OpenShift Dedicated 4

Installing, accessing, and deleting OpenShift Dedicated clusters

Installing, accessing, and deleting OpenShift Dedicated clusters

Last Updated: 2024-10-03

OpenShift Dedicated 4 Installing, accessing, and deleting OpenShift Dedicated clusters

Installing, accessing, and deleting OpenShift Dedicated clusters

Legal Notice

Abstract

This document provides information on how to install OpenShift Dedicated clusters. The document also provides details on how to configure identity providers.

Table of Contents

CHAPTER 1. CREATING A CLUSTER ON AWS

You can install OpenShift Dedicated on Amazon Web Services (AWS) by using your own AWS account through the Customer Cloud Subscription (CCS) model or by using an AWS infrastructure account that is owned by Red Hat.

1.1. PREREQUISITES

- You reviewed the introduction to OpenShift Dedicated and the documentation on architecture concepts.
- You reviewed the OpenShift Dedicated cloud deployment options.

1.2. CREATING A CLUSTER ON AWS WITH CCS

By using the Customer Cloud Subscription (CCS) billing model, you can create an OpenShift Dedicated cluster in an existing Amazon Web Services (AWS) account that you own.

You must meet several prerequisites if you use the CCS model to deploy and manage OpenShift Dedicated into your AWS account.

Prerequisites

- You have configured your AWS account for use with OpenShift Dedicated.
- You have not deployed any services in your AWS account.
- You have configured the AWS account quotas and limits that are required to support the desired cluster size.
- You have an **osdCcsAdmin** AWS Identity and Access Management (IAM) user with the **AdministratorAccess** policy attached.
- You have set up a service control policy (SCP) in your AWS organization. For more information, see *Minimum required service control policy (SCP)*.
- Consider having **Business Support** or higher from AWS.
- If you are configuring a cluster-wide proxy, you have verified that the proxy is accessible from the VPC that the cluster is being installed into. The proxy must also be accessible from the private subnets of the VPC.

Procedure

1. Log in to OpenShift Cluster Manager and click **Create cluster**.
2. On the **Create an OpenShift cluster** page, select **Create cluster** in the **Red Hat OpenShift Dedicated** row.
3. Under **Billing model**, configure the subscription type and infrastructure type:
    a. Select a subscription type. For information about OpenShift Dedicated subscription options, see Cluster subscriptions and registration in the OpenShift Cluster Manager documentation.

NOTE

The subscription types that are available to you depend on your OpenShift Dedicated subscriptions and resource quotas. For more information, contact your sales representative or Red Hat support.

b. Select the **Customer Cloud Subscription** infrastructure type to deploy OpenShift Dedicated in an existing cloud provider account that you own.

c. Click **Next**.

4. Select **Run on Amazon Web Services**.

5. After selecting your cloud provider, review and complete the listed **Prerequisites**. Select the checkbox to acknowledge that you have read and completed all of the prerequisites.

6. Provide your AWS account details:

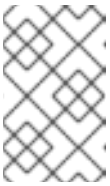
a. Enter your **AWS account ID**.

b. Enter your **AWS access key ID** and **AWS secret access key** for your AWS IAM user account.

NOTE

Revoking these credentials in AWS results in a loss of access to any cluster created with these credentials.

c. Optional: You can select **Bypass AWS service control policy (SCP) checks** to disable the SCP checks.



NOTE

Some AWS SCPs can cause the installation to fail, even if you have the required permissions. Disabling the SCP checks allows an installation to proceed. The SCP is still enforced even if the checks are bypassed.

7. Click **Next** to validate your cloud provider account and go to the **Cluster details** page.

8. On the **Cluster details** page, provide a name for your cluster and specify the cluster details:

a. Add a **Cluster name**.

b. Optional: Cluster creation generates a domain prefix as a subdomain for your provisioned cluster on **openshiftapps.com**. If the cluster name is less than or equal to 15 characters, that name is used for the domain prefix. If the cluster name is longer than 15 characters, the domain prefix is randomly generated to a 15 character string.
To customize the subdomain, select the **Create customize domain prefix** checkbox, and enter your domain prefix name in the **Domain prefix** field. The domain prefix cannot be longer than 15 characters, must be unique within your organization, and cannot be changed after cluster creation.

c. Select a cluster version from the **Version** drop-down menu.

d. Select a cloud provider region from the **Region** drop-down menu.

e. Select a **Single zone** or **Multi-zone** configuration.

f. Leave **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat Site Reliability Engineer (SRE) platform metrics. This option is enabled by default.

g. Optional: Select **Enable additional etcd encryption** if you require etcd key value encryption. With this option, the etcd key values are encrypted, but the keys are not. This option is in addition to the control plane storage encryption that encrypts the etcd volumes in OpenShift Dedicated clusters by default.

NOTE

By enabling etcd encryption for the key values in etcd, you will incur a performance overhead of approximately 20%. The overhead is a result of introducing this second layer of encryption, in addition to the default control plane storage encryption that encrypts the etcd volumes. Consider enabling etcd encryption only if you specifically require it for your use case.

h. Optional: Select **Encrypt persistent volumes with customer keys** if you want to provide your own AWS Key Management Service (KMS) key Amazon Resource Name (ARN). The key is used for encrypting all control plane, infrastructure, worker node root volumes, and persistent volumes in your cluster.

IMPORTANT

Only persistent volumes (PVs) created from the default storage class are encrypted with this specific key.

PVs created by using any other storage class are still encrypted, but the PVs are not encrypted with this key unless the storage class is specifically configured to use this key.

i. Click **Next**.

9. On the **Default machine pool** page, select a **Compute node instance type** and a **Compute node count**. The number and types of nodes that are available depend on your OpenShift Dedicated subscription. If you are using multiple availability zones, the compute node count is per zone.

NOTE

After your cluster is created, you can change the number of compute nodes in your cluster, but you cannot change the compute node instance type in a machine pool. The number and types of nodes available to you depend on your OpenShift Dedicated subscription.

10. Choose your preference for the Instance Metadata Service (IMDS) type, either using both IMDSv1 and IMDSv2 types or requiring your EC2 instances to use only IMDSv2. You can access instance metadata from a running instance in two ways:

- Instance Metadata Service Version 1 (IMDSv1) - a request/response method
- Instance Metadata Service Version 2 (IMDSv2) - a session-oriented method

IMPORTANT

The Instance Metadata Service settings cannot be changed after your cluster is created.

NOTE

IMDSv2 uses session-oriented requests. With session-oriented requests, you create a session token that defines the session duration, which can range from a minimum of one second to a maximum of six hours. During the specified duration, you can use the same session token for subsequent requests. After the specified duration expires, you must create a new session token to use for future requests.

For more information regarding IMDS, see Instance metadata and user data in the AWS documentation.

11. Optional: Expand **Edit node labels** to add labels to your nodes. Click **Add label** to add more node labels and select **Next**.

12. On the **Network configuration** page, select **Public** or **Private** to use either public or private API endpoints and application routes for your cluster.

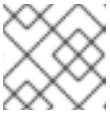
IMPORTANT

If you are using private API endpoints, you cannot access your cluster until you update the network settings in your cloud provider account.

13. Optional: To install the cluster in an existing AWS Virtual Private Cloud (VPC):

    a. Select **Install into an existing VPC**

    b. If you are installing into an existing VPC and opted to use private API endpoints, you can select **Use a PrivateLink**. This option enables connections to the cluster by Red Hat Site Reliability Engineering (SRE) using only AWS PrivateLink endpoints.



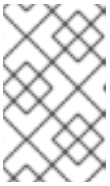
NOTE

The **Use a PrivateLink** option cannot be changed after a cluster is created.

    c. If you are installing into an existing VPC and you want to enable an HTTP or HTTPS proxy for your cluster, select **Configure a cluster-wide proxy**.

14. Click **Next**.

15. If you opted to install the cluster in an existing AWS VPC, provide your **Virtual Private Cloud (VPC) subnet settings** and select **Next**. You must have created the Cloud network address translation (NAT) and a Cloud router. See the "Additional resources" section for information about Cloud NATs and Google VPCs.



NOTE

You must ensure that your VPC is configured with a public and a private subnet for each availability zone that you want the cluster installed into. If you opted to use PrivateLink, only private subnets are required.

a. Optional: Expand **Additional security groups** and select additional custom security groups to apply to nodes in the machine pools that are created by default. You must have already created the security groups and associated them with the VPC that you selected for this cluster. You cannot add or edit security groups to the default machine pools after you create the cluster.
By default, the security groups you specify are added for all node types. Clear the **Apply the same security groups to all node types** checkbox to apply different security groups for each node type.

For more information, see the requirements for *Security groups* under *Additional resources*.

16. If you opted to configure a cluster-wide proxy, provide your proxy configuration details on the **Cluster-wide proxy** page:

a. Enter a value in at least one of the following fields:

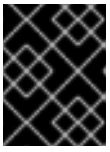
- Specify a valid **HTTP proxy URL**
- Specify a valid **HTTPS proxy URL**
- In the **Additional trust bundle** field, provide a PEM encoded X.509 certificate bundle. The bundle is added to the trusted certificate store for the cluster nodes. An additional trust bundle file is required if you use a TLS-inspecting proxy unless the identity certificate for the proxy is signed by an authority from the Red Hat Enterprise Linux CoreOS (RHCOS) trust bundle. This requirement applies regardless of whether the proxy is transparent or requires explicit configuration using the **http-proxy** and **https-proxy** arguments.

b. Click **Next**.
For more information about configuring a proxy with OpenShift Dedicated, see *Configuring a cluster-wide proxy*.

17. In the **CIDR ranges** dialog, configure custom classless inter-domain routing (CIDR) ranges or use the defaults that are provided.

NOTE

If you are installing into a VPC, the **Machine CIDR** range must match the VPC subnets.



