Red Hat Advanced Cluster Management for Kubernetes 2.3

凭证

了解更多信息，了解如何创建和管理集群凭证。

Last Updated: 2023-02-24

Red Hat Advanced Cluster Management for Kubernetes 2.3 凭证

了解更多信息，了解如何创建和管理集群凭证。

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

摘要

了解更多信息，了解如何创建和管理集群凭证。

目录

第 1 章 管理凭证概述

您可以创建和管理集群凭证。要使用 Red Hat Advanced Cluster Management for Kubernetes 在云服务供应商处创建 Red Hat OpenShift Container Platform 集群，需要一个*凭证*。凭据存储云提供商的访问信息。每个提供程序帐户都需要自己的凭据，就像单个提供程序中的每个域一样。

凭据存储为 Kubernetes secret。secret 复制到受管集群的命名空间，以便受管集群的控制器可以访问 secret。更新凭证时，secret 的副本会在受管集群命名空间中自动更新。

注：对现有的受管集群，pull secret 或 SSH 密钥的更改不会反映，因为它们已使用原始凭证置备。

需要的访问权限 ： Edit

- 为 Amazon Web Services 创建凭证
- 为 Microsoft Azure 创建凭证
- 为 Google Cloud Platform 创建凭证
- 为 VMware vSphere 创建凭证
- 为 Red Hat OpenStack Platform 创建凭证
- 为裸机创建凭证
- 为 Red Hat OpenShift Cluster Manager 创建凭证
- 为 Ansible Automation Platform 创建凭证

1.1. 为 AMAZON WEB SERVICES 创建凭证

您需要一个凭证才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 Amazon Web Services (AWS) 上部署和管理 Red Hat OpenShift Container Platform 集群。

需要的访问权限 ： Edit

备注：这个过程必须在使用 Red Hat Advanced Cluster Management for Kubernetes 创建集群之前完成。

- 先决条件
- 使用控制台创建凭证
- 使用控制台编辑凭证
- 删除凭证

1.1.1. 先决条件

创建凭证前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在 Amazon Web Services (AWS) 上创建 Kubernetes 集群

- AWS 登录凭证，其中包括访问密钥 ID 和 secret 访问密钥。请参阅了解和获取您的安全凭证。
- 允许在 AWS 上安装集群的帐户权限。有关如何配置的说明，请参阅配置 AWS 帐户。

1.1.2. 使用控制台创建凭证

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建凭证，请完成以下步骤：

1. 从导航菜单中，导航到 **Credentials**。此时会显示现有的凭证。
2. 选择 **Add credential**。
3. 选择 **Amazon Web Services** 作为您的供应商。
4. 为您的凭证添加一个名称。
5. 从列表中选择凭证的命名空间。
   提示： 为方便起见，同时为了提高安全性，创建一个命名空间，专门用于托管您的凭证。
6. 您可以选择为您的凭证添加 *基本 DNS 域*。如果您将基本 DNS 域添加到凭证中，则在使用此凭证创建集群时，会自动填充到正确的字段中。
7. 为您的 AWS 帐户添加 *AWS 访问密钥 ID*。登录 AWS 以查找此 ID。
8. 添加 *AWS Secret 访问密钥*。
9. 输入您的 *Red Hat OpenShift pull secret*。您可以从 Pull secret 下载 pull secret。
10. 添加可让您连接到集群的 *SSH 私钥*和 *SSH 公钥*。您可以使用现有密钥对，或使用密钥生成程序创建新密钥对。请参阅生成 SSH 私钥并将其添加到代理中，以了解有关如何生成密钥的更多信息。
11. 点击 **Create**。
12. 查看新凭据信息，然后单击 **Add**。添加凭证时，会将其添加到凭证列表中。

要创建使用此凭证的集群，您可以完成在 Amazon Web Services 上创建集群中的步骤。

1.1.3. 使用控制台编辑凭证

完成以下步骤，在 Amazon Web Services (AWS) 上为 Red Hat OpenShift Container Platform 集群编辑凭证：

