Red Hat Advanced Cluster Management for Kubernetes 2.5

Credentials

Read more to learn how to create and manage your cluster credentials.

Last Updated: 2023-07-13

Red Hat Advanced Cluster Management for Kubernetes 2.5 Credentials

Read more to learn how to create and manage your cluster credentials.

Legal Notice

Abstract

Read more to learn how to create and manage your cluster credentials.

Table of Contents

CHAPTER 1. MANAGING CREDENTIALS OVERVIEW

You can create and manage your cluster credentials. A *credential* is required to create a Red Hat OpenShift Container Platform cluster on a cloud service provider with Red Hat Advanced Cluster Management for Kubernetes. The credential stores the access information for a cloud provider. Each provider account requires its own credential, as does each domain on a single provider.

Credentials are stored as Kubernetes secrets. Secrets are copied to the namespace of a managed cluster so that the controllers for the managed cluster can access the secrets. When a credential is updated, the copies of the secret are automatically updated in the managed cluster namespaces.

Note: Changes to the pull secret or SSH keys of cloud provider credentials are not reflected for existing managed clusters, as they have already been provisioned using the original credentials.

Required access: Edit

- Creating a credential for Amazon Web Services
- Creating a credential for Microsoft Azure
- Creating a credential for Google Cloud Platform
- Creating a credential for VMware vSphere
- Creating a credential for Red Hat OpenStack Platform
- Creating a credential for Red Hat Virtualization
- Creating a credential for bare metal
- Creating a credential for Red Hat OpenShift Cluster Manager
- Creating a credential for Ansible Automation Platform
- Creating a credential for an on-premises environment

1.1. CREATING A CREDENTIAL FOR AMAZON WEB SERVICES

You need a credential to use Red Hat Advanced Cluster Management for Kubernetes console to deploy and manage an Red Hat OpenShift Container Platform cluster on Amazon Web Services (AWS).

Required access: Edit

Note: This procedure must be done before you can create a cluster with Red Hat Advanced Cluster Management for Kubernetes.

1.1.1. Prerequisites

You must have the following prerequisites before creating a credential:

- A deployed Red Hat Advanced Cluster Management for Kubernetes hub cluster
- Internet access for your Red Hat Advanced Cluster Management for Kubernetes hub cluster so it can create the Kubernetes cluster on Amazon Web Services (AWS)

- AWS login credentials, which include access key ID and secret access key. See Understanding and getting your security credentials.

- Account permissions that allow installing clusters on AWS. See Configuring an AWS account for instructions on how to configure.

1.1.2. Managing a credential by using the console

To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console.

Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, both for convenience and added security.

You can optionally add a *Base DNS domain* for your credential. If you add the base DNS domain to the credential, it is automatically populated in the correct field when you create a cluster with this credential. See the following steps:

1. Add your *AWS access key ID* for your AWS account. Log in to AWS to find your ID.

2. In the Red Hat Advanced Cluster Management, provide the contents for your new *AWS Secret Access Key*.

3. If you want to enable a proxy, enter the proxy information:

   - HTTP proxy URL: The URL that should be used as a proxy for **HTTP** traffic.

   - HTTPS proxy URL: The secure proxy URL that should be used for **HTTPS** traffic. If no value is provided, the same value as the **HTTP Proxy URL** is used for both **HTTP** and **HTTPS**.

   - No proxy domains: A comma-separated list of domains that should bypass the proxy. Begin a domain name with a period **.** to include all of the subdomains that are in that domain. Add and asterisk ***** to bypass the proxy for all destinations.

   - Additional trust bundle: The contents of the certificate file that is required to access the mirror registry.

4. Enter your *Red Hat OpenShift pull secret*. You can download your pull secret from Pull secret.

5. Add your *SSH private key* and *SSH public key*, which allows you to connect to the cluster. You can use an existing key pair, or create a new one with key generation program.

See Generating an SSH private key and adding it to the agent for more information about how to generate a key.

You can create a cluster that uses this credential by completing the steps in Creating a cluster on Amazon Web Services.

You can edit your credential in the console. If the cluster was created by using this provider connection, then the **<cluster-name>-aws-creds>** secret from **<cluster-namespace>** will get updated with the new credentials.

Note: Updating credentials does not work for cluster pool claimed clusters.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.

1.1.3. Creating an opaque secret by using the API

To create an opaque secret for Amazon Web Services by using the API, apply YAML content in the YAML preview window that is similar to the following example:

```
kind: Secret
metadata:
  name: <managed-cluster-name>-aws-creds
  namespace: <managed-cluster-namespace>
type: Opaque
data:
  aws_access_key_id: $(echo -n "${AWS_KEY}" | base64 -w0)
  aws_secret_access_key: $(echo -n "${AWS_SECRET}" | base64 -w0)
```

Note: The opaque secret is created in the managed cluster namespace you chose. Hive uses the opaque secret to provision the cluster. When provisioning the cluster by using the Red Hat Advanced Cluster Management console, the credentials you previoulsy created are copied to the managed cluster namespace as the opaque secret.

