Red Hat OpenShift Service on AWS 4

ROSA with HCP クラスターのインストール

Red Hat OpenShift Service on AWS (ROSA) クラスターのインストール、アクセス、および削除

Last Updated: 2024-11-29

Red Hat OpenShift Service on AWS 4 ROSA with HCP クラスターのインストール

Red Hat OpenShift Service on AWS (ROSA) クラスターのインストール、アクセス、および削除

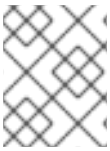
法律上の通知

概要

このドキュメントでは、Hosted Control Plane を使用して、Red Hat OpenShift Service on AWS (ROSA) クラスターをインストールする方法を説明します。

目次

第1章 デフォルトのオプションを使用した ROSA WITH HCP クラスターの作成



注記

ROSA Classic のクイックスタートガイドをお探しの場合は、Red Hat OpenShift Service on AWS クイックスタートガイド を参照してください。

Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane は、Red Hat OpenShift Service on AWS (ROSA) クラスターを作成するためのより効率的で信頼性の高いアーキテクチャーを提供します。ROSA with HCP では、各クラスターに ROSA サービスアカウントで分離された専用のコントロールプレーンがあります。

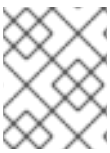
デフォルトのオプションと AWS Identity and Access Management (IAM) リソースの自動作成を使用して、ROSA with HCP クラスターをすばやく作成します。ROSA CLI (**rosa**) を使用してクラスターをデプロイできます。

重要

既存の ROSA クラスターを Hosted Control Plane アーキテクチャーにアップグレードまたは変換することはできないため、ROSA with HCP の機能を使用するには新しいクラスターを作成する必要があります。

重要

現在、ROSA with HCP では 複数の AWS アカウント間での VPC の共有 はサポートされていません。別の AWS アカウントから共有されているサブネットに ROSA with HCP クラスターをインストールしないでください。詳細は、"Are multiple ROSA clusters in a single VPC supported?" を参照してください。



注記

ROSA with HCP クラスターは、AWS Security Token Service (STS) 認証のみをサポートします。

関連資料

- ROSA with HCP と ROSA Classic の比較は、アーキテクチャーモデルの比較 のドキュメントを参照してください。
- ROSA CLI を使用して自動モードで ROSA with HCP の使用を開始する方法 については、AWS ドキュメントを参照してください。

関連情報

サポートされている証明書の完全なリストは、「Red Hat OpenShift Service on AWS のプロセスとセキュリティーについて」の コンプライアンス セクションを参照してください。

自動作成モードに関する考慮事項

このドキュメントの手順では、ROSA CLI の **auto** モードを使用して、現在の AWS アカウントを使用して必要な IAM リソースを即座に作成します。必要なリソースには、アカウント全体の IAM ロールおよびポリシー、クラスター固有の Operator ロール、ならびに OpenID Connect (OIDC) ID プロバイダーが含まれます。

または、IAM リソースを自動的にデプロイする代わりに、IAM リソースの作成に必要な **aws** コマンドを出力する **manual** モードを使用することもできます。

次のステップ

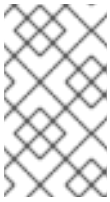
- AWS の前提条件 を満たしていることを確認する。

1.1. デフォルトのクラスター仕様の概要

デフォルトのインストールオプションを使用して、Security Token Service (STS) で Red Hat OpenShift Service on AWS (ROSA) クラスターをすばやく作成できます。次の要約では、デフォルトのクラスター仕様を説明します。

表1.1 STS クラスター仕様のデフォルト ROSA

コンポーネント	デフォルトの仕様
アカウントおよびロール	• デフォルトの IAM ロールの接頭辞: **ManagedOpenShift** • クラスター管理者ロールは作成されない
クラスター設定	• デフォルトのクラスターバージョン: 最新 • Red Hat OpenShift Cluster Manager Hybrid Cloud Console を使用したインストール用のデフォルトの AWS リージョン: us-east-1 (US East, North Virginia) • 可用性: データプレーンの単一ゾーン • EC2 インスタンスメタデータサービス (IMDS) が有効になっており、IMDSv1 または IMDSv2 の使用が許可されています (トークンはオプション) • ユーザー定義プロジェクトの監視: 有効
暗号化	• クラウドストレージは保存時に暗号化されます。 • 追加の etcd 暗号化が有効になっていません。 • デフォルトの AWS Key Management Service (KMS) キーは、永続データの暗号化キーとして使用される
コントロールプレーンノードの設定	• コントロールプレーンノードのインスタンスタイプ: m5.2xlarge (8 vCPU, 32 GiB RAM) • コントロールプレーンノード数: 3

コンポーネント	デフォルトの仕様
インフラストラクチャーノードの設定	• インフラストラクチャーノードインスタンスタイプ: r5.xlarge (4 vCPU, 32 GiB RAM) • インフラストラクチャーノード数: 2
コンピュートノードマシンプール	• コンピュートノードインスタンスタイプ: m5.xlarge (4 vCPU 16, GiB RAM) • コンピュートノード数: 2 • 自動スケーリング: 無効 • 追加のノードラベルなし
ネットワーク設定	• クラスターのプライバシー: パブリック • 独自の Virtual Private Cloud (VPC) を設定しておく必要があります。 • クラスター全体のプロキシーは設定されていません。
Classless Inter-Domain Routing (CIDR) の範囲	• Machine CIDR: 10.0.0.0/16 • Service CIDR: 172.30.0.0/16 • Pod CIDR: 10.128.0.0/16 • Host prefix: /23
クラスターのロールおよびポリシー	• Operator ロールおよび OpenID Connect (OIDC) プロバイダーの作成に使用されるモード: **auto**  **注記** Hybrid Cloud Console で OpenShift Cluster Manager を使用するインストールの場合、**auto** モードには管理者権限が割り当てられた OpenShift Cluster Manager ロールが必要です。 • デフォルトの Operator ロールの接頭辞: **<cluster_name>-<4_digit_random_string>**
クラスター更新戦略	• 個別の更新 • ノードドレインの 1 時間の猶予期間

