OpenShift Dedicated 4

Getting started

Getting started with OpenShift Dedicated

Last Updated: 2024-05-08

OpenShift Dedicated 4 Getting started

Getting started with OpenShift Dedicated

Legal Notice

Abstract

Getting started with your OpenShift Dedicated cluster.

Table of Contents

CHAPTER 1. UNDERSTANDING YOUR CLOUD DEPLOYMENT OPTIONS

You can install OpenShift Dedicated on Amazon Web Services (AWS) or Google Cloud Platform (GCP) using a cloud account that you own or using a cloud account that is owned by Red Hat. This document provides details about the cloud deployment options for OpenShift Dedicated clusters.

1.1. OVERVIEW OF THE OPENSHIFT DEDICATED CLOUD DEPLOYMENT OPTIONS

OpenShift Dedicated offers OpenShift Container Platform clusters as a managed service on Amazon Web Services (AWS) or Google Cloud Platform (GCP).

Through the Customer Cloud Subscription (CCS) model, you can deploy clusters in an existing AWS or GCP cloud account that you own.

Alternatively, you can install OpenShift Dedicated in a cloud account that is owned by Red Hat.

1.1.1. Deploying clusters using the Customer Cloud Subscription (CCS) model

The Customer Cloud Subscription (CCS) model enables you to deploy Red Hat managed OpenShift Dedicated clusters in an existing AWS or GCP account that you own. Red Hat requires several prerequisites be met in order to provide this service, and this service is supported by Red Hat Site Reliability Engineers (SRE).

In the CCS model, the customer pays the cloud infrastructure provider directly for cloud costs, and the cloud infrastructure account is part of an organization owned by the customer, with specific access granted to Red Hat. In this model, the customer pays Red Hat for the CCS subscription and pays the cloud provider for the cloud costs.

By using the CCS model, you can use the services that are provided by your cloud provider, in addition to the services provided by Red Hat.

1.1.2. Deploying clusters in Red Hat cloud accounts

As an alternative to the CCS model, you can deploy OpenShift Dedicated clusters in AWS or GCP cloud accounts that are owned by Red Hat. With this model, Red Hat is responsible for the cloud account and the cloud infrastructure costs are paid directly by Red Hat. The customer only pays the Red Hat subscription costs.

1.2. NEXT STEPS

- Creating a cluster on AWS
- Creating a cluster on GCP

CHAPTER 2. GETTING STARTED WITH OPENSHIFT DEDICATED

Follow this getting started document to quickly create a OpenShift Dedicated cluster, grant user access, deploy your first application, and learn how to scale and delete your cluster.

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 AN OPENSHIFT DEDICATED CLUSTER

You can install OpenShift Dedicated in your own cloud provider account through the Customer Cloud Subscription (CCS) model or in a cloud account that is owned by Red Hat. For more information about the deployment options for OpenShift Dedicated, see Understanding your cloud deployment options .

Choose from one of the following methods to deploy your cluster.

2.2.1. Creating a cluster using the CCS model

Complete the steps in one of the following sections to deploy OpenShift Dedicated in a cloud account that you own:

- **Creating a cluster on AWS with CCS**: You can install OpenShift Dedicated in your own Amazon Web Services (AWS) account by using the CCS model.
- **Creating a cluster on GCP with CCS**: You can install OpenShift Dedicated in your own Google Cloud Platform (GCP) account by using the CCS model.
- **Creating a cluster on GCP with Google Cloud Marketplace**: You can install OpenShift Dedicated in your own Google Cloud Platform (GCP) account with Google Cloud Marketplace.

2.2.2. Creating a cluster using a Red Hat cloud account

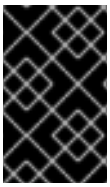
Complete the steps in one of the following sections to deploy OpenShift Dedicated in a cloud account that is owned by Red Hat:

- **Creating a cluster on AWS with a Red Hat cloud account**: You can install OpenShift Dedicated in an AWS account that is owned by Red Hat.
- **Creating a cluster on GCP with a Red Hat cloud account**: You can install OpenShift Dedicated in an GCP account that is owned by Red Hat.

2.3. CONFIGURING AN IDENTITY PROVIDER

After you have installed OpenShift Dedicated, you must configure your cluster to use an identity provider. You can then add members to your identity provider to grant them access to your cluster.