1.2. CREATING A CREDENTIAL FOR MICROSOFT AZURE

You need a credential to use Red Hat Advanced Cluster Management for Kubernetes console to create and manage a Red Hat OpenShift Container Platform cluster on Microsoft Azure or on Microsoft Azure Government.

Required access: Edit

Note: This procedure is a prerequisite for creating a cluster with Red Hat Advanced Cluster Management for Kubernetes.

1.2.1. Prerequisites

You must have the following prerequisites before creating a credential:

- A deployed Red Hat Advanced Cluster Management for Kubernetes hub cluster.
- Internet access for your Red Hat Advanced Cluster Management for Kubernetes hub cluster so that it can create the Kubernetes cluster on Azure.
- Azure login credentials, which include your Base Domain Resource Group and Azure Service Principal JSON. See azure.microsoft.com.
- Account permissions that allow installing clusters on Azure. See How to configure Cloud Services and Configuring an Azure account for more information.

1.2.2. Managing a credential by using the console

To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console. Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, both for convenience and added security.

1. **Optional:** Add a *Base DNS domain* for your credential. If you add the base DNS domain to the credential, it is automatically populated in the correct field when you create a cluster with this credential.

2. Select whether the environment for your cluster is **AzurePublicCloud** or **AzureUSGovernmentCloud**. The settings are different for the the Azure Government environment, so ensure that this is set correctly.

3. Add your *Base domain resource group name* for your Azure account. This entry is the resource name that you created with your Azure account. You can find your Base Domain Resource Group Name by selecting **Home** > **DNS Zones** in the Azure interface. See Create an Azure service principal with the Azure CLI to find your base domain resource group name.

4. In the Red Hat Advanced Cluster Management, provide the contents for your *Client ID*. This value is generated as the **appId** property when you create a service principal with the following command:

   ```
   az ad sp create-for-rbac --role Contributor --name <service_principal>
   ```

   Replace *service_principal* with the name of your service principal.

5. Add your *Client Secret*. This value is generated as the **password** property when you create a service principal with the following command:

   ```
   az ad sp create-for-rbac --role Contributor --name <service_principal>
   ```

   Replace *service_principal* with the name of your service principal.

6. Add your *Subscription ID*. This value is the **id** property in the output of the following command:

   ```
   az account show
   ```

7. Add your *Tenant ID*. This value is the **tenantId** property in the output of the following command:

   ```
   az account show
   ```

8. If you want to enable a proxy, enter the proxy information:

   - HTTP proxy URL: The URL that should be used as a proxy for **HTTP** traffic.
   - HTTPS proxy URL: The secure proxy URL that should be used for **HTTPS** traffic. If no value is provided, the same value as the **HTTP Proxy URL** is used for both **HTTP** and **HTTPS**.
   - No proxy domains: A comma-separated list of domains that should bypass the proxy. Begin a domain name with a period **.** to include all of the subdomains that are in that domain. Add and asterisk ***** to bypass the proxy for all destinations.
   - Additional trust bundle: The contents of the certificate file that is required to access the mirror registry.

9. Enter your *Red Hat OpenShift pull secret*. You can download your pull secret from Pull secret.

10. Add your *SSH private key* and *SSH public key* to use to connect to the cluster. You can use an existing key pair, or create a new pair using a key generation program. See Generating an SSH private key and adding it to the agent for more information about how to generate a key.

You can create a cluster that uses this credential by completing the steps in Creating a cluster on Microsoft Azure.

You can edit your credential in the console.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.

1.2.3. Creating an opaque secret by using the API

To create an opaque secret for Microsoft Azure by using the API instead of the console, apply YAML content in the YAML preview window that is similar to the following example:

```
kind: Secret
metadata:
  name: <managed-cluster-name>-azure-creds
  namespace: <managed-cluster-namespace>
type: Opaque
data:
  baseDomainResourceGroupName: $(echo -n "${azure_resource_group_name}" | base64 -w0)
  osServicePrincipal.json: $(base64 -w0 "${AZURE_CRED_JSON}")
```

Note: The opaque secret is created in the managed cluster namespace you chose. Hive uses the opaque secret to provision the cluster. When provisioning the cluster by using the Red Hat Advanced Cluster Management console, the credentials you previoulsy created are copied to the managed cluster namespace as the opaque secret.

1.3. CREATING A CREDENTIAL FOR GOOGLE CLOUD PLATFORM

You need a credential to use Red Hat Advanced Cluster Management for Kubernetes console to create and manage a Red Hat OpenShift Container Platform cluster on Google Cloud Platform (GCP).

Required access: Edit

Note: This procedure is a prerequisite for creating a cluster with Red Hat Advanced Cluster Management for Kubernetes.

1.3.1. Prerequisites

You must have the following prerequisites before creating a credential:

- A deployed Red Hat Advanced Cluster Management for Kubernetes hub cluster
- Internet access for your Red Hat Advanced Cluster Management for Kubernetes hub cluster so it can create the Kubernetes cluster on GCP
- GCP login credentials, which include user Google Cloud Platform Project ID and Google Cloud Platform service account JSON key. See Creating and managing projects.
- Account permissions that allow installing clusters on GCP. See Configuring a GCP project for instructions on how to configure an account.