1.2. ROSA WITH HCP の前提条件

ROSA with HCP クラスターを作成するには、次のものが必要です。

- 設定された仮想プライベートクラウド (VPC)
- アカウント全体のロール
- OIDC 設定
- オペレーターのロール

1.2.1. ROSA with HCP クラスター用の仮想プライベートクラウドの作成

ROSA with HCP クラスターを作成するには、Virtual Private Cloud (VPC) が必要です。次の方法を使用して VPC を作成できます。

- Terraform テンプレートを使用して VPC を作成する
- AWS コンソールで VPC リソースを手動で作成する

注記

Terraform の手順はテストとデモンストレーションを目的としています。独自のインストールでは、独自に使用するために VPC にいくつかの変更を加える必要があります。また、この Terraform スクリプトを使用するときは、クラスターをインストールする予定のリージョンと同じリージョンにあることを確認する必要があります。これらの例では、**us-east-2** を使用します。

Terraform を使用した Virtual Private Cloud の作成
Terraform は、確立されたテンプレートを使用してさまざまなリソースを作成できるツールです。次のプロセスでは、必要に応じてデフォルトのオプションを使用して、ROSA with HCP クラスターを作成します。Terraform の使用の詳細は、関連情報を参照してください。

前提条件

- マシンに Terraform バージョン 1.4.0 以降がインストールされている。
- マシンに Git がインストールされている。

手順

1. シェルプロンプトを開き、次のコマンドを実行して Terraform VPC リポジトリーのクローンを作成します。

```
$ git clone https://github.com/openshift-cs/terraform-vpc-example
```

2. 次のコマンドを実行して、作成したディレクトリーに移動します。

```
$ cd terraform-vpc-example
```

3. 次のコマンドを実行して、Terraform ファイルを開始します。

```
$ terraform init
```

このプロセスが完了すると、初期化を確認するメッセージが表示されます。

4. 既存の Terraform テンプレートに基づいて VPC Terraform プランを構築するには、**plan** コマンドを実行します。AWS リージョンを含める必要があります。クラスター名の指定を選択できます。**terraform plan** が完了すると、**rosa.tfplan** ファイルが **hypershift-tf** ディレクトリーに追加されます。オプションの詳細は、Terraform VPC リポジトリーの README ファイル を参照してください。

```
$ terraform plan -out rosa.tfplan -var region=<region>
```

5. 次のコマンドを実行して、このプランファイルを適用して VPC を構築します。

```
$ terraform apply rosa.tfplan
```

a. 任意: 次のコマンドを実行して、Terraform でプロビジョニングされたプライベート、パブリック、およびマシンプールのサブネット ID の値を環境変数としてキャプチャーし、ROSA with HCP クラスターを作成するときに使用できます。

```
$ export SUBNET_IDS=$(terraform output -raw cluster-subnets-string)
```

b. 次のコマンドを使用して、変数が正しく設定されたことを確認できます。

```
$ echo $SUBNET_IDS
```

出力例

```
$ subnet-0a6a57e0f784171aa,subnet-078e84e5b10ecf5b0
```

関連情報

- ニーズに合わせて VPC をカスタマイズするときに使用できるすべてのオプションの詳細なリストは、Terraform VPC リポジトリーを参照してください。

Virtual Private Cloud を手動で作成する

Terraform を使用する代わりに Virtual Private Cloud (VPC) を手動で作成することを選択した場合は、AWS コンソールの VPC ページ に移動します。VPC は、次の表に示す要件を満たしている必要があります。

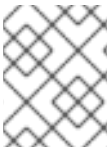
表1.2 VPC の要件

要件	詳細
VPC 名	クラスターを作成するときは、特定の VPC 名と ID が必要です。
CIDR 範囲	VPC CIDR 範囲はマシンの CIDR と一致する必要があります。
アベイラビリティーゾーン	単一ゾーンの場合は 1 つの可用性ゾーンが必要で、複数ゾーンの場合は 3 つの可用性ゾーンが必要です。

要件	詳細
パブリックサブネット	パブリッククラスターには、NAT ゲートウェイを備えたパブリックサブネットが 1 つ必要です。プライベートクラスターにはパブリックサブネットは必要ありません。
DNS ホスト名と解決	DNS ホスト名と解決が有効になっていることを確認する必要があります。

サブネットへのタグ付け
VPC を使用して ROSA with HCP クラスターを作成する前に、VPC サブネットにタグを付ける必要があります。自動サービスのプリフライトチェックでは、これらのリソースを使用する前に、これらのリソースが正しくタグ付けされていることを確認します。次の表は、リソースを次のようにタグ付けする方法を示しています。

リソース	キー	値
パブリックサブネット	**kubernetes.io/role/elb**	**1** または値なし
プライベートサブネット	**kubernetes.io/role/internal-elb**	**1** または値なし



