



# OpenShift Container Platform 4.10

## Updating clusters

Updating OpenShift Container Platform clusters



# OpenShift Container Platform 4.10 Updating clusters

---

Updating OpenShift Container Platform clusters

## Legal Notice

Copyright © 2023 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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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 updating, or upgrading, OpenShift Container Platform clusters. Updating your cluster is a simple process that does not require you to take your cluster offline.

## Table of Contents

<b>CHAPTER 1. UPDATING CLUSTERS OVERVIEW</b> .....	<b>5</b>
1.1. UNDERSTANDING OPENSIFT CONTAINER PLATFORM UPDATES	5
1.2. UNDERSTANDING UPDATE CHANNELS AND RELEASES	5
1.3. UNDERSTANDING CLUSTER OPERATOR CONDITION TYPES	5
<b>CHAPTER 2. UNDERSTANDING CLUSTER VERSION CONDITION TYPES</b> .....	<b>7</b>
2.1. PREPARING TO PERFORM AN EUS-TO-EUS UPDATE	7
2.2. UPDATING A CLUSTER USING THE WEB CONSOLE	7
2.3. UPDATING A CLUSTER WITHIN A MINOR VERSION USING THE COMMAND-LINE INTERFACE (CLI)	8
2.4. PERFORMING A CANARY ROLLOUT UPDATE	8
2.5. UPDATING A CLUSTER THAT INCLUDES RHEL COMPUTE MACHINES	8
2.6. UPDATING A CLUSTER IN A DISCONNECTED ENVIRONMENT	8
2.7. UPDATING HARDWARE ON NODES RUNNING IN VSPHERE	9
<b>CHAPTER 3. UNDERSTANDING OPENSIFT UPDATES</b> .....	<b>10</b>
3.1. INTRODUCTION TO OPENSIFT UPDATES	10
3.1.1. Common questions about update availability	10
3.1.2. About the OpenShift Update Service	12
3.1.3. Common terms	12
3.1.4. Additional resources	13
3.2. HOW CLUSTER UPDATES WORK	13
3.2.1. Evaluation of update availability	14
3.2.2. Release images	16
3.2.3. Update process workflow	17
3.2.4. Understanding how manifests are applied during an update	17
3.2.5. Understanding how the Machine Config Operator updates nodes	19
<b>CHAPTER 4. UNDERSTANDING UPDATE CHANNELS AND RELEASES</b> .....	<b>22</b>
4.1. UPDATE CHANNELS	23
4.1.1. fast-4.10 channel	23
4.1.2. stable-4.10 channel	23
4.1.3. eus-4.y channel	23
4.1.4. candidate-4.10 channel	23
4.1.5. Update recommendations in the channel	24
4.1.6. Update recommendations and Conditional Updates	24
4.1.7. Choosing the correct channel for your cluster	24
4.1.8. Restricted network clusters	25
4.1.9. Switching between channels	25
<b>CHAPTER 5. UNDERSTANDING OPENSIFT CONTAINER PLATFORM UPDATE DURATION</b> .....	<b>27</b>
5.1. PREREQUISITES	27
5.2. FACTORS AFFECTING UPDATE DURATION	27
5.3. CLUSTER UPDATE PHASES	27
5.3.1. Cluster Version Operator target update payload deployment	27
5.3.2. Machine Config Operator node updates	27
5.4. ESTIMATING CLUSTER UPDATE TIME	29
5.5. RED HAT ENTERPRISE LINUX (RHEL) COMPUTE NODES	30
<b>CHAPTER 6. PREPARING TO PERFORM AN EUS-TO-EUS UPDATE</b> .....	<b>31</b>
6.1. EUS-TO-EUS UPDATE	31
6.1.1. EUS-to-EUS update using the web console	32
6.1.2. EUS-to-EUS update using the CLI	33

6.1.3. EUS-to-EUS update for layered products and Operators installed through Operator Lifecycle Manager	35
<b>CHAPTER 7. PREPARING TO UPDATE A CLUSTER WITH MANUALLY MAINTAINED CREDENTIALS</b> . . . . .	<b>37</b>
7.1. UPDATE REQUIREMENTS FOR CLUSTERS WITH MANUALLY MAINTAINED CREDENTIALS	37
7.1.1. Cloud credential configuration options and update requirements by platform type	37
7.1.2. Determining the Cloud Credential Operator mode by using the web console	39
7.1.3. Determining the Cloud Credential Operator mode by using the CLI	41
7.2. CONFIGURING THE CLOUD CREDENTIAL OPERATOR UTILITY FOR A CLUSTER UPDATE	43
7.3. UPDATING CLOUD PROVIDER RESOURCES WITH THE CLOUD CREDENTIAL OPERATOR UTILITY	45
7.4. UPDATING CLOUD PROVIDER RESOURCES WITH MANUALLY MAINTAINED CREDENTIALS	47
7.5. INDICATING THAT THE CLUSTER IS READY TO UPGRADE	48
<b>CHAPTER 8. UPDATING A CLUSTER USING THE WEB CONSOLE</b> . . . . .	<b>50</b>
8.1. PREREQUISITES	50
8.2. PERFORMING A CANARY ROLLOUT UPDATE	51
8.3. PAUSING A MACHINEHEALTHCHECK RESOURCE BY USING THE WEB CONSOLE	52
8.4. ABOUT UPDATING SINGLE NODE OPENSIFT CONTAINER PLATFORM	52
8.5. UPDATING A CLUSTER BY USING THE WEB CONSOLE	53
8.6. CHANGING THE UPDATE SERVER BY USING THE WEB CONSOLE	54
<b>CHAPTER 9. UPDATING A CLUSTER USING THE CLI</b> . . . . .	<b>56</b>
9.1. PREREQUISITES	56
9.2. PAUSING A MACHINEHEALTHCHECK RESOURCE	57
9.3. ABOUT UPDATING SINGLE NODE OPENSIFT CONTAINER PLATFORM	58
9.4. UPDATING A CLUSTER BY USING THE CLI	58
9.5. UPDATING ALONG A CONDITIONAL UPGRADE PATH	61
9.6. CHANGING THE UPDATE SERVER BY USING THE CLI	62
<b>CHAPTER 10. PERFORMING A CANARY ROLLOUT UPDATE</b> . . . . .	<b>63</b>
10.1. ABOUT THE CANARY ROLLOUT UPDATE PROCESS AND MCPS	64
10.2. ABOUT PERFORMING A CANARY ROLLOUT UPDATE	64
10.3. CREATING MACHINE CONFIG POOLS TO PERFORM A CANARY ROLLOUT UPDATE	65
10.4. PAUSING THE MACHINE CONFIG POOLS	67
10.5. PERFORMING THE CLUSTER UPDATE	68
10.6. UNPAUSING THE MACHINE CONFIG POOLS	68
10.6.1. In case of application failure	68
10.7. MOVING A NODE TO THE ORIGINAL MACHINE CONFIG POOL	68
<b>CHAPTER 11. UPDATING A CLUSTER THAT INCLUDES RHEL COMPUTE MACHINES</b> . . . . .	<b>70</b>
11.1. PREREQUISITES	70
11.2. UPDATING A CLUSTER BY USING THE WEB CONSOLE	70
11.3. OPTIONAL: ADDING HOOKS TO PERFORM ANSIBLE TASKS ON RHEL MACHINES	72
11.3.1. About Ansible hooks for upgrades	72
11.3.2. Configuring the Ansible inventory file to use hooks	72
11.3.3. Available hooks for RHEL compute machines	73
11.4. UPDATING RHEL COMPUTE MACHINES IN YOUR CLUSTER	73
<b>CHAPTER 12. UPDATING A CLUSTER IN A DISCONNECTED ENVIRONMENT</b> . . . . .	<b>77</b>
12.1. ABOUT CLUSTER UPDATES IN A DISCONNECTED ENVIRONMENT	77
12.1.1. Mirroring the OpenShift Container Platform image repository	77
12.1.2. Performing a cluster update in a disconnected environment	77
12.1.3. Uninstalling the OpenShift Update Service from a cluster	77
12.2. MIRRORING THE OPENSIFT CONTAINER PLATFORM IMAGE REPOSITORY	77
12.2.1. Prerequisites	77

12.2.2. Preparing your mirror host	78
12.2.2.1. Installing the OpenShift CLI by downloading the binary	78
Installing the OpenShift CLI on Linux	78
Installing the OpenShift CLI on Windows	78
Installing the OpenShift CLI on macOS	79
12.2.2.2. Configuring credentials that allow images to be mirrored	79
12.2.3. Mirroring the OpenShift Container Platform image repository	81
12.3. UPDATING A CLUSTER IN A DISCONNECTED ENVIRONMENT USING THE OPENSIFT UPDATE SERVICE	85
12.3.1. Using the OpenShift Update Service in a disconnected environment	85
12.3.2. Prerequisites	85
12.3.3. Configuring access to a secured registry for the OpenShift Update Service	85
12.3.4. Updating the global cluster pull secret	86
12.3.5. Installing the OpenShift Update Service Operator	87
12.3.5.1. Installing the OpenShift Update Service Operator by using the web console	87
12.3.5.2. Installing the OpenShift Update Service Operator by using the CLI	88
12.3.6. Creating the OpenShift Update Service graph data container image	90
12.3.7. Creating an OpenShift Update Service application	91
12.3.7.1. Creating an OpenShift Update Service application by using the web console	91
12.3.7.2. Creating an OpenShift Update Service application by using the CLI	92
12.3.7.2.1. Configuring the Cluster Version Operator (CVO)	93
12.3.8. Next steps	94
12.4. UPDATING A CLUSTER IN A DISCONNECTED ENVIRONMENT WITHOUT THE OPENSIFT UPDATE SERVICE	95
12.4.1. Prerequisites	95
12.4.2. Pausing a MachineHealthCheck resource	95
12.4.3. Retrieving a release image digest	96
12.4.4. Upgrading the disconnected cluster	97
12.4.5. Configuring image registry repository mirroring	98
12.4.6. Widening the scope of the mirror image catalog to reduce the frequency of cluster node reboots	102
12.4.7. Additional resources	104
12.5. UNINSTALLING THE OPENSIFT UPDATE SERVICE FROM A CLUSTER	104
12.5.1. Deleting an OpenShift Update Service application	104
12.5.1.1. Deleting an OpenShift Update Service application by using the web console	104
12.5.1.2. Deleting an OpenShift Update Service application by using the CLI	104
12.5.2. Uninstalling the OpenShift Update Service Operator	105
12.5.2.1. Uninstalling the OpenShift Update Service Operator by using the web console	105
12.5.2.2. Uninstalling the OpenShift Update Service Operator by using the CLI	105
<b>CHAPTER 13. UPDATING HARDWARE ON NODES RUNNING ON VSPHERE</b> .....	<b>108</b>
13.1. UPDATING VIRTUAL HARDWARE ON VSPHERE	108
13.1.1. Updating the virtual hardware for control plane nodes on vSphere	108
13.1.2. Updating the virtual hardware for compute nodes on vSphere	109
13.1.3. Updating the virtual hardware for template on vSphere	110
13.2. SCHEDULING AN UPDATE FOR VIRTUAL HARDWARE ON VSPHERE	111





# CHAPTER 1. UPDATING CLUSTERS OVERVIEW

You can update an OpenShift Container Platform 4 cluster with a single operation by using the web console or the OpenShift CLI (**oc**).

## 1.1. UNDERSTANDING OPENSIFT CONTAINER PLATFORM UPDATES

[About the OpenShift Update Service](#): For clusters with internet access, Red Hat provides over-the-air updates by using an OpenShift Container Platform update service as a hosted service located behind public APIs.

## 1.2. UNDERSTANDING UPDATE CHANNELS AND RELEASES

[Update channels and releases](#): With update channels, you can choose an update strategy. Update channels are specific to a minor version of OpenShift Container Platform. Update channels only control release selection and do not impact the version of the cluster that you install. The **openshift-install** binary file for a specific version of the OpenShift Container Platform always installs that minor version. For more information, see the following:

- [Upgrading version paths](#)
- [Understanding fast and stable channel use and strategies](#)
- [Understanding restricted network clusters](#)
- [Switching between channels](#)
- [Understanding conditional updates](#)

## 1.3. UNDERSTANDING CLUSTER OPERATOR CONDITION TYPES

The status of cluster Operators includes their condition type, which informs you of the current state of your Operator's health. The following definitions cover a list of some common ClusterOperator condition types. Operators that have additional condition types and use Operator-specific language have been omitted.

The Cluster Version Operator (CVO) is responsible for collecting the status conditions from cluster Operators so that cluster administrators can better understand the state of the OpenShift Container Platform cluster.

- **Available**: The condition type **Available** indicates that an Operator is functional and available in the cluster. If the status is **False**, at least one part of the operand is non-functional and the condition requires an administrator to intervene.
- **Progressing**: The condition type **Progressing** indicates that an Operator is actively rolling out new code, propagating configuration changes, or otherwise moving from one steady state to another. Operators do not report the condition type **Progressing** as **True** when they are reconciling a previous known state. If the observed cluster state has changed and the Operator is reacting to it, then the status reports back as **True**, since it is moving from one steady state to another.
- **Degraded**: The condition type **Degraded** indicates that an Operator has a current state that does not match its required state over a period of time. The period of time can vary by component, but a **Degraded** status represents persistent observation of an Operator's condition. As a result, an Operator does not fluctuate in and out of the **Degraded** state.

There might be a different condition type if the transition from one state to another does not persist over a long enough period to report **Degraded**. An Operator does not report **Degraded** during the course of a normal update. An Operator may report **Degraded** in response to a persistent infrastructure failure that requires eventual administrator intervention.



#### NOTE

This condition type is only an indication that something may need investigation and adjustment. As long as the Operator is available, the **Degraded** condition does not cause user workload failure or application downtime.

- Upgradeable: The condition type **Upgradeable** indicates whether the Operator is safe to update based on the current cluster state. The message field contains a human-readable description of what the administrator needs to do for the cluster to successfully update. The CVO allows updates when this condition is **True**, **Unknown** or missing. When the **Upgradeable** status is **False**, only minor updates are impacted, and the CVO prevents the cluster from performing impacted updates unless forced.

## CHAPTER 2. UNDERSTANDING CLUSTER VERSION CONDITION TYPES

The Cluster Version Operator (CVO) monitors cluster Operators and other components, and is responsible for collecting the status of both the cluster version and its Operators. This status includes the condition type, which informs you of the health and current state of the OpenShift Container Platform cluster.

In addition to **Available**, **Progressing**, and **Upgradeable**, there are condition types that affect cluster versions and Operators.

- **Failing**: The cluster version condition type **Failing** indicates that a cluster cannot reach its desired state, is unhealthy, and requires an administrator to intervene.
- **Invalid**: The cluster version condition type **Invalid** indicates that the cluster version has an error that prevents the server from taking action. The CVO only reconciles the current state as long as this condition is set.
- **RetrievedUpdates**: The cluster version condition type **RetrievedUpdates** indicates whether or not available updates have been retrieved from the upstream update server. The condition is **Unknown** before retrieval, **False** if the updates either recently failed or could not be retrieved, or **True** if the **availableUpdates** field is both recent and accurate.
- **ReleaseAccepted**: The cluster version condition type **ReleaseAccepted** with a **True** status indicates that the requested release payload was successfully loaded without failure during image verification and precondition checking.

### 2.1. PREPARING TO PERFORM AN EUS-TO-EUS UPDATE

[Preparing to perform an EUS-to-EUS update](#) : Due to fundamental Kubernetes design, all OpenShift Container Platform updates between minor versions must be serialized. You must update from OpenShift Container Platform 4.8 to 4.9, and then to 4.10. You cannot update from OpenShift Container Platform 4.8 to 4.10 directly. However, if you want to update between two Extended Update Support (EUS) versions, you can do so by incurring only a single reboot of non-control plane hosts. For more information, see the following:

- [Updating EUS-to-EUS](#)

### 2.2. UPDATING A CLUSTER USING THE WEB CONSOLE

[Updating a cluster within a minor version using the web console](#) : You can update an OpenShift Container Platform cluster by using the web console. The following steps update a cluster within a minor version. You can use the same instructions for updating a cluster between minor versions.

- [Performing a canary rollout update](#)
- [Pausing a MachineHealthCheck resource](#)
- [About updating OpenShift Container Platform on a single-node cluster](#)
- [Updating a cluster by using the web console](#)
- [Changing the update server by using the web console](#)

## 2.3. UPDATING A CLUSTER WITHIN A MINOR VERSION USING THE COMMAND-LINE INTERFACE (CLI)

[Updating a cluster within a minor version using the CLI](#) : You can update an OpenShift Container Platform cluster within a minor version by using the OpenShift CLI (**oc**). The following steps update a cluster within a minor version. You can use the same instructions for updating a cluster between minor versions.

- [Pausing a MachineHealthCheck resource](#)
- [About updating OpenShift Container Platform on a single-node cluster](#)
- [Updating a cluster by using the CLI](#)
- [Changing the update server by using the CLI](#)

## 2.4. PERFORMING A CANARY ROLLOUT UPDATE

[Performing a canary rollout update](#) : By controlling the rollout of an update to the worker nodes, you can ensure that mission-critical applications stay available during the whole update, even if the update process causes your applications to fail. Depending on your organizational needs, you might want to update a small subset of worker nodes, evaluate cluster and workload health over a period of time, and then update the remaining nodes. This is referred to as a *canary* update. Alternatively, you might also want to fit worker node updates, which often requires a host reboot, into smaller defined maintenance windows when it is not possible to take a large maintenance window to update the entire cluster at one time. You can perform the following procedures:

- [Creating machine configuration pools to perform a canary rollout update](#)
- [Pausing the machine configuration pools](#)
- [Performing the cluster update](#)
- [Unpausing the machine configuration pools](#)
- [Moving a node to the original machine configuration pool](#)

## 2.5. UPDATING A CLUSTER THAT INCLUDES RHEL COMPUTE MACHINES

[Updating a cluster that includes RHEL compute machines](#) : You can update an OpenShift Container Platform cluster. If your cluster contains Red Hat Enterprise Linux (RHEL) machines, you must perform additional steps to update those machines. You can perform the following procedures:

- [Updating a cluster by using the web console](#)
- [Optional: Adding hooks to perform Ansible tasks on RHEL machines](#)
- [Updating RHEL compute machines in your cluster](#)

## 2.6. UPDATING A CLUSTER IN A DISCONNECTED ENVIRONMENT

[About cluster updates in a disconnected environment](#) : If your mirror host cannot access both the internet and the cluster, you can mirror the images to a file system that is disconnected from that

environment. You can then bring that host or removable media across that gap. If the local container registry and the cluster are connected to the mirror host of a registry, you can directly push the release images to the local registry.

- [Preparing your mirror host](#)
- [Configuring credentials that allow images to be mirrored](#)
- [Mirroring the OpenShift Container Platform image repository](#)
- [Updating the disconnected cluster](#)
- [Configuring image registry repository mirroring](#)
- [Widening the scope of the mirror image catalog to reduce the frequency of cluster node reboots](#)
- [Installing the OpenShift Update Service Operator](#)
- [Creating an OpenShift Update Service application](#)
- [Deleting an OpenShift Update Service application](#)
- [Uninstalling the OpenShift Update Service Operator](#)

## 2.7. UPDATING HARDWARE ON NODES RUNNING IN VSPHERE

[Updating hardware on vSphere](#): You must ensure that your nodes running in vSphere are running on the hardware version supported by OpenShift Container Platform. Currently, hardware version 13 or later is supported for vSphere virtual machines in a cluster. For more information, see the following:

- [Updating virtual hardware on vSphere](#)
- [Scheduling an update for virtual hardware on vSphere](#)



### IMPORTANT

Using hardware version 13 for your cluster nodes running on vSphere is now deprecated. This version is still fully supported, but support will be removed in a future version of OpenShift Container Platform. Hardware version 15 is now the default for vSphere virtual machines in OpenShift Container Platform.

## CHAPTER 3. UNDERSTANDING OPENSIFT UPDATES

### 3.1. INTRODUCTION TO OPENSIFT UPDATES

With OpenShift Container Platform 4, you can update an OpenShift Container Platform cluster with a single operation by using the web console or the OpenShift CLI (**oc**). Platform administrators can view new update options either by going to **Administration** → **Cluster Settings** in the web console or by looking at the output of the **oc adm upgrade** command.

Red Hat hosts a public OpenShift Update Service (OSUS), which serves a graph of update possibilities based on the OpenShift Container Platform release images in the official registry. The graph contains update information for any public OCP release. OpenShift Container Platform clusters are configured to connect to the OSUS by default, and the OSUS responds to clusters with information about known update targets.

An update begins when either a cluster administrator or an automatic update controller edits the custom resource (CR) of the Cluster Version Operator (CVO) with a new version. To reconcile the cluster with the newly specified version, the CVO retrieves the target release image from an image registry and begins to apply changes to the cluster.



#### NOTE

Operators previously installed through Operator Lifecycle Manager (OLM) follow a different process for updates. See [Updating installed Operators](#) for more information.

The target release image contains manifest files for all cluster components that form a specific OCP version. When updating the cluster to a new version, the CVO applies manifests in separate stages called Runlevels. Most, but not all, manifests support one of the cluster Operators. As the CVO applies a manifest to a cluster Operator, the Operator might perform update tasks to reconcile itself with its new specified version.

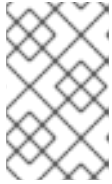
The CVO monitors the state of each applied resource and the states reported by all cluster Operators. The CVO only proceeds with the update when all manifests and cluster Operators in the active Runlevel reach a stable condition. After the CVO updates the entire control plane through this process, the Machine Config Operator (MCO) updates the operating system and configuration of every node in the cluster.

#### 3.1.1. Common questions about update availability

There are several factors that affect if and when an update is made available to an OpenShift Container Platform cluster. The following list provides common questions regarding the availability of an update:

##### What are the differences between each of the update channels?

- A new release is initially added to the **candidate** channel.
- After successful final testing, a release on the **candidate** channel is promoted to the **fast** channel, an errata is published, and the release is now fully supported.
- After a delay, a release on the **fast** channel is finally promoted to the **stable** channel. This delay represents the only difference between the **fast** and **stable** channels.

**NOTE**

For the latest z-stream releases, this delay may generally be a week or two. However, the delay for initial updates to the latest minor version may take much longer, generally 45-90 days.

- Releases promoted to the **stable** channel are simultaneously promoted to the **eus** channel. The primary purpose of the **eus** channel is to serve as a convenience for clusters performing an EUS-to-EUS update.

**Is a release on the **stable** channel safer or more supported than a release on the **fast** channel?**

- If a regression is identified for a release on a **fast** channel, it will be resolved and managed to the same extent as if that regression was identified for a release on the **stable** channel.
- The only difference between releases on the **fast** and **stable** channels is that a release only appears on the **stable** channel after it has been on the **fast** channel for some time, which provides more time for new update risks to be discovered.

**What does it mean if an update is supported but not recommended?**

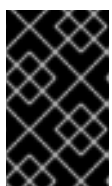
- Red Hat continuously evaluates data from multiple sources to determine whether updates from one version to another lead to issues. If an issue is identified, an update path may no longer be recommended to users. However, even if the update path is not recommended, customers are still supported if they perform the update.
- Red Hat does not block users from updating to a certain version. Red Hat may declare conditional update risks, which may or may not apply to a particular cluster.
  - Declared risks provide cluster administrators more context about a supported update. Cluster administrators can still accept the risk and update to that particular target version. This update is always supported despite not being recommended in the context of the conditional risk.

**What if I see that an update to a particular release is no longer recommended?**

- If Red Hat removes update recommendations from any supported release due to a regression, a superseding update recommendation will be provided to a future version that corrects the regression. There may be a delay while the defect is corrected, tested, and promoted to your selected channel.

**How long until the next z-stream release is made available on the **fast** and **stable** channels?**

- While the specific cadence can vary based on a number of factors, new z-stream releases for the latest minor version are typically made available about every week. Older minor versions, which have become more stable over time, may take much longer for new z-stream releases to be made available.