1.3.2. Managing a credential by using the console

To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console.

Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, for both convenience and security.

You can optionally add a *Base DNS domain* for your credential. If you add the base DNS domain to the credential, it is automatically populated in the correct field when you create a cluster with this credential. See the following steps:

1. Add your *Google Cloud Platform project ID* for your GCP account. Log in to GCP to retrieve your settings.

2. Add your *Google Cloud Platform service account JSON key* . See the (https://cloud.google.com/iam/docs/creating-managing-service-accounts) to create your service account JSON key. Follow the steps for the GCP console.

3. In the Red Hat Advanced Cluster Management, provide the contents for your new *Google Cloud Platform service account JSON key*.

4. If you want to enable a proxy, enter the proxy information:

   - HTTP proxy URL: The URL that should be used as a proxy for **HTTP** traffic.
   - HTTPS proxy URL: The secure proxy URL that should be used for **HTTPS** traffic. If no value is provided, the same value as the **HTTP Proxy URL** is used for both **HTTP** and **HTTPS**.
   - No proxy domains: A comma-separated list of domains that should bypass the proxy. Begin a domain name with a period **.** to include all of the subdomains that are in that domain. Add and asterisk ***** to bypass the proxy for all destinations.
   - Additional trust bundle: The contents of the certificate file that is required to access the mirror registry.

5. Enter your *Red Hat OpenShift pull secret* . You can download your pull secret from Pull secret.

6. Add your *SSH private key* and *SSH public key* so you can access the cluster. You can use an existing key pair, or create a new pair using a key generation program.

See Generating an SSH private key and adding it to the agent for more information about how to generate a key.

You can use this connection when you create a cluster by completing the steps in Creating a cluster on Google Cloud Platform.

You can edit your credential in the console.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.

1.3.3. Creating an opaque secret by using the API

To create an opaque secret for Google Cloud Platform by using the API instead of the console, apply YAML content in the YAML preview window that is similar to the following example:

```
kind: Secret
metadata:
  name: <managed-cluster-name>-gcp-creds
  namespace: <managed-cluster-namespace>
type: Opaque
data:
  osServiceAccount.json: $(base64 -w0 "${GCP_CRED_JSON}")
```

Note: The opaque secret is created in the managed cluster namespace you chose. Hive uses the opaque secret to provision the cluster. When provisioning the cluster by using the Red Hat Advanced Cluster Management console, the credentials you previoulsy created are copied to the managed cluster namespace as the opaque secret.

1.4. CREATING A CREDENTIAL FOR VMWARE VSPHERE

You need a credential to use Red Hat Advanced Cluster Management for Kubernetes console to deploy and manage a Red Hat OpenShift Container Platform cluster on VMware vSphere. Only OpenShift Container Platform versions 4.5.x, and later, are supported.

Required access: Edit

Note: This procedure must be done before you can create a cluster with Red Hat Advanced Cluster Management.

1.4.1. Prerequisites

You must have the following prerequisites before you create a credential:

- A deployed Red Hat Advanced Cluster Management hub cluster on OpenShift Container Platform version 4.6 or later.
- Internet access for your Red Hat Advanced Cluster Management hub cluster so it can create the Kubernetes cluster on VMware vSphere.
- VMware vSphere login credentials and vCenter requirements configured for OpenShift Container Platform when using installer-provisioned infrastructure. See Installing a cluster on vSphere with customizations. These credentials include the following information:
  - vCenter account privileges.
  - Cluster resources.
  - DHCP available.
  - ESXi hosts have time synchronized (for example, NTP).

1.4.2. Managing a credential by using the console

To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console.

Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, both for convenience and added security.

You can optionally add a *Base DNS domain* for your credential. If you add the base DNS domain to the credential, it is automatically populated in the correct field when you create a cluster with this credential. See the following steps:

1. Add your *VMware vCenter server fully-qualified host name or IP address* . The value must be defined in the vCenter server root CA certificate. If possible, use the fully-qualified host name.
2. Add your *VMware vCenter username*.

3. Add your *VMware vCenter password*.

4. Add your *VMware vCenter root CA certificate*.

   a. You can download your certificate in the **download.zip** package with the certificate from your VMware vCenter server at: **https://<vCenter_address>/certs/download.zip**. Replace *vCenter_address* with the address to your vCenter server.

   b. Unpackage the **download.zip**.

   c. Use the certificates from the **certs/<platform>** directory that have a **.0** extension. **Tip:** You can use the **ls certs/<platform>** command to list all of the available certificates for your platform.
   Replace ***<platform>*** with the abbreviation for your platform: **lin**, **mac**, or **win**.

