INTERFACE=eth0
...

```

- Set the net queues to 2 for a device with **interfaceName** equal to **eth0** and any devices that have a **vendorID=0x1af4** with the following performance profile:

```

apiVersion: performance.openshift.io/v2
metadata:
  name: performance
spec:
  kind: PerformanceProfile
  spec:
    cpu:
      reserved: 0-1 #total = 2
      isolated: 2-8
    net:
      userLevelNetworking: true
    devices:

```

```
- interfaceName = eth0
- vendorID = 0x1af4
...
```

- Verify the queue status after the profile is applied:

```
$ ethtool -l ens4
```

Example output

```
Channel parameters for ens4:
Pre-set maximums:
RX:      0
TX:      0
Other:    0
Combined: 4
Current hardware settings:
RX:      0
TX:      0
Other:    0
Combined: 2 1
```

- 1** The total count of reserved CPUs for all supported devices with **vendorID=0x1af4** is set to 2. For example, if there is another network device **ens2** with **vendorID=0x1af4**, it will also have the total net queues set to 2. Similarly, a device with **interfaceName** equal to **eth0** will have total net queues set to 2.

16.6.3. Logging associated with adjusting NIC queues

Log messages detailing the assigned devices are recorded in the respective Tuned daemon logs. The following messages might be recorded to the **/var/log/tuned/tuned.log** file:

- An **INFO** message is recorded detailing the successfully assigned devices:

```
INFO tuned.plugins.base: instance net_test (net): assigning devices ens1, ens2, ens3
```

- A **WARNING** message is recorded if none of the devices can be assigned:

```
WARNING tuned.plugins.base: instance net_test: no matching devices available
```

16.7. PERFORMING END-TO-END TESTS FOR PLATFORM VERIFICATION

The Cloud-native Network Functions (CNF) tests image is a containerized test suite that validates features required to run CNF payloads. You can use this image to validate a CNF-enabled OpenShift cluster where all the components required for running CNF workloads are installed.

The tests run by the image are split into three different phases:

- Simple cluster validation
- Setup

- End to end tests

The validation phase checks that all the features required to be tested are deployed correctly on the cluster.

Validations include:

- Targeting a machine config pool that belong to the machines to be tested
- Enabling SCTP on the nodes
- Enabling xt_u32 kernel module via machine config
- Having the Performance Addon Operator installed
- Having the SR-IOV Operator installed
- Having the PTP Operator installed
- Enabling the **contain-mount-namespace** mode via machine config
- Using OVN-kubernetes as the cluster network provider

Latency tests, a part of the CNF-test container, also require the same validations. For more information about running a latency test, see the Running the latency tests section.

The tests need to perform an environment configuration every time they are executed. This involves items such as creating SR-IOV node policies, performance profiles, or PTP profiles. Allowing the tests to configure an already configured cluster might affect the functionality of the cluster. Also, changes to configuration items such as SR-IOV node policy might result in the environment being temporarily unavailable until the configuration change is processed.

16.7.1. Prerequisites

- The test entrypoint is **/usr/bin/test-run.sh**. It runs both a setup test set and the real conformance test suite. The minimum requirement is to provide it with a kubeconfig file and its related **\$KUBECONFIG** environment variable, mounted through a volume.
- The tests assumes that a given feature is already available on the cluster in the form of an Operator, flags enabled on the cluster, or machine configs.
- Some tests require a pre-existing machine config pool to append their changes to. This must be created on the cluster before running the tests.

The default worker pool is **worker-cnf** and can be created with the following manifest:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
metadata:
  name: worker-cnf
  labels:
    machineconfiguration.openshift.io/role: worker-cnf
spec:
  machineConfigSelector:
    matchExpressions:
      - {
        key: machineconfiguration.openshift.io/role,
```

```

    operator: In,
    values: [worker-cnf, worker],
  }
  paused: false
  nodeSelector:
    matchLabels:
      node-role.kubernetes.io/worker-cnf: ""

```

You can use the **ROLE_WORKER_CNF** variable to override the worker pool name:

```

$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig -e
ROLE_WORKER_CNF=custom-worker-pool registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9
/usr/bin/test-run.sh

```



NOTE

Currently, not all tests run selectively on the nodes belonging to the pool.

16.7.2. Dry run

Use this command to run in dry-run mode. This is useful for checking what is in the test suite and provides output for all of the tests the image would run.

```

$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig
registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-run.sh -ginkgo.dryRun -ginkgo.v

```

16.7.3. Disconnected mode

The CNF tests image support running tests in a disconnected cluster, meaning a cluster that is not able to reach outer registries. This is done in two steps:

1. Performing the mirroring.
2. Instructing the tests to consume the images from a custom registry.

16.7.3.1. Mirroring the images to a custom registry accessible from the cluster

A **mirror** executable is shipped in the image to provide the input required by **oc** to mirror the images needed to run the tests to a local registry.

Run this command from an intermediate machine that has access both to the cluster and to registry.redhat.io over the internet:

```

$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig
registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/mirror -registry my.local.registry:5000/ | oc
image mirror -f -

```

Then, follow the instructions in the following section about overriding the registry used to fetch the images.

16.7.3.2. Instruct the tests to consume those images from a custom registry

This is done by setting the **IMAGE_REGISTRY** environment variable:

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig -e
IMAGE_REGISTRY="my.local.registry:5000/" -e CNF_TESTS_IMAGE="custom-cnf-tests-
image:latests" registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-run.sh
```

16.7.3.3. Mirroring to the cluster internal registry

OpenShift Container Platform provides a built-in container image registry, which runs as a standard workload on the cluster.

Procedure

1. Gain external access to the registry by exposing it with a route:

```
$ oc patch configs.imageregistry.operator.openshift.io/cluster --patch '{"spec":
{"defaultRoute":true}}' --type=merge
```

2. Fetch the registry endpoint:

```
REGISTRY=$(oc get route default-route -n openshift-image-registry --template='{{ .spec.host
}}')
```

3. Create a namespace for exposing the images:

```
$ oc create ns cnftests
```

4. Make that image stream available to all the namespaces used for tests. This is required to allow the tests namespaces to fetch the images from the **cnftests** image stream.

```
$ oc policy add-role-to-user system:image-puller system:serviceaccount:sctptest:default --
namespace=cnftests
```

```
$ oc policy add-role-to-user system:image-puller system:serviceaccount:cnf-features-
testing:default --namespace=cnftests
```

```
$ oc policy add-role-to-user system:image-puller system:serviceaccount:performance-addon-
operators-testing:default --namespace=cnftests
```

```
$ oc policy add-role-to-user system:image-puller system:serviceaccount:dpdk-testing:default
--namespace=cnftests
```

```
$ oc policy add-role-to-user system:image-puller system:serviceaccount:sriov-conformance-
testing:default --namespace=cnftests
```

```
$ oc policy add-role-to-user system:image-puller system:serviceaccount:xt-u32-testing:default
--namespace=cnftests
```

```
$ oc policy add-role-to-user system:image-puller system:serviceaccount:vrf-testing:default --
namespace=cnftests
```

```
$ oc policy add-role-to-user system:image-puller system:serviceaccount:gatekeeper-testing:default --namespace=cnftests
```

```
$ oc policy add-role-to-user system:image-puller system:serviceaccount:ovs-qos-testing:default --namespace=cnftests
```

- Retrieve the docker secret name and auth token:

```
SECRET=$(oc -n cnftests get secret | grep builder-docker | awk {'print $1'})
TOKEN=$(oc -n cnftests get secret $SECRET -o jsonpath="{.data[\".dockercfg\"]}" | base64 --decode | jq '["image-registry.openshift-image-registry.svc:5000"].auth')
```

- Write a **dockerauth.json** similar to this:

```
echo "{\"auths\": { \"$REGISTRY\": { \"auth\": $TOKEN } }}" > dockerauth.json
```

- Do the mirroring:

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/mirror -registry $REGISTRY/cnftests | oc image mirror --insecure=true -a=$(pwd)/dockerauth.json -f -
```

- Run the tests:

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig -e IMAGE_REGISTRY=image-registry.openshift-image-registry.svc:5000/cnftests cnf-tests-local:latest /usr/bin/test-run.sh
```

16.7.3.4. Mirroring a different set of images

Procedure

- The **mirror** command tries to mirror the u/s images by default. This can be overridden by passing a file with the following format to the image:

```
[
  {
    "registry": "public.registry.io:5000",
    "image": "imageforcnftests:4.9"
  },
  {
    "registry": "public.registry.io:5000",
    "image": "imagefordpdk:4.9"
  }
]
```

- Pass it to the **mirror** command, for example saving it locally as **images.json**. With the following command, the local path is mounted in **/kubeconfig** inside the container and that can be passed to the mirror command.

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig
registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/mirror --registry
"my.local.registry:5000/" --images "/kubeconfig/images.json" | oc image mirror -f -
```

16.7.4. Running in a single node cluster

Running tests on a single node cluster causes the following limitations to be imposed:

- Longer timeouts for certain tests, including SR-IOV and SCTP tests
- Tests requiring master and worker nodes are skipped

Longer timeouts concern SR-IOV and SCTP tests. Reconfiguration requiring node reboots cause a reboot of the entire environment, including the OpenShift control plane, and therefore takes longer to complete. All PTP tests requiring a master and worker node are skipped. No additional configuration is needed because the tests check for the number of nodes at startup and adjust test behavior accordingly.

PTP tests can run in Discovery mode. The tests look for a PTP master configured outside of the cluster.

For more information, see the Discovery mode section.

To enable Discovery mode, the tests must be instructed by setting the **DISCOVERY_MODE** environment variable as follows:

```
$ docker run -v $(pwd)/:/kubeconfig:Z -e KUBECONFIG=/kubeconfig/kubeconfig -e
DISCOVERY_MODE=true registry.redhat.io/openshift-kni/cnf-tests /usr/bin/test-run.sh
```

Required parameters

- **ROLE_WORKER_CNF=master** - Required because master is the only machine pool to which the node will belong.
- **XT_U32TEST_HAS_NON_CNF_WORKERS=false** - Required to instruct the xt_u32 negative test to skip because there are only nodes where the module is loaded.
- **SCTPTEST_HAS_NON_CNF_WORKERS=false** - Required to instruct the SCTP negative test to skip because there are only nodes where the module is loaded.

16.7.5. Impact of tests on the cluster

Depending on the feature, running the test suite could cause different impacts on the cluster. In general, only the SCTP tests do not change the cluster configuration. All of the other features have various impacts on the configuration.

16.7.5.1. SCTP

SCTP tests just run different pods on different nodes to check connectivity. The impacts on the cluster are related to running simple pods on two nodes.

16.7.5.2. XT_U32

XT_U32 tests run pods on different nodes to check iptables rule that utilize xt_u32. The impacts on the cluster are related to running simple pods on two nodes.

16.7.5.3. SR-IOV

SR-IOV tests require changes in the SR-IOV network configuration, where the tests create and destroy different types of configuration.

This might have an impact if existing SR-IOV network configurations are already installed on the cluster, because there may be conflicts depending on the priority of such configurations.

At the same time, the result of the tests might be affected by existing configurations.

16.7.5.4. PTP

PTP tests apply a PTP configuration to a set of nodes of the cluster. As with SR-IOV, this might conflict with any existing PTP configuration already in place, with unpredictable results.

16.7.5.5. Performance

Performance tests apply a performance profile to the cluster. The effect of this is changes in the node configuration, reserving CPUs, allocating memory huge pages, and setting the kernel packages to be realtime. If an existing profile named **performance** is already available on the cluster, the tests do not deploy it.

16.7.5.6. DPDK

DPDK relies on both performance and SR-IOV features, so the test suite configures both a performance profile and SR-IOV networks, so the impacts are the same as those described in SR-IOV testing and performance testing.

16.7.5.7. Container-mount-namespace

The validation test for **container-mount-namespace** mode only checks that the appropriate **MachineConfig** objects are present and active, and has no additional impact on the node.

16.7.5.8. Cleaning up

After running the test suite, all the dangling resources are cleaned up.

16.7.6. Override test image parameters

Depending on the requirements, the tests can use different images. There are two images used by the tests that can be changed using the following environment variables:

- **CNF_TESTS_IMAGE**
- **DPDK_TESTS_IMAGE**

For example, to change the **CNF_TESTS_IMAGE** with a custom registry run the following command:

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig -e  
CNF_TESTS_IMAGE="custom-cnf-tests-image:latest" registry.redhat.io/openshift4/cnf-tests-  
rhel8:v4.9 /usr/bin/test-run.sh
```

16.7.6.1. Ginkgo parameters

The test suite is built upon the ginkgo BDD framework. This means that it accepts parameters for filtering or skipping tests.

You can use the **-ginkgo.focus** parameter to filter a set of tests:

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig
registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-run.sh -ginkgo.focus="performance|sctp"
```

You can run only the latency test using the **-ginkgo.focus** parameter.

To run only the latency test, you must provide the **-ginkgo.focus** parameter and the **PERF_TEST_PROFILE** environment variable that contains the name of the performance profile that needs to be tested. For example:

```
$ docker run --rm -v $KUBECONFIG:/kubeconfig -e KUBECONFIG=/kubeconfig -e
LATENCY_TEST_RUN=true -e LATENCY_TEST_RUNTIME=600 -e
OSLAT_MAXIMUM_LATENCY=20 -e PERF_TEST_PROFILE=<performance_profile_name>
registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-run.sh -ginkgo.focus="\[performance\]\[config\]\[performance\]\ Latency\ Test"
```



NOTE

There is a particular test that requires both SR-IOV and SCTP. Given the selective nature of the **focus** parameter, this test is triggered by only placing the **sriov** matcher. If the tests are executed against a cluster where SR-IOV is installed but SCTP is not, adding the **-ginkgo.skip=SCTP** parameter causes the tests to skip SCTP testing.

16.7.6.2. Available features

The set of available features to filter are:

- **performance**
- **sriov**
- **ptp**
- **sctp**
- **xt_u32**
- **dpdk**
- **container-mount-namespace**

16.7.7. Discovery mode

Discovery mode allows you to validate the functionality of a cluster without altering its configuration. Existing environment configurations are used for the tests. The tests attempt to find the configuration items needed and use those items to execute the tests. If resources needed to run a specific test are not found, the test is skipped, providing an appropriate message to the user. After the tests are finished, no cleanup of the pre-configured configuration items is done, and the test environment can be immediately used for another test run.

Some configuration items are still created by the tests. These are specific items needed for a test to run; for example, a SR-IOV Network. These configuration items are created in custom namespaces and are cleaned up after the tests are executed.

An additional bonus is a reduction in test run times. As the configuration items are already there, no time is needed for environment configuration and stabilization.

To enable discovery mode, the tests must be instructed by setting the **DISCOVERY_MODE** environment variable as follows:

```
$ docker run -v $(pwd)/:/kubeconfig:Z -e KUBECONFIG=/kubeconfig/kubeconfig -e  
DISCOVERY_MODE=true registry.redhat.io/openshift-kni/cnf-tests /usr/bin/test-run.sh
```

16.7.7.1. Required environment configuration prerequisites

SR-IOV tests

Most SR-IOV tests require the following resources:

- **SriovNetworkNodePolicy**.
- At least one with the resource specified by **SriovNetworkNodePolicy** being allocatable; a resource count of at least 5 is considered sufficient.

Some tests have additional requirements:

- An unused device on the node with available policy resource, with link state **DOWN** and not a bridge slave.
- A **SriovNetworkNodePolicy** with a MTU value of **9000**.

DPDK tests

The DPDK related tests require:

- A performance profile.
- A SR-IOV policy.
- A node with resources available for the SR-IOV policy and available with the **PerformanceProfile** node selector.

PTP tests

- A slave **PtpConfig** (**ptp4IOpts="-s"** ,**phc2sysOpts="-a -r"**).
- A node with a label matching the slave **PtpConfig**.

SCTP tests

- **SriovNetworkNodePolicy**.
- A node matching both the **SriovNetworkNodePolicy** and a **MachineConfig** that enables SCTP.

XT_U32 tests

- A node with a machine config that enables XT_U32.

Performance Operator tests

Various tests have different requirements. Some of them are:

- A performance profile.
- A performance profile having **profile.Spec.CPU.Isolated = 1**.
- A performance profile having **profile.Spec.RealTimeKernel.Enabled == true**.
- A node with no huge pages usage.

Container-mount-namespaces tests

- A node with a machine config which enables **container-mount-namespaces** mode

16.7.7.2. Limiting the nodes used during tests

The nodes on which the tests are executed can be limited by specifying a **NODES_SELECTOR** environment variable. Any resources created by the test are then limited to the specified nodes.

```
$ docker run -v $(pwd)/:/kubeconfig:Z -e KUBECONFIG=/kubeconfig/kubeconfig -e
NODES_SELECTOR=node-role.kubernetes.io/worker-cnf registry.redhat.io/openshift-kni/cnf-tests
/usr/bin/test-run.sh
```

16.7.7.3. Using a single performance profile

The resources needed by the DPDK tests are higher than those required by the performance test suite. To make the execution faster, the performance profile used by tests can be overridden using one that also serves the DPDK test suite.

To do this, a profile like the following one can be mounted inside the container, and the performance tests can be instructed to deploy it.

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: performance
spec:
  cpu:
    isolated: "4-15"
    reserved: "0-3"
  hugepages:
    defaultHugepagesSize: "1G"
  pages:
    - size: "1G"
      count: 16
      node: 0
  realTimeKernel:
    enabled: true
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: ""
```

**NOTE**

When you configure reserved and isolated CPUs, the infra containers in pods use the reserved CPUs and the application containers use the isolated CPUs.

To override the performance profile used, the manifest must be mounted inside the container and the tests must be instructed by setting the **PERFORMANCE_PROFILE_MANIFEST_OVERRIDE** parameter as follows:

```
$ docker run -v $(pwd)/:/kubeconfig:Z -e KUBECONFIG=/kubeconfig/kubeconfig -e
PERFORMANCE_PROFILE_MANIFEST_OVERRIDE=/kubeconfig/manifest.yaml
registry.redhat.io/openshift-kni/cnf-tests /usr/bin/test-run.sh
```

16.7.7.4. Disabling the performance profile cleanup

When not running in discovery mode, the suite cleans up all the created artifacts and configurations. This includes the performance profile.

When deleting the performance profile, the machine config pool is modified and nodes are rebooted. After a new iteration, a new profile is created. This causes long test cycles between runs.

To speed up this process, set **CLEAN_PERFORMANCE_PROFILE="false"** to instruct the tests not to clean the performance profile. In this way, the next iteration will not need to create it and wait for it to be applied.

```
$ docker run -v $(pwd)/:/kubeconfig:Z -e KUBECONFIG=/kubeconfig/kubeconfig -e
CLEAN_PERFORMANCE_PROFILE="false" registry.redhat.io/openshift-kni/cnf-tests /usr/bin/test-
run.sh
```

16.7.8. Running the latency tests

Assuming the **kubeconfig** file is in the current folder, the command for running the test suite is:

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig
registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-run.sh
```

This allows your **kubeconfig** file to be consumed from inside the running container.

**WARNING**

You must run the latency tests in Discovery mode. The latency tests can change the configuration of your cluster if you do not run in Discovery mode.

In OpenShift Container Platform 4.9, you can also run latency tests from the CNF-test container. The latency test allows the to validate that node tuning is sufficient for your workload.

Three tools measure the latency of the system:

- **hwlatdetect**
- **cyclicttest**
- **oslat**

Each tool has a specific use. Use the tools in sequence to achieve reliable test results.

1. The **hwlatdetect** tool measures the baseline that the bare hardware can achieve. Before proceeding with the next latency test, ensure that the number measured by **hwlatdetect** meets the required threshold because hardware latency spikes cannot be fixed by operating system tuning.
2. The **cyclicttest** tool verifies the timer latency after **hwlatdetect** passes validation. The **cyclicttest** tool schedules a repeated timer and measures the difference between the desired and the actual trigger times. The difference can uncover basic issues with the tuning caused by interrupts or process priorities.
3. The **oslat** tool behaves similarly to a CPU-intensive DPDK application and measures all the interruptions and disruptions to the busy loop that simulates CPU heavy data processing.

By default, the latency tests are disabled. To enable the latency test, you must add the **LATENCY_TEST_RUN** environment variable to the test invocation and set its value to **true**. For example, **LATENCY_TEST_RUN=true**.

The test introduces the following environment variables:

- **LATENCY_TEST_CPUS** variable specifies the number of CPUs that the pod running the latency tests uses.
- **LATENCY_TEST_RUNTIME** variable specifies the amount of time in seconds that the latency test must run.
- **CYCLICTEST_MAXIMUM_LATENCY** variable specifies the maximum latency in microseconds that all threads expect before waking up during the **cyclicttest** run.
- **HWLATDETECT_MAXIMUM_LATENCY** variable specifies the maximum acceptable hardware latency in microseconds for the workload and operating system.
- **OSLAT_MAXIMUM_LATENCY** variable specifies the maximum acceptable latency in microseconds for the **oslat** test results.
- **MAXIMUM_LATENCY** is a unified variable you can apply for all tests.



