OpenShift Container Platform 4.3

Updating clusters

Updating OpenShift Container Platform clusters

Last Updated: 2020-04-07

OpenShift Container Platform 4.3 Updating clusters

Updating OpenShift Container Platform clusters

Legal Notice

Abstract

This document provides instructions for updating, or upgrading, OpenShift Container Platform clusters. In version , updating your cluster is a simple process that does not require you to take your cluster offline.

Table of Contents

CHAPTER 1. UPDATING A CLUSTER BETWEEN MINOR VERSIONS

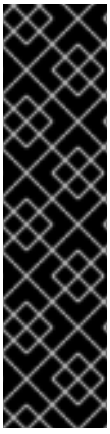
You can update, or upgrade, an OpenShift Container Platform cluster between minor versions.

NOTE

Because of the difficulty of changing update channels by using **oc**, use the web console to change the update channel. It is recommended to complete the update process within the web console. You can follow the steps in Updating a cluster within a minor version by using the CLI to complete the update after you change to a 4.3 channel.

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 upgrade fails and you must restore your cluster to a previous state.



IMPORTANT

If you are upgrading to this release from OpenShift Container Platform 4.2, you must restart all Pods after the upgrade is complete.

This is because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

1.1. ABOUT THE OPENSHIFT CONTAINER PLATFORM UPDATE SERVICE

The OpenShift Container Platform update service is the hosted service that provides over-the-air updates to both OpenShift Container Platform and Red Hat Enterprise Linux CoreOS (RHCOS). It provides a graph, or diagram that contain *vertices* and the *edges* that connect them, of component Operators. The edges in the graph show which versions you can safely update to, and the vertices are update payloads that specify the intended state of the managed cluster components.

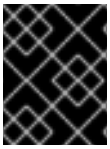
The Cluster Version Operator (CVO) in your cluster checks with the OpenShift Container Platform update service to see the valid updates and update paths based on current component versions and information in the graph. When you request an update, the OpenShift Container Platform CVO uses the release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

To allow the OpenShift Container Platform update service to provide only compatible updates, a release verification pipeline exists to drive 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 Container Platform update service notifies you that it is available.

IMPORTANT

Because the update service displays all valid updates, you must not force an update to a version that the update service does not display.

During continuous update mode, two controllers run. One continuously updates the payload manifests, applies them to the cluster, and outputs the status of the controlled rollout of the Operators, whether they are available, upgrading, or failed. The second controller polls the OpenShift Container Platform update service to determine if updates are available.



IMPORTANT

Reverting your cluster to a previous version, or a rollback, is not supported. Only upgrading to a newer version is supported.

During the upgrade process, the Machine Config Operator (MCO) applies the new configuration to your cluster machines. It cordons the number of nodes that is specified by the **maxUnavailable** field on the machine configuration pool and marks them as unavailable. By default, this value is set to **1**. It 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 on these machines because you must update the OpenShift API on them first. Because the specification for the new version is 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 nodes that are unavailable is set to ensure that normal cluster operations are likely to continue with that number of machines out of service.

1.2. OPENSHIFT CONTAINER PLATFORM UPGRADE CHANNELS AND RELEASES

In OpenShift Container Platform 4.1, Red Hat introduced the concept of channels for recommending the appropriate release versions for cluster upgrade. By controlling the pace of upgrades, these upgrade channels allow you to choose an upgrade strategy. Upgrade channels are tied to a minor version of OpenShift Container Platform. For instance, OpenShift Container Platform 4.3 upgrade channels will never include an upgrade to a 4.4 release. This strategy ensures that administrators explicitly decide to upgrade to the next minor version of OpenShift Container Platform. Upgrade 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 4.3 offers the following upgrade channels:

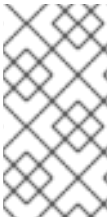
- **candidate-4.3**
- **fast-4.3**
- **stable-4.3**

candidate-4.3 channel

The **candidate-4.3** channel contains candidate builds for a z-stream (4.3.z) release. Release candidates contain all the features of the product but are not supported. Use release candidate versions to test feature acceptance and assist in qualifying the next version of OpenShift Container Platform. A release candidate is any build that is available in the candidate channel, including ones that do not contain **-rc** in their names. After a version is available in the candidate channel, it goes through more quality checks. If it meets the quality standard, it is promoted to the **fast-4.3** or **stable-4.3** channels. Because of this

strategy, if a specific release is available in both the **candidate-4.3** channel and in the **fast-4.3** or **stable-4.3** channels, it is a Red Hat supported version. The **candidate-4.3** channel can include release versions from which there are no recommended updates in any channel.

You can use the **candidate-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.



NOTE

Release candidates differ from the nightly builds found on the https://www.openshift.com/try site. Nightly builds are available for early access to features, but updating to or from nightly builds is neither recommended nor supported. Nightly builds are not available in any upgrade channel.

fast-4.3 channel

The **fast-4.3** channel is updated with new 4.3 versions as soon as Red Hat declares the given version as a general availability release. As such, these releases are fully supported, are production quality, and have performed well while available as a release candidate in the **candidate-4.3** channel from where they were promoted. Some time after a release appears in the **fast-4.3** channel, it is added to the **stable-4.3** channel. Releases never appear in the **stable-4.3** channel before they appear in the **fast-4.3** channel.

