OpenShift Dedicated 4

Administering a cluster

An overview of administering a cluster for OpenShift Dedicated 4

Last Updated: 2020-06-18

OpenShift Dedicated 4 Administering a cluster

An overview of administering a cluster for OpenShift Dedicated 4

Legal Notice

Abstract

This document provides details on how to administer an OpenShift Dedicated 4 cluster.

Table of Contents

CHAPTER 1. THE DEDICATED-ADMIN ROLE

As an administrator of an OpenShift Dedicated cluster, your account has additional permissions and access to all user-created projects in your organization's cluster. While logged in to an account with this role, the basic developer CLI (the **oc** command) allows you increased visibility and management capabilities over objects across projects, while the administrator CLI (commands under the **oc adm** command) allow you to complete additional operations.

NOTE

While your account does have these increased permissions, the actual cluster maintenance and host configuration is still performed by the OpenShift Operations Team. If you would like to request a change to your cluster that you cannot perform using the administrator CLI, open a support case on the Red Hat Customer Portal .

1.1. LOGGING IN AND VERIFYING PERMISSIONS

You can log in as an OpenShift Dedicated cluster administration via the web console or CLI, just as you would if you were an application developer.

When you log in to the web console, all user-created projects across the cluster are visible from the main **Projects** page.

Use the standard **oc login** command to log in with the CLI:

```
$ oc login <your_instance_url>
```

All projects are visible using:

```
$ oc get projects
```

When your account has the **dedicated-admins-cluster** cluster role bound to it, you are automatically bound to the **dedicated-admins-project** for any new projects that are created by users in the cluster.

To verify if your account has administrator privileges, run the following command against a user-created project to view its default role bindings. If you are a cluster administrator, you will see your account listed under subjects for the **dedicated-admins-project-0** and **dedicated-admins-project-1** role bindings for the project:

```
$ oc describe rolebinding.rbac -n <project_name>

Name:  admin
Labels:  <none>
Annotations: <none>
Role:
  Kind: ClusterRole
  Name: admin
Subjects:
  Kind Name   Namespace
  ---- ----   ---------
  User fred@example.com 1


Name:  dedicated-admins-project
```

```
Labels:  <none>
Annotations: <none>
Role:
  Kind: ClusterRole
  Name: dedicated-admins-project
Subjects:
  Kind Name   Namespace
  ---- ----   ---------
  User alice@example.com 2
  User bob@example.com 3
...
```

1 The **fred@example.com** user is a normal, project-scoped administrator for this project.

2 3 The **alice@example.com** and **bob@example.com** users are cluster administrators.

To view details on your increased permissions, and the sets of verbs and resources associated with the **dedicated-admins-cluster** and **dedicated-admins-project** roles, run the following:

```
$ oc describe clusterrole.rbac dedicated-admins-cluster
$ oc describe clusterrole.rbac dedicated-admins-project
```

1.2. MANAGING OPENSHIFT DEDICATED ADMINISTRATORS

Administrator roles are managed using a **dedicated-admins** group on the cluster. Existing members of this group can edit membership via the Red Hat OpenShift Cluster Manager site.

1.2.1. Adding a user

1. Navigate to the **Cluster Details** page and **Users** tab.
2. Click the **Add user** button. (first user only)
3. Enter the user name and select the group (**dedicated-admins**)
4. Click the **Add** button.

1.2.2. Removing a user

1. Navigate to the **Cluster Details** page and **Users** tab.
2. Click the **X** to the right of the user / group combination to be deleted..

1.3. GRANTING PERMISSIONS TO USERS OR GROUPS

To grant permissions to other users or groups, you can add, or *bind*, a role to them using the following commands:

```
$ oc adm policy add-role-to-user <role> <user_name>
$ oc adm policy add-role-to-group <role> <group_name>
```

1.4. MANAGING SERVICE ACCOUNTS

Service accounts are API objects that exist within each project. To manage service accounts, you can use the **oc** command with the **sa** or **serviceaccount** object type or use the web console.