   For example: **certs/lin/3a343545.0**

   Best practice: Link together multiple certificates with a **.0** extension using the following command:

   ```
   cat certs/lin/*.0 > ca.crt
   ```

5. Add your *VMware vSphere cluster name*.

6. Add your *VMware vSphere datacenter*.

7. Add your *VMware vSphere default datastore*.

8. For disconnected installations only: Complete the fields in the **Configuration for disconnected installation** subsection with the required information:

   - *Image content source*: This value contains the disconnected registry path. The path contains the hostname, port, and repository path to all of the installation images for disconnected installations. Example: **repository.com:5000/openshift/ocp-release**.
     The path creates an image content source policy mapping in the **install-config.yaml** to the Red Hat OpenShift Container Platform release images. As an example, **repository.com:5000** produces this **imageContentSource** content:

     ```
     imageContentSources:
     - mirrors:
       - registry.example.com:5000/ocp4
       source: quay.io/openshift-release-dev/ocp-release-nightly
     - mirrors:
       - registry.example.com:5000/ocp4
       source: quay.io/openshift-release-dev/ocp-release
     - mirrors:
       - registry.example.com:5000/ocp4
       source: quay.io/openshift-release-dev/ocp-v4.0-art-dev
     ```

   - *Additional trust bundle*: This value provides the contents of the certificate file that is required to access the mirror registry.
     Note: If you are deploying managed clusters from a hub that is in a disconnected environment, and want them to be automatically imported post install, add an Image Content Source Policy to the **install-config.yaml** file by using the **YAML** editor. A sample entry is shown in the following example:

```
imageContentSources:
- mirrors:
  - registry.example.com:5000/rhacm2
  source: registry.redhat.io/rhacm2
```

9. If you want to enable a proxy, enter the proxy information:
    - HTTP proxy URL: The URL that should be used as a proxy for **HTTP** traffic.
    - HTTPS proxy URL: The secure proxy URL that should be used for **HTTPS** traffic. If no value is provided, the same value as the **HTTP Proxy URL** is used for both **HTTP** and **HTTPS**.
    - No proxy domains: A comma-separated list of domains that should bypass the proxy. Begin a domain name with a period **.** to include all of the subdomains that are in that domain. Add and asterisk ***** to bypass the proxy for all destinations.
    - Additional trust bundle: The contents of the certificate file that is required to access the mirror registry.
10. Enter your *Red Hat OpenShift pull secret*. You can download your pull secret from Pull secret.
11. Add your *SSH private key* and *SSH public key*, which allows you to connect to the cluster. You can use an existing key pair, or create a new one with key generation program. See Generating a key pair for cluster node SSH access for more information.

You can create a cluster that uses this credential by completing the steps in Creating a cluster on VMware vSphere.

You can edit your credential in the console.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.

1.4.3. Creating an opaque secret by using the API

To create an opaque secret for VMware vSphere by using the API instead of the console, apply YAML content in the YAML preview window that is similar to the following example:

```
kind: Secret
metadata:
    name: <managed-cluster-name>-vsphere-creds
    namespace: <managed-cluster-namespace>
type: Opaque
data:
    username: $(echo -n "${VMW_USERNAME}" | base64 -w0)
    password.json: $(base64 -w0 "${VMW_PASSWORD}")
```

Note: The opaque secret is created in the managed cluster namespace you chose. Hive uses the opaque secret to provision the cluster. When provisioning the cluster by using the Red Hat Advanced Cluster Management console, the credentials you previoulsy created are copied to the managed cluster namespace as the opaque secret.

1.5. CREATING A CREDENTIAL FOR RED HAT OPENSTACK

You need a credential to use Red Hat Advanced Cluster Management for Kubernetes console to deploy and manage a Red Hat OpenShift Container Platform cluster on Red Hat OpenStack Platform. Only OpenShift Container Platform versions 4.5.x, and later, are supported.

Note: This procedure must be done before you can create a cluster with Red Hat Advanced Cluster Management.

1.5.1. Prerequisites

You must have the following prerequisites before you create a credential:

- A deployed Red Hat Advanced Cluster Management hub cluster on OpenShift Container Platform version 4.6 or later.
- Internet access for your Red Hat Advanced Cluster Management hub cluster so it can create the Kubernetes cluster on Red Hat OpenStack Platform.
- Red Hat OpenStack Platform login credentials and Red Hat OpenStack Platform requirements configured for OpenShift Container Platform when using installer-provisioned infrastructure. See Installing a cluster on OpenStack with customizations .
- Download or create a **clouds.yaml** file for accessing the CloudStack API. Within the **clouds.yaml** file:
  - Determine the cloud auth section name to use.
  - Add a line for the **password**, immediately following the **username** line.

1.5.2. Managing a credential by using the console

To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console.

Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, for both convenience and added security.

1. Add your Red Hat OpenStack Platform **clouds.yaml** file contents. The contents of the **clouds.yaml** file, including the password, provide the required information for connecting to the Red Hat OpenStack Platform server. The file contents **must** include the password, which you add to a new line immediately after the **username**.
2. Add your Red Hat OpenStack Platform cloud name. This entry is the name specified in the cloud section of the **clouds.yaml** to use for establishing communication to the Red Hat OpenStack Platform server.
3. You can optionally add a Base DNS domain for your credential. If you add the base DNS domain to the credential, it is automatically populated in the correct field when you create a cluster with this credential.
4. For disconnected installations only: Complete the fields in the **Configuration for disconnected installation** subsection with the required information:
   - *Cluster OS image*: This value contains the URL to the image to use for Red Hat OpenShift Container Platform cluster machines.