You can use the **fast-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.

stable-4.3 channel

While the **fast-4.3** channel contains releases as soon as their errata are published, releases are added to the **stable-4.3** channel after a delay of several hours to a day. During this delay, data is collected from Red Hat SRE teams, Red Hat support services, and pre-production and production environments that participate in connected customer program about the stability of the release.

You can use the **stable-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.

Upgrade version paths

OpenShift Container Platform maintains an upgrade recommendation service that understands the version of OpenShift Container Platform you have installed as well as the path to take within the channel you choose to get you to the next release. You can imagine seeing the following in the **fast-4.3** channel:

- 4.3.0
- 4.3.1
- 4.3.3
- 4.3.4

The service recommends only upgrades that have been tested and have no serious issues. If your cluster is on 4.3.1 and OpenShift Container Platform suggests 4.3.4, then it is safe for you to update from .4.3.1 to .4.3.4. Do not rely on consecutive patch numbers. In this example, 4.3.2 is not, and never was, available in the channel. The update service will not suggest updating to a version of OpenShift Container Platform that contains known vulnerabilities.

Update stability depends on your channel. The presence of an update recommendation in the **candidate-4.3** channel does not imply that the update is supported. It means that no serious issues have been found with the update yet, but there might not be significant traffic through the update to suggest stability. The presence of an update recommendation in the **fast-4.3** or **stable-4.3** channels is a

declaration that the update is fully supported while it is in the channel. While releases will never be removed from a channel, update recommendations that exhibit serious issues will be removed from all channels. Updates initiated after the update recommendation has been removed might not be supported.

Red Hat will eventually provide supported update paths from any supported release in the **fast-4.3** or **stable-4.3** channels to the latest release in 4.3.z, although there can be delays while safe paths away from troubled releases are constructed and verified.

Fast and stable channel use and strategies

The **fast-4.3** and **stable-4.3** channels present a choice between receiving general availability releases as soon as they are available or allowing Red Hat to control the rollout of those updates. If issues are detected during rollout or at a later time, upgrades to that version might be blocked in both the **fast-4.3** and **stable-4.3** channels, and a new version might be introduced that becomes the new preferred upgrade target.

Customers can improve this process by configuring pre-production systems on the **fast-4.3** channel, configuring production systems on the **stable-4.3** channel, and participating in Red Hat's connected customer program. Red Hat uses this program to observe the impact of updates on your specific hardware and software configurations. Future releases might improve or alter the pace at which updates move from the **fast-4.3** to the **stable-4.3** channel.

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 upgrades. During upgrade, 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.

Switching between channels

Your cluster is still supported if you change from the **stable-4.3** channel to the **fast-4.3** channel. Although you can switch to the **candidate-4.3** channel at any time, some releases in that channel might be unsupported release candidates. You can switch from the **candidate-4.3** channel to the **fast-4.3** channel if your current release is a general availability release. You can always switch from the **fast-4.3** channel to the **stable-4.3** channel, although if the current release was recently promoted to **fast-{product-stable}** there can be a delay of up to a day for the release to be promoted to **stable-4.3**. If you change to a channel that does not include your current release, an alert displays and no updates can be recommended, but you can safely change back to your original channel at any point.

1.3. 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.

Procedure

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

2. For production clusters, ensure that the **CHANNEL** is set to the correct channel for your current minor version, such as **stable-4.3**.

IMPORTANT

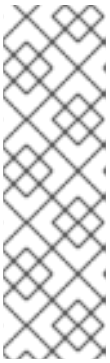
For production clusters, you must subscribe to a stable-* or fast-* channel.

- If the **UPDATE STATUS** is not **Updates Available**, you cannot upgrade your cluster.
- The **DESIRED VERSION** indicates the cluster version that your cluster is running or is updating to.

3. Click **Updates Available**, select the highest available version and click **Update**. The **UPDATE STATUS** changes to **Updating**, and you can review the progress of the Operator upgrades on the **Cluster Operators** tab.

4. If you are upgrading to this release from OpenShift Container Platform 4.2, you must restart all Pods after the upgrade is complete. You can do this using the following command, which requires the OpenShift CLI (**oc**):

```
$ for I in $(oc get ns -o jsonpath='{range .items[*]} {.metadata.name}{"\n"} {end}'); \
    do oc delete pods --all -n $I; \
    sleep 1; \
    done
```



NOTE

Restarting all Pods is required because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

5. 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-* or fast-* channel for the next minor version, and update to the version that you want in that channel.

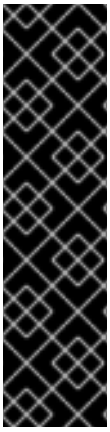
You might need to perform several intermediate updates until you reach the version that you want.

CHAPTER 2. UPDATING A CLUSTER WITHIN A MINOR VERSION FROM THE WEB CONSOLE

You can update, or upgrade, an OpenShift Container Platform cluster by using the web console.

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 upgrade fails and you must restore your cluster to a previous state.



IMPORTANT

If you are upgrading to this release from OpenShift Container Platform 4.3.3 or earlier, you must restart all Pods after the upgrade is complete.

This is because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

2.1. ABOUT THE OPENSHIFT CONTAINER PLATFORM UPDATE SERVICE

The OpenShift Container Platform update service is the hosted service that provides over-the-air updates to both OpenShift Container Platform and Red Hat Enterprise Linux CoreOS (RHCOS). It provides a graph, or diagram that contain *vertices* and the *edges* that connect them, of component Operators. The edges in the graph show which versions you can safely update to, and 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 Container Platform 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 OpenShift Container Platform CVO uses the release image for that update to upgrade your cluster. The release artifacts are hosted in Quay as container images.