**IMPORTANT**

These are only estimates based on past data about z-stream releases. Red Hat reserves the right to change the release frequency as needed. Any number of issues could cause irregularities and delays in this release cadence.

- Once a z-stream release is published, it also appears in the **fast** channel for that minor version. After a delay, the z-stream release may then appear in that minor version's **stable** channel.

## Additional resources

- [Understanding update channels and releases](#)

### 3.1.2. About the OpenShift Update Service

The OpenShift Update Service (OSUS) provides update recommendations to OpenShift Container Platform, including Red Hat Enterprise Linux CoreOS (RHCOS). It provides a graph, or diagram, that contains the *vertices* of component Operators and the *edges* that connect them. The edges in the graph show which versions you can safely update to. The vertices are update payloads that specify the intended state of the managed cluster components.

The Cluster Version Operator (CVO) in your cluster checks with the OpenShift Update Service to see the valid updates and update paths based on current component versions and information in the graph. When you request an update, the CVO uses the corresponding release image to update your cluster. The release artifacts are hosted in Quay as container images.

To allow the OpenShift Update Service to provide only compatible updates, a release verification pipeline drives automation. Each release artifact is verified for compatibility with supported cloud platforms and system architectures, as well as other component packages. After the pipeline confirms the suitability of a release, the OpenShift Update Service notifies you that it is available.



#### IMPORTANT

The OpenShift Update Service displays all recommended updates for your current cluster. If an update path is not recommended by the OpenShift Update Service, it might be because of a known issue with the update or the target release.

Two controllers run during continuous update mode. The first controller continuously updates the payload manifests, applies the manifests to the cluster, and outputs the controlled rollout status of the Operators to indicate whether they are available, upgrading, or failed. The second controller polls the OpenShift Update Service to determine if updates are available.



#### IMPORTANT

Only updating to a newer version is supported. Reverting or rolling back your cluster to a previous version is not supported. If your update fails, contact Red Hat support.

During the update process, the Machine Config Operator (MCO) applies the new configuration to your cluster machines. The MCO cordons the number of nodes specified by the **maxUnavailable** field on the machine configuration pool and marks them unavailable. By default, this value is set to **1**. The MCO then applies the new configuration and reboots the machine.

If you use Red Hat Enterprise Linux (RHEL) machines as workers, the MCO does not update the kubelet because you must update the OpenShift API on the machines first.

With the specification for the new version applied to the old kubelet, the RHEL machine cannot return to the **Ready** state. You cannot complete the update until the machines are available. However, the maximum number of unavailable nodes is set to ensure that normal cluster operations can continue with that number of machines out of service.

The OpenShift Update Service is composed of an Operator and one or more application instances.

### 3.1.3. Common terms



## Control plane

The *control plane*, which is composed of control plane machines, manages the OpenShift Container Platform cluster. The control plane machines manage workloads on the compute machines, which are also known as worker machines.

## Cluster Version Operator

The *Cluster Version Operator* (CVO) starts the update process for the cluster. It checks with OSUS based on the current cluster version and retrieves the graph which contains available or possible update paths.

## Machine Config Operator

The *Machine Config Operator* (MCO) is a cluster-level Operator that manages the operating system and machine configurations. Through the MCO, platform administrators can configure and update systemd, CRI-O and Kubelet, the kernel, NetworkManager, and other system features on the worker nodes.

## OpenShift Update Service

The *OpenShift Update Service* (OSUS) provides over-the-air updates to OpenShift Container Platform, including to Red Hat Enterprise Linux CoreOS (RHCOS). It provides a graph, or diagram, that contains the vertices of component Operators and the edges that connect them.

## Channels

*Channels* declare an update strategy tied to minor versions of OpenShift Container Platform. The OSUS uses this configured strategy to recommend update edges consistent with that strategy.

## Recommended update edge

A *recommended update edge* is a recommended update between OpenShift Container Platform releases. Whether a given update is recommended can depend on the cluster's configured channel, current version, known bugs, and other information. OSUS communicates the recommended edges to the CVO, which runs in every cluster.

## Extended Update Support

All post-4.7 even-numbered minor releases are labeled as *Extended Update Support* (EUS) releases. These releases introduce a verified update path between EUS releases, permitting customers to streamline updates of worker nodes and formulate update strategies of EUS-to-EUS OpenShift Container Platform releases that result in fewer reboots of worker nodes.

For more information, see [Red Hat OpenShift Extended Update Support \(EUS\) Overview](#) .

## Additional resources

- [Machine config overview](#)
- [Using the OpenShift Update Service in a disconnected environment](#)
- [Update channels](#)

### 3.1.4. Additional resources

- For more detailed information about each major aspect of the update process, see [How cluster updates work](#).

## 3.2. HOW CLUSTER UPDATES WORK

The following sections describe each major aspect of the OpenShift Container Platform (OCP) update process in detail. For a general overview of how updates work, see the [Introduction to OpenShift updates](#).

### 3.2.1. Evaluation of update availability

The Cluster Version Operator (CVO) periodically queries the OpenShift Update Service (OSUS) for the most recent data about update possibilities. This data is based on the cluster's subscribed channel. The CVO then saves information about update recommendations into either the **availableUpdates** or **conditionalUpdates** field of its **ClusterVersion** resource.

The CVO periodically checks the conditional updates for update risks. These risks are conveyed through the data served by the OSUS, which contains information for each version about known issues that might affect a cluster updated to that version. Most risks are limited to clusters with specific characteristics, such as clusters with a certain size or clusters that are deployed in a particular cloud platform.

The CVO continuously evaluates its cluster characteristics against the conditional risk information for each conditional update. If the CVO finds that the cluster matches the criteria, the CVO stores this information in the **conditionalUpdates** field of its **ClusterVersion** resource. If the CVO finds that the cluster does not match the risks of an update, or that there are no risks associated with the update, it stores the target version in the **availableUpdates** field of its **ClusterVersion** resource.

The user interface, either the web console or the OpenShift CLI (**oc**), presents this information in sectioned headings to the administrator. Each **supported but not recommended** update recommendation contains a link to further resources about the risk so that the administrator can make an informed decision about the update.

You can inspect all available updates with the following command:

```
$ oc adm upgrade --include-not-recommended
```

The additional **--include-not-recommended** parameter includes updates that are available but not recommended due to a known risk that applies to the cluster.

#### Example output

```
Cluster version is 4.10.22

Upstream is unset, so the cluster will use an appropriate default.
Channel: fast-4.11 (available channels: candidate-4.10, candidate-4.11, eus-4.10, fast-4.10, fast-4.11,
stable-4.10)

Recommended updates:

VERSION  IMAGE
4.10.26  quay.io/openshift-release-dev/ocp-
release@sha256:e1fa1f513068082d97d78be643c369398b0e6820afab708d26acda2262940954
4.10.25  quay.io/openshift-release-dev/ocp-
release@sha256:ed84fb3fbe026b3bbb4a2637ddd874452ac49c6ead1e15675f257e28664879cc
4.10.24  quay.io/openshift-release-dev/ocp-
release@sha256:aab51636460b5a9757b736a29bc92ada6e6e6282e46b06e6fd483063d590d62a
4.10.23  quay.io/openshift-release-dev/ocp-
release@sha256:e40e49d722cb36a95fa1c03002942b967ccbd7d68de10e003f0baa69abad457b
```

Supported but not recommended updates:

```
Version: 4.11.0
Image: quay.io/openshift-release-dev/ocp-
release@sha256:300bce8246cf880e792e106607925de0a404484637627edf5f517375517d54a4
Recommended: False
Reason: RPMOSTreeTimeout
Message: Nodes with substantial numbers of containers and CPU contention may not reconcile
machine configuration https://bugzilla.redhat.com/show\_bug.cgi?id=2111817#c22
```

One way to inspect the underlying availability data created by the CVO is by querying the **ClusterVersion** resource with the following command:

```
$ oc get clusterversion version -o json | jq '.status.availableUpdates'
```

### Example output

```
[
  {
    "channels": [
      "candidate-4.11",
      "candidate-4.12",
      "fast-4.11",
      "fast-4.12"
    ],
    "image": "quay.io/openshift-release-dev/ocp-
release@sha256:400267c7f4e61c6bfa0a59571467e8bd85c9188e442cbd820cc8263809be3775",
    "url": "https://access.redhat.com/errata/RHBA-2023:3213",
    "version": "4.11.41"
  },
  ...
]
```

A similar command can be used to check conditional updates:

```
$ oc get clusterversion version -o json | jq '.status.conditionalUpdates'
```

### Example output

```
[
  {
    "conditions": [
      {
        "lastTransitionTime": "2023-05-30T16:28:59Z",
        "message": "The 4.11.36 release only resolves an installation issue
https://issues.redhat.com/browse/OCPBUGS-11663 , which does not affect already running clusters.
4.11.36 does not include fixes delivered in recent 4.11.z releases and therefore upgrading from these
versions would cause fixed bugs to reappear. Red Hat does not recommend upgrading clusters to
4.11.36 version for this reason. https://access.redhat.com/solutions/7007136",
        "reason": "PatchesOlderRelease",
        "status": "False",
        "type": "Recommended"
      }
    ],
  },
]
```

```

"release": {
  "channels": [...],
  "image": "quay.io/openshift-release-dev/ocp-
release@sha256:8c04176b771a62abd801fcda3e952633566c8b5ff177b93592e8e8d2d1f8471d",
  "url": "https://access.redhat.com/errata/RHBA-2023:1733",
  "version": "4.11.36"
},
"risks": [...]
},
...
]

```

### Additional resources

- [Update recommendation removals and Conditional Updates](#)

### 3.2.2. Release images

A release image is the delivery mechanism for a specific OpenShift Container Platform (OCP) version. It contains the release metadata, a Cluster Version Operator (CVO) binary matching the release version, every manifest needed to deploy individual OpenShift cluster Operators, and a list of SHA digest-versioned references to all container images that make up this OpenShift version.

You can inspect the content of a specific release image by running the following command:

```
$ oc adm release extract <release image>
```

### Example output

```

$ oc adm release extract quay.io/openshift-release-dev/ocp-release:4.12.6-x86_64
Extracted release payload from digest
sha256:800d1e39d145664975a3bb7cbc6e674fbf78e3c45b5dde9ff2c5a11a8690c87b created at
2023-03-01T12:46:29Z

$ ls
0000_03_authorization-openshift_01_rolebindingrestriction.crd.yaml
0000_03_config-operator_01_proxy.crd.yaml
0000_03_marketplace-operator_01_operatorhub.crd.yaml
0000_03_marketplace-operator_02_operatorhub.cr.yaml
0000_03_quota-openshift_01_clusterresourcequota.crd.yaml ❶
...
0000_90_service-ca-operator_02_prometheusrrolebinding.yaml ❷
0000_90_service-ca-operator_03_servicemonitor.yaml
0000_99_machine-api-operator_00_tombstones.yaml
image-references ❸
release-metadata

```

- ❶ Manifest for **ClusterResourceQuota** CRD, to be applied on Runlevel 03
- ❷ Manifest for **PrometheusRoleBinding** resource for the **service-ca-operator**, to be applied on Runlevel 90
- ❸ List of SHA digest-versioned references to all required images

### 3.2.3. Update process workflow

The following steps represent a detailed workflow of the OpenShift Container Platform (OCP) update process:

1. The target version is stored in the **spec.desiredUpdate.version** field of the **ClusterVersion** resource, which may be managed through the web console or the CLI.
2. The Cluster Version Operator (CVO) detects that the **desiredUpdate** in the **ClusterVersion** resource differs from the current cluster version. Using graph data from the OpenShift Update Service, the CVO resolves the desired cluster version to a pull spec for the release image.
3. The CVO validates the integrity and authenticity of the release image. Red Hat publishes cryptographically-signed statements about published release images at predefined locations by using image SHA digests as unique and immutable release image identifiers. The CVO utilizes a list of built-in public keys to validate the presence and signatures of the statement matching the checked release image.
4. The CVO creates a job named **version-\$version-\$hash** in the **openshift-cluster-version** namespace. This job uses containers that are executing the release image, so the cluster downloads the image through the container runtime. The job then extracts the manifests and metadata from the release image to a shared volume that is accessible to the CVO.
5. The CVO validates the extracted manifests and metadata.
6. The CVO checks some preconditions to ensure that no problematic condition is detected in the cluster. Certain conditions can prevent updates from proceeding. These conditions are either determined by the CVO itself, or reported by individual cluster Operators that detect some details about the cluster that the Operator considers problematic for the update.
7. The CVO records the accepted release in **status.desired** and creates a **status.history** entry about the new update.
8. The CVO begins applying the manifests from the release image. Cluster Operators are updated in separate stages called Runlevels, and the CVO ensures that all Operators in a Runlevel finish updating before it proceeds to the next level.
9. Manifests for the CVO itself are applied early in the process. When the CVO deployment is applied, the current CVO pod terminates, and a CVO pod using the new version starts. The new CVO proceeds to apply the remaining manifests.
10. The update proceeds until the entire control plane is updated to the new version. Individual cluster Operators might perform update tasks on their domain of the cluster, and while they do so, they report their state through the **Progressing=True** condition.
11. The Machine Config Operator (MCO) manifests are applied towards the end of the process. The updated MCO then begins updating the system configuration and operating system of every node. Each node might be drained, updated, and rebooted before it starts to accept workloads again.

The cluster reports as updated after the control plane update is finished, usually before all nodes are updated. After the update, the CVO maintains all cluster resources to match the state delivered in the release image.

### 3.2.4. Understanding how manifests are applied during an update

Some manifests supplied in a release image must be applied in a certain order because of the

dependencies between them. For example, the **CustomResourceDefinition** resource must be created before the matching custom resources. Additionally, there is a logical order in which the individual cluster Operators must be updated to minimize disruption in the cluster. The Cluster Version Operator (CVO) implements this logical order through the concept of Runlevels.

These dependencies are encoded in the filenames of the manifests in the release image:

```
0000_<runlevel>_<component>_<manifest-name>.yaml
```

For example:

```
0000_03_config-operator_01_proxy.crd.yaml
```

The CVO internally builds a dependency graph for the manifests, where the CVO obeys the following rules:

- During an update, manifests at a lower Runlevel are applied before those at a higher Runlevel.
- Within one Runlevel, manifests for different components can be applied in parallel.
- Within one Runlevel, manifests for a single component are applied in lexicographic order.

The CVO then applies manifests following the generated dependency graph.



#### NOTE

For some resource types, the CVO monitors the resource after its manifest is applied, and considers it to be successfully updated only after the resource reaches a stable state. Achieving this stable state can take some time. This is especially true for cluster Operators, which might perform their own update actions in the cluster after the CVO deploys their new versions. While the additional update actions take place, these cluster Operators temporarily set their **Progressing** condition to **True**.

The CVO waits until all cluster Operators in the Runlevel meet the following conditions before it proceeds to the next Runlevel:

- The cluster Operators have an **Available=True** condition.
- The cluster Operators have a **Degraded=False** condition.
- The cluster Operators declare they have achieved the desired version in their ClusterOperator resource.

Some actions can take significant time to finish. The CVO waits for the actions to complete in order to ensure the subsequent Runlevels can proceed safely. The process of applying all manifests is expected to take 60 to 120 minutes in total; see **Understanding OpenShift Container Platform update duration** for more information about factors that influence update duration.

✓ Completed
🔄 In progress
⌚ Waiting



341\_OpenShift\_0623

In the previous example diagram, the CVO is waiting until all work is completed at Runlevel 20. The CVO has applied all manifests to the Operators in the Runlevel, but the **kube-apiserver-operator ClusterOperator** performs some actions after its new version was deployed. The **kube-apiserver-operator ClusterOperator** declares this progress through the **Progressing=True** condition and by not declaring the new version as reconciled in its **status.versions**. The CVO waits until the ClusterOperator reports an acceptable status, and then it will start applying manifests at Runlevel 25.

### Additional resources

- [Understanding OpenShift Container Platform update duration](#)

### 3.2.5. Understanding how the Machine Config Operator updates nodes

The Machine Config Operator (MCO) applies a new machine configuration to each control plane node and compute node. During the machine configuration update, control plane nodes and compute nodes are organized into their own machine config pools, where the pools of machines are updated in parallel. The **.spec.maxUnavailable** parameter, which has a default value of **1**, determines how many nodes in a machine config pool can simultaneously undergo the update process.

When the machine configuration update process begins, the MCO checks the amount of currently

unavailable nodes in a pool. If there are fewer unavailable nodes than the value of **.spec.maxUnavailable**, the MCO initiates the following sequence of actions on available nodes in the pool:

1. Cordon and drain the node



#### NOTE

When a node is cordoned, workloads cannot be scheduled to it.

2. Update the system configuration and operating system (OS) of the node
3. Reboot the node
4. Uncordon the node

A node undergoing this process is unavailable until it is uncordoned and workloads can be scheduled to it again. The MCO begins updating nodes until the number of unavailable nodes is equal to the value of **.spec.maxUnavailable**.

As a node completes its update and becomes available, the number of unavailable nodes in the machine config pool is once again fewer than **.spec.maxUnavailable**. If there are remaining nodes that need to be updated, the MCO initiates the update process on a node until the **.spec.maxUnavailable** limit is once again reached. This process repeats until each control plane node and compute node has been updated.

The following example workflow describes how this process might occur in a machine config pool with 5 nodes, where **.spec.maxUnavailable** is 3 and all nodes are initially available:

1. The MCO cordons nodes 1, 2, and 3, and begins to drain them.
2. Node 2 finishes draining, reboots, and becomes available again. The MCO cordons node 4 and begins draining it.
3. Node 1 finishes draining, reboots, and becomes available again. The MCO cordons node 5 and begins draining it.
4. Node 3 finishes draining, reboots, and becomes available again.
5. Node 5 finishes draining, reboots, and becomes available again.
6. Node 4 finishes draining, reboots, and becomes available again.

Because the update process for each node is independent of other nodes, some nodes in the example above finish their update out of the order in which they were cordoned by the MCO.

You can check the status of the machine configuration update by running the following command:

```
$ 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	rendered-worker-1d871ac76e1951d32b2fe92369879826	False	True	False	2
1	1	0	22h		

### Additional resources

- [Machine config overview](#)

## CHAPTER 4. UNDERSTANDING UPDATE CHANNELS AND RELEASES

Update channels are the mechanism by which users declare the OpenShift Container Platform minor version they intend to update their clusters to. They also allow users to choose the timing and level of support their updates will have through the **fast**, **stable**, **candidate**, and **eus** channel options. The Cluster Version Operator uses an update graph based on the channel declaration, along with other conditional information, to provide a list of recommended and conditional updates available to the cluster.

Update channels correspond to a minor version of OpenShift Container Platform. The version number in the channel represents the target minor version that the cluster will eventually be updated to, even if it is higher than the cluster's current minor version.

For instance, OpenShift Container Platform 4.10 update channels provide the following recommendations:

- Updates within 4.10.
- Updates within 4.9.
- Updates from 4.9 to 4.10, allowing all 4.9 clusters to eventually update to 4.10, even if they do not immediately meet the minimum z-stream version requirements.
- **eus-4.10** only: updates within 4.8.
- **eus-4.10** only: updates from 4.8 to 4.9 to 4.10, allowing all 4.8 clusters to eventually update to 4.10.

4.10 update channels do not recommend updates to 4.11 or later releases. This strategy ensures that administrators must explicitly decide to update to the next minor version of OpenShift Container Platform.

Update channels control only release selection and do not impact the version of the cluster that you install. The **openshift-install** binary file for a specific version of OpenShift Container Platform always installs that version.

OpenShift Container Platform 4.10 offers the following update channels:

- **stable-4.10**
- **eus-4.y** (only offered for EUS versions and meant to facilitate updates between EUS versions)
- **fast-4.10**
- **candidate-4.10**

If you do not want the Cluster Version Operator to fetch available updates from the update recommendation service, you can use the **oc adm upgrade channel** command in the OpenShift CLI to configure an empty channel. This configuration can be helpful if, for example, a cluster has restricted network access and there is no local, reachable update recommendation service.

**WARNING**

Red Hat recommends updating to versions suggested by OpenShift Update Service only. For a minor version update, versions must be contiguous. Red Hat does not test updates to noncontiguous versions and cannot guarantee compatibility with earlier versions.

## 4.1. UPDATE CHANNELS

### 4.1.1. fast-4.10 channel

The **fast-4.10** channel is updated with new versions of OpenShift Container Platform 4.10 as soon as Red Hat declares the version as a general availability (GA) release. As such, these releases are fully supported and purposed to be used in production environments.

### 4.1.2. stable-4.10 channel

While the **fast-4.10** channel contains releases as soon as their errata are published, releases are added to the **stable-4.10** channel after a delay. During this delay, data is collected from multiple sources and analyzed for indications of product regressions. Once a significant number of data points have been collected, and absent negative signals, these releases are added to the stable channel.

**NOTE**

Since the time required to obtain a significant number of data points varies based on many factors, Service Level Objective (SLO) is not offered for the delay duration between fast and stable channels. For more information, please see "Choosing the correct channel for your cluster"

Newly installed clusters default to using stable channels.

### 4.1.3. eus-4.y channel

In addition to the stable channel, all even-numbered minor versions of OpenShift Container Platform offer [Extended Update Support](#) (EUS). Releases promoted to the stable channel are also simultaneously promoted to the EUS channels. The primary purpose of the EUS channels is to serve as a convenience for clusters performing an EUS-to-EUS update.

**NOTE**

Both standard and non-EUS subscribers can access all EUS repositories and necessary RPMs (**rhel-\*-eus-rpms**) to be able to support critical purposes such as debugging and building drivers.

### 4.1.4. candidate-4.10 channel

The **candidate-4.10** channel offers unsupported early access to releases as soon as they are built. Releases present only in candidate channels may not contain the full feature set of eventual GA

releases or features may be removed prior to GA. Additionally, these releases have not been subject to full Red Hat Quality Assurance and may not offer update paths to later GA releases. Given these caveats, the candidate channel is only suitable for testing purposes where destroying and recreating a cluster is acceptable.

### 4.1.5. Update recommendations in the channel

OpenShift Container Platform maintains an update recommendation service that knows your installed OpenShift Container Platform version and the path to take within the channel to get you to the next release. Update paths are also limited to versions relevant to your currently selected channel and its promotion characteristics.

You can imagine seeing the following releases in your channel:

- 4.10.0
- 4.10.1
- 4.10.3
- 4.10.4

The service recommends only updates that have been tested and have no known serious regressions. For example, if your cluster is on 4.10.1 and OpenShift Container Platform suggests 4.10.4, then it is recommended to update from 4.10.1 to 4.10.4.



#### IMPORTANT

Do not rely on consecutive patch numbers. In this example, 4.10.2 is not and never was available in the channel, therefore updates to 4.10.2 are not recommended or supported.

### 4.1.6. Update recommendations and Conditional Updates

Red Hat monitors newly released versions and update paths associated with those versions before and after they are added to supported channels.

If Red Hat removes update recommendations from any supported release, a superseding update recommendation will be provided to a future version that corrects the regression. There may however be a delay while the defect is corrected, tested, and promoted to your selected channel.

Beginning in OpenShift Container Platform 4.10, when update risks are confirmed, they are declared as Conditional Update risks for the relevant updates. Each known risk may apply to all clusters or only clusters matching certain conditions. Some examples include having the **Platform** set to **None** or the CNL provider set to **OpenShiftSDN**. The Cluster Version Operator (CVO) continually evaluates known risks against the current cluster state. If no risks match, the update is recommended. If the risk matches, those updates are supported but not recommended, and a reference link is provided. The reference link helps the cluster admin decide if they would like to accept the risk and update anyway.

When Red Hat chooses to declare Conditional Update risks, that action is taken in all relevant channels simultaneously. Declaration of a Conditional Update risk may happen either before or after the update has been promoted to supported channels.

### 4.1.7. Choosing the correct channel for your cluster

Choosing the appropriate channel involves two decisions.

First, select the minor version you want for your cluster update. Selecting a channel which matches your current version ensures that you only apply z-stream updates and do not receive feature updates. Selecting an available channel which has a version greater than your current version will ensure that after one or more updates your cluster will have updated to that version. Your cluster will only be offered channels which match its current version, the next version, or the next EUS version.



## NOTE

Due to the complexity involved in planning updates between versions many minors apart, channels that assist in planning updates beyond a single EUS-to-EUS update are not offered.

Second, you should choose your desired rollout strategy. You may choose to update as soon as Red Hat declares a release GA by selecting from fast channels or you may want to wait for Red Hat to promote releases to the stable channel. Update recommendations offered in the **fast-4.10** and **stable-4.10** are both fully supported and benefit equally from ongoing data analysis. The promotion delay before promoting a release to the stable channel represents the only difference between the two channels. Updates to the latest z-streams are generally promoted to the stable channel within a week or two, however the delay when initially rolling out updates to the latest minor is much longer, generally 45–90 days. Please consider the promotion delay when choosing your desired channel, as waiting for promotion to the stable channel may affect your scheduling plans.

Additionally, there are several factors which may lead an organization to move clusters to the fast channel either permanently or temporarily including:

- The desire to apply a specific fix known to affect your environment without delay.
- Application of CVE fixes without delay. CVE fixes may introduce regressions, so promotion delays still apply to z-streams with CVE fixes.
- Internal testing processes. If it takes your organization several weeks to qualify releases it is best test concurrently with our promotion process rather than waiting. This also assures that any telemetry signal provided to Red Hat is factored into our rollout, so issues relevant to you can be fixed faster.

### 4.1.8. Restricted network clusters

If you manage the container images for your OpenShift Container Platform clusters yourself, you must consult the Red Hat errata that is associated with product releases and note any comments that impact updates. During an update, the user interface might warn you about switching between these versions, so you must ensure that you selected an appropriate version before you bypass those warnings.

### 4.1.9. Switching between channels

A channel can be switched from the web console or through the **adm upgrade channel** command:

```
$ oc adm upgrade channel <channel>
```

The web console will display an alert if you switch to a channel that does not include the current release. The web console does not recommend any updates while on a channel without the current release. You can return to the original channel at any point, however.

Changing your channel might impact the supportability of your cluster. The following conditions might apply:

- Your cluster is still supported if you change from the **stable-4.10** channel to the **fast-4.10** channel.
- You can switch to the **candidate-4.10** channel at any time, but some releases for this channel might be unsupported.
- You can switch from the **candidate-4.10** channel to the **fast-4.10** channel if your current release is a general availability release.
- You can always switch from the **fast-4.10** channel to the **stable-4.10** channel. There is a possible delay of up to a day for the release to be promoted to **stable-4.10** if the current release was recently promoted.

#### Additional resources

- [Updating along a conditional upgrade path](#)
- [Choosing the correct channel for your cluster](#)

## CHAPTER 5. UNDERSTANDING OPENSIFT CONTAINER PLATFORM UPDATE DURATION

OpenShift Container Platform update duration varies based on the deployment topology. This page helps you understand the factors that affect update duration and estimate how long the cluster update takes in your environment.

### 5.1. PREREQUISITES

- You are familiar with [OpenShift Container Platform architecture](#) and [OpenShift Container Platform updates](#).

### 5.2. FACTORS AFFECTING UPDATE DURATION

The following factors can affect your cluster update duration:

- The reboot of compute nodes to the new machine configuration by Machine Config Operator (MCO)
  - The value of **MaxUnavailable** in the machine config pool
  - The minimum number or percentages of replicas set in pod disruption budget (PDB)
- The number of nodes in the cluster
- The health of the cluster nodes

### 5.3. CLUSTER UPDATE PHASES

In OpenShift Container Platform, the cluster update happens in two phases:

- Cluster Version Operator (CVO) target update payload deployment
- Machine Config Operator (MCO) node updates

#### 5.3.1. Cluster Version Operator target update payload deployment

The Cluster Version Operator (CVO) retrieves the target update release image and applies to the cluster. All components which run as pods are updated during this phase, whereas the host components are updated by the Machine Config Operator (MCO). This process might take 60 to 120 minutes.



#### NOTE

The CVO phase of the update does not restart the nodes.

#### Additional resources

- [Introduction to OpenShift Updates](#)

#### 5.3.2. Machine Config Operator node updates

The Machine Config Operator (MCO) applies a new machine configuration to each control plane and compute node. During this process, the MCO performs the following sequential actions on each node of the cluster:

1. Cordon and drain all the nodes
2. Update the operating system (OS)
3. Reboot the nodes
4. Uncordon all nodes and schedule workloads on the node



## NOTE

When a node is cordoned, workloads cannot be scheduled to it.

The time to complete this process depends on several factors including the node and infrastructure configuration. This process might take 5 or more minutes to complete per node.

In addition to MCO, you should consider the impact of the following parameters:

- The control plane node update duration is predictable and oftentimes shorter than compute nodes, because the control plane workloads are tuned for graceful updates and quick drains.
- You can update the compute nodes in parallel by setting the **maxUnavailable** field to greater than **1** in the Machine Config Pool (MCP). The MCO cordons the number of nodes specified in **maxUnavailable** and marks them unavailable for update.
- When you increase **maxUnavailable** on the MCP, it can help the pool to update more quickly. However, if **maxUnavailable** is set too high, and several nodes are cordoned simultaneously, the pod disruption budget (PDB) guarded workloads could fail to drain because a schedulable node cannot be found to run the replicas. If you increase **maxUnavailable** for the MCP, ensure that you still have sufficient schedulable nodes to allow PDB guarded workloads to drain.
- Before you begin the update, you must ensure that all the nodes are available. Any unavailable nodes can significantly impact the update duration because the node unavailability affects the **maxUnavailable** and pod disruption budgets.

To check the status of nodes from the terminal, run the following command:

```
$ oc get node
```

## Example Output

```
NAME                                STATUS          ROLES    AGE    VERSION
ip-10-0-137-31.us-east-2.compute.internal Ready,SchedulingDisabled worker 12d
v1.23.5+3afdacb
ip-10-0-151-208.us-east-2.compute.internal Ready          master 12d
v1.23.5+3afdacb
ip-10-0-176-138.us-east-2.compute.internal Ready          master 12d
v1.23.5+3afdacb
ip-10-0-183-194.us-east-2.compute.internal Ready          worker 12d
v1.23.5+3afdacb
ip-10-0-204-102.us-east-2.compute.internal Ready          master 12d
```



```
v1.23.5+3afdacb
ip-10-0-207-224.us-east-2.compute.internal Ready worker 12d
v1.23.5+3afdacb
```

If the status of the node is **NotReady** or **SchedulingDisabled**, then the node is not available and this impacts the update duration.

You can check the status of nodes from the **Administrator** perspective in the web console by expanding **Compute** → **Node**.

### Additional resources

- [Machine config overview](#)
- [Pod disruption budget](#)

## 5.4. ESTIMATING CLUSTER UPDATE TIME

Historical update duration of similar clusters provides you the best estimate for the future cluster updates. However, if the historical data is not available, you can use the following convention to estimate your cluster update time:

Cluster update time = CVO target update payload deployment time + (# node update iterations x MCO node update time)

A node update iteration consists of one or more nodes updated in parallel. The control plane nodes are always updated in parallel with the compute nodes. In addition, one or more compute nodes can be updated in parallel based on the **maxUnavailable** value.

For example, to estimate the update time, consider an OpenShift Container Platform cluster with three control plane nodes and six compute nodes and each host takes about 5 minutes to reboot.



### NOTE

The time it takes to reboot a particular node varies significantly. In cloud instances, the reboot might take about 1 to 2 minutes, whereas in physical bare metal hosts the reboot might take more than 15 minutes.

### Scenario-1

When you set **maxUnavailable** to **1** for both the control plane and compute nodes Machine Config Pool (MCP), then all the six compute nodes will update one after another in each iteration:

Cluster update time = 60 + (6 x 5) = 90 minutes

### Scenario-2

When you set **maxUnavailable** to **2** for the compute node MCP, then two compute nodes will update in parallel in each iteration. Therefore it takes total three iterations to update all the nodes.

Cluster update time = 60 + (3 x 5) = 75 minutes



## IMPORTANT

The default setting for **maxUnavailable** is **1** for all the MCPs in OpenShift Container Platform. It is recommended that you do not change the **maxUnavailable** in the control plane MCP.

## 5.5. RED HAT ENTERPRISE LINUX (RHEL) COMPUTE NODES

Red Hat Enterprise Linux (RHEL) compute nodes require an additional usage of **openshift-ansible** to update node binary components. The actual time spent updating RHEL compute nodes should not be significantly different from Red Hat Enterprise Linux CoreOS (RHCOS) compute nodes.

### Additional resources

- [Updating RHEL compute machines](#)

## CHAPTER 6. PREPARING TO PERFORM AN EUS-TO-EUS UPDATE

Due to fundamental Kubernetes design, all OpenShift Container Platform updates between minor versions must be serialized. You must update from OpenShift Container Platform <4.y> to <4.y+1>, and then to <4.y+2>. You cannot update from OpenShift Container Platform <4.y> to <4.y+2> directly. However, administrators who want to update between two Extended Update Support (EUS) versions can do so incurring only a single reboot of non-control plane hosts.



### IMPORTANT

EUS-to-EUS updates are only viable between **even-numbered minor versions** of OpenShift Container Platform.

There are a number of caveats to consider when attempting an EUS-to-EUS update.

- EUS-to-EUS updates are only offered after updates between all versions involved have been made available in **stable** channels.
- If you encounter issues during or after upgrading to the odd-numbered minor version but before upgrading to the next even-numbered version, then remediation of those issues may require that non-control plane hosts complete the update to the odd-numbered version before moving forward.
- You can do a partial update by updating the worker or custom pool nodes to accommodate the time it takes for maintenance.
- You can complete the update process during multiple maintenance windows by pausing at intermediate steps. However, plan to complete the entire update within 60 days. This is critical to ensure that normal cluster automation processes are completed including those associated with certificate rotation.
- Until the machine config pools are unpaused and the update is complete, some features and bugs fixes in <4.y+1> and <4.y+2> of OpenShift Container Platform are not available.
- All the clusters might update using EUS channels for a conventional update without pools paused, but only clusters with non control-plane **MachineConfigPools** objects can do EUS-to-EUS update with pools paused.

### 6.1. EUS-TO-EUS UPDATE

The following procedure pauses all non-master machine config pools and performs updates from OpenShift Container Platform 4.8 to 4.9 to 4.10, then unpauses the previously paused machine config pools. Following this procedure reduces the total update duration and the number of times worker nodes are restarted.

#### Prerequisites

- Review the release notes for OpenShift Container Platform 4.9 and 4.10
- Review the release notes and product lifecycles for any layered products and Operator Lifecycle Manager (OLM) Operators. Some may require updates either before or during an EUS-to-EUS update.

## 6.1.1. EUS-to-EUS update using the web console

### Prerequisites

- Verify that machine config pools are unpaused.
- Have access to the web console as a user with **admin** privileges.

### Procedure

1. Using the Administrator perspective on the web console, update any Operator Lifecycle Manager (OLM) Operators to the versions that are compatible with your intended updated version. You can find more information on how to perform this action in "Updating installed Operators"; see "Additional resources".
2. Verify that all machine config pools display a status of **Up to date** and that no machine config pool displays a status of **UPDATING**.  
To view the status of all machine config pools, click **Compute** → **MachineConfigPools** and review the contents of the **Update status** column.



#### NOTE

If your machine config pools have an **Updating** status, please wait for this status to change to **Up to date**. This process could take several minutes.

3. Set your channel to **eus-<4.y+2>**.  
To set your channel, click **Administration** → **Cluster Settings** → **Channel**. You can edit your channel by clicking on the current hyperlinked channel.
4. Pause all worker machine pools except for the master pool. You can perform this action on the **MachineConfigPools** tab under the **Compute** page. Select the vertical ellipses next to the machine config pool you'd like to pause and click **Pause updates**.
5. Update to version <4.y+1> and complete up to the **Save** step. You can find more information on how to perform these actions in "Updating a cluster by using the web console"; see "Additional resources".
6. Ensure that the <4.y+1> updates are complete by viewing the **Last completed version** of your cluster. You can find this information on the **Cluster Settings** page under the **Details** tab.
7. If necessary, update your OLM Operators by using the Administrator perspective on the web console. You can find more information on how to perform these actions in "Updating installed Operators"; see "Additional resources".
8. Update to version <4.y+2> and complete up to the **Save** step. You can find more information on how to perform these actions in "Updating a cluster by using the web console"; see "Additional resources".
9. Ensure that the <4.y+2> update is complete by viewing the **Last completed version** of your cluster. You can find this information on the **Cluster Settings** page under the **Details** tab.
10. Unpause all previously paused machine config pools. You can perform this action on the **MachineConfigPools** tab under the **Compute** page. Select the vertical ellipses next to the machine config pool you'd like to unpause and click **Unpause updates**.

**IMPORTANT**

If pools are not unpaused, the cluster is not permitted to upgrade to any future minor versions, and maintenance tasks such as certificate rotation are inhibited. This puts the cluster at risk for future degradation.

11. Verify that your previously paused pools are updated and that your cluster has completed the update to version <4.y+2>.

You can verify that your pools have updated on the **MachineConfigPools** tab under the **Compute** page by confirming that the **Update status** has a value of **Up to date**.

You can verify that your cluster has completed the update by viewing the **Last completed version** of your cluster. You can find this information on the **Cluster Settings** page under the **Details** tab.

**Additional resources**

- [Preparing for an Operator update](#)
- [Updating a cluster by using the web console](#)
- [Updating installed Operators](#)

**6.1.2. EUS-to-EUS update using the CLI****Prerequisites**

- Verify that machine config pools are unpaused.
- Update the OpenShift CLI (**oc**) to the target version before each update.

**IMPORTANT**

It is highly discouraged to skip this prerequisite. If the OpenShift CLI (**oc**) is not updated to the target version before your update, unexpected issues may occur.

**Procedure**

1. Using the Administrator perspective on the web console, update any Operator Lifecycle Manager (OLM) Operators to the versions that are compatible with your intended updated version. You can find more information on how to perform this action in "Updating installed Operators"; see "Additional resources".
2. Verify that all machine config pools display a status of **UPDATED** and that no machine config pool displays a status of **UPDATING**. To view the status of all machine config pools, run the following command:

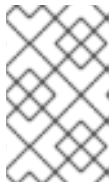
```
$ oc get mcp
```

**Example output**

```
NAME      CONFIG                                UPDATED  UPDATING
master    rendered-master-ecbb9582781c1091e1c9f19d50cf836c  True     False
worker    rendered-worker-00a3f0c68ae94e747193156b491553d5   True     False
```

- 
- Your current version is <4.y>, and your intended version to update is <4.y+2>. Change to the **eus-<4.y+2>** channel by running the following command:

```
$ oc adm upgrade channel eus-<4.y+2>
```

**NOTE**

If you receive an error message indicating that **eus-<4.y+2>** is not one of the available channels, this indicates that Red Hat is still rolling out EUS version updates. This rollout process generally takes 45-90 days starting at the GA date.

- Pause all worker machine pools except for the master pool by running the following command:

```
$ oc patch mcp/worker --type merge --patch '{"spec":{"paused":true}}'
```

**NOTE**

You cannot pause the master pool.

- Update to the latest version by running the following command:

```
$ oc adm upgrade --to-latest
```

**Example output**

```
Updating to latest version <4.y+1.z>
```

- Review the cluster version to ensure that the updates are complete by running the following command:

```
$ oc adm upgrade
```

**Example output**

```
Cluster version is <4.y+1.z>
```

```
...
```

- Update to version <4.y+2> by running the following command:

```
$ oc adm upgrade --to-latest
```

- Retrieve the cluster version to ensure that the <4.y+2> updates are complete by running the following command:

```
$ oc adm upgrade
```

**Example output**

```
Cluster version is <4.y+1.z>
```

```
...
```

- To update your worker nodes to <4.y+2>, unpause all previously paused machine config pools by running the following command:

```
$ oc patch mcp/worker --type merge --patch '{"spec":{"paused":false}}'
```



### IMPORTANT

If pools are not unpaused, the cluster is not permitted to update to any future minor versions, and maintenance tasks such as certificate rotation are inhibited. This puts the cluster at risk for future degradation.

- Verify that your previously paused pools are updated and that the update to version <4.y+2> is complete by running the following command:

```
$ oc get mcp
```

### Example output

```
NAME      CONFIG                                UPDATED  UPDATING
master    rendered-master-52da4d2760807cb2b96a3402179a9a4c  True    False
worker    rendered-worker-4756f60eccae96fb9dcb4c392c69d497  True    False
```

### Additional resources

- [Updating installed Operators](#)

## 6.1.3. EUS-to-EUS update for layered products and Operators installed through Operator Lifecycle Manager

In addition to the EUS-to-EUS update steps mentioned for the web console and CLI, there are additional steps to consider when performing EUS-to-EUS updates for clusters with the following:

- Layered products
- Operators installed through Operator Lifecycle Manager (OLM)

### What is a layered product?

Layered products refer to products that are made of multiple underlying products that are intended to be used together and cannot be broken into individual subscriptions. For examples of layered OpenShift Container Platform products, see [Layered Offering On OpenShift](#).

As you perform an EUS-to-EUS update for the clusters of layered products and those of Operators that have been installed through OLM, you must complete the following:

- Ensure that all of your Operators previously installed through OLM are updated to their latest version in their latest channel. Updating the Operators ensures that they have a valid update path when the default OperatorHub catalogs switch from the current minor version to the next during a cluster update. For information on how to update your Operators, see "Preparing for an Operator update" in "Additional resources".

2. Confirm the cluster version compatibility between the current and intended Operator versions. You can verify which versions your OLM Operators are compatible with by using the [Red Hat OpenShift Container Platform Operator Update Information Checker](#).

As an example, here are the steps to perform an EUS-to-EUS update from <4.y> to <4.y+2> for OpenShift Data Foundation (ODF). This can be done through the CLI or web console. For information on how to update clusters through your desired interface, see *EUS-to-EUS update using the web console* and "EUS-to-EUS update using the CLI" in "Additional resources".

### Example workflow

1. Pause the worker machine pools.
2. Upgrade OpenShift <4.y> → OpenShift <4.y+1>.
3. Upgrade ODF <4.y> → ODF <4.y+1>.
4. Upgrade OpenShift <4.y+1> → OpenShift <4.y+2>.
5. Upgrade to ODF <4.y+2>.
6. Unpause the worker machine pools.



### NOTE

The upgrade to ODF <4.y+2> can happen before or after worker machine pools have been unpaused.

### Additional resources

- [Preparing for an Operator update](#)
- [EUS-to-EUS update using the web console](#)
- [EUS-to-EUS update using the CLI](#)



## CHAPTER 7. PREPARING TO UPDATE A CLUSTER WITH MANUALLY MAINTAINED CREDENTIALS

The Cloud Credential Operator (CCO) **Upgradable** status for a cluster with manually maintained credentials is **False** by default.

- For minor releases, for example, from 4.10 to 4.11, this status prevents you from updating until you have addressed any updated permissions and annotated the **CloudCredential** resource to indicate that the permissions are updated as needed for the next version. This annotation changes the **Upgradable** status to **True**.
- For z-stream releases, for example, from 4.10.0 to 4.10.1, no permissions are added or changed, so the update is not blocked.

Before updating a cluster with manually maintained credentials, you must accommodate any new or changed credentials in the release image for the version of OpenShift Container Platform you are updating to.

### 7.1. UPDATE REQUIREMENTS FOR CLUSTERS WITH MANUALLY MAINTAINED CREDENTIALS

Before you update a cluster that uses manually maintained credentials with the Cloud Credential Operator (CCO), you must update the cloud provider resources for the new release.

If the cloud credential management for your cluster was configured using the CCO utility (**ccoctl**), use the **ccoctl** utility to update the resources. Clusters that were configured to use manual mode without the **ccoctl** utility require manual updates for the resources.

After updating the cloud provider resources, you must update the **upgradeable-to** annotation for the cluster to indicate that it is ready to update.



#### NOTE

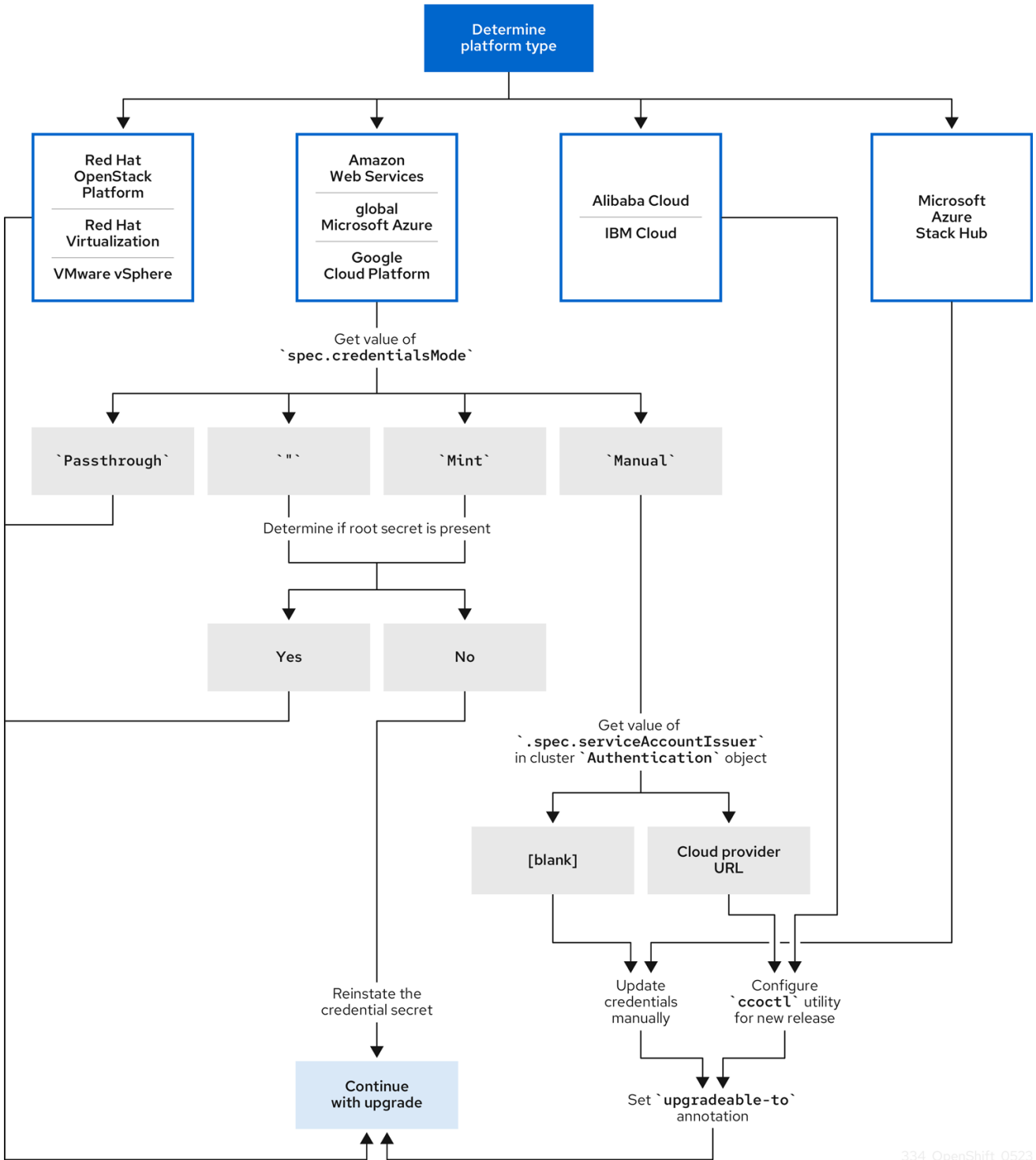
The process to update the cloud provider resources and the **upgradeable-to** annotation can only be completed by using command line tools.

#### 7.1.1. Cloud credential configuration options and update requirements by platform type

Some platforms only support using the CCO in one mode. For clusters that are installed on those platforms, the platform type determines the credentials update requirements.

For platforms that support using the CCO in multiple modes, you must determine which mode the cluster is configured to use and take the required actions for that configuration.

Figure 7.1. Credentials update requirements by platform type



334\_OpenShift\_0523

**Red Hat OpenStack Platform (RHOSP), Red Hat Virtualization (RHV), and VMware vSphere**

These platforms do not support using the CCO in manual mode. Clusters on these platforms handle changes in cloud provider resources automatically and do not require an update to the **upgradeable-to** annotation. Administrators of clusters on these platforms should skip the manually maintained credentials section of the update process.

**Alibaba Cloud and IBM Cloud**

Clusters installed on these platforms are configured using the **ccoctl** utility. Administrators of clusters on these platforms must take the following actions:

1. Configure the **ccoctl** utility for the new release.
2. Use the **ccoctl** utility to update the cloud provider resources.
3. Indicate that the cluster is ready to update with the **upgradeable-to** annotation.

### Microsoft Azure Stack Hub

These clusters use manual mode with long-lived credentials and do not use the **ccoctl** utility. Administrators of clusters on these platforms must take the following actions:

1. Manually update the cloud provider resources for the new release.
2. Indicate that the cluster is ready to update with the **upgradeable-to** annotation.

### Amazon Web Services (AWS), global Microsoft Azure, and Google Cloud Platform (GCP)

Clusters installed on these platforms support multiple CCO modes.

The required update process depends on the mode that the cluster is configured to use. If you are not sure what mode the CCO is configured to use on your cluster, you can use the web console or the CLI to determine this information.

### Additional resources

- [Determining the Cloud Credential Operator mode by using the web console](#)
- [Determining the Cloud Credential Operator mode by using the CLI](#)
- [Configuring the Cloud Credential Operator utility for a cluster update](#)
- [Updating cloud provider resources with manually maintained credentials](#)
- [About the Cloud Credential Operator](#)

## 7.1.2. Determining the Cloud Credential Operator mode by using the web console

You can determine what mode the Cloud Credential Operator (CCO) is configured to use by using the web console.



### NOTE

Only Amazon Web Services (AWS), global Microsoft Azure, and Google Cloud Platform (GCP) clusters support multiple CCO modes.

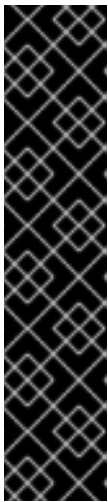
### Prerequisites

- You have access to an OpenShift Container Platform account with cluster administrator permissions.

### Procedure

1. Log in to the OpenShift Container Platform web console as a user with the **cluster-admin** role.
2. Navigate to **Administration** → **Cluster Settings**.

3. On the **Cluster Settings** page, select the **Configuration** tab.
4. Under **Configuration resource**, select **CloudCredential**.
5. On the **CloudCredential details** page, select the **YAML** tab.
6. In the YAML block, check the value of **spec.credentialsMode**. The following values are possible, though not all are supported on all platforms:
  - **"**: The CCO is operating in the default mode. In this configuration, the CCO operates in mint or passthrough mode, depending on the credentials provided during installation.
  - **Mint**: The CCO is operating in mint mode.
  - **Passthrough**: The CCO is operating in passthrough mode.
  - **Manual**: The CCO is operating in manual mode.



### IMPORTANT

To determine the specific configuration of an AWS or GCP cluster that has a **spec.credentialsMode** of **"**, **Mint**, or **Manual**, you must investigate further.

AWS and GCP clusters support using mint mode with the root secret deleted. If the cluster is specifically configured to use mint mode or uses mint mode by default, you must determine if the root secret is present on the cluster before updating.

An AWS or GCP cluster that uses manual mode might be configured to create and manage cloud credentials from outside of the cluster using the AWS Security Token Service (STS) or GCP Workload Identity. You can determine whether your cluster uses this strategy by examining the cluster **Authentication** object.

7. AWS or GCP clusters that use mint mode only: To determine whether the cluster is operating without the root secret, navigate to **Workloads** → **Secrets** and look for the root secret for your cloud provider.



### NOTE

Ensure that the **Project** dropdown is set to **All Projects**.

Platform	Secret name
AWS	<b>aws-creds</b>
GCP	<b>gcp-credentials</b>

- If you see one of these values, your cluster is using mint or passthrough mode with the root secret present.
- If you do not see these values, your cluster is using the CCO in mint mode with the root secret removed.

8. AWS or GCP clusters that use manual mode only: To determine whether the cluster is configured to create and manage cloud credentials from outside of the cluster, you must check the cluster **Authentication** object YAML values.
  - a. Navigate to **Administration** → **Cluster Settings**.
  - b. On the **Cluster Settings** page, select the **Configuration** tab.
  - c. Under **Configuration resource**, select **Authentication**.
  - d. On the **Authentication details** page, select the **YAML** tab.
  - e. In the YAML block, check the value of the **.spec.serviceAccountIssuer** parameter.
    - A value that contains a URL that is associated with your cloud provider indicates that the CCO is using manual mode with AWS STS or GCP Workload Identity to create and manage cloud credentials from outside of the cluster. These clusters are configured using the **ccoctl** utility.
    - An empty value ("") indicates that the cluster is using the CCO in manual mode but was not configured using the **ccoctl** utility.

### Next steps

- If you are updating a cluster that has the CCO operating in mint or passthrough mode and the root secret is present, you do not need to update any cloud provider resources and can continue to the next part of the update process.
- If your cluster is using the CCO in mint mode with the root secret removed, you must reinstate the credential secret with the administrator-level credential before continuing to the next part of the update process.
- If your cluster was configured using the CCO utility (**ccoctl**), you must take the following actions:
  - a. Configure the **ccoctl** utility for the new release and use it to update the cloud provider resources.
  - b. Update the **upgradeable-to** annotation to indicate that the cluster is ready to update.
- If your cluster is using the CCO in manual mode but was not configured using the **ccoctl** utility, you must take the following actions:
  - a. Manually update the cloud provider resources for the new release.
  - b. Update the **upgradeable-to** annotation to indicate that the cluster is ready to update.

### Additional resources

- [Configuring the Cloud Credential Operator utility for a cluster update](#)
- [Updating cloud provider resources with manually maintained credentials](#)

## 7.1.3. Determining the Cloud Credential Operator mode by using the CLI

You can determine what mode the Cloud Credential Operator (CCO) is configured to use by using the CLI.

**NOTE**

Only Amazon Web Services (AWS), global Microsoft Azure, and Google Cloud Platform (GCP) clusters support multiple CCO modes.

**Prerequisites**

- You have access to an OpenShift Container Platform account with cluster administrator permissions.
- You have installed the OpenShift CLI (**oc**).

**Procedure**

1. Log in to **oc** on the cluster as a user with the **cluster-admin** role.
2. To determine the mode that the CCO is configured to use, enter the following command:

```
$ oc get cloudcredentials cluster \
  -o=jsonpath={.spec.credentialsMode}
```

The following output values are possible, though not all are supported on all platforms:

- **"**: The CCO is operating in the default mode. In this configuration, the CCO operates in mint or passthrough mode, depending on the credentials provided during installation.
- **Mint**: The CCO is operating in mint mode.
- **Passthrough**: The CCO is operating in passthrough mode.
- **Manual**: The CCO is operating in manual mode.

**IMPORTANT**

To determine the specific configuration of an AWS or GCP cluster that has a **spec.credentialsMode** of **"**, **Mint**, or **Manual**, you must investigate further.

AWS and GCP clusters support using mint mode with the root secret deleted. If the cluster is specifically configured to use mint mode or uses mint mode by default, you must determine if the root secret is present on the cluster before updating.

An AWS or GCP cluster that uses manual mode might be configured to create and manage cloud credentials from outside of the cluster using the AWS Security Token Service (STS) or GCP Workload Identity. You can determine whether your cluster uses this strategy by examining the cluster **Authentication** object.

3. AWS or GCP clusters that use mint mode only: To determine whether the cluster is operating without the root secret, run the following command:

```
$ oc get secret <secret_name> \
  -n=kube-system
```

where **<secret\_name>** is **aws-creds** for AWS or **gcp-credentials** for GCP.

If the root secret is present, the output of this command returns information about the secret. An error indicates that the root secret is not present on the cluster.

4. AWS or GCP clusters that use manual mode only: To determine whether the cluster is configured to create and manage cloud credentials from outside of the cluster, run the following command:

```
$ oc get authentication cluster \
  -o jsonpath \
  --template='{ .spec.serviceAccountIssuer }'
```

This command displays the value of the **.spec.serviceAccountIssuer** parameter in the cluster **Authentication** object.

- An output of a URL that is associated with your cloud provider indicates that the CCO is using manual mode with AWS STS or GCP Workload Identity to create and manage cloud credentials from outside of the cluster. These clusters are configured using the **ccoctl** utility.
- An empty output indicates that the cluster is using the CCO in manual mode but was not configured using the **ccoctl** utility.

### Next steps

- If you are updating a cluster that has the CCO operating in mint or passthrough mode and the root secret is present, you do not need to update any cloud provider resources and can continue to the next part of the update process.
- If your cluster is using the CCO in mint mode with the root secret removed, you must reinstate the credential secret with the administrator-level credential before continuing to the next part of the update process.
- If your cluster was configured using the CCO utility (**ccoctl**), you must take the following actions:
  - a. Configure the **ccoctl** utility for the new release and use it to update the cloud provider resources.
  - b. Update the **upgradeable-to** annotation to indicate that the cluster is ready to update.
- If your cluster is using the CCO in manual mode but was not configured using the **ccoctl** utility, you must take the following actions:
  - a. Manually update the cloud provider resources for the new release.
  - b. Update the **upgradeable-to** annotation to indicate that the cluster is ready to update.

### Additional resources

- [Configuring the Cloud Credential Operator utility for a cluster update](#)
- [Updating cloud provider resources with manually maintained credentials](#)

## 7.2. CONFIGURING THE CLOUD CREDENTIAL OPERATOR UTILITY FOR A CLUSTER UPDATE

To upgrade a cluster that uses the Cloud Credential Operator (CCO) in manual mode to create and manage cloud credentials from outside of the cluster, extract and prepare the CCO utility (**ccoctl**) binary.



## NOTE

The **ccoctl** utility is a Linux binary that must run in a Linux environment.

## Prerequisites

- You have access to an OpenShift Container Platform account with cluster administrator access.
- You have installed the OpenShift CLI (**oc**).
- Your cluster was configured using the **ccoctl** utility to create and manage cloud credentials from outside of the cluster.

## Procedure

1. Obtain the OpenShift Container Platform release image:

```
$ RELEASE_IMAGE=$(./openshift-install version | awk 'release image/ {print $3}')
```

2. Get the CCO container image from the OpenShift Container Platform release image:

```
$ CCO_IMAGE=$(oc adm release info --image-for='cloud-credential-operator' $RELEASE_IMAGE)
```



## NOTE

Ensure that the architecture of the **\$RELEASE\_IMAGE** matches the architecture of the environment in which you will use the **ccoctl** tool.

3. Extract the **ccoctl** binary from the CCO container image within the OpenShift Container Platform release image:

```
$ oc image extract $CCO_IMAGE --file="/usr/bin/ccoctl" -a ~/.pull-secret
```

4. Change the permissions to make **ccoctl** executable:

```
$ chmod 775 ccoctl
```

## Verification

- To verify that **ccoctl** is ready to use, display the help file:

```
$ ccoctl --help
```

### Output of **ccoctl --help**

```
OpenShift credentials provisioning tool
```



**Usage:**

```
ccoctl [command]
```

**Available Commands:**

```
alibabacloud Manage credentials objects for alibaba cloud
```

```
aws          Manage credentials objects for AWS cloud
```

```
gcp         Manage credentials objects for Google cloud
```

```
help       Help about any command
```

```
ibmcloud   Manage credentials objects for IBM Cloud
```

**Flags:**

```
-h, --help  help for ccoctl
```

Use "ccoctl [command] --help" for more information about a command.

## 7.3. UPDATING CLOUD PROVIDER RESOURCES WITH THE CLOUD CREDENTIAL OPERATOR UTILITY

The process for upgrading an OpenShift Container Platform cluster that was configured using the CCO utility (**ccoctl**) is similar to creating the cloud provider resources during installation.

**NOTE**

By default, **ccoctl** creates objects in the directory in which the commands are run. To create the objects in a different directory, use the **--output-dir** flag. This procedure uses **<path\_to\_ccoctl\_output\_dir>** to refer to this directory.

On AWS clusters, some **ccoctl** commands make AWS API calls to create or modify AWS resources. You can use the **--dry-run** flag to avoid making API calls. Using this flag creates JSON files on the local file system instead. You can review and modify the JSON files and then apply them with the AWS CLI tool using the **--cli-input-json** parameters.

**Prerequisites**

- Obtain the OpenShift Container Platform release image for the version that you are upgrading to.
- Extract and prepare the **ccoctl** binary from the release image.

**Procedure**

1. Extract the list of **CredentialsRequest** custom resources (CRs) from the OpenShift Container Platform release image by running the following command:

```
$ oc adm release extract --credentials-requests \
  --cloud=<provider_type> \
  --to=<path_to_directory_with_list_of_credentials_requests>/credrequests \
  quay.io/<path_to>/ocp-release:<version>
```

where:

- **<provider\_type>** is the value for your cloud provider. Valid values are **alibabacloud**, **aws**, **gcp**, and **ibmcloud**.

- **credrequests** is the directory where the list of **CredentialsRequest** objects is stored. This command creates the directory if it does not exist.
2. For each **CredentialsRequest** CR in the release image, ensure that a namespace that matches the text in the **spec.secretRef.namespace** field exists in the cluster. This field is where the generated secrets that hold the credentials configuration are stored.

### Sample AWS CredentialsRequest object

```

apiVersion: cloudcredential.openshift.io/v1
kind: CredentialsRequest
metadata:
  name: cloud-credential-operator-iam-ro
  namespace: openshift-cloud-credential-operator
spec:
  secretRef:
    name: cloud-credential-operator-iam-ro-creds
    namespace: openshift-cloud-credential-operator 1
  providerSpec:
    apiVersion: cloudcredential.openshift.io/v1
    kind: AWSProviderSpec
    statementEntries:
      - effect: Allow
        action:
          - iam:GetUser
          - iam:GetUserPolicy
          - iam:ListAccessKeys
        resource: "*"

```

- 1** This field indicates the namespace which needs to exist to hold the generated secret.

The **CredentialsRequest** CRs for other platforms have a similar format with different platform-specific values.

3. For any **CredentialsRequest** CR for which the cluster does not already have a namespace with the name specified in **spec.secretRef.namespace**, create the namespace:

```
$ oc create namespace <component_namespace>
```

4. Use the **ccoctl** tool to process all **CredentialsRequest** objects in the **credrequests** directory by running the command for your cloud provider. The following commands process **CredentialsRequest** objects:
  - Alibaba Cloud: **ccoctl alibabacloud create-ram-users**
  - Amazon Web Services (AWS): **ccoctl aws create-iam-roles**
  - Google Cloud Platform (GCP): **ccoctl gcp create-all**
  - IBM Cloud: **ccoctl ibmcloud create-service-id**



## IMPORTANT

Refer to the **ccoctl** utility instructions in the installation content for your cloud provider for important platform-specific details about the required arguments and special considerations.

For each **CredentialsRequest** object, **ccoctl** creates the required provider resources and a permissions policy as defined in each **CredentialsRequest** object from the OpenShift Container Platform release image.

5. Apply the secrets to your cluster:

```
$ ls <path_to_ccoctl_output_dir>/manifests/*-credentials.yaml | xargs -l{} oc apply -f {}
```

## Verification

You can verify that the required provider resources and permissions policies are created by querying the cloud provider. For more information, refer to your cloud provider documentation on listing roles or service accounts.

## Next steps

- Update the **upgradeable-to** annotation to indicate that the cluster is ready to upgrade.

## Additional resources

- [Creating Alibaba Cloud credentials for OpenShift Container Platform components with the \*\*ccoctl\*\* tool](#)
- [Creating AWS resources with the Cloud Credential Operator utility](#)
- [Creating GCP resources with the Cloud Credential Operator utility](#)
- [Manually creating IAM for IBM Cloud VPC](#)
- [Indicating that the cluster is ready to upgrade](#)

## 7.4. UPDATING CLOUD PROVIDER RESOURCES WITH MANUALLY MAINTAINED CREDENTIALS

Before upgrading a cluster with manually maintained credentials, you must create any new credentials for the release image that you are upgrading to. You must also review the required permissions for existing credentials and accommodate any new permissions requirements in the new release for those components.

### Procedure

1. Extract and examine the **CredentialsRequest** custom resource for the new release.  
The "Manually creating IAM" section of the installation content for your cloud provider explains how to obtain and use the credentials required for your cloud.
2. Update the manually maintained credentials on your cluster:
  - Create new secrets for any **CredentialsRequest** custom resources that are added by the new release image.

- If the **CredentialsRequest** custom resources for any existing credentials that are stored in secrets have changed permissions requirements, update the permissions as required.

### Next steps

- Update the **upgradeable-to** annotation to indicate that the cluster is ready to upgrade.

### Additional resources

- [Manually creating IAM for AWS](#)
- [Manually creating IAM for Azure](#)
- [Manually creating IAM for Azure Stack Hub](#)
- [Manually creating IAM for GCP](#)
- [Indicating that the cluster is ready to upgrade](#)

## 7.5. INDICATING THAT THE CLUSTER IS READY TO UPGRADE

The Cloud Credential Operator (CCO) **Upgradeable** status for a cluster with manually maintained credentials is **False** by default.

### Prerequisites

- For the release image that you are upgrading to, you have processed any new credentials manually or by using the Cloud Credential Operator utility (**ccoctl**).
- You have installed the OpenShift CLI (**oc**).

### Procedure

1. Log in to **oc** on the cluster as a user with the **cluster-admin** role.
2. Edit the **CloudCredential** resource to add an **upgradeable-to** annotation within the **metadata** field by running the following command:

```
$ oc edit cloudcredential cluster
```

#### Text to add

```
...
metadata:
  annotations:
    cloudcredential.openshift.io/upgradeable-to: <version_number>
...
```

Where **<version\_number>** is the version that you are upgrading to, in the format **x.y.z**. For example, use **4.10.2** for OpenShift Container Platform 4.10.2.

It may take several minutes after adding the annotation for the upgradeable status to change.

### Verification

1. In the **Administrator** perspective of the web console, navigate to **Administration** → **Cluster Settings**.
2. To view the CCO status details, click **cloud-credential** in the **Cluster Operators** list.
  - If the **Upgradeable** status in the **Conditions** section is **False**, verify that the **upgradeable-to** annotation is free of typographical errors.
3. When the **Upgradeable** status in the **Conditions** section is **True**, begin the OpenShift Container Platform upgrade.

## CHAPTER 8. UPDATING A CLUSTER USING THE WEB CONSOLE

You can update, or upgrade, an OpenShift Container Platform cluster by using the web console. The following steps update a cluster within a minor version. You can use the same instructions for updating a cluster between minor versions.



### NOTE

Use the web console or `oc adm upgrade channel <channel>` to change the update channel. You can follow the steps in [Updating a cluster using the CLI](#) to complete the update after you change to a 4.10 channel.

### 8.1. PREREQUISITES

- Have access to the cluster as a user with **admin** privileges. See [Using RBAC to define and apply permissions](#).
- Have a recent [etcd backup](#) in case your update fails and you must [restore your cluster to a previous state](#).
- Support for RHEL7 workers is removed in OpenShift Container Platform 4.10. You must replace RHEL7 workers with RHEL8 or RHCOS workers before upgrading to OpenShift Container Platform 4.10. Red Hat does not support in-place RHEL7 to RHEL8 updates for RHEL workers; those hosts must be replaced with a clean operating system install.
- Ensure all Operators previously installed through Operator Lifecycle Manager (OLM) are updated to their latest version in their latest channel. Updating the Operators ensures they have a valid update path when the default OperatorHub catalogs switch from the current minor version to the next during a cluster update. See [Updating installed Operators](#) for more information.
- Ensure that all machine config pools (MCPs) are running and not paused. Nodes associated with a paused MCP are skipped during the update process. You can pause the MCPs if you are performing a canary rollout update strategy.
- To accommodate the time it takes to update, you are able to do a partial update by updating the worker or custom pool nodes. You can pause and resume within the progress bar of each pool.
- If your cluster uses manually maintained credentials, update the cloud provider resources for the new release. For more information, including how to determine if this is a requirement for your cluster, see [Preparing to update a cluster with manually maintained credentials](#).
- If you run an Operator or you have configured any application with the pod disruption budget, you might experience an interruption during the upgrade process. If **minAvailable** is set to 1 in **PodDisruptionBudget**, the nodes are drained to apply pending machine configs which might block the eviction process. If several nodes are rebooted, all the pods might run on only one node, and the **PodDisruptionBudget** field can prevent the node drain.



## IMPORTANT

- When an update is failing to complete, the Cluster Version Operator (CVO) reports the status of any blocking components while attempting to reconcile the update. Rolling your cluster back to a previous version is not supported. If your update is failing to complete, contact Red Hat support.
- Using the **unsupportedConfigOverrides** section to modify the configuration of an Operator is unsupported and might block cluster updates. You must remove this setting before you can update your cluster.

### Additional resources

- [Support policy for unmanaged Operators](#)

## 8.2. PERFORMING A CANARY ROLLOUT UPDATE

In some specific use cases, you might want a more controlled update process where you do not want specific nodes updated concurrently with the rest of the cluster. These use cases include, but are not limited to:

- You have mission-critical applications that you do not want unavailable during the update. You can slowly test the applications on your nodes in small batches after the update.
- You have a small maintenance window that does not allow the time for all nodes to be updated, or you have multiple maintenance windows.

The rolling update process is **not** a typical update workflow. With larger clusters, it can be a time-consuming process that requires you execute multiple commands. This complexity can result in errors that can affect the entire cluster. It is recommended that you carefully consider whether your organization wants to use a rolling update and carefully plan the implementation of the process before you start.

The rolling update process described in this topic involves:

- Creating one or more custom machine config pools (MCPs).
- Labeling each node that you do not want to update immediately to move those nodes to the custom MCPs.
- Pausing those custom MCPs, which prevents updates to those nodes.
- Performing the cluster update.
- Unpausing one custom MCP, which triggers the update on those nodes.
- Testing the applications on those nodes to make sure the applications work as expected on those newly-updated nodes.
- Optionally removing the custom labels from the remaining nodes in small batches and testing the applications on those nodes.



## NOTE

Pausing an MCP prevents the Machine Config Operator from applying any configuration changes on the associated nodes. Pausing an MCP also prevents any automatically-rotated certificates from being pushed to the associated nodes, including the automatic CA rotation of the **kube-apiserver-to-kubelet-signer** CA certificate. If the MCP is paused when the **kube-apiserver-to-kubelet-signer** CA certificate expires and the MCO attempts to automatically renew the certificate, the new certificate is created but not applied across the nodes in the respective machine config pool. This causes failure in multiple **oc** commands, including but not limited to **oc debug**, **oc logs**, **oc exec**, and **oc attach**. Pausing an MCP should be done with careful consideration about the **kube-apiserver-to-kubelet-signer** CA certificate expiration and for short periods of time only.

If you want to use the canary rollout update process, see [Performing a canary rollout update](#) .

## 8.3. PAUSING A MACHINEHEALTHCHECK RESOURCE BY USING THE WEB CONSOLE


During the upgrade process, nodes in the cluster might become temporarily unavailable. In the case of worker nodes, the machine health check might identify such nodes as unhealthy and reboot them. To avoid rebooting such nodes, pause all the **MachineHealthCheck** resources before updating the cluster.

### Prerequisites

- You have access to the cluster with **cluster-admin** privileges.
- You have access to the OpenShift Container Platform web console.

### Procedure

1. Log in to the OpenShift Container Platform web console.
2. Navigate to **Compute** → **MachineHealthChecks**.
3. To pause the machine health checks, add the **cluster.x-k8s.io/paused=""** annotation to each **MachineHealthCheck** resource. For example, to add the annotation to the **machine-api-termination-handler** resource, complete the following steps:

- a. Click the Options menu  next to the **machine-api-termination-handler** and click **Edit annotations**.
- b. In the **Edit annotations** dialog, click **Add more**.
- c. In the **Key** and **Value** fields, add **cluster.x-k8s.io/paused** and **""** values, respectively, and click **Save**.

## 8.4. ABOUT UPDATING SINGLE NODE OPENSIFT CONTAINER PLATFORM

You can update, or upgrade, a single-node OpenShift Container Platform cluster by using either the console or CLI.



However, note the following limitations:

- The prerequisite to pause the **MachineHealthCheck** resources is not required because there is no other node to perform the health check.
- Restoring a single-node OpenShift Container Platform cluster using an etcd backup is not officially supported. However, it is good practice to perform the etcd backup in case your upgrade fails. If your control plane is healthy, you might be able to restore your cluster to a previous state by using the backup.
- Updating a single-node OpenShift Container Platform cluster requires downtime and can include an automatic reboot. The amount of downtime depends on the update payload, as described in the following scenarios:
  - If the update payload contains an operating system update, which requires a reboot, the downtime is significant and impacts cluster management and user workloads.
  - If the update contains machine configuration changes that do not require a reboot, the downtime is less, and the impact on the cluster management and user workloads is lessened. In this case, the node draining step is skipped with single-node OpenShift Container Platform because there is no other node in the cluster to reschedule the workloads to.
  - If the update payload does not contain an operating system update or machine configuration changes, a short API outage occurs and resolves quickly.



### IMPORTANT

There are conditions, such as bugs in an updated package, that can cause the single node to not restart after a reboot. In this case, the update does not rollback automatically.

#### Additional resources

- For information on which machine configuration changes require a reboot, see the note in [Understanding the Machine Config Operator](#).

## 8.5. UPDATING A CLUSTER BY USING THE WEB CONSOLE

If updates are available, you can update your cluster from the web console.

You can find information about available OpenShift Container Platform advisories and updates [in the errata section](#) of the Customer Portal.

#### Prerequisites

- Have access to the web console as a user with **admin** privileges.
- Pause all **MachineHealthCheck** resources.

#### Procedure

1. From the web console, click **Administration** → **Cluster Settings** and review the contents of the **Details** tab.

- For production clusters, ensure that the **Channel** is set to the correct channel for the version that you want to update to, such as **stable-4.10**.



### IMPORTANT

For production clusters, you must subscribe to a **stable-\***, **eus-\*** or **fast-\*** channel.



### NOTE

When you are ready to move to the next minor version, choose the channel that corresponds to that minor version. The sooner the update channel is declared, the more effectively the cluster can recommend update paths to your target version. The cluster might take some time to evaluate all the possible updates that are available and offer the best update recommendations to choose from. Update recommendations can change over time, as they are based on what update options are available at the time.

If you cannot see an update path to your target minor version, keep updating your cluster to the latest patch release for your current version until the next minor version is available in the path.

- If the **Update status** is not **Updates available**, you cannot update your cluster.
  - **Select channel** indicates the cluster version that your cluster is running or is updating to.
- Select a version to update to, and click **Save**.  
The Input channel **Update status** changes to **Update to <product-version> in progress** and you can review the progress of the cluster update by watching the progress bars for the Operators and nodes.



### NOTE

If you are upgrading your cluster to the next minor version, like version 4.y to 4.(y+1), it is recommended to confirm your nodes are upgraded before deploying workloads that rely on a new feature. Any pools with worker nodes that are not yet updated are displayed on the **Cluster Settings** page.

- After the update completes and the Cluster Version Operator refreshes the available updates, check if more updates are available in your current channel.
  - If updates are available, continue to perform updates in the current channel until you can no longer update.
  - If no updates are available, change the **Channel** to the **stable-\***, **eus-\*** or **fast-\*** channel for the next minor version, and update to the version that you want in that channel.

You might need to perform several intermediate updates until you reach the version that you want.

## 8.6. CHANGING THE UPDATE SERVER BY USING THE WEB CONSOLE

Changing the update server is optional. If you have an OpenShift Update Service (OSUS) installed and configured locally, you must set the URL for the server as the **upstream** to use the local server during updates.

## Procedure

1. Navigate to **Administration** → **Cluster Settings**, click **version**.
2. Click the **YAML** tab and then edit the **upstream** parameter value:

### Example output