注記

少なくとも 1 つのプライベートサブネットと、該当する場合は 1 つのパブリックサブネットにタグを付ける必要があります。

前提条件

- VPC を作成している。
- **aws** CLI をインストールしている。

手順

1. 次のコマンドを実行して、ターミナルでリソースにタグを付けます。
   a. パブリックサブネットの場合は、以下を実行します。

```
$ aws ec2 create-tags --resources <public-subnet-id> --tags
Key=kubernetes.io/role/elb,Value=1
```

   b. プライベートサブネットの場合は、以下を実行します。

```
$ aws ec2 create-tags --resources <private-subnet-id> --tags
Key=kubernetes.io/role/internal-elb,Value=1
```

検証

- 次のコマンドを実行して、タグが正しく適用されていることを確認します。

```
$ aws ec2 describe-tags --filters "Name=resource-id,Values=<subnet_id>"
```

出力例

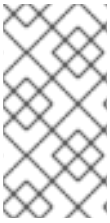
```
TAGS    Name                    <subnet-id>       subnet  <prefix>-subnet-public1-us-east-1a
TAGS    kubernetes.io/role/elb  <subnet-id>       subnet  1
```

関連情報

- Get Started with Amazon VPC
- HashiCorp Terraform ドキュメント
- サブネットの自動検出

1.2.2. アカウント全体の STS ロールおよびポリシーの作成

Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) を使用して、Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane クラスターを作成する前に、Operator ポリシーを含む、必要なアカウント全体のロールとポリシーを作成します。



注記

ROSA with HCP クラスターには、AWS 管理ポリシーがアタッチされたアカウントと Operator ロールが必要です。顧客管理のポリシーはサポートされていません。ROSA with HCP クラスターの AWS 管理ポリシーの詳細は、AWS managed policies for ROSA account roles を参照してください。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。
- 利用可能な AWS サービスクォータがある。
- AWS コンソールで ROSA サービスを有効にしている。
- インストールホストに、最新の ROSA CLI (**rosa**) をインストールして設定している。
- ROSA CLI を使用して Red Hat アカウントにログインしている。

手順

1. AWS アカウントに存在しない場合は、次のコマンドを実行して、必要なアカウント全体の STS ロールを作成し、ポリシーをアタッチします。

```
$ rosa create account-roles --hosted-cp
```

2. オプション: 次のコマンドを実行して、接頭辞を環境変数として設定します。

```
$ export ACCOUNT_ROLES_PREFIX=<account_role_prefix>
```

- 次のコマンドを実行して、変数の値を表示します。

```
$ echo $ACCOUNT_ROLES_PREFIX
```

出力例

```
ManagedOpenShift
```

ROSA の AWS 管理 IAM ポリシーの詳細は、AWS managed IAM policies for ROSA を参照してください。

1.2.3. OpenID Connect 設定の作成

ROSA with HCP クラスターを使用する場合は、クラスターを作成する前に OpenID Connect (OIDC) 設定を作成する必要があります。この設定は、OpenShift Cluster Manager で使用するために登録されています。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。
- Red Hat OpenShift Service on AWS の AWS 前提条件を完了している。
- インストールホストに、最新の Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールして設定している。

手順

1. AWS リソースと一緒に OIDC 設定を作成するには、次のコマンドを実行します。

```
$ rosa create oidc-config --mode=auto --yes
```

このコマンドは次の情報を返します。

出力例

```
? Would you like to create a Managed (Red Hat hosted) OIDC Configuration Yes
I: Setting up managed OIDC configuration
I: To create Operator Roles for this OIDC Configuration, run the following command and
remember to replace <user-defined> with a prefix of your choice:
 rosa create operator-roles --prefix <user-defined> --oidc-config-id 13cdr6b
If you are going to create a Hosted Control Plane cluster please include '--hosted-cp'
I: Creating OIDC provider using 'arn:aws:iam::4540112244:user/userName'
? Create the OIDC provider? Yes
I: Created OIDC provider with ARN 'arn:aws:iam::4540112244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/13cdr6b'
```

クラスターを作成するときは、OIDC 設定 ID を指定する必要があります。CLI 出力では、**--mode auto** のこの値が提供されます。それ以外の場合は、**--mode manual** の **aws** CLI 出力に基づいてこれらの値を決定する必要があります。

2. オプション: OIDC 設定 ID を変数として保存して、後で使用できます。次のコマンドを実行して変数を保存します。

```
$ export OIDC_ID=<oidc_config_id>
```
1

1 上記の出力例では、OIDC 設定 ID は 13cdr6b です。

- 次のコマンドを実行して、変数の値を表示します。

```
$ echo $OIDC_ID
```

出力例

```
13cdr6b
```

検証

- ユーザー組織に関連付けられているクラスターで使用できる可能な OIDC 設定をリストできます。以下のコマンドを実行します。

```
$ rosa list oidc-config
```

出力例

```
ID                               MANAGED  ISSUER URL
SECRET ARN
2330dbs0n8m3chkkr25gkkcd8pnj3lk2  true
https://dvbwgdztaeq9o.cloudfront.net/2330dbs0n8m3chkkr25gkkcd8pnj3lk2
233hvnrjoqu14jltk6lhbhf2tj11f8un  false    https://oidc-r7u1.s3.us-east-1.amazonaws.com
aws:secretsmanager:us-east-1:242819244:secret:rosa-private-key-oidc-r7u1-tM3MDN
```