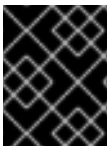
To allow the OpenShift Container Platform update service to provide only compatible updates, a release verification pipeline exists to drive automation. Each release artifact is verified for compatibility with supported cloud platforms and system architectures as well as other component packages. After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

IMPORTANT

Because the update service displays all valid updates, you must not force an update to a version that the update service does not display.

During continuous update mode, two controllers run. One continuously updates the payload manifests,

applies them to the cluster, and outputs the status of the controlled rollout of the Operators, whether they are available, upgrading, or failed. The second controller polls the OpenShift Container Platform update service to determine if updates are available.



IMPORTANT

Reverting your cluster to a previous version, or a rollback, is not supported. Only upgrading to a newer version is supported.

During the upgrade process, the Machine Config Operator (MCO) applies the new configuration to your cluster machines. It cordons the number of nodes that is specified by the **maxUnavailable** field on the machine configuration pool and marks them as unavailable. By default, this value is set to **1**. It 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 on these machines because you must update the OpenShift API on them first. Because the specification for the new version is 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 nodes that are unavailable is set to ensure that normal cluster operations are likely to continue with that number of machines out of service.

2.2. OPENSHIFT CONTAINER PLATFORM UPGRADE CHANNELS AND RELEASES

In OpenShift Container Platform 4.1, Red Hat introduced the concept of channels for recommending the appropriate release versions for cluster upgrade. By controlling the pace of upgrades, these upgrade channels allow you to choose an upgrade strategy. Upgrade channels are tied to a minor version of OpenShift Container Platform. For instance, OpenShift Container Platform 4.3 upgrade channels will never include an upgrade to a 4.4 release. This strategy ensures that administrators explicitly decide to upgrade to the next minor version of OpenShift Container Platform. Upgrade 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.

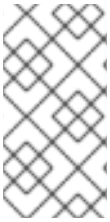
OpenShift Container Platform 4.3 offers the following upgrade channels:

- **candidate-4.3**
- **fast-4.3**
- **stable-4.3**

candidate-4.3 channel

The **candidate-4.3** channel contains candidate builds for a z-stream (4.3.z) release. Release candidates contain all the features of the product but are not supported. Use release candidate versions to test feature acceptance and assist in qualifying the next version of OpenShift Container Platform. A release candidate is any build that is available in the candidate channel, including ones that do not contain **-rc** in their names. After a version is available in the candidate channel, it goes through more quality checks. If it meets the quality standard, it is promoted to the **fast-4.3** or **stable-4.3** channels. Because of this strategy, if a specific release is available in both the **candidate-4.3** channel and in the **fast-4.3** or **stable-4.3** channels, it is a Red Hat supported version. The **candidate-4.3** channel can include release versions from which there are no recommended updates in any channel.

You can use the **candidate-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.



NOTE

Release candidates differ from the nightly builds found on the https://www.openshift.com/try site. Nightly builds are available for early access to features, but updating to or from nightly builds is neither recommended nor supported. Nightly builds are not available in any upgrade channel.

fast-4.3 channel

The **fast-4.3** channel is updated with new 4.3 versions as soon as Red Hat declares the given version as a general availability release. As such, these releases are fully supported, are production quality, and have performed well while available as a release candidate in the **candidate-4.3** channel from where they were promoted. Some time after a release appears in the **fast-4.3** channel, it is added to the **stable-4.3** channel. Releases never appear in the **stable-4.3** channel before they appear in the **fast-4.3** channel.

You can use the **fast-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.

stable-4.3 channel

While the **fast-4.3** channel contains releases as soon as their errata are published, releases are added to the **stable-4.3** channel after a delay of several hours to a day. During this delay, data is collected from Red Hat SRE teams, Red Hat support services, and pre-production and production environments that participate in connected customer program about the stability of the release.

You can use the **stable-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.

Upgrade version paths

OpenShift Container Platform maintains an upgrade recommendation service that understands the version of OpenShift Container Platform you have installed as well as the path to take within the channel you choose to get you to the next release. You can imagine seeing the following in the **fast-4.3** channel:

- 4.3.0
- 4.3.1
- 4.3.3
- 4.3.4

The service recommends only upgrades that have been tested and have no serious issues. If your cluster is on 4.3.1 and OpenShift Container Platform suggests 4.3.4, then it is safe for you to update from .4.3.1 to .4.3.4. Do not rely on consecutive patch numbers. In this example, 4.3.2 is not, and never was, available in the channel. The update service will not suggest updating to a version of OpenShift Container Platform that contains known vulnerabilities.

Update stability depends on your channel. The presence of an update recommendation in the **candidate-4.3** channel does not imply that the update is supported. It means that no serious issues have been found with the update yet, but there might not be significant traffic through the update to suggest stability. The presence of an update recommendation in the **fast-4.3** or **stable-4.3** channels is a declaration that the update is fully supported while it is in the channel. While releases will never be removed from a channel, update recommendations that exhibit serious issues will be removed from all channels. Updates initiated after the update recommendation has been removed might not be supported.

Red Hat will eventually provide supported update paths from any supported release in the **fast-4.3** or **stable-4.3** channels to the latest release in 4.3.z, although there can be delays while safe paths away from troubled releases are constructed and verified.