- *Image content sources*: This value contains the disconnected registry path. The path contains the hostname, port, and repository path to all of the installation images for disconnected installations. Example: **repository.com:5000/openshift/ocp-release**.
  The path creates an image content source policy mapping in the **install-config.yaml** to the Red Hat OpenShift Container Platform release images. As an example, **repository.com:5000** produces this **imageContentSource** content:

  ```
  imageContentSources:
  - mirrors:
    - registry.example.com:5000/ocp4
    source: quay.io/openshift-release-dev/ocp-release-nightly
  - mirrors:
    - registry.example.com:5000/ocp4
    source: quay.io/openshift-release-dev/ocp-release
  - mirrors:
    - registry.example.com:5000/ocp4
    source: quay.io/openshift-release-dev/ocp-v4.0-art-dev
  ```

- *Additional trust bundle*: This value provides the contents of the certificate file that is required to access the mirror registry.
  Note: If you are deploying managed clusters from a hub that is in a disconnected environment, and want them to be automatically imported post install, add an Image Content Source Policy to the **install-config.yaml** file by using the **YAML** editor. A sample entry is shown in the following example:

  ```
  imageContentSources:
  - mirrors:
    - registry.example.com:5000/rhacm2
    source: registry.redhat.io/rhacm2
  ```

5. If you want to enable a proxy, enter the proxy information:

   - HTTP proxy URL: The URL that should be used as a proxy for **HTTP** traffic.

   - HTTPS proxy URL: The secure proxy URL that should be used for **HTTPS** traffic. If no value is provided, the same value as the **HTTP Proxy URL** is used for both **HTTP** and **HTTPS**.

   - No proxy domains: A comma-separated list of domains that should bypass the proxy. Begin a domain name with a period **.** to include all of the subdomains that are in that domain. Add and asterisk ***** to bypass the proxy for all destinations.

   - Additional trust bundle: The contents of the certificate file that is required to access the mirror registry.

6. Enter your Red Hat OpenShift Pull Secret. You can download your pull secret from Pull secret.

7. Add your SSH Private Key and SSH Public Key, which allows you to connect to the cluster. You can use an existing key pair, or create a new one with key generation program. See Generating a key pair for cluster node SSH access for more information.

8. Click **Create**.

9. Review the new credential information, then click **Add**. When you add the credential, it is added to the list of credentials.

You can create a cluster that uses this credential by completing the steps in Creating a cluster on Red Hat OpenStack Platform.

You can edit your credential in the console.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.

1.5.3. Creating an opaque secret by using the API

To create an opaque secret for Red Hat OpenStack Platform by using the API instead of the console, apply YAML content in the YAML preview window that is similar to the following example:

```
kind: Secret
metadata:
   name: <managed-cluster-name>-osp-creds
   namespace: <managed-cluster-namespace>
type: Opaque
data:
   clouds.yaml: $(base64 -w0 "${OSP_CRED_YAML}") cloud: $(echo -n "openstack" | base64 -w0)
```

Note: The opaque secret is created in the managed cluster namespace you chose. Hive uses the opaque secret to provision the cluster. When provisioning the cluster by using the Red Hat Advanced Cluster Management console, the credentials you previoulsy created are copied to the managed cluster namespace as the opaque secret.

1.6. CREATING A CREDENTIAL FOR RED HAT VIRTUALIZATION

You need a credential to use Red Hat Advanced Cluster Management for Kubernetes console to deploy and manage a Red Hat OpenShift Container Platform cluster on Red Hat Virtualization.

Note: This procedure must be done before you can create a cluster with Red Hat Advanced Cluster Management.

1.6.1. Prerequisites

You must have the following prerequisites before you create a credential:

- A deployed Red Hat Advanced Cluster Management hub cluster on OpenShift Container Platform version 4.7 or later.
- Internet access for your Red Hat Advanced Cluster Management hub cluster so it can create the Kubernetes cluster on Red Hat Virtualization.
- Red Hat Virtualization login credentials for a configured Red Hat Virtualization environment. See Installation Guide in the Red Hat Virtualization documentation. The following list shows the required information:
  - oVirt URL
  - oVirt fully-qualified domain name (FQDN)
  - oVirt username
  - oVirt password

  - oVirt CA/Certificate

- Optional: Proxy information, if you are enabling a proxy.
- Red Hat OpenShift Container Platform pull secret information. You can download your pull secret from Pull secret.
- SSH private and public keys for transferring information for the final cluster.
- Account permissions that allow installing clusters on oVirt.

1.6.2. Managing a credential by using the console

To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console.

Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, for both convenience and added security.