1. 从导航菜单中，导航到 **Credentials**。此时会显示现有的凭证。
2. 查找您要编辑的凭证，并点击以更新凭证。
3. 点 **Edit** 并为 Amazon Web Services (AWS) 输入新的云凭证。
4. 单击 **Save** 以更新凭据。

如果使用这个供应商连接创建集群，则来自 **<cluster-namespace>** 的 **<cluster-name>-aws-creds>** secret 将使用新凭证进行更新。

注：更新凭证不适用于集群池声明的集群。

1.1.4. 删除凭证

当您不再管理使用凭证的集群时，请删除凭证来保护凭证中的信息。

1. 从导航菜单中，导航到 **Credentials**。
2. 选择要批量删除的 **Actions**，或者选择您要删除的凭证旁边的选项菜单。
3. 选择 **Delete credentials** 或 **Delete credential**。

1.2. 为 MICROSOFT AZURE 创建凭证

您需要一个凭证才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 Microsoft Azure 上创建和管理 Red Hat OpenShift Container Platform 集群。

需要的访问权限 ： Edit

注：这个过程是使用 Red Hat Advanced Cluster Management for Kubernetes 创建集群的先决条件。

- 先决条件
- 使用控制台创建凭证
- 删除凭证

1.2.1. 先决条件

创建凭证前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群。
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在 Azure 上创建 Kubernetes 集群
- Azure 登录凭证，其中包括您的基域资源组和 Azure Service Principal JSON。请参阅 azure.microsoft.com。
- 允许在 Azure 上安装集群的帐户权限。如需更多信息，请参阅如何配置 Cloud Services 和配置 Azure 帐户。

1.2.2. 使用控制台创建凭证

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建凭证，请完成以下步骤：

1. 从导航菜单中，导航到 **Credentials**。此时会显示现有的凭证。
2. 选择 **Add credential**。
3. 选择 **Microsoft Azure** 作为您的供应商。
4. 为您的凭证添加一个名称。
5. 从列表中选择凭证的命名空间。
   提示： 为方便起见，同时为了提高安全性，您可以创建一个命名空间，专门用于托管凭证。

6. 您可以选择为您的凭证添加 *基本 DNS 域*。如果您将基本 DNS 域添加到凭证中，则在使用此凭证创建集群时，会自动填充到正确的字段中。

7. 为您的 Azure 帐户添加 *基本域资源组名称*。此条目是您使用 Azure 帐户创建的资源名称。您可以在 Azure 界面中选择 **Home** > **DNS Zones** 来查找您的基域资源组名称。您的基本域资源组名称位于条目的 *Resource Group* 列中，其中包含应用到您的帐户的基本 DNS 域。

8. 添加您的 *客户端 ID*。当您使用以下命令创建服务主体时，这个值作为 **appId** 属性被生成：

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

   将 *service_principal* 替换为您的服务主体名。

9. 添加您的 *客户端 Secret*。当您使用以下命令创建服务主体时，这个值作为 **password** 属性被生成：

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

   将 *service_principal* 替换为您的服务主体名。

10. 添加您的 *订阅 ID*。这个值是以下命令输出中的 **id** 属性：

    ```
    az account show
    ```

11. 添加您的 *租户 ID*。这个值是以下命令输出中的 **tenantId** 属性：

    ```
    az account show
    ```

12. 输入您的 *Red Hat OpenShift pull secret*。您可以从 Pull secret 下载 pull secret。

13. 添加用于连接到集群的 *SSH 私钥*和 *SSH 公钥*。您可以使用现有密钥对，或使用密钥生成程序创建新密钥对。请参阅生成 SSH 私钥并将其添加到代理中，以了解有关如何生成密钥的更多信息。