1.2.4. Operator のロールとポリシーの作成

ROSA with HCP クラスターを使用する場合は、Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane (HCP) デプロイメントに必要な Operator IAM ロールを作成する必要があります。クラスター Operator は、Operator のロールを使用して、バックエンドストレージ、クラウドプロバイダーの認証情報、クラスターへの外部アクセスの管理など、クラスター操作を実行するために必要な一時的なアクセス許可を取得します。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。
- インストールホストに、最新の Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールして設定している。
- アカウント全体の AWS ロールを作成している。

手順

1. 次のコマンドを使用して、接頭辞名を環境変数に設定します。

```
$ export OPERATOR_ROLES_PREFIX=<prefix_name>
```

2. Operator ロールを作成するには、次のコマンドを実行します。

```
$ rosa create operator-roles --hosted-cp --prefix=$OPERATOR_ROLES_PREFIX --oidc-config-id=$OIDC_ID --installer-role-arn arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role
```

次の内訳は、Operator ロール作成のオプションを示しています。

```
$ rosa create operator-roles --hosted-cp
 --prefix=$OPERATOR_ROLES_PREFIX (1)
 --oidc-config-id=$OIDC_ID (2)
 --installer-role-arn
arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role (3)
```

(1) これらの Operator ロールを作成するときは、接頭辞を指定する必要があります。そうしないとエラーが発生します。演算子接頭辞は、このセクションの関連情報を参照してください。

(2) この値は、ROSA with HCP クラスター用に作成した OIDC 設定 ID です。

(3) この値は、ROSA アカウントロールの作成時に作成したインストーラーロールの ARN です。

ROSA with HCP クラスター用の正しいロールを作成するには、**--hosted-cp** パラメーターを含める必要があります。このコマンドは次の情報を返します。

出力例

```
? Role creation mode: auto
? Operator roles prefix: <pre-filled_prefix> (1)
? OIDC Configuration ID: 23soa2bgvpek9kmes9s7os0a39i13qm4 | https://dvbwgdztaeq9o.cloudfront.net/23soa2bgvpek9kmes9s7os0a39i13qm4 (2)
? Create hosted control plane operator roles: Yes
W: More than one Installer role found
? Installer role ARN: arn:aws:iam::4540112244:role/<prefix>-HCP-ROSA-Installer-Role
? Permissions boundary ARN (optional):
I: Reusable OIDC Configuration detected. Validating trusted relationships to operator roles:
I: Creating roles using 'arn:aws:iam::4540112244:user/<userName>'
I: Created role '<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials' with ARN 'arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials'
I: Created role '<prefix>-openshift-cloud-network-config-controller-cloud-credenti' with ARN 'arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-controller-cloud-credenti'
I: Created role '<prefix>-kube-system-kube-controller-manager' with ARN 'arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager'
I: Created role '<prefix>-kube-system-capa-controller-manager' with ARN 'arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager'
I: Created role '<prefix>-kube-system-control-plane-operator' with ARN 'arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator'
I: Created role '<prefix>-kube-system-kms-provider' with ARN 'arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider'
I: Created role '<prefix>-openshift-image-registry-installer-cloud-credentials' with ARN
```

```
'arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-credentials'
I: Created role '<prefix>-openshift-ingress-operator-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials'
I: To create a cluster with these roles, run the following command:
 rosa create cluster --sts --oidc-config-id 23soa2bgvpek9kmes9s7os0a39i13qm4 --operator-
roles-prefix <prefix> --hosted-cp
```

1. このフィールドには、最初の作成コマンドで設定した接頭辞が事前に入力されます。
2. このフィールドでは、ROSA with HCP クラスター用に作成した OIDC 設定を選択する必要があります。

これで、Operator ロールが作成され、ROSA with HCP クラスターの作成に使用できるようになりました。

検証

- ROSA アカウントに関連付けられている Operator ロールをリスト表示できます。以下のコマンドを実行します。

```
$ rosa list operator-roles
```

出力例

```
I: Fetching operator roles
ROLE PREFIX  AMOUNT IN BUNDLE
<prefix>      8
? Would you like to detail a specific prefix Yes 1
? Operator Role Prefix: <prefix>
ROLE NAME                                          ROLE ARN
VERSION  MANAGED
<prefix>-kube-system-capa-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager
4.13     No
<prefix>-kube-system-control-plane-operator
arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator
4.13     No
<prefix>-kube-system-kms-provider
arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider                    4.13
No
<prefix>-kube-system-kube-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager
4.13     No
<prefix>-openshift-cloud-network-config-controller-cloud-credenti
arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-controller-cloud-
credenti  4.13     No
<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
4.13     No
<prefix>-openshift-image-registry-installer-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-credentials
4.13     No
```

```
<prefix>-openshift-ingress-operator-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials
4.13     No
```

1. コマンドを実行すると、AWS アカウントに関連付けられているすべての接頭辞が表示され、この接頭辞に関連付けられているロールの数が記録されます。これらのロールとその詳細をすべて表示する必要がある場合は、詳細プロンプトで "Yes" と入力すると、これらのロールが詳細とともにリストされます。