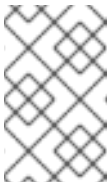
IMPORTANT

CIDR configurations cannot be changed later. Confirm your selections with your network administrator before proceeding.

18. On the **Cluster update strategy** page, configure your update preferences:

a. Choose a cluster update method:

- Select **Individual updates** if you want to schedule each update individually. This is the default option.
- Select **Recurring updates** to update your cluster on your preferred day and start time, when updates are available.



NOTE

You can review the end-of-life dates in the update lifecycle documentation for OpenShift Dedicated. For more information, see OpenShift Dedicated update life cycle .

b. Provide administrator approval based on your cluster update method:
   - Individual updates: If you select an update version that requires approval, provide an administrator's acknowledgment and click **Approve and continue**.
   - Recurring updates: If you selected recurring updates for your cluster, provide an administrator's acknowledgment and click **Approve and continue**. OpenShift Cluster Manager does not start scheduled y-stream updates for minor versions without receiving an administrator's acknowledgment.

c. If you opted for recurring updates, select a preferred day of the week and upgrade start time in UTC from the drop-down menus.

d. Optional: You can set a grace period for **Node draining** during cluster upgrades. A **1 hour** grace period is set by default.

e. Click **Next**.

NOTE

In the event of critical security concerns that significantly impact the security or stability of a cluster, Red Hat Site Reliability Engineering (SRE) might schedule automatic updates to the latest z-stream version that is not impacted. The updates are applied within 48 hours after customer notifications are provided. For a description of the critical impact security rating, see Understanding Red Hat security ratings .

19. Review the summary of your selections and click **Create cluster** to start the cluster installation. The installation takes approximately 30-40 minutes to complete.
20. Optional: On the **Overview** tab, you can enable the delete protection feature by selecting **Enable**, which is located directly under **Delete Protection: Disabled**. This will prevent your cluster from being deleted. To disable delete protection, select **Disable**. By default, clusters are created with the delete protection feature disabled.

Verification

- You can monitor the progress of the installation in the **Overview** page for your cluster. You can view the installation logs on the same page. Your cluster is ready when the **Status** in the **Details** section of the page is listed as **Ready**.

1.3. CREATING A CLUSTER ON AWS WITH A RED HAT CLOUD ACCOUNT

Through OpenShift Cluster Manager, you can create an OpenShift Dedicated cluster on Amazon Web Services (AWS) using a standard cloud provider account owned by Red Hat.

Procedure

1. Log in to OpenShift Cluster Manager and click **Create cluster**.
2. In the **Cloud** tab, click **Create cluster** in the **Red Hat OpenShift Dedicated** row.
3. Under **Billing model**, configure the subscription type and infrastructure type:
   a. Select the **Annual** subscription type. Only the **Annual** subscription type is available when you deploy a cluster using a Red Hat cloud account.
   For information about OpenShift Dedicated subscription options, see Cluster subscriptions and registration in the OpenShift Cluster Manager documentation.

   NOTE

   You must have the required resource quota for the **Annual** subscription type to be available. For more information, contact your sales representative or Red Hat support.

   b. Select the **Red Hat cloud account** infrastructure type to deploy OpenShift Dedicated in a cloud provider account that is owned by Red Hat.
   c. Click **Next**.
4. Select **Run on Amazon Web Services** and click **Next**.
5. On the **Cluster details** page, provide a name for your cluster and specify the cluster details:
   a. Add a **Cluster name**.
   b. Optional: Cluster creation generates a domain prefix as a subdomain for your provisioned cluster on **openshiftapps.com**. If the cluster name is less than or equal to 15 characters, that name is used for the domain prefix. If the cluster name is longer than 15 characters, the domain prefix is randomly generated as a 15-character string.
   To customize the subdomain, select the **Create custom domain prefix** checkbox, and enter your domain prefix name in the **Domain prefix** field. The domain prefix cannot be longer than 15 characters, must be unique within your organization, and cannot be changed after cluster creation.
   c. Select a cluster version from the **Version** drop-down menu.
   d. Select a cloud provider region from the **Region** drop-down menu.
   e. Select a **Single zone** or **Multi-zone** configuration.
   f. Select a **Persistent storage** capacity for the cluster. For more information, see the *Storage* section in the OpenShift Dedicated service definition.
   g. Specify the number of **Load balancers** that you require for your cluster. For more information, see the *Load balancers* section in the OpenShift Dedicated service definition.

h. Leave **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat Site Reliability Engineer (SRE) platform metrics. This option is enabled by default.

i. Optional: Select **Enable additional etcd encryption** if you require etcd key value encryption. With this option, the etcd key values are encrypted, but not the keys. This option is in addition to the control plane storage encryption that encrypts the etcd volumes in OpenShift Dedicated clusters by default.

NOTE

By enabling etcd encryption for the key values in etcd, you will incur a performance overhead of approximately 20%. The overhead is a result of introducing this second layer of encryption, in addition to the default control plane storage encryption that encrypts the etcd volumes. Consider enabling etcd encryption only if you specifically require it for your use case.

j. Click **Next**.

6. On the **Default machine pool** page, select a **Compute node instance type** and a **Compute node count**. The number and types of nodes that are available depend on your OpenShift Dedicated subscription. If you are using multiple availability zones, the compute node count is per zone.

NOTE

After your cluster is created, you can change the number of compute nodes, but you cannot change the compute node instance type in a machine pool. For clusters that use the CCS model, you can add machine pools after installation that use a different instance type. The number and types of nodes available to you depend on your OpenShift Dedicated subscription.

7. Optional: Expand **Edit node labels** to add labels to your nodes. Click **Add label** to add more node labels and select **Next**.

8. In the **Cluster privacy** dialog, select **Public** or **Private** to use either public or private API endpoints and application routes for your cluster.

9. Click **Next**.

10. In the **CIDR ranges** dialog, configure custom classless inter-domain routing (CIDR) ranges or use the defaults that are provided.

IMPORTANT

CIDR configurations cannot be changed later. Confirm your selections with your network administrator before proceeding.

If the cluster privacy is set to **Private**, you cannot access your cluster until you configure private connections in your cloud provider.

11. On the **Cluster update strategy** page, configure your update preferences:

a. Choose a cluster update method:

- Select **Individual updates** if you want to schedule each update individually. This is the default option.
- Select **Recurring updates** to update your cluster on your preferred day and start time, when updates are available.

NOTE

You can review the end-of-life dates in the update lifecycle documentation for OpenShift Dedicated. For more information, see OpenShift Dedicated update life cycle .

b. Provide administrator approval based on your cluster update method:

- Individual updates: If you select an update version that requires approval, provide an administrator's acknowledgment and click **Approve and continue**.
- Recurring updates: If you selected recurring updates for your cluster, provide an administrator's acknowledgment and click **Approve and continue**. OpenShift Cluster Manager does not start scheduled y-stream updates for minor versions without receiving an administrator's acknowledgment.

c. If you opted for recurring updates, select a preferred day of the week and upgrade start time in UTC from the drop-down menus.

d. Optional: You can set a grace period for **Node draining** during cluster upgrades. A **1 hour** grace period is set by default.

e. Click **Next**.

NOTE

In the event of critical security concerns that significantly impact the security or stability of a cluster, Red Hat Site Reliability Engineering (SRE) might schedule automatic updates to the latest z-stream version that is not impacted. The updates are applied within 48 hours after customer notifications are provided. For a description of the critical impact security rating, see Understanding Red Hat security ratings .

12. Review the summary of your selections and click **Create cluster** to start the cluster installation. The installation takes approximately 30-40 minutes to complete.

13. Optional: On the **Overview** tab, you can enable the delete protection feature by selecting **Enable**, which is located directly under **Delete Protection: Disabled**. This will prevent your cluster from being deleted. To disable delete protection, select **Disable**. By default, clusters are created with the delete protection feature disabled.

Verification

- You can monitor the progress of the installation in the **Overview** page for your cluster. You can view the installation logs on the same page. Your cluster is ready when the **Status** in the **Details** section of the page is listed as **Ready**.

1.4. ADDITIONAL RESOURCES

- For information about configuring a proxy with OpenShift Dedicated, see Configuring a cluster-wide proxy.
- For details about the AWS service control policies required for CCS deployments, see Minimum required service control policy (SCP).
- For information about persistent storage for OpenShift Dedicated, see the Storage section in the OpenShift Dedicated service definition.
- For information about load balancers for OpenShift Dedicated, see the Load balancers section in the OpenShift Dedicated service definition.
- For more information about etcd encryption, see the etcd encryption service definition .
- For information about the end-of-life dates for OpenShift Dedicated versions, see the OpenShift Dedicated update life cycle .
- For information about the requirements for custom additional security groups, see Additional custom security groups.

CHAPTER 2. CREATING A CLUSTER ON GCP

You can install OpenShift Dedicated on Google Cloud Platform (GCP) by using your own GCP account through the Customer Cloud Subscription (CCS) model or by using a GCP infrastructure account that is owned by Red Hat.

2.1. PREREQUISITES

- You reviewed the introduction to OpenShift Dedicated and the documentation on architecture concepts.
- You reviewed the OpenShift Dedicated cloud deployment options.

2.2. CREATING A CLUSTER ON GCP WITH CCS

By using the Customer Cloud Subscription (CCS) billing model, you can create an OpenShift Dedicated cluster in an existing Google Cloud Platform (GCP) account that you own.

You must meet several prerequisites if you use the CCS model to deploy and manage OpenShift Dedicated into your GCP account.

Prerequisites

- You have configured your GCP account for use with OpenShift Dedicated.
- You have configured the GCP account quotas and limits that are required to support the desired cluster size.
- You have created a GCP project.

NOTE

The project name must be 10 characters or less.