```
...
spec:
  clusterID: db93436d-7b05-42cc-b856-43e11ad2d31a
  upstream: '<update-server-url>' 1
...
```

- 1** The **<update-server-url>** variable specifies the URL for the update server.

The default **upstream** is **[https://api.openshift.com/api/upgrades\\_info/v1/graph](https://api.openshift.com/api/upgrades_info/v1/graph)**.

3. Click **Save**.

## Additional resources

- [Understanding update channels and releases](#)

## CHAPTER 9. UPDATING A CLUSTER USING THE CLI

You can update, or upgrade, an OpenShift Container Platform cluster within a minor version by using the OpenShift CLI (**oc**). You can also update a cluster between minor versions by following the same instructions.

### 9.1. PREREQUISITES

- Have access to the cluster as a user with **admin** privileges. See [Using RBAC to define and apply permissions](#).
- Have a recent [etcd backup](#) in case your update fails and you must [restore your cluster to a previous state](#).
- Support for RHEL7 workers is removed in OpenShift Container Platform 4.10. You must replace RHEL7 workers with RHEL8 or RHCOS workers before upgrading to OpenShift Container Platform 4.10. Red Hat does not support in-place RHEL7 to RHEL8 updates for RHEL workers; those hosts must be replaced with a clean operating system install.
- Ensure all Operators previously installed through Operator Lifecycle Manager (OLM) are updated to their latest version in their latest channel. Updating the Operators ensures they have a valid update path when the default OperatorHub catalogs switch from the current minor version to the next during a cluster update. See [Updating installed Operators](#) for more information.
- Ensure that all machine config pools (MCPs) are running and not paused. Nodes associated with a paused MCP are skipped during the update process. You can pause the MCPs if you are performing a canary rollout update strategy.
- If your cluster uses manually maintained credentials, update the cloud provider resources for the new release. For more information, including how to determine if this is a requirement for your cluster, see [Preparing to update a cluster with manually maintained credentials](#).
- Ensure that you address all **Upgradeable=False** conditions so the cluster allows an upgrade to the next minor version. You can run the **oc adm upgrade** command for an output of all **Upgradeable=False** conditions and the condition reasoning to help you prepare for a minor version update.
- If you run an Operator or you have configured any application with the pod disruption budget, you might experience an interruption during the upgrade process. If **minAvailable** is set to 1 in **PodDisruptionBudget**, the nodes are drained to apply pending machine configs which might block the eviction process. If several nodes are rebooted, all the pods might run on only one node, and the **PodDisruptionBudget** field can prevent the node drain.



#### IMPORTANT

- When an update is failing to complete, the Cluster Version Operator (CVO) reports the status of any blocking components while attempting to reconcile the update. Rolling your cluster back to a previous version is not supported. If your update is failing to complete, contact Red Hat support.
- Using the **unsupportedConfigOverrides** section to modify the configuration of an Operator is unsupported and might block cluster updates. You must remove this setting before you can update your cluster.

## Additional resources

- [Support policy for unmanaged Operators](#)

## 9.2. PAUSING A MACHINEHEALTHCHECK RESOURCE

During the upgrade process, nodes in the cluster might become temporarily unavailable. In the case of worker nodes, the machine health check might identify such nodes as unhealthy and reboot them. To avoid rebooting such nodes, pause all the **MachineHealthCheck** resources before updating the cluster.

### Prerequisites

- Install the OpenShift CLI (**oc**).

### Procedure

1. To list all the available **MachineHealthCheck** resources that you want to pause, run the following command:

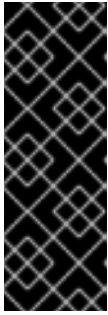
```
$ oc get machinehealthcheck -n openshift-machine-api
```

2. To pause the machine health checks, add the **cluster.x-k8s.io/paused=""** annotation to the **MachineHealthCheck** resource. Run the following command:

```
$ oc -n openshift-machine-api annotate mhc <mhc-name> cluster.x-k8s.io/paused=""
```

The annotated **MachineHealthCheck** resource resembles the following YAML file:

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineHealthCheck
metadata:
  name: example
  namespace: openshift-machine-api
  annotations:
    cluster.x-k8s.io/paused: ""
spec:
  selector:
    matchLabels:
      role: worker
  unhealthyConditions:
  - type: "Ready"
    status: "Unknown"
    timeout: "300s"
  - type: "Ready"
    status: "False"
    timeout: "300s"
  maxUnhealthy: "40%"
status:
  currentHealthy: 5
  expectedMachines: 5
```



## IMPORTANT

Resume the machine health checks after updating the cluster. To resume the check, remove the pause annotation from the **MachineHealthCheck** resource by running the following command:

```
$ oc -n openshift-machine-api annotate mhc <mhc-name> cluster.x-k8s.io/paused-
```

## 9.3. ABOUT UPDATING SINGLE NODE OPENSIFT CONTAINER PLATFORM

You can update, or upgrade, a single-node OpenShift Container Platform cluster by using either the console or CLI.

However, note the following limitations:

- The prerequisite to pause the **MachineHealthCheck** resources is not required because there is no other node to perform the health check.
- Restoring a single-node OpenShift Container Platform cluster using an etcd backup is not officially supported. However, it is good practice to perform the etcd backup in case your upgrade fails. If your control plane is healthy, you might be able to restore your cluster to a previous state by using the backup.
- Updating a single-node OpenShift Container Platform cluster requires downtime and can include an automatic reboot. The amount of downtime depends on the update payload, as described in the following scenarios:
  - If the update payload contains an operating system update, which requires a reboot, the downtime is significant and impacts cluster management and user workloads.
  - If the update contains machine configuration changes that do not require a reboot, the downtime is less, and the impact on the cluster management and user workloads is lessened. In this case, the node draining step is skipped with single-node OpenShift Container Platform because there is no other node in the cluster to reschedule the workloads to.
  - If the update payload does not contain an operating system update or machine configuration changes, a short API outage occurs and resolves quickly.



## IMPORTANT

There are conditions, such as bugs in an updated package, that can cause the single node to not restart after a reboot. In this case, the update does not rollback automatically.

### Additional resources

- For information on which machine configuration changes require a reboot, see the note in [Understanding the Machine Config Operator](#).

## 9.4. UPDATING A CLUSTER BY USING THE CLI

If updates are available, you can update your cluster by using the OpenShift CLI (**oc**).

You can find information about available OpenShift Container Platform advisories and updates [in the errata section](#) of the Customer Portal.

## Prerequisites

- Install the OpenShift CLI (**oc**) that matches the version for your updated version.
- Log in to the cluster as user with **cluster-admin** privileges.
- Pause all **MachineHealthCheck** resources.

## Procedure

1. View the available updates and note the version number of the update that you want to apply:

```
$ oc adm upgrade
```

### Example output

```
Cluster version is 4.9.23
```

```
Upstream is unset, so the cluster will use an appropriate default.
```

```
Channel: stable-4.9 (available channels: candidate-4.10, candidate-4.9, fast-4.10, fast-4.9, stable-4.10, stable-4.9, eus-4.10)
```

```
Recommended updates:
```

```
VERSION IMAGE
```

```
4.9.24 quay.io/openshift-release-dev/ocp-release@sha256:6a899c54dda6b844bb12a247e324a0f6cde367e880b73ba110c056df6d018032
```

```
4.9.25 quay.io/openshift-release-dev/ocp-release@sha256:2eafde815e543b92f70839972f585cc52aa7c37aa72d5f3c8bc886b0fd45707a
```

```
4.9.26 quay.io/openshift-release-dev/ocp-release@sha256:3ccd09dd08c303f27a543351f787d09b83979cd31cf0b4c6ff56cd68814ef6c8
```

```
4.9.27 quay.io/openshift-release-dev/ocp-release@sha256:1c7db78eec0cf05df2cead44f69c0e4b2c3234d5635c88a41e1b922c3bedae16
```

```
4.9.28 quay.io/openshift-release-dev/ocp-release@sha256:4084d94969b186e20189649b5affba7da59f7d1943e4e5bc7ef78b981eafb7a8
```

```
4.9.29 quay.io/openshift-release-dev/ocp-release@sha256:b04ca01d116f0134a102a57f86c67e5b1a3b5da1c4a580af91d521b8fa0aa6ec
```

```
4.9.31 quay.io/openshift-release-dev/ocp-release@sha256:2a28b8ebb53d67dd80594421c39e36d9896b1e65cb54af81fbb86ea9ac3bf2d7
```

```
4.9.32 quay.io/openshift-release-dev/ocp-release@sha256:ecdb6d0df547b857eaf0edb5574ddd64ca6d9aff1fa61fd1ac6fb641203bedfa
```

**NOTE**

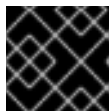
For details and information on how to perform an **EUS-to-EUS** channel upgrade, please refer to the *Preparing to perform an EUS-to-EUS upgrade* page, listed in the Additional resources section.

- Based on your organization requirements, set the appropriate upgrade channel. For example, you can set your channel to **stable-4.10**, **fast-4.10**, or **eus-4.10**. For more information about channels, refer to *Understanding update channels and releases* listed in the Additional resources section.

```
$ oc adm upgrade channel <channel>
```

For example, to set the channel to **stable-4.10**:

```
$ oc adm upgrade channel stable-4.10
```

**IMPORTANT**

For production clusters, you must subscribe to a **stable-\***, **eus-\***, or **fast-\*** channel.

**NOTE**

When you are ready to move to the next minor version, choose the channel that corresponds to that minor version. The sooner the update channel is declared, the more effectively the cluster can recommend update paths to your target version. The cluster might take some time to evaluate all the possible updates that are available and offer the best update recommendations to choose from. Update recommendations can change over time, as they are based on what update options are available at the time.

If you cannot see an update path to your target minor version, keep updating your cluster to the latest patch release for your current version until the next minor version is available in the path.

- Apply an update:

- To update to the latest version:

```
$ oc adm upgrade --to-latest=true 1
```

- To update to a specific version:

```
$ oc adm upgrade --to=<version> 1
```

**1 1** **<version>** is the update version that you obtained from the output of the **oc adm upgrade** command.

- Review the status of the Cluster Version Operator:

```
$ oc adm upgrade
```



- After the update completes, you can confirm that the cluster version has updated to the new version:

```
$ oc get clusterversion
```

### Example output

Cluster version is <version>

Upstream is unset, so the cluster will use an appropriate default.

Channel: stable-4.10 (available channels: candidate-4.10, candidate-4.11, eus-4.10, fast-4.10, fast-4.11, stable-4.10)

No updates available. You may force an upgrade to a specific release image, but doing so might not be supported and might result in downtime or data loss.



### NOTE

If the **oc get clusterversion** command displays the following error while the **PROGRESSING** status is **True**, you can ignore the error.

```
NAME      VERSION AVAILABLE PROGRESSING SINCE STATUS
version 4.10.26 True      True      24m  Unable to apply 4.11.0-rc.7: an
unknown error has occurred: MultipleErrors
```

- If you are upgrading your cluster to the next minor version, such as version X.y to X.(y+1), it is recommended to confirm that your nodes are upgraded before deploying workloads that rely on a new feature:

```
$ oc get nodes
```

### Example output

```
NAME                                STATUS ROLES  AGE  VERSION
ip-10-0-168-251.ec2.internal  Ready  master  82m  v1.23.12+8a6bfe4
ip-10-0-170-223.ec2.internal  Ready  master  82m  v1.23.12+8a6bfe4
ip-10-0-179-95.ec2.internal   Ready  worker  70m  v1.23.12+8a6bfe4
ip-10-0-182-134.ec2.internal  Ready  worker  70m  v1.23.12+8a6bfe4
ip-10-0-211-16.ec2.internal   Ready  master  82m  v1.23.12+8a6bfe4
ip-10-0-250-100.ec2.internal  Ready  worker  69m  v1.23.12+8a6bfe4
```

### Additional resources

- [Preparing to perform an EUS-to-EUS update](#)
- [Understanding update channels and releases](#)

## 9.5. UPDATING ALONG A CONDITIONAL UPGRADE PATH

You can update along a recommended conditional upgrade path using the web console or the OpenShift CLI (**oc**). When a conditional update is not recommended for your cluster, you can update along a conditional upgrade path using the OpenShift CLI (**oc**) 4.10 or later.

## Procedure

1. To view the description of the update when it is not recommended because a risk might apply, run the following command:

```
$ oc adm upgrade --include-not-recommended
```

2. If the cluster administrator evaluates the potential known risks and decides it is acceptable for the current cluster, then the administrator can waive the safety guards and proceed the update by running the following command:

```
$ oc adm upgrade --allow-not-recommended --to <version> <.>
```

<.> **<version>** is the supported but not recommended update version that you obtained from the output of the previous command.

## Additional resources

- [Understanding update channels and releases](#)

## 9.6. CHANGING THE UPDATE SERVER BY USING THE CLI

Changing the update server is optional. If you have an OpenShift Update Service (OSUS) installed and configured locally, you must set the URL for the server as the **upstream** to use the local server during updates. The default value for **upstream** is **https://api.openshift.com/api/upgrades\_info/v1/graph**.

## Procedure

- Change the **upstream** parameter value in the cluster version:

```
$ oc patch clusterversion/version --patch '{"spec":{"upstream":"<update-server-url>"}}' --type=merge
```

The **<update-server-url>** variable specifies the URL for the update server.

## Example output

```
clusterversion.config.openshift.io/version patched
```

## CHAPTER 10. PERFORMING A CANARY ROLLOUT UPDATE

There might be some scenarios where you want a more controlled rollout of an update to the worker nodes in order to ensure that mission-critical applications stay available during the whole update, even if the update process causes your applications to fail. Depending on your organizational needs, you might want to update a small subset of worker nodes, evaluate cluster and workload health over a period of time, then update the remaining nodes. This is commonly referred to as a *canary* update. Or, you might also want to fit worker node updates, which often require a host reboot, into smaller defined maintenance windows when it is not possible to take a large maintenance window to update the entire cluster at one time.

In these scenarios, you can create multiple custom machine config pools (MCPs) to prevent certain worker nodes from updating when you update the cluster. After the rest of the cluster is updated, you can update those worker nodes in batches at appropriate times.

For example, if you have a cluster with 100 nodes with 10% excess capacity, maintenance windows that must not exceed 4 hours, and you know that it takes no longer than 8 minutes to drain and reboot a worker node, you can leverage MCPs to meet your goals. For example, you could define four MCPs, named **workerpool-canary**, **workerpool-A**, **workerpool-B**, and **workerpool-C**, with 10, 30, 30, and 30 nodes respectively.

During your first maintenance window, you would pause the MCP for **workerpool-A**, **workerpool-B**, and **workerpool-C**, then initiate the cluster update. This updates components that run on top of OpenShift Container Platform and the 10 nodes which are members of the **workerpool-canary** MCP, because that pool was not paused. The other three MCPs are not updated, because they were paused. If for some reason, you determine that your cluster or workload health was negatively affected by the **workerpool-canary** update, you would then cordon and drain all nodes in that pool while still maintaining sufficient capacity until you have diagnosed the problem. When everything is working as expected, you would then evaluate the cluster and workload health before deciding to unpause, and thus update, **workerpool-A**, **workerpool-B**, and **workerpool-C** in succession during each additional maintenance window.

While managing worker node updates using custom MCPs provides flexibility, it can be a time-consuming process that requires you execute multiple commands. This complexity can result in errors that can affect the entire cluster. It is recommended that you carefully consider your organizational needs and carefully plan the implementation of the process before you start.



### NOTE

It is not recommended to update the MCPs to different OpenShift Container Platform versions. For example, do not update one MCP from 4.y.10 to 4.y.11 and another to 4.y.12. This scenario has not been tested and might result in an undefined cluster state.



### IMPORTANT

Pausing a machine config pool prevents the Machine Config Operator from applying any configuration changes on the associated nodes. Pausing an MCP also prevents any automatically-rotated certificates from being pushed to the associated nodes, including the automatic CA rotation of the **kube-apiserver-to-kubelet-signer** CA certificate. If the MCP is paused when the **kube-apiserver-to-kubelet-signer** CA certificate expires and the MCO attempts to automatically renew the certificate, the new certificate is created but not applied across the nodes in the respective machine config pool. This causes failure in multiple **oc** commands, including but not limited to **oc debug**, **oc logs**, **oc exec**, and **oc attach**. Pausing an MCP should be done with careful consideration about the **kube-apiserver-to-kubelet-signer** CA certificate expiration and for short periods of time only.

## 10.1. ABOUT THE CANARY ROLLOUT UPDATE PROCESS AND MCPS

In OpenShift Container Platform, nodes are not considered individually. Nodes are grouped into machine config pools (MCP). There are two MCPs in a default OpenShift Container Platform cluster: one for the control plane nodes and one for the worker nodes. An OpenShift Container Platform update affects all MCPs concurrently.

During the update, the Machine Config Operator (MCO) drains and cordons all nodes within a MCP up to the specified **maxUnavailable** number of nodes (if specified), by default **1**. Draining and cordoning a node deschedules all pods on the node and marks the node as unschedulable. After the node is drained, the Machine Config Daemon applies a new machine configuration, which can include updating the operating system (OS). Updating the OS requires the host to reboot.

To prevent specific nodes from being updated, and thus, not drained, cordoned, and updated, you can create custom MCPs. Then, pause those MCPs to ensure that the nodes associated with those MCPs are not updated. The MCO does not update any paused MCPs. You can create one or more custom MCPs, which can give you more control over the sequence in which you update those nodes. After you update the nodes in the first MCP, you can verify the application compatibility, and then update the rest of the nodes gradually to the new version.



### NOTE

To ensure the stability of the control plane, creating a custom MCP from the control plane nodes is not supported. The Machine Config Operator (MCO) ignores any custom MCP created for the control plane nodes.

You should give careful consideration to the number of MCPs you create and the number of nodes in each MCP, based on your workload deployment topology. For example, if you need to fit updates into specific maintenance windows, you need to know how many nodes that OpenShift Container Platform can update within a window. This number is dependent on your unique cluster and workload characteristics.

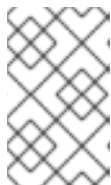
Also, you need to consider how much extra capacity you have available in your cluster. For example, in the case where your applications fail to work as expected on the updated nodes, you can cordon and drain those nodes in the pool, which moves the application pods to other nodes. You need to consider how much extra capacity you have available in order to determine the number of custom MCPs you need and how many nodes are in each MCP. For example, if you use two custom MCPs and 50% of your nodes are in each pool, you need to determine if running 50% of your nodes would provide sufficient quality-of-service (QoS) for your applications.

You can use this update process with all documented OpenShift Container Platform update processes. However, the process does not work with Red Hat Enterprise Linux (RHEL) machines, which are updated using Ansible playbooks.

## 10.2. ABOUT PERFORMING A CANARY ROLLOUT UPDATE

This topic describes the general workflow of this canary rollout update process. The steps to perform each task in the workflow are described in the following sections.

1. Create MCPs based on the worker pool. The number of nodes in each MCP depends on a few factors, such as your maintenance window duration for each MCP, and the amount of reserve capacity, meaning extra worker nodes, available in your cluster.

**NOTE**

You can change the **maxUnavailable** setting in an MCP to specify the percentage or the number of machines that can be updating at any given time. The default is 1.

2. Add a node selector to the custom MCPs. For each node that you do not want to update simultaneously with the rest of the cluster, add a matching label to the nodes. This label associates the node to the MCP.