関連情報

- オペレーター接頭辞については、カスタム Operator IAM ロール接頭辞 を参照してください。

1.3. CLI を使用した ROSA WITH HCP クラスターの作成

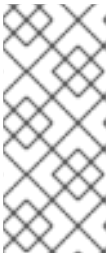
Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) を使用してクラスターを作成する場合は、デフォルトのオプションを選択してクラスターを迅速に作成できます。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。
- 利用可能な AWS サービスクォータがある。
- AWS コンソールで ROSA サービスを有効にしている。
- インストールホストに、最新の ROSA CLI (**rosa**) をインストールして設定している。**rosa version** を実行して、現在インストールされている ROSA CLI のバージョンを確認します。新しいバージョンが利用可能な場合、CLI はこのアップグレードをダウンロードするためのリンクを提供します。
- ROSA CLI を使用して Red Hat アカウントにログインしている。
- OIDC 設定が作成されている。
- AWS Elastic Load Balancing (ELB) サービスロールが AWS アカウントに存在することを確認している。

手順

1. ROSA with HCP クラスターを作成するには、次のいずれかのコマンドを使用します。



注記

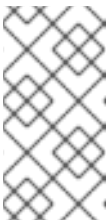
ROSA with HCP クラスターを作成する場合、デフォルトのマシン Classless Inter-Domain Routing (CIDR) は **10.0.0.0/16** です。これが VPC サブネットの CIDR 範囲に対応していない場合は、次のコマンドに **--machine-cidr <address_block>** を追加します。Red Hat OpenShift Service on AWS のデフォルト CIDR 範囲の詳細は、「CIDR 範囲の定義」を参照してください。

- 環境変数を設定していない場合は、以下のコマンドを実行します。

```
$ rosa create cluster --cluster-name=<cluster_name> \ <.>
```

```
--mode=auto --hosted-cp [--private] \ <.>
--operator-roles-prefix <operator-role-prefix> \ <.>
--oidc-config-id <id-of-oidc-configuration> \
--subnet-ids=<public-subnet-id>,<private-subnet-id>
```

<.> クラスターの名前を指定します。クラスター名が 15 文字を超える場合、openshiftapps.com でプロビジョニングされたクラスターのサブドメインとして自動生成されたドメイン接頭辞が含まれます。サブドメインをカスタマイズするには、**--domain-prefix** フラグを使用します。ドメイン接頭辞は 15 文字を超えてはならず、一意である必要があり、クラスターの作成後に変更できません。<.> オプション: **--private** 引数は、プライベート ROSA with HCP クラスターを作成するために使用されます。この引数を使用する場合は、**--subnet-ids** にプライベートサブネット ID のみを使用するようにしてください。<.> デフォルトでは、クラスター固有の Operator のロール名には、クラスター名とランダムな 4 桁のハッシュが接頭辞として付けられます。オプションで、ロール名の **<cluster_name>-<hash>** を置き換えるカスタム接頭辞を指定できます。接頭辞は、クラスター固有の Operator IAM ロールを作成するときに適用されます。接頭辞の詳細は、**カスタム Operator IAM ロール接頭辞について** を参照してください。



注記

関連するアカウント全体のロールを作成したときにカスタム ARN パスを指定した場合、カスタムパスは自動的に検出されます。カスタムパスは、後のステップで作成するときに、クラスター固有の Operator ロールに適用されます。

- 環境変数を設定する場合、単一の初期マシンプールを備え、パブリックまたはプライベートに利用可能な API および Ingress を使用するクラスターを作成するには、次のコマンドを実行します。

```
$ rosa create cluster --private --cluster-name=<cluster_name> \
    --mode=auto --hosted-cp --operator-roles-prefix=$OPERATOR_ROLES_PREFIX \
    --oidc-config-id=$OIDC_ID --subnet-ids=$SUBNET_IDS
```

- 環境変数を設定する場合、単一の初期マシンプール、パブリックに利用可能な API、およびパブリックに利用可能な Ingress を備えたクラスターを作成するには、次のコマンドを実行します。

```
$ rosa create cluster --cluster-name=<cluster_name> --mode=auto \
    --hosted-cp --operator-roles-prefix=$OPERATOR_ROLES_PREFIX \
    --oidc-config-id=$OIDC_ID --subnet-ids=$SUBNET_IDS
```

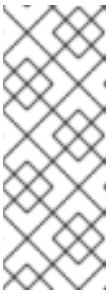
2. 次のコマンドを実行して、クラスターのステータスを確認します。

```
$ rosa describe cluster --cluster=<cluster_name>
```

以下の **State** フィールドの変更は、クラスターインストールの進捗として出力に表示されます。

- **pending (Preparing account)**
- **installing (DNS setup in progress)**
- **installing**

- **ready**



注記

インストールが失敗した場合や、**State** フィールドが 10 分以上 **ready** に変わらない場合は、インストールのトラブルシューティングのドキュメントで詳細を確認してください。詳細は、**インストールのトラブルシューティング**を参照してください。Red Hat サポートにサポートを依頼する手順は、**Red Hat OpenShift Service on AWS のサポートを受ける**を参照してください。

3. Red Hat OpenShift Service on AWS インストールプログラムのログを監視して、クラスター作成の進行状況を追跡します。ログを確認するには、次のコマンドを実行します。

```
$ rosa logs install --cluster=<cluster_name> --watch \ <.>
```