14. 点击 **Create**。

15. 查看新凭据信息，然后单击 **Add**。添加凭证时，会将其添加到凭证列表中。

要创建使用此凭证的集群，您可以完成在 Microsoft Azure 上创建集群中的步骤。

1.2.3. 删除凭证

当您不再管理使用凭证的集群时，请删除凭证来保护凭证中的信息。

1. 从导航菜单中，导航到 **Credentials**。

2. 选择要批量删除的 **Actions**，或者选择您要删除的凭证旁边的选项菜单。

3. 选择 **Delete credentials** 或 ***Delete credential**。

1.3. 为 GOOGLE CLOUD PLATFORM 创建凭证

您需要一个凭证才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 Google Cloud Platform (GCP) 上创建和管理 Red Hat OpenShift Container Platform 集群。

需要的访问权限 ： Edit

注：这个过程是使用 Red Hat Advanced Cluster Management for Kubernetes 创建集群的先决条件。

- 先决条件
- 使用控制台创建凭证
- 删除凭证

1.3.1. 先决条件

创建凭证前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在 GCP 上创建 Kubernetes 集群
- GCP 登录凭证，其中包括用户 Google Cloud Platform 项目 ID 和 Google Cloud Platform 服务帐户 JSON 密钥。请参阅创建和管理项目。
- 允许在 GCP 上安装集群的帐户权限。有关如何配置帐户的说明，请参阅配置 GCP 项目。

1.3.2. 使用控制台创建凭证

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建凭证，请完成以下步骤：

1. 从导航菜单中，导航到 **Credentials**。此时会显示现有的凭证。
2. 选择 **Add credential**。
3. 选择 **Google Cloud Platform** 作为您的供应商。
4. 为您的凭证添加一个名称。
5. 从列表中选择凭证的命名空间。
   提示： 为方便和安全起见，创建一个命名空间，专门用于托管您的凭证。
6. 您可以选择为您的凭证添加 *基本 DNS 域*。如果您将基本 DNS 域添加到凭证中，则在使用此凭证创建集群时，会自动填充到正确的字段中。
7. 为您的 GCP 帐户添加 *Google Cloud Platform 项目 ID*。登录到 GCP 以检索您的设置。
8. 添加 *Google Cloud Platform 服务帐户 JSON 密钥*。完成以下步骤创建带有正确权限的服务帐户：
   a. 在 GCP 主菜单中，选择 **IAM & Admin** 并启动 **Service Accounts applet**。
   b. 选择 **Create Service Account**。
   c. 提供服务帐户的 *Name*、*Service account ID* 和 *Description*。
   d. 选择 **Create** 来创建服务帐户。
   e. 选择 **Owner** 角色，然后点 **Continue**。
   f. 点 **Create Key**

g. 选择 **JSON** 并点 **Create**。

h. 将生成的文件保存到您的计算机中。

i. 提供 *Google Cloud Platform 服务帐户 JSON 密钥* 的内容。

9. 输入您的 *Red Hat OpenShift pull secret*。您可以从 Pull secret 下载 pull secret。

10. 添加 *SSH 私钥*和 *SSH 公钥*以便您访问集群。您可以使用现有密钥对，或使用密钥生成程序创建新密钥对。请参阅生成 SSH 私钥并将其添加到代理中，以了解有关如何生成密钥的更多信息。

11. 点击 **Create**。

12. 查看新凭据信息，然后单击 **Add**。添加凭证时，会将其添加到凭证列表中。

您可以在创建集群时使用此连接，完成在 Google Cloud Platform 上创建集群 中的步骤。

1.3.3. 删除凭证

当您不再管理使用凭证的集群时，请删除凭证来保护凭证中的信息。

1. 从导航菜单中，导航到 **Credentials**。

2. 选择要批量删除的 **Actions**，或者选择您要删除的凭证旁边的选项菜单。

3. 选择 **Delete credentials** 或 ***Delete credential**。

1.4. 为 VMWARE VSPHERE 创建凭证

您需要一个凭证才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 VMware vSphere 上部署和管理 Red Hat OpenShift Container Platform 集群。**注：**仅支持 OpenShift Container Platform 版本 4.5.x 及更新的版本。

