Red Hat Advanced Cluster Management for Kubernetes 2.4

認証情報

クラスター認証情報の作成および管理の詳細

Last Updated: 2022-10-02

Red Hat Advanced Cluster Management for Kubernetes 2.4 認証情報

クラスター認証情報の作成および管理の詳細

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.

法律上の通知

概要

クラスター認証情報の作成および管理の詳細をご覧ください。

目次

第1章 認証情報の管理の概要

クラスターの認証情報を作成して管理できます。Red Hat Advanced Cluster Management for Kubernetes でクラウドサービスプロバイダーに Red Hat OpenShift Container Platform クラスターを作成するには、**認証情報** が必要です。認証情報では、クラウドプロバイダーのアクセス情報を保存します。1 つのプロバイダーのドメインごとに独自の認証情報が必要になるのと同様に、プロバイダーアカウントごとに独自の認証情報が必要です。

認証情報は Kubernetes Secret として保存されます。シークレットはマネージドクラスターの namespace にコピーされ、マネージドクラスターのコントローラーがシークレットにアクセスできるようになります。認証情報が更新されると、シークレットのコピーはマネージドクラスターの namespace で自動的に更新されます。

注記: 元の認証情報を使用してすでにプロビジョニングされているため、クラウドプロバイダーの認証情報のプルシークレットまたは SSH キーへの変更は、既存のマネージドクラスターに反映されません。

必要なアクセス: 編集

- Amazon Web Services の認証情報の作成
- Microsoft Azure の認証情報の作成
- Google Cloud Platform の認証情報の作成
- VMware vSphere の認証情報の作成
- Red Hat OpenStack Platform の認証情報の作成
- ベアメタルの認証情報の作成
- Red Hat OpenShift Cluster Manager の認証情報の作成
- Ansible Automation Platform の認証情報の作成
- オンプレミス環境の認証情報の作成

1.1. AMAZON WEB SERVICES の認証情報の作成

Red Hat Advanced Cluster Management for Kubernetes コンソールを使用して、Amazon Web Services (AWS) で Red Hat OpenShift Container Platform クラスターを作成して管理するには、認証情報が必要です。

必要なアクセス: 編集

注記: Red Hat Advanced Cluster Management for Kubernetes でクラスターを作成する前に、以下の手順を実行する必要があります。

1.1.1. 前提条件

認証情報を作成する前に、以下の前提条件を満たす必要があります。

- Red Hat Advanced Cluster Management for Kubernetes のハブクラスターをデプロイしておく。

- Amazon Web Services (AWS) で Kubernetes クラスターを作成できるようにする Red Hat Advanced Cluster Management for Kubernetes ハブクラスターでのインターネットアクセスがある。
- アクセスキー ID およびシークレットアクセスキーなど、AWS のログイン認証情報。Understanding and getting your AWS credentials を参照してください。
- AWS でクラスターをインストールできるようにするアカウントのパーミッション。設定の方法は、AWS アカウントの設定 を参照してください。

1.1.2. コンソールを使用した認証情報の管理

Red Hat Advanced Cluster Management for Kubernetes コンソールから認証情報を作成するには、以下のコンソールでの手順を実行します。

ナビゲーションメニューから開始します。**Credentials** をクリックし、既存の認証情報オプションから選択します。**ヒント:** 便宜上およびセキュリティー上、認証情報のホスト専用の namespace を作成します。

オプションで、認証情報の **ベース DNS ドメイン** を追加できます。ベース DNS ドメインを認証情報に追加した場合には、この認証情報でクラスターを作成すると、このベース DNS ドメインは自動的に正しいフィールドに設定されます。以下の手順を参照してください。

1. AWS アカウントの **AWS アクセスキー ID** を追加します。AWS にログインして ID を見つけます。
2. Red Hat Advanced Cluster Management で、新しい**AWS シークレットアクセスキーの**コンテンツを提供します。
3. **Red Hat OpenShift pull secret** を入力します。Pull secret からプルシークレットをダウンロードします。
4. **SSH 秘密鍵** と **SSH 公開鍵** を追加し、クラスターに接続できるようにします。既存のキーペアを使用するか、キー生成プログラムで新しいキーを作成できます。