Fast and stable channel use and strategies

The **fast-4.3** and **stable-4.3** channels present a choice between receiving general availability releases as soon as they are available or allowing Red Hat to control the rollout of those updates. If issues are detected during rollout or at a later time, upgrades to that version might be blocked in both the **fast-4.3** and **stable-4.3** channels, and a new version might be introduced that becomes the new preferred upgrade target.

Customers can improve this process by configuring pre-production systems on the **fast-4.3** channel, configuring production systems on the **stable-4.3** channel, and participating in Red Hat's connected customer program. Red Hat uses this program to observe the impact of updates on your specific hardware and software configurations. Future releases might improve or alter the pace at which updates move from the **fast-4.3** to the **stable-4.3** channel.

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 upgrades. During upgrade, 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.

Switching between channels

Your cluster is still supported if you change from the **stable-4.3** channel to the **fast-4.3** channel. Although you can switch to the **candidate-4.3** channel at any time, some releases in that channel might be unsupported release candidates. You can switch from the **candidate-4.3** channel to the **fast-4.3** channel if your current release is a general availability release. You can always switch from the **fast-4.3** channel to the **stable-4.3** channel, although if the current release was recently promoted to **fast-{product-stable}** there can be a delay of up to a day for the release to be promoted to **stable-4.3**. If you change to a channel that does not include your current release, an alert displays and no updates can be recommended, but you can safely change back to your original channel at any point.

2.3. 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.

Procedure

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

2. For production clusters, ensure that the **CHANNEL** is set to the correct channel for the version that you want to update to, your current minor version, such as **stable-4.3**.

IMPORTANT

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

- If the **UPDATE STATUS** is not **Updates Available**, you cannot upgrade your cluster.
- The **DESIRED VERSION** indicates the cluster version that your cluster is running or is updating to.

3. Click **Updates Available**, select a version to update to, the highest available version and click **Update**. The **UPDATE STATUS** changes to **Updating**, and you can review the progress of the Operator upgrades on the **Cluster Operators** tab.

4. If you are upgrading to this release from OpenShift Container Platform 4.3.3 or earlier, 4.2, you must restart all Pods after the upgrade is complete. You can do this using the following command, which requires the OpenShift CLI (**oc**):

```
$ for I in $(oc get ns -o jsonpath='{range .items[*]} {.metadata.name}{"\n"} {end}'); \
    do oc delete pods --all -n $I; \
    sleep 1; \
    done
```

NOTE

Restarting all Pods is required because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

5. 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-* or fast-* channel for the next minor version, and update to the version that you want in that channel.

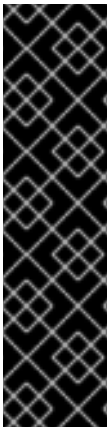
   You might need to perform several intermediate updates until you reach the version that you want.

CHAPTER 3. UPDATING A CLUSTER WITHIN A MINOR VERSION BY USING THE CLI

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

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 upgrade fails and you must restore your cluster to a previous state.



IMPORTANT

If you are upgrading to this release from OpenShift Container Platform 4.3.3 or earlier, you must restart all Pods after the upgrade is complete.

This is because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

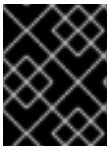
After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

3.1. ABOUT THE OPENSHIFT CONTAINER PLATFORM UPDATE SERVICE

The OpenShift Container Platform update service is the hosted service that provides over-the-air updates to both OpenShift Container Platform and Red Hat Enterprise Linux CoreOS (RHCOS). It provides a graph, or diagram that contain *vertices* and the *edges* that connect them, of component Operators. The edges in the graph show which versions you can safely update to, and 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 Container Platform 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 OpenShift Container Platform CVO uses the release image for that update to upgrade your cluster. The release artifacts are hosted in Quay as container images.

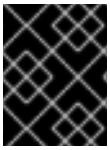
To allow the OpenShift Container Platform update service to provide only compatible updates, a release verification pipeline exists to drive automation. Each release artifact is verified for compatibility with supported cloud platforms and system architectures as well as other component packages. After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



IMPORTANT

Because the update service displays all valid updates, you must not force an update to a version that the update service does not display.

During continuous update mode, two controllers run. One continuously updates the payload manifests, applies them to the cluster, and outputs the status of the controlled rollout of the Operators, whether they are available, upgrading, or failed. The second controller polls the OpenShift Container Platform update service to determine if updates are available.



IMPORTANT

Reverting your cluster to a previous version, or a rollback, is not supported. Only upgrading to a newer version is supported.

During the upgrade process, the Machine Config Operator (MCO) applies the new configuration to your cluster machines. It cordons the number of nodes that is specified by the **maxUnavailable** field on the machine configuration pool and marks them as unavailable. By default, this value is set to **1**. It 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 on these machines because you must update the OpenShift API on them first. Because the specification for the new version is 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 nodes that are unavailable is set to ensure that normal cluster operations are likely to continue with that number of machines out of service.