需要的访问权限 ： Edit

注：必须在使用 Red Hat Advanced Cluster Management 创建集群前完成此步骤。

- 先决条件
- 使用控制台创建凭证
- 删除凭证

1.4.1. 先决条件

创建凭证前必须满足以下先决条件：

- 在 OpenShift Container Platform 版本 4.6 或更高版本上部署了 Red Hat Advanced Cluster Management hub 集群。
- 可通过互联网访问 Red Hat Advanced Cluster Management hub 集群，以便它在 VMware vSphere 上创建 Kubernetes 集群。
- 使用安装程序置备的基础架构时为 OpenShift Container Platform 配置了 VMware vSphere 登录凭证和 vCenter 要求。请参阅在 vSphere 上安装集群。这些凭证包括以下信息：

- vCenter 帐户权限。
- 集群资源。
- DHCP 可用。
- ESXi 主机的时间已同步（例如： NTP）。

1.4.2. 使用控制台创建凭证

要从 Red Hat Advanced Cluster Management 控制台创建凭证，请完成以下步骤：

1. 从导航菜单中，导航到 **Credentials**。此时会显示现有的凭证。
2. 选择 **Add credential**。
3. 选择 **VMware vSphere** 作为您的供应商。
4. 为您的凭证添加一个名称。
5. 从列表中选择凭证的命名空间。
   提示： 为方便起见，同时为了提高安全性，创建一个命名空间，专门用于托管您的凭证。
6. 您可以选择为您的凭证添加 *基本 DNS 域*。如果您将基本 DNS 域添加到凭证中，则在使用此凭证创建集群时，会自动填充到正确的字段中。
7. 添加 *VMware vCenter 服务器完全限定主机名或 IP 地址*。该值必须在 vCenter 服务器 root CA 证书中定义。如果可能，请使用完全限定主机名。
8. 添加 *VMware vCenter 用户名*。
9. 添加 *VMware vCenter 密码*。
10. 添加 *VMware vCenter root CA 证书*。
    a. 您可以使用 VMware vCenter 服务器的证书在 **download.zip** 软件包中下载证书，地址为 **https://<vCenter_address>/certs/download.zip**。将 *vCenter_address* 替换为 vCenter 服务器的地址。
    b. 解包 **download.zip**。
    c. 使用 **certs/<platform>** 目录中包含 **.0** 扩展名的证书。**提示：** 您可以使用 **ls certs/<platform>** 命令列出平台的所有可用证书。
    将 ***<platform>*** 替换为您的平台的缩写：**lin**、**mac** 或 **win**.

    例如： **certs/lin/3a343545.0**
11. 添加 *VMware vSphere 集群名称*。
12. 添加 *VMware vSphere 数据中心*。
13. 添加 *VMware vSphere 默认数据存储*。
14. 输入您的 *Red Hat OpenShift pull secret*。您可以从 Pull secret 下载 pull secret。
15. 添加可让您连接到集群的 *SSH 私钥*和 *SSH 公钥*。您可以使用现有密钥对，或使用密钥生成程序创建新密钥对。如需更多信息，请参阅生成 SSH 私钥并将其添加到代理中。

16. 点击 **Create**。
17. 查看新凭据信息，然后单击 **Add**。添加凭证时，会将其添加到凭证列表中。

要创建使用此凭证的集群，您可以完成在 VMware vSphere 上创建集群 中的步骤。

1.4.3. 删除凭证

当您不再管理使用凭证的集群时，请删除凭证来保护凭证中的信息。

1. 从导航菜单中，导航到 **Credentials**。
2. 选择您要删除的凭证旁的选项菜单。
3. 选择 **Delete credential**。

1.5. 为 RED HAT OPENSTACK 创建凭证

您需要一个凭证才能使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在 Red Hat OpenStack Platform 上部署和管理 Red Hat OpenShift Container Platform 集群。注：仅支持 OpenShift Container Platform 版本 4.5.x 及更新的版本。