キー生成の方法は、SSH プライベートキーの生成およびエージェントへの追加 を参照してください。

「Amazon Web Services でのクラスターの作成」の手順を実行して、この認証情報を使用するクラスターを作成 します。

コンソールで認証情報を編集できます。このプロバイダー接続を使用してクラスターが作成された場合には、**<cluster-namespace>** からの **<cluster-name>-aws-creds>** シークレットが新規の認証情報に更新されます。

注記: クラスタープールが要求したクラスターでは、認証情報は更新されません。

認証情報を使用するクラスターの管理を終了する場合には、認証情報を削除して認証情報内にある情報を保護します。**Actions** を選択して、一括削除するか、削除する認証情報の横にあるオプションメニューを選択します。

1.2. MICROSOFT AZURE の認証情報の作成

Red Hat Advanced Cluster Management for Kubernetes コンソールを使用して、Microsoft Azure または Microsoft Azure Government で Red Hat OpenShift Container Platform クラスターを作成して管理するには、認証情報が必要です。

必要なアクセス: 編集

注記: 以下の手順は、Red Hat Advanced Cluster Management for Kubernetes でクラスターを作成するための前提条件となっています。

1.2.1. 前提条件

認証情報を作成する前に、以下の前提条件を満たす必要があります。

- Red Hat Advanced Cluster Management for Kubernetes のハブクラスターをデプロイしておく。
- Azure で Kubernetes クラスターを作成できるようにする Red Hat Advanced Cluster Management for Kubernetes ハブクラスターでのインターネットアクセスがある。
- ベースドメインのリソースグループおよび Azure Service Principal JSON などの Azure ログイン認証情報。azure.microsoft.com を参照してください。
- Azre でクラスターがインストールできるようにするアカウントのパーミッション。詳細は、How to configure Cloud Services および Azure アカウントの設定 を参照してください。

1.2.2. コンソールを使用した認証情報の管理

Red Hat Advanced Cluster Management for Kubernetes コンソールから認証情報を作成するには、以下のコンソールでの手順を実行します。ナビゲーションメニューから開始します。**Credentials** をクリックし、既存の認証情報オプションから選択します。**ヒント:** 便宜上およびセキュリティー上、認証情報のホスト専用の namespace を作成します。

1. **オプション:** 認証情報の **ベース DNS ドメイン** を追加します。ベース DNS ドメインを認証情報に追加した場合には、この認証情報でクラスターを作成すると、このベース DNS ドメインは自動的に正しいフィールドに設定されます。
2. クラスターの環境が **AzurePublicCloud** または、**AzureUSGovernmentCloud** であるかを選択します。この設定は Azure Government 環境とは異なるため、これが正しく設定されていることを確認します。
3. Azure アカウントの **ベースドメインリソースグループ名** を追加します。このエントリーは、Azure アカウントで作成したリソース名です。Azure インターフェースで **Home** > **DNS Zones** を選択することで、ベースドメインのリソースグループ名を検索できます。ベースドメインリソースグループ名を見つけるには、Azure CLI で Azure サービスプリンシパルの作成 を参照してください。
4. Red Hat Advanced Cluster Management で、**クライアント ID** のコンテンツを提供します。この値は、以下のコマンドを使用してサービスプリンシパルを作成すると、 **appId** プロパティーとして設定されます。

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

   service_principal は、お使いのサービスプリンシパル名に置き換えます。
5. **Client Secret** を追加します。この値は、以下のコマンドを使用してサービスプリンシパルを作成すると、 **password** プロパティーとして設定されます。

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

   service_principal は、お使いのサービスプリンシパル名に置き換えます。

6. **Subscription ID** を追加します。以下のコマンドの出力では、この値は、**id** プロパティーになります。

```
az account show
```

7. **Tenant ID** を追加します。以下のコマンドの出力では、この値は、**tenantId** プロパティーになります。

```
az account show
```

8. **Red Hat OpenShift pull secret** を入力します。Pull secret からプルシークレットをダウンロードします。

9. クラスターへの接続に使用する **SSH 秘密鍵** と **SSH 公開鍵** を追加します。既存のキーペアを使用するか、キー生成プログラムで新しいキーを作成できます。キー生成の方法は、SSH プライベートキーの生成およびエージェントへの追加 を参照してください。