3.2. OPENSHIFT CONTAINER PLATFORM UPGRADE CHANNELS AND RELEASES

In OpenShift Container Platform 4.1, Red Hat introduced the concept of channels for recommending the appropriate release versions for cluster upgrade. By controlling the pace of upgrades, these upgrade channels allow you to choose an upgrade strategy. Upgrade channels are tied to a minor version of OpenShift Container Platform. For instance, OpenShift Container Platform 4.3 upgrade channels will never include an upgrade to a 4.4 release. This strategy ensures that administrators explicitly decide to upgrade to the next minor version of OpenShift Container Platform. Upgrade 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 4.3 offers the following upgrade channels:

- **candidate-4.3**
- **fast-4.3**
- **stable-4.3**

candidate-4.3 channel

The **candidate-4.3** channel contains candidate builds for a z-stream (4.3.z) release. Release candidates contain all the features of the product but are not supported. Use release candidate versions to test feature acceptance and assist in qualifying the next version of OpenShift Container Platform. A release candidate is any build that is available in the candidate channel, including ones that do not contain **-rc** in their names. After a version is available in the candidate channel, it goes through more quality checks. If it meets the quality standard, it is promoted to the **fast-4.3** or **stable-4.3** channels. Because of this strategy, if a specific release is available in both the **candidate-4.3** channel and in the **fast-4.3** or **stable-4.3** channels, it is a Red Hat supported version. The **candidate-4.3** channel can include release versions from which there are no recommended updates in any channel.

You can use the **candidate-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.

NOTE

Release candidates differ from the nightly builds found on the https://www.openshift.com/try site. Nightly builds are available for early access to features, but updating to or from nightly builds is neither recommended nor supported. Nightly builds are not available in any upgrade channel.

fast-4.3 channel

The **fast-4.3** channel is updated with new 4.3 versions as soon as Red Hat declares the given version as a general availability release. As such, these releases are fully supported, are production quality, and have performed well while available as a release candidate in the **candidate-4.3** channel from where they were promoted. Some time after a release appears in the **fast-4.3** channel, it is added to the **stable-4.3** channel. Releases never appear in the **stable-4.3** channel before they appear in the **fast-4.3** channel.

You can use the **fast-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.

stable-4.3 channel

While the **fast-4.3** channel contains releases as soon as their errata are published, releases are added to the **stable-4.3** channel after a delay of several hours to a day. During this delay, data is collected from Red Hat SRE teams, Red Hat support services, and pre-production and production environments that participate in connected customer program about the stability of the release.

You can use the **stable-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.

Upgrade version paths

OpenShift Container Platform maintains an upgrade recommendation service that understands the version of OpenShift Container Platform you have installed as well as the path to take within the channel you choose to get you to the next release. You can imagine seeing the following in the **fast-4.3** channel:

- 4.3.0
- 4.3.1
- 4.3.3
- 4.3.4

The service recommends only upgrades that have been tested and have no serious issues. If your cluster is on 4.3.1 and OpenShift Container Platform suggests 4.3.4, then it is safe for you to update from .4.3.1 to .4.3.4. Do not rely on consecutive patch numbers. In this example, 4.3.2 is not, and never was, available in the channel. The update service will not suggest updating to a version of OpenShift Container Platform that contains known vulnerabilities.

Update stability depends on your channel. The presence of an update recommendation in the **candidate-4.3** channel does not imply that the update is supported. It means that no serious issues have been found with the update yet, but there might not be significant traffic through the update to suggest stability. The presence of an update recommendation in the **fast-4.3** or **stable-4.3** channels is a declaration that the update is fully supported while it is in the channel. While releases will never be removed from a channel, update recommendations that exhibit serious issues will be removed from all channels. Updates initiated after the update recommendation has been removed might not be supported.

Red Hat will eventually provide supported update paths from any supported release in the **fast-4.3** or **stable-4.3** channels to the latest release in 4.3.z, although there can be delays while safe paths away from troubled releases are constructed and verified.

Fast and stable channel use and strategies

The **fast-4.3** and **stable-4.3** channels present a choice between receiving general availability releases as soon as they are available or allowing Red Hat to control the rollout of those updates. If issues are detected during rollout or at a later time, upgrades to that version might be blocked in both the **fast-4.3** and **stable-4.3** channels, and a new version might be introduced that becomes the new preferred upgrade target.

Customers can improve this process by configuring pre-production systems on the **fast-4.3** channel, configuring production systems on the **stable-4.3** channel, and participating in Red Hat's connected customer program. Red Hat uses this program to observe the impact of updates on your specific hardware and software configurations. Future releases might improve or alter the pace at which updates move from the **fast-4.3** to the **stable-4.3** channel.

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 upgrades. During upgrade, 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.

Switching between channels

Your cluster is still supported if you change from the **stable-4.3** channel to the **fast-4.3** channel. Although you can switch to the **candidate-4.3** channel at any time, some releases in that channel might be unsupported release candidates. You can switch from the **candidate-4.3** channel to the **fast-4.3** channel if your current release is a general availability release. You can always switch from the **fast-4.3** channel to the **stable-4.3** channel, although if the current release was recently promoted to **fast-{product-stable}** there can be a delay of up to a day for the release to be promoted to **stable-4.3**. If you change to a channel that does not include your current release, an alert displays and no updates can be recommended, but you can safely change back to your original channel at any point.

3.3. 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 version of the OpenShift Command-line Interface (CLI), commonly known as **oc**, that matches the version for your updated version.
- Log in to the cluster as user with **cluster-admin** privileges.
- Install the **jq** package.