**NOTE**

Do not remove the default worker label from the nodes. The nodes **must** have a role label to function properly in the cluster.

3. Pause the MCPs you do not want to update as part of the update process.

**NOTE**

Pausing the MCP also pauses the kube-apiserver-to-kubelet-signer automatic CA certificates rotation. New CA certificates are generated at 292 days from the installation date and old certificates are removed 365 days from the installation date. See the [Understand CA cert auto renewal in Red Hat OpenShift 4](#) to find out how much time you have before the next automatic CA certificate rotation. Make sure the pools are unpaused when the CA cert rotation happens. If the MCPs are paused, the cert rotation does not happen, which causes the cluster to become degraded and causes failure in multiple **oc** commands, including but not limited to **oc debug**, **oc logs**, **oc exec**, and **oc attach**.

4. Perform the cluster update. The update process updates the MCPs that are not paused, including the control plane nodes.
5. Test the applications on the updated nodes to ensure they are working as expected.
6. Unpause the remaining MCPs one-by-one and test the applications on those nodes until all worker nodes are updated. Unpausing an MCP starts the update process for the nodes associated with that MCP. You can check the progress of the update from the web console by clicking **Administration** → **Cluster settings**. Or, use the **oc get machineconfigpools** CLI command.
7. Optionally, remove the custom label from updated nodes and delete the custom MCPs.

## 10.3. CREATING MACHINE CONFIG POOLS TO PERFORM A CANARY ROLLOUT UPDATE

The first task in performing this canary rollout update is to create one or more machine config pools (MCP).

1. Create an MCP from a worker node.
  - a. List the worker nodes in your cluster.

```
$ oc get -l 'node-role.kubernetes.io/master!=*' -o 'jsonpath={range .items[*]}
{.metadata.name}{"\n"}{end}' nodes
```

-

**Example output**

```
ci-ln-pwnll6b-f76d1-s8t9n-worker-a-s75z4
ci-ln-pwnll6b-f76d1-s8t9n-worker-b-dglj2
ci-ln-pwnll6b-f76d1-s8t9n-worker-c-lldbm
```

- b. For the nodes you want to delay, add a custom label to the node:

```
$ oc label node <node name> node-role.kubernetes.io/<custom-label>=
```

For example:

```
$ oc label node ci-ln-0qv1yp2-f76d1-kl2tq-worker-a-j2ssz node-
role.kubernetes.io/workerpool-canary=
```

**Example output**

```
node/ci-ln-gtrwm8t-f76d1-spbl7-worker-a-xk76k labeled
```

- c. Create the new MCP:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
metadata:
  name: workerpool-canary 1
spec:
  machineConfigSelector:
    matchExpressions: 2
    - {
      key: machineconfiguration.openshift.io/role,
      operator: In,
      values: [worker,workerpool-canary]
    }
  nodeSelector:
    matchLabels:
      node-role.kubernetes.io/workerpool-canary: "" 3
```

- 1** Specify a name for the MCP.
- 2** Specify the **worker** and custom MCP name.
- 3** Specify the custom label you added to the nodes that you want in this pool.

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

**Example output**

```
machineconfigpool.machineconfiguration.openshift.io/workerpool-canary created
```

- d. View the list of MCPs in the cluster and their current state:

-

```
$ oc get machineconfigpool
```

### Example output

```

NAME          CONFIG                                UPDATED  UPDATING
DEGRADED     MACHINECOUNT  READYMACHINECOUNT
UPDATEDMACHINECOUNT  DEGRADEDMACHINECOUNT  AGE
master       rendered-master-b0bb90c4921860f2a5d8a2f8137c1867      True
False       False          3           3           3           0           97m
workerpool-canary rendered-workerpool-canary-87ba3dec1ad78cb6aecebf7fbb476a36
True        False          False        1           1           1           0           2m42s
worker       rendered-worker-87ba3dec1ad78cb6aecebf7fbb476a36      True
False       False          2           2           2           0           97m

```

The new machine config pool, **workerpool-canary**, is created and the number of nodes to which you added the custom label are shown in the machine counts. The worker MCP machine counts are reduced by the same number. It can take several minutes to update the machine counts. In this example, one node was moved from the **worker** MCP to the **workerpool-canary** MCP.

## 10.4. PAUSING THE MACHINE CONFIG POOLS

In this canary rollout update process, after you label the nodes that you do not want to update with the rest of your OpenShift Container Platform cluster and create the machine config pools (MCPs), you pause those MCPs. Pausing an MCP prevents the Machine Config Operator (MCO) from updating the nodes associated with that MCP.



### NOTE

Pausing the MCP also pauses the kube-apiserver-to-kubelet-signer automatic CA certificates rotation. New CA certificates are generated at 292 days from the installation date and old certificates are removed 365 days from the installation date. See the [Understand CA cert auto renewal in Red Hat OpenShift 4](#) to find out how much time you have before the next automatic CA certificate rotation. Make sure the pools are unpaused when the CA cert rotation happens. If the MCPs are paused, the cert rotation does not happen, which causes the cluster to become degraded and causes failure in multiple **oc** commands, including but not limited to **oc debug**, **oc logs**, **oc exec**, and **oc attach**.

To pause an MCP:

1. Patch the MCP that you want paused:

```
$ oc patch mcp/<mcp_name> --patch '{"spec":{"paused":true}}' --type=merge
```

For example:

```
$ oc patch mcp/workerpool-canary --patch '{"spec":{"paused":true}}' --type=merge
```

### Example output

```
machineconfigpool.machineconfiguration.openshift.io/workerpool-canary patched
```

## 10.5. PERFORMING THE CLUSTER UPDATE

When the MCPs enter ready state, you can perform the cluster update. See one of the following update methods, as appropriate for your cluster:

- [Updating a cluster using the web console](#)
- [Updating a cluster using the CLI](#)

After the update is complete, you can start to unpause the MCPs one-by-one.

## 10.6. UNPAUSING THE MACHINE CONFIG POOLS

In this canary rollout update process, after the OpenShift Container Platform update is complete, unpause your custom MCPs one-by-one. Unpausing an MCP allows the Machine Config Operator (MCO) to update the nodes associated with that MCP.

To unpause an MCP:

1. Patch the MCP that you want to unpause:

```
$ oc patch mcp/<mcp_name> --patch '{"spec":{"paused":false}}' --type=merge
```

For example:

```
$ oc patch mcp/workerpool-canary --patch '{"spec":{"paused":false}}' --type=merge
```

### Example output

```
machineconfigpool.machineconfiguration.openshift.io/workerpool-canary patched
```

You can check the progress of the update by using the **oc get machineconfigpools** command.

2. Test your applications on the updated nodes to ensure that they are working as expected.
3. Unpause any other paused MCPs one-by-one and verify that your applications work.

### 10.6.1. In case of application failure

In case of a failure, such as your applications not working on the updated nodes, you can cordon and drain the nodes in the pool, which moves the application pods to other nodes to help maintain the quality-of-service for the applications. This first MCP should be no larger than the excess capacity.

## 10.7. MOVING A NODE TO THE ORIGINAL MACHINE CONFIG POOL

In this canary rollout update process, after you have unpaused a custom machine config pool (MCP) and verified that the applications on the nodes associated with that MCP are working as expected, you should move the node back to its original MCP by removing the custom label you added to the node.



### IMPORTANT

A node must have a role to be properly functioning in the cluster.



To move a node to its original MCP:

1. Remove the custom label from the node.

```
$ oc label node <node_name> node-role.kubernetes.io/<custom-label>-
```

For example:

```
$ oc label node ci-ln-0qv1yp2-f76d1-kl2tq-worker-a-j2ssz node-
role.kubernetes.io/workerpool-canary-
```

### Example output

```
node/ci-ln-0qv1yp2-f76d1-kl2tq-worker-a-j2ssz labeled
```

The MCO moves the nodes back to the original MCP and reconciles the node to the MCP configuration.

2. View the list of MCPs in the cluster and their current state:

```
$oc get mcp
```

NAME	CONFIG	UPDATED	UPDATING
DEGRADED	MACHINECOUNT	READYMACHINECOUNT	UPDATEDMACHINECOUNT
DEGRADEDMACHINECOUNT	AGE		
master	rendered-master-1203f157d053fd987c7cbd91e3fbc0ed	True	False
False	3 3 3 0	61m	
workerpool-canary	rendered-mcp-noupdate-5ad4791166c468f3a35cd16e734c9028	True	False
False	False 0 0 0 0	21m	
worker	rendered-worker-5ad4791166c468f3a35cd16e734c9028	True	False
False	3 3 3 0	61m	

The node is removed from the custom MCP and moved back to the original MCP. It can take several minutes to update the machine counts. In this example, one node was moved from the removed **workerpool-canary** MCP to the `worker` MCP.

3. Optional: Delete the custom MCP:

```
$ oc delete mcp <mcp_name>
```

## CHAPTER 11. UPDATING A CLUSTER THAT INCLUDES RHEL COMPUTE MACHINES

You can update, or upgrade, an OpenShift Container Platform cluster. If your cluster contains Red Hat Enterprise Linux (RHEL) machines, you must perform more steps to update those machines.

### 11.1. PREREQUISITES

- Have access to the cluster as a user with **admin** privileges. See [Using RBAC to define and apply permissions](#).
- Have a recent [etcd backup](#) in case your update fails and you must [restore your cluster to a previous state](#).
- Support for RHEL7 workers is removed in OpenShift Container Platform 4.10. You must replace RHEL7 workers with RHEL8 or RHCOS workers before upgrading to OpenShift Container Platform 4.10. Red Hat does not support in-place RHEL7 to RHEL8 updates for RHEL workers; those hosts must be replaced with a clean operating system install.
- If your cluster uses manually maintained credentials, update the cloud provider resources for the new release. For more information, including how to determine if this is a requirement for your cluster, see [Preparing to update a cluster with manually maintained credentials](#).
- If you run an Operator or you have configured any application with the pod disruption budget, you might experience an interruption during the upgrade process. If **minAvailable** is set to 1 in **PodDisruptionBudget**, the nodes are drained to apply pending machine configs which might block the eviction process. If several nodes are rebooted, all the pods might run on only one node, and the **PodDisruptionBudget** field can prevent the node drain.

#### Additional resources

- [Support policy for unmanaged Operators](#)

### 11.2. UPDATING A CLUSTER BY USING THE WEB CONSOLE

If updates are available, you can update your cluster from the web console.

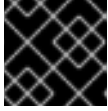
You can find information about available OpenShift Container Platform advisories and updates [in the errata section](#) of the Customer Portal.

#### Prerequisites

- Have access to the web console as a user with **admin** privileges.
- Pause all **MachineHealthCheck** resources.

#### Procedure

1. From the web console, click **Administration** → **Cluster Settings** and review the contents of the **Details** tab.
2. For production clusters, ensure that the **Channel** is set to the correct channel for the version that you want to update to, such as **stable-4.10**.



## IMPORTANT

For production clusters, you must subscribe to a **stable-\***, **eus-\*** or **fast-\*** channel.



## NOTE

When you are ready to move to the next minor version, choose the channel that corresponds to that minor version. The sooner the update channel is declared, the more effectively the cluster can recommend update paths to your target version. The cluster might take some time to evaluate all the possible updates that are available and offer the best update recommendations to choose from. Update recommendations can change over time, as they are based on what update options are available at the time.

If you cannot see an update path to your target minor version, keep updating your cluster to the latest patch release for your current version until the next minor version is available in the path.

- If the **Update status** is not **Updates available**, you cannot update your cluster.
  - **Select channel** indicates the cluster version that your cluster is running or is updating to.
3. Select a version to update to, and click **Save**.  
The Input channel **Update status** changes to **Update to <product-version> in progress**, and you can review the progress of the cluster update by watching the progress bars for the Operators and nodes.



## NOTE

If you are upgrading your cluster to the next minor version, like version 4.y to 4.(y+1), it is recommended to confirm your nodes are upgraded before deploying workloads that rely on a new feature. Any pools with worker nodes that are not yet updated are displayed on the **Cluster Settings** page.

4. After the update completes and the Cluster Version Operator refreshes the available updates, check if more updates are available in your current channel.
- If updates are available, continue to perform updates in the current channel until you can no longer update.
  - If no updates are available, change the **Channel** to the **stable-\***, **eus-\*** or **fast-\*** channel for the next minor version, and update to the version that you want in that channel.

You might need to perform several intermediate updates until you reach the version that you want.



## NOTE

When you update a cluster that contains Red Hat Enterprise Linux (RHEL) worker machines, those workers temporarily become unavailable during the update process. You must run the upgrade playbook against each RHEL machine as it enters the **NotReady** state for the cluster to finish updating.

## 11.3. OPTIONAL: ADDING HOOKS TO PERFORM ANSIBLE TASKS ON RHEL MACHINES

You can use *hooks* to run Ansible tasks on the RHEL compute machines during the OpenShift Container Platform update.

### 11.3.1. About Ansible hooks for upgrades

When you update OpenShift Container Platform, you can run custom tasks on your Red Hat Enterprise Linux (RHEL) nodes during specific operations by using *hooks*. Hooks allow you to provide files that define tasks to run before or after specific update tasks. You can use hooks to validate or modify custom infrastructure when you update the RHEL compute nodes in you OpenShift Container Platform cluster.

Because when a hook fails, the operation fails, you must design hooks that are idempotent, or can run multiple times and provide the same results.

Hooks have the following important limitations: - Hooks do not have a defined or versioned interface. They can use internal **openshift-ansible** variables, but it is possible that the variables will be modified or removed in future OpenShift Container Platform releases. - Hooks do not have error handling, so an error in a hook halts the update process. If you get an error, you must address the problem and then start the upgrade again.

### 11.3.2. Configuring the Ansible inventory file to use hooks

You define the hooks to use when you update the Red Hat Enterprise Linux (RHEL) compute machines, which are also known as worker machines, in the **hosts** inventory file under the **all:vars** section.

#### Prerequisites

- You have access to the machine that you used to add the RHEL compute machines cluster. You must have access to the **hosts** Ansible inventory file that defines your RHEL machines.

#### Procedure

1. After you design the hook, create a YAML file that defines the Ansible tasks for it. This file must be a set of tasks and cannot be a playbook, as shown in the following example:

```
---
# Trivial example forcing an operator to acknowledge the start of an upgrade
# file=/home/user/openshift-ansible/hooks/pre_compute.yml

- name: note the start of a compute machine update
  debug:
    msg: "Compute machine upgrade of {{ inventory_hostname }} is about to start"

- name: require the user agree to start an upgrade
  pause:
    prompt: "Press Enter to start the compute machine update"
```

2. Modify the **hosts** Ansible inventory file to specify the hook files. The hook files are specified as parameter values in the **[all:vars]** section, as shown:

#### Example hook definitions in an inventory file

```
[all:vars]
openshift_node_pre_upgrade_hook=/home/user/openshift-ansible/hooks/pre_node.yml
openshift_node_post_upgrade_hook=/home/user/openshift-ansible/hooks/post_node.yml
```

To avoid ambiguity in the paths to the hook, use absolute paths instead of a relative paths in their definitions.

### 11.3.3. Available hooks for RHEL compute machines

You can use the following hooks when you update the Red Hat Enterprise Linux (RHEL) compute machines in your OpenShift Container Platform cluster.

Hook name	Description
<code>openshift_node_pre_cordon_hook</code>	<ul style="list-style-type: none"> <li>● Runs <b>before</b> each node is cordoned.</li> <li>● This hook runs against <b>each node</b> in serial.</li> <li>● If a task must run against a different host, the task must use <code>delegate_to</code> or <code>local_action</code>.</li> </ul>
<code>openshift_node_pre_upgrade_hook</code>	<ul style="list-style-type: none"> <li>● Runs <b>after</b> each node is cordoned but <b>before</b> it is updated.</li> <li>● This hook runs against <b>each node</b> in serial.</li> <li>● If a task must run against a different host, the task must use <code>delegate_to</code> or <code>local_action</code>.</li> </ul>
<code>openshift_node_pre_uncordon_hook</code>	<ul style="list-style-type: none"> <li>● Runs <b>after</b> each node is updated but <b>before</b> it is uncordoned.</li> <li>● This hook runs against <b>each node</b> in serial.</li> <li>● If a task must run against a different host, they task must use <code>delegate_to</code> or <code>local_action</code>.</li> </ul>
<code>openshift_node_post_upgrade_hook</code>	<ul style="list-style-type: none"> <li>● Runs <b>after</b> each node uncordoned. It is the <b>last</b> node update action.</li> <li>● This hook runs against <b>each node</b> in serial.</li> <li>● If a task must run against a different host, the task must use <code>delegate_to</code> or <code>local_action</code>.</li> </ul>

## 11.4. UPDATING RHEL COMPUTE MACHINES IN YOUR CLUSTER

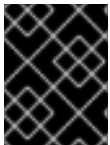
After you update your cluster, you must update the Red Hat Enterprise Linux (RHEL) compute machines in your cluster.



### IMPORTANT

Red Hat Enterprise Linux (RHEL) versions 8.5–8.8 are supported for RHEL compute machines.

You can also update your compute machines to another minor version of OpenShift Container Platform if you are using RHEL as the operating system. You do not need to exclude any RPM packages from RHEL when performing a minor version update.

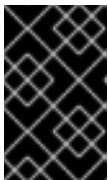


### IMPORTANT

You cannot upgrade RHEL 7 compute machines to RHEL 8. You must deploy new RHEL 8 hosts, and the old RHEL 7 hosts should be removed.

## Prerequisites

- You updated your cluster.



### IMPORTANT

Because the RHEL machines require assets that are generated by the cluster to complete the update process, you must update the cluster before you update the RHEL worker machines in it.

- You have access to the local machine that you used to add the RHEL compute machines to your cluster. You must have access to the **hosts** Ansible inventory file that defines your RHEL machines and the **upgrade** playbook.
- For updates to a minor version, the RPM repository is using the same version of OpenShift Container Platform that is running on your cluster.

## Procedure

1. Stop and disable firewalld on the host:

```
# systemctl disable --now firewalld.service
```



### NOTE

By default, the base OS RHEL with "Minimal" installation option enables firewalld service. Having the firewalld service enabled on your host prevents you from accessing OpenShift Container Platform logs on the worker. Do not enable firewalld later if you wish to continue accessing OpenShift Container Platform logs on the worker.

2. Enable the repositories that are required for OpenShift Container Platform 4.10:
  - a. On the machine that you run the Ansible playbooks, update the required repositories:

```
# subscription-manager repos --disable=rhel-7-server-ose-4.9-rpms \
--enable=rhel-7-server-ose-4.10-rpms
```



### IMPORTANT

As of OpenShift Container Platform 4.10.23, running the Ansible playbooks on RHEL 7 is deprecated, and suggested only for the purpose of updating existing installations. After completing this procedure, you must either upgrade the Ansible host to RHEL 8, or create a new Ansible host on a RHEL 8 system and copy over the inventories from the old Ansible host. Starting with OpenShift Container Platform 4.11, the Ansible playbooks are provided only for RHEL 8.

- b. On the machine that you run the Ansible playbooks, update the required packages, including **openshift-ansible**:

```
# yum update openshift-ansible openshift-clients
```

- c. On each RHEL compute node, update the required repositories:

```
# subscription-manager repos --disable=rhocp-4.9-for-rhel-8-x86_64-rpms \
--enable=rhocp-4.10-for-rhel-8-x86_64-rpms
```

3. Update a RHEL worker machine:

- a. Review your Ansible inventory file at `/<path>/inventory/hosts` and update its contents so that the RHEL 8 machines are listed in the **[workers]** section, as shown in the following example:

```
[all:vars]
ansible_user=root
#ansible_become=True

openshift_kubeconfig_path=~/.kube/config"

[workers]
mycluster-rhel8-0.example.com
mycluster-rhel8-1.example.com
mycluster-rhel8-2.example.com
mycluster-rhel8-3.example.com
```

- b. Change to the **openshift-ansible** directory:

```
$ cd /usr/share/ansible/openshift-ansible
```

- c. Run the **upgrade** playbook:

```
$ ansible-playbook -i /<path>/inventory/hosts playbooks/upgrade.yml 1
```

- 1** For **<path>**, specify the path to the Ansible inventory file that you created.

**NOTE**

The **upgrade** playbook only upgrades the OpenShift Container Platform packages. It does not update the operating system packages.

- After you update all of the workers, confirm that all of your cluster nodes have updated to the new version:

```
# oc get node
```

**Example output**

NAME	STATUS	ROLES	AGE	VERSION
mycluster-control-plane-0	Ready	master	145m	v1.23.0
mycluster-control-plane-1	Ready	master	145m	v1.23.0
mycluster-control-plane-2	Ready	master	145m	v1.23.0
mycluster-rhel8-0	Ready	worker	98m	v1.23.0
mycluster-rhel8-1	Ready	worker	98m	v1.23.0
mycluster-rhel8-2	Ready	worker	98m	v1.23.0
mycluster-rhel8-3	Ready	worker	98m	v1.23.0

- Optional: Update the operating system packages that were not updated by the **upgrade** playbook. To update packages that are not on 4.10, use the following command:

```
# yum update
```

**NOTE**

You do not need to exclude RPM packages if you are using the same RPM repository that you used when you installed 4.10.



## CHAPTER 12. UPDATING A CLUSTER IN A DISCONNECTED ENVIRONMENT

### 12.1. ABOUT CLUSTER UPDATES IN A DISCONNECTED ENVIRONMENT

A disconnected environment is one in which your cluster nodes cannot access the internet. For this reason, you must populate a registry with the installation images. If your registry host cannot access both the internet and the cluster, you can mirror the images to a file system that is disconnected from that environment and then bring that host or removable media across that gap. If the local container registry and the cluster are connected to the mirror registry's host, you can directly push the release images to the local registry.

A single container image registry is sufficient to host mirrored images for several clusters in the disconnected network.

#### 12.1.1. Mirroring the OpenShift Container Platform image repository

To update a cluster in a disconnected environment, your cluster environment must have access to a mirror registry that has the necessary images and resources for your targeted update. The following page has instructions for mirroring images onto a repository in your disconnected cluster:

- [Mirroring the OpenShift Container Platform image repository](#)

#### 12.1.2. Performing a cluster update in a disconnected environment

You can use one of the following procedures to update a disconnected OpenShift Container Platform cluster:

- [Updating a cluster in a disconnected environment using the OpenShift Update Service](#)
- [Updating a cluster in a disconnected environment without the OpenShift Update Service](#)

#### 12.1.3. Uninstalling the OpenShift Update Service from a cluster

You can use the following procedure to uninstall a local copy of the OpenShift Update Service (OSUS) from your cluster:

- [Uninstalling the OpenShift Update Service from a cluster](#)

### 12.2. MIRRORING THE OPENSIFT CONTAINER PLATFORM IMAGE REPOSITORY

You must mirror container images onto a mirror registry before you can update a cluster in a disconnected environment. You can also use this procedure in connected environments to ensure your clusters run only approved container images that have satisfied your organizational controls for external content.

#### 12.2.1. 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 Red Hat Quay.

## 12.2.2. 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.

### 12.2.2.1. 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 4.10. Download and install the new version of **oc**. If you are upgrading a cluster in a disconnected environment, install the **oc** version that you plan to upgrade to.

### 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 v4.10 Linux Client** entry and save the file.
4. Unpack the archive:

```
$ tar xvf <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 v4.10 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 v4.10 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>
```

#### 12.2.2.2. 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.



#### WARNING

Do not use this image registry credentials file as the pull secret when you install a cluster. If you provide this file when you install cluster, all of the machines in the cluster will have write access to your mirror registry.

**WARNING**

This process requires that you have write access to a container image registry on the mirror registry and adds the credentials to a registry pull secret.

**Prerequisites**

- You configured a mirror registry to use in your disconnected environment.
- You identified an image repository location on your mirror registry to mirror images into.
- You provisioned a mirror registry account that allows images to be uploaded to that image repository.

**Procedure**

Complete the following steps on the installation host:

1. Download your **registry.redhat.io** pull secret from the [Red Hat OpenShift Cluster Manager](#) .
2. Make a copy of your pull secret in JSON format:

```
$ cat ./pull-secret | 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"
    }
  }
}
```

3. Generate the base64-encoded user name and password or token for your mirror registry:

```
$ echo -n '<user_name>:<password>' | base64 -w0 1
BGVtbYk3ZHAAtqXs=
```

- 1** For **<user\_name>** and **<password>**, specify the user name and password that you configured for your registry.

4. Edit the JSON file and add a section that describes your registry to it:

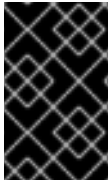
```
"auths": {
  "<mirror_registry>": { 1
    "auth": "<credentials>", 2
    "email": "you@example.com"
  }
},
```

- 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:8443**
- 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": "BGVtbYk3ZHAAtqXs=",
      "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"
    }
  }
}
```

### 12.2.3. Mirroring the OpenShift Container Platform image repository



## IMPORTANT

To avoid excessive memory usage by the OpenShift Update Service application, you must mirror release images to a separate repository as described in the following procedure.