NOTE

A variable that is specific to certain tests has precedence over the unified variable.

You can use the **ginkgo.focus** flag to run a specific test.

16.7.8.1. Running hwlatdetect

To perform the **hwlatdetect**, run the following command:

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig -e
LATENCY_TEST_RUN=true -e DISCOVERY_MODE=true -e ROLE_WORKER_CNF=worker-cnf -e
```

```
LATENCY_TEST_RUNTIME=600 -e MAXIMUM_LATENCY=20 registry.redhat.io/openshift4/cnf-
tests-rhel8:v4.9 /usr/bin/test-run.sh -ginko.focus="hwlatdetect"
```

The above command runs the **hwlatdetect** tool for 10 minutes (600 seconds). The test runs successfully when the maximum observed latency is lower than **MAXIMUM_LATENCY** (20 μ s), and the command line displays **SUCCESS!**.

Example failure output

```
$ docker run -v $KUBECONFIG:/root/kubeconfig:Z -e KUBECONFIG=/root/kubeconfig -e
PERF_TEST_PROFILE=performance -e ROLE_WORKER_CNF=worker-cnf -e
LATENCY_TEST_RUN=true -e LATENCY_TEST_RUNTIME=40 -e MAXIMUM_LATENCY=1 -e
LATENCY_TEST_CPUS=10 -e DISCOVERY_MODE=true quay.io/titzhak/cnf-tests:latest usr/bin/test-
run.sh -ginkgo.focus="hwlatdetect" 1
running /usr/bin//validation suite -ginkgo.focus=hwlatdetect
```

...

Discovery mode enabled, skipping setup

```
running /usr/bin//cnftests -ginkgo.focus=hwlatdetect
```

10812 09:53:57.108148 [19 request.go:668] Waited for 1.049207747s due to client-side throttling, not priority and fairness, request:

```
GET:https://api.cnfdc8.t5g.lab.eng.bos.redhat.com:6443/apis/autoscaling/v1?timeout=32s
```

Running Suite: CNF Features e2e integration tests

=====

Random Seed: 1628762033

Will run 1 of 138 specs

[illegible]

- [SLOW TEST:26.144 seconds]

[performance] Latency Test

```
/go/src/github.com/openshift-kni/cnf-features-deploy/vendor/github.com/openshift-kni/performance-addon-operators/func-tests/4 latency/latency.go:84
```

with the hwlatdetect image

```
/go/src/github.com/openshift-kni/cnf-features-deploy/vendor/github.com/openshift-kni/performance-  
addon-operators/functests/4 latency/latency.go:224
```

should succeed

```

/go/src/github.com/openshift-kni/cnf-features-deploy/vendor/github.com/openshift-kni/performance-
addon-operators/func-tests/4 latency/latency.go:232

```

SSSSSSSSSSSSSSSSSSSSSSSSSSSSSS

detector: tracer

parameters:

Latency threshold: 1us **2**

Sample window: 10000000us

Sample width: 950000us

Non-sampling period: 9050000us

Output File: None

Starting test

test finished

Max Latency: 35us **3**

Samples recorded: 2

Samples exceeding threshold: 2

```
ts: 1628174377.074638224, inner:20, outer:35
ts: 1628174387.359881340, inner:21, outer:34
; err: exit status 1
goroutine 1 [running]:
k8s.io/klog.stacks(0xc000070200, 0xc000106400, 0x21b, 0x3c2)
    /remote-source/app/vendor/k8s.io/klog/klog.go:875 +0xb9
k8s.io/klog.(*loggingT).output(0x5bed00, 0xc000000003, 0xc00010a0e0, 0x53ea81, 0x7, 0x33, 0x0)
    /remote-source/app/vendor/k8s.io/klog/klog.go:826 +0x35f
k8s.io/klog.(*loggingT).printf(0x5bed00, 0x3, 0x5082da, 0x33, 0xc000113f58, 0x2, 0x2)
    /remote-source/app/vendor/k8s.io/klog/klog.go:707 +0x153
k8s.io/klog.Fatalf(...)
    /remote-source/app/vendor/k8s.io/klog/klog.go:1276
main.main()
    /remote-source/app/cnf-tests/pod-utils/hwlatdetect-runner/main.go:51 +0x897
```

- 1 The docker arguments provided by the user.
- 2 The latency threshold configured by the user using the **MAX_LATENCY** or the **HWLATDETECT_MAX_LATENCY** environment variables.
- 3 The maximum latency value measured during the test.

16.7.8.2. Running cyclictest

To perform the **cyclictest**, run the following command:

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig -e
LATENCY_TEST_RUN=true -e DISCOVERY_MODE=true -e ROLE_WORKER_CNF=worker-cnf -e
LATENCY_TEST_CPUS=10 -e LATENCY_TEST_RUNTIME=600 -e MAXIMUM_LATENCY=20
registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-run.sh -ginkgo.focus="cyclictest"
```

The above command runs the **cyclictest** tool for 10 minutes (600 seconds). The test runs successfully when the maximum observed latency is lower than **MAXIMUM_LATENCY** (20 μ s), and the command line displays **SUCCESS!**.

Example failure output

```
$docker run -v $KUBECONFIG:/root/kubeconfig:Z -e KUBECONFIG=/root/kubeconfig -e
PERF_TEST_PROFILE=performance -e ROLE_WORKER_CNF=worker-cnf -e
LATENCY_TEST_RUN=true -e LATENCY_TEST_RUNTIME=600 -e MAXIMUM_LATENCY=20 -e
LATENCY_TEST_CPUS=10 -e DISCOVERY_MODE=true quay.io/titzhak/cnf-tests:latest usr/bin/test-
run.sh -ginkgo.v -ginkgo.focus="cyclictest" 1
```

```
Discovery mode enabled, skipping setup
running /usr/bin/cnftests -ginkgo.v -ginkgo.focus=cyclictest
I0811 15:02:36.350033    20 request.go:668] Waited for 1.049965918s due to client-side throttling,
not priority and fairness, request:
GET:https://api.cnfdc8.t5g.lab.eng.bos.redhat.com:6443/apis/machineconfiguration.openshift.io/v1?
timeout=32s
Running Suite: CNF Features e2e integration tests
=====
Random Seed: 1628694153
Will run 1 of 138 specs
```

[illegible]

```
[performance] Latency Test with the cyclictst image
should succeed
```

```
/go/src/github.com/openshift-kni/cnf-features-deploy/vendor/github.com/openshift-kni/performance-addon-operators/functests/4_latency/latency.go:200
```

STEP: Waiting two minutes to download the latencyTest image

STEP: Waiting another two minutes to give enough time for the cluster to move the pod to Succeeded phase

Aug 11 15:03:06.826: [INFO]: found mcd machine-config-daemon-wf4w8 for node cnfdc8.clus2.t5g.lab.eng.bos.redhat.com

- Failure [22.527 seconds]

[performance] Latency Test

```
/go/src/github.com/openshift-kni/cnf-features-deploy/vendor/github.com/openshift-kni/performance-  
addon-operators/functests/4_latency/latency.go:84
```

with the cyclicttest image

```
/go/src/github.com/openshift-kni/cnf-features-deploy/vendor/github.com/openshift-kni/performance-addon-operators/functests/4_latency/latency.go:188
```

should succeed [It]

```
/go/src/github.com/openshift-kni/cnf-features-deploy/vendor/github.com/openshift-kni/performance-  
addon-operators/functests/4_latency/latency.go:200
```

The current latency 17 is bigger than the expected one 20 **2**

Expected

```
<bool>: false
```

to be true

```
/go/src/github.com/openshift-kni/cnf-features-deploy/vendor/github.com/openshift-kni/performance-  
addon-operators/functests/4_latency/latency.go:219
```

Log file created at: 2021/08/11 15:02:51

Running on machine: cyclicttest-**knk7d**

Binary: Built with gc go1.16.6 for linux/amd64

Log line format: [IWEF]mmdd hh:mm:ss.uuuuuu threadid file:line] msg

```
10811 15:02:51.092254 1 node.go:37] Environment information: /proc/cmdline: BOOT_IMAGE=
(hd0,gpt3)/ostree/rhcos-
```

612d89f4519a53ad0b1a132f4add78372661bfb3994f5fe115654971aa58a543/vmlinuz-4.18.0-

```
305.10.2.rt7.83.el8 4.x86_64 ip=dhcp random.trust_cpu=on console=tty0 console=ttyS0,115200n8
```

```
ostree=/ostree/boot.1/rhcos/612d89f4519a53ad0b1a132f4add78372661bfb3994f5fe115654971aa58a5
43/0 ignition.platform.id=openstack root=UUID=5a4ddf16-9372-44d9-ac4e-3ee329e16ab3 rw
```

```
rootflags=priquota skew tick=1 nohz=on rcu nocbs=1-3
```

```
tuned.non_isolcpus=000000ff,ffffff,ffffff,ffffff1 intel_pstate=disable nosoftlockup tsc=nowatchdog
intel_iommu=on iommu=pt isolcpus=managed irq.1-3
```

```
systemd.cpu affinity=0,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
```

32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96.

```
97.98.99.100.101.102.103 default hugepagesz=1G hugepagesz=2M hugepages=128
```

```
nmi_watchdog=0 audit=0 mce=off processor.max_cstate=1 idle=poll intel_idle.max_cstate=0
```

```
10811 15:02:51.092427      1 node.go:44] Environment information: kernel version 4.18.0-
```

305.10.2.rt7.83.el8 4.x86 64

```
10811 15:02:51.092450      1 main.go:48] running the cyclictest command with arguments [-D 600 -p
```

```
1 -t 10 -a 2,4,6,8,10,54,56,58,60,62 -h 30 -i 1000 --quiet
```

```
10811 15:03:06.147253      1 main.go:54] succeeded to run the cyclictst command: #
```

```
/dev/cpu_dma_latency set to 0us
```

```
# Histogram
000000 000000 000000 000000 000000 000000 000000 000000 000000 000000 000000
000001 000000 005561 027778 037704 011987 000000 120755 238981 081847 300186
000002 587440 581106 564207 554323 577416 590635 474442 357940 513895 296033
000003 011751 011441 006449 006761 008409 007904 002893 002066 003349 003089
000004 000527 001079 000914 000712 001451 001120 000779 000283 000350 000251

More histogram entries ...
# Min Latencies: 00002 00001 00001 00001 00001 00002 00001 00001 00001 00001
# Avg Latencies: 00002 00002 00002 00001 00002 00002 00001 00001 00001 00001
# Max Latencies: 00018 00465 00361 00395 00208 00301 02052 00289 00327 00114 4
# Histogram Overflows: 00000 00220 00159 00128 00202 00017 00069 00059 00045 00120
# Histogram Overflow at cycle number:
# Thread 0:
# Thread 1: 01142 01439 05305 ... # 00190 others
# Thread 2: 20895 21351 30624 ... # 00129 others
# Thread 3: 01143 17921 18334 ... # 00098 others
# Thread 4: 30499 30622 31566 ... # 00172 others
# Thread 5: 145221 170910 171888 ...
# Thread 6: 01684 26291 30623 ...# 00039 others
# Thread 7: 28983 92112 167011 ... 00029 others
# Thread 8: 45766 56169 56171 ...# 00015 others
# Thread 9: 02974 08094 13214 ... # 00090 others
```

- 1 The docker arguments provided by the user.
- 2 The user is notified about the measured latency and the configured latency.
- 3 The arguments for the **cyclictest** command.
- 4 The maximum latencies measured on each thread.

16.7.8.3. Running oslat

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig -e
LATENCY_TEST_RUN=true -e DISCOVERY_MODE=true -e ROLE_WORKER_CNF=worker-cnf -e
LATENCY_TEST_CPUS=7 -e LATENCY_TEST_RUNTIME=600 -e MAXIMUM_LATENCY=20
registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-run.sh -ginkgo.focus="oslat"
```

The above command runs the **cyclictest** tool for 10 minutes (600 seconds). The test runs successfully when the maximum observed latency is lower than **MAXIMUM_LATENCY** (20 μ s), and the command line displays **SUCCESS!**.

Example failure output

```
$ docker run -v $KUBECONFIG:/root/kubeconfig:Z -e KUBECONFIG=/root/kubeconfig -e
IMAGE_REGISTRY=quay.io/titzhak -e CNF_TESTS_IMAGE=cnf-tests:latest -e
PERF_TEST_PROFILE=performance -e ROLE_WORKER_CNF=worker-cnf -e
LATENCY_TEST_RUN=true -e LATENCY_TEST_RUNTIME=600 -e DISCOVERY_MODE=true -e
MAXIMUM_LATENCY=20 -e LATENCY_TEST_CPUS=7 quay.io/titzhak/cnf-tests:latest /usr/bin/test-
run.sh -ginkgo.v -ginkgo.focus="oslat" 1

running /usr/bin/validationsuite -ginkgo.v -ginkgo.focus=oslat
10829 12:36:55.386776      8 request.go:668] Waited for 1.000303471s due to client-side throttling,
```

```
GET:https://api.cnfdc8.t5g.lab.eng.bos.redhat.com:6443/apis/authentication.k8s.io/v1?timeout=32s
```

```
running /usr/bin//cnftests -ginkgo.v -ginkgo.focus=oslat
```

not priority and fairness, request:

timeout=32s

Will run 1 of 142 specs

should succeed

STEP: Waiting two minutes to download the latencyTest image

Aug 29 12:37:59.324: [INFO]: found mcd machine-config-daemon-wf4w8 for node

[performance] Latency Test

with the oslat image

should succeed [It]

— 99 —

Expected

to be true

Running on machine: oslat-57c2g

Log line format: [IWEF]mmdd hh:mm:ss.uuuuuu threadid file:line] msg

```
(hd0,gpt3)/ostree/rhcos-
```

```
305.10.2.rt7.83.el8_4.x86_64 ip=dhcp random.trust_cpu=on console=tty0 console=ttyS0.115200n8
```

```
43/0 ignition.platform.id=openstack root=UUID=5a4ddf16-9372-44d9-ac4e-3ee329e16ab3 rw
```



```

rootflags=prjquota skew_tick=1 nohz=on rcu_nocbs=1-3
tuned.non_isolcpus=000000ff,ffffff,ffffff,ffffff1 intel_pstate=disable nosoftlockup tsc=nowatchdog
intel_iommu=on iommu=pt isolcpus=managed_irq,1-3
systemd.cpu_affinity=0,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,6
4,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,
97,98,99,100,101,102,103 default_hugepagesz=1G hugepagesz=2M hugepages=128
nmi_watchdog=0 audit=0 mce=off processor.max_cstate=1 idle=poll intel_idle.max_cstate=0
l0829 13:25:21.569345      1 node.go:44] Environment information: kernel version 4.18.0-
305.10.2.rt7.83.el8_4.x86_64
l0829 13:25:21.569367      1 main.go:53] Running the oslat command with arguments [--duration 600
--rtprio 1 --cpu-list 4,6,52,54,56,58 --cpu-main-thread 2] 3
l0829 13:35:22.632263      1 main.go:59] Succeeded to run the oslat command: oslat V 2.00
Total runtime: 600 seconds
Thread priority: SCHED_FIFO:1
CPU list: 4,6,52,54,56,58
CPU for main thread: 2
Workload: no
Workload mem: 0 (KiB)
Preheat cores: 6

Pre-heat for 1 seconds...
Test starts...
Test completed.

Core: 4 6 52 54 56 58
CPU Freq: 2096 2096 2096 2096 2096 2096 (Mhz)
001 (us): 19390720316 19141129810 20265099129 20280959461 19391991159 19119877333
002 (us): 5304 5249 5777 5947 6829 4971
003 (us): 28 14 434 47 208 21
004 (us): 1388 853 123568 152817 5576 0
005 (us): 207850 223544 103827 91812 227236 231563
006 (us): 60770 122038 277581 323120 122633 122357
007 (us): 280023 223992 63016 25896 214194 218395
008 (us): 40604 25152 24368 4264 24440 25115
009 (us): 6858 3065 5815 810 3286 2116
010 (us): 1947 936 1452 151 474 361
...
Minimum: 1 1 1 1 1 1 (us)
Average: 1.000 1.000 1.000 1.000 1.000 1.000 (us)
Maximum: 37 38 49 28 28 19 (us) 4
Max-Min: 36 37 48 27 27 18 (us)
Duration: 599.667 599.667 599.667 599.667 599.667 599.667 (sec)

```

1 3 The list of CPUs running the **oslat** command. Seven CPUs are provided through the **LATENCY_TEST_CPUS** variable. Only six CPUs are displayed in total because one is used to run the **oslat** tool.

2 The user is notified about the measured latency and the configured latency.

4 The maximum latency values in microseconds that are measured on each CPU.

16.7.9. Troubleshooting

The cluster must be reached from within the container. You can verify this by running:

```
$ docker run -v $(pwd)/:/kubeconfig -e KUBECONFIG=/kubeconfig/kubeconfig
registry.redhat.io/openshift-kni/cnf-tests oc get nodes
```

If this does not work, it could be caused by spanning across DNS, MTU size, or firewall issues.

16.7.10. Test reports

CNF end-to-end tests produce two outputs: a JUnit test output and a test failure report.

16.7.10.1. JUnit test output

A JUnit-compliant XML is produced by passing the **--junit** parameter together with the path where the report is dumped:

```
$ docker run -v $(pwd)/:/kubeconfig -v $(pwd)/junitdest:/path/to/junit -e
KUBECONFIG=/kubeconfig/kubeconfig registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-
run.sh --junit /path/to/junit
```

16.7.10.2. Test failure report

A report with information about the cluster state and resources for troubleshooting can be produced by passing the **--report** parameter with the path where the report is dumped:

```
$ docker run -v $(pwd)/:/kubeconfig -v $(pwd)/reportdest:/path/to/report -e
KUBECONFIG=/kubeconfig/kubeconfig registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-
run.sh --report /path/to/report
```

16.7.10.3. A note on podman

When executing podman as non root and non privileged, mounting paths can fail with "permission denied" errors. To make it work, append **:Z** to the volumes creation; for example, **-v \$(pwd)/:/kubeconfig:Z** to allow podman to do the proper SELinux relabeling.

16.7.10.4. Running on OpenShift Container Platform 4.4

With the exception of the following, the CNF end-to-end tests are compatible with OpenShift Container Platform 4.4:

```
[test_id:28466][crit:high][vendor:cnf-qe@redhat.com][level:acceptance] Should contain configuration
injected through openshift-node-performance profile
[test_id:28467][crit:high][vendor:cnf-qe@redhat.com][level:acceptance] Should contain configuration
injected through the openshift-node-performance profile
```

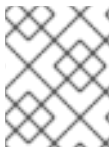
You can skip these tests by adding the **-ginkgo.skip "28466|28467"** parameter.

16.7.10.5. Using a single performance profile

The DPDK tests require more resources than what is required by the performance test suite. To make the execution faster, you can override the performance profile used by the tests using a profile that also serves the DPDK test suite.

To do this, use a profile like the following one that can be mounted inside the container, and the performance tests can be instructed to deploy it.

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: performance
spec:
  cpu:
    isolated: "5-15"
    reserved: "0-4"
  hugepages:
    defaultHugepagesSize: "1G"
  pages:
    - size: "1G"
      count: 16
      node: 0
  realTimeKernel:
    enabled: true
  numa:
    topologyPolicy: "best-effort"
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: ""
```



NOTE

When you configure reserved and isolated CPUs, the infra containers in pods use the reserved CPUs and the application containers use the isolated CPUs.

To override the performance profile, the manifest must be mounted inside the container and the tests must be instructed by setting the **PERFORMANCE_PROFILE_MANIFEST_OVERRIDE**:

```
$ docker run -v $(pwd)/:/kubeconfig:Z -e KUBECONFIG=/kubeconfig/kubeconfig -e
PERFORMANCE_PROFILE_MANIFEST_OVERRIDE=/kubeconfig/manifest.yaml
registry.redhat.io/openshift4/cnf-tests-rhel8:v4.9 /usr/bin/test-run.sh
```

16.8. DEBUGGING LOW LATENCY CNF TUNING STATUS

The **PerformanceProfile** custom resource (CR) contains status fields for reporting tuning status and debugging latency degradation issues. These fields report on conditions that describe the state of the operator's reconciliation functionality.

A typical issue can arise when the status of machine config pools that are attached to the performance profile are in a degraded state, causing the **PerformanceProfile** status to degrade. In this case, the machine config pool issues a failure message.

The Performance Addon Operator contains the **performanceProfile.spec.status.Conditions** status field:

```
Status:
Conditions:
  Last Heartbeat Time: 2020-06-02T10:01:24Z
  Last Transition Time: 2020-06-02T10:01:24Z
```

```

Status:      True
Type:        Available
Last Heartbeat Time: 2020-06-02T10:01:24Z
Last Transition Time: 2020-06-02T10:01:24Z
Status:      True
Type:        Upgradeable
Last Heartbeat Time: 2020-06-02T10:01:24Z
Last Transition Time: 2020-06-02T10:01:24Z
Status:      False
Type:        Progressing
Last Heartbeat Time: 2020-06-02T10:01:24Z
Last Transition Time: 2020-06-02T10:01:24Z
Status:      False
Type:        Degraded

```

The **Status** field contains **Conditions** that specify **Type** values that indicate the status of the performance profile:

Available

All machine configs and Tuned profiles have been created successfully and are available for cluster components are responsible to process them (NTO, MCO, Kubelet).