Procedure

1. Ensure that your cluster is available:

```
$ oc get clusterversion
```

```
NAME      VERSION   AVAILABLE   PROGRESSING   SINCE   STATUS
version   4.3.0     True        False         158m    Cluster version is 4.3.0
```

2. Review the current update channel information and confirm that your channel is set to **stable-4.3**:

```
$ oc get clusterversion -o json|jq ".items[0].spec"

{
  "channel": "stable-4.3",
  "clusterID": "990f7ab8-109b-4c95-8480-2bd1deec55ff",
  "upstream": "https://api.openshift.com/api/upgrades_info/v1/graph"
}
```

IMPORTANT

For production clusters, you must subscribe to a **stable-*** channel.

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

```
$ oc adm upgrade

Cluster version is 4.1.0

Updates:

VERSION IMAGE
4.1.2   quay.io/openshift-release-dev/ocp-release@sha256:9c5f0df8b192a0d7b46cd5f6a4da2289c155fd5302dec7954f8f06c878160b8b
```

4. 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) **<version>** is the update version that you obtained from the output of the previous command.

5. Review the status of the Cluster Version Operator:

```
$ oc get clusterversion -o json|jq ".items[0].spec"

{
  "channel": "stable-4.3",
  "clusterID": "990f7ab8-109b-4c95-8480-2bd1deec55ff",
  "desiredUpdate": {
    "force": false,
```

```
    "image": "quay.io/openshift-release-dev/ocp-
release@sha256:9c5f0df8b192a0d7b46cd5f6a4da2289c155fd5302dec7954f8f06c878160b8b",

    "version": "4.3.1" (1)
  },
  "upstream": "https://api.openshift.com/api/upgrades_info/v1/graph"
}
```

(1) If the **version** number in the **desiredUpdate** stanza matches the value that you specified, the update is in progress.

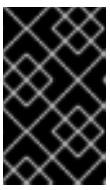
6. Review the cluster version status history to monitor the status of the update. It might take some time for all the objects to finish updating.

```
$ oc get clusterversion -o json|jq ".items[0].status.history"

[
  {
    "completionTime": null,
    "image": "quay.io/openshift-release-dev/ocp-
release@sha256:9c5f0df8b192a0d7b46cd5f6a4da2289c155fd5302dec7954f8f06c878160b8b",

    "startedTime": "2019-06-19T20:30:50Z",
    "state": "Partial",
    "verified": true,
    "version": "4.1.2"
  },
  {
    "completionTime": "2019-06-19T20:30:50Z",
    "image": "quay.io/openshift-release-dev/ocp-
release@sha256:b8307ac0f3ec4ac86c3f3b52846425205022da52c16f56ec31cbe428501001d6
",
    "startedTime": "2019-06-19T17:38:10Z",
    "state": "Completed",
    "verified": false,
    "version": "4.1.0"
  }
]
```

The history contains a list of the most recent versions applied to the cluster. This value is updated when the CVO applies an update. The list is ordered by date, where the newest update is first in the list. Updates in the history have state **Completed** if the rollout completed and **Partial** if the update failed or did not complete.



IMPORTANT

If an upgrade fails, the Operator stops and reports the status of the failing component. Rolling your cluster back to a previous version is not supported. If your upgrade fails, contact Red Hat support.

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

```
$ oc get clusterversion
```

```
NAME      VERSION     AVAILABLE   PROGRESSING   SINCE     STATUS
version   4.1.2       True        False         2m        Cluster version is 4.1.2
```

8. If you are upgrading to this release from OpenShift Container Platform 4.3.3 or earlier, you must restart all Pods after the upgrade is complete. You can do this using the following command:

```
$ for I in $(oc get ns -o jsonpath='{range .items[*]} {.metadata.name}{"\n"} {end}'); \
    do oc delete pods --all -n $I; \
    sleep 1; \
    done
```

NOTE

Restarting all Pods is required because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

CHAPTER 4. 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.

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 upgrade fails and you must restore your cluster to a previous state.

IMPORTANT

If you are upgrading to this release from OpenShift Container Platform 4.2, you must restart all Pods after the upgrade is complete.

This is because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

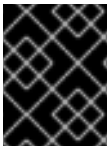
After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

4.1. ABOUT THE OPENSHIFT CONTAINER PLATFORM UPDATE SERVICE

The OpenShift Container Platform update service is the hosted service that provides over-the-air updates to both OpenShift Container Platform and Red Hat Enterprise Linux CoreOS (RHCOS). It provides a graph, or diagram that contain *vertices* and the *edges* that connect them, of component Operators. The edges in the graph show which versions you can safely update to, and 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 Container Platform 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 OpenShift Container Platform CVO uses the release image for that update to upgrade your cluster. The release artifacts are hosted in Quay as container images.

To allow the OpenShift Container Platform update service to provide only compatible updates, a release verification pipeline exists to drive 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 Container Platform update service notifies you that it is available.



IMPORTANT

Because the update service displays all valid updates, you must not force an update to a version that the update service does not display.

During continuous update mode, two controllers run. One continuously updates the payload manifests, applies them to the cluster, and outputs the status of the controlled rollout of the Operators, whether they are available, upgrading, or failed. The second controller polls the OpenShift Container Platform update service to determine if updates are available.

IMPORTANT

Reverting your cluster to a previous version, or a rollback, is not supported. Only upgrading to a newer version is supported.

During the upgrade process, the Machine Config Operator (MCO) applies the new configuration to your cluster machines. It cordons the number of nodes that is specified by the **maxUnavailable** field on the machine configuration pool and marks them as unavailable. By default, this value is set to **1**. It 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 on these machines because you must update the OpenShift API on them first. Because the specification for the new version is 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 nodes that are unavailable is set to ensure that normal cluster operations are likely to continue with that number of machines out of service.