- You have enabled the Google Cloud Resource Manager API in your GCP project. For more information about enabling APIs for your project, see the Google Cloud documentation.
- You have an IAM service account in GCP called **osd-ccs-admin** with the following roles attached:
  - Compute Admin
  - DNS Administrator
  - Security Admin
  - Service Account Admin
  - Service Account Key Admin
  - Service Account User
  - Organization Policy Viewer
  - Service Management Administrator

- Service Usage Admin
- Storage Admin
- Compute Load Balancer Admin
- Role Viewer
- Role Administrator

- You have created a key for your **osd-ccs-admin** GCP service account and exported it to a file named **osServiceAccount.json**.

NOTE

For more information about creating a key for your GCP service account and exporting it to a JSON file, see Creating service account keys in the Google Cloud documentation.

- Consider having Enhanced Support or higher from GCP.
- To prevent potential conflicts, consider having no other resources provisioned in the project prior to installing OpenShift Dedicated.
- If you are configuring a cluster-wide proxy, you have verified that the proxy is accessible from the VPC that the cluster is being installed into.

Procedure

1. Log in to OpenShift Cluster Manager and click **Create cluster**.
2. On the **Create an OpenShift cluster** page, select **Create cluster** in the **Red Hat OpenShift Dedicated** row.
3. Under **Billing model**, configure the subscription type and infrastructure type:
   a. Select a subscription type. For information about OpenShift Dedicated subscription options, see Cluster subscriptions and registration in the OpenShift Cluster Manager documentation.

NOTE

The subscription types that are available to you depend on your OpenShift Dedicated subscriptions and resource quotas. For more information, contact your sales representative or Red Hat support.

   b. Select the **Customer Cloud Subscription** infrastructure type to deploy OpenShift Dedicated in an existing cloud provider account that you own.
   c. Click **Next**.
4. Select **Run on Google Cloud Platform**
5. After selecting your cloud provider, review and complete the listed **Prerequisites**. Select the checkbox to acknowledge that you have read and completed all of the prerequisites.

6. Provide your GCP service account private key in JSON format. You can either click **Browse** to locate and attach a JSON file or add the details in the **Service account JSON** field.

7. Click **Next** to validate your cloud provider account and go to the **Cluster details** page.

8. On the **Cluster details** page, provide a name for your cluster and specify the cluster details:

   a. Add a **Cluster name**.

   b. Optional: Cluster creation generates a domain prefix as a subdomain for your provisioned cluster on **openshiftapps.com**. If the cluster name is less than or equal to 15 characters, that name is used for the domain prefix. If the cluster name is longer than 15 characters, the domain prefix is randomly generated to a 15 character string.
   To customize the subdomain, select the **Create customize domain prefix** checkbox, and enter your domain prefix name in the **Domain prefix** field. The domain prefix cannot be longer than 15 characters, must be unique within your organization, and cannot be changed after cluster creation.

   c. Select a cluster version from the **Version** drop-down menu.

   d. Select a cloud provider region from the **Region** drop-down menu.

   e. Select a **Single zone** or **Multi-zone** configuration.

   f. Optional: Select **Enable Secure Boot for Shielded VMs** to use Shielded VMs when installing your cluster. For more information, see Shielded VMs.

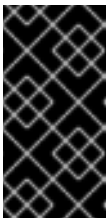
   IMPORTANT

   To successfully create a cluster, you must select **Enable Secure Boot support for Shielded VMs** if your organization has the policy constraint **constraints/compute.requireShieldedVm** enabled. For more information regarding GCP organizational policy constraints, see Organization policy constraints.

   g. Leave **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat Site Reliability Engineer (SRE) platform metrics. This option is enabled by default.

9. Optional: Expand **Advanced Encryption** to make changes to encryption settings.

   a. Select **Use Custom KMS keys** to use custom KMS keys. If you prefer not to use custom KMS keys, leave the default setting **Use default KMS Keys**.

   IMPORTANT

   To use custom KMS keys, the IAM service account **osd-ccs-admin** must be granted the **Cloud KMS CryptoKey Encrypter/Decrypter** role. For more information about granting roles on a resource, see Granting roles on a resource.

   With **Use Custom KMS keys** selected:

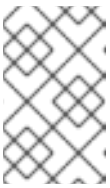
      i. Select a key ring location from the **Key ring location** drop-down menu.

      ii. Select a key ring from the **Key ring** drop-down menu.

iii. Select a key name from the **Key name** drop-down menu.

iv. Provide the **KMS Service Account**

b. Optional: Select **Enable FIPS cryptography** if you require your cluster to be FIPS validated.



NOTE

If **Enable FIPS cryptography** is selected, **Enable additional etcd encryption** is enabled by default and cannot be disabled. You can select **Enable additional etcd encryption** without selecting **Enable FIPS cryptography**.

c. Optional: Select **Enable additional etcd encryption** if you require etcd key value encryption. With this option, the etcd key values are encrypted, but the keys are not. This option is in addition to the control plane storage encryption that encrypts the etcd volumes in OpenShift Dedicated clusters by default.

NOTE

By enabling etcd encryption for the key values in etcd, you will incur a performance overhead of approximately 20%. The overhead is a result of introducing this second layer of encryption, in addition to the default control plane storage encryption that encrypts the etcd volumes. Consider enabling etcd encryption only if you specifically require it for your use case.

d. Click **Next**.

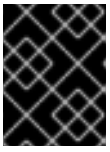
10. On the **Default machine pool** page, select a **Compute node instance type** and a **Compute node count**. The number and types of nodes that are available depend on your OpenShift Dedicated subscription. If you are using multiple availability zones, the compute node count is per zone.

NOTE

After your cluster is created, you can change the number of compute nodes in your cluster, but you cannot change the compute node instance type in a machine pool. The number and types of nodes available to you depend on your OpenShift Dedicated subscription.

11. Optional: Expand **Edit node labels** to add labels to your nodes. Click **Add label** to add more node labels and select **Next**.

12. On the **Network configuration** page, select **Public** or **Private** to use either public or private API endpoints and application routes for your cluster.



IMPORTANT

If you are using private API endpoints, you cannot access your cluster until you update the network settings in your cloud provider account.

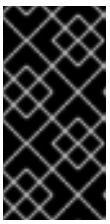
13. Optional: To install the cluster in an existing GCP Virtual Private Cloud (VPC):

a. Select **Install into an existing VPC**

b. If you are installing into an existing VPC and you want to enable an HTTP or HTTPS proxy for your cluster, select **Configure a cluster-wide proxy**.

14. Click **Next**.

15. Optional: To install the cluster into a GCP Shared VPC:

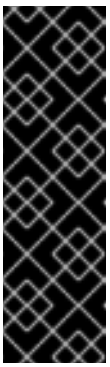


IMPORTANT

To install a cluster into a Shared VPC, you must use OpenShift Dedicated version 4.13.15 or above. Additionally, the VPC owner of the host project must enable a project as a host project in their Google Cloud console. For more information, see Enable a host project .

a. Select **Install into GCP Shared VPC**.

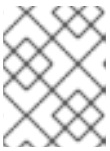
b. Specify the **Host project ID**. If the specified host project ID is incorrect, cluster creation fails.



IMPORTANT

Once you complete the steps within the cluster configuration wizard and click **Create Cluster**, the cluster will go into the "Installation Waiting" state. At this point, you must contact the VPC owner of the host project, who must assign the dynamically-generated service account the following roles: **Compute Network Administrator**, **Compute Security Administrator**, and **DNS Administrator**. The VPC owner of the host project has 30 days to grant the listed permissions before the cluster creation fails. For information about Shared VPC permissions, see Provision Shared VPC.

16. If you opted to install the cluster in an existing GCP VPC, provide your **Virtual Private Cloud (VPC) subnet settings** and select **Next**. You must have created the Cloud network address translation (NAT) and a Cloud router. See the "Additional resources" section for information about Cloud NATs and Google VPCs.



NOTE

If you are installing a cluster into a Shared VPC, the VPC name and subnets are shared from the host project.

17. If you opted to configure a cluster-wide proxy, provide your proxy configuration details on the **Cluster-wide proxy** page:

a. Enter a value in at least one of the following fields:

- Specify a valid **HTTP proxy URL**.
- Specify a valid **HTTPS proxy URL**.
- In the **Additional trust bundle** field, provide a PEM encoded X.509 certificate bundle. The bundle is added to the trusted certificate store for the cluster nodes. An additional trust bundle file is required if you use a TLS-inspecting proxy unless the identity certificate for the proxy is signed by an authority from the Red Hat Enterprise Linux

CoreOS (RHCOS) trust bundle. This requirement applies regardless of whether the proxy is transparent or requires explicit configuration using the **http-proxy** and **https-proxy** arguments.

b. Click **Next**.
For more information about configuring a proxy with OpenShift Dedicated, see *Configuring a cluster-wide proxy*.

18. In the **CIDR ranges** dialog, configure custom classless inter-domain routing (CIDR) ranges or use the defaults that are provided.

NOTE

If you are installing into a VPC, the **Machine CIDR** range must match the VPC subnets.

IMPORTANT

CIDR configurations cannot be changed later. Confirm your selections with your network administrator before proceeding.

19. On the **Cluster update strategy** page, configure your update preferences:

a. Choose a cluster update method:

- Select **Individual updates** if you want to schedule each update individually. This is the default option.
- Select **Recurring updates** to update your cluster on your preferred day and start time, when updates are available.

NOTE

You can review the end-of-life dates in the update lifecycle documentation for OpenShift Dedicated. For more information, see OpenShift Dedicated update life cycle .

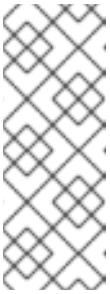
b. Provide administrator approval based on your cluster update method:

- Individual updates: If you select an update version that requires approval, provide an administrator's acknowledgment and click **Approve and continue**.
- Recurring updates: If you selected recurring updates for your cluster, provide an administrator's acknowledgment and click **Approve and continue**. OpenShift Cluster Manager does not start scheduled y-stream updates for minor versions without receiving an administrator's acknowledgment.

c. If you opted for recurring updates, select a preferred day of the week and upgrade start time in UTC from the drop-down menus.

d. Optional: You can set a grace period for **Node draining** during cluster upgrades. A **1 hour** grace period is set by default.

e. Click **Next**.