1. Add the basic information for your new credential. You can optionally add a Base DNS domain, which is automatically populated in the correct field when you create a cluster with this credential. If you do not add it to the credential, you can add it when you create the cluster.
2. Add the required information for your Red Hat Virtualization environment.
3. If you want to enable a proxy, enter the proxy information:
   - HTTP Proxy URL: The URL that should be used as a proxy for **HTTP** traffic.
   - HTTPS Proxy URL: The secure proxy URL that should be used when using **HTTPS** traffic. If no value is provided, the same value as the **HTTP Proxy URL** is used for both **HTTP** and **HTTPS**.
   - No Proxy domains: A comma-separated list of domains that should bypass the proxy. Begin a domain name with a period **.** to include all of the subdomains that are in that domain. Add and asterisk ***** to bypass the proxy for all destinations.
4. Enter your Red Hat OpenShift Container Platform pull secret. You can download your pull secret from Pull secret.
5. Add your SSH Private Key and SSH Public Key, which allows you to connect to the cluster. You can use an existing key pair, or create a new one with a key generation program. See Generating akey pair for cluster node SSH access for more information.
6. Review the new credential information, then click **Add**. When you add the credential, it is added to the list of credentials.

You can create a cluster that uses this credential by completing the steps in Creating a cluster on Red Hat Virtualization.

You can edit your credential in the console.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.

1.7. CREATING A CREDENTIAL FOR BARE METAL

You need a credential to use the Red Hat Advanced Cluster Management for Kubernetes console to deploy and manage a Red Hat OpenShift Container Platform cluster in a bare metal environment. The credential specifies the connection to a provisioning node that is used as a bootstrap host virtual machine (VM) when creating the cluster.

Required access: Edit

- Prerequisites
- Preparing a provisioning host
- Managing a credential by using the console

1.7.1. Prerequisites

You need the following prerequisites before creating a credential:

- A Red Hat Advanced Cluster Management for Kubernetes hub cluster that is deployed. When managing bare metal clusters, you must have the hub cluster installed on Red Hat OpenShift Container Platform version 4.6 or later.
- Internet access for your Red Hat Advanced Cluster Management for Kubernetes hub cluster so it can create the Kubernetes cluster on your bare metal server.
- For a disconnected environment, you must have a configured mirror registry where you can copy the release images for your cluster creation. See Mirroring images for a disconnected installation in the OpenShift Container Platform documentation for more information.
- Account permissions that support installing clusters on the bare metal infrastructure.

1.7.2. Preparing a provisioning host

When you create a bare metal credential and cluster, you must have a provisioning host. The provisioning host is an available bootstrap host VM for the installation. This can be a VM or a service running Kernel-based virtual machine (KVM). You need the details of this host when you are creating the credential and the cluster. Complete the following steps to configure a provisioner host:

1. Log in to the provisioner node using **SSH**.
2. Create a non-root user (user-name) and provide that user with sudo privileges by running the following commands:

```
useradd <user-name>
passwd <password>
echo "<user-name> ALL=(root) NOPASSWD:ALL" | tee -a /etc/sudoers.d/<user-name>
chmod 0440 /etc/sudoers.d/<user-name>
```

3. Create an SSH key for the new user by entering the following command:

```
su - <user-name> -c "ssh-keygen -t rsa -f /home/<user-name>/.ssh/id_rsa -N ""
```

4. Log in as the new user on the provisioner node.

```
su - <user-name>
[user-name@provisioner ~]$
```

5. Use Red Hat Subscription Manager to register the provisioner node by entering the following commands:

   ```
   sudo subscription-manager register --username=<user-name> --password=<password> --
   auto-attach
   sudo subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms --enable=rhel-
   8-for-x86_64-baseos-rpms
   ```

   For more information about Red Hat Subscription Manager, see Using and Configuring Red Hat Subscription Manager in the Red Hat OpenShift Container Platform documentation.

6. Install required packages by running the following command:

   ```
   sudo dnf install -y libvirt qemu-kvm mkisofs python3-devel jq ipmitool
   ```

7. Modify the user to add the **libvirt** group to the newly created user.

   ```
   sudo usermod --append --groups libvirt <user-name>
   ```

8. Restart **firewalld** and enable the **http** service by entering the following commands:

   ```
   sudo systemctl start firewalld
   sudo firewall-cmd --zone=public --add-service=http --permanent
   sudo firewall-cmd --reload
   ```

9. Start and enable the **libvirtd** service by entering the following commands:

   ```
   sudo systemctl enable libvirtd --now
   ```

10. Create the default storage pool and start it by entering the following commands:

    ```
    sudo virsh pool-define-as --name default --type dir --target /var/lib/libvirt/images
    sudo virsh pool-start default
    sudo virsh pool-autostart default
    ```

11. Configure networking:

    a. Export the value of **PUB_CONN** to the name of the NIC of the **baremetal** network by running the following command:

       ```
       export PUB_CONN=<baremetal-nic-name>
       ```

    b. Configure the **baremetal** network:

       ```
       sudo nohup bash -c """
           nmcli con down "$PUB_CONN"
           nmcli con delete "$PUB_CONN"
           # RHEL 8.1 appends the word "System" in front of the connection, delete in case it
       exists
           nmcli con down "System $PUB_CONN"
       ```

```
nmcli con delete "System $PUB_CONN"
nmcli connection add ifname baremetal type bridge con-name baremetal
nmcli con add type bridge-slave ifname \"$PUB_CONN"\ master baremetal
pkill dhclient;dhclient baremetal
```