Upgradeable

Indicates whether the resources maintained by the Operator are in a state that is safe to upgrade.

Progressing

Indicates that the deployment process from the performance profile has started.

Degraded

Indicates an error if:

- Validation of the performance profile has failed.
- Creation of all relevant components did not complete successfully.

Each of these types contain the following fields:

Status

The state for the specific type (**true** or **false**).

Timestamp

The transaction timestamp.

Reason string

The machine readable reason.

Message string

The human readable reason describing the state and error details, if any.

16.8.1. Machine config pools

A performance profile and its created products are applied to a node according to an associated machine config pool (MCP). The MCP holds valuable information about the progress of applying the machine configurations created by performance addons that encompass kernel args, kube config, huge pages allocation, and deployment of rt-kernel. The performance addons controller monitors changes in the MCP and updates the performance profile status accordingly.

The only conditions returned by the MCP to the performance profile status is when the MCP is **Degraded**, which leads to **performanceProfile.status.condition.Degraded = true**.

Example

The following example is for a performance profile with an associated machine config pool (**worker-cnf**) that was created for it:

1. The associated machine config pool is in a degraded state:

```
# oc get mcp
```

Example output

```
NAME      CONFIG                                UPDATED  UPDATING  DEGRADED
MACHINECOUNT  READYMACHINECOUNT  UPDATEDMACHINECOUNT
DEGRADEDMACHINECOUNT  AGE
master     rendered-master-2ee57a93fa6c9181b546ca46e1571d2d  True  False
False  3      3      3      0      2d21h
worker     rendered-worker-d6b2bdc07d9f5a59a6b68950acf25e5f  True  False
False  2      2      2      0      2d21h
worker-cnf rendered-worker-cnf-6c838641b8a08ff08dbd8b02fb63f7c False  True
True  2      1      1      1      2d20h
```

2. The **describe** section of the MCP shows the reason:

```
# oc describe mcp worker-cnf
```

Example output

```
Message:      Node node-worker-cnf is reporting: "prepping update:
machineconfig.machineconfiguration.openshift.io \"rendered-worker-cnf-
40b9996919c08e335f3ff230ce1d170\" not
found"
Reason:      1 nodes are reporting degraded status on sync
```

3. The degraded state should also appear under the performance profile **status** field marked as **degraded = true**:

```
# oc describe performanceprofiles performance
```

Example output

```
Message: Machine config pool worker-cnf Degraded Reason: 1 nodes are reporting
degraded status on sync.
Machine config pool worker-cnf Degraded Message: Node yquinn-q8s5v-w-b-
z5lqn.c.openshift-gce-devel.internal is
reporting: "prepping update: machineconfig.machineconfiguration.openshift.io
\"rendered-worker-cnf-40b9996919c08e335f3ff230ce1d170\" not found". Reason:
MCPDegraded
Status: True
Type: Degraded
```

16.9. COLLECTING LOW LATENCY TUNING DEBUGGING DATA FOR RED HAT SUPPORT

When opening a support case, it is helpful to provide debugging information about your cluster to Red Hat Support.

The **must-gather** tool enables you to collect diagnostic information about your OpenShift Container Platform cluster, including node tuning, NUMA topology, and other information needed to debug issues with low latency setup.

For prompt support, supply diagnostic information for both OpenShift Container Platform and low latency tuning.

16.9.1. About the must-gather tool

The **oc adm must-gather** CLI command collects the information from your cluster that is most likely needed for debugging issues, such as:

- Resource definitions
- Audit logs
- Service logs

You can specify one or more images when you run the command by including the **--image** argument. When you specify an image, the tool collects data related to that feature or product. When you run **oc adm must-gather**, a new pod is created on the cluster. The data is collected on that pod and saved in a new directory that starts with **must-gather.local**. This directory is created in your current working directory.

16.9.2. About collecting low latency tuning data

Use the **oc adm must-gather** CLI command to collect information about your cluster, including features and objects associated with low latency tuning, including:

- The Performance Addon Operator namespaces and child objects.
- **MachineConfigPool** and associated **MachineConfig** objects.
- The Node Tuning Operator and associated Tuned objects.
- Linux Kernel command line options.
- CPU and NUMA topology
- Basic PCI device information and NUMA locality.

To collect Performance Addon Operator debugging information with **must-gather**, you must specify the Performance Addon Operator **must-gather** image:

```
--image=registry.redhat.io/openshift4/performance-addon-operator-must-gather-rhel8:v4.9.
```

16.9.3. Gathering data about specific features

You can gather debugging information about specific features by using the **oc adm must-gather** CLI command with the **--image** or **--image-stream** argument. The **must-gather** tool supports multiple images, so you can gather data about more than one feature by running a single command.



NOTE

To collect the default **must-gather** data in addition to specific feature data, add the **--image-stream=openshift/must-gather** argument.

Prerequisites

- Access to the cluster as a user with the **cluster-admin** role.
- The OpenShift Container Platform CLI (oc) installed.

Procedure

1. Navigate to the directory where you want to store the **must-gather** data.
2. Run the **oc adm must-gather** command with one or more **--image** or **--image-stream** arguments. For example, the following command gathers both the default cluster data and information specific to the Performance Addon Operator:

```
$ oc adm must-gather \
  --image-stream=openshift/must-gather \ 1
  --image=registry.redhat.io/openshift4/performance-addon-operator-must-gather-rhel8:v4.9 2
```

1 The default OpenShift Container Platform **must-gather** image.

2 The **must-gather** image for low latency tuning diagnostics.

3. Create a compressed file from the **must-gather** directory that was created in your working directory. For example, on a computer that uses a Linux operating system, run the following command:

```
$ tar cvaf must-gather.tar.gz must-gather.local.5421342344627712289/ 1
```

1 Replace **must-gather-local.5421342344627712289/** with the actual directory name.

4. Attach the compressed file to your support case on the [Red Hat Customer Portal](#).

Additional resources

- For more information about MachineConfig and KubeletConfig, see [Managing nodes](#).
- For more information about the Node Tuning Operator, see [Using the Node Tuning Operator](#).
- For more information about the PerformanceProfile, see [Configuring huge pages](#).
- For more information about consuming huge pages from your containers, see [How huge pages are consumed by apps](#).

CHAPTER 17. CREATING A PERFORMANCE PROFILE

Learn about the Performance Profile Creator (PPC) and how you can use it to create a performance profile.

17.1. ABOUT THE PERFORMANCE PROFILE CREATOR

The Performance Profile Creator (PPC) is a command-line tool, delivered with the Performance Addon Operator, used to create the performance profile. The tool consumes **must-gather** data from the cluster and several user-supplied profile arguments. The PPC generates a performance profile that is appropriate for your hardware and topology.

The tool is run by one of the following methods:

- Invoking **podman**
- Calling a wrapper script

17.1.1. Gathering data about your cluster using **must-gather**

The Performance Profile Creator (PPC) tool requires **must-gather** data. As a cluster administrator, run **must-gather** to capture information about your cluster.

Prerequisites

- Access to the cluster as a user with the **cluster-admin** role.
- Access to the Performance Addon Operator image.
- The OpenShift CLI (**oc**) installed.

Procedure

1. Navigate to the directory where you want to store the **must-gather** data.
2. Run **must-gather** on your cluster:

```
$ oc adm must-gather --image=<PAO_image> --dest-dir=<dir>
```



NOTE

must-gather must be run with the **performance-addon-operator-must-gather** image. The output can optionally be compressed. Compressed output is required if you are running the Performance Profile Creator wrapper script.

Example

```
$ oc adm must-gather --image=registry.redhat.io/openshift4/performance-addon-operator-must-gather-rhel8:v4.9 --dest-dir=must-gather
```

3. Create a compressed file from the **must-gather** directory:

```
$ tar cvaf must-gather.tar.gz must-gather/
```


17.1.2. Running the Performance Profile Creator using podman

As a cluster administrator, you can run **podman** and the Performance Profile Creator to create a performance profile.

Prerequisites

- Access to the cluster as a user with the **cluster-admin** role.
- A cluster installed on bare metal hardware.
- A node with **podman** and OpenShift CLI (**oc**) installed.

Procedure

1. Check the machine config pool:

```
$ oc get mcp
```

Example output

NAME	CONFIG	UPDATED	UPDATING	DEGRADED
MACHINECOUNT	READYMACHINECOUNT	UPDATEDMACHINECOUNT		
DEGRADEDMACHINECOUNT	AGE			
master	rendered-master-acd1358917e9f98cbdb599aea622d78b	True	False	
False 3	3	3	0	22h
worker-cnf	rendered-worker-cnf-1d871ac76e1951d32b2fe92369879826	False	True	
False 2	1	1	0	22h

2. Use Podman to authenticate to **registry.redhat.io**:

```
$ podman login registry.redhat.io
```

```
Username: myrhusername
Password: *****
```

3. Optional: Display help for the PPC tool:

```
$ podman run --entrypoint performance-profile-creator
registry.redhat.io/openshift4/performance-addon-rhel8-operator:v4.9 -h
```

Example output

A tool that automates creation of Performance Profiles

Usage:
performance-profile-creator [flags]

Flags:

--disable-ht	Disable Hyperthreading
-h, --help	help for performance-profile-creator

<code>--info string</code>	Show cluster information; requires <code>--must-gather-dir-path</code> , ignore the other arguments. [Valid values: log, json] (default "log")
<code>--mcp-name string</code> (required)	MCP name corresponding to the target machines
<code>--must-gather-dir-path string</code>	Must gather directory path (default "must-gather")
<code>--power-consumption-mode string</code>	The power consumption mode. [Valid values: default, low-latency, ultra-low-latency] (default "default")
<code>--profile-name string</code>	Name of the performance profile to be created (default "performance")
<code>--reserved-cpu-count int</code>	Number of reserved CPUs (required)
<code>--rt-kernel</code>	Enable Real Time Kernel (required)
<code>--split-reserved-cpus-across-numa</code>	Split the Reserved CPUs across NUMA nodes
<code>--topology-manager-policy string</code>	Kubelet Topology Manager Policy of the performance profile to be created. [Valid values: single-numa-node, best-effort, restricted] (default "restricted")
<code>--user-level-networking</code>	Run with User level Networking(DPDK) enabled

4. Run the Performance Profile Creator tool in discovery mode:



NOTE

Discovery mode inspects your cluster using the output from **must-gather**. The output produced includes information on:

- The NUMA cell partitioning with the allocated CPU ids
- Whether hyperthreading is enabled

Using this information you can set appropriate values for some of the arguments supplied to the Performance Profile Creator tool.

```
$ podman run --entrypoint performance-profile-creator -v /must-gather:/must-gather:z
registry.redhat.io/openshift4/performance-addon-rhel8-operator:v4.9 --info log --must-gather-
dir-path /must-gather
```



NOTE

This command uses the performance profile creator as a new entry point to **podman**. It maps the **must-gather** data for the host into the container image and invokes the required user-supplied profile arguments to produce the **my-performance-profile.yaml** file.

The **-v** option can be the path to either:

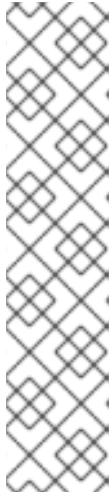
- The **must-gather** output directory
- An existing directory containing the **must-gather** decompressed tarball

The **info** option requires a value which specifies the output format. Possible values are log and JSON. The JSON format is reserved for debugging.

5. Run **podman**:

```
$ podman run --entrypoint performance-profile-creator -v /must-gather:/must-gather:z
```

```
registry.redhat.io/openshift4/performance-addon-rhel8-operator:v4.9 --mcp-name=worker-cnf
--reserved-cpu-count=20 --rt-kernel=true --split-reserved-cpus-across-numa=false --topology-
manager-policy=single-numa-node --must-gather-dir-path /must-gather --power-
consumption-mode=ultra-low-latency > my-performance-profile.yaml
```



NOTE

The Performance Profile Creator arguments are shown in the Performance Profile Creator arguments table. The following arguments are required:

- **reserved-cpu-count**
- **mcp-name**
- **rt-kernel**

The **mcp-name** argument in this example is set to **worker-cnf** based on the output of the command **oc get mcp**. For Single Node OpenShift (SNO) use **--mcp-name=master**.

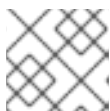
6. Review the created YAML file:

```
$ cat my-performance-profile.yaml
```

Example output

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: performance
spec:
  additionalKernelArgs:
    - nmi_watchdog=0
    - audit=0
    - mce=off
    - processor.max_cstate=1
    - intel_idle.max_cstate=0
    - idle=poll
  cpu:
    isolated: 1,3,5,7,9,11,13,15,17,19-39,41,43,45,47,49,51,53,55,57,59-79
    reserved: 0,2,4,6,8,10,12,14,16,18,40,42,44,46,48,50,52,54,56,58
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: ""
  numa:
    topologyPolicy: single-numa-node
  realTimeKernel:
    enabled: true
```

7. Apply the generated profile:



NOTE

Install the Performance Addon Operator before applying the profile.

```
$ oc apply -f my-performance-profile.yaml
```

17.1.2.1. How to run **podman** to create a performance profile

The following example illustrates how to run **podman** to create a performance profile with 20 reserved CPUs that are to be split across the NUMA nodes.

Node hardware configuration:

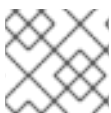
- 80 CPUs
- Hyperthreading enabled
- Two NUMA nodes
- Even numbered CPUs run on NUMA node 0 and odd numbered CPUs run on NUMA node 1

Run **podman** to create the performance profile:

```
$ podman run --entrypoint performance-profile-creator -v /must-gather:/must-gather:z
registry.redhat.io/openshift4/performance-addon-rhel8-operator:v4.9 --mcp-name=worker-cnf --
reserved-cpu-count=20 --rt-kernel=true --split-reserved-cpus-across-numa=true --must-gather-dir-
path /must-gather > my-performance-profile.yaml
```

The created profile is described in the following YAML:

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: performance
spec:
  cpu:
    isolated: 10-39,50-79
    reserved: 0-9,40-49
  nodeSelector:
    node-role.kubernetes.io/worker-cnf: ""
  numa:
    topologyPolicy: restricted
  realTimeKernel:
    enabled: true
```



NOTE

In this case, 10 CPUs are reserved on NUMA node 0 and 10 are reserved on NUMA node 1.

17.1.3. Running the Performance Profile Creator wrapper script

The performance profile wrapper script simplifies the running of the Performance Profile Creator (PPC) tool. It hides the complexities associated with running **podman** and specifying the mapping directories and it enables the creation of the performance profile.

Prerequisites

- Access to the Performance Addon Operator image.

- Access to the **must-gather** tarball.

Procedure

1. Create a file on your local machine named, for example, **run-perf-profile-creator.sh**:

```
$ vi run-perf-profile-creator.sh
```

2. Paste the following code into the file:

```
#!/bin/bash

readonly CONTAINER_RUNTIME=${CONTAINER_RUNTIME:-podman}
readonly CURRENT_SCRIPT=$(basename "$0")
readonly CMD="${CONTAINER_RUNTIME} run --entrypoint performance-profile-creator"
readonly IMG_EXISTS_CMD="${CONTAINER_RUNTIME} image exists"
readonly IMG_PULL_CMD="${CONTAINER_RUNTIME} image pull"
readonly MUST_GATHER_VOL="/must-gather"

PAO_IMG="registry.redhat.io/openshift4/performance-addon-rhel8-operator:v4.9"
MG_TARBALL=""
DATA_DIR=""

usage() {
    print "Wrapper usage:"
    print "  ${CURRENT_SCRIPT} [-h] [-p image][-t path] -- [performance-profile-creator flags]"
    print ""
    print "Options:"
    print "  -h          help for ${CURRENT_SCRIPT}"
    print "  -p          Performance Addon Operator image"
    print "  -t          path to a must-gather tarball"

    ${IMG_EXISTS_CMD} "${PAO_IMG}" && ${CMD} "${PAO_IMG}" -h
}

function cleanup {
    [ -d "${DATA_DIR}" ] && rm -rf "${DATA_DIR}"
}
trap cleanup EXIT

exit_error() {
    print "error: $"
    usage
    exit 1
}

print() {
    echo "$*" >&2
}

check_requirements() {
    ${IMG_EXISTS_CMD} "${PAO_IMG}" || ${IMG_PULL_CMD} "${PAO_IMG}" || \
        exit_error "Performance Addon Operator image not found"

    [ -n "${MG_TARBALL}" ] || exit_error "Must-gather tarball file path is mandatory"
```

```

[ -f "${MG_TARBALL}" ] || exit_error "Must-gather tarball file not found"

DATA_DIR=$(mktemp -d -t "${CURRENT_SCRIPT}XXXX") || exit_error "Cannot create the
data directory"
tar -zxf "${MG_TARBALL}" --directory "${DATA_DIR}" || exit_error "Cannot decompress the
must-gather tarball"
chmod a+rx "${DATA_DIR}"

return 0
}

main() {
while getopts 'hp:t:' OPT; do
case "${OPT}" in
h)
usage
exit 0
;;
p)
PAO_IMG="${OPTARG}"
;;
t)
MG_TARBALL="${OPTARG}"
;;
?)
exit_error "invalid argument: ${OPTARG}"
;;
esac
done
shift $((OPTIND - 1))

check_requirements || exit 1

${CMD} -v "${DATA_DIR}:${MUST_GATHER_VOL}:z" "${PAO_IMG}" "$@" --must-gather-
dir-path "${MUST_GATHER_VOL}"
echo "" 1>&2
}

main "$@"

```

3. Add execute permissions for everyone on this script:

```
$ chmod a+x run-perf-profile-creator.sh
```

4. Optional: Display the **run-perf-profile-creator.sh** command usage:

```
$ ./run-perf-profile-creator.sh -h
```

Expected output

```

Wrapper usage:
run-perf-profile-creator.sh [-h] [-p image][ -t path] -- [performance-profile-creator flags]

Options:
-h                help for run-perf-profile-creator.sh

```

- p Performance Addon Operator image **1**
- t path to a must-gather tarball **2**

A tool that automates creation of Performance Profiles

Usage:

performance-profile-creator [flags]

Flags:

- disable-ht Disable Hyperthreading
- h, --help help for performance-profile-creator
- info string Show cluster information; requires --must-gather-dir-path, ignore the other arguments. [Valid values: log, json] (default "log")
- mcp-name string MCP name corresponding to the target machines (required)
- must-gather-dir-path string Must gather directory path (default "must-gather")
- power-consumption-mode string The power consumption mode. [Valid values: default, low-latency, ultra-low-latency] (default "default")
- profile-name string Name of the performance profile to be created (default "performance")
- reserved-cpu-count int Number of reserved CPUs (required)
- rt-kernel Enable Real Time Kernel (required)
- split-reserved-cpus-across-numa Split the Reserved CPUs across NUMA nodes
- topology-manager-policy string Kubelet Topology Manager Policy of the performance profile to be created. [Valid values: single-numa-node, best-effort, restricted] (default "restricted")
- user-level-networking Run with User level Networking(DPDK) enabled



NOTE

There two types of arguments:

- Wrapper arguments namely **-h**, **-p** and **-t**
- PPC arguments

1 Optional: Specify the Performance Addon Operator image. If not set, the default upstream image is used: **registry.redhat.io/openshift4/performance-addon-rhel8-operator:v4.9**.

2 **-t** is a required wrapper script argument and specifies the path to a **must-gather** tarball.

5. Run the performance profile creator tool in discovery mode:



NOTE

Discovery mode inspects your cluster using the output from **must-gather**. The output produced includes information on:

- The NUMA cell partitioning with the allocated CPU IDs
- Whether hyperthreading is enabled

Using this information you can set appropriate values for some of the arguments supplied to the Performance Profile Creator tool.

```
$ ./run-perf-profile-creator.sh -t /must-gather/must-gather.tar.gz -- --info=log
```



NOTE

The **info** option requires a value which specifies the output format. Possible values are log and JSON. The JSON format is reserved for debugging.

- Check the machine config pool:

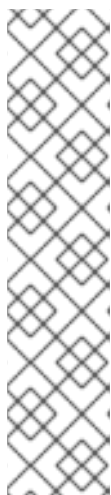
```
$ oc get mcp
```

Example output

NAME	CONFIG	UPDATED	UPDATING	DEGRADED
MACHINECOUNT	READYMACHINECOUNT	UPDATEDMACHINECOUNT		
DEGRADEDMACHINECOUNT	AGE			
master	rendered-master-acd1358917e9f98cbdb599aea622d78b	True	False	
False	3 3 3 0	22h		
worker-cnf	rendered-worker-cnf-1d871ac76e1951d32b2fe92369879826	False	True	
False	2 1 1 0	22h		

- Create a performance profile:

```
$ ./run-perf-profile-creator.sh -t /must-gather/must-gather.tar.gz -- --mcp-name=worker-cnf --reserved-cpu-count=2 --rt-kernel=true > my-performance-profile.yaml
```



NOTE

The Performance Profile Creator arguments are shown in the Performance Profile Creator arguments table. The following arguments are required:

- **reserved-cpu-count**
- **mcp-name**
- **rt-kernel**

The **mcp-name** argument in this example is set to **worker-cnf** based on the output of the command **oc get mcp**. For Single Node OpenShift (SNO) use **--mcp-name=master**.