4.2. OPENSHIFT CONTAINER PLATFORM UPGRADE CHANNELS AND RELEASES

In OpenShift Container Platform 4.1, Red Hat introduced the concept of channels for recommending the appropriate release versions for cluster upgrade. By controlling the pace of upgrades, these upgrade channels allow you to choose an upgrade strategy. Upgrade channels are tied to a minor version of OpenShift Container Platform. For instance, OpenShift Container Platform 4.3 upgrade channels will never include an upgrade to a 4.4 release. This strategy ensures that administrators explicitly decide to upgrade to the next minor version of OpenShift Container Platform. Upgrade 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.

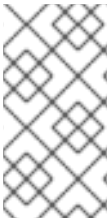
OpenShift Container Platform 4.3 offers the following upgrade channels:

- **candidate-4.3**
- **fast-4.3**
- **stable-4.3**

candidate-4.3 channel

The **candidate-4.3** channel contains candidate builds for a z-stream (4.3.z) release. Release candidates contain all the features of the product but are not supported. Use release candidate versions to test feature acceptance and assist in qualifying the next version of OpenShift Container Platform. A release candidate is any build that is available in the candidate channel, including ones that do not contain **-rc** in their names. After a version is available in the candidate channel, it goes through more quality checks. If it meets the quality standard, it is promoted to the **fast-4.3** or **stable-4.3** channels. Because of this strategy, if a specific release is available in both the **candidate-4.3** channel and in the **fast-4.3** or **stable-4.3** channels, it is a Red Hat supported version. The **candidate-4.3** channel can include release versions from which there are no recommended updates in any channel.

You can use the **candidate-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.



NOTE

Release candidates differ from the nightly builds found on the https://www.openshift.com/try site. Nightly builds are available for early access to features, but updating to or from nightly builds is neither recommended nor supported. Nightly builds are not available in any upgrade channel.

fast-4.3 channel

The **fast-4.3** channel is updated with new 4.3 versions as soon as Red Hat declares the given version as a general availability release. As such, these releases are fully supported, are production quality, and have performed well while available as a release candidate in the **candidate-4.3** channel from where they were promoted. Some time after a release appears in the **fast-4.3** channel, it is added to the **stable-4.3** channel. Releases never appear in the **stable-4.3** channel before they appear in the **fast-4.3** channel.

You can use the **fast-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.

stable-4.3 channel

While the **fast-4.3** channel contains releases as soon as their errata are published, releases are added to the **stable-4.3** channel after a delay of several hours to a day. During this delay, data is collected from Red Hat SRE teams, Red Hat support services, and pre-production and production environments that participate in connected customer program about the stability of the release.

You can use the **stable-4.3** channel to upgrade from a previous minor version of OpenShift Container Platform.

Upgrade version paths

OpenShift Container Platform maintains an upgrade recommendation service that understands the version of OpenShift Container Platform you have installed as well as the path to take within the channel you choose to get you to the next release. You can imagine seeing the following in the **fast-4.3** channel:

- 4.3.0
- 4.3.1
- 4.3.3
- 4.3.4

The service recommends only upgrades that have been tested and have no serious issues. If your cluster is on 4.3.1 and OpenShift Container Platform suggests 4.3.4, then it is safe for you to update from .4.3.1 to .4.3.4. Do not rely on consecutive patch numbers. In this example, 4.3.2 is not, and never was, available in the channel. The update service will not suggest updating to a version of OpenShift Container Platform that contains known vulnerabilities.

Update stability depends on your channel. The presence of an update recommendation in the **candidate-4.3** channel does not imply that the update is supported. It means that no serious issues have been found with the update yet, but there might not be significant traffic through the update to suggest stability. The presence of an update recommendation in the **fast-4.3** or **stable-4.3** channels is a declaration that the update is fully supported while it is in the channel. While releases will never be removed from a channel, update recommendations that exhibit serious issues will be removed from all channels. Updates initiated after the update recommendation has been removed might not be supported.

Red Hat will eventually provide supported update paths from any supported release in the **fast-4.3** or **stable-4.3** channels to the latest release in 4.3.z, although there can be delays while safe paths away from troubled releases are constructed and verified.

Fast and stable channel use and strategies

The **fast-4.3** and **stable-4.3** channels present a choice between receiving general availability releases as soon as they are available or allowing Red Hat to control the rollout of those updates. If issues are detected during rollout or at a later time, upgrades to that version might be blocked in both the **fast-4.3** and **stable-4.3** channels, and a new version might be introduced that becomes the new preferred upgrade target.

Customers can improve this process by configuring pre-production systems on the **fast-4.3** channel, configuring production systems on the **stable-4.3** channel, and participating in Red Hat's connected customer program. Red Hat uses this program to observe the impact of updates on your specific hardware and software configurations. Future releases might improve or alter the pace at which updates move from the **fast-4.3** to the **stable-4.3** channel.

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 upgrades. During upgrade, 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.

Switching between channels

Your cluster is still supported if you change from the **stable-4.3** channel to the **fast-4.3** channel. Although you can switch to the **candidate-4.3** channel at any time, some releases in that channel might be unsupported release candidates. You can switch from the **candidate-4.3** channel to the **fast-4.3** channel if your current release is a general availability release. You can always switch from the **fast-4.3** channel to the **stable-4.3** channel, although if the current release was recently promoted to **fast-{product-stable}** there can be a delay of up to a day for the release to be promoted to **stable-4.3**. If you change to a channel that does not include your current release, an alert displays and no updates can be recommended, but you can safely change back to your original channel at any point.