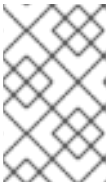


NOTE

In the event of critical security concerns that significantly impact the security or stability of a cluster, Red Hat Site Reliability Engineering (SRE) might schedule automatic updates to the latest z-stream version that is not impacted. The updates are applied within 48 hours after customer notifications are provided. For a description of the critical impact security rating, see Understanding Red Hat security ratings .

20. Review the summary of your selections and click **Create cluster** to start the cluster installation. The installation takes approximately 30-40 minutes to complete.

21. Optional: On the **Overview** tab, you can enable the delete protection feature by selecting **Enable**, which is located directly under **Delete Protection: Disabled**. This will prevent your cluster from being deleted. To disable delete protection, select **Disable**. By default, clusters are created with the delete protection feature disabled.



NOTE

If you delete a cluster that was installed into a GCP Shared VPC, inform the VPC owner of the host project to remove the IAM policy roles granted to the service account that was referenced during cluster creation.

Verification

- You can monitor the progress of the installation in the **Overview** page for your cluster. You can view the installation logs on the same page. Your cluster is ready when the **Status** in the **Details** section of the page is listed as **Ready**.

2.3. CREATING A CLUSTER ON GCP WITH GOOGLE CLOUD MARKETPLACE

When creating an OpenShift Dedicated (OSD) cluster on Google Cloud through the OpenShift Cluster Manager Hybrid Cloud Console, customers can select Google Cloud Marketplace as their preferred billing model. This billing model allows Red Hat customers to take advantage of their Google Committed Use Discounts (CUD) towards OpenShift Dedicated purchased through the Google Cloud Marketplace. Additionally, OSD pricing is consumption-based and customers are billed directly through their Google Cloud account.

Procedure

1. Log in to OpenShift Cluster Manager and click **Create cluster**.
2. In the **Cloud** tab, click **Create cluster** in the **Red Hat OpenShift Dedicated** row.
3. Under **Billing model**, configure the subscription type and infrastructure type:
   a. Select the **On-Demand** subscription type.
   b. From the drop-down menu, select **Google Cloud Marketplace**.
   c. Select the **Customer Cloud Subscription** infrastructure type.
   d. Click **Next**.

4. On the **Cloud provider** page, read the provided prerequisites and the Google terms and conditions. Add your service account key.

    a. Click the **Review Google Terms and Agreements** link.

    b. To continue creating the cluster, click the checkbox indicating that you agree to the Google terms and agreements.

    c. Add your service account key.

    NOTE

    For more information about service account keys, click the information icon located next to **Service account key**.

    d. Click **Next** to validate your cloud provider account and go to the **Cluster details** page.

5. On the **Cluster details** page, provide a name for your cluster and specify the cluster details:

    a. Add a **Cluster name**.

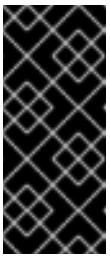
    b. Optional: Cluster creation generates a domain prefix as a subdomain for your provisioned cluster on **openshiftapps.com**. If the cluster name is less than or equal to 15 characters, that name is used for the domain prefix. If the cluster name is longer than 15 characters, the domain prefix is randomly generated as a 15-character string.
    To customize the subdomain, select the **Create custom domain prefix** checkbox, and enter your domain prefix name in the **Domain prefix** field. The domain prefix cannot be longer than 15 characters, must be unique within your organization, and cannot be changed after cluster creation.

    c. Select a cluster version from the **Version** drop-down menu.

    d. Select a cloud provider region from the **Region** drop-down menu.

    e. Select a **Single zone** or **Multi-zone** configuration.

    f. Optional: Select **Enable Secure Boot for Shielded VMs** to use Shielded VMs when installing your cluster. For more information, see Shielded VMs.

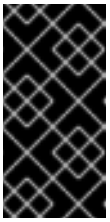
    IMPORTANT

    To successfully create a cluster, you must select **Enable Secure Boot support for Shielded VMs** if your organization has the policy constraint **constraints/compute.requireShieldedVm** enabled. For more information regarding GCP organizational policy constraints, see Organization policy constraints.

    g. Leave **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat Site Reliability Engineer (SRE) platform metrics. This option is enabled by default.

6. Optional: Expand **Advanced Encryption** to make changes to encryption settings.

    a. Select **Use Custom KMS keys** to use custom KMS keys. If you prefer not to use custom KMS keys, leave the default setting **Use default KMS Keys**.



IMPORTANT

To use custom KMS keys, the IAM service account **osd-ccs-admin** must be granted the **Cloud KMS CryptoKey Encrypter/Decrypter** role. For more information about granting roles on a resource, see Granting roles on a resource.

With **Use Custom KMS keys** selected:

i. Select a key ring location from the **Key ring location** drop-down menu.

ii. Select a key ring from the **Key ring** drop-down menu.

iii. Select a key name from the **Key name** drop-down menu.

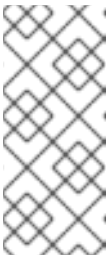
iv. Provide the **KMS Service Account**

b. Optional: Select **Enable FIPS cryptography** if you require your cluster to be FIPS validated.

NOTE

If **Enable FIPS cryptography** is selected, **Enable additional etcd encryption** is enabled by default and cannot be disabled. You can select **Enable additional etcd encryption** without selecting **Enable FIPS cryptography**.

c. Optional: Select **Enable additional etcd encryption** if you require etcd key value encryption. With this option, the etcd key values are encrypted, but the keys are not. This option is in addition to the control plane storage encryption that encrypts the etcd volumes in OpenShift Dedicated clusters by default.



NOTE

By enabling etcd encryption for the key values in etcd, you incur a performance overhead of approximately 20%. The overhead is a result of introducing this second layer of encryption, in addition to the default control plane storage encryption that encrypts the etcd volumes. Consider enabling etcd encryption only if you specifically require it for your use case.

7. Click **Next**.

8. On the **Machine pool** page, select a **Compute node instance type** and a **Compute node count**. The number and types of nodes that are available depend on your OpenShift Dedicated subscription. If you are using multiple availability zones, the compute node count is per zone.

NOTE

After your cluster is created, you can change the number of compute nodes, but you cannot change the compute node instance type in a created machine pool. You can add machine pools after installation that use a customized instance type. The number and types of nodes available to you depend on your OpenShift Dedicated subscription.

9. Optional: Expand **Add node labels** to add labels to your nodes. Click **Add additional label** to add more node labels.

10. Click **Next**.

11. In the **Cluster privacy** dialog, select **Public** or **Private** to use either public or private API endpoints and application routes for your cluster.

12. Optional: To install the cluster in an existing GCP Virtual Private Cloud (VPC):

    a. Select **Install into an existing VPC**.

    b. If you are installing into an existing VPC and you want to enable an HTTP or HTTPS proxy for your cluster, select **Configure a cluster-wide proxy**.

13. Click **Next**.

14. Optional: To install the cluster into a GCP Shared VPC:

IMPORTANT

To install a cluster into a Shared VPC, you must use OpenShift Dedicated version 4.13.15 or above. Additionally, the VPC owner of the host project must enable a project as a host project in their Google Cloud console. For more information, see Enable a host project .

    a. Select **Install into GCP Shared VPC**.

    b. Specify the **Host project ID**. If the specified host project ID is incorrect, cluster creation fails.

IMPORTANT

Once you complete the steps within the cluster configuration wizard and click **Create Cluster**, the cluster will go into the "Installation Waiting" state. At this point, you must contact the VPC owner of the host project, who must assign the dynamically-generated service account the following roles: **Compute Network Administrator**, **Compute Security Administrator**, and **DNS Administrator**. The VPC owner of the host project has 30 days to grant the listed permissions before the cluster creation fails. For information about Shared VPC permissions, see Provision Shared VPC.

15. If you opted to install the cluster in an existing GCP VPC, provide your **Virtual Private Cloud (VPC) subnet settings** and select **Next**. You must have created the Cloud network address translation (NAT) and a Cloud router. See the "Additional resources" section for information about Cloud NATs and Google VPCs.

NOTE

If you are installing a cluster into a Shared VPC, the VPC name and subnets are shared from the host project.

16. Click **Next**.

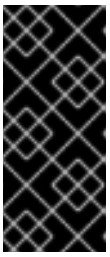
17. If you opted to configure a cluster-wide proxy, provide your proxy configuration details on the **Cluster-wide proxy** page:

    a. Enter a value in at least one of the following fields:

- Specify a valid **HTTP proxy URL**
- Specify a valid **HTTPS proxy URL**
- In the **Additional trust bundle** field, provide a PEM encoded X.509 certificate bundle. The bundle is added to the trusted certificate store for the cluster nodes. An additional trust bundle file is required if you use a TLS-inspecting proxy unless the identity certificate for the proxy is signed by an authority from the Red Hat Enterprise Linux CoreOS (RHCOS) trust bundle. This requirement applies regardless of whether the proxy is transparent or requires explicit configuration using the **http-proxy** and **https-proxy** arguments.

b. Click **Next**.
For more information about configuring a proxy with OpenShift Dedicated, see *Configuring a cluster-wide proxy*.

18. In the **CIDR ranges** dialog, configure custom classless inter-domain routing (CIDR) ranges or use the defaults that are provided.



IMPORTANT

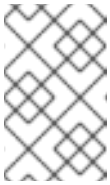
CIDR configurations cannot be changed later. Confirm your selections with your network administrator before proceeding.

If the cluster privacy is set to **Private**, you cannot access your cluster until you configure private connections in your cloud provider.