<.> オプション: インストールの進行中に新しいログメッセージを監視するには、**--watch** 引数を使用します。

1.4. 次のステップ

- ROSA クラスターへのアクセス
- 通知連絡先の追加

1.5. 関連情報

- 手動モードを使用して ROSA クラスターをデプロイする手順は、カスタマイズを使用したクラスターの作成 を参照してください。
- STS を使用する Red Hat OpenShift Service on AWS をデプロイするのに必要な AWS Identity Access Management (IAM) リソースの詳細は、STS を使用するクラスターの IAM リソースについて を参照してください。
- セキュリティーグループの要件については、追加のカスタムセキュリティーグループ を参照してください。
- オプションで Operator ロール名接頭辞を設定する方法の詳細は、カスタム Operator IAM ロール接頭辞について を参照してください。
- STS を使用する ROSA をインストールするための前提条件の詳細は、STS を使用する ROSA の AWS の前提条件 を参照してください。
- **auto** モードと **manual** モードを使用して必要な STS リソースを作成する方法の詳細は、自動デプロイメントモードと手動デプロイメントモードについて を参照してください。
- AWS IAM で OpenID Connect (OIDC) アイデンティティープロバイダーの使用に関する詳細は、AWS ドキュメントの Creating OpenID Connect (OIDC) identity providers を参照してください。
- ROSA クラスターのインストールのトラブルシューティングの詳細は、インストールのトラブルシューティング を参照してください。
- Red Hat サポートにサポートを依頼する手順は、Red Hat OpenShift Service on AWS のサポートを受ける を参照してください。

第2章 TERRAFORM を使用した ROSA クラスターの作成

2.1. TERRAFORM を使用したデフォルトの ROSA クラスターの作成

デフォルトのクラスターオプションで設定された Terraform クラスターテンプレートを使用して、Red Hat OpenShift Service on AWS (ROSA) クラスターを迅速に作成します。

以下で説明するクラスター作成プロセスでは、次のリソースを使用して ROSA with HCP クラスターを準備する Terraform 設定を使用します。

- マネージド **oidc-config** 設定を使用する OIDC プロバイダー
- 関連する AWS Managed ROSA ポリシーを備えた IAM Operator ロールの前提条件
- 関連する AWS Managed ROSA ポリシーを含む IAM アカウントロール
- STS を使用する ROSA クラスターの作成に必要な他のすべての AWS リソース

2.1.1. Terraform の概要

Terraform は、リソースを設定すると必要に応じてそれらのリソースをレプリケートできる infrastructure-as-code ツールです。Terraform は、宣言的言語を使用して作成タスクを実行します。インフラストラクチャーリソースの任意の最終状態を宣言すると、Terraform は仕様に合わせてリソースを作成します。

前提条件

Terraform 設定内で Red Hat Cloud Services プロバイダー を使用するには、次の前提条件を満たす必要があります。

- Red Hat OpenShift Service on AWS (ROSA) コマンドラインインターフェイス (CLI) ツールをインストールしている。
- オフライン Red Hat OpenShift Cluster Manager トークン がある。
- Terraform バージョン 1.4.6 以降をインストールしている。
- AWS アカウント全体の IAM ロールを作成している。
  特定のアカウント全体の IAM ロールとポリシーが ROSA のサポート、インストール、コントロールプレーン、コンピューティング機能に必要な STS 権限を提供する。これには、アカウント全体の Operator ポリシーが含まれます。AWS アカウントロールの詳細は、関連情報を参照してください。
- リソースの作成に必要な AWS アカウント と関連する認証情報 がある。認証情報は AWS プロバイダー用に設定されています。AWS Terraform プロバイダーのドキュメント で、Authentication and Configuration セクションを参照してください。
- Terraform を操作する AWS IAM ロールポリシーに、少なくとも以下の権限がある。権限については、AWS コンソールで確認してください。

例2.1 Terraform の最小限の AWS 権限

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:CreatePolicyVersion",
        "iam:UpdateAssumeRolePolicy",
        "secretsmanager:DescribeSecret",
        "iam:ListRoleTags",
        "secretsmanager:PutSecretValue",
        "secretsmanager:CreateSecret",
        "iam:TagRole",
        "secretsmanager:DeleteSecret",
        "iam:UpdateOpenIDConnectProviderThumbprint",
        "iam:DeletePolicy",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "secretsmanager:GetSecretValue",
        "iam:DetachRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicyTags",
        "iam:ListRolePolicies",
        "iam:DeleteOpenIDConnectProvider",
        "iam:DeleteInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:DeleteRole",
        "iam:TagPolicy",
        "iam:CreateOpenIDConnectProvider",
        "iam:CreatePolicy",
        "secretsmanager:GetResourcePolicy",
        "iam:ListPolicyVersions",
        "iam:UpdateRole",
        "iam:GetOpenIDConnectProvider",
        "iam:TagOpenIDConnectProvider",
        "secretsmanager:TagResource",
        "sts:AssumeRoleWithWebIdentity",
        "iam:ListRoles"
      ],
      "Resource": [
        "arn:aws:secretsmanager:*:<ACCOUNT_ID>:secret:*",
        "arn:aws:iam::<ACCOUNT_ID>:instance-profile/*",
        "arn:aws:iam::<ACCOUNT_ID>:role/*",
        "arn:aws:iam::<ACCOUNT_ID>:oidc-provider/*",
        "arn:aws:iam::<ACCOUNT_ID>:policy/*"
      ]
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:*"
        ],
      "Resource": "*"
```