注：必须在使用 Red Hat Advanced Cluster Management 创建集群前完成此步骤。

1.5.1. 先决条件

创建凭证前必须满足以下先决条件：

- 在 OpenShift Container Platform 版本 4.6 或更高版本上部署了 Red Hat Advanced Cluster Management hub 集群。
- 可通过互联网访问 Red Hat Advanced Cluster Management hub 集群，以便它在 Red Hat OpenStack Platform 上创建 Kubernetes 集群。
- 使用安装程序置备的基础架构时，为 OpenShift Container Platform 配置 Red Hat OpenStack Platform 登录凭证和 Red Hat OpenStack Platform 要求。请参阅在 OpenStack 上安装集群。
- 下载或创建 **clouds.yaml** 文件来访问 CloudStack API。在 **clouds.yaml** 文件中：
  - 确定要使用的云身份验证部分名称。
  - 在 **username** 行后马上添加一个 **password** 行。

1.5.2. 使用控制台创建凭证

要从 Red Hat Advanced Cluster Management 控制台创建凭证，请完成以下步骤：

1. 从导航菜单中，导航到 **Credentials**。在 *Credentials* 页面中，会显示现有的凭证。
2. 选择 **Add credentials** 以在 *Add credentials_* 编辑器中输入凭证信息。
3. 选择 **Red Hat OpenStack Platform** 作为您的凭证类型。
4. 为您的凭证添加一个名称。
5. 从列表中选择凭证的命名空间。

提示： 为方便起见，同时为了提高安全性，创建一个命名空间，专门用于托管您的凭证。

6. 添加 Red Hat OpenStack Platform **cloud.yaml** 文件内容。**clouds.yaml** 文件的内容（包括密码）提供了连接到 Red Hat OpenStack Platform 服务器所需的信息。文件内容**必**须包含密码，它是一个紧接在 **username** 后面的一个新行。

7. 添加您的 Red Hat OpenStack Platform 名称。此条目是在 **clouds.yaml** 的 cloud 部分中指定的名称，用于建立与 Red Hat OpenStack Platform 服务器的通信。

8. 您可以选择为您的凭证添加基本 DNS 域。如果您将基本 DNS 域添加到凭证中，则在使用此凭证创建集群时，会自动填充到正确的字段中。

9. 输入 Red Hat OpenShift Pull Secret。您可以从 Pull secret 下载 pull secret。

10. 添加可让您连接到集群的 SSH 私钥和 SSH 公钥。您可以使用现有密钥对，或使用密钥生成程序创建新密钥对。如需更多信息，请参阅生成 SSH 私钥并将其添加到代理中。

11. 点击 **Create**。

12. 查看新凭据信息，然后单击 **Add**。添加凭证时，会将其添加到凭证列表中。

要创建使用此凭证的集群，您可以完成在 Red Hat OpenStack Platform 上创建集群 中的步骤。

1.5.3. 删除凭证

当您不再管理使用凭证的集群时，请删除凭证来保护凭证中的信息。

1. 从导航菜单中，导航到 **Credentials**。

2. 选择要批量删除的 **Actions**，或者选择您要删除的凭证旁边的选项菜单。

3. 选择 **Delete credentials** 或 ***Delete credential**。

1.6. 为裸机创建凭证

您需要一个凭证来使用 Red Hat Advanced Cluster Management for Kubernetes 控制台在裸机环境中部署和管理 Red Hat OpenShift Container Platform 集群。凭证指定到在创建集群时用作 bootstrap 主机虚拟机 (VM) 的置备节点的连接。

需要的访问权限 ： Edit

- 先决条件
- 准备置备主机
- 使用控制台创建凭证
- 删除凭证

1.6.1. 先决条件

创建凭证前需要满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群。在管理裸机集群时，必须在 Red Hat OpenShift Container Platform 版本 4.6 或更高版本上安装了 hub 集群。

- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群，以便它在裸机服务器上创建 Kubernetes 集群
- 对于断开连接的环境，您必须配置了一个镜像 registry，您可以在其中复制发行镜像以进行集群创建。如需更多信息，请参阅 OpenShift Container Platform 文档中的用于断开连接的安装的镜像。
- 支持在裸机基础架构上安装集群的帐户权限。