19. On the **Cluster update strategy** page, configure your update preferences:

a. Choose a cluster update method:

- Select **Individual updates** if you want to schedule each update individually. This is the default option.
- Select **Recurring updates** to update your cluster on your preferred day and start time, when updates are available.



NOTE

You can review the end-of-life dates in the update lifecycle documentation for OpenShift Dedicated. For more information, see OpenShift Dedicated update life cycle.

b. Provide administrator approval based on your cluster update method:

- Individual updates: If you select an update version that requires approval, provide an administrator's acknowledgment and click **Approve and continue**.
- Recurring updates: If you selected recurring updates for your cluster, provide an administrator's acknowledgment and click **Approve and continue**. OpenShift Cluster Manager does not start scheduled y-stream updates for minor versions without receiving an administrator's acknowledgment.

c. If you opted for recurring updates, select a preferred day of the week and upgrade start time in UTC from the drop-down menus.

d. Optional: You can set a grace period for **Node draining** during cluster upgrades. A **1 hour** grace period is set by default.

e. Click **Next**.

NOTE

In the event of critical security concerns that significantly impact the security or stability of a cluster, Red Hat Site Reliability Engineering (SRE) might schedule automatic updates to the latest z-stream version that is not impacted. The updates are applied within 48 hours after customer notifications are provided. For a description of the critical impact security rating, see Understanding Red Hat security ratings .

20. Review the summary of your selections and click **Create cluster** to start the cluster installation. The installation takes approximately 30-40 minutes to complete.

21. Optional: On the **Overview** tab, you can enable the delete protection feature by selecting **Enable**, which is located directly under **Delete Protection: Disabled**. This will prevent your cluster from being deleted. To disable delete protection, select **Disable**. By default, clusters are created with the delete protection feature disabled.

Verification

- You can monitor the progress of the installation in the **Overview** page for your cluster. You can view the installation logs on the same page. Your cluster is ready when the **Status** in the **Details** section of the page is listed as **Ready**.

2.4. CREATING A CLUSTER ON GCP WITH A RED HAT CLOUD ACCOUNT

Through OpenShift Cluster Manager, you can create an OpenShift Dedicated cluster on Google Cloud Platform (GCP) using a standard cloud provider account owned by Red Hat.

Procedure

1. Log in to OpenShift Cluster Manager and click **Create cluster**.
2. In the **Cloud** tab, click **Create cluster** in the **Red Hat OpenShift Dedicated** row.
3. Under **Billing model**, configure the subscription type and infrastructure type:

   a. Select the **Annual** subscription type. Only the **Annual** subscription type is available when you deploy a cluster using a Red Hat cloud account.
   For information about OpenShift Dedicated subscription options, see Cluster subscriptions and registration in the OpenShift Cluster Manager documentation.

NOTE

You must have the required resource quota for the **Annual** subscription type to be available. For more information, contact your sales representative or Red Hat support.

b. Select the **Red Hat cloud account**infrastructure type to deploy OpenShift Dedicated in a cloud provider account that is owned by Red Hat.

c. Click **Next**.

4. Select **Run on Google Cloud Platform**and click **Next**.

5. On the **Cluster details** page, provide a name for your cluster and specify the cluster details:

a. Add a **Cluster name**.

b. Optional: Cluster creation generates a domain prefix as a subdomain for your provisioned cluster on **openshiftapps.com**. If the cluster name is less than or equal to 15 characters, that name is used for the domain prefix. If the cluster name is longer than 15 characters, the domain prefix is randomly generated as a 15-character string.
To customize the subdomain, select the **Create custom domain prefix**checkbox, and enter your domain prefix name in the **Domain prefix** field. The domain prefix cannot be longer than 15 characters, must be unique within your organization, and cannot be changed after cluster creation.

c. Select a cluster version from the **Version** drop-down menu.

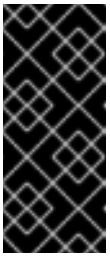
d. Select a cloud provider region from the **Region** drop-down menu.

e. Select a **Single zone** or **Multi-zone** configuration.

f. Select a **Persistent storage** capacity for the cluster. For more information, see the *Storage* section in the OpenShift Dedicated service definition.

g. Specify the number of **Load balancers** that you require for your cluster. For more information, see the *Load balancers* section in the OpenShift Dedicated service definition.

h. Optional: Select **Enable Secure Boot for Shielded VMs**to use Shielded VMs when installing your cluster. For more information, see Shielded VMs.



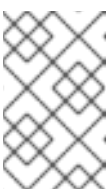
IMPORTANT

To successfully create a cluster, you must select **Enable Secure Boot support for Shielded VMs** if your organization has the policy constraint **constraints/compute.requireShieldedVm** enabled. For more information regarding GCP organizational policy constraints, see Organization policy constraints.

i. Leave **Enable user workload monitoring**selected to monitor your own projects in isolation from Red Hat Site Reliability Engineer (SRE) platform metrics. This option is enabled by default.

6. Optional: Expand **Advanced Encryption** to make changes to encryption settings.

a. Optional: Select **Enable FIPS cryptography**if you require your cluster to be FIPS validated.



NOTE

If **Enable FIPS cryptography**is selected, **Enable additional etcd encryption** is enabled by default and cannot be disabled. You can select **Enable additional etcd encryption** without selecting **Enable FIPS cryptography**.

b. Optional: Select **Enable additional etcd encryption** if you require etcd key value encryption. With this option, the etcd key values are encrypted, but not the keys. This option is in addition to the control plane storage encryption that encrypts the etcd volumes in OpenShift Dedicated clusters by default.

NOTE

By enabling etcd encryption for the key values in etcd, you will incur a performance overhead of approximately 20%. The overhead is a result of introducing this second layer of encryption, in addition to the default control plane storage encryption that encrypts the etcd volumes. Consider enabling etcd encryption only if you specifically require it for your use case.

c. Click **Next**.

7. On the **Default machine pool** page, select a **Compute node instance type** and a **Compute node count**. The number and types of nodes that are available depend on your OpenShift Dedicated subscription. If you are using multiple availability zones, the compute node count is per zone.

NOTE

After your cluster is created, you can change the number of compute nodes, but you cannot change the compute node instance type in a machine pool. For clusters that use the CCS model, you can add machine pools after installation that use a different instance type. The number and types of nodes available to you depend on your OpenShift Dedicated subscription.

8. Optional: Expand **Edit node labels** to add labels to your nodes. Click **Add label** to add more node labels and select **Next**.

9. In the **Cluster privacy** dialog, select **Public** or **Private** to use either public or private API endpoints and application routes for your cluster.

10. Click **Next**.

11. In the **CIDR ranges** dialog, configure custom classless inter-domain routing (CIDR) ranges or use the defaults that are provided.

IMPORTANT

CIDR configurations cannot be changed later. Confirm your selections with your network administrator before proceeding.

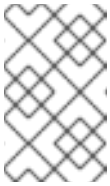
If the cluster privacy is set to **Private**, you cannot access your cluster until you configure private connections in your cloud provider.

12. On the **Cluster update strategy** page, configure your update preferences:

a. Choose a cluster update method:

- Select **Individual updates** if you want to schedule each update individually. This is the default option.

- Select **Recurring updates** to update your cluster on your preferred day and start time, when updates are available.



NOTE

You can review the end-of-life dates in the update lifecycle documentation for OpenShift Dedicated. For more information, see OpenShift Dedicated update life cycle .

b. Provide administrator approval based on your cluster update method:

- Individual updates: If you select an update version that requires approval, provide an administrator's acknowledgment and click **Approve and continue**.
- Recurring updates: If you selected recurring updates for your cluster, provide an administrator's acknowledgment and click **Approve and continue**. OpenShift Cluster Manager does not start scheduled y-stream updates for minor versions without receiving an administrator's acknowledgment.

c. If you opted for recurring updates, select a preferred day of the week and upgrade start time in UTC from the drop-down menus.

d. Optional: You can set a grace period for **Node draining** during cluster upgrades. A **1 hour** grace period is set by default.

e. Click **Next**.

NOTE

In the event of critical security concerns that significantly impact the security or stability of a cluster, Red Hat Site Reliability Engineering (SRE) might schedule automatic updates to the latest z-stream version that is not impacted. The updates are applied within 48 hours after customer notifications are provided. For a description of the critical impact security rating, see Understanding Red Hat security ratings .

13. Review the summary of your selections and click **Create cluster** to start the cluster installation. The installation takes approximately 30-40 minutes to complete.

14. Optional: On the **Overview** tab, you can enable the delete protection feature by selecting **Enable**, which is located directly under **Delete Protection: Disabled**. This will prevent your cluster from being deleted. To disable delete protection, select **Disable**. By default, clusters are created with the delete protection feature disabled.

Verification

- You can monitor the progress of the installation in the **Overview** page for your cluster. You can view the installation logs on the same page. Your cluster is ready when the **Status** in the **Details** section of the page is listed as **Ready**.

2.5. CREATING A CLUSTER ON GCP WITH RED HAT MARKETPLACE

When creating an OpenShift Dedicated (OSD) cluster on Google Cloud through the OpenShift Cluster Manager Hybrid Cloud Console, customers can select Red Hat Marketplace as their preferred billing model. OSD pricing is consumption-based and customers are billed directly through their Red Hat

Marketplace account.

Procedure

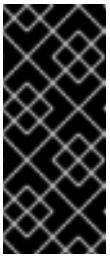
1. Log in to OpenShift Cluster Manager and click **Create cluster**.
2. In the **Cloud** tab, click **Create cluster** in the **Red Hat OpenShift Dedicated** row.
3. Under **Billing model**, configure the subscription type and infrastructure type:
   a. Select the **On-Demand** subscription type.
   b. From the drop-down menu, select **Red Hat Marketplace**.
   c. Click **Next**.
4. On the **Cloud provider** page:
   a. Select **Google Cloud** as your cloud provider.
   b. Click the checkbox indicating that you have read and completed all the prerequisites necessary to continue creating your cluster.
   c. Add your service account key.