- Review the created YAML file:

```
$ cat my-performance-profile.yaml
```

Example output

```
apiVersion: performance.openshift.io/v2
kind: PerformanceProfile
metadata:
  name: performance
spec:
```

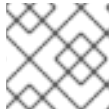


```

cpu:
  isolated: 1-39,41-79
  reserved: 0,40
nodeSelector:
  node-role.kubernetes.io/worker-cnf: ""
numa:
  topologyPolicy: restricted
realTimeKernel:
  enabled: false

```

9. Apply the generated profile:




NOTE


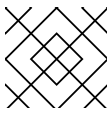
Install the Performance Addon Operator before applying the profile.

```
$ oc apply -f my-performance-profile.yaml
```

17.1.4. Performance Profile Creator arguments

Table 17.1. Performance Profile Creator arguments

Argument	Description
disable-ht	<p>Disable hyperthreading.</p> <p>Possible values: true or false.</p> <p>Default: false.</p> <div>  <p>WARNING</p> <p>If this argument is set to true you should not disable hyperthreading in the BIOS. Disabling hyperthreading is accomplished with a kernel command line argument.</p> </div>

Argument	Description
info	<p>This captures cluster information and is used in discovery mode only. Discovery mode also requires the must-gather-dir-path argument. If any other arguments are set they are ignored.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • log • JSON <div>  <div> <p>NOTE</p> <p>These options define the output format with the JSON format being reserved for debugging.</p> </div> </div> <p>Default: log.</p>
mcp-name	<p>MCP name for example worker-cnf corresponding to the target machines. This parameter is required.</p>
must-gather-dir-path	<p>Must gather directory path. This parameter is required.</p> <p>When the user runs the tool with the wrapper script must-gather is supplied by the script itself and the user must not specify it.</p>
power-consumption-mode	<p>The power consumption mode.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • default • low-latency • ultra-low-latency <p>Default: default.</p>
profile-name	<p>Name of the performance profile to create. Default: performance.</p>
reserved-cpu-count	<p>Number of reserved CPUs. This parameter is required.</p> <div>  <div> <p>NOTE</p> <p>This must be a natural number. A value of 0 is not allowed.</p> </div> </div>

Argument	Description
rt-kernel	<p>Enable real-time kernel. This parameter is required.</p> <p>Possible values: true or false.</p>
split-reserved-cpus-across-numa	<p>Split the reserved CPUs across NUMA nodes.</p> <p>Possible values: true or false.</p> <p>Default: false.</p>
topology-manager-policy	<p>Kubelet Topology Manager policy of the performance profile to be created.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • single-numa-node • best-effort • restricted <p>Default: restricted.</p>
user-level-networking	<p>Run with user level networking (DPDK) enabled.</p> <p>Possible values: true or false.</p> <p>Default: false.</p>

17.2. ADDITIONAL RESOURCES

- For more information about the **must-gather** tool, see [Gathering data about your cluster](#).

CHAPTER 18. DEPLOYING DISTRIBUTED UNITS AT SCALE IN A DISCONNECTED ENVIRONMENT

Use zero touch provisioning (ZTP) to provision distributed units at new edge sites in a disconnected environment. The workflow starts when the site is connected to the network and ends with the CNF workload deployed and running on the site nodes.



IMPORTANT

ZTP for RAN deployments 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/>.

18.1. PROVISIONING EDGE SITES AT SCALE

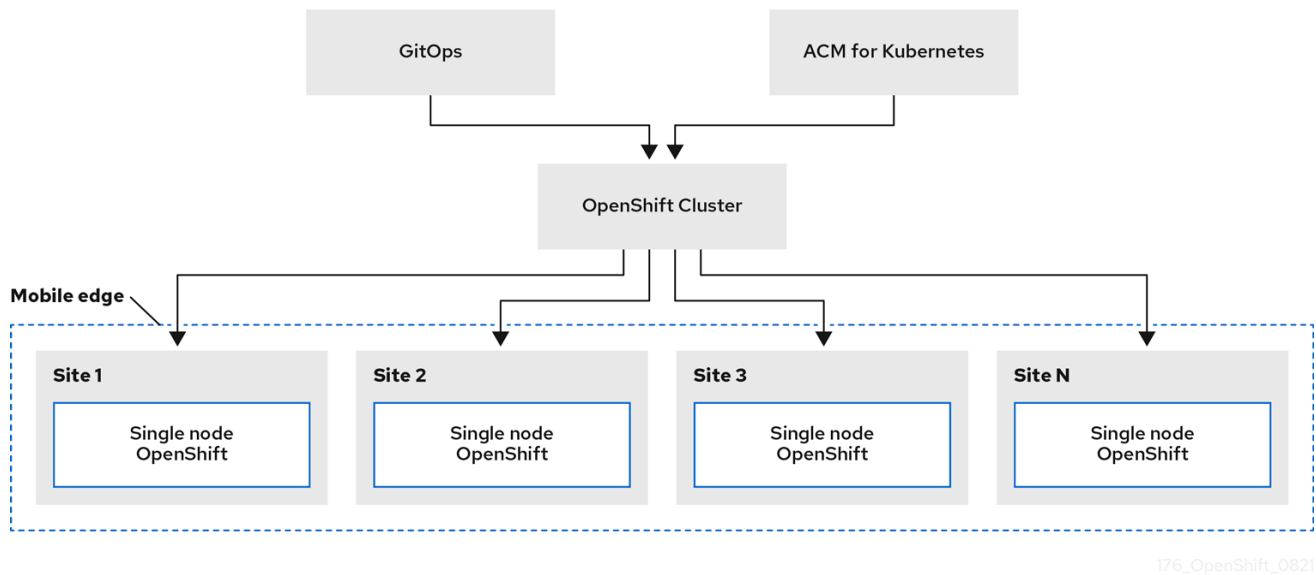
Telco edge computing presents extraordinary challenges with managing hundreds to tens of thousands of clusters in hundreds of thousands of locations. These challenges require fully-automated management solutions with, as closely as possible, zero human interaction.

Zero touch provisioning (ZTP) allows you to provision new edge sites with declarative configurations of bare-metal equipment at remote sites. Template or overlay configurations install OpenShift Container Platform features that are required for CNF workloads. End-to-end functional test suites are used to verify CNF related features. All configurations are declarative in nature.

You start the workflow by creating declarative configurations for ISO images that are delivered to the edge nodes to begin the installation process. The images are used to repeatedly provision large numbers of nodes efficiently and quickly, allowing you keep up with requirements from the field for far edge nodes.

Service providers are deploying a more distributed mobile network architecture allowed by the modular functional framework defined for 5G. This allows service providers to move from appliance-based radio access networks (RAN) to open cloud RAN architecture, gaining flexibility and agility in delivering services to end users.

The following diagram shows how ZTP works within a far edge framework.



18.2. THE GITOPS APPROACH

ZTP uses the GitOps deployment set of practices for infrastructure deployment that allows developers to perform tasks that would otherwise fall under the purview of IT operations. GitOps achieves these tasks using declarative specifications stored in Git repositories, such as YAML files and other defined patterns, that provide a framework for deploying the infrastructure. The declarative output is leveraged by the Open Cluster Manager (OCM) for multisite deployment.

One of the motivators for a GitOps approach is the requirement for reliability at scale. This is a significant challenge that GitOps helps solve.

GitOps addresses the reliability issue by providing traceability, RBAC, and a single source of truth for the desired state of each site. Scale issues are addressed by GitOps providing structure, tooling, and event driven operations through webhooks.

18.3. ABOUT ZTP AND DISTRIBUTED UNITS ON SINGLE NODES

You can install a distributed unit (DU) on a single node at scale with Red Hat Advanced Cluster Management (RHACM) (ACM) using the assisted installer (AI) and the policy generator with core-reduction technology enabled. The DU installation is done using zero touch provisioning (ZTP) in a disconnected environment.

ACM manages clusters in a hub and spoke architecture, where a single hub cluster manages many spoke clusters. ACM applies radio access network (RAN) policies from predefined custom resources (CRs). Hub clusters running ACM provision and deploy the spoke clusters using ZTP and AI. DU installation follows the AI installation of OpenShift Container Platform on a single node.

The AI service handles provisioning of OpenShift Container Platform on single nodes running on bare metal. ACM ships with and deploys the assisted installer when the **MultiClusterHub** custom resource is installed.

With ZTP and AI, you can provision OpenShift Container Platform single nodes to run your DUs at scale. A high level overview of ZTP for distributed units in a disconnected environment is as follows:

- A hub cluster running ACM manages a disconnected internal registry that mirrors the OpenShift Container Platform release images. The internal registry is used to provision the spoke single nodes.

- You manage the bare metal host machines for your DUs in an inventory file that uses YAML for formatting. You store the inventory file in a Git repository.
- You install the DU bare metal host machines on site, and make the hosts ready for provisioning. To be ready for provisioning, the following is required for each bare metal host:
 - Network connectivity - including DNS for your network. Hosts should be reachable through the hub and managed spoke clusters. Ensure there is layer 3 connectivity between the hub and the host where you want to install your hub cluster.
 - Baseboard Management Controller (BMC) details for each host - ZTP uses BMC details to connect the URL and credentials for accessing the BMC. Create spoke cluster definition CRs. These define the relevant elements for the managed clusters. Required CRs are as follows:

Custom Resource	Description
Namespace	Namespace for the managed single node cluster.
BMCSecret CR	Credentials for the host BMC.
Image Pull Secret CR	Pull secret for the disconnected registry.
AgentClusterInstall	Specifies the single node cluster's configuration such as networking, number of supervisor (control plane) nodes, and so on.
ClusterDeployment	Defines the cluster name, domain, and other details.
KlusterletAddonConfig	Manages installation and termination of add-ons on the ManagedCluster for ACM.
ManagedCluster	Describes the managed cluster for ACM.
InfraEnv	Describes the installation ISO to be mounted on the destination node that the assisted installer service creates. This is the final step of the manifest creation phase.
BareMetalHost	Describes the details of the bare metal host, including BMC and credentials details.

- When a change is detected in the host inventory repository, a host management event is triggered to provision the new or updated host.
- The host is provisioned. When the host is provisioned and successfully rebooted, the host agent reports **Ready** status to the hub cluster.

18.4. ZERO TOUCH PROVISIONING BUILDING BLOCKS

ACM deploys single node OpenShift (SNO), which is OpenShift Container Platform installed on single nodes, leveraging zero touch provisioning (ZTP). The initial site plan is broken down into smaller components and initial configuration data is stored in a Git repository. Zero touch provisioning uses a declarative GitOps approach to deploy these nodes. The deployment of the nodes includes:

- Installing the host operating system (RHCOS) on a blank server.
- Deploying OpenShift Container Platform on single nodes.
- Creating cluster policies and site subscriptions.
- Leveraging a GitOps deployment topology for a develop once, deploy anywhere model.
- Making the necessary network configurations to the server operating system.
- Deploying profile Operators and performing any needed software-related configuration, such as performance profile, PTP, and SR-IOV.
- Downloading images needed to run workloads (CNFs).

18.5. SINGLE NODE CLUSTERS

You use zero touch provisioning (ZTP) to deploy single node clusters to run distributed units (DUs) on small hardware footprints at disconnected far edge sites. A single node cluster runs OpenShift Container Platform on top of one bare metal machine, hence the single node. Edge servers contain a single node with supervisor functions and worker functions on the same host that are deployed at low bandwidth or disconnected edge sites.

OpenShift Container Platform is configured on the single node to use workload partitioning. Workload partitioning separates cluster management workloads from user workloads and can run the cluster management workloads on a reserved set of CPUs. Workload partitioning is useful for resource-constrained environments, such as single-node production deployments, where you want to reserve most of the CPU resources for user workloads and configure OpenShift Container Platform to use fewer CPU resources within the host.

A single node cluster hosting a DU application on a node is divided into the following configuration categories:

- Common - Values are the same for all single node cluster sites managed by a hub cluster.
- Pools of sites - Common across a pool of sites where a pool size can be 1 to n .
- Site specific - Likely specific to a site with no overlap with other sites, for example, a vlan.

18.6. SITE PLANNING CONSIDERATIONS FOR DISTRIBUTED UNIT DEPLOYMENTS

Site planning for distributed units (DU) deployments is complex. The following is an overview of the tasks that you complete before the DU hosts are brought online in the production environment.

- Develop a network model. The network model depends on various factors such as the size of the area of coverage, number of hosts, projected traffic load, DNS, and DHCP requirements.
- Decide how many DU radio nodes are required to provide sufficient coverage and redundancy for your network.

- Develop mechanical and electrical specifications for the DU host hardware.
- Develop a construction plan for individual DU site installations.
- Tune host BIOS settings for production, and deploy the BIOS configuration to the hosts.
- Install the equipment on-site, connect hosts to the network, and apply power.
- Configure on-site switches and routers.
- Perform basic connectivity tests for the host machines.
- Establish production network connectivity, and verify host connections to the network.
- Provision and deploy on-site DU hosts at scale.
- Test and verify on-site operations, performing load and scale testing of the DU hosts before finally bringing the DU infrastructure online in the live production environment.

18.7. LOW LATENCY FOR DISTRIBUTED UNITS (DUS)

Low latency is an integral part of the development of 5G networks. Telecommunications networks require as little signal delay as possible to ensure quality of service in a variety of critical use cases.

Low latency processing is essential for any communication with timing constraints that affect functionality and security. For example, 5G Telco applications require a guaranteed one millisecond one-way latency to meet Internet of Things (IoT) requirements. Low latency is also critical for the future development of autonomous vehicles, smart factories, and online gaming. Networks in these environments require almost a real-time flow of data.

Low latency systems are about guarantees with regards to response and processing times. This includes keeping a communication protocol running smoothly, ensuring device security with fast responses to error conditions, or just making sure a system is not lagging behind when receiving a lot of data. Low latency is key for optimal synchronization of radio transmissions.

OpenShift Container Platform enables low latency processing for DUs running on COTS hardware by using a number of technologies and specialized hardware devices:

Real-time kernel for RHCOS

Ensures workloads are handled with a high degree of process determinism.

CPU isolation

Avoids CPU scheduling delays and ensures CPU capacity is available consistently.

NUMA awareness

Aligns memory and huge pages with CPU and PCI devices to pin guaranteed container memory and huge pages to the NUMA node. This decreases latency and improves performance of the node.

Huge pages memory management

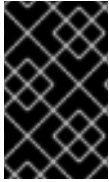
Using huge page sizes improves system performance by reducing the amount of system resources required to access page tables.

Precision timing synchronization using PTP

Allows synchronization between nodes in the network with sub-microsecond accuracy.

18.8. CONFIGURING BIOS FOR DISTRIBUTED UNIT BARE-METAL HOSTS

Distributed unit (DU) hosts require the BIOS to be configured before the host can be provisioned. The BIOS configuration is dependent on the specific hardware that runs your DUs and the particular requirements of your installation.

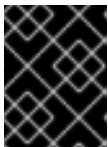


IMPORTANT

In this Developer Preview release, configuration and tuning of BIOS for DU bare-metal host machines is the responsibility of the customer. Automatic setting of BIOS is not handled by the zero touch provisioning workflow.

Procedure

1. Set the **UEFI/BIOS Boot Mode** to **UEFI**.
2. In the host boot sequence order, set **Hard drive first**
3. Apply the specific BIOS configuration for your hardware. The following table describes a representative BIOS configuration for an Intel Xeon Skylake or Intel Cascade Lake server, based on the Intel FlexRAN 4G and 5G baseband PHY reference design.



IMPORTANT

The exact BIOS configuration depends on your specific hardware and network requirements. The following sample configuration is for illustrative purposes only.

Table 18.1. Sample BIOS configuration for an Intel Xeon Skylake or Cascade Lake server

BIOS Setting	Configuration
CPU Power and Performance Policy	Performance
Uncore Frequency Scaling	Disabled
Performance P-limit	Disabled
Enhanced Intel SpeedStep [®] Tech	Enabled
Intel Configurable TDP	Enabled
Configurable TDP Level	Level 2
Intel [®] Turbo Boost Technology	Enabled
Energy Efficient Turbo	Disabled
Hardware P-States	Disabled

BIOS Setting	Configuration
Package C-State	C0/C1 state
C1E	Disabled
Processor C6	Disabled

**NOTE**

Enable global SR-IOV and VT-d settings in the BIOS for the host. These settings are relevant to bare-metal environments.

18.9. PREPARING THE DISCONNECTED ENVIRONMENT

Before you can provision distributed units (DU) at scale, you must install Red Hat Advanced Cluster Management (RHACM), which handles the provisioning of the DUs.

RHACM is deployed as an Operator on the OpenShift Container Platform hub cluster. It controls clusters and applications from a single console with built-in security policies. RHACM provisions and manage your DU hosts. To install RHACM in a disconnected environment, you create a mirror registry that mirrors the Operator Lifecycle Manager (OLM) catalog that contains the required Operator images. OLM manages, installs, and upgrades Operators and their dependencies in the cluster.

You also use a disconnected mirror host to serve the RHCOS ISO and RootFS disk images that provision the DU bare-metal host operating system.

Before you install a cluster on infrastructure that you provision in a restricted network, you must mirror the required container images into that environment. You can also use this procedure in unrestricted networks to ensure your clusters only use container images that have satisfied your organizational controls on external content.

**IMPORTANT**

You must have access to the internet to obtain the necessary container images. In this procedure, you place the mirror registry on a mirror host that has access to both your network and the internet. If you do not have access to a mirror host, use the disconnected procedure to copy images to a device that you can move across network boundaries.

18.9.1. Disconnected environment prerequisites

You must have a container image registry that supports [Docker v2-2](#) in the location that will host the OpenShift Container Platform cluster, such as one of the following registries:

- [Red Hat Quay](#)
- [JFrog Artifactory](#)
- [Sonatype Nexus Repository](#)
- [Harbor](#)

If you have an entitlement to Red Hat Quay, see the documentation on deploying Red Hat Quay [for proof-of-concept purposes](#) or [by using the Quay Operator](#). If you need additional assistance selecting and installing a registry, contact your sales representative or Red Hat support.

18.9.2. About the mirror registry

You can mirror the images that are required for OpenShift Container Platform installation and subsequent product updates to a container mirror registry such as Red Hat Quay, JFrog Artifactory, Sonatype Nexus Repository, or Harbor. If you do not have access to a large-scale container registry, you can use the *mirror registry for Red Hat OpenShift*, a small-scale container registry included with OpenShift Container Platform subscriptions.

You can use any container registry that supports [Docker v2-2](#), such as Red Hat Quay, the *mirror registry for Red Hat OpenShift*, Artifactory, Sonatype Nexus Repository, or Harbor. Regardless of your chosen registry, the procedure to mirror content from Red Hat hosted sites on the internet to an isolated image registry is the same. After you mirror the content, you configure each cluster to retrieve this content from your mirror registry.



IMPORTANT

The internal registry of the OpenShift Container Platform cluster cannot be used as the target registry because it does not support pushing without a tag, which is required during the mirroring process.

If choosing a container registry that is not the *mirror registry for Red Hat OpenShift*, it must be reachable by every machine in the clusters that you provision. If the registry is unreachable, installation, updating, or normal operations such as workload relocation might fail. For that reason, you must run mirror registries in a highly available way, and the mirror registries must at least match the production availability of your OpenShift Container Platform clusters.

When you populate your mirror registry with OpenShift Container Platform images, you can follow two scenarios. If you have a host that can access both the internet and your mirror registry, but not your cluster nodes, you can directly mirror the content from that machine. This process is referred to as *connected mirroring*. If you have no such host, you must mirror the images to a file system and then bring that host or removable media into your restricted environment. This process is referred to as *disconnected mirroring*.

For mirrored registries, to view the source of pulled images, you must review the **Trying to access** log entry in the CRI-O logs. Other methods to view the image pull source, such as using the **crictl images** command on a node, show the non-mirrored image name, even though the image is pulled from the mirrored location.

Additional resources

For information on viewing the CRI-O logs to view the image source, see [Viewing the image pull source](#).

18.9.3. Preparing your mirror host

Before you perform the mirror procedure, you must prepare the host to retrieve content and push it to the remote location.

18.9.3.1. Installing the OpenShift CLI by downloading the binary

You can install the OpenShift CLI (**oc**) to interact with OpenShift Container Platform from a command-line interface. You can install **oc** on Linux, Windows, or macOS.



IMPORTANT

If you installed an earlier version of **oc**, you cannot use it to complete all of the commands in OpenShift Container Platform 4.9. Download and install the new version of **oc**.

Installing the OpenShift CLI on Linux

You can install the OpenShift CLI (**oc**) binary on Linux by using the following procedure.