1.6.2. 准备置备主机

创建裸机凭证和集群时，必须具有可用的置备主机。置备主机为安装提供 bootstrap 主机虚拟机。它可以是虚拟机，也可以是运行基于内核的虚拟机 (KVM) 的服务。创建凭证和集群时，您需要此主机的详细信息。完成以下步骤以配置置备主机：

1. 使用 **SSH** 登录 provisioner 节点。
2. 运行以下命令，创建非 root 用户 (user-name) 并为该用户提供 sudo 权限：

```
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. 输入以下命令为新用户创建 SSH 密钥：

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

4. 使用新创建的用户登陆到 provisioner 节点。

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

5. 输入以下命令使用 Red Hat Subscription Manager 来注册 provisioner 节点：

```
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
```

   如需有关 Red Hat Subscription Manager 的更多信息，请参阅 Red Hat OpenShift Container Platform 文档中的使用和配置 Red Hat Subscription Manager。

6. 运行以下命令安装所需的软件包：

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

7. 修改用户以便为新创建的用户中添加 **libvirt** 组。

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

8. 输入以下命令重启 **firewalld** 并启用 **http** 服务：

```
sudo systemctl start firewalld
```

```
sudo firewall-cmd --zone=public --add-service=http --permanent
sudo firewall-cmd --add-port=5000/tcp --zone=libvirt  --permanent
sudo firewall-cmd --add-port=5000/tcp --zone=public   --permanent
sudo firewall-cmd --reload
```

9. 输入以下命令启动并启用 **libvirtd** 服务：

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

10. 输入以下命令创建默认存储池并启动它：

```
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. 查看 followsig 示例来配置网络：

- *置备网络（IPv4 地址）*

```
sudo nohup bash -c """
    nmcli con down "$PROV_CONN"
    nmcli con delete "$PROV_CONN"
    # RHEL 8.1 appends the word "System" in front of the connection, delete in case it
exists
    nmcli con down "System $PROV_CONN"
    nmcli con delete "System $PROV_CONN"
    nmcli connection add ifname provisioning type bridge con-name provisioning
    nmcli con add type bridge-worker ifname "$PROV_CONN" master provisioning
    nmcli connection modify provisioning ipv4.addresses 172.22.0.1/24 ipv4.method
manual
    nmcli con down provisioning
    nmcli con up provisioning"""
```

完成此步骤后，SSH 连接可能会断开。

IPv4 地址可以是任何无法使用 baremetal 网络路由的地址。

- *置备网络（IPv6 地址）*

```
sudo nohup bash -c """
    nmcli con down "$PROV_CONN"
    nmcli con delete "$PROV_CONN"
    # RHEL 8.1 appends the word "System" in front of the connection, delete in case it
exists
    nmcli con down "System $PROV_CONN"
    nmcli con delete "System $PROV_CONN"
    nmcli connection add ifname provisioning type bridge con-name provisioning
    nmcli con add type bridge-worker ifname "$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"""
```

完成此步骤后，SSH 连接可能会断开。

IPv6 地址可以是任何无法使用 baremetal 网络路由的地址。

在使用 IPv6 地址时，请确保启用了 UEFI，并且将 UEFI PXE 设置设为 IPv6 协议。

12. 使用 SSH 重新连接到 provisioner 节点（如果需要）。

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

13. 运行以下命令验证连接网桥是否已正确创建：

```
nmcli con show
```

您返回的结果类似以下内容：

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-worker-eno1	76a8ed50-c7e5-4999-b4f6-6d9014dd0812	Ethernet	eno1

bridge-worker-eno2	f31c3353-54b7-48de-893a-02d2b34c4736	Ethernet	eno2

14. 通过以下步骤创建 **pull-secret.txt** 文件：

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

a. 在 Web 浏览器中，导航到 Install OpenShift on Bare Metal with user-provisioned infrastructure，再向下滚动到 *Downloads* 部分。