   NOTE

   For more information about service account keys, click the information icon located next to **Service account key**.

   d. Click **Next** to validate your cloud provider account and go to the **Cluster details** page.
5. On the **Cluster details** page, provide a name for your cluster and specify the cluster details:
   a. Add a **Cluster name**.
   b. Optional: Cluster creation generates a domain prefix as a subdomain for your provisioned cluster on **openshiftapps.com**. If the cluster name is less than or equal to 15 characters, that name is used for the domain prefix. If the cluster name is longer than 15 characters, the domain prefix is randomly generated as a 15-character string.
   To customize the subdomain, select the **Create custom domain prefix** checkbox, and enter your domain prefix name in the **Domain prefix** field. The domain prefix cannot be longer than 15 characters, must be unique within your organization, and cannot be changed after cluster creation.
   c. Select a cluster version from the **Version** drop-down menu.
   d. Select a cloud provider region from the **Region** drop-down menu.
   e. Select a **Single zone** or **Multi-zone** configuration.
   f. Optional: Select **Enable Secure Boot for Shielded VMs** to use Shielded VMs when installing your cluster. For more information, see Shielded VMs.



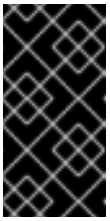
IMPORTANT

To successfully create a cluster, you must select **Enable Secure Boot support for Shielded VMs** if your organization has the policy constraint **constraints/compute.requireShieldedVm** enabled. For more information regarding GCP organizational policy constraints, see Organization policy constraints.

g. Leave **Enable user workload monitoring** selected to monitor your own projects in isolation from Red Hat Site Reliability Engineer (SRE) platform metrics. This option is enabled by default.

6. Optional: Expand **Advanced Encryption** to make changes to encryption settings.

a. Select **Use Custom KMS keys** to use custom KMS keys. If you prefer not to use custom KMS keys, leave the default setting **Use default KMS Keys**.



IMPORTANT

To use custom KMS keys, the IAM service account **osd-ccs-admin** must be granted the **Cloud KMS CryptoKey Encrypter/Decrypter** role. For more information about granting roles on a resource, see Granting roles on a resource.

With **Use Custom KMS keys** selected:

i. Select a key ring location from the **Key ring location** drop-down menu.

ii. Select a key ring from the **Key ring** drop-down menu.

iii. Select a key name from the **Key name** drop-down menu.

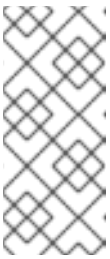
iv. Provide the **KMS Service Account**

b. Optional: Select **Enable FIPS cryptography** if you require your cluster to be FIPS validated.

NOTE

If **Enable FIPS cryptography** is selected, **Enable additional etcd encryption** is enabled by default and cannot be disabled. You can select **Enable additional etcd encryption** without selecting **Enable FIPS cryptography**.

c. Optional: Select **Enable additional etcd encryption** if you require etcd key value encryption. With this option, the etcd key values are encrypted, but not the keys. This option is in addition to the control plane storage encryption that encrypts the etcd volumes in OpenShift Dedicated clusters by default.



NOTE

By enabling etcd encryption for the key values in etcd, you incur a performance overhead of approximately 20%. The overhead is a result of introducing this second layer of encryption, in addition to the default control plane storage encryption that encrypts the etcd volumes. Consider enabling etcd encryption only if you specifically require it for your use case.

7. Click **Next**.

8. On the **Machine pool** page, select a **Compute node instance type** and a **Compute node count**. The number and types of nodes that are available depend on your OpenShift Dedicated subscription. If you are using multiple availability zones, the compute node count is per zone.

NOTE

After your cluster is created, you can change the number of compute nodes, but you cannot change the compute node instance type in a created machine pool. You can add machine pools after installation that use a customized instance type. The number and types of nodes available to you depend on your OpenShift Dedicated subscription.

9. Optional: Expand **Add node labels** to add labels to your nodes. Click **Add additional label** to add more node labels.

10. Click **Next**.

11. In the **Cluster privacy** dialog, select **Public** or **Private** to use either public or private API endpoints and application routes for your cluster.

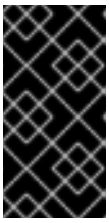
12. Optional: To install the cluster in an existing GCP Virtual Private Cloud (VPC):

    a. Select **Install into an existing VPC**.

    b. If you are installing into an existing VPC and you want to enable an HTTP or HTTPS proxy for your cluster, select **Configure a cluster-wide proxy**.

13. Click **Next**.

14. Optional: To install the cluster into a GCP Shared VPC:

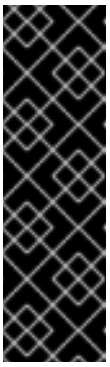


IMPORTANT

To install a cluster into a Shared VPC, you must use OpenShift Dedicated version 4.13.15 or above. Additionally, the VPC owner of the host project must enable a project as a host project in their Google Cloud console. For more information, see Enable a host project .

    a. Select **Install into GCP Shared VPC**.

    b. Specify the **Host project ID**. If the specified host project ID is incorrect, cluster creation fails.



IMPORTANT

Once you complete the steps within the cluster configuration wizard and click **Create Cluster**, the cluster will go into the "Installation Waiting" state. At this point, you must contact the VPC owner of the host project, who must assign the dynamically-generated service account the following roles: **Compute Network Administrator**, **Compute Security Administrator**, and **DNS Administrator**. The VPC owner of the host project has 30 days to grant the listed permissions before the cluster creation fails. For information about Shared VPC permissions, see Provision Shared VPC.

15. If you opted to install the cluster in an existing GCP VPC, provide your **Virtual Private Cloud (VPC) subnet settings** and select **Next**. You must have created the Cloud network address translation (NAT) and a Cloud router. See the "Additional resources" section for information about Cloud NATs and Google VPCs.

NOTE

If you are installing a cluster into a Shared VPC, the VPC name and subnets are shared from the host project.

16. Click **Next**.

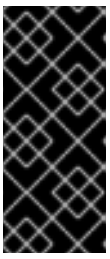
17. If you opted to configure a cluster-wide proxy, provide your proxy configuration details on the **Cluster-wide proxy** page:

    a. Enter a value in at least one of the following fields:

    - Specify a valid **HTTP proxy URL**
    - Specify a valid **HTTPS proxy URL**
    - In the **Additional trust bundle** field, provide a PEM encoded X.509 certificate bundle. The bundle is added to the trusted certificate store for the cluster nodes. An additional trust bundle file is required if you use a TLS-inspecting proxy unless the identity certificate for the proxy is signed by an authority from the Red Hat Enterprise Linux CoreOS (RHCOS) trust bundle. This requirement applies regardless of whether the proxy is transparent or requires explicit configuration using the **http-proxy** and **https-proxy** arguments.

    b. Click **Next**.
    For more information about configuring a proxy with OpenShift Dedicated, see *Configuring a cluster-wide proxy*.

18. In the **CIDR ranges** dialog, configure custom classless inter-domain routing (CIDR) ranges or use the defaults that are provided.



IMPORTANT

CIDR configurations cannot be changed later. Confirm your selections with your network administrator before proceeding.

If the cluster privacy is set to **Private**, you cannot access your cluster until you configure private connections in your cloud provider.

19. On the **Cluster update strategy** page, configure your update preferences:

    a. Choose a cluster update method:

    - Select **Individual updates** if you want to schedule each update individually. This is the default option.
    - Select **Recurring updates** to update your cluster on your preferred day and start time, when updates are available.

NOTE

You can review the end-of-life dates in the update lifecycle documentation for OpenShift Dedicated. For more information, see OpenShift Dedicated update life cycle .

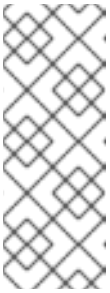
b. Provide administrator approval based on your cluster update method:

- Individual updates: If you select an update version that requires approval, provide an administrator's acknowledgment and click **Approve and continue**.
- Recurring updates: If you selected recurring updates for your cluster, provide an administrator's acknowledgment and click **Approve and continue**. OpenShift Cluster Manager does not start scheduled y-stream updates for minor versions without receiving an administrator's acknowledgment.

c. If you opted for recurring updates, select a preferred day of the week and upgrade start time in UTC from the drop-down menus.

d. Optional: You can set a grace period for **Node draining** during cluster upgrades. A **1 hour** grace period is set by default.

e. Click **Next**.



NOTE

In the event of critical security concerns that significantly impact the security or stability of a cluster, Red Hat Site Reliability Engineering (SRE) might schedule automatic updates to the latest z-stream version that is not impacted. The updates are applied within 48 hours after customer notifications are provided. For a description of the critical impact security rating, see Understanding Red Hat security ratings .

20. Review the summary of your selections and click **Create cluster** to start the cluster installation. The installation takes approximately 30-40 minutes to complete.

21. Optional: On the **Overview** tab, you can enable the delete protection feature by selecting **Enable**, which is located directly under **Delete Protection: Disabled**. This will prevent your cluster from being deleted. To disable delete protection, select **Disable**. By default, clusters are created with the delete protection feature disabled.

Verification

- You can monitor the progress of the installation in the **Overview** page for your cluster. You can view the installation logs on the same page. Your cluster is ready when the **Status** in the **Details** section of the page is listed as **Ready**.

2.6. ADDITIONAL RESOURCES

- For information about configuring a proxy with OpenShift Dedicated, see Configuring a cluster-wide proxy.
- For information about persistent storage for OpenShift Dedicated, see the Storage section in the OpenShift Dedicated service definition.

- For information about load balancers for OpenShift Dedicated, see the Load balancers section in the OpenShift Dedicated service definition.
- For more information about etcd encryption, see the etcd encryption service definition .
- For information about the end-of-life dates for OpenShift Dedicated versions, see the OpenShift Dedicated update life cycle .
- For general information on Cloud network address translation(NAT) that is required for cluster-wide proxy, see Cloud NAT overview in the Google documentation.
- For general information on Cloud routers that are required for the cluster-wide proxy, see Cloud Router overview in the Google documentation.
- For information on creating VPCs within your Google Cloud Provider account, see Create and manage VPC networks in the Google documentation.

CHAPTER 3. CONFIGURING IDENTITY PROVIDERS

After your OpenShift Dedicated cluster is created, you must configure identity providers to determine how users log in to access the cluster.

3.1. UNDERSTANDING IDENTITY PROVIDERS

OpenShift Dedicated includes a built-in OAuth server. Developers and administrators obtain OAuth access tokens to authenticate themselves to the API. As an administrator, you can configure OAuth to specify an identity provider after you install your cluster. Configuring identity providers allows users to log in and access the cluster.

3.1.1. Supported identity providers

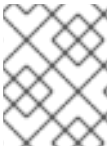
You can configure the following types of identity providers:

Identity provider	Description
GitHub or GitHub Enterprise	Configure a GitHub identity provider to validate usernames and passwords against GitHub or GitHub Enterprise's OAuth authentication server.
GitLab	Configure a GitLab identity provider to use GitLab.com or any other GitLab instance as an identity provider.
Google	Configure a Google identity provider using Google's OpenID Connect integration.
LDAP	Configure an LDAP identity provider to validate usernames and passwords against an LDAPv3 server, using simple bind authentication.
OpenID Connect	Configure an OpenID Connect (OIDC) identity provider to integrate with an OIDC identity provider using an Authorization Code Flow.
htpasswd	Configure an htpasswd identity provider for a single, static administration user. You can log in to the cluster as the user to troubleshoot issues.  **IMPORTANT** The htpasswd identity provider option is included only to enable the creation of a single, static administration user. htpasswd is not supported as a general-use identity provider for OpenShift Dedicated. For the steps to configure the single user, see *Configuring an htpasswd identity provider*.

3.1.2. Identity provider parameters

The following parameters are common to all identity providers:

Parameter	Description
name	The provider name is prefixed to provider user names to form an identity name.
mappingMethod	Defines how new identities are mapped to users when they log in. Enter one of the following values: **claim** The default value. Provisions a user with the identity's preferred user name. Fails if a user with that user name is already mapped to another identity. **lookup** Looks up an existing identity, user identity mapping, and user, but does not automatically provision users or identities. This allows cluster administrators to set up identities and users manually, or using an external process. Using this method requires you to manually provision users. **add** Provisions a user with the identity's preferred user name. If a user with that user name already exists, the identity is mapped to the existing user, adding to any existing identity mappings for the user. Required when multiple identity providers are configured that identify the same set of users and map to the same user names.



NOTE

When adding or changing identity providers, you can map identities from the new provider to existing users by setting the **mappingMethod** parameter to **add**.

3.2. CONFIGURING A GITHUB IDENTITY PROVIDER

Configure a GitHub identity provider to validate user names and passwords against GitHub or GitHub Enterprise's OAuth authentication server and access your OpenShift Dedicated cluster. OAuth facilitates a token exchange flow between OpenShift Dedicated and GitHub or GitHub Enterprise.

WARNING

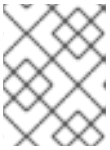
Configuring GitHub authentication allows users to log in to OpenShift Dedicated with their GitHub credentials. To prevent anyone with any GitHub user ID from logging in to your OpenShift Dedicated cluster, you must restrict access to only those in specific GitHub organizations or teams.

Prerequisites

- The OAuth application must be created directly within the GitHub organization settings by the GitHub organization administrator.
- GitHub organizations or teams are set up in your GitHub account.

Procedure

1. From OpenShift Cluster Manager, navigate to the **Cluster List** page and select the cluster that you need to configure identity providers for.
2. Click the **Access control** tab.
3. Click **Add identity provider**.



NOTE

You can also click the **Add Oauth configuration** link in the warning message displayed after cluster creation to configure your identity providers.

4. Select **GitHub** from the drop-down menu.
5. Enter a unique name for the identity provider. This name cannot be changed later.
   - An **OAuth callback URL** is automatically generated in the provided field. You will use this to register the GitHub application.

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     For example:

     ```
     https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/github
     ```

6. Register an application on GitHub.
7. Return to OpenShift Dedicated and select a mapping method from the drop-down menu. **Claim** is recommended in most cases.
8. Enter the **Client ID** and **Client secret** provided by GitHub.
9. Enter a **hostname**. A hostname must be entered when using a hosted instance of GitHub Enterprise.
10. Optional: You can use a certificate authority (CA) file to validate server certificates for the configured GitHub Enterprise URL. Click **Browse** to locate and attach a **CA file** to the identity provider.
11. Select **Use organizations** or **Use teams** to restrict access to a particular GitHub organization or a GitHub team.
12. Enter the name of the organization or team you would like to restrict access to. Click **Add more** to specify multiple organizations or teams that users can be a member of.
13. Click **Confirm**.

Verification

- The configured identity provider is now visible on the **Access control** tab of the **Cluster List** page.

3.3. CONFIGURING A GITLAB IDENTITY PROVIDER

Configure a GitLab identity provider to use GitLab.com or any other GitLab instance as an identity provider.

Prerequisites

- If you use GitLab version 7.7.0 to 11.0, you connect using the OAuth integration. If you use GitLab version 11.1 or later, you can use OpenID Connect (OIDC) to connect instead of OAuth.

Procedure

1. From OpenShift Cluster Manager, navigate to the **Cluster List** page and select the cluster that you need to configure identity providers for.
2. Click the **Access control** tab.
3. Click **Add identity provider**.

NOTE

You can also click the **Add Oauth configuration** link in the warning message displayed after cluster creation to configure your identity providers.

4. Select **GitLab** from the drop-down menu.
5. Enter a unique name for the identity provider. This name cannot be changed later.
   - An **OAuth callback URL** is automatically generated in the provided field. You will provide this URL to GitLab.

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     For example:

     ```
     https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/gitlab
     ```

6. Add a new application in GitLab .
7. Return to OpenShift Dedicated and select a mapping method from the drop-down menu. **Claim** is recommended in most cases.
8. Enter the **Client ID** and **Client secret** provided by GitLab.
9. Enter the **URL** of your GitLab provider.
10. Optional: You can use a certificate authority (CA) file to validate server certificates for the configured GitLab URL. Click **Browse** to locate and attach a **CA file** to the identity provider.
11. Click **Confirm**.

Verification

- The configured identity provider is now visible on the **Access control** tab of the **Cluster List** page.

3.4. CONFIGURING A GOOGLE IDENTITY PROVIDER

Configure a Google identity provider to allow users to authenticate with their Google credentials.

WARNING

Using Google as an identity provider allows any Google user to authenticate to your server. You can limit authentication to members of a specific hosted domain with the **hostedDomain** configuration attribute.

Procedure

1. From OpenShift Cluster Manager, navigate to the **Cluster List** page and select the cluster that you need to configure identity providers for.
2. Click the **Access control** tab.
3. Click **Add identity provider**.

NOTE

You can also click the **Add Oauth configuration** link in the warning message displayed after cluster creation to configure your identity providers.

4. Select **Google** from the drop-down menu.
5. Enter a unique name for the identity provider. This name cannot be changed later.
   - An **OAuth callback URL** is automatically generated in the provided field. You will provide this URL to Google.

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     For example:

     ```
     https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/google
     ```

6. Configure a Google identity provider using Google's OpenID Connect integration.
7. Return to OpenShift Dedicated and select a mapping method from the drop-down menu. **Claim** is recommended in most cases.
8. Enter the **Client ID** of a registered Google project and the **Client secret** issued by Google.
9. Enter a hosted domain to restrict users to a Google Apps domain.
10. Click **Confirm**.

Verification

- The configured identity provider is now visible on the **Access control** tab of the **Cluster List** page.

3.5. CONFIGURING A LDAP IDENTITY PROVIDER

Configure the LDAP identity provider to validate user names and passwords against an LDAPv3 server, using simple bind authentication.

Prerequisites

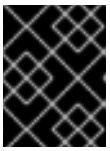
- When configuring a LDAP identity provider, you will need to enter a configured **LDAP URL**. The configured URL is an RFC 2255 URL, which specifies the LDAP host and search parameters to use. The syntax of the URL is:

```
ldap://host:port/basedn?attribute?scope?filter
```

URL component	Description
ldap	For regular LDAP, use the string **ldap**. For secure LDAP (LDAPS), use **ldaps** instead.
host:port	The name and port of the LDAP server. Defaults to **localhost:389** for ldap and **localhost:636** for LDAPS.
basedn	The DN of the branch of the directory where all searches should start from. At the very least, this must be the top of your directory tree, but it could also specify a subtree in the directory.
attribute	The attribute to search for. Although RFC 2255 allows a comma-separated list of attributes, only the first attribute will be used, no matter how many are provided. If no attributes are provided, the default is to use **uid**. It is recommended to choose an attribute that will be unique across all entries in the subtree you will be using.
scope	The scope of the search. Can be either **one** or **sub**. If the scope is not provided, the default is to use a scope of **sub**.
filter	A valid LDAP search filter. If not provided, defaults to **(objectClass=*)**

When doing searches, the attribute, filter, and provided user name are combined to create a search filter that looks like:

```
(&(<filter>)(<attribute>=<username>))
```



IMPORTANT

If the LDAP directory requires authentication to search, specify a **bindDN** and **bindPassword** to use to perform the entry search.

Procedure

1. From OpenShift Cluster Manager, navigate to the **Cluster List** page and select the cluster that you need to configure identity providers for.
2. Click the **Access control** tab.
3. Click **Add identity provider**.

NOTE

You can also click the **Add Oauth configuration** link in the warning message displayed after cluster creation to configure your identity providers.

4. Select **LDAP** from the drop-down menu.
5. Enter a unique name for the identity provider. This name cannot be changed later.
6. Select a mapping method from the drop-down menu. **Claim** is recommended in most cases.
7. Enter a **LDAP URL** to specify the LDAP search parameters to use.
8. Optional: Enter a **Bind DN** and **Bind password**.
9. Enter the attributes that will map LDAP attributes to identities.
    - Enter an **ID** attribute whose value should be used as the user ID. Click **Add more** to add multiple ID attributes.
    - Optional: Enter a **Preferred username** attribute whose value should be used as the display name. Click **Add more** to add multiple preferred username attributes.
    - Optional: Enter an **Email** attribute whose value should be used as the email address. Click **Add more** to add multiple email attributes.
10. Optional: Click **Show advanced Options** to add a certificate authority (CA) file to your LDAP identity provider to validate server certificates for the configured URL. Click **Browse** to locate and attach a **CA file** to the identity provider.
11. Optional: Under the advanced options, you can choose to make the LDAP provider **Insecure**. If you select this option, a CA file cannot be used.

IMPORTANT

If you are using an insecure LDAP connection (ldap:// or port 389), then you must check the **Insecure** option in the configuration wizard.

12. Click **Confirm**.

Verification

- The configured identity provider is now visible on the **Access control** tab of the **Cluster List** page.

3.6. CONFIGURING AN OPENID IDENTITY PROVIDER

Configure an OpenID identity provider to integrate with an OpenID Connect identity provider using an Authorization Code Flow.

IMPORTANT

The Authentication Operator in OpenShift Dedicated requires that the configured OpenID Connect identity provider implements the OpenID Connect Discovery specification.

Claims are read from the JWT **id_token** returned from the OpenID identity provider and, if specified, from the JSON returned by the Issuer URL.

At least one claim must be configured to use as the user's identity.

You can also indicate which claims to use as the user's preferred user name, display name, and email address. If multiple claims are specified, the first one with a non-empty value is used. The standard claims are:

Claim	Description
preferred_username	The preferred user name when provisioning a user. A shorthand name that the user wants to be referred to as, such as **janedoe**. Typically a value that corresponding to the user's login or username in the authentication system, such as username or email.
email	Email address.
name	Display name.

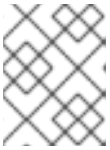
See the OpenID claims documentation for more information.

Prerequisites

- Before you configure OpenID Connect, check the installation prerequisites for any Red Hat product or service you want to use with your OpenShift Dedicated cluster.

Procedure

1. From OpenShift Cluster Manager, navigate to the **Cluster List** page and select the cluster that you need to configure identity providers for.
2. Click the **Access control** tab.
3. Click **Add identity provider**.



NOTE

You can also click the **Add Oauth configuration** link in the warning message displayed after cluster creation to configure your identity providers.

4. Select **OpenID** from the drop-down menu.

5. Enter a unique name for the identity provider. This name cannot be changed later.
   - An **OAuth callback URL** is automatically generated in the provided field.

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     For example:

     ```
     https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/openid
     ```

6. Register a new OpenID Connect client in the OpenID identity provider by following the steps to create an authorization request .
7. Return to OpenShift Dedicated and select a mapping method from the drop-down menu. **Claim** is recommended in most cases.
8. Enter a **Client ID** and **Client secret** provided from OpenID.
9. Enter an **Issuer URL**. This is the URL that the OpenID provider asserts as the Issuer Identifier. It must use the https scheme with no URL query parameters or fragments.
10. Enter an **Email** attribute whose value should be used as the email address. Click **Add more** to add multiple email attributes.
11. Enter a **Name** attribute whose value should be used as the preferred username. Click **Add more** to add multiple preferred usernames.
12. Enter a **Preferred username** attribute whose value should be used as the display name. Click **Add more** to add multiple display names.
13. Optional: Click **Show advanced Options** to add a certificate authority (CA) file to your OpenID identity provider.
14. Optional: Under the advanced options, you can add **Additional scopes**. By default, the **OpenID** scope is requested.
15. Click **Confirm**.

Verification

- The configured identity provider is now visible on the **Access control** tab of the **Cluster List** page.

3.7. CONFIGURING AN HTPASSWD IDENTITY PROVIDER

Configure an htpasswd identity provider to create a single, static user with cluster administration privileges. You can log in to your cluster as the user to troubleshoot issues.

IMPORTANT

The htpasswd identity provider option is included only to enable the creation of a single, static administration user. htpasswd is not supported as a general-use identity provider for OpenShift Dedicated.

Procedure

1. From OpenShift Cluster Manager, navigate to the **Cluster List** page and select your cluster.
2. Select **Access control → Identity providers**.
3. Click **Add identity provider**.
4. Select **HTPasswd** from the **Identity Provider** drop-down menu.
5. Add a unique name in the **Name** field for the identity provider.
6. Use the suggested username and password for the static user, or create your own.

NOTE

The credentials defined in this step are not visible after you select **Add** in the following step. If you lose the credentials, you must recreate the identity provider and define the credentials again.

7. Select **Add** to create the htpasswd identity provider and the single, static user.
8. Grant the static user permission to manage the cluster:
   a. Under **Access control → Cluster Roles and Access**, select **Add user**.
   b. Enter the **User ID** of the static user that you created in the preceding step.
   c. Select a **Group.**
      - If you are installing OpenShift Dedicated using the Customer Cloud Subscription (CCS) infrastructure type, choose either the **dedicated-admins** or **cluster-admins** group. Users in the **dedicated-admins** group have standard administrative privileges for OpenShift Dedicated. Users in the **cluster-admins** group have full administrative access to the cluster.
      - If you are installing OpenShift Dedicated using the Red Hat cloud account infrastructure type, the **dedicated-admins** group is automatically selected.
   d. Select **Add user** to grant the administration privileges to the user.

Verification

- The configured htpasswd identity provider is visible on the **Access control → Identity providers** page.

NOTE

After creating the identity provider, synchronization usually completes within two minutes. You can log in to the cluster as the user after the htpasswd identity provider becomes available.

- The single, administrative user is visible on the **Access control → Cluster Roles and Access** page. The administration group membership of the user is also displayed.

Additional resources

- Customer administrator user

3.8. ACCESSING YOUR CLUSTER

After you have configured your identity providers, users can access the cluster from Red Hat OpenShift Cluster Manager.

Prerequisites

- You logged in to OpenShift Cluster Manager.
- You created an OpenShift Dedicated cluster.
- You configured an identity provider for your cluster.
- You added your user account to the configured identity provider.

Procedure

1. From OpenShift Cluster Manager, click on the cluster you want to access.
2. Click **Open Console**.
3. Click on your identity provider and provide your credentials to log into the cluster.
4. Click **Open console** to open the web console for your cluster.
5. Click on your identity provider and provide your credentials to log in to the cluster. Complete any authorization requests that are presented by your provider.

CHAPTER 4. REVOKING PRIVILEGES AND ACCESS TO AN OPENSHIFT DEDICATED CLUSTER

As cluster owner, you can revoke admin privileges and user access to a OpenShift Dedicated cluster.

4.1. REVOKING ADMINISTRATOR PRIVILEGES FROM A USER

Follow the steps in this section to revoke **dedicated-admin** privileges from a user.

Prerequisites

- You logged in to OpenShift Cluster Manager.
- You created an OpenShift Dedicated cluster.
- You have configured a GitHub identity provider for your cluster and added an identity provider user.
- You granted **dedicated-admin** privileges to a user.

Procedure

1. Navigate to OpenShift Cluster Manager and select your cluster.
2. Click the **Access control** tab.
3. In the **Cluster Roles and Access** tab, select  next to a user and click **Delete**.

Verification

- After revoking the privileges, the user is no longer listed as part of the **dedicated-admins** group under **Access control → Cluster Roles and Access** on the OpenShift Cluster Manager page for your cluster.

4.2. REVOKING USER ACCESS TO A CLUSTER

You can revoke cluster access from an identity provider user by removing them from your configured identity provider.

You can configure different types of identity providers for your OpenShift Dedicated cluster. The following example procedure revokes cluster access for a member of a GitHub organization or team that is configured for identity provision to the cluster.

Prerequisites

- You have an OpenShift Dedicated cluster.
- You have a GitHub user account.
- You have configured a GitHub identity provider for your cluster and added an identity provider user.

Procedure

1. Navigate to github.com and log in to your GitHub account.
2. Remove the user from your GitHub organization or team:
   - If your identity provider configuration uses a GitHub organization, follow the steps in Removing a member from your organization in the GitHub documentation.
   - If your identity provider configuration uses a team within a GitHub organization, follow the steps in Removing organization members from a team in the GitHub documentation.

Verification

- After removing the user from your identity provider, the user cannot authenticate into the cluster.

CHAPTER 5. DELETING AN OPENSHIFT DEDICATED CLUSTER

As cluster owner, you can delete your OpenShift Dedicated clusters.

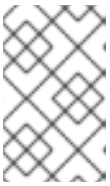
5.1. DELETING YOUR CLUSTER

You can delete your OpenShift Dedicated cluster in Red Hat OpenShift Cluster Manager.

- You logged in to OpenShift Cluster Manager.
- You created an OpenShift Dedicated cluster.

Procedure

1. From OpenShift Cluster Manager, click on the cluster you want to delete.
2. Select **Delete cluster** from the **Actions** drop-down menu.
3. Type the name of the cluster highlighted in bold, then click **Delete**. Cluster deletion occurs automatically.



NOTE

If you delete a cluster that was installed into a GCP Shared VPC, inform the VPC owner of the host project to remove the IAM policy roles granted to the service account that was referenced during cluster creation.