「Microsoft Azure でのクラスターの作成」の手順を実行して、この認証情報を使用するクラスターを作成 します。

コンソールで認証情報を編集できます。

認証情報を使用するクラスターの管理を終了する場合には、認証情報を削除して認証情報内にある情報を保護します。**Actions** を選択して、一括削除するか、削除する認証情報の横にあるオプションメニューを選択します。

1.3. GOOGLE CLOUD PLATFORM の認証情報の作成

Red Hat Advanced Cluster Management for Kubernetes コンソールを使用して、Google Cloud Platform (GCP) で Red Hat OpenShift Container Platform クラスターを作成して管理するには、認証情報が必要です。

必要なアクセス: 編集

注記: 以下の手順は、Red Hat Advanced Cluster Management for Kubernetes でクラスターを作成するための前提条件となっています。

1.3.1. 前提条件

認証情報を作成する前に、以下の前提条件を満たす必要があります。

- Red Hat Advanced Cluster Management for Kubernetes のハブクラスターをデプロイしておく。
- GCP で Kubernetes クラスターを作成できるようにする Red Hat Advanced Cluster Management for Kubernetes ハブクラスターでのインターネットアクセスがある。
- ユーザーの Google Cloud Platform プロジェクト ID および Google Cloud Platform サービスアカウント JSON キーなど、GCP ログインの認証情報。「Creating and managing projects」を参照してください。
- GCP でクラスターがインストールできるようにするアカウントのパーミッション。アカウントの設定方法は、GCP プロジェクトの設定 を参照してください。

1.3.2. コンソールを使用した認証情報の管理

Red Hat Advanced Cluster Management for Kubernetes コンソールから認証情報を作成するには、以下のコンソールでの手順を実行します。

ナビゲーションメニューから開始します。**Credentials** をクリックし、既存の認証情報オプションから選択します。**ヒント:** 便宜上およびセキュリティー上、認証情報のホスト専用の namespace を作成します。

オプションで、認証情報の **ベース DNS ドメイン** を追加できます。ベース DNS ドメインを認証情報に追加した場合には、この認証情報でクラスターを作成すると、このベース DNS ドメインは自動的に正しいフィールドに設定されます。以下の手順を参照してください。

1. GCP アカウントの **Google Cloud Platform project ID** を追加します。GCP にログインして設定を取得します。
2. **Google Cloud Platform service account JSON key** を追加します。https://cloud.google.com/iam/docs/creating-managing-service-accounts を参照して、サービスアカウントの JSON キーを作成してください。GCP コンソールの手順に従います。
3. Red Hat Advanced Cluster Management で、新しい **Google CloudPlatform サービスアカウントの JSON キー** のコンテンツを提供します。
4. **Red Hat OpenShift pull secret** を入力します。Pull secret からプルシークレットをダウンロードします。
5. クラスターにアクセスできるように **SSH 秘密鍵** と **SSH 公開鍵** を追加します。既存のキーペアを使用するか、キー生成プログラムで新しいキーを作成できます。

キー生成の方法は、SSH プライベートキーの生成およびエージェントへの追加 を参照してください。

「Google Cloud Platform でのクラスターの作成」の手順を実行して、クラスターの作成時に このコネクションを使用できます。

コンソールで認証情報を編集できます。

認証情報を使用するクラスターの管理を終了する場合には、認証情報を削除して認証情報内にある情報を保護します。**Actions** を選択して、一括削除するか、削除する認証情報の横にあるオプションメニューを選択します。

1.4. VMWARE VSPHERE の認証情報の作成

Red Hat Advanced Cluster Management for Kubernetes コンソールを使用して、VMware vSphere で Red Hat OpenShift Container Platform クラスターを作成して管理するには、認証情報が必要です。**注記:** OpenShift Container Platform バージョン 4.5.x 以降のみがサポートされます。

必要なアクセス: 編集

注記: Red Hat Advanced Cluster Management でクラスターを作成する前に、以下の手順を実行する必要があります。

1.4.1. 前提条件

認証情報を作成する前に、以下の前提条件を満たす必要があります。

- OpenShift Container Platform バージョン 4.6 以降に、Red Hat Advanced Cluster Management ハブクラスターをデプロイしておく。