b. 点 **Copy pull secret**。

c. 将内容粘贴到 **pull-secret.txt** 文件中，并将内容保存到 **user-name** 用户的主目录中。

您已准备好创建裸机凭证。

1.6.3. 使用控制台创建凭证

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建凭证，请完成以下步骤：

1. 从导航菜单中，导航到 **Credentials**。此时会显示现有的凭证。
2. 选择 **Add credential**。
3. 选择 **Bare metal** 作为您的供应商。
4. 为您的凭证添加一个名称。
5. 从列表中选择凭证的命名空间。
   提示： 为方便起见，同时为了提高安全性，创建一个命名空间，专门用于托管您的凭证。
6. 您可以选择为您的凭证添加*基本 DNS 域*。如果您将基本 DNS 域添加到凭证中，则在使用此凭证创建集群时，会自动填充到正确的字段中。如果没有添加 DNS 域，您可以在创建集群时添加它。
7. 添加 *libvirt URI*。libvirt URI 适用于您为 bootstrap 节点创建的置备节点。libvirt URI 应该类似以下示例：

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

- 使用您连接到调配主机上的 libvirt 守护进程的方法替换 **qemu+ssh**。
- 使用有权在置备主机上创建 bootstrap 节点的用户名替换 **user-name**。
- 将 **provision-host.com** 替换为您的调配主机的链接。这可以是 IP 地址或完全限定域名地址。
  如需更多信息，请参阅连接 URI。

8. 为调配主机添加 SSH 已知主机的列表。这个值可以是 IP 地址或完全限定域名地址，但最好使用您在 libvirt URI 值中使用的相同格式。

9. 输入您的 *Red Hat OpenShift pull secret*。您可以从 Pull secret 下载 pull secret。

10. 添加 *SSH 私钥* 和 *SSH 公钥* 以便您可以访问集群。您可以使用现有密钥，或使用密钥生成程序创建新密钥。请参阅生成 SSH 私钥并将其添加到代理中，以了解有关如何生成密钥的更多信息。

11. 只用于断开连接的安装： 使用所需信息完成 为**断开连接的安装**部分中的字段：

    - *Image registry mirror*：此值包含断开连接的 registry 路径。该路径包含所有用于断开连接的安装镜像的主机名、端口和库路径。示例： **repository.com:5000/openshift/ocp-release**。该路径会在 **install-config.yaml** 中创建一个到 Red Hat OpenShift Container Platform 发行镜像的镜像内容源策略映射。例如，**repository.com:5000** 生成此 **imageContentSource** 内容：

      ```
      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*：此值包含用于 bootstrap 机器的镜像的 URL。

    - *Cluster OS image*：此值包含用于 Red Hat OpenShift Container Platform 集群机器的镜像的 URL。

    - *Additional trust bundle* ：此值提供访问镜像 registry 所需的证书文件内容。
      注： 如果您要从断开连接的环境中的一个 hub 部署受管集群，并希望在安装后自动导入它们，使用 **YAML** 编辑器将镜像内容源策略添加到 **install-config.yaml** 文件中。以下示例中显示了一个示例：

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

12. 点击 **Create**。

13. 查看新凭据信息，然后单击 **Add**。添加凭证时，会将其添加到凭证列表中。

要创建使用此凭证的集群，您可以完成在裸机上创建集群中的步骤。

1.6.4. 删除凭证

当您不再管理使用凭证的集群时，请删除凭证来保护凭证中的信息。

1. 从导航菜单中，导航到 **Credentials**。

2. 选择您要删除的凭证的选项菜单。

3. 选择 **Delete credential**。

1.7. 为 RED HAT OPENSHIFT CLUSTER MANAGER 创建凭证

添加 OpenShift Cluster Manager 凭证，以便您可以发现集群。

需要的访问权限：Administrator

1.7.1. 先决条件

您需要一个 console.redhat.com 帐户。稍后，您将需要这个值，它可从 console.redhat.com/openshift/token 获取。