Procedure

1. Navigate to the [OpenShift Container Platform downloads page](#) on the Red Hat Customer Portal.
2. Select the appropriate version in the **Version** drop-down menu.
3. Click **Download Now** next to the **OpenShift v4.9 Linux Client** entry and save the file.
4. Unpack the archive:

```
$ tar xvfz <file>
```

5. Place the **oc** binary in a directory that is on your **PATH**.
To check your **PATH**, execute the following command:

```
$ echo $PATH
```

After you install the OpenShift CLI, it is available using the **oc** command:

```
$ oc <command>
```

Installing the OpenShift CLI on Windows

You can install the OpenShift CLI (**oc**) binary on Windows by using the following procedure.

Procedure

1. Navigate to the [OpenShift Container Platform downloads page](#) on the Red Hat Customer Portal.
2. Select the appropriate version in the **Version** drop-down menu.
3. Click **Download Now** next to the **OpenShift v4.9 Windows Client** entry and save the file.
4. Unzip the archive with a ZIP program.
5. Move the **oc** binary to a directory that is on your **PATH**.
To check your **PATH**, open the command prompt and execute the following command:

```
C:\> path
```

After you install the OpenShift CLI, it is available using the **oc** command:

```
C:\> oc <command>
```

Installing the OpenShift CLI on macOS

You can install the OpenShift CLI (**oc**) binary on macOS by using the following procedure.

Procedure

1. Navigate to the [OpenShift Container Platform downloads page](#) on the Red Hat Customer Portal.
2. Select the appropriate version in the **Version** drop-down menu.
3. Click **Download Now** next to the **OpenShift v4.9 MacOSX Client** entry and save the file.
4. Unpack and unzip the archive.
5. Move the **oc** binary to a directory on your PATH.
To check your **PATH**, open a terminal and execute the following command:

```
$ echo $PATH
```

After you install the OpenShift CLI, it is available using the **oc** command:

```
$ oc <command>
```

18.9.3.2. Configuring credentials that allow images to be mirrored

Create a container image registry credentials file that allows mirroring images from Red Hat to your mirror.

Prerequisites

- You configured a mirror registry to use in your restricted network.

Procedure

Complete the following steps on the installation host:

1. Download your **registry.redhat.io** pull secret from the [Pull Secret](#) page on the Red Hat OpenShift Cluster Manager site and save it to a **.json** file.
2. Generate the base64-encoded user name and password or token for your mirror registry:

```
$ echo -n '<user_name>:<password>' | base64 -w0 1
BGVtbYk3ZHAqXs=
```

- 1 For **<user_name>** and **<password>**, specify the user name and password that you configured for your registry.

3. Make a copy of your pull secret in JSON format:

```
$ cat ./pull-secret.text | jq . > <path>/<pull_secret_file_in_json> 1
```

- 1 Specify the path to the folder to store the pull secret in and a name for the JSON file that you create.

The contents of the file resemble the following example:

```
{
  "auths": {
    "cloud.openshift.com": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
    "quay.io": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
    "registry.connect.redhat.com": {
      "auth": "NTE3Njg5Nj...",
      "email": "you@example.com"
    },
    "registry.redhat.io": {
      "auth": "NTE3Njg5Nj...",
      "email": "you@example.com"
    }
  }
}
```

4. Edit the new file and add a section that describes your registry to it:

```
"auths": {
  "<mirror_registry>": { 1
    "auth": "<credentials>", 2
    "email": "you@example.com"
  },
}
```

- 1 For **<mirror_registry>**, specify the registry domain name, and optionally the port, that your mirror registry uses to serve content. For example, **registry.example.com** or **registry.example.com:5000**
- 2 For **<credentials>**, specify the base64-encoded user name and password for the mirror registry.

The file resembles the following example:

```
{
  "auths": {
    "registry.example.com": {
      "auth": "BGVtbYk3ZHAqXs=",
      "email": "you@example.com"
    },
    "cloud.openshift.com": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
    "quay.io": {
      "auth": "b3BlbnNo...",
      "email": "you@example.com"
    },
  }
}
```

```

    "registry.connect.redhat.com": {
      "auth": "NTE3Njg5Nj...",
      "email": "you@example.com"
    },
    "registry.redhat.io": {
      "auth": "NTE3Njg5Nj...",
      "email": "you@example.com"
    }
  }
}

```

18.9.3.3. Mirroring the OpenShift Container Platform image repository

Mirror the OpenShift Container Platform image repository to your registry to use during cluster installation or upgrade.

Prerequisites

- Your mirror host has access to the internet.
- You configured a mirror registry to use in your restricted network and can access the certificate and credentials that you configured.
- You downloaded the pull secret from the [Pull Secret](#) page on the Red Hat OpenShift Cluster Manager site and modified it to include authentication to your mirror repository.
- If you use self-signed certificates that do not set a Subject Alternative Name, you must precede the **oc** commands in this procedure with **GODEBUG=x509ignoreCN=0**. If you do not set this variable, the **oc** commands will fail with the following error:

```

x509: certificate relies on legacy Common Name field, use SANs or temporarily enable
Common Name matching with GODEBUG=x509ignoreCN=0

```

Procedure

Complete the following steps on the mirror host:

1. Review the [OpenShift Container Platform downloads page](#) to determine the version of OpenShift Container Platform that you want to install and determine the corresponding tag on the [Repository Tags](#) page.
2. Set the required environment variables:
 - a. Export the release version:

```
$ OCP_RELEASE=<release_version>
```

For **<release_version>**, specify the tag that corresponds to the version of OpenShift Container Platform to install, such as **4.5.4**.

- b. Export the local registry name and host port:

```
$ LOCAL_REGISTRY='<local_registry_host_name>:<local_registry_host_port>'
```

For **<local_registry_host_name>**, specify the registry domain name for your mirror repository, and for **<local_registry_host_port>**, specify the port that it serves content on.

- c. Export the local repository name:

```
$ LOCAL_REPOSITORY='<local_repository_name>'
```

For **<local_repository_name>**, specify the name of the repository to create in your registry, such as **ocp4/openshift4**.

- d. Export the name of the repository to mirror:

```
$ PRODUCT_REPO='openshift-release-dev'
```

For a production release, you must specify **openshift-release-dev**.

- e. Export the path to your registry pull secret:

```
$ LOCAL_SECRET_JSON='<path_to_pull_secret>'
```

For **<path_to_pull_secret>**, specify the absolute path to and file name of the pull secret for your mirror registry that you created.

- f. Export the release mirror:

```
$ RELEASE_NAME="ocp-release"
```

For a production release, you must specify **ocp-release**.

- g. Export the type of architecture for your server, such as **x86_64**:

```
$ ARCHITECTURE=<server_architecture>
```

- h. Export the path to the directory to host the mirrored images:

```
$ REMOVABLE_MEDIA_PATH=<path> 1
```

1 Specify the full path, including the initial forward slash (/) character.

3. Mirror the version images to the mirror registry:

- If your mirror host does not have internet access, take the following actions:
 - i. Connect the removable media to a system that is connected to the internet.
 - ii. Review the images and configuration manifests to mirror:

```
$ oc adm release mirror -a ${LOCAL_SECRET_JSON} \
  --from=quay.io/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE}-
  ${ARCHITECTURE} \
  --to=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY} \
  --to-release-
  image=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}-
  ${ARCHITECTURE} --dry-run
```


- iii. Record the entire **imageContentSources** section from the output of the previous command. The information about your mirrors is unique to your mirrored repository, and you must add the **imageContentSources** section to the **install-config.yaml** file during installation.
- iv. Mirror the images to a directory on the removable media:

```
$ oc adm release mirror -a ${LOCAL_SECRET_JSON} --to-
dir=${REMOVABLE_MEDIA_PATH}/mirror
quay.io/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE}-
${ARCHITECTURE}
```

- v. Take the media to the restricted network environment and upload the images to the local container registry.

```
$ oc image mirror -a ${LOCAL_SECRET_JSON} --from-
dir=${REMOVABLE_MEDIA_PATH}/mirror
"file://openshift/release:${OCP_RELEASE}*"
${LOCAL_REGISTRY}/${LOCAL_REPOSITORY} ❶
```

- ❶ For **REMOVABLE_MEDIA_PATH**, you must use the same path that you specified when you mirrored the images.

- If the local container registry is connected to the mirror host, take the following actions:
 - i. Directly push the release images to the local registry by using following command:

```
$ oc adm release mirror -a ${LOCAL_SECRET_JSON} \
--from=quay.io/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE}-
${ARCHITECTURE} \
--to=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY} \
--to-release-
image=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}-
${ARCHITECTURE}
```

This command pulls the release information as a digest, and its output includes the **imageContentSources** data that you require when you install your cluster.

- ii. Record the entire **imageContentSources** section from the output of the previous command. The information about your mirrors is unique to your mirrored repository, and you must add the **imageContentSources** section to the **install-config.yaml** file during installation.



NOTE

The image name gets patched to Quay.io during the mirroring process, and the podman images will show Quay.io in the registry on the bootstrap virtual machine.

- 4. To create the installation program that is based on the content that you mirrored, extract it and pin it to the release:
 - If your mirror host does not have internet access, run the following command:

```
$ oc adm release extract -a ${LOCAL_SECRET_JSON} --command=openshift-install
"${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}"
```

- If the local container registry is connected to the mirror host, run the following command:

```
$ oc adm release extract -a ${LOCAL_SECRET_JSON} --command=openshift-install
"${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}-
${ARCHITECTURE}"
```



IMPORTANT

To ensure that you use the correct images for the version of OpenShift Container Platform that you selected, you must extract the installation program from the mirrored content.

You must perform this step on a machine with an active internet connection.

If you are in a disconnected environment, use the **--image** flag as part of `must-gather` and point to the payload image.

5. For clusters using installer-provisioned infrastructure, run the following command:

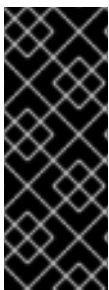
```
$ openshift-install
```

18.9.3.4. Adding RHCOS ISO and RootFS images to a disconnected mirror host

Before you install a cluster on infrastructure that you provision, you must create Red Hat Enterprise Linux CoreOS (RHCOS) machines for it to use. Use a disconnected mirror to host the RHCOS images you require to provision your distributed unit (DU) bare-metal hosts.

Prerequisites

- Deploy and configure an HTTP server to host the RHCOS image resources on the network. You must be able to access the HTTP server from your computer, and from the machines that you create.



IMPORTANT

The RHCOS images might not change with every release of OpenShift Container Platform. You must download images with the highest version that is less than or equal to the OpenShift Container Platform version that you install. Use the image versions that match your OpenShift Container Platform version if they are available. You require ISO and RootFS images to install RHCOS on the DU hosts. RHCOS qcow2 images are not supported for this installation type.

Procedure

1. Log in to the mirror host.
2. Obtain the RHCOS ISO and RootFS images from mirror.openshift.com, for example:
 - a. Export the required image names and OpenShift Container Platform version as environment variables:

```
$ export ISO_IMAGE_NAME=<iso_image_name> 1
```

```
$ export ROOTFS_IMAGE_NAME=<rootfs_image_name> 1
```

```
$ export OCP_VERSION=<ocp_version> 1
```

1 ISO image name, for example, **rhcos-4.9.0-fc.1-x86_64-live.x86_64.iso**

1 RootFS image name, for example, **rhcos-4.9.0-fc.1-x86_64-live-rootfs.x86_64.img**

1 OpenShift Container Platform version, for example, **latest-4.9**

b. Download the required images:

```
$ sudo wget https://mirror.openshift.com/pub/openshift-v4/dependencies/rhcos/pre-release/${OCP_VERSION}/${ISO_IMAGE_NAME} -O /var/www/html/${ISO_IMAGE_NAME}
```

```
$ sudo wget https://mirror.openshift.com/pub/openshift-v4/dependencies/rhcos/pre-release/${OCP_VERSION}/${ROOTFS_IMAGE_NAME} -O /var/www/html/${ROOTFS_IMAGE_NAME}
```

Verification steps

- Verify that the images downloaded successfully and are being served on the disconnected mirror host, for example:

```
$ wget http://$(hostname)/${ISO_IMAGE_NAME}
```

Expected output

```
...
Saving to: rhcos-4.9.0-fc.1-x86_64-live.x86_64.iso
rhcos-4.9.0-fc.1-x86_64- 11%[====> ] 10.01M 4.71MB/s
...
```

18.10. INSTALLING RED HAT ADVANCED CLUSTER MANAGEMENT IN A DISCONNECTED ENVIRONMENT

You use Red Hat Advanced Cluster Management (RHACM) on a hub cluster in the disconnected environment to manage the deployment of distributed unit (DU) profiles on multiple managed spoke clusters.

Prerequisites

- Install the OpenShift Container Platform CLI (**oc**).
- Log in as a user with **cluster-admin** privileges.
- Configure a disconnected mirror registry for use in the cluster.

**NOTE**

If you want to deploy Operators to the spoke clusters, you must also add them to this registry. See [Mirroring an Operator catalog](#) for more information.

Procedure

- Install RHACM on the hub cluster in the disconnected environment. See [Installing RHACM in a disconnected environment](#).

18.11. ENABLING ASSISTED INSTALLER SERVICE ON BARE METAL

The Assisted Installer Service (AIS) deploys OpenShift Container Platform clusters. Red Hat Advanced Cluster Management (RHACM) ships with AIS. AIS is deployed when you enable the MultiClusterHub Operator on the RHACM hub cluster.

For distributed units (DUs), RHACM supports OpenShift Container Platform deployments that run on a single bare-metal host. The single node cluster acts as both a control plane and a worker node.

Prerequisites

- Install OpenShift Container Platform 4.9 on a hub cluster.
- Install RHACM and create the **MultiClusterHub** resource.
- Create persistent volume custom resources (CR) for database and file system storage.
- You have installed the OpenShift CLI (**oc**).

Procedure

1. Modify the **HiveConfig** resource to enable the feature gate for Assisted Installer:

```
$ oc patch hiveconfig hive --type merge -p '{"spec":
{"targetNamespace":"hive","logLevel":"debug","featureGates":{"custom":{"enabled":
["AlphaAgentInstallStrategy"]},"featureSet":"Custom"}}}'
```

2. Modify the **Provisioning** resource to allow the Bare Metal Operator to watch all namespaces:

```
$ oc patch provisioning provisioning-configuration --type merge -p '{"spec":
{"watchAllNamespaces": true }}'
```

3. Create the **AgentServiceConfig** CR.

- a. Save the following YAML in the **agent_service_config.yaml** file:

```
apiVersion: agent-install.openshift.io/v1beta1
kind: AgentServiceConfig
metadata:
  name: agent
spec:
  databaseStorage:
    accessModes:
      - ReadWriteOnce
  resources:
```

```

requests:
  storage: <db_volume_size> ❶
filesystemStorage:
  accessModes:
  - ReadWriteOnce
resources:
  requests:
    storage: <fs_volume_size> ❷
osImages: ❸
  - openshiftVersion: "<ocp_version>" ❹
    version: "<ocp_release_version>" ❺
    url: "<iso_url>" ❻
    rootFSUrl: "<root_fs_url>" ❼
    cpuArchitecture: "x86_64"

```

- ❶ Volume size for the **databaseStorage** field, for example **10Gi**.
- ❷ Volume size for the **filesystemStorage** field, for example **20Gi**.
- ❸ List of OS image details. Example describes a single OpenShift Container Platform OS version.
- ❹ OpenShift Container Platform version to install, for example, **4.8**.
- ❺ Specific install version, for example, **47.83.202103251640-0**.
- ❻ ISO url, for example, https://mirror.openshift.com/pub/openshift-v4/dependencies/rhcos/4.7/4.7.7/rhcos-4.7.7-x86_64-live.x86_64.iso.
- ❼ Root FS image URL, for example, https://mirror.openshift.com/pub/openshift-v4/dependencies/rhcos/4.7/4.7.7/rhcos-live-rootfs.x86_64.img

- b. Create the **AgentServiceConfig** CR by running the following command:

```
$ oc create -f agent_service_config.yaml
```

Example output

```
agentserviceconfig.agent-install.openshift.io/agent created
```

18.12. ZTP CUSTOM RESOURCES

Zero touch provisioning (ZTP) uses custom resource (CR) objects to extend the Kubernetes API or introduce your own API into a project or a cluster. These CRs contain the site-specific data required to install and configure a cluster for RAN applications.

A custom resource definition (CRD) file defines your own object kinds. Deploying a CRD into the managed cluster causes the Kubernetes API server to begin serving the specified CR for the entire lifecycle.

For each CR in the **<site>.yaml** file on the managed cluster, ZTP uses the data to create installation CRs in a directory named for the cluster.

ZTP provides two ways for defining and installing CRs on managed clusters: a manual approach when you are provisioning a single cluster and an automated approach when provisioning multiple clusters.

Manual CR creation for single clusters

Use this method when you are creating CRs for a single cluster. This is a good way to test your CRs before deploying on a larger scale.

Automated CR creation for multiple managed clusters

Use the automated SiteConfig method when you are installing multiple managed clusters, for example, in batches of up to 100 clusters. SiteConfig uses ArgoCD as the engine for the GitOps method of site deployment. After completing a site plan that contains all of the required parameters for deployment, a policy generator creates the manifests and applies them to the hub cluster.

Both methods create the CRs shown in the following table. On the cluster site, an automated Discovery image ISO file creates a directory with the site name and a file with the cluster name. Every cluster has its own namespace, and all of the CRs are under that namespace. The namespace and the CR names match the cluster name.

Resource	Description	Usage
BareMetalHost	Contains the connection information for the Baseboard Management Controller (BMC) of the target bare metal machine.	Provides access to the BMC in order to load and boot the Discovery image ISO on the target machine by using the Redfish protocol.
InfraEnv	Contains information for pulling OpenShift Container Platform onto the target bare metal machine.	Used with ClusterDeployment to generate the Discovery ISO for the managed cluster.
AgentClusterInstall	Specifies the managed cluster's configuration such as networking and the number of supervisor (control plane) nodes. Shows the kubeconfig and credentials when the installation is complete.	Specifies the managed cluster configuration information and provides status during the installation of the cluster.
ClusterDeployment	References the AgentClusterInstall to use.	Used with InfraEnv to generate the Discovery ISO for the managed cluster.
NMStateConfig	Provides network configuration information such as MAC to IP mapping, DNS server, default route, and other network settings. This is not needed if DHCP is used.	Sets up a static IP address for the managed cluster's Kube API server.
Agent	Contains hardware information about the target bare metal machine.	Created automatically on the hub when the target machine's Discovery image ISO boots.

Resource	Description	Usage
ManagedCluster	When a cluster is managed by the hub, it must be imported and known. This Kubernetes object provides that interface.	The hub uses this resource to manage and show the status of managed clusters.
KlusterletAddonConfig	Contains the list of services provided by the hub to be deployed to a ManagedCluster .	Tells the hub which add-on services to deploy to a ManagedCluster .
Namespace	Logical space for ManagedCluster resources existing on the hub. Unique per site.	Propagates resources to the ManagedCluster .
Secret	Two custom resources are created: BMC Secret and Image Pull Secret .	<ul style="list-style-type: none"> • BMC Secret authenticates into the target bare metal machine using its username and password. • Image Pull Secret contains authentication information for the OpenShift Container Platform image installed on the target bare metal machine.
ClusterImageSet	Contains OpenShift Container Platform image information such as the repository and image name.	Passed into resources to provide OpenShift Container Platform images.

18.13. CREATING CUSTOM RESOURCES TO INSTALL A SINGLE MANAGED CLUSTER

This procedure tells you how to manually create and deploy a single managed cluster. If you are creating multiple clusters, perhaps hundreds, use the **SiteConfig** method described in “Creating ZTP custom resources for multiple managed clusters”.

Prerequisites

- Enable Assisted Installer Service.
- Ensure network connectivity:
 - The container within the hub must be able to reach the Baseboard Management Controller (BMC) address of the target bare metal machine.

- The managed cluster must be able to resolve and reach the hub's API **hostname** and ***.app** hostname. Example of the hub's API and ***.app** hostname:

```
console-openshift-console.apps.hub-cluster.internal.domain.com
api.hub-cluster.internal.domain.com
```

- The hub must be able to resolve and reach the API and ***.app** hostname of the managed cluster. Here is an example of the managed cluster's API and ***.app** hostname:

```
console-openshift-console.apps.sno-managed-cluster-1.internal.domain.com
api.sno-managed-cluster-1.internal.domain.com
```

- A DNS Server that is IP reachable from the target bare metal machine.
- A target bare metal machine for the managed cluster with the following hardware minimums:
 - 4 CPU or 8 vCPU
 - 32 GiB RAM
 - 120 GiB Disk for root filesystem
- When working in a disconnected environment, the release image needs to be mirrored. Use this command to mirror the release image:

```
oc adm release mirror -a <pull_secret.json>
--from=quay.io/openshift-release-dev/ocp-release:{{ mirror_version_spoke_release }}
--to={{ provisioner_cluster_registry }}/ocp4 --to-release-image={{
provisioner_cluster_registry }}/ocp4:{{ mirror_version_spoke_release }}
```

- You mirrored the ISO and **rootfs** used to generate the spoke cluster ISO to an HTTP server and configured the settings to pull images from there.
The images must match the version of the **ClusterImageSet**. To deploy a 4.9.0 version, the **rootfs** and ISO need to be set at 4.9.0.