### Prerequisites

- You configured a mirror registry to use in your disconnected environment and can access the certificate and credentials that you configured.
- You downloaded the [pull secret from the Red Hat OpenShift Cluster Manager](#) and modified it to include authentication to your mirror repository.
- If you use self-signed certificates, you have specified a Subject Alternative Name in the certificates.

### Procedure

1. Use the [Red Hat OpenShift Container Platform Upgrade Graph visualizer and update planner](#) to plan an update from one version to another. The OpenShift Upgrade Graph provides channel graphs and a way to confirm that there is an update path between your current and intended cluster versions.
2. Set the required environment variables:

- a. Export the release version:

```
$ export OCP_RELEASE=<release_version>
```

For **<release\_version>**, specify the tag that corresponds to the version of OpenShift Container Platform to which you want to update, 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. If you are using the OpenShift Update Service, export an additional local repository name to contain the release images:

```
$ LOCAL_RELEASE_IMAGES_REPOSITORY='<local_release_images_repository_name>'
```

For **<local\_release\_images\_repository\_name>**, specify the name of the repository to create in your registry, such as **ocp4/openshift4-release-images**.

- e. Export the name of the repository to mirror:

```
$ PRODUCT_REPO='openshift-release-dev'
```

For a production release, you must specify **openshift-release-dev**.

- f. 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.



#### NOTE

If your cluster uses an **ImageContentSourcePolicy** object to configure repository mirroring, you can use only global pull secrets for mirrored registries. You cannot add a pull secret to a project.

- g. Export the release mirror:

```
$ RELEASE_NAME="ocp-release"
```

For a production release, you must specify **ocp-release**.

- h. Export the type of architecture for your server, such as **x86\_64**:

```
$ ARCHITECTURE=<server_architecture>
```

- i. 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. Review the images and configuration manifests to mirror:

```
$ oc adm release mirror -a ${LOCAL_SECRET_JSON} --to-dir=${REMOVABLE_MEDIA_PATH}/mirror quay.io/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE}-${ARCHITECTURE} --dry-run
```

4. 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. Mirror the images and configuration manifests 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}

```

- iii. Take the media to the disconnected 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} 1

```

- 1** For **REMOVABLE\_MEDIA\_PATH**, you must use the same path that you specified when you mirrored the images.

- iv. Use **oc** command-line interface (CLI) to log in to the cluster that you are upgrading.

- v. Apply the mirrored release image signature config map to the connected cluster:

```

| $ oc apply -f ${REMOVABLE_MEDIA_PATH}/mirror/config/<image_signature_file>
| 1

```

- 1** For **<image\_signature\_file>**, specify the path and name of the file, for example, **signature-sha256-81154f5c03294534.yaml**.

- vi. If you are using the OpenShift Update Service, mirror the release image to a separate repository:

```

| $ oc image mirror -a ${LOCAL_SECRET_JSON}
| ${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}-
| ${ARCHITECTURE}
| ${LOCAL_REGISTRY}/${LOCAL_RELEASE_IMAGES_REPOSITORY}:${OCP_REL
| EASE}-${ARCHITECTURE}

```

- If the local container registry and the cluster are connected to the mirror host, take the following actions:
  - i. Directly push the release images to the local registry and apply the config map to the cluster 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} --apply-release-image-
| signature

```



#### NOTE

If you include the **--apply-release-image-signature** option, do not create the config map for image signature verification.

- ii. If you are using the OpenShift Update Service, mirror the release image to a separate repository:



```
$ oc image mirror -a ${LOCAL_SECRET_JSON}
${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}-
${ARCHITECTURE}
${LOCAL_REGISTRY}/${LOCAL_RELEASE_IMAGES_REPOSITORY}:${OCP_REL
EASE}-${ARCHITECTURE}
```

## 12.3. UPDATING A CLUSTER IN A DISCONNECTED ENVIRONMENT USING THE OPENSIFT UPDATE SERVICE

To get an update experience similar to connected clusters, you can use the following procedures to install and configure the OpenShift Update Service in a disconnected environment.

### 12.3.1. Using the OpenShift Update Service in a disconnected environment

The OpenShift Update Service (OSUS) provides update recommendations to OpenShift Container Platform clusters. Red Hat publicly hosts the OpenShift Update Service, and clusters in a connected environment can connect to the service through public APIs to retrieve update recommendations.

However, clusters in a disconnected environment cannot access these public APIs to retrieve update information. To have a similar update experience in a disconnected environment, you can install and configure the OpenShift Update Service locally so that it is available within the disconnected environment.

A single OSUS instance is capable of serving recommendations to thousands of clusters. OSUS can be scaled horizontally to cater to more clusters by changing the replica value. So for most disconnected use cases, one OSUS instance is enough. For example, Red Hat hosts just one OSUS instance for the entire fleet of connected clusters.

If you want to keep update recommendations separate in different environments, you can run one OSUS instance for each environment. For example, in a case where you have separate test and stage environments, you might not want a cluster in a stage environment to receive update recommendations to version A if that version has not been tested in the test environment yet.

The following sections describe how to install a local OSUS instance and configure it to provide update recommendations to a cluster.

#### Additional resources

- [About the OpenShift Update Service](#)
- [Understanding update channels and releases](#)

### 12.3.2. Prerequisites

- You must have the **oc** command-line interface (CLI) tool installed.
- You must provision a local container image registry with the container images for your update, as described in [Mirroring the OpenShift Container Platform image repository](#).

### 12.3.3. Configuring access to a secured registry for the OpenShift Update Service

If the release images are contained in a registry whose HTTPS X.509 certificate is signed by a custom certificate authority, complete the steps in [Configuring additional trust stores for image registry access](#) along with following changes for the update service.

The OpenShift Update Service Operator needs the config map key name **updateservice-registry** in the registry CA cert.

### Image registry CA config map example for the update service

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: my-registry-ca
data:
  updateservice-registry: | 1
    -----BEGIN CERTIFICATE-----
    ...
    -----END CERTIFICATE-----
  registry-with-port.example.com..5000: | 2
    -----BEGIN CERTIFICATE-----
    ...
    -----END CERTIFICATE-----
```

- 1** The OpenShift Update Service Operator requires the config map key name `updateservice-registry` in the registry CA cert.
- 2** If the registry has the port, such as **registry-with-port.example.com:5000**, `:` should be replaced with `..`

### 12.3.4. Updating the global cluster pull secret

You can update the global pull secret for your cluster by either replacing the current pull secret or appending a new pull secret.

The procedure is required when users use a separate registry to store images than the registry used during installation.

#### Prerequisites

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

#### Procedure

1. Optional: To append a new pull secret to the existing pull secret, complete the following steps:
  - a. Enter the following command to download the pull secret:

```
$ oc get secret/pull-secret -n openshift-config --template='{{index .data
".dockerconfigjson" | base64decode}}' ><pull_secret_location> 1
```

- 1** Provide the path to the pull secret file.

- b. Enter the following command to add the new pull secret:

```
$ oc registry login --registry="<registry>" \ 1
--auth-basic="<username>:<password>" \ 2
--to=<pull_secret_location> 3
```

- 1 Provide the new registry. You can include multiple repositories within the same registry, for example: `--registry="<registry/my-namespace/my-repository>"`.
- 2 Provide the credentials of the new registry.
- 3 Provide the path to the pull secret file.

Alternatively, you can perform a manual update to the pull secret file.

2. Enter the following command to update the global pull secret for your cluster:

```
$ oc set data secret/pull-secret -n openshift-config --from-file=.dockerconfigson=
<pull_secret_location> 1
```

- 1 Provide the path to the new pull secret file.

This update is rolled out to all nodes, which can take some time depending on the size of your cluster.



#### NOTE

As of OpenShift Container Platform 4.7.4, changes to the global pull secret no longer trigger a node drain or reboot.

### 12.3.5. Installing the OpenShift Update Service Operator

To install the OpenShift Update Service, you must first install the OpenShift Update Service Operator by using the OpenShift Container Platform web console or CLI.



#### NOTE

For clusters that are installed on disconnected environments, also known as disconnected clusters, Operator Lifecycle Manager by default cannot access the Red Hat-provided OperatorHub sources hosted on remote registries because those remote sources require full internet connectivity. For more information, see [Using Operator Lifecycle Manager on restricted networks](#).

#### 12.3.5.1. Installing the OpenShift Update Service Operator by using the web console

You can use the web console to install the OpenShift Update Service Operator.

##### Procedure

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

**NOTE**

Enter **Update Service** into the **Filter by keyword...** field to find the Operator faster.

2. Choose **OpenShift Update Service** from the list of available Operators, and click **Install**.
  - a. Channel **v1** is selected as the **Update Channel** since it is the only channel available in this release.
  - b. Select **A specific namespace on the cluster** under **Installation Mode**.
  - c. Select a namespace for **Installed Namespace** or accept the recommended namespace **openshift-update-service**.
  - d. Select an **Approval Strategy**:
    - The **Automatic** strategy allows Operator Lifecycle Manager (OLM) to automatically update the Operator when a new version is available.
    - The **Manual** strategy requires a cluster administrator to approve the Operator update.
  - e. Click **Install**.
3. Verify that the OpenShift Update Service Operator is installed by switching to the **Operators** → **Installed Operators** page.
4. Ensure that **OpenShift Update Service** is listed in the selected namespace with a **Status** of **Succeeded**.

### 12.3.5.2. Installing the OpenShift Update Service Operator by using the CLI

You can use the OpenShift CLI (**oc**) to install the OpenShift Update Service Operator.

#### Procedure

1. Create a namespace for the OpenShift Update Service Operator:
  - a. Create a **Namespace** object YAML file, for example, **update-service-namespace.yaml**, for the OpenShift Update Service Operator:

```
apiVersion: v1
kind: Namespace
metadata:
  name: openshift-update-service
  annotations:
    openshift.io/node-selector: ""
  labels:
    openshift.io/cluster-monitoring: "true" 1
```

- 1** Set the **openshift.io/cluster-monitoring** label to enable Operator-recommended cluster monitoring on this namespace.

- b. Create the namespace:

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

For example:

```
$ oc create -f update-service-namespace.yaml
```

2. Install the OpenShift Update Service Operator by creating the following objects:

- a. Create an **OperatorGroup** object YAML file, for example, **update-service-operator-group.yaml**:

```
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: update-service-operator-group
spec:
  targetNamespaces:
  - openshift-update-service
```

- b. Create an **OperatorGroup** object:

```
$ oc -n openshift-update-service create -f <filename>.yaml
```

For example:

```
$ oc -n openshift-update-service create -f update-service-operator-group.yaml
```

- c. Create a **Subscription** object YAML file, for example, **update-service-subscription.yaml**:

### Example Subscription

```
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: update-service-subscription
spec:
  channel: v1
  installPlanApproval: "Automatic"
  source: "redhat-operators" 1
  sourceNamespace: "openshift-marketplace"
  name: "cincinnati-operator"
```

- 1** Specify the name of the catalog source that provides the Operator. For clusters that do not use a custom Operator Lifecycle Manager (OLM), specify **redhat-operators**. If your OpenShift Container Platform cluster is installed in a disconnected environment, specify the name of the **CatalogSource** object created when you configured Operator Lifecycle Manager (OLM).

- d. Create the **Subscription** object:

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

For example:

```
$ oc -n openshift-update-service create -f update-service-subscription.yaml
```

The OpenShift Update Service Operator is installed to the **openshift-update-service** namespace and targets the **openshift-update-service** namespace.

3. Verify the Operator installation:

```
$ oc -n openshift-update-service get clusterserviceversions
```

### Example output

```
NAME                DISPLAY                VERSION  REPLACES  PHASE
update-service-operator.v4.6.0  OpenShift Update Service  4.6.0    Succeeded
...
```

If the OpenShift Update Service Operator is listed, the installation was successful. The version number might be different than shown.

### Additional resources

- [Installing Operators in your namespace](#) .

## 12.3.6. Creating the OpenShift Update Service graph data container image

The OpenShift Update Service requires a graph-data container image, from which the OpenShift Update Service retrieves information about channel membership and blocked update edges. Graph data is typically fetched directly from the upgrade graph data repository. In environments where an internet connection is unavailable, loading this information from an init container is another way to make the graph data available to the OpenShift Update Service. The role of the init container is to provide a local copy of the graph data, and during pod initialization, the init container copies the data to a volume that is accessible by the service.

### Procedure

1. Create a Dockerfile, for example, **./Dockerfile**, containing the following:

```
FROM registry.access.redhat.com/ubi8/ubi:8.1

RUN curl -L -o cincinnati-graph-data.tar.gz
https://api.openshift.com/api/upgrades_info/graph-data

RUN mkdir -p /var/lib/cincinnati-graph-data && tar xvfz cincinnati-graph-data.tar.gz -C
/var/lib/cincinnati-graph-data/ --no-overwrite-dir --no-same-owner

CMD ["/bin/bash", "-c", "exec cp -rp /var/lib/cincinnati-graph-data/* /var/lib/cincinnati/graph-
data"]
```

2. Use the docker file created in the above step to build a graph-data container image, for example, **registry.example.com/openshift/graph-data:latest**:

```
$ podman build -f ./Dockerfile -t registry.example.com/openshift/graph-data:latest
```

3. Push the graph-data container image created in the previous step to a repository that is accessible to the OpenShift Update Service, for example, **registry.example.com/openshift/graph-data:latest**:

```
$ podman push registry.example.com/openshift/graph-data:latest
```



#### NOTE

To push a graph data image to a local registry in a disconnected environment, copy the graph-data container image created in the previous step to a repository that is accessible to the OpenShift Update Service. Run **oc image mirror --help** for available options.

### 12.3.7. Creating an OpenShift Update Service application

You can create an OpenShift Update Service application by using the OpenShift Container Platform web console or CLI.

#### 12.3.7.1. Creating an OpenShift Update Service application by using the web console

You can use the OpenShift Container Platform web console to create an OpenShift Update Service application by using the OpenShift Update Service Operator.

#### Prerequisites

- The OpenShift Update Service Operator has been installed.
- The OpenShift Update Service graph-data container image has been created and pushed to a repository that is accessible to the OpenShift Update Service.
- The current release and update target releases have been mirrored to a locally accessible registry.

#### Procedure

1. In the web console, click **Operators → Installed Operators**.
2. Choose **OpenShift Update Service** from the list of installed Operators.
3. Click the **Update Service** tab.
4. Click **Create UpdateService**.
5. Enter a name in the **Name** field, for example, **service**.
6. Enter the local pullspec in the **Graph Data Image** field to the graph-data container image created in "Creating the OpenShift Update Service graph data container image", for example, **registry.example.com/openshift/graph-data:latest**.
7. In the **Releases** field, enter the local registry and repository created to contain the release images in "Mirroring the OpenShift Container Platform image repository", for example, **registry.example.com/ocp4/openshift4-release-images**.
8. Enter **2** in the **Replicas** field.

9. Click **Create** to create the OpenShift Update Service application.
10. Verify the OpenShift Update Service application:
  - From the **UpdateServices** list in the **Update Service** tab, click the Update Service application just created.
  - Click the **Resources** tab.
  - Verify each application resource has a status of **Created**.

### 12.3.7.2. Creating an OpenShift Update Service application by using the CLI

You can use the OpenShift CLI (**oc**) to create an OpenShift Update Service application.

#### Prerequisites

- The OpenShift Update Service Operator has been installed.
- The OpenShift Update Service graph-data container image has been created and pushed to a repository that is accessible to the OpenShift Update Service.
- The current release and update target releases have been mirrored to a locally accessible registry.

#### Procedure

1. Configure the OpenShift Update Service target namespace, for example, **openshift-update-service**:

```
$ NAMESPACE=openshift-update-service
```

The namespace must match the **targetNamespaces** value from the operator group.

2. Configure the name of the OpenShift Update Service application, for example, **service**:

```
$ NAME=service
```

3. Configure the local registry and repository for the release images as configured in "Mirroring the OpenShift Container Platform image repository", for example, **registry.example.com/ocp4/openshift4-release-images**:

```
$ RELEASE_IMAGES=registry.example.com/ocp4/openshift4-release-images
```

4. Set the local pullspec for the graph-data image to the graph-data container image created in "Creating the OpenShift Update Service graph data container image", for example, **registry.example.com/openshift/graph-data:latest**:

```
$ GRAPH_DATA_IMAGE=registry.example.com/openshift/graph-data:latest
```

5. Create an OpenShift Update Service application object:

```
$ oc -n "${NAMESPACE}" create -f - <<EOF
apiVersion: updateservice.operator.openshift.io/v1
```



```

kind: UpdateService
metadata:
  name: ${NAME}
spec:
  replicas: 2
  releases: ${RELEASE_IMAGES}
  graphDataImage: ${GRAPH_DATA_IMAGE}
EOF

```

6. Verify the OpenShift Update Service application:

- a. Use the following command to obtain a policy engine route:

```

$ while sleep 1; do POLICY_ENGINE_GRAPH_URI="$(oc -n "${NAMESPACE}" get -o
jsonpath='{.status.policyEngineURI}/api/upgrades_info/v1/graph{"\n"}' updateservice
"${NAME}")"; SCHEME="${POLICY_ENGINE_GRAPH_URI%%:*}"; if test "${SCHEME}"
= http -o "${SCHEME}" = https; then break; fi; done

```

You might need to poll until the command succeeds.

- b. Retrieve a graph from the policy engine. Be sure to specify a valid version for **channel**. For example, if running in OpenShift Container Platform 4.10, use **stable-4.10**:

```

$ while sleep 10; do HTTP_CODE="$(curl --header Accept:application/json --output
/dev/stderr --write-out "%{http_code}" "${POLICY_ENGINE_GRAPH_URI}?
channel=stable-4.6")"; if test "${HTTP_CODE}" -eq 200; then break; fi; echo
"${HTTP_CODE}"; done

```

This polls until the graph request succeeds; however, the resulting graph might be empty depending on which release images you have mirrored.



#### NOTE

The policy engine route name must not be more than 63 characters based on RFC-1123. If you see **ReconcileCompleted** status as **false** with the reason **CreateRouteFailed** caused by **host must conform to DNS 1123 naming convention and must be no more than 63 characters**, try creating the Update Service with a shorter name.

#### 12.3.7.2.1. Configuring the Cluster Version Operator (CVO)

After the OpenShift Update Service Operator has been installed and the OpenShift Update Service application has been created, the Cluster Version Operator (CVO) can be updated to pull graph data from the locally installed OpenShift Update Service.

#### Prerequisites

- The OpenShift Update Service Operator has been installed.
- The OpenShift Update Service graph-data container image has been created and pushed to a repository that is accessible to the OpenShift Update Service.
- The current release and update target releases have been mirrored to a locally accessible registry.
- The OpenShift Update Service application has been created.

## Procedure

1. Set the OpenShift Update Service target namespace, for example, **openshift-update-service**:

```
$ NAMESPACE=openshift-update-service
```

2. Set the name of the OpenShift Update Service application, for example, **service**:

```
$ NAME=service
```

3. Obtain the policy engine route:

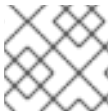
```
$ POLICY_ENGINE_GRAPH_URI="$(oc -n "${NAMESPACE}" get -o jsonpath='{.status.policyEngineURI}/api/upgrades_info/v1/graph{"\n"}' updateservice "${NAME}")"
```

4. Set the patch for the pull graph data:

```
$ PATCH="{\"spec\":{\"upstream\": \"${POLICY_ENGINE_GRAPH_URI}\"}"
```

5. Patch the CVO to use the local OpenShift Update Service:

```
$ oc patch clusterversion version -p $PATCH --type merge
```



### NOTE

See [Enabling the cluster-wide proxy](#) to configure the CA to trust the update server.

## 12.3.8. Next steps

Before updating your cluster, confirm that the following conditions are met:

- The Cluster Version Operator (CVO) is configured to use your locally-installed OpenShift Update Service application.
- The release image signature config map for the new release is applied to your cluster.



### NOTE

The release image signature config map allows the Cluster Version Operator (CVO) to ensure the integrity of release images by verifying that the actual image signatures match the expected signatures.

- The current release and update target release images are mirrored to a locally accessible registry.
- A recent graph data container image has been mirrored to your local registry.

After you configure your cluster to use the locally-installed OpenShift Update Service and local mirror registry, you can use any of the following update methods:

- [Updating a cluster using the web console](#)

- [Updating a cluster using the CLI](#)
- [Preparing to perform an EUS-to-EUS update](#)
- [Performing a canary rollout update](#)
- [Updating a cluster that includes RHEL compute machines](#)

## 12.4. UPDATING A CLUSTER IN A DISCONNECTED ENVIRONMENT WITHOUT THE OPENSIFT UPDATE SERVICE

Use the following procedures to update a cluster in a disconnected environment without access to the OpenShift Update Service.

### 12.4.1. Prerequisites

- You must have the **oc** command-line interface (CLI) tool installed.
- You must provision a local container image registry with the container images for your update, as described in [Mirroring the OpenShift Container Platform image repository](#).
- You must have access to the cluster as a user with **admin** privileges. See [Using RBAC to define and apply permissions](#).
- You must have a recent [etcd backup](#) in case your update fails and you must [restore your cluster to a previous state](#).
- You must ensure that all machine config pools (MCPs) are running and not paused. Nodes associated with a paused MCP are skipped during the update process. You can pause the MCPs if you are performing a canary rollout update strategy.
- If your cluster uses manually maintained credentials, update the cloud provider resources for the new release. For more information, including how to determine if this is a requirement for your cluster, see [Preparing to update a cluster with manually maintained credentials](#).
- If you run an Operator or you have configured any application with the pod disruption budget, you might experience an interruption during the upgrade process. If **minAvailable** is set to 1 in **PodDisruptionBudget**, the nodes are drained to apply pending machine configs which might block the eviction process. If several nodes are rebooted, all the pods might run on only one node, and the **PodDisruptionBudget** field can prevent the node drain.

### 12.4.2. Pausing a MachineHealthCheck resource

During the upgrade process, nodes in the cluster might become temporarily unavailable. In the case of worker nodes, the machine health check might identify such nodes as unhealthy and reboot them. To avoid rebooting such nodes, pause all the **MachineHealthCheck** resources before updating the cluster.

#### Prerequisites

- Install the OpenShift CLI (**oc**).