1.7.2. 添加凭证

最佳实践：在每个命名空间中仅创建一个凭证。

您需要添加凭证来发现集群。如果没有凭证，请查看以下过程。

1. 从产品导航中，点 **Credentials**。
2. 点 **Add credentials** 按钮，进入 *Add credentials* 页面。
3. 选择 OpenShift Cluster Manager 凭据*type*，然后点 **Next**。
4. 输入凭证的以下基本信息：
   - 输入凭证的任何唯一名称。
   - 输入一个您可以访问的命名空间。分配给此命名空间的所有用户也可以访问这些资源。与此凭证相关的所有发现资源都在同一命名空间中创建。您创建的每个凭证都必须分配给一个唯一的现有命名空间。
5. 点击 **Next**。
6. 输入 OpenShift Cluster Manager API 令牌，该令牌可以从 console.redhat.com/openshift/token 获取。
7. 点 **Next** 查看您的选择或返回一个步骤。
8. 查看新凭据信息，然后单击 **Add**。添加凭证时，会将其添加到凭证列表中。

1.7.3. 删除凭证

当您不再管理使用凭证的集群时，请删除凭证来保护凭证中的信息。

1. 从导航菜单中，导航到 **Credentials**。
2. 选择要批量删除的 **Actions**，或者选择您要删除的凭证旁边的选项菜单。
3. 选择 **Delete credentials** 或 **Delete credential**。

如果您的凭证被删除，或者 OpenShift Cluster Manager API 令牌已过期或被撤销，则会删除相关的发现集群。

1.8. 为 ANSIBLE AUTOMATION PLATFORM 创建凭证

您需要一个凭证来使用 Red Hat Advanced Cluster Management for Kubernetes 控制台来部署和管理使用 Red Hat Ansible Automation Platform 的 Red Hat OpenShift Container Platform 集群。

需要的访问权限 ： Edit

备注：这个过程必须在使用 Red Hat Advanced Cluster Management for Kubernetes 创建集群之前完成。

- 先决条件
- 使用控制台创建凭证
- 删除凭证

1.8.1. 先决条件

创建凭证前必须满足以下先决条件：

- 已部署 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- 可通过互联网访问 Red Hat Advanced Cluster Management for Kubernetes hub 集群
- Ansible 登录凭据，其中包括 Ansible Tower 主机名和 OAuth 令牌；请参阅 Ansible Tower 的凭据。
- 允许您安装 hub 集群并使用 Ansible 的帐户权限。了解有关 Ansible 用户的更多信息。

1.8.2. 使用控制台创建凭证

要从 Red Hat Advanced Cluster Management for Kubernetes 控制台创建凭证，请完成以下步骤：

1. 从导航菜单中，导航到 **Credentials**。此时会显示现有的凭证选项。
2. 选择 **Add credential**。
3. 选择 **Red Hat Ansible Automation Platform** 作为您的供应商。
4. 为您的凭证添加一个名称。
5. 从列表中选择凭证的命名空间。
   提示： 为方便起见，同时为了提高安全性，创建一个命名空间，专门用于托管您的凭证。
6. 点击 **Create**。
7. 查看新凭据信息，然后单击 **Add**。添加凭证时，会将其添加到凭证列表中。

从 Red Hat Advanced Cluster Management 版本 2.3 开始，在创建 Ansible 凭证时提供的 Ansible Token 和主机 URL 会自动更新在编辑凭证时使用该凭证的自动化。更新复制到任何使用 Ansible 凭据的自动化中，包括与集群生命周期、监管和应用程序管理自动化相关的自动化。这可确保自动化在更新凭证后继续运行。

Ansible 凭据在自动化中自动更新，您在凭据中更新该凭据时使用该凭据。

1.8.3. 删除凭证

当您不再管理使用凭证的集群时，请删除凭证来保护凭证中的信息。

1. 从导航菜单中，导航到 **Credentials**。
2. 选择要批量删除的 **Actions**，或者选择您要删除的凭证旁边的选项菜单。
3. 选择 **Delete credentials** 或 **Delete credential**。