The SSH connection might disconnect after you complete this step.

c. If you are deploying with an optional provisioning network complete the following steps:

   i. Export the **provisioning** network NIC name by running the following command:

   ```
   export PROV_CONN=<prov-nic-name>
   ```

   ii. Configure the provisioning network:

   ```
   sudo nohup bash -c """
       nmcli con down "$PROV_CONN"
       nmcli con delete "$PROV_CONN"
       nmcli connection add ifname baremetal type bridge con-name provisioning
       nmcli con add type bridge-slave ifname \"$PROV_CONN\" master provisioning
       nmcli connection modify provisioning ipv6.addresses fd00:1101::1/64 ipv6.method manual
       nmcli con down provisioning
       nmcli con up provisioning
   ```

   The SSH connection might disconnect after you complete this step.

   The IPv6 address can be any address as long as it is not routable using the **baremetal** network.

   Ensure that UEFI is enabled and UEFI PXE settings are set to the IPv6 protocol when using IPv6 addressing.

   iii. Configure the IPv4 address on the provisioning network connection:

   ```
   nmcli connection modify provisioning ipv4.addresses 172.22.0.254/24 ipv4.method manual
   ```

12. Reconnect to the provisioner node by using **ssh** (if required).

    ```
    # ssh <user-name>@provisioner.<cluster-name>.<domain>
    ```

13. Verify the connection bridges have been correctly created by running the following command:

    ```
    sudo nmcli con show
    ```

    Your returned results resemble the following content:

NAME	UUID	TYPE	DEVICE

baremetal	4d5133a5-8351-4bb9-bfd4-3af264801530	bridge	baremetal
provisioning	43942805-017f-4d7d-a2c2-7cb3324482ed	bridge	provisioning
virbr0	d9bca40f-eee1-410b-8879-a2d4bb0465e7	bridge	virbr0
bridge-slave-eno1	76a8ed50-c7e5-4999-b4f6-6d9014dd0812	ethernet	eno1
bridge-slave-eno2	f31c3353-54b7-48de-893a-02d2b34c4736	ethernet	eno2

14. Create a **pull-secret.txt** file by completing the following steps:

```
vim pull-secret.txt
```

   a. In a web browser, navigate to Install OpenShift on Bare Metal with user-provisioned infrastructure, and scroll down to the *Downloads* section.

   b. Click **Copy pull secret**.

   c. Paste the contents into the **pull-secret.txt** file and save the contents in the home directory of the **user-name** user.

You are ready to create your bare metal credential.

1.7.3. Managing a credential by using the console

To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console.

Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, both for convenience and added security.

1. You can optionally add a *Base DNS domain* for your credential. If you add the base DNS domain to the credential, it is automatically populated in the correct field when you create a cluster with this credential. If you do not add the DNS domain, you can add it when you create your cluster.

2. Add your *libvirt URI*. The libvirt URI is for your provisioning node that you created for your bootstrap node. Your libvirt URI should resemble the following example:

```
<qemu+ssh>://<user-name>@<provision-host.com>/system
```

- Replace **qemu+ssh** with your method of connecting to the libvirt daemon on the provisioning host.
- Replace **user-name** with the user name that has access to create the bootstrap node on the provisioning host.
- Replace **provision-host.com** with a link to your provisioning host. This can be either an IP address or a fully-qualified domain name address.
  See Connection URIs for more information.

3. Add a list of your SSH known hosts for the provisioning host. This value can be an IP address or a fully-qualified domain name address, but is best to use the same format that you used in the libvirt URI value.

4. For disconnected installations only: Complete the fields in the **Configuration for disconnected installation** subsection with the required information:

   - *Image registry mirror*: This value contains the disconnected registry path. The path contains the hostname, port, and repository path to all of the installation images for disconnected installations. Example: **repository.com:5000/openshift/ocp-release**.
     The path creates an image content source policy mapping in the **install-config.yaml** to the Red Hat OpenShift Container Platform release images. As an example, **repository.com:5000** produces this **imageContentSource** content:

     ```
     imageContentSources:
     - mirrors:
       - registry.example.com:5000/ocp4
       source: quay.io/openshift-release-dev/ocp-release-nightly
     - mirrors:
       - registry.example.com:5000/ocp4
       source: quay.io/openshift-release-dev/ocp-release
     - mirrors:
       - registry.example.com:5000/ocp4
       source: quay.io/openshift-release-dev/ocp-v4.0-art-dev
     ```

   - *Bootstrap OS image*: This value contains the URL to the image to use for the bootstrap machine.
   - *Cluster OS image*: This value contains the URL to the image to use for Red Hat OpenShift Container Platform cluster machines.
   - *Additional trust bundle*: This value provides the contents of the certificate file that is required to access the mirror registry.
     Note: If you are deploying managed clusters from a hub that is in a disconnected environment, and want them to be automatically imported post install, add an Image Content Source Policy to the **install-config.yaml** file by using the **YAML** editor. A sample entry is shown in the following example:

     ```
     imageContentSources:
     - mirrors:
       - registry.example.com:5000/rhacm2
       source: registry.redhat.io/rhacm2
     ```

5. If you want to enable a proxy, enter the proxy information:

- HTTP proxy URL: The URL that should be used as a proxy for **HTTP** traffic.
- HTTPS proxy URL: The secure proxy URL that should be used for **HTTPS** traffic. If no value is provided, the same value as the **HTTP Proxy URL** is used for both **HTTP** and **HTTPS**.
- No proxy domains: A comma-separated list of domains that should bypass the proxy. Begin a domain name with a period **.** to include all of the subdomains that are in that domain. Add and asterisk ***** to bypass the proxy for all destinations.
- Additional trust bundle: The contents of the certificate file that is required to access the mirror registry.

6. Enter your *Red Hat OpenShift pull secret* . You can download your pull secret from Pull secret.
7. Add your *SSH private key* and your *SSH public key* so you can access the cluster. You can use an existing key, or use a key generation program to create a new one. See Generating an SSH private key and adding it to the agent for more information about how to generate a key.

You can create a cluster that uses this credential by completing the steps in Creating a cluster on bare metal.

You can edit your credential in the console.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.

1.8. CREATING A CREDENTIAL FOR RED HAT OPENSHIFT CLUSTER MANAGER

Add an OpenShift Cluster Manager credential so that you can discover clusters.

Required access: Administrator

1.8.1. Prerequisites

You need access to a console.redhat.com account. Later you will need the value that can be obtained from console.redhat.com/openshift/token.

1.8.2. Managing a credential by using the console

You need to add your credential to discover clusters. To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console.

Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, both for convenience and added security.

Your OpenShift Cluster Manager API token can be obtained from console.redhat.com/openshift/token.

You can edit your credential in the console.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.

If your credential is removed, or your OpenShift Cluster Manager API token expires or is revoked, then the associated discovered clusters are removed.

1.9. CREATING A CREDENTIAL FOR ANSIBLE AUTOMATION PLATFORM

You need a credential to use Red Hat Advanced Cluster Management for Kubernetes console to deploy and manage an Red Hat OpenShift Container Platform cluster that is using Red Hat Ansible Automation Platform.

Required access: Edit

Note: This procedure must be done before you can create an Ansible job template to enable automation on a Red Hat Advanced Cluster Management cluster.

1.9.1. Prerequisites

You must have the following prerequisites before creating a credential:

- A deployed Red Hat Advanced Cluster Management for Kubernetes hub cluster
- Internet access for your Red Hat Advanced Cluster Management for Kubernetes hub cluster
- Ansible login credentials, which includes Ansible Tower hostname and OAuth token; see Credentials for Ansible Tower.
- Account permissions that allow you to install hub clusters and work with Ansible. Learn more about Ansible users.

1.9.2. Managing a credential by using the console

To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console.

Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, both for convenience and added security.

The Ansible Token and host URL that you provide when you create your Ansible credential are automatically updated for the automations that use that credential when you edit the credential. The updates are copied to any automations that use that Ansible credential, including those related to cluster lifecycle, governance, and application management automations. This ensures that the automations continue to run after the credential is updated.

You can edit your credential in the console. Ansible credentials are automatically updated in your automation that use that credential when you update them in the credential.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.

1.10. CREATING A CREDENTIAL FOR AN ON-PREMISES ENVIRONMENT

You need a credential to use the Red Hat Advanced Cluster Management for Kubernetes console to deploy and manage a Red Hat OpenShift Container Platform cluster in an on-premises environment. The credential specifies the connections that are used for the cluster.

Required access: Edit

- Prerequisites
- Managing a credential by using the console

1.10.1. Prerequisites

You need the following prerequisites before creating a credential:

- A Red Hat Advanced Cluster Management hub cluster that is deployed.
- Internet access for your Red Hat Advanced Cluster Management for Kubernetes hub cluster so it can create the Kubernetes cluster on your infrastructure environment.
- For a disconnected environment, you must have a configured mirror registry where you can copy the release images for your cluster creation. See Mirroring images for a disconnected installation in the OpenShift Container Platform documentation for more information.
- Account permissions that support installing clusters on the on-premises environment.

1.10.2. Managing a credential by using the console

To create a credential from the Red Hat Advanced Cluster Management for Kubernetes console, complete the steps in the console.

Start at the navigation menu. Click **Credentials** to choose from existing credential options. **Tip:** Create a namespace specifically to host your credentials, both for convenience and added security.

1. You can optionally add a *Base DNS domain* for your credential. If you add the base DNS domain to the credential, it is automatically populated in the correct field when you create a cluster with this credential. If you do not add the DNS domain, you can add it when you create your cluster.
2. Enter your *Red Hat OpenShift pull secret* . You can download your pull secret from Pull secret. See Using image pull secrets for more information about pull secrets.
3. Select **Add** to create your credential.

When you are no longer managing a cluster that is using a credential, delete the credential to protect the information in the credential. Select **Actions** to delete in bulk, or select the options menu beside the credential that you want to delete.