You can configure different identity provider types for your OpenShift Dedicated cluster. Supported types include GitHub, GitHub Enterprise, GitLab, Google, LDAP, OpenID Connect, and htpasswd identity providers.



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.

The following procedure configures a GitHub identity provider as an example.

WARNING

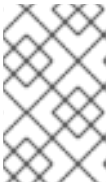
Configuring GitHub authentication allows users to log in to OpenShift Dedicated with their GitHub credentials. To prevent anyone with any GitHub user ID from logging in to your OpenShift Dedicated cluster, you must restrict access to only those in specific GitHub organizations or teams.

Prerequisites

- You logged in to OpenShift Cluster Manager.
- You created an OpenShift Dedicated cluster.
- You have a GitHub user account.
- You created a GitHub organization in your GitHub account. For more information, see Creating a new organization from scratch in the GitHub documentation.
- If you are restricting user access to a GitHub team, you have created a team within your GitHub organization. For more information, see Creating a team in the GitHub documentation.

Procedure

1. Navigate to OpenShift Cluster Manager and select your cluster.
2. Select **Access control → Identity providers**.
3. Select the **GitHub** identity provider type from the **Add identity provider** drop-down menu.
4. Enter a unique name for the identity provider. The name cannot be changed later.
5. Register an OAuth application in your GitHub organization by following the steps in the GitHub documentation.



NOTE

You must register the OAuth app under your GitHub organization. If you register an OAuth application that is not owned by the organization that contains your cluster users or teams, then user authentication to the cluster will not succeed.

- For the homepage URL in your GitHub OAuth app configuration, specify the **https://oauth-openshift.apps.<cluster_name>.<cluster_domain>** portion of the **OAuth callback URL** that is automatically generated in the **Add a GitHub identity provider** page on OpenShift Cluster Manager.
  The following is an example of a homepage URL for a GitHub identity provider:

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

- For the authorization callback URL in your GitHub OAuth app configuration, specify the full **OAuth callback URL** that is automatically generated in the **Add a GitHub identity provider** page on OpenShift Cluster Manager. The full URL has the following syntax:

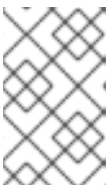
  ```
  https://oauth-openshift.apps.<cluster_name>.
  <cluster_domain>/oauth2callback/<idp_provider_name>
  ```

6. Return to the **Edit identity provider: GitHub** dialog in OpenShift Cluster Manager and select **Claim** from the **Mapping method** drop-down menu.
7. Enter the **Client ID** and **Client secret** for your GitHub OAuth application. The GitHub page for your OAuth app provides the ID and secret.
8. Optional: Enter a **hostname**.

NOTE

A hostname must be entered when using a hosted instance of GitHub Enterprise.

9. Optional: You can specify a certificate authority (CA) file to validate server certificates for a configured GitHub Enterprise URL. Click **Browse** to locate and attach a **CA file** to the identity provider.
10. Select **Use organizations** or **Use teams** to restrict access to a GitHub organization or a GitHub team within an organization.
11. Enter the name of the organization or team you would like to restrict access to. Click **Add more** to specify multiple organizations or teams.



NOTE

Specified organizations must own an OAuth app that was registered by using the preceding steps. If you specify a team, it must exist within an organization that owns an OAuth app that was registered by using the preceding steps.

12. Click **Add** to apply the identity provider configuration.

NOTE

It might take approximately two minutes for the identity provider configuration to become active.

Verification

- After the configuration becomes active, the identity provider is listed under **Access control → Identity providers** on the OpenShift Cluster Manager page for your cluster.

Additional resources

- For detailed steps to configure each of the supported identity provider types, see Configuring identity providers.

2.4. GRANTING ADMINISTRATOR PRIVILEGES TO A USER

After you have configured an identity provider for your cluster and added a user to the identity provider, you can grant **dedicated-admin** cluster privileges to the user.

Prerequisites

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

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, click **Add user**.
4. Enter the user ID of an identity provider user.
5. Click **Add user** to grant **dedicated-admin** cluster privileges to the user.

Verification

- After granting the privileges, the user is listed as part of the **dedicated-admins** group under **Access control → Cluster Roles and Access** on the OpenShift Cluster Manager page for your cluster.