- VMware vSphere で Kubernetes クラスターを作成できるようにする Red Hat Advanced Cluster Management ハブクラスターでのインターネットアクセスがある。
- インストーラーでプロビジョニングされるインフラストラクチャーを使用する場合に OpenShift Container Platform 向けに設定された VMware vSphere ログイン認証情報および vCenter 要件。クラスターの vSphere へのインストールについて 参照してください。これらの認証除法には、以下の情報が含まれます。
  - vCenter アカウントの権限
  - クラスターリソース
  - HDCP が利用できる
  - 時間を同期した ESXi ホスト (例: NTP)

1.4.2. コンソールを使用した認証情報の管理

Red Hat Advanced Cluster Management for Kubernetes コンソールから認証情報を作成するには、以下のコンソールでの手順を実行します。

ナビゲーションメニューから開始します。**Credentials** をクリックし、既存の認証情報オプションから選択します。**ヒント:** 便宜上およびセキュリティー上、認証情報のホスト専用の namespace を作成します。

オプションで、認証情報の **ベース DNS ドメイン** を追加できます。ベース DNS ドメインを認証情報に追加した場合には、この認証情報でクラスターを作成すると、このベース DNS ドメインは自動的に正しいフィールドに設定されます。以下の手順を参照してください。

1. **VMware vCenter サーバーの完全修飾ホスト名または IP アドレス** を追加します。値は vCenter サーバーのルート CA 証明書に定義する必要があります。可能な場合は、完全修飾ホスト名を使用します。
2. **VMware vCenter のユーザー名** を追加します。
3. **VMware vCenter パスワード** を追加します。
4. **VMware vCenter ルート CA 証明書** を追加します。
   a. VMware vCenter サーバー (**https://<vCenter_address>/certs/download.zip**) から **download.zip** として証明書をダウンロードできます。**vCenter_address** は、vCenter サーバーのアドレスに置き換えます。
   b. **download.zip** のパッケージを展開します。
   c. 拡張が **.0** の **certs/<platform>** ディレクトリーから証明書を使用します。**ヒント: ls certs/<platform>** コマンドを使用して、お使いのプラットフォームで使用可能な全証明書を一覧表示できます。
   <platform> は、**lin**、**mac** または **win** など、お使いのプラットフォームに置き換えます。

   例: **certs/lin/3a343545.0**
5. **VMware vSphere クラスター名** を追加します。
6. **VMware vSphere データセンター** を追加します。
7. **VMware vSphere デフォルトデータストア** を追加します。

8. **Red Hat OpenShift pull secret** を入力します。Pull secret からプルシークレットをダウンロードします。

9. **SSH 秘密鍵** と **SSH 公開鍵** を追加し、クラスターに接続できるようにします。

既存のキーペアを使用するか、キー生成プログラムで新しいキーを作成できます。詳細は、「SSH プライベートキーの生成およびエージェントへの追加」を 参照してください。

「VMware vSphere でのクラスターの作成」の手順を実行して、この認証情報を使用するクラスターを作成 します。

コンソールで認証情報を編集できます。

認証情報を使用するクラスターの管理を終了する場合には、認証情報を削除して認証情報内にある情報を保護します。**Actions** を選択して、一括削除するか、削除する認証情報の横にあるオプションメニューを選択します。

1.5. RED HAT OPENSTACK の認証情報の作成

Red Hat Advanced Cluster Management for Kubernetes コンソールを使用して、Red Hat OpenStack Platform で Red Hat OpenShift Container Platform クラスターを作成して管理するには、認証情報が必要です。**注記:** OpenShift Container Platform バージョン 4.5.x 以降のみがサポートされます。

注記: Red Hat Advanced Cluster Management でクラスターを作成する前に、以下の手順を実行する必要があります。

1.5.1. 前提条件

認証情報を作成する前に、以下の前提条件を満たす必要があります。

- OpenShift Container Platform バージョン 4.6 以降に、Red Hat Advanced Cluster Management ハブクラスターをデプロイしておく。
- Red Hat OpenStack Platform で Kubernetes クラスターを作成できるように Red Hat Advanced Cluster Management ハブクラスターでのインターネットアクセスがある。
- インストーラーでプロビジョニングされるインフラストラクチャーを使用する場合に OpenShift Container Platform 向けに設定された Red Hat OpenStack Platform ログイン認証情報および Red Hat OpenStack Platform の要件。「クラスターの OpenStack へのインストール」を参照してください。
- CloudStack API にアクセスするための **clouds.yaml** ファイルをダウンロードまたは作成する。**clouds.yaml** ファイルで以下を行います。
  - 使用する cloud auth セクション名を決定します。
  - **username** 行の直後に、**password** の行を追加します。