```
    }
  ]
}
```

Terraform を使用する場合の考慮事項

一般に、Terraform を使用してクラウドリソースを管理する場合は、すべての変更が Terraform 方法論を使用して実行されることを前提として行う必要があります。AWS コンソールや Red Hat コンソールなど、Terraform 外部のツールを使用して Terraform によって作成されたクラウドリソースを変更する場合は注意してください。Terraform によってすでに管理されているクラウドリソースを管理するために Terraform 外部のツールを使用すると、宣言した Terraform 設定から設定のドリフトが発生します。

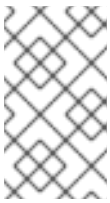
たとえば、Red Hat Hybrid Cloud Console を使用して Terraform で作成されたクラスターをアップグレードする場合は、今後の設定変更を適用する前に Terraform の状態を調整する必要があります。詳細は、HashiCorp Developer ドキュメントの Manage resources in Terraform state を参照してください。

2.1.2. デフォルトのクラスター仕様の概要

表2.1 STS クラスター仕様のデフォルト ROSA

コンポーネント	デフォルトの仕様
アカウントおよびロール	• デフォルトの IAM ロールの接頭辞: **rosa-<6-digit-alphanumeric-string>** • クラスター管理者ロールは作成されない
クラスター設定	• デフォルトのクラスターバージョン: **4.14** • クラスター名: **rosa-<6-digit-alphanumeric-string>** • Red Hat OpenShift Cluster Manager Hybrid Cloud Console を使用したインストール用のデフォルトの AWS リージョン: us-east-2 (US East, Ohio) • 可用性: データプレーンのマルチゾーン • EC2 インスタンスメタデータサービス (IMDS) が有効になっており、IMDSv1 または IMDSv2 の使用が許可されています (トークンはオプション) • ユーザー定義プロジェクトの監視: 有効
暗号化	• クラウドストレージは保存時に暗号化されます。 • 追加の etcd 暗号化が有効になっていません。 • デフォルトの AWS Key Management Service (KMS) キーは、永続データの暗号化キーとして使用されます。 • AWS Key Management Service (KMS) キー暗号化は、デフォルトでは有効になっていません。

コンポーネント	デフォルトの仕様
コントロールプレーンノードの設定	• コントロールプレーンノードのインスタンスタイプ: m5.2xlarge (8 vCPU, 32 GiB RAM) • コントロールプレーンノード数: 3
インフラストラクチャーノードの設定	• インフラストラクチャーノードインスタンスタイプ: r5.xlarge (4 vCPU, 32 GiB RAM) • インフラストラクチャーノード数: 2
コンピュートノードマシンプール	• コンピュートノードインスタンスタイプ: m5.xlarge (4 vCPU 16, GiB RAM) • Compute node count: 3 • 自動スケーリング: 無効 • 追加のノードラベルなし
ネットワーク設定	• クラスターのプライバシー: パブリックまたはプライベート • Terraform クラスターの作成プロセス中に、新しい VPC を作成することを選択できます。 • 独自の Virtual Private Cloud (VPC) を設定しておく必要があります。 • クラスター全体のプロキシーは設定されていません。
Classless Inter-Domain Routing (CIDR) の範囲	• Machine CIDR: 10.0.0.0/16 • Service CIDR: 172.30.0.0/16 • Pod CIDR: 10.128.0.0/14 • Host prefix: /23

コンポーネント	デフォルトの仕様
クラスターのロールおよびポリシー	• Operator ロールおよび OpenID Connect (OIDC) プロバイダーの作成に使用されるモード: **auto**  **注記** Hybrid Cloud Console で OpenShift Cluster Manager を使用するインストールの場合、**auto** モードには管理者権限が割り当てられた OpenShift Cluster Manager ロールが必要です。 • デフォルトの Operator ロールの接頭辞: **rosa-<6-digit-alphanumeric-string>**
クラスター更新戦略	• 個別の更新 • ノードドレインの 1 時間の猶予期間

2.1.3. Terraform を使用したデフォルトの ROSA クラスターの作成

以下に概説するクラスター作成プロセスでは、Terraform を使用して、アカウント全体の IAM ロールとマネージド OIDC 設定を使用する ROSA クラスターを作成する方法を示します。

2.1.3.1. Terraform 用の環境の準備

Terraform を使用して Red Hat OpenShift Service on AWS クラスターを作成する前に、オフラインの Red Hat OpenShift Cluster Manager トークン をエクスポートする必要があります。

手順

1. **オプション**: この手順の実行中、現在のディレクトリーに Terraform ファイルが作成されます。次のコマンドを実行すると、これらのファイルを保存する新しいディレクトリーを作成してそこに移動できます。

```
$ mkdir terraform-cluster && cd terraform-cluster
```

2. オフラインの Red Hat OpenShift Cluster Manager トークン を使用して、アカウントに権限を付与します。

3. オフライントークンをコピーし、次のコマンドを実行してトークンを環境変数として設定します。

```
$ export RHCS_TOKEN=<your_offline_token>
```

注記

この環境変数は、マシンの再起動やターミナルの終了など、各セッションの終了時にリセットされます。

検証

- トークンをエクスポートしたら、次のコマンドを実行して値を確認します。

```
$ echo $RHCS_TOKEN
```

2.1.3.2. ローカルでの Terraform ファイルの作成

オフラインの Red Hat OpenShift Cluster Manager トークン を設定した後、クラスターを構築するために Terraform ファイルをローカルで作成する必要があります。このファイルは、次のコードテンプレートを使用して作成できます。

手順

1. 次のコマンドを実行して、**main.tf** ファイルを作成します。

```
$ cat<<-EOF>main.tf
#
# Copyright (c) 2023 Red Hat, Inc.
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#   http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#
terraform {
  required_providers {
    aws = {
      source  = "hashicorp/aws"
      version = ">= 4.20.0"
    }
    rhcs = {
      version = ">= 1.6.3"
      source  = "terraform-redhat/rhcs"
    }
  }
}