#### Procedure

1. To list all the available **MachineHealthCheck** resources that you want to pause, run the following command:

```
$ oc get machinehealthcheck -n openshift-machine-api
```

- To pause the machine health checks, add the **cluster.x-k8s.io/paused=""** annotation to the **MachineHealthCheck** resource. Run the following command:

```
$ oc -n openshift-machine-api annotate mhc <mhc-name> cluster.x-k8s.io/paused=""
```

The annotated **MachineHealthCheck** resource resembles the following YAML file:

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineHealthCheck
metadata:
  name: example
  namespace: openshift-machine-api
  annotations:
    cluster.x-k8s.io/paused: ""
spec:
  selector:
    matchLabels:
      role: worker
  unhealthyConditions:
  - type: "Ready"
    status: "Unknown"
    timeout: "300s"
  - type: "Ready"
    status: "False"
    timeout: "300s"
  maxUnhealthy: "40%"
status:
  currentHealthy: 5
  expectedMachines: 5
```

### IMPORTANT

Resume the machine health checks after updating the cluster. To resume the check, remove the pause annotation from the **MachineHealthCheck** resource by running the following command:

```
$ oc -n openshift-machine-api annotate mhc <mhc-name> cluster.x-k8s.io/paused-
```

### 12.4.3. Retrieving a release image digest

In order to update a cluster in a disconnected environment using the **oc adm upgrade** command with the **--to-image** option, you must reference the sha256 digest that corresponds to your targeted release image.

#### Procedure

- Run the following command on a device that is connected to the internet:

```
$ oc adm release info -o 'jsonpath={.digest}' quay.io/openshift-release-dev/ocp-release:${OCP_RELEASE_VERSION}-${ARCHITECTURE}
```

For **{OCP\_RELEASE\_VERSION}**, specify the version of OpenShift Container Platform to which you want to update, such as **4.10.16**.

For **{ARCHITECTURE}**, specify the architecture of the cluster, such as **x86\_64**, **aarch64**, **s390x**, or **ppc64le**.

### Example output

```
sha256:a8bfba3b6dddd1a2fbbead7dac65fe4fb8335089e4e7cae327f3bad334add31d
```

2. Copy the sha256 digest for use when updating your cluster.

## 12.4.4. Upgrading the disconnected cluster

Update the disconnected cluster to the OpenShift Container Platform version that you downloaded the release images for.



### NOTE

If you have a local OpenShift Update Service, you can update by using the connected web console or CLI instructions instead of this procedure.

### Prerequisites

- You mirrored the images for the new release to your registry.
- You applied the release image signature ConfigMap for the new release to your cluster.



### NOTE

The release image signature config map allows the Cluster Version Operator (CVO) to ensure the integrity of release images by verifying that the actual image signatures match the expected signatures.

- You obtained the sha256 digest for your targeted release image.
- You installed the OpenShift CLI (**oc**).
- You paused all **MachineHealthCheck** resources.

### Procedure

- Update the cluster:

```
$ oc adm upgrade --allow-explicit-upgrade --to-image  
${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}@<digest> 1
```

- 1** The **<digest>** value is the sha256 digest for the targeted release image, for example, **sha256:81154f5c03294534e1eaf0319bef7a601134f891689ccede5d705ef659aa8c92**

If you use an **ImageContentSourcePolicy** for the mirror registry, you can use the canonical registry name instead of **LOCAL\_REGISTRY**.

**NOTE**

You can only configure global pull secrets for clusters that have an **ImageContentSourcePolicy** object. You cannot add a pull secret to a project.

### 12.4.5. Configuring image registry repository mirroring

Setting up container registry repository mirroring enables you to do the following:

- Configure your OpenShift Container Platform cluster to redirect requests to pull images from a repository on a source image registry and have it resolved by a repository on a mirrored image registry.
- Identify multiple mirrored repositories for each target repository, to make sure that if one mirror is down, another can be used.

The attributes of repository mirroring in OpenShift Container Platform include:

- Image pulls are resilient to registry downtimes.
- Clusters in disconnected environments can pull images from critical locations, such as quay.io, and have registries behind a company firewall provide the requested images.
- A particular order of registries is tried when an image pull request is made, with the permanent registry typically being the last one tried.
- The mirror information you enter is added to the **/etc/containers/registries.conf** file on every node in the OpenShift Container Platform cluster.
- When a node makes a request for an image from the source repository, it tries each mirrored repository in turn until it finds the requested content. If all mirrors fail, the cluster tries the source repository. If successful, the image is pulled to the node.

Setting up repository mirroring can be done in the following ways:

- At OpenShift Container Platform installation:  
By pulling container images needed by OpenShift Container Platform and then bringing those images behind your company's firewall, you can install OpenShift Container Platform into a datacenter that is in a disconnected environment.
- After OpenShift Container Platform installation:  
Even if you don't configure mirroring during OpenShift Container Platform installation, you can do so later using the **ImageContentSourcePolicy** object.

The following procedure provides a post-installation mirror configuration, where you create an **ImageContentSourcePolicy** object that identifies:

- The source of the container image repository you want to mirror.
- A separate entry for each mirror repository you want to offer the content requested from the source repository.

**NOTE**

You can only configure global pull secrets for clusters that have an **ImageContentSourcePolicy** object. You cannot add a pull secret to a project.

## Prerequisites

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

## Procedure

1. Configure mirrored repositories, by either:
  - Setting up a mirrored repository with Red Hat Quay, as described in [Red Hat Quay Repository Mirroring](#). Using Red Hat Quay allows you to copy images from one repository to another and also automatically sync those repositories repeatedly over time.
  - Using a tool such as **skopeo** to copy images manually from the source directory to the mirrored repository.  
For example, after installing the skopeo RPM package on a Red Hat Enterprise Linux (RHEL) 7 or RHEL 8 system, use the **skopeo** command as shown in this example:

```
$ skopeo copy \
docker://registry.access.redhat.com/ubi8/ubi-
minimal@sha256:5cfbaf45ca96806917830c183e9f37df2e913b187adb32e89fd83fa455eba
a6 \
docker://example.io/example/ubi-minimal
```

In this example, you have a container image registry that is named **example.io** with an image repository named **example** to which you want to copy the **ubi8/ubi-minimal** image from **registry.access.redhat.com**. After you create the registry, you can configure your OpenShift Container Platform cluster to redirect requests made of the source repository to the mirrored repository.

2. Log in to your OpenShift Container Platform cluster.
3. Create an **ImageContentSourcePolicy** file (for example, **registryrepomirror.yaml**), replacing the source and mirrors with your own registry and repository pairs and images:

```
apiVersion: operator.openshift.io/v1alpha1
kind: ImageContentSourcePolicy
metadata:
  name: ubi8repo
spec:
  repositoryDigestMirrors:
  - mirrors:
    - example.io/example/ubi-minimal 1
    - example.com/example/ubi-minimal 2
    source: registry.access.redhat.com/ubi8/ubi-minimal 3
  - mirrors:
    - mirror.example.com/redhat
    source: registry.redhat.io/openshift4 4
  - mirrors:
    - mirror.example.com
    source: registry.redhat.io 5
  - mirrors:
    - mirror.example.net/image
    source: registry.example.com/example/myimage 6
  - mirrors:
    - mirror.example.net
```

```

source: registry.example.com/example 7
- mirrors:
- mirror.example.net/registry-example-com
source: registry.example.com 8

```

- 1** Indicates the name of the image registry and repository.
- 2** Indicates multiple mirror repositories for each target repository. If one mirror is down, the target repository can use another mirror.
- 3** Indicates the registry and repository containing the content that is mirrored.
- 4** You can configure a namespace inside a registry to use any image in that namespace. If you use a registry domain as a source, the **ImageContentSourcePolicy** resource is applied to all repositories from the registry.
- 5** If you configure the registry name, the **ImageContentSourcePolicy** resource is applied to all repositories from a source registry to a mirror registry.
- 6** Pulls the image **mirror.example.net/image@sha256:....**
- 7** Pulls the image **myimage** in the source registry namespace from the mirror **mirror.example.net/myimage@sha256:....**
- 8** Pulls the image **registry.example.com/example/myimage** from the mirror registry **mirror.example.net/registry-example-com/example/myimage@sha256:....**. The **ImageContentSourcePolicy** resource is applied to all repositories from a source registry to a mirror registry **mirror.example.net/registry-example-com**.

4. Create the new **ImageContentSourcePolicy** object:

```
$ oc create -f registryrepolmirror.yaml
```

After the **ImageContentSourcePolicy** object is created, the new settings are deployed to each node and the cluster starts using the mirrored repository for requests to the source repository.

5. To check that the mirrored configuration settings, are applied, do the following on one of the nodes.
  - a. List your nodes:

```
$ oc get node
```

#### Example output

NAME	STATUS	ROLES	AGE	VERSION
ip-10-0-137-44.ec2.internal	Ready	worker	7m	v1.24.0
ip-10-0-138-148.ec2.internal	Ready	master	11m	v1.24.0
ip-10-0-139-122.ec2.internal	Ready	master	11m	v1.24.0
ip-10-0-147-35.ec2.internal	Ready	worker	7m	v1.24.0
ip-10-0-153-12.ec2.internal	Ready	worker	7m	v1.24.0
ip-10-0-154-10.ec2.internal	Ready	master	11m	v1.24.0

The **Imagecontentsourcepolicy** resource does not restart the nodes.



- b. Start the debugging process to access the node:

```
$ oc debug node/ip-10-0-147-35.ec2.internal
```

### Example output

```
Starting pod/ip-10-0-147-35ec2internal-debug ...  
To use host binaries, run `chroot /host`
```

- c. Change your root directory to **/host**:

```
sh-4.2# chroot /host
```

- d. Check the **/etc/containers/registries.conf** file to make sure the changes were made:

```
sh-4.2# cat /etc/containers/registries.conf
```

### Example output

```
unqualified-search-registries = ["registry.access.redhat.com", "docker.io"]  
short-name-mode = ""
```

```
[[registry]]  
prefix = ""  
location = "registry.access.redhat.com/ubi8/ubi-minimal"  
mirror-by-digest-only = true
```

```
[[registry.mirror]]  
location = "example.io/example/ubi-minimal"
```

```
[[registry.mirror]]  
location = "example.com/example/ubi-minimal"
```

```
[[registry]]  
prefix = ""  
location = "registry.example.com"  
mirror-by-digest-only = true
```

```
[[registry.mirror]]  
location = "mirror.example.net/registry-example-com"
```

```
[[registry]]  
prefix = ""  
location = "registry.example.com/example"  
mirror-by-digest-only = true
```

```
[[registry.mirror]]  
location = "mirror.example.net"
```

```
[[registry]]  
prefix = ""  
location = "registry.example.com/example/myimage"  
mirror-by-digest-only = true
```

```
[[registry.mirror]]
  location = "mirror.example.net/image"
```

```
[[registry]]
  prefix = ""
  location = "registry.redhat.io"
  mirror-by-digest-only = true
```

```
[[registry.mirror]]
  location = "mirror.example.com"
```

```
[[registry]]
  prefix = ""
  location = "registry.redhat.io/openshift4"
  mirror-by-digest-only = true
```

```
[[registry.mirror]]
  location = "mirror.example.com/redhat"
```

- e. Pull an image digest to the node from the source and check if it is resolved by the mirror. **ImageContentSourcePolicy** objects support image digests only, not image tags.

```
sh-4.2# podman pull --log-level=debug registry.access.redhat.com/ubi8/ubi-
minimal@sha256:5cfbaf45ca96806917830c183e9f37df2e913b187adb32e89fd83fa455eba
a6
```

## Troubleshooting repository mirroring

If the repository mirroring procedure does not work as described, use the following information about how repository mirroring works to help troubleshoot the problem.

- The first working mirror is used to supply the pulled image.
- The main registry is only used if no other mirror works.
- From the system context, the **Insecure** flags are used as fallback.
- The format of the **/etc/containers/registries.conf** file has changed recently. It is now version 2 and in TOML format.

### 12.4.6. Widening the scope of the mirror image catalog to reduce the frequency of cluster node reboots

You can scope the mirrored image catalog at the repository level or the wider registry level. A widely scoped **ImageContentSourcePolicy** resource reduces the number of times the nodes need to reboot in response to changes to the resource.

To widen the scope of the mirror image catalog in the **ImageContentSourcePolicy** resource, perform the following procedure.

#### Prerequisites

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

- Configure a mirrored image catalog for use in your disconnected cluster.

## Procedure

1. Run the following command, specifying values for **<local\_registry>**, **<pull\_spec>**, and **<pull\_secret\_file>**:

```
$ oc adm catalog mirror <local_registry>/<pull_spec> <local_registry> -a <pull_secret_file> --
  icsp-scope=registry
```

where:

**<local\_registry>**

is the local registry you have configured for your disconnected cluster, for example, **local.registry:5000**.

**<pull\_spec>**

is the pull specification as configured in your disconnected registry, for example, **redhat/redhat-operator-index:v4.10**

**<pull\_secret\_file>**

is the **registry.redhat.io** pull secret in **.json** file format. You can download the [pull secret from the Red Hat OpenShift Cluster Manager](#).

The **oc adm catalog mirror** command creates a **/redhat-operator-index-manifests** directory and generates **imageContentSourcePolicy.yaml**, **catalogSource.yaml**, and **mapping.txt** files.

2. Apply the new **ImageContentSourcePolicy** resource to the cluster:

```
$ oc apply -f imageContentSourcePolicy.yaml
```

## Verification

- Verify that **oc apply** successfully applied the change to **ImageContentSourcePolicy**:

```
$ oc get ImageContentSourcePolicy -o yaml
```

### Example output

```
apiVersion: v1
items:
- apiVersion: operator.openshift.io/v1alpha1
  kind: ImageContentSourcePolicy
  metadata:
    annotations:
      kubectl.kubernetes.io/last-applied-configuration: |

      {"apiVersion":"operator.openshift.io/v1alpha1","kind":"ImageContentSourcePolicy","metadata":
      {"annotations":{"name":"redhat-operator-index"},"spec":{"repositoryDigestMirrors":
      [{"mirrors":["local.registry:5000"],"source":"registry.redhat.io"]}}}
  ...
```

After you update the **ImageContentSourcePolicy** resource, OpenShift Container Platform deploys the new settings to each node and the cluster starts using the mirrored repository for requests to the source repository.

### 12.4.7. Additional resources

- [Using Operator Lifecycle Manager on restricted networks](#)
- [Machine Config Overview](#)

## 12.5. UNINSTALLING THE OPENSIFT UPDATE SERVICE FROM A CLUSTER

To remove a local copy of the OpenShift Update Service (OSUS) from your cluster, you must first delete the OSUS application and then uninstall the OSUS Operator.

### 12.5.1. Deleting an OpenShift Update Service application

You can delete an OpenShift Update Service application by using the OpenShift Container Platform web console or CLI.

#### 12.5.1.1. Deleting an OpenShift Update Service application by using the web console

You can use the OpenShift Container Platform web console to delete an OpenShift Update Service application by using the OpenShift Update Service Operator.

#### Prerequisites

- The OpenShift Update Service Operator has been installed.

#### Procedure

1. In the web console, click **Operators** → **Installed Operators**.
2. Choose **OpenShift Update Service** from the list of installed Operators.
3. Click the **Update Service** tab.
4. From the list of installed OpenShift Update Service applications, select the application to be deleted and then click **Delete UpdateService**.
5. From the **Delete UpdateService?** confirmation dialog, click **Delete** to confirm the deletion.

#### 12.5.1.2. Deleting an OpenShift Update Service application by using the CLI

You can use the OpenShift CLI (**oc**) to delete an OpenShift Update Service application.

#### Procedure

1. Get the OpenShift Update Service application name using the namespace the OpenShift Update Service application was created in, for example, **openshift-update-service**:

```
$ oc get updateservice -n openshift-update-service
```

### Example output

```
NAME    AGE
service 6s
```

2. Delete the OpenShift Update Service application using the **NAME** value from the previous step and the namespace the OpenShift Update Service application was created in, for example, **openshift-update-service**:

```
$ oc delete updateservice service -n openshift-update-service
```

### Example output

```
updateservice.updateservice.operator.openshift.io "service" deleted
```

## 12.5.2. Uninstalling the OpenShift Update Service Operator

You can uninstall the OpenShift Update Service Operator by using the OpenShift Container Platform web console or CLI.

### 12.5.2.1. Uninstalling the OpenShift Update Service Operator by using the web console

You can use the OpenShift Container Platform web console to uninstall the OpenShift Update Service Operator.

#### Prerequisites

- All OpenShift Update Service applications have been deleted.

#### Procedure

1. In the web console, click **Operators** → **Installed Operators**.
2. Select **OpenShift Update Service** from the list of installed Operators and click **Uninstall Operator**.
3. From the **Uninstall Operator?** confirmation dialog, click **Uninstall** to confirm the uninstallation.

### 12.5.2.2. Uninstalling the OpenShift Update Service Operator by using the CLI

You can use the OpenShift CLI (**oc**) to uninstall the OpenShift Update Service Operator.

#### Prerequisites

- All OpenShift Update Service applications have been deleted.

#### Procedure

1. Change to the project containing the OpenShift Update Service Operator, for example, **openshift-update-service**:

```
$ oc project openshift-update-service
```

**Example output**

```
Now using project "openshift-update-service" on server "https://example.com:6443".
```

- Get the name of the OpenShift Update Service Operator operator group:

```
$ oc get operatorgroup
```

**Example output**

```
NAME                                AGE
openshift-update-service-fprx2     4m41s
```

- Delete the operator group, for example, **openshift-update-service-fprx2**:

```
$ oc delete operatorgroup openshift-update-service-fprx2
```

**Example output**

```
operatorgroup.operators.coreos.com "openshift-update-service-fprx2" deleted
```

- Get the name of the OpenShift Update Service Operator subscription:

```
$ oc get subscription
```

**Example output**

```
NAME                PACKAGE                SOURCE                CHANNEL
update-service-operator  update-service-operator  updateservice-index-catalog  v1
```

- Using the **Name** value from the previous step, check the current version of the subscribed OpenShift Update Service Operator in the **currentCSV** field:

```
$ oc get subscription update-service-operator -o yaml | grep "currentCSV"
```

**Example output**

```
currentCSV: update-service-operator.v0.0.1
```

- Delete the subscription, for example, **update-service-operator**:

```
$ oc delete subscription update-service-operator
```

**Example output**

```
subscription.operators.coreos.com "update-service-operator" deleted
```

- Delete the CSV for the OpenShift Update Service Operator using the **currentCSV** value from the previous step:

```
┆ $ oc delete clusterserviceversion update-service-operator.v0.0.1
```

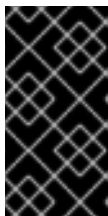
### Example output

```
┆ clusterserviceversion.operators.coreos.com "update-service-operator.v0.0.1" deleted
```

## CHAPTER 13. UPDATING HARDWARE ON NODES RUNNING ON VSPHERE

You must ensure that your nodes running in vSphere are running on the hardware version supported by OpenShift Container Platform. Currently, hardware version 13 or later is supported for vSphere virtual machines in a cluster.

You can update your virtual hardware immediately or schedule an update in vCenter.



### IMPORTANT

Using hardware version 13 for your cluster nodes running on vSphere is now deprecated. This version is still fully supported, but support will be removed in a future version of OpenShift Container Platform. Hardware version 15 is now the default for vSphere virtual machines in OpenShift Container Platform.

### 13.1. UPDATING VIRTUAL HARDWARE ON VSPHERE

To update the hardware of your virtual machines (VMs) on VMware vSphere, update your virtual machines separately to reduce the risk of downtime for your cluster.

#### 13.1.1. Updating the virtual hardware for control plane nodes on vSphere

To reduce the risk of downtime, it is recommended that control plane nodes be upgraded serially. This ensures that the Kubernetes API remains available and etcd retains quorum.

#### Prerequisites

- You have cluster administrator permissions to execute the required permissions in the vCenter instance hosting your OpenShift Container Platform cluster.
- Your vSphere ESXi hosts are version 6.7U3 or later.

#### Procedure

1. List the control plane nodes in your cluster.

```
$ oc get nodes -l node-role.kubernetes.io/master
```

#### Example output

```
NAME                STATUS  ROLES  AGE  VERSION
control-plane-node-0 Ready   master 75m  v1.23.0
control-plane-node-1 Ready   master 75m  v1.23.0
control-plane-node-2 Ready   master 75m  v1.23.0
```

Note the names of your control plane nodes.

2. Mark the control plane node as unschedulable.

```
$ oc adm cordon <control_plane_node>
```



3. Shut down the virtual machine (VM) associated with the control plane node. Do this in the vSphere client by right-clicking the VM and selecting **Power** → **Shut Down Guest OS**. Do not shut down the VM using **Power Off** because it might not shut down safely.
4. Upgrade the VM in the vSphere client. Follow [Upgrading a virtual machine to the latest hardware version](#) in the VMware documentation for more information.
5. Power on the VM associated with the control plane node. Do this in the vSphere client by right-clicking the VM and selecting **Power On**.
6. Wait for the node to report as **Ready**:

```
$ oc wait --for=condition=Ready node/<control_plane_node>
```

7. Mark the control plane node as schedulable again:

```
$ oc adm uncordon <control_plane_node>
```

8. Repeat this procedure for each control plane node in your cluster.

### 13.1.2. Updating the virtual hardware for compute nodes on vSphere

To reduce the risk of downtime, it is recommended that compute nodes be upgraded serially.



#### NOTE

Multiple compute nodes can be upgraded in parallel given workloads are tolerant of having multiple nodes in a **NotReady** state. It is the responsibility of the administrator to ensure that the required compute nodes are available.

#### Prerequisites

- You have cluster administrator permissions to execute the required permissions in the vCenter instance hosting your OpenShift Container Platform cluster.
- Your vSphere ESXi hosts are version 6.7U3 or later.

#### Procedure

1. List the compute nodes in your cluster.

```
$ oc get nodes -l node-role.kubernetes.io/worker
```

#### Example output

```
NAME           STATUS  ROLES  AGE  VERSION
compute-node-0 Ready   worker 30m  v1.23.0
compute-node-1 Ready   worker 30m  v1.23.0
compute-node-2 Ready   worker 30m  v1.23.0
```

Note the names of your compute nodes.

2. Mark the compute node as unschedulable:

■

```
$ oc adm cordon <compute_node>
```

3. Evacuate the pods from the compute node. There are several ways to do this. For example, you can evacuate all or selected pods on a node:

```
$ oc adm drain <compute_node> [--pod-selector=<pod_selector>]
```

See the "Understanding how to evacuate pods on nodes" section for other options to evacuate pods from a node.

4. Shut down the virtual machine (VM) associated with the compute node. Do this in the vSphere client by right-clicking the VM and selecting **Power** → **Shut Down Guest OS**. Do not shut down the VM using **Power Off** because it might not shut down safely.
5. Upgrade the VM in the vSphere client. Follow [Upgrading a virtual machine to the latest hardware version](#) in the VMware documentation for more information.
6. Power on the VM associated with the compute node. Do this in the vSphere client by right-clicking the VM and selecting **Power On**.
7. Wait for the node to report as **Ready**:

```
$ oc wait --for=condition=Ready node/<compute_node>
```

8. Mark the compute node as schedulable again:

```
$ oc adm uncordon <compute_node>
```

9. Repeat this procedure for each compute node in your cluster.

### 13.1.3. Updating the virtual hardware for template on vSphere

#### Prerequisites

- You have cluster administrator permissions to execute the required permissions in the vCenter instance hosting your OpenShift Container Platform cluster.
- Your vSphere ESXi hosts are version 6.7U3 or later.

#### Procedure

1. If the RHCOS template is configured as a vSphere template follow [Convert a Template to a Virtual Machine](#) in the VMware documentation prior to the next step.



#### NOTE

Once converted from a template, do not power on the virtual machine.

2. Update the VM in the vSphere client. Follow [Upgrading a virtual machine to the latest hardware version](#) in the VMware documentation for more information.
3. Convert the VM in the vSphere client from a VM to template. Follow [Convert a Virtual Machine to a Template in the vSphere Client](#) in the VMware documentation for more information.

### Additional resources

- [Understanding how to evacuate pods on nodes](#)

## 13.2. SCHEDULING AN UPDATE FOR VIRTUAL HARDWARE ON VSPHERE

Virtual hardware updates can be scheduled to occur when a virtual machine is powered on or rebooted. You can schedule your virtual hardware updates exclusively in vCenter by following [Schedule a Compatibility Upgrade for a Virtual Machine](#) in the VMware documentation.

When scheduling an upgrade prior to performing an upgrade of OpenShift Container Platform, the virtual hardware update occurs when the nodes are rebooted during the course of the OpenShift Container Platform upgrade.