1.5.2. コンソールを使用した認証情報の管理

Red Hat Advanced Cluster Management for Kubernetes コンソールから認証情報を作成するには、以下のコンソールでの手順を実行します。

ナビゲーションメニューから開始します。**Credentials** をクリックし、既存の認証情報オプションから選択します。**ヒント:** 便宜上およびセキュリティー向上のため、認証情報のホスト専用の namespace を作成します。

1. Red Hat OpenStack Platform の **clouds.yaml** ファイルの内容を追加します。パスワードを含む **clouds.yaml** ファイルの内容で、Red Hat OpenStack Platform サーバーへの接続に必要な情報を提供します。ファイルの内容には、**username** の直後に新たに追加したパスワードを含める **必要** があります。

2. Red Hat OpenStack Platform クラウド名を追加します。このエントリーは、Red Hat OpenStack Platform サーバーへの通信確立に使用する **clouds.yaml** の cloud セクションで指定した名前です。

3. オプションで、認証情報のベース DNS ドメインを追加できます。ベース DNS ドメインを認証情報に追加した場合には、この認証情報でクラスターを作成すると、このベース DNS ドメインは自動的に正しいフィールドに設定されます。

4. Red Hat OpenShift プルシークレットを入力します。Pull secret からプルシークレットをダウンロードします。

5. SSH 秘密鍵とSSH 公開鍵を追加し、クラスターに接続できるようにします。既存のキーペアを使用するか、キー生成プログラムで新しいキーを作成できます。詳細は、「SSH プライベートキーの生成およびエージェントへの追加」を参照してください。

6. **Create** をクリックします。

7. 新規の認証情報を確認し、**Add** をクリックします。認証情報を追加すると、認証情報の一覧に追加されます。

「Red Hat OpenStack Platform でのクラスターの作成」の手順を実行して、この認証情報を使用するクラスター を作成します。

コンソールで認証情報を編集できます。

認証情報を使用するクラスターの管理を終了する場合には、認証情報を削除して認証情報内にある情報を保護します。**Actions** を選択して、一括削除するか、削除する認証情報の横にあるオプションメニューを選択します。

1.6. ベアメタルの認証情報の作成

Red Hat Advanced Cluster Management for Kubernetes コンソールを使用して、ベアメタル環境で Red Hat OpenShift Container Platform クラスターをデプロイして管理するには、認証情報が必要です。この認証情報で、プロビジョニングノードへの接続を指定します。このノードは、クラスター作成時にブートストラップのホスト仮想マシン (VM) として使用します。

必要なアクセス: 編集

- 前提条件
- プロビジョニングホストの準備
- コンソールを使用した認証情報の管理

1.6.1. 前提条件

認証情報を作成する前に、以下の前提条件を満たす必要があります。

- Red Hat Advanced Cluster Management for Kubernetes のハブクラスターをデプロイしておく。ベアメタルクラスターを管理する場合は、Red Hat OpenShift Container Platform バージョン 4.6 以降に、ハブクラスターを インストールする必要があります。

- ベアメタルサーバーで Kubernetes クラスターを作成できるようにする Red Hat Advanced Cluster Management for Kubernetes ハブクラスターでのインターネットアクセスがある。
- 切断された環境では、クラスター作成用のリリースイメージをコピーできるミラーレジストリーを設定しておく。詳細は、OpenShift Container Platform ドキュメントの 非接続インストールのイメージのミラーリング を参照してください。
- ベアメタルインフラストラクチャーでのクラスターのインストールをサポートするするアカウントのパーミッション。

1.6.2. プロビジョニングホストの準備

ベアメタルの認証情報とクラスターを作成する場合には、プロビジョニングホストが必要となります。プロビジョニングホストは、インストールに使用できるブートストラップホストの仮想マシンです。これは、KVM (Kernel-based Virtual Machine) を実行している仮想マシンまたはサービスです。認証情報やクラスターを作成する時に、このホストの詳細が必要になります。以下の手順でプロビジョニングホストを設定します。

1. プロビジョナーノードには **SSH** を使用してログインします。
2. root 以外のユーザー (user-name) を作成し、そのユーザーに sudo 権限に割り当てて、以下のコマンドを実行します。

```
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. 次のコマンドを入力して、新しいユーザーの SSH キーを作成します。

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

4. プロビジョナーノードに、新しいユーザーとしてログインします。

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

5. Red Hat Subscription Manager を使用して、以下のコマンドを入力してプロビジョナーノードを登録します。

```
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
```

   Red Hat Subscription Manager の詳細は、Red Hat OpenShift Container Platform ドキュメントの「Subscription Manager の使用および設定」を参照してください。

6. 以下のコマンドを実行して、必要なパッケージをインストールします。

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

7. ユーザーを変更して、新たに作成したユーザーに **libvirt** グループを追加します。

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

8. 以下のコマンドを入力して、**firewalld** を再起動し、**http** サービスを有効にします。

```
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. 以下のコマンドを入力して、**libvirtd** サービスを起動し、有効にします。

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

10. 次のコマンドを入力して、デフォルトのストレージプールを作成し、起動します。

```
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. ネットワーク設定の以下の例を参照してください。

- **プロビジョニングネットワーク (IPv4アドレス)**

```
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 $PROV_CONN"
    nmcli connection add ifname provisioning type bridge con-name provisioning
    nmcli con add type bridge-slave ifname "$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"""
```

この手順を完了すると、SSH 接続が切断される場合があります。

IPv4 アドレスは、ベアメタルネットワークでルーティングできなければ、どのようなアドレスでも構いません。

- **プロビジョニングネットワーク (IPv6 アドレス)**

```
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-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"""
```

この手順を完了すると、SSH 接続が切断される場合があります。

IPv6 アドレスは、ベアメタルネットワークでルーティングできなければ、どのようなアドレスでも構いません。

IPv6 アドレスを使用する場合に UEFI PXE 設定が有効にされており、UEFI PXE 設定が IPv6 プロトコルに設定されていることを確認します。

12. **ssh** を使用してプロビジョナーノードに再接続します (必要な場合)。

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

13. 以下のコマンドを実行して、接続ブリッジが正しく作成されていることを確認します。

```
nmcli con show
```

検索結果は、以下のような内容になります。

名前	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. 以下の手順で **pull-secret.txt** ファイルを作成します。

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

   a. Webブラウザーで 「Install OpenShift on Bare Metal with user-provisioned infrastructure 」にアクセスし、「**Downloads**」セクションまでスクロールします。

   b. **Copy pull secret** をクリックします。

   c. その内容を **pull-secret.txt** に貼り付けて、**user-name** ユーザーのホームディレクトリーに保存します。

これで、ベアメタルの認証情報を作成する準備が整いました。

1.6.3. コンソールを使用した認証情報の管理

Red Hat Advanced Cluster Management for Kubernetes コンソールから認証情報を作成するには、以下のコンソールでの手順を実行します。

ナビゲーションメニューから開始します。**Credentials** をクリックし、既存の認証情報オプションから選択します。**ヒント:** 便宜上およびセキュリティー上、認証情報のホスト専用の namespace を作成します。

1. オプションで、認証情報の **ベース DNS ドメイン** を追加できます。ベース DNS ドメインを認証情報に追加した場合には、この認証情報でクラスターを作成すると、このベース DNS ドメインは自動的に正しいフィールドに設定されます。DNS ドメインを追加していない場合は、クラスターの作成時に追加できます。

2. **libvirt URI** を追加します。libvirt URI は、ブートストラップノード向けに作成したプロビジョニングノードを追加してください。libvirt URI は以下の例のようになります。

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

- **qemu+ssh** は、プロビジョニングホスト上の libvirt デーモンに接続する方法に置き換えてください。
- **user-name** は、プロビジョニングホストにブートストラップノードを作成するアクセス権があるユーザー名に置き換えてください。
- **provision-host.com** は、プロビジョニングホストへのリンクに置き換えてください。これは、IP アドレスまたは完全修飾ドメイン名アドレスのいずれかです。
  詳細は、Connection URIs を参照してください。

3. プロビジョニングホストに SSH の既知ホストのリストを追加します。この値には、IP アドレスまたは完全修飾ドメイン名アドレスを指定できますが、libvirt URI 値で使用したのと同じ形式を使用することをお勧めします。

4. **Red Hat OpenShift pull secret**を入力します。Pull secret からプルシークレットをダウンロードします。

5. クラスターにアクセスできるように **SSH 秘密鍵** と **SSH 公開鍵** を追加します。既存のキーを使用するか、キー生成プログラムを使用して新しいキーを作成できます。キー生成の方法は、「SSH プライベートキーの生成およびエージェントへの追加」を参照してください。

6. オフラインインストールのみ: **Configuration for disconnected installation**サブセクションのフィールドに必要な情報を入力します。

   - **Image registry mirror**: この値には、オフラインのレジストリーパスを含みます。このパスには、オフラインインストールに使用する全インストールイメージのホスト名、ポート、レジストリーパスが含まれます。例: **repository.com:5000/openshift/ocp-release**.
     このパスは、Red Hat OpenShift Container Platform リリースイメージに対して、**install-config.yaml** のイメージコンテンツソースポリシーのマッピングを作成します。たとえば、**repository.com:5000** は以下の **imageContentSource** コンテンツを作成します。

     ```
     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**: この値には、ブートストラップマシンに使用するイメージの URL が含まれます。
   - **Cluster OS image**: この値には、Red Hat OpenShift Container Platform クラスターマシンに使用するイメージの URL が含まれます。
   - **Additional trust bundle**: この値で、ミラーレジストリーへのアクセスに必要な証明書ファイルのコンテンツを指定します。
     注記: 非接続環境にあるハブクラスターからマネージドクラスターをデプロイして、インストール後の設定を自動的にインポートする場合には、**YAML** エディターを使用してイメージコンテンツソースポリシーを **install-config.yaml** ファイルに追加します。エントリーの例を以下に示します。

     ```
     imageContentSources:
     ```

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

ベアメタルでのクラスターの作成 の手順を実行して、この認証情報を使用するクラスターを作成 します。

コンソールで認証情報を編集できます。

認証情報を使用するクラスターの管理を終了する場合には、認証情報を削除して認証情報内にある情報を保護します。**Actions** を選択して、一括削除するか、削除する認証情報の横にあるオプションメニューを選択します。

1.7. RED HAT OPENSHIFT CLUSTER MANAGER の認証情報の作成

クラスターを検出できるように OpenShift Cluster Manager の認証情報を追加します。

必要なアクセス権限:: 管理者

1.7.1. 前提条件

cloud.redhat.com アカウントへのアクセスが必要です。console.redhat.com/openshift/token から取得できる値が後で必要になります。

1.7.2. コンソールを使用した認証情報の管理

クラスター検出用の認証情報を追加する必要があります。Red Hat Advanced Cluster Management for Kubernetes コンソールから認証情報を作成するには、以下のコンソールでの手順を実行します。

ナビゲーションメニューから開始します。**Credentials** をクリックし、既存の認証情報オプションから選択します。**ヒント:** 便宜上およびセキュリティー上、認証情報のホスト専用の namespace を作成します。

OpenShift Cluster Manager API トークンは、console.redhat.com/openshift/token から取得できます。

コンソールで認証情報を編集できます。

認証情報を使用するクラスターの管理を終了する場合には、認証情報を削除して認証情報内にある情報を保護します。**Actions** を選択して、一括削除するか、削除する認証情報の横にあるオプションメニューを選択します。

認証情報が削除されるか、または OpenShift Cluster Manager API トークンの有効期限が切れるか、または取り消されると、関連付けられた検出クラスターが削除されます。

1.8. ANSIBLE AUTOMATION PLATFORM の認証情報の作成

Red Hat Advanced Cluster Management for Kubernetes コンソールを使用して、Red Hat Ansible Automation Platform を使用する Red Hat OpenShift Container Platform クラスターをデプロイして管理するには、認証情報が必要です。

必要なアクセス: 編集

注意: この手順は、Ansible ジョブテンプレートを作成して Red Hat Advanced Cluster Management クラスターで自動化を有効にする前に実行する必要があります。

1.8.1. 前提条件

認証情報を作成する前に、以下の前提条件を満たす必要があります。

- Red Hat Advanced Cluster Management for Kubernetes のハブクラスターをデプロイしておく。
- Red Hat Advanced Cluster Management for Kubernetes のハブクラスターへのインターネット接続。
- Ansible Tower ホスト名および OAuth トークンを含む Ansible ログイン認証情報。「Ansible Tower の認証情報」を参照してください。
- ハブクラスターのインストールおよび Ansible 操作をできるようにするアカウントパーミッション。Ansible ユーザー の詳細を確認してください。

1.8.2. コンソールを使用した認証情報の管理

Red Hat Advanced Cluster Management for Kubernetes コンソールから認証情報を作成するには、以下のコンソールでの手順を実行します。

ナビゲーションメニューから開始します。**Credentials** をクリックし、既存の認証情報オプションから選択します。**ヒント:** 便宜上およびセキュリティー上、認証情報のホスト専用の namespace を作成します。

Ansible 認証情報の作成時に指定する Ansible トークンとホストの URL は、認証情報の編集時にその認証情報を使用する自動化向けに、自動で更新されます。更新は、クラスターライフサイクル、ガバナンス、およびアプリケーション管理の自動化に関連するものなど、Ansible 認証情報を使用する自動化にコピーされます。これにより、認証情報の更新後も自動化が引き続き実行されます。

コンソールで認証情報を編集できます。Ansible 認証情報は、認証情報の更新時に、対象の認証情報を使用する自動化で、自動的に更新されあす。

認証情報を使用するクラスターの管理を終了する場合には、認証情報を削除して認証情報内にある情報を保護します。**Actions** を選択して、一括削除するか、削除する認証情報の横にあるオプションメニューを選択します。

1.9. オンプレミス環境の認証情報の作成

Red Hat Advanced Cluster Management for Kubernetes コンソールを使用して、オンプレミス環境で Red Hat OpenShift Container Platform クラスターをデプロイして管理するには、認証情報が必要です。認証情報では、クラスターに使用される接続を指定します。

必要なアクセス: 編集

- 前提条件
- コンソールを使用した認証情報の管理

1.9.1. 前提条件

認証情報を作成する前に、以下の前提条件を満たす必要があります。

- Red Hat Advanced Cluster Management ハブクラスターをデプロイしている。

- Red Hat Advanced Cluster Management for Kubernetes ハブクラスターでのインターネットアクセスを有効にし、インフラストラクチャー環境で Kubernetes クラスターを作成できるようにする。
- 切断された環境では、クラスター作成用のリリースイメージをコピーできるミラーレジストリーを設定しておく。詳細は、OpenShift Container Platform ドキュメントの 非接続インストールのイメージのミラーリング を参照してください。
- オンプレミス環境でのクラスターのインストールをサポートするアカウントのパーミッション。

1.9.2. コンソールを使用した認証情報の管理

Red Hat Advanced Cluster Management for Kubernetes コンソールから認証情報を作成するには、以下のコンソールでの手順を実行します。

ナビゲーションメニューから開始します。**Credentials** をクリックし、既存の認証情報オプションから選択します。**ヒント:** 便宜上およびセキュリティー上、認証情報のホスト専用の namespace を作成します。

1. オプションで、認証情報の **ベース DNS ドメイン** を追加できます。ベース DNS ドメインを認証情報に追加した場合には、この認証情報でクラスターを作成すると、このベース DNS ドメインは自動的に正しいフィールドに設定されます。DNS ドメインを追加していない場合は、クラスターの作成時に追加できます。
2. **Red Hat OpenShift pull secret** を入力します。Pull secret からプルシークレットをダウンロードします。プルシークレットの詳細は、イメージプルシークレットの使用 を参照してください。
3. **Add** を選択して認証情報を作成します。

認証情報を使用するクラスターの管理を終了する場合には、認証情報を削除して認証情報内にある情報を保護します。**Actions** を選択して、一括削除するか、削除する認証情報の横にあるオプションメニューを選択します。