# Export token using the RHCS_TOKEN environment variable
provider "rhcs" {}

provider "aws" {
  region = var.aws_region
  ignore_tags {
    key_prefixes = ["kubernetes.io/"]
  }
  default_tags {
    tags = var.default_aws_tags
```

```
  }
}

data "aws_availability_zones" "available" {}

locals {
  # Extract availability zone names for the specified region, limit it to 3 if multi az or 1 if single
  region_azs = var.multi_az ? slice([for zone in data.aws_availability_zones.available.names :
format("%s", zone)], 0, 3) : slice([for zone in data.aws_availability_zones.available.names :
format("%s", zone)], 0, 1)
}

resource "random_string" "random_name" {
  length  = 6
  special = false
  upper   = false
}

locals {
  worker_node_replicas = var.multi_az ? 3 : 2
  # If cluster_name is not null, use that, otherwise generate a random cluster name
  cluster_name = coalesce(var.cluster_name, "rosa-\${random_string.random_name.result}")
}

# The network validator requires an additional 60 seconds to validate Terraform clusters.
resource "time_sleep" "wait_60_seconds" {
  count = var.create_vpc ? 1 : 0
  depends_on = [module.vpc]
  create_duration = "60s"
}

module "rosa-hcp" {
  source                 = "terraform-redhat/rosa-hcp/rhcs"
  version                = "1.6.3"
  cluster_name           = local.cluster_name
  openshift_version      = var.openshift_version
  account_role_prefix    = local.cluster_name
  operator_role_prefix   = local.cluster_name
  replicas               = local.worker_node_replicas
  aws_availability_zones = local.region_azs
  create_oidc            = true
  private                = var.private_cluster
  aws_subnet_ids         = var.create_vpc ? var.private_cluster ?
module.vpc[0].private_subnets : concat(module.vpc[0].public_subnets,
module.vpc[0].private_subnets) : var.aws_subnet_ids
  create_account_roles   = true
  create_operator_roles  = true
# Optional: Configure a cluster administrator user <.>
#
# Option 1: Default cluster-admin user
# Create an administrator user (cluster-admin) and automatically
# generate a password by uncommenting the following parameter:
#  create_admin_user = true
# Generated administrator credentials are displayed in terminal output.
#
# Option 2: Specify administrator username and password
```

```
# Create an administrator user and define your own password
# by uncommenting and editing the values of the following parameters:
#  admin_credentials_username = <username>
#  admin_credentials_password = <password>

  depends_on = [time_sleep.wait_60_seconds]
}
EOF
```

<.> オプション: 適切なパラメーターのコメントを解除し、必要に応じて値を編集して、クラスターの作成中に管理者ユーザーを作成します。

2. 次のコマンドを実行して、**variables.tf** ファイルを作成します。

注記

クラスターを構築するコマンドを実行する **前** に、このファイルをコピーして編集します。

```
$ cat<<-EOF>variables.tf
#
# Copyright (c) 2023 Red Hat, Inc.
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#   http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#
variable "openshift_version" {
  type        = string
  default     = "4.14.20"
  description = "Desired version of OpenShift for the cluster, for example '4.14.20'. If version is
greater than the currently running version, an upgrade will be scheduled."
}

variable "create_vpc" {
  type        = bool
  description = "If you would like to create a new VPC, set this value to 'true'. If you do not
want to create a new VPC, set this value to 'false'."
}

# ROSA Cluster info
variable "cluster_name" {
  default     = null
  type        = string
  description = "The name of the ROSA cluster to create"
}
```

```
variable "additional_tags" {
  default = {
    Terraform   = "true"
    Environment = "dev"
  }
  description = "Additional AWS resource tags"
  type        = map(string)
}

variable "multi_az" {
  type        = bool
  description = "Multi AZ Cluster for High Availability"
  default     = true
}

variable "worker_node_replicas" {
  default     = 3
  description = "Number of worker nodes to provision. Single zone clusters need at least 2
nodes, multizone clusters need at least 3 nodes"
  type        = number
}

variable "aws_subnet_ids" {
  type        = list(any)
  description = "A list of either the public or public + private subnet IDs to use for the cluster
blocks to use for the cluster"
  default     = ["subnet-01234567890abcdef", "subnet-01234567890abcdef", "subnet-
01234567890abcdef"]
}

variable "private_cluster" {
  type        = bool
  description = "If you want to create a private cluster, set this value to 'true'. If you want a
publicly available cluster, set this value to 'false'."
}

#VPC Info
variable "vpc_name" {
  type        = string
  description = "VPC Name"
  default     = "tf-qs-vpc"
}

variable "vpc_cidr_block" {
  type        = string
  description = "value of the CIDR block to use for the VPC"
  default     = "10.0.0.0/16"
}

variable "private_subnet_cidrs" {
  type        = list(any)
  description = "The CIDR blocks to use for the private subnets"
  default     = ["10.0.1.0/24", "10.0.2.0/24", "10.0.3.0/24"]
}

variable "public_subnet_cidrs" {
```

```
  type        = list(any)
  description = "The CIDR blocks to use for the public subnets"
  default     = ["10.0.101.0/24", "10.0.102.0/24", "10.0.103.0/24"]
}

variable "single_nat_gateway" {
  type        = bool
  description = "Single NAT or per NAT for subnet"
  default     = false
}

#AWS Info
variable