4.3. 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.

Procedure

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

2. For production clusters, ensure that the **CHANNEL** is set to the correct channel for the version that you want to update to, your current minor version, such as **stable-4.3**.

IMPORTANT

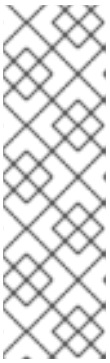
For production clusters, you must subscribe to a stable-* or fast-* channel.

- If the **UPDATE STATUS** is not **Updates Available**, you cannot upgrade your cluster.
- The **DESIRED VERSION** indicates the cluster version that your cluster is running or is updating to.

3. Click **Updates Available**, select a version to update to, the highest available version and click **Update**. The **UPDATE STATUS** changes to **Updating**, and you can review the progress of the Operator upgrades on the **Cluster Operators** tab.

4. If you are upgrading to this release from OpenShift Container Platform 4.3.3 or earlier, 4.2, you must restart all Pods after the upgrade is complete. You can do this using the following command, which requires the OpenShift CLI (**oc**):

```
$ for I in $(oc get ns -o jsonpath='{range .items[*]} {.metadata.name}{"\n"} {end}'); \
    do oc delete pods --all -n $I; \
    sleep 1; \
    done
```



NOTE

Restarting all Pods is required because the service CA is automatically rotated as of OpenShift Container Platform 4.3.5. 4.3.5. The service CA is rotated during the upgrade and a restart is required afterward to ensure that all services are using the new service CA before the previous service CA expires.

After this one-time manual restart, subsequent upgrades and rotations will ensure restart before the service CA expires without requiring manual intervention.

5. 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-* 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.

4.4. (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.

4.4.1. 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.

4.4.2. 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.

4.4.3. 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
openshift_node_pre_cordon_hook	• Runs **before** each node is cordoned. • This hook runs against **each node** in serial. • If a task must run against a different host, the task must use **delegate_to** or **local_action**.
openshift_node_pre_upgrade_hook	• Runs **after** each node is cordoned but **before** it is updated. • This hook runs against **each node** in serial. • If a task must run against a different host, the task must use **delegate_to** or **local_action**.
openshift_node_pre_uncordon_hook	• Runs **after** each node is updated but **before** it is uncordoned. • This hook runs against **each node** in serial. • If a task must run against a different host, they task must use **delegate_to** or **local_action**.
openshift_node_post_upgrade_hook	• Runs **after** each node uncordoned. It is the **last** node update action. • This hook runs against **each node** in serial. • If a task must run against a different host, the task must use **delegate_to** or **local_action**.

4.5. 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.

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 compute machines in it.

- 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 and the **upgrade** playbook.

Procedure

1. Stop and disable firewalld on the host:

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

NOTE

You must not enable firewalld later. If you do, you cannot access OpenShift Container Platform logs on the worker.

2. Enable the repositories that are required for OpenShift Container Platform 4.3:
   a. On the machine that you run the Ansible playbooks, update the required repositories:

```
# subscription-manager repos --disable=rhel-7-server-ansible-2.7-rpms  \
                           --disable=rhel-7-server-ose-4.2-rpms \
                           --enable=rhel-7-server-ansible-2.8-rpms \
                           --enable=rhel-7-server-ose-4.3-rpms
```

   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=rhel-7-server-ose-4.2-rpms \
                           --enable=rhel-7-server-ose-4.3-rpms
```

3. Update a RHEL worker machine:
   a. Review the current node status to determine which RHEL worker to update:

```
# oc get node
NAME                    STATUS                     ROLES    AGE    VERSION
mycluster-control-plane-0   Ready                      master   145m   v1.16.2
mycluster-control-plane-1   Ready                      master   145m   v1.16.2
mycluster-control-plane-2   Ready                      master   145m   v1.16.2
mycluster-rhel7-0           NotReady,SchedulingDisabled   worker   98m
v1.14.6+97c81d00e
```

```
mycluster-rhel7-1   Ready   worker   98m   v1.14.6+97c81d00e
mycluster-rhel7-2   Ready   worker   98m   v1.14.6+97c81d00e
mycluster-rhel7-3   Ready   worker   98m   v1.14.6+97c81d00e
```

Note which machine has the **NotReady,SchedulingDisabled** status.

b. Review your Ansible inventory file at **/<path>/inventory/hosts** and update its contents so that only the machine with the **NotReady,SchedulingDisabled** status is 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-rhel7-0.example.com
```

c. Change to the **openshift-ansible** directory and run the **upgrade** playbook:

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

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

4. Follow the process in the previous step to update each RHEL worker machine in your cluster.

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

```
# oc get node
NAME                      STATUS                        ROLES    AGE    VERSION
mycluster-control-plane-0   Ready                         master   145m   v1.16.2
mycluster-control-plane-1   Ready                         master   145m   v1.16.2
mycluster-control-plane-2   Ready                         master   145m   v1.16.2
mycluster-rhel7-0         NotReady,SchedulingDisabled   worker   98m    v1.16.2
mycluster-rhel7-1         Ready                         worker   98m    v1.16.2
mycluster-rhel7-2         Ready                         worker   98m    v1.16.2
mycluster-rhel7-3         Ready                         worker   98m    v1.16.2
```