The **dedicated-admin** service creates the **dedicated-admins** group. This group is granted the roles at the cluster or individual project level. Users can be assigned to this group and group membership defines who has OpenShift Dedicated administrator access. However, by design, service accounts cannot be added to regular groups.

Instead, the dedicated-admin service creates a special project for this purpose named **dedicated-admin**. The service account group for this project is granted OpenShift Dedicated **admin** roles, granting OpenShift Dedicated administrator access to all service accounts within the **dedicated-admin** project. These service accounts can then be used to perform any actions that require OpenShift Dedicated administrator access.

Users that are members of the **dedicated-admins** group, and thus have been granted the **dedicated-admin** role, have **edit** access to the **dedicated-admin** project. This allows these users to manage the service accounts in this project and create new ones as needed.

To get a list of existing service accounts in the current project, run:

```
$ oc get sa
NAME       SECRETS   AGE
builder    2         2d
default    2         2d
deployer   2         2d
```

To create a new service account, run:

```
$ oc create sa <service-account-name>
```

As soon as a service account is created, two secrets are automatically added to it:

- an API token
- credentials for the OpenShift Container Registry

These can be seen by describing the service account:

```
$ oc describe sa <service-account-name>
```

The system ensures that service accounts always have an API token and registry credentials.

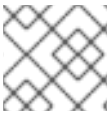
The generated API token and registry credentials do not expire, but they can be revoked by deleting the secret. When the secret is deleted, a new one is automatically generated to take its place.

1.5. MANAGING QUOTAS AND LIMIT RANGES

As an administrator, you are able to view, create, and modify quotas and limit ranges on other projects. This allows you to better constrain how compute resources and objects are consumed by users across the cluster.

1.6. INSTALLING OPERATORS FROM THE OPERATORHUB

OpenShift Dedicated administrators can install Operators from a curated list provided by the OperatorHub. This makes the Operator available to all developers on your cluster to create Custom Resources and applications using that Operator.



NOTE

Privileged and custom Operators cannot be installed.

Administrators can only install Operators to the default **openshift-operators** namespace, except for the Cluster Logging Operator, which requires the **openshift-logging** namespace.

Additional resources

- Adding Operators to a cluster

CHAPTER 2. THE CLUSTER-ADMIN ROLE

As an administrator of OpenShift Dedicated with Customer Cloud Subscriptions (CCS), you can request additional permissions and access to the **cluster-admin** role within your organization's cluster. While logged into an account with the cluster-admin role, users have increased permissions to run privileged security contexts and install additional Operators for their environment.

2.1. ENABLING THE CLUSTER-ADMIN ROLE FOR YOUR CLUSTER

The cluster-admin role must be enabled at the cluster level before it can be assigned to a user.

Prerequisites

1. Open a technical support case with Red Hat to request that **cluster-admin** be enabled for your cluster.

Procedure

1. In the OpenShift Cluster Manager, select the cluster you want to assign cluster-admin privileges.
2. Under the **Actions** dropdown menu, select **Allow cluster-admin access**.

2.2. GRANTING THE CLUSTER-ADMIN ROLE TO USERS

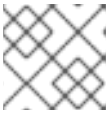
After enabling cluster-admin rights on your cluster, you can assign the role to users.

Prerequisites

- Cluster access with cluster owner permissions

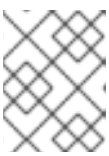
Procedure

1. In the OpenShift Cluster Manager, select the cluster you want to assign cluster-admin privileges.
2. Under the **Access Control** tab, locate the **Cluster Administrative Users** section. Click **Add user**.
3. After determining an appropriate User ID, select **cluster-admin** from the **Group** selection, then click **Add user**.



NOTE

Cluster-admin user creation can take several minutes to complete.



NOTE

Existing dedicated-admin users cannot elevate their role to cluster-admin. A new user must be created with the cluster-admin role assigned.