Procedure

1. Create a **ClusterImageSet** for each specific cluster version that needs to be deployed. A **ClusterImageSet** has the following format:

```
apiVersion: hive.openshift.io/v1
kind: ClusterImageSet
metadata:
  name: openshift-4.9.0-rc.0 ❶
spec:
  releaseImage: quay.io/openshift-release-dev/ocp-release:4.9.0-x86_64 ❷
```

- ❶ **name** is the descriptive version that you want to deploy.
- ❷ **releaseImage** needs to point to the specific release image to deploy.

2. Create the **Namespace** definition for the managed cluster:

```
apiVersion: v1
```



```

kind: Namespace
metadata:
  name: <cluster-name> 1
  labels:
    name: <cluster-name> 2

```

1 **2** **cluster-name** is the name of the managed cluster to provision.

3. Create the **BMC Secret** custom resource:

```

apiVersion: v1
data:
  password: <bmc-password> 1
  username: <bmc-username> 2
kind: Secret
metadata:
  name: <cluster-name>-bmc-secret
  namespace: <cluster-name>
type: Opaque

```

1 **bmc-password** is the password to the target bare metal machine. Must be base-64 encoded.

2 **bmc-username** is the username to the target bare metal machine. Must be base-64 encoded.

4. Create the **Image Pull Secret** custom resource:

```

apiVersion: v1
data:
  .dockerconfigjson: <pull-secret> 1
kind: Secret
metadata:
  name: assisted-deployment-pull-secret
  namespace: <cluster-name>
type: kubernetes.io/dockerconfigjson

```

1 **pull-secret** is the OpenShift Container Platform pull secret. Must be base-64 encoded.

5. Create the **AgentClusterInstall** custom resource:

```

apiVersion: extensions.hive.openshift.io/v1beta1
kind: AgentClusterInstall
metadata:
  # Only include the annotation if using OVN, otherwise omit the annotation
  annotations:
    agent-install.openshift.io/install-config-overrides: '{"networking":
{"networkType":"OVNKubernetes"}}'
  name: <cluster-name>
  namespace: <cluster-name>
spec:
  clusterDeploymentRef:

```

```

name: <cluster-name>
imageSetRef:
  name: <cluster-image-set> 1
networking:
  clusterNetwork:
    - cidr: <cluster-network-cidr> 2
      hostPrefix: 23
  machineNetwork:
    - cidr: <machine-network-cidr> 3
  serviceNetwork:
    - <service-network-cidr> 4
provisionRequirements:
  controlPlaneAgents: 1
  workerAgents: 0
sshPublicKey: <public-key> 5

```

- 1 **cluster-image-set** is the name of the ClusterImageSet custom resource used to install OpenShift Container Platform on the bare metal machine.
- 2 **cluster-network-cidr** is a block of IPv4 or IPv6 addresses in CIDR notation used for communication among cluster nodes.
- 3 **machine-network-cidr** is a block of IPv4 or IPv6 addresses in CIDR notation used for the target bare metal server external communication. Also used to determine the API and Ingress VIP addresses when provisioning DU single node clusters.
- 4 **service-network-cidr** is a block of IPv4 or IPv6 addresses in CIDR notation used for cluster services internal communication.
- 5 **public-key** entered as plain text can be used to SSH into the node after it is installed.



NOTE

If you want to configure a static IP for the managed cluster at this point, see the procedure in this document for configuring static IP addresses for managed clusters.

6. Create the **ClusterDeployment** custom resource:

```

apiVersion: hive.openshift.io/v1
kind: ClusterDeployment
metadata:
  name: <cluster-name>
  namespace: <cluster-name>
spec:
  baseDomain: <base-domain> 1
  clusterInstallRef:
    group: extensions.hive.openshift.io
    kind: AgentClusterInstall
    name: <cluster-name>
    version: v1beta1
  clusterName: <cluster-name>
  platform:
    agentBareMetal:

```

```

agentSelector:
  matchLabels:
    cluster-name: <cluster-name>
pullSecretRef:
  name: assisted-deployment-pull-secret

```

- 1 **base-domain** is the managed cluster's base domain.

7. Create the **KlusterletAddonConfig** custom resource:

```

apiVersion: agent.open-cluster-management.io/v1
kind: KlusterletAddonConfig
metadata:
  name: <cluster-name>
  namespace: <cluster-name>
spec:
  clusterName: <cluster-name>
  clusterNamespace: <cluster-name>
  clusterLabels:
    cloud: auto-detect
    vendor: auto-detect
  applicationManager:
    enabled: true
  certPolicyController:
    enabled: false
  iamPolicyController:
    enabled: false
  policyController:
    enabled: true
  searchCollector:
    enabled: false 1

```

- 1 **enabled:** is set to either **true** to enable KlusterletAddonConfig or **false** to disable the KlusterletAddonConfig. Keep **searchCollector** disabled.

8. Create the **ManagedCluster** custom resource:

```

apiVersion: cluster.open-cluster-management.io/v1
kind: ManagedCluster
metadata:
  name: <cluster-name>
spec:
  hubAcceptsClient: true

```

9. Create the **InfraEnv** custom resource:

```

apiVersion: agent-install.openshift.io/v1beta1
kind: InfraEnv
metadata:
  name: <cluster-name>
  namespace: <cluster-name>
spec:
  clusterRef:

```

```

name: <cluster-name>
namespace: <cluster-name>
sshAuthorizedKey: <public-key> ❶
agentLabelSelector:
  matchLabels:
    cluster-name: <cluster-name>
pullSecretRef:
  name: assisted-deployment-pull-secret

```

- ❶ Enter **public-key** as plain text and use it to SSH into the target bare metal machine when the host is booted from the ISO.

10. Create the **BareMetalHost** custom resource:

```

apiVersion: metal3.io/v1alpha1
kind: BareMetalHost
metadata:
  name: <cluster-name>
  namespace: <cluster-name>
  annotations:
    inspect.metal3.io: disabled
  labels:
    infraenvs.agent-install.openshift.io: "<cluster-name>"
spec:
  bootMode: "UEFI"
  bmc:
    address: <bmc-address> ❶
    disableCertificateVerification: true
    credentialsName: <cluster-name>-bmc-secret
  bootMACAddress: <mac-address> ❷
  automatedCleaningMode: disabled
  online: true

```

- ❶ **bmc-address** is the baseboard management console address of the installation ISO on the target bare metal machine.

- ❷ **mac-address** is the target bare metal machine's MAC address.

Optionally, you can add **bmac.agent-install.openshift.io/hostname: <host-name>** as an annotation to set the managed cluster's hostname, otherwise it will default to either a hostname from the DHCP server or local host.

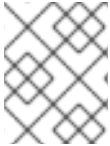
11. After you have created the custom resources, push the entire directory of generated custom resources to the Git repository you created for storing the custom resources.

Next step

To provision additional clusters, repeat this procedure for each cluster.

18.13.1. Configuring static IP addresses for managed clusters

Optionally, after creating the **AgentClusterInstall** custom resource, you can configure static IP addresses for the managed clusters.



NOTE

You must create this custom resource before creating the **ClusterDeployment** custom resource.

Prerequisites

- Deploy and configure the **AgentClusterInstall** custom resource.

Procedure

1. Create a **NMStateConfig** custom resource:

```
apiVersion: agent-install.openshift.io/v1beta1
kind: NMStateConfig
metadata:
  name: <cluster-name>
  namespace: <cluster-name>
  labels:
    sno-cluster-<cluster-name>: <cluster-name>
spec:
  config:
    interfaces:
      - name: eth0
        type: ethernet
        state: up
        ipv4:
          enabled: true
          address:
            - ip: <ip-address> 1
              prefix-length: <public-network-prefix> 2
          dhcp: false
    dns-resolver:
      config:
        server:
          - <dns-resolver> 3
    routes:
      config:
        - destination: 0.0.0.0/0
          next-hop-address: <gateway> 4
          next-hop-interface: eth0
          table-id: 254
    interfaces:
      - name: "eth0" 5
        macAddress: <mac-address> 6
```

- 1 **ip-address** is the static IP address of the target bare metal machine.
- 2 **public-network-prefix** is the static IP address's subnet prefix for the target bare metal machine.
- 3 **dns-resolver** is the DNS server for the target bare metal machine.
- 4 **gateway** is the gateway for the target bare metal machine.

- 5 **name** must match the name specified in the **interfaces** section.
 - 6 **mac-address** is the mac address of the interface.
2. When creating the **BareMetalHost** custom resource, ensure that one of its mac addresses matches a mac address in the **NMStateConfig** target bare metal machine.
 3. When creating the **InfraEnv** custom resource, reference the label from the **NMStateConfig** custom resource in the **InfraEnv** custom resource:

```
apiVersion: agent-install.openshift.io/v1beta1
kind: InfraEnv
metadata:
  name: <cluster-name>
  namespace: <cluster-name>
spec:
  clusterRef:
    name: <cluster-name>
    namespace: <cluster-name>
  sshAuthorizedKey: <public-key>
  agentLabelSelector:
    matchLabels:
      cluster-name: <cluster-name>
  pullSecretRef:
    name: assisted-deployment-pull-secret
  nmStateConfigLabelSelector:
    matchLabels:
      sno-cluster-<cluster-name>: <cluster-name> # Match this label
```

18.13.2. Automated Discovery image ISO process for provisioning clusters

After you create the custom resources, the following actions happen automatically:

1. A Discovery image ISO file is generated and booted on the target machine.
2. When the ISO file successfully boots on the target machine it reports the hardware information of the target machine.
3. After all hosts are discovered, OpenShift Container Platform is installed.
4. When OpenShift Container Platform finishes installing, the hub installs the **klusterlet** service on the target cluster.
5. The requested add-on services are installed on the target cluster.

The Discovery image ISO process finishes when the **Agent** custom resource is created on the hub for the managed cluster.

18.13.3. Checking the managed cluster status

Ensure that cluster provisioning was successful by checking the cluster status.

Prerequisites

- All of the custom resources have been configured and provisioned, and the **Agent** custom resource is created on the hub for the managed cluster.

Procedure

1. Check the status of the managed cluster:

```
$ oc get managedcluster
```

True indicates the managed cluster is ready.

2. Check the agent status:

```
$ oc get agent -n <cluster-name>
```

3. Use the **describe** command to provide an in-depth description of the agent's condition. Statuses to be aware of include **BackendError**, **InputError**, **ValidationsFailing**, **InstallationFailed**, and **AgentIsConnected**. These statuses are relevant to the **Agent** and **AgentClusterInstall** custom resources.

```
$ oc describe agent -n <cluster-name>
```

4. Check the cluster provisioning status:

```
$ oc get agentclusterinstall -n <cluster-name>
```

5. Use the **describe** command to provide an in-depth description of the cluster provisioning status:

```
$ oc describe agentclusterinstall -n <cluster-name>
```

6. Check the status of the managed cluster's add-on services:

```
$ oc get managedclusteraddon -n <cluster-name>
```

7. Retrieve the authentication information of the **kubeconfig** file for the managed cluster:

```
$ oc get secret -n <cluster-name> <cluster-name>-admin-kubeconfig -o jsonpath={.data.kubeconfig} | base64 -d > <directory>/<cluster-name>-kubeconfig
```

18.13.4. Configuring a managed cluster for a disconnected environment

After you have completed the preceding procedure, follow these steps to configure the managed cluster for a disconnected environment.

Prerequisites

- A disconnected installation of Red Hat Advanced Cluster Management (RHACM) 2.3.
- Host the **rootfs** and **iso** images on an HTTPD server.

Procedure

1. Create a **ConfigMap** containing the mirror registry config:

```

apiVersion: v1
kind: ConfigMap
metadata:
  name: assisted-installer-mirror-config
  namespace: assisted-installer
  labels:
    app: assisted-service
data:
  ca-bundle.crt: <certificate> ❶
  registries.conf: | ❷
    unqualified-search-registries = ["registry.access.redhat.com", "docker.io"]

    [[registry]]
      location = <mirror-registry-url> ❸
      insecure = false
      mirror-by-digest-only = true

```

- ❶ **certificate** is the mirror registry's certificate used when creating the mirror registry.
- ❷ **registry-config** is the configuration for the mirror registry.
- ❸ **mirror-registry-url** is the URL of the mirror registry.

This updates **mirrorRegistryRef** in the **AgentServiceConfig** custom resource, as shown below:

Example output

```

apiVersion: agent-install.openshift.io/v1beta1
kind: AgentServiceConfig
metadata:
  name: agent
  namespace: assisted-installer
spec:
  databaseStorage:
    volumeName: <db-pv-name>
    accessModes:
      - ReadWriteOnce
    resources:
      requests:
        storage: <db-storage-size>
  filesystemStorage:
    volumeName: <fs-pv-name>
    accessModes:
      - ReadWriteOnce
    resources:
      requests:
        storage: <fs-storage-size>
  mirrorRegistryRef:
    name: 'assisted-installer-mirror-config'
  osImages:

```



```
- openshiftVersion: <ocp-version>
  rootfs: <rootfs-url> 1
  url: <iso-url> 2
```

1 **2** **rootfs-url** and the **iso-url** must match the URLs of the HTTPD server.

- For disconnected installations, you must deploy an NTP clock that is reachable through the disconnected network. You can do this by configuring chrony to act as server, editing the `/etc/chrony.conf` file, and adding the following allowed IPv6 range:

```
# Allow NTP client access from local network.
#allow 192.168.0.0/16
local stratum 10
bindcmdaddress ::
allow 2620:52:0:1310::/64
```

18.13.5. Configuring IPv6 addresses for a disconnected environment

Optionally, when you are creating the **AgentClusterInstall** custom resource, you can configure IPV6 addresses for the managed clusters.

Procedure

- In the **AgentClusterInstall** custom resource, modify the IP addresses in **clusterNetwork** and **serviceNetwork** for IPv6 addresses:

```
apiVersion: extensions.hive.openshift.io/v1beta1
kind: AgentClusterInstall
metadata:
  # Only include the annotation if using OVN, otherwise omit the annotation
  annotations:
    agent-install.openshift.io/install-config-overrides: '{"networking":
{"networkType":"OVNKubernetes"}}'
  name: <cluster-name>
  namespace: <cluster-name>
spec:
  clusterDeploymentRef:
    name: <cluster-name>
  imageSetRef:
    name: <cluster-image-set>
  networking:
    clusterNetwork:
      - cidr: "fd01::/48"
        hostPrefix: 64
    machineNetwork:
      - cidr: <machine-network-cidr>
    serviceNetwork:
      - "fd02::/112"
  provisionRequirements:
    controlPlaneAgents: 1
    workerAgents: 0
  sshPublicKey: <public-key>
```

2. Update the **NMStateConfig** custom resource with the IPv6 addresses you defined.

18.13.6. Troubleshooting the managed cluster

Use this procedure to diagnose any installation issues that might occur with the managed clusters.

Procedure

1. Check the status of the managed cluster:

```
$ oc get managedcluster
```

Example output

NAME	HUB ACCEPTED AGE	MANAGED CLUSTER URLS	JOINED	AVAILABLE
SNO-cluster	true	True True	2d19h	

If the status in the **AVAILABLE** column is **True**, the managed cluster is being managed by the hub.

If the status in the **AVAILABLE** column is **Unknown**, the managed cluster is not being managed by the hub. Use the following steps to continue checking to get more information.

2. Check the **AgentClusterInstall** install status:

```
$ oc get clusterdeployment -n <cluster-name>
```

Example output

NAME	PLATFORM	REGION	CLUSTERTYPE	INSTALLED	INFRAID
Sno0026	agent-baremetal		false	Initialized	
2d14h					

If the status in the **INSTALLED** column is **false**, the installation was unsuccessful.

3. If the installation failed, enter the following command to review the status of the AgentClusterInstall resource:

```
$ oc describe agentclusterinstall -n <cluster-name> <cluster-name>
```

4. Resolve the errors and reset the cluster:

- a. Remove the cluster's namespace:

```
$ oc delete namespace <cluster-name>
```

This deletes all of the namespace-scoped custom resources created for this cluster.

- b. Remove the cluster's managed cluster resource:

```
$ oc delete managedcluster <cluster-name>
```

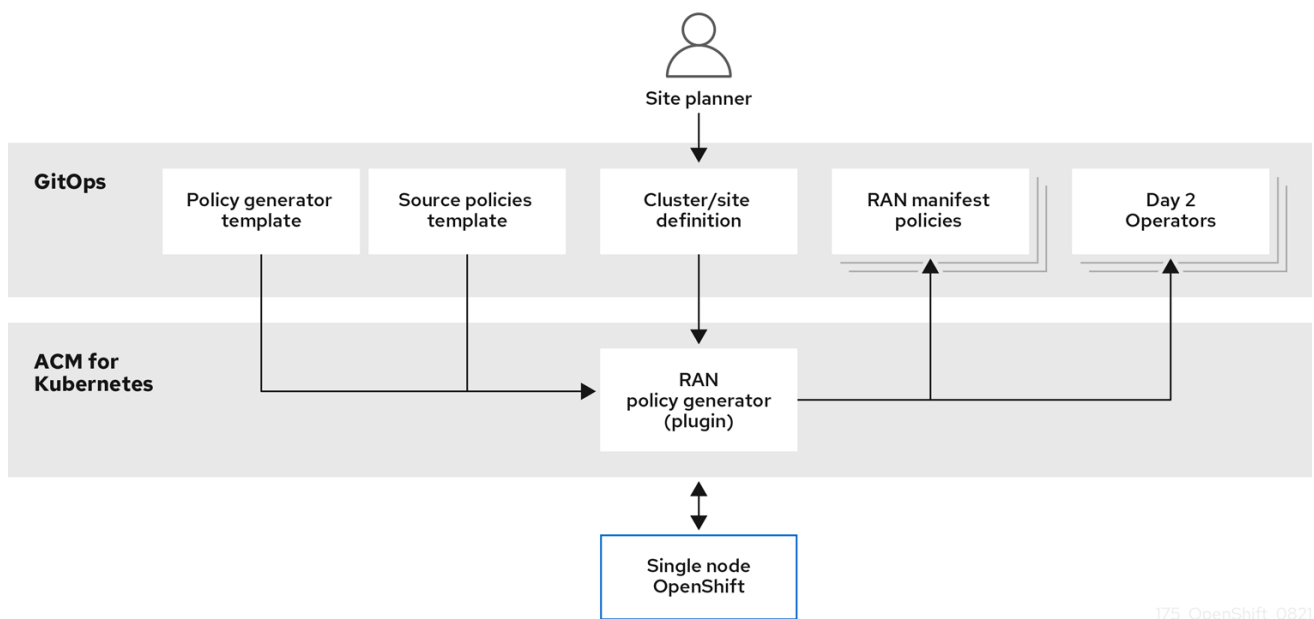
- c. Recreate the custom resources for the managed cluster.

18.14. APPLYING THE RAN POLICIES FOR MONITORING CLUSTER ACTIVITY

Zero touch provisioning (ZTP) uses Red Hat Advanced Cluster Management (RHACM) to apply the radio access network (RAN) policies using a policy-based governance approach to automatically monitor cluster activity.

The policy generator (PolicyGen) is a Kustomize plugin that facilitates creating ACM policies from predefined custom resources. There are three main items: Policy Categorization, Source CR policy, and PolicyGenTemplate. PolicyGen relies on these to generate the policies and their placement bindings and rules.

The following diagram shows how the RAN policy generator interacts with GitOps and ACM.



175_OpenShift_0821

RAN policies are categorized into three main groups:

Common

A policy that exists in the **Common** category is applied to all clusters to be represented by the site plan.

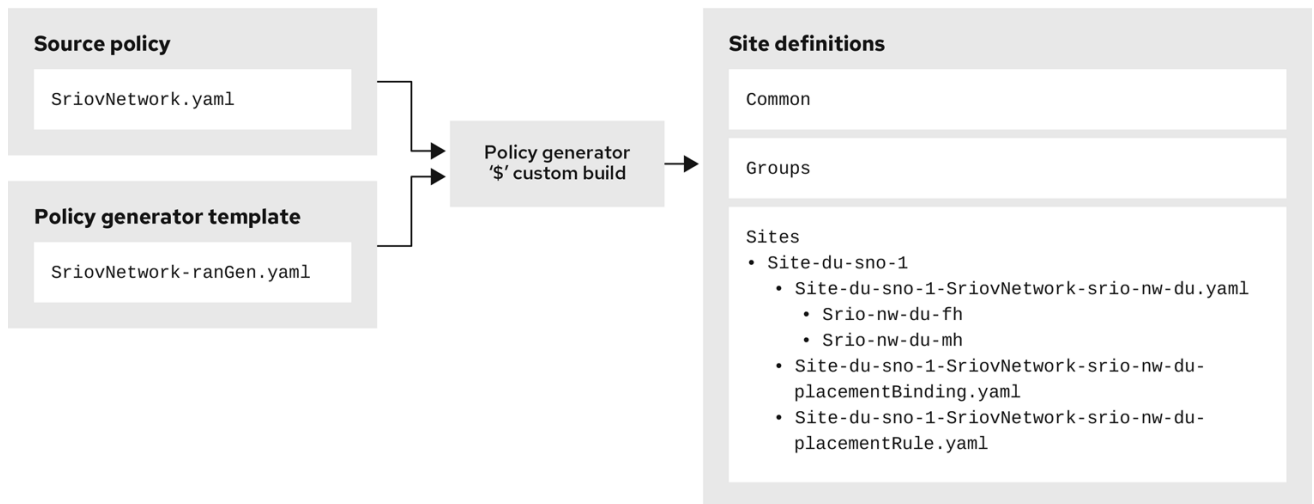
Groups

A policy that exists in the **Groups** category is applied to a group of clusters. Every group of clusters could have their own policies that exist under the Groups category. For example, **Groups/group1** could have its own policies that are applied to the clusters belonging to **group1**.

Sites

A policy that exists in the **Sites** category is applied to a specific cluster. Any cluster could have its own policies that exist in the **Sites** category. For example, **Sites/cluster1** will have its own policies applied to **cluster1**.

The following diagram shows how policies are generated.



175_OpenShift_0821

18.14.1. Applying source custom resource policies

Source custom resource policies include the following:

- SR-IOV policies
- PTP policies
- Performance Add-on Operator policies
- MachineConfigPool policies
- SCTP policies

You need to define the source custom resource that generates the ACM policy with consideration of possible overlay to its metadata or spec/data. For example, a **common-namespace-policy** contains a **Namespace** definition that exists in all managed clusters. This **namespace** is placed under the Common category and there are no changes for its spec or data across all clusters.

Namespace policy example

The following example shows the source custom resource for this namespace:

```

apiVersion: v1
kind: Namespace
metadata:
  name: openshift-sriov-network-operator
labels:
  openshift.io/run-level: "1"
  
```

Example output

The generated policy that applies this **namespace** includes the **namespace** as it is defined above without any change, as shown in this example:

```

apiVersion: policy.open-cluster-management.io/v1
kind: Policy
metadata:
  name: common-sriov-sub-ns-policy
  
```

```

namespace: common-sub
annotations:
  policy.open-cluster-management.io/categories: CM Configuration Management
  policy.open-cluster-management.io/controls: CM-2 Baseline Configuration
  policy.open-cluster-management.io/standards: NIST SP 800-53
spec:
  remediationAction: enforce
  disabled: false
  policy-templates:
    - objectDefinition:
        apiVersion: policy.open-cluster-management.io/v1
        kind: ConfigurationPolicy
        metadata:
          name: common-sriov-sub-ns-policy-config
        spec:
          remediationAction: enforce
          severity: low
          namespaceSelector:
            exclude:
              - kube-*
            include:
              - '*'
        object-templates:
          - complianceType: musthave
            objectDefinition:
              apiVersion: v1
              kind: Namespace
              metadata:
                labels:
                  openshift.io/run-level: "1"
                name: openshift-sriov-network-operator

```

SRIOV policy example

The following example shows a **SriovNetworkNodePolicy** definition that exists in different clusters with a different specification for each cluster. The example also shows the source custom resource for the **SriovNetworkNodePolicy**:

```

apiVersion: sriovnetwork.openshift.io/v1
kind: SriovNetworkNodePolicy
metadata:
  name: sriov-nnp
  namespace: openshift-sriov-network-operator
spec:
  # The $ tells the policy generator to overlay/remove the spec.item in the generated policy.
  deviceType: $deviceType
  isRdma: false
  nicSelector:
    pfNames: [$pfNames]
  nodeSelector:
    node-role.kubernetes.io/worker: ""
  numVfs: $numVfs
  priority: $priority
  resourceName: $resourceName

```

Example output

The **SriovNetworkNodePolicy** name and **namespace** are the same for all clusters, so both are defined in the source **SriovNetworkNodePolicy**. However, the generated policy requires the **\$deviceType**, **\$numVfs**, as input parameters in order to adjust the policy for each cluster. The generated policy is shown in this example:

```
apiVersion: policy.open-cluster-management.io/v1
kind: Policy
metadata:
  name: site-du-sno-1-sriov-nnp-mh-policy
  namespace: sites-sub
  annotations:
    policy.open-cluster-management.io/categories: CM Configuration Management
    policy.open-cluster-management.io/controls: CM-2 Baseline Configuration
    policy.open-cluster-management.io/standards: NIST SP 800-53
spec:
  remediationAction: enforce
  disabled: false
  policy-templates:
    - objectDefinition:
        apiVersion: policy.open-cluster-management.io/v1
        kind: ConfigurationPolicy
        metadata:
          name: site-du-sno-1-sriov-nnp-mh-policy-config
        spec:
          remediationAction: enforce
          severity: low
          namespaceselector:
            exclude:
              - kube-*
            include:
              - '*'
        object-templates:
          - complianceType: musthave
            objectDefinition:
              apiVersion: sriovnetwork.openshift.io/v1
              kind: SriovNetworkNodePolicy
              metadata:
                name: sriov-nnp-du-mh
                namespace: openshift-sriov-network-operator
              spec:
                deviceType: vfio-pci
                isRdma: false
                nicSelector:
                  pfNames:
                    - ens7f0
                nodeSelector:
                  node-role.kubernetes.io/worker: ""
                numVfs: 8
                resourceName: du_mh
```



NOTE

Defining the required input parameters as **\$value**, for example **\$deviceType**, is not mandatory. The **\$** tells the policy generator to overlay or remove the item from the generated policy. Otherwise, the value does not change.

18.14.2. The PolicyGenTemplate

The **PolicyGenTemplate.yaml** file is a Custom Resource Definition (CRD) that tells PolicyGen where to categorize the generated policies and which items need to be overlaid.

The following example shows the **PolicyGenTemplate.yaml** file:

```
apiVersion: ran.openshift.io/v1
kind: PolicyGenTemplate
metadata:
  name: "group-du-sno"
  namespace: "group-du-sno"
spec:
  bindingRules:
    group-du-sno: ""
  mcp: "master"
  sourceFiles:
    - fileName: ConsoleOperatorDisable.yaml
      policyName: "console-policy"
    - fileName: ClusterLogging.yaml
      policyName: "cluster-log-policy"
  spec:
    curation:
      curator:
        schedule: "30 3 * * *"
    collection:
      logs:
        type: "fluentd"
        fluentd: {}
```

The **group-du-ranGen.yaml** file defines a group of policies under a group named **group-du**. This file defines a **MachineConfigPool worker-du** that is used as the node selector for any other policy defined in **sourceFiles**. An ACM policy is generated for every source file that exists in **sourceFiles**. And, a single placement binding and placement rule is generated to apply the cluster selection rule for **group-du** policies.

Using the source file **PtpConfigSlave.yaml** as an example, the **PtpConfigSlave** has a definition of a **PtpConfig** custom resource (CR). The generated policy for the **PtpConfigSlave** example is named **group-du-ptp-config-policy**. The **PtpConfig** CR defined in the generated **group-du-ptp-config-policy** is named **du-ptp-slave**. The **spec** defined in **PtpConfigSlave.yaml** is placed under **du-ptp-slave** along with the other **spec** items defined under the source file.

The following example shows the **group-du-ptp-config-policy**:

```
apiVersion: policy.open-cluster-management.io/v1
kind: Policy
metadata:
  name: group-du-ptp-config-policy
  namespace: groups-sub
  annotations:
    policy.open-cluster-management.io/categories: CM Configuration Management
    policy.open-cluster-management.io/controls: CM-2 Baseline Configuration
    policy.open-cluster-management.io/standards: NIST SP 800-53
spec:
  remediationAction: enforce
  disabled: false
```

```

policy-templates:
- objectDefinition:
  apiVersion: policy.open-cluster-management.io/v1
  kind: ConfigurationPolicy
  metadata:
    name: group-du-ntp-config-policy-config
  spec:
    remediationAction: enforce
    severity: low
    namespaceselector:
      exclude:
        - kube-*
      include:
        - '*'
  object-templates:
  - complianceType: musthave
    objectDefinition:
      apiVersion: ntp.openshift.io/v1
      kind: NtpConfig
      metadata:
        name: slave
        namespace: openshift-ntp
      spec:
        recommend:
          - match:
          - nodeLabel: node-role.kubernetes.io/worker-du
            priority: 4
            profile: slave
        profile:
          - interface: ens5f0
            name: slave
            phc2sysOpts: -a -r -n 24
            ptp4lConf: |
              [global]
              #
              # Default Data Set
              #
              twoStepFlag 1
              slaveOnly 0
              priority1 128
              priority2 128
              domainNumber 24
              ....

```

18.14.3. Considerations when creating custom resource policies

- The custom resources used to create the ACM policies should be defined with consideration of possible overlay to its metadata and spec/data. For example, if the custom resource **metadata.name** does not change between clusters then you should set the **metadata.name** value in the custom resource file. If the custom resource will have multiple instances in the same cluster, then the custom resource **metadata.name** must be defined in the policy template file.
- In order to apply the node selector for a specific machine config pool, you have to set the node selector value as **\$mcp** in order to let the policy generator overlay the **\$mcp** value with the defined mcp in the policy template.

- Subscription source files do not change.

18.14.4. Generating RAN policies

Prerequisites

- Install Kustomize
- Install the [Kustomize Policy Generator plug-in](#)

Procedure

1. Configure the **kustomization.yaml** file to reference the **policyGenerator.yaml** file. The following example shows the PolicyGenerator definition:

```
apiVersion: policyGenerator/v1
kind: PolicyGenerator
metadata:
  name: acm-policy
  namespace: acm-policy-generator
# The arguments should be given and defined as below with same order --
policyGenTempPath= --sourcePath= --outPath= --stdout --customResources
argsOneLiner: ./ranPolicyGenTempExamples ./sourcePolicies ./out true false
```

Where:

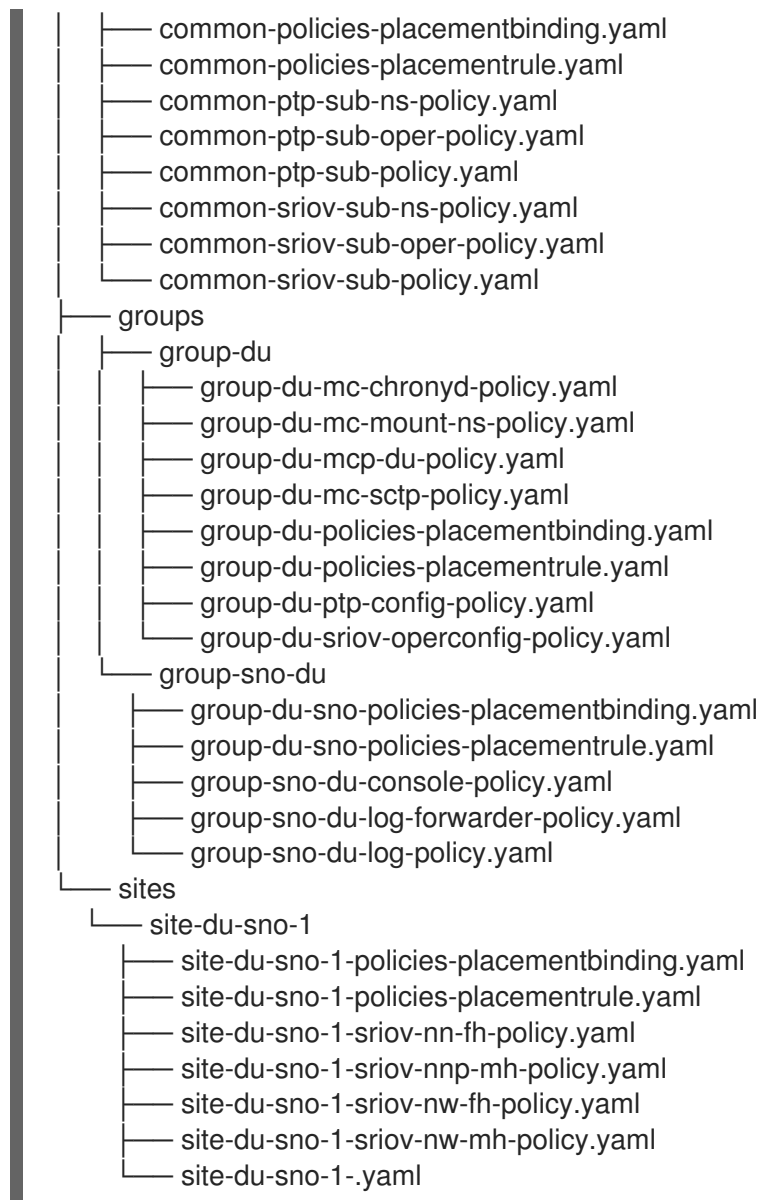
- **policyGenTempPath** is the path to the **policyGenTemp** files.
 - **sourcePath**: is the path to the source policies.
 - **outPath**: is the path to save the generated ACM policies.
 - **stdout**: If **true**, prints the generated policies to the console.
 - **customResources**: If **true** generates the CRs from the **sourcePolicies** files without ACM policies.
2. Test PolicyGen by running the following commands:

```
$ cd cnf-features-deploy/ztp/ztp-policy-generator/
```

```
$ XDG_CONFIG_HOME=./ kustomize build --enable-alpha-plugins
```

An **out** directory is created with the expected policies, as shown in this example:

```
out
├── common
│   ├── common-log-sub-ns-policy.yaml
│   ├── common-log-sub-oper-policy.yaml
│   ├── common-log-sub-policy.yaml
│   ├── common-pao-sub-catalog-policy.yaml
│   ├── common-pao-sub-ns-policy.yaml
│   ├── common-pao-sub-oper-policy.yaml
│   └── common-pao-sub-policy.yaml
```

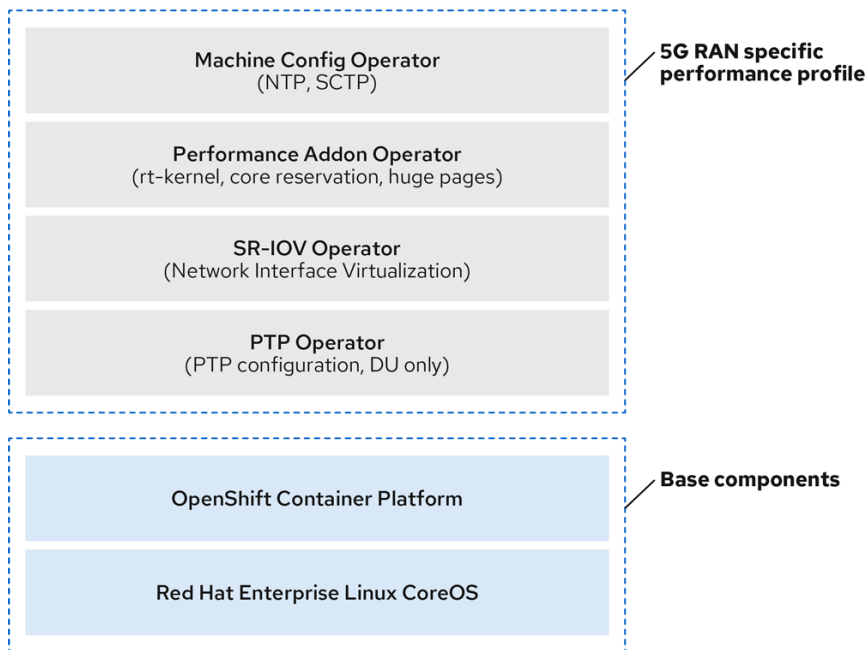


The common policies are flat because they will be applied to all clusters. However, the groups and sites have subdirectories for each group and site as they will be applied to different clusters.

18.15. CLUSTER PROVISIONING

Zero touch provisioning (ZTP) provisions clusters using a layered approach. The base components consist of Red Hat Enterprise Linux CoreOS (RHCOS), the basic operating system for the cluster, and OpenShift Container Platform. After these components are installed, the worker node can join the existing cluster. When the node has joined the existing cluster, the 5G RAN profile Operators are applied.

The following diagram illustrates this architecture.



177_OpenShift_0821

The following RAN Operators are deployed on every cluster:

- Machine Config
- Precision Time Protocol (PTP)
- Performance Addon Operator
- SR-IOV
- Local Storage Operator
- Logging Operator

18.15.1. Machine Config Operator

The Machine Config Operator enables system definitions and low-level system settings such as workload partitioning, NTP, and SCTP. This Operator is installed with OpenShift Container Platform.

A performance profile and its created products are applied to a node according to an associated machine config pool (MCP). The MCP holds valuable information about the progress of applying the machine configurations created by performance addons that encompass kernel args, kube config, huge pages allocation, and deployment of the realtime kernel (rt-kernel). The performance addons controller monitors changes in the MCP and updates the performance profile status accordingly.

18.15.2. Performance Addon Operator

The Performance Addon Operator provides the ability to enable advanced node performance tunings on a set of nodes.

OpenShift Container Platform provides a Performance Addon Operator to implement automatic tuning to achieve low latency performance for OpenShift Container Platform applications. The cluster administrator uses this performance profile configuration that makes it easier to make these changes in a more reliable way.

The administrator can specify updating the kernel to **rt-kernel**, reserving CPUs for management workloads, and using CPUs for running the workloads.

18.15.3. SR-IOV Operator

The Single Root I/O Virtualization (SR-IOV) Network Operator manages the SR-IOV network devices and network attachments in your cluster.

The SR-IOV Operator allows network interfaces to be virtual and shared at a device level with networking functions running within the cluster.

The SR-IOV Network Operator adds the **SriovOperatorConfig.sriovnetwork.openshift.io** CustomResourceDefinition resource. The Operator automatically creates a SriovOperatorConfig custom resource named **default** in the **openshift-sriov-network-operator** namespace. The **default** custom resource contains the SR-IOV Network Operator configuration for your cluster.

18.15.4. Precision Time Protocol Operator

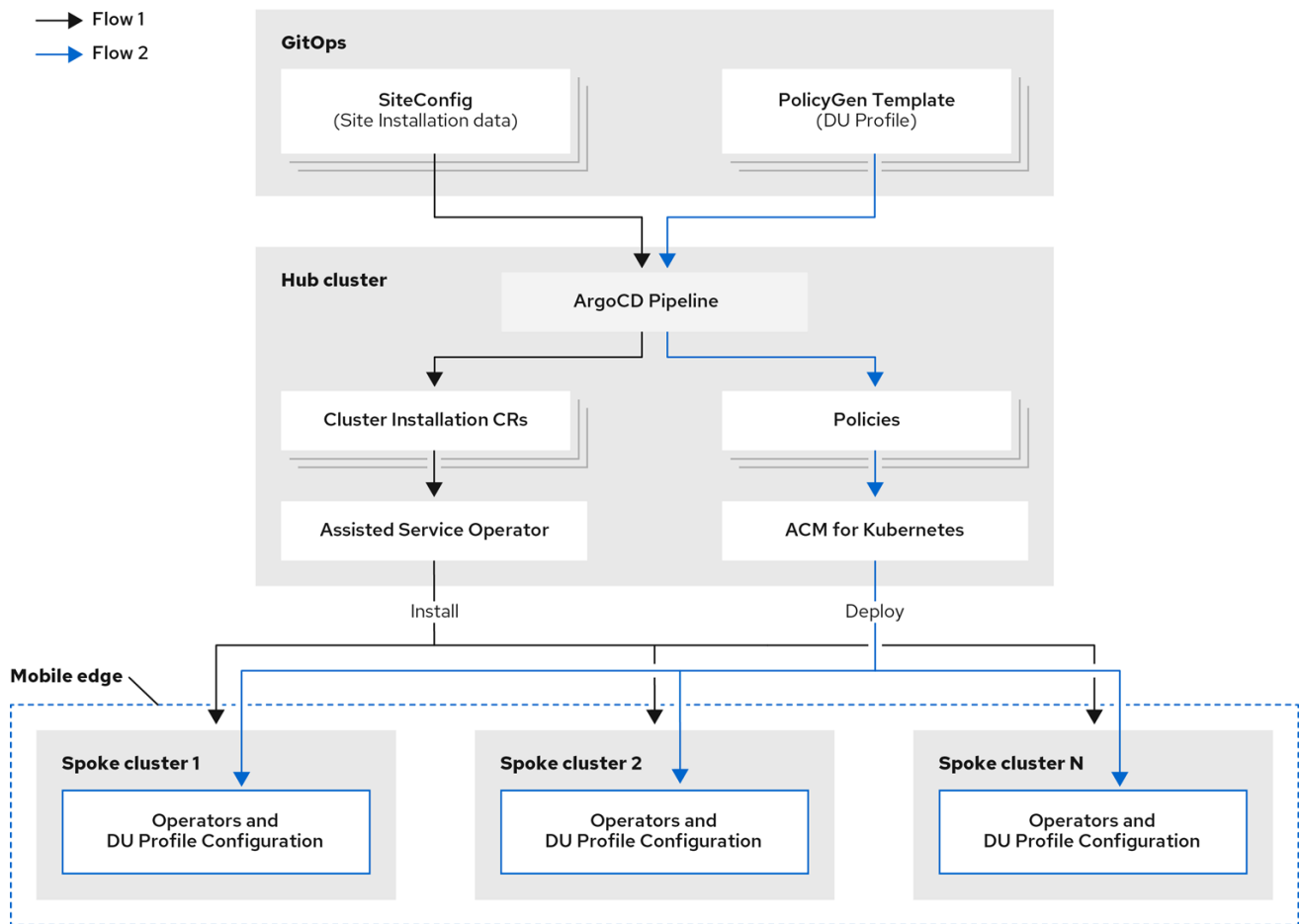
The Precision Time Protocol (PTP) Operator is a protocol used to synchronize clocks in a network. When used in conjunction with hardware support, PTP is capable of sub-microsecond accuracy. PTP support is divided between the kernel and user space.

The clocks synchronized by PTP are organized in a master-worker hierarchy. The workers are synchronized to their masters, which may be workers to their own masters. The hierarchy is created and updated automatically by the best master clock (BMC) algorithm, which runs on every clock. When a clock has only one port, it can be master or worker, such a clock is called an ordinary clock (OC). A clock with multiple ports can be master on one port and worker on another, such a clock is called a boundary clock (BC). The top-level master is called the grandmaster clock, which can be synchronized by using a Global Positioning System (GPS) time source. By using a GPS-based time source, disparate networks can be synchronized with a high-degree of accuracy.

18.16. CREATING ZTP CUSTOM RESOURCES FOR MULTIPLE MANAGED CLUSTERS

If you are installing multiple managed clusters, zero touch provisioning (ZTP) uses ArgoCD and **SiteConfig** to manage the processes that create the custom resources (CR) and generate and apply the policies for multiple clusters, in batches of no more than 100, using the GitOps approach.

Installing and deploying the clusters is a two stage process, as shown here:



183_OpenShift_0921

18.16.1. Prerequisites for deploying the ZTP pipeline

- Openshift cluster version 4.8 or higher and Red Hat GitOps Operator is installed.
- Red Hat Advanced Cluster Management (RHACM) version 2.3 or above is installed.
- For disconnected environments, make sure your source data Git repository and **ztp-site-generator** container image are accessible from the hub cluster.
- If you want additional custom content, such as extra install manifests or custom resources (CR) for policies, add them to the `/usr/src/hook/ztp/source-crs/extra-manifest/` directory. Similarly, you can add additional configuration CRs, as referenced from a **PolicyGenTemplate**, to the `/usr/src/hook/ztp/source-crs/` directory.

- Create a **Containerfile** that adds your additional manifests to the Red Hat provided image, for example:

```
FROM <registry fqdn>/ztp-site-generator:latest 1
COPY myInstallManifest.yaml /usr/src/hook/ztp/source-crs/extra-manifest/
COPY mySourceCR.yaml /usr/src/hook/ztp/source-crs/
```

- 1 **<registry fqdn>** must point to a registry containing the **ztp-site-generator** container image provided by Red Hat.

- Build a new container image that includes these additional files:

```
$> podman build Containerfile.example
```

18.16.2. Installing the GitOps ZTP pipeline

The procedures in this section tell you how to complete the following tasks:

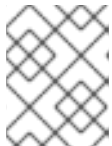
- Prepare the Git repository you need to host site configuration data.
- Configure the hub cluster for generating the required installation and policy custom resources (CR).
- Deploy the managed clusters using zero touch provisioning (ZTP).

18.16.2.1. Preparing the ZTP Git repository

Create a Git repository for hosting site configuration data. The zero touch provisioning (ZTP) pipeline requires read access to this repository.

Procedure

1. Create a directory structure with separate paths for the **SiteConfig** and **PolicyGenTemplate** custom resources (CR).
2. Add **pre-sync.yaml** and **post-sync.yaml** from **resource-hook-example/<policygentemplates>/** to the path for the **PolicyGenTemplate** CRs.
3. Add **pre-sync.yaml** and **post-sync.yaml** from **resource-hook-example/<siteconfig>/** to the path for the **SiteConfig** CRs.



NOTE

If your hub cluster operates in a disconnected environment, you must update the **image** for all four pre and post sync hook CRs.

4. Apply the **policygentemplates.ran.openshift.io** and **siteconfigs.ran.openshift.io** CR definitions.

18.16.2.2. Preparing the hub cluster for ZTP

You can configure your hub cluster with a set of ArgoCD applications that generate the required installation and policy custom resources (CR) for each site based on a zero touch provisioning (ZTP) GitOps flow.

Procedure

1. Install the Red Hat OpenShift GitOps Operator on your hub cluster.
2. Extract the administrator password for ArgoCD:

```
$ oc get secret openshift-gitops-cluster -n openshift-gitops -o  
jsonpath='{.data.admin\.password}' | base64 -d
```

3. Prepare the ArgoCD pipeline configuration:

- a. Extract the ArgoCD deployment CRs from the ZTP site generator container using the latest container image version:

```
$ mkdir ztp
$ podman run --rm -v `pwd`/ztp:/mnt/ztp:Z registry.redhat.io/openshift4/ztp-site-generator-
rhel8:v4.9.0-1 /bin/bash -c "cp -ar /usr/src/hook/ztp/* /mnt/ztp/"
```

The remaining steps in this section relate to the **ztp/gitops-subscriptions/argocd/** directory.

- b. Modify the source values of the two ArgoCD applications, **deployment/clusters-app.yaml** and **deployment/policies-app.yaml** with appropriate URL, **targetRevision** branch, and path values. The path values must match those used in your Git repository.

Modify **deployment/clusters-app.yaml**:

```
apiVersion: v1
kind: Namespace
metadata:
  name: clusters-sub
---
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: clusters
  namespace: openshift-gitops
spec:
  destination:
    server: https://kubernetes.default.svc
    namespace: clusters-sub
  project: default
  source:
    path: ztp/gitops-subscriptions/argocd/resource-hook-example/siteconfig 1
    repoURL: https://github.com/openshift-kni/cnf-features-deploy 2
    targetRevision: master 3
  syncPolicy:
    automated:
      prune: true
      selfHeal: true
    syncOptions:
      - CreateNamespace=true
```

1 **path** is the **ztp/gitops-subscriptions/argocd/** file path that contains the **siteconfig** CRs for the clusters.

2 **repoURL** is the URL of the Git repository that contains the **siteconfig** custom resources that define site configuration for installing clusters.

3 **targetRevision** is the branch on the Git repository that contains the relevant site configuration data.

- c. Modify **deployment/policies-app.yaml**:

```
apiVersion: v1
kind: Namespace
```

```

metadata:
  name: policies-sub
---
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: policies
  namespace: openshift-gitops
spec:
  destination:
    server: https://kubernetes.default.svc
    namespace: policies-sub
  project: default
  source:
    directory:
      recurse: true
    path: ztp/gitops-subscriptions/argocd/resource-hook-example/policygentemplates
    1
    repoURL: https://github.com/openshift-kni/cnf-features-deploy
    2
    targetRevision: master
    3
  syncPolicy:
    automated:
      prune: true
      selfHeal: true
    syncOptions:
      - CreateNamespace=true

```

- 1 **path** is the **ztp/gitops-subscriptions/argocd/** file path that contains the **policygentemplates** CRs for the clusters.
- 2 **repoURL** is the URL of the Git repository that contains the **policygentemplates** custom resources that specify configuration data for the site.
- 3 **targetRevision** is the branch on the Git repository that contains the relevant configuration data.

4. To apply the pipeline configuration to your hub cluster, enter this command:

```
$ oc apply -k ./deployment
```

18.16.3. Creating the site secrets

Add the required secrets for the site to the hub cluster. These resources must be in a namespace with a name that matches the cluster name.

Procedure

1. Create a secret for authenticating to the site Baseboard Management Controller (BMC). Ensure the secret name matches the name used in the **SiteConfig**. In this example, the secret name is **test-sno-bmh-secret**:

```

apiVersion: v1
kind: Secret
metadata:

```



```

name: test-sno-bmh-secret
namespace: test-sno
data:
  password: dGVtcA==
  username: cm9vdA==
type: Opaque

```

2. Create the pull secret for the site. The pull secret must contain all credentials necessary for installing OpenShift and all add-on Operators. In this example, the secret name is **assisted-deployment-pull-secret**:

```

apiVersion: v1
kind: Secret
metadata:
  name: assisted-deployment-pull-secret
  namespace: test-sno
type: kubernetes.io/dockerconfigjson
data:
  .dockerconfigjson: <Your pull secret base64 encoded>

```



NOTE

The secrets are referenced from the **SiteConfig** custom resource (CR) by name. The namespace must match the **SiteConfig** namespace.

18.16.4. Creating the SiteConfig custom resources

ArgoCD acts as the engine for the GitOps method of site deployment. After completing a site plan that contains the required custom resources for the site installation, a policy generator creates the manifests and applies them to the hub cluster.

Procedure

1. Create one or more **SiteConfig** custom resources, **site-config.yaml** files, that contains the site-plan data for the clusters. For example:

```

apiVersion: ran.openshift.io/v1
kind: SiteConfig
metadata:
  name: "test-sno"
  namespace: "test-sno"
spec:
  baseDomain: "clus2.t5g.lab.eng.bos.redhat.com"
  pullSecretRef:
    name: "assisted-deployment-pull-secret"
  clusterImageSetNameRef: "openshift-4.9"
  sshPublicKey: "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDB3dwhI5X0ZxGBb9VK7wclcPHLc8n7WYyKjTNIn
FjYNP9J+Zoc/ii+I3YbGUTuqilDwZN5rVlwBux2nUyVXDfaM5kPd9kACmxWtfEWtyVR0otbrNW
wRfKuC2h6cOd1lRBM1q6lzJ4d7+JVoltAxsabqLoCbK3svxaZoKAaK7jdGG030yvJzZaNm4PiT
y39VQXXKcIMDmicxEBwZx1UsA8yWQsiOQ5brod9KQRXWAAST779gbvtgXR2L+MnVNROE
Hf1nEjZJwjwaHxoDQYHYKERxKRHIWFtmy5dNT6BbvOpJ2e5osDFPMEd41d2mUJTfxXiC1nv
yjk9lrf8YJYnqJgBlxi0lxElUKH7mTdKykHiPrDH5D2pRlp+Donl4n+sw6qoDc/3571O93+RQ6kUS
AgAsvWiXrEfB/7kGgAa/BD5FeipkFrbSEpKPVu+gue1AQeJcz9BuLqdyPUQj2VUySkSg0FuGb

```

```

G7fxkKeF1h3Sga7nuDOzRxck4l/8Z7FxMF/e8DmaBpgHAUIfxXnRqAlmY9TyAZUEMT5ZPSvB
RZNNmLbfex1n3NLcov/GEpQOqEYcjG5y57gJ60/av4oqjcVmgtaSOOAS0kZ3y9YDhjsaOcpm
RYYijJn8URAH7NrW8EZsvAoF6GUt6xHq5T258c6xSYUm5L0iKvBqrOW9EjbLw==
root@cnfdc2.clus2.t5g.lab.eng.bos.redhat.com"
clusters:
- clusterName: "test-sno"
  clusterType: "sno"
  clusterProfile: "du"
  clusterLabels:
    group-du-sno: ""
    common: true
    sites : "test-sno"
  clusterNetwork:
    - cidr: 1001:db9::/48
      hostPrefix: 64
  machineNetwork:
    - cidr: 2620:52:0:10e7::/64
  serviceNetwork:
    - 1001:db7::/112
  additionalNTPSources:
    - 2620:52:0:1310::1f6
  nodes:
    - hostName: "test-sno.clus2.t5g.lab.eng.bos.redhat.com"
      bmcAddress: "idrac-
virtualmedia+https://[2620:52::10e7:f602:70ff:fee4:f4e2]/redfish/v1/Systems/System.Embedded.
1"
      bmcCredentialsName:
        name: "test-sno-bmh-secret"
      bootMACAddress: "0C:42:A1:8A:74:EC"
      bootMode: "UEFI"
      rootDeviceHints:
        hctl: '0:1:0'
      cpuset: "0-1,52-53"
      nodeNetwork:
        interfaces:
          - name: eno1
            macAddress: "0C:42:A1:8A:74:EC"
      config:
        interfaces:
          - name: eno1
            type: ethernet
            state: up
            macAddress: "0C:42:A1:8A:74:EC"
            ipv4:
              enabled: false
            ipv6:
              enabled: true
              address:
                - ip: 2620:52::10e7:e42:a1ff:fe8a:900
                  prefix-length: 64
        dns-resolver:
          config:
            search:
              - clus2.t5g.lab.eng.bos.redhat.com
            server:
              - 2620:52:0:1310::1f6

```

```

routes:
  config:
    - destination: ::/0
      next-hop-interface: eno1
      next-hop-address: 2620:52:0:10e7::fc
      table-id: 254

```

2. Save the files and push them to the zero touch provisioning (ZTP) Git repository accessible from the hub cluster and defined as a source repository of the ArgoCD application.

ArgoCD detects that the application is out of sync. Upon sync, either automatic or manual, ArgoCD synchronizes the **PolicyGenTemplate** to the hub cluster and launches the associated resource hooks. These hooks are responsible for generating the policy wrapped configuration CRs that apply to the spoke cluster. The resource hooks convert the site definitions to installation custom resources and applies them to the hub cluster:

- **Namespace** - Unique per site
- **AgentClusterInstall**
- **BareMetalHost**
- **ClusterDeployment**
- **InfraEnv**
- **NMStateConfig**
- **ExtraManifestsConfigMap** - Extra manifests. The additional manifests include workload partitioning, chronyd, mountpoint hiding, sctp enablement, and more.
- **ManagedCluster**
- **KlusterletAddonConfig**

Red Hat Advanced Cluster Management (RHACM) (ACM) deploys the hub cluster.

18.16.5. Creating the PolicyGenTemplates

Use the following procedure to create the **PolicyGenTemplates** you will need for generating policies in your Git repository for the hub cluster.

Procedure

1. Create the **PolicyGenTemplates** and save them to the zero touch provisioning (ZTP) Git repository accessible from the hub cluster and defined as a source repository of the ArgoCD application.
2. ArgoCD detects that the application is out of sync. Upon sync, either automatic or manual, ArgoCD applies the new **PolicyGenTemplate** to the hub cluster and launches the associated resource hooks. These hooks are responsible for generating the policy wrapped configuration CRs that apply to the spoke cluster and perform the following actions:
 - a. Create the Red Hat Advanced Cluster Management (RHACM) (ACM) policies according to the basic distributed unit (DU) profile and required customizations.

- b. Apply the generated policies to the hub cluster.

The ZTP process creates policies that direct ACM to apply the desired configuration to the cluster nodes.

18.16.6. Checking the installation status

The ArgoCD pipeline detects the **SiteConfig** and **PolicyGenTemplate** custom resources (CRs) in the Git repository and syncs them to the hub cluster. In the process, it generates installation and policy CRs and applies them to the hub cluster. You can monitor the progress of this synchronization in the ArgoCD dashboard.

Procedure

1. Monitor the progress of cluster installation using the following commands:

```
$ export CLUSTER=<clusterName>
```

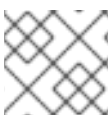
```
$ oc get agentclusterinstall -n $CLUSTER $CLUSTER -o jsonpath='{.status.conditions[?(@.type=="Completed")]}' | jq
```

```
$ curl -sk $(oc get agentclusterinstall -n $CLUSTER $CLUSTER -o jsonpath='{.status.debugInfo.eventsURL}') | jq '[-2,-1]'
```

2. Use the Red Hat Advanced Cluster Management (RHACM) (ACM) dashboard to monitor the progress of policy reconciliation.

18.16.7. Site cleanup

To remove a site and the associated installation and policy custom resources (CRs), remove the **SiteConfig** and site-specific **PolicyGenTemplate** CRs from the Git repository. The pipeline hooks remove the generated CRs.



NOTE

Before removing a **SiteConfig** CR you must detach the cluster from ACM.

18.16.7.1. Removing the ArgoCD pipeline

Use the following procedure if you want to remove the ArgoCD pipeline and all generated artifacts.

Procedure

1. Detach all clusters from ACM.
2. Delete all **SiteConfig** and **PolicyGenTemplate** custom resources (CRs) from your Git repository.
3. Delete the following namespaces:
 - All policy namespaces:

```
$ oc get policy -A
```

- **clusters-sub**
- **policies-sub**

4. Process the directory using the Kustomize tool:

```
$ oc delete -k cnf-features-deploy/ztp/gitops-subscriptions/argocd/deployment
```

18.17. TROUBLESHOOTING GITOPS ZTP

As noted, the ArgoCD pipeline synchronizes the **SiteConfig** and **PolicyGenTemplate** custom resources (CR) from the Git repository to the hub cluster. During this process, post-sync hooks create the installation and policy CRs that are also applied to the hub cluster. Use the following procedures to troubleshoot issues that might occur in this process.

18.17.1. Validating the generation of installation CRs

SiteConfig applies Installation custom resources (CR) to the hub cluster in a namespace with the name matching the site name. To check the status, enter the following command:

```
$ oc get AgentClusterInstall -n <clusterName>
```

If no object is returned, use the following procedure to troubleshoot the ArgoCD pipeline flow from **SiteConfig** to the installation CRs.

Procedure

1. Check the synchronization of the **SiteConfig** to the hub cluster using either of the following commands:

```
$ oc get siteconfig -A
```

or

```
$ oc get siteconfig -n clusters-sub
```

If the **SiteConfig** is missing, one of the following situations has occurred:

- The **clusters** application failed to synchronize the CR from the Git repository to the hub. Use the following command to verify this:

```
$ oc describe -n openshift-gitops application clusters
```

Check for **Status: Synced** and that the **Revision:** is the SHA of the commit you pushed to the subscribed repository.

- The pre-sync hook failed, possibly due to a failure to pull the container image. Check the ArgoCD dashboard for the status of the pre-sync job in the **clusters** application.

2. Verify the post hook job ran:

```
$ oc describe job -n clusters-sub siteconfig-post
```

- If successful, the returned output indicates **succeeded: 1**.
 - If the job fails, ArgoCD retries it. In some cases, the first pass will fail and the second pass will indicate that the job passed.
3. Check for errors in the post hook job:

```
$ oc get pod -n clusters-sub
```

Note the name of the **siteconfig-post-xxxxx** pod:

```
$ oc logs -n clusters-sub siteconfig-post-xxxxx
```

If the logs indicate errors, correct the conditions and push the corrected **SiteConfig** or **PolicyGenTemplate** to the Git repository.

18.17.2. Validating the generation of policy CRs

ArgoCD generates the policy custom resources (CRs) in the same namespace as the **PolicyGenTemplate** from which they were created. The same troubleshooting flow applies to all policy CRs generated from **PolicyGenTemplates** regardless of whether they are common, group, or site based.

To check the status of the policy CRs, enter the following commands:

```
$ export NS=<namespace>
```

```
$ oc get policy -n $NS
```

The returned output displays the expected set of policy wrapped CRs. If no object is returned, use the following procedure to troubleshoot the ArgoCD pipeline flow from **SiteConfig** to the policy CRs.

Procedure

1. Check the synchronization of the **PolicyGenTemplate** to the hub cluster:

```
$ oc get policygentemplate -A
```

or

```
$ oc get policygentemplate -n $NS
```

If the **PolicyGenTemplate** is not synchronized, one of the following situations has occurred:

- The clusters application failed to synchronize the CR from the Git repository to the hub. Use the following command to verify this:

```
$ oc describe -n openshift-gitops application clusters
```

Check for **Status: Synced** and that the **Revision:** is the SHA of the commit you pushed to the subscribed repository.

- The pre-sync hook failed, possibly due to a failure to pull the container image. Check the ArgoCD dashboard for the status of the pre-sync job in the **clusters** application.
2. Ensure the policies were copied to the cluster namespace. When ACM recognizes that policies apply to a **ManagedCluster**, ACM applies the policy CR objects to the cluster namespace:

```
$ oc get policy -n <clusterName>
```

ACM copies all applicable common, group, and site policies here. The policy names are **<policyNamespace>** and **<policyName>**.

3. Check the placement rule for any policies not copied to the cluster namespace. The **matchSelector** in the **PlacementRule** for those policies should match the labels on the **ManagedCluster**:

```
$ oc get placementrule -n $NS
```

4. Make a note of the **PlacementRule** name for the missing common, group, or site policy:

```
oc get placementrule -n $NS <placementRuleName> -o yaml
```

- The **status decisions** value should include your cluster name.
- The **key value** of the **matchSelector** in the spec should match the labels on your managed cluster. Check the labels on **ManagedCluster**:

```
oc get ManagedCluster $CLUSTER -o jsonpath='{.metadata.labels}' | jq
```

Example

```
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: group-test1-policies-placementrules
  namespace: group-test1-policies
spec:
  clusterSelector:
    matchExpressions:
      - key: group-test1
        operator: In
        values:
          - ""
  status:
    decisions:
      - clusterName: <myClusterName>
        clusterNamespace: <myClusterName>
```

5. Ensure all policies are compliant:

```
oc get policy -n $CLUSTER
```

If the Namespace, OperatorGroup, and Subscription policies are compliant but the Operator configuration policies are not it is likely that the Operators did not install.