Additional resources

- Customer administrator user

2.5. 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.

2.6. DEPLOYING AN APPLICATION FROM THE DEVELOPER CATALOG

From the OpenShift Dedicated web console, you can deploy a test application from the Developer Catalog and expose it with a route.

Prerequisites

- You logged in to the Red Hat Hybrid Cloud Console .
- You created a OpenShift Dedicated cluster.
- You configured an identity provider for your cluster.
- You added your user account to the configured identity provider.

Procedure

1. Go to the **Clusters** page in OpenShift Cluster Manager.
2. Click the options icon (⋮) next to the cluster you want to view.
3. Click **Open console**.
4. Your cluster console opens in a new browser window. Login to your Red Hat account with your configured identity provider credentials.
5. In the **Administrator** perspective, select **Home → Projects → Create Project**.
6. Enter a name for your project and optionally add a **Display Name** and **Description**.
7. Click **Create** to create the project.

8. Switch to the **Developer** perspective and select **+Add**. Verify that the selected **Project** is the one that you just created.
9. In the **Developer Catalog** dialog, select **All services**.
10. In the **Developer Catalog** page, select **Languages → JavaScript** from the menu.
11. Click **Node.js**, and then click **Create** to open the **Create Source-to-Image application** page.

NOTE

You might need to click **Clear All Filters** to display the **Node.js** option.

12. In the **Git** section, click **Try sample**.
13. Add a unique name in the **Name** field. The value will be used to name the associated resources.
14. Confirm that **Deployment** and **Create a route** are selected.
15. Click **Create** to deploy the application. It will take a few minutes for the pods to deploy.
16. Optional: Check the status of the pods in the **Topology** pane by selecting your **Node.js** app and reviewing its sidebar. You must wait for the **nodejs** build to complete and for the **nodejs** pod to be in a **Running** state before continuing.
17. When the deployment is complete, click the route URL for the application, which has a format similar to the following:

```
https://nodejs-<project>.<cluster_name>.<hash>.<region>.openshiftapps.com/
```

A new tab in your browser opens with a message similar to the following:

```
Welcome to your Node.js application on OpenShift
```

18. Optional: Delete the application and clean up the resources that you created:
    a. In the **Administrator** perspective, navigate to **Home → Projects**.
    b. Click the action menu for your project and select **Delete Project**.

2.7. SCALING YOUR CLUSTER

You can scale the number of load balancers, the persistent storage capacity, and the node count for your OpenShift Dedicated cluster from OpenShift Cluster Manager.

Prerequisites

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

Procedure

- To scale the number of load balancers or the persistent storage capacity:

1. Navigate to OpenShift Cluster Manager and select your cluster.
2. Select **Edit load balancers and persistent storage** from the **Actions** drop-down menu.
3. Select how many **Load balancers** that you want to scale to.
4. Select the **Persistent storage** capacity that you want to scale to.
5. Click **Apply**. Scaling occurs automatically.

- To scale the node count:
  1. Navigate to OpenShift Cluster Manager and select your cluster.
  2. Select **Edit node count** from the **Actions** drop-down menu.
  3. Select a **Machine pool**.
  4. Select a **Node count** per zone.
  5. Click **Apply**. Scaling occurs automatically.

Verification

- In the **Overview** tab under the **Details** heading, you can review the load balancer configuration, persistent storage details, and actual and desired node counts.

Additional resources

- For information about machine pools, see About machine pools.
- For detailed steps to enable autoscaling for compute nodes in your cluster, see About autoscaling nodes on a cluster.

2.8. 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.

2.9. 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.

2.10. 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.

2.11. NEXT STEPS

- Adding services to a cluster using the OpenShift Cluster Manager console
- About machine pools
- About autoscaling nodes on a cluster
- Configuring the monitoring stack

2.12. ADDITIONAL RESOURCES

- For information about the end-of-life dates for OpenShift Dedicated versions, see the OpenShift Dedicated update life cycle.
- For more information about deploying OpenShift Dedicated clusters, see Creating a cluster on AWS and Creating a cluster on GCP.
- For documentation on upgrading your cluster, see OpenShift Dedicated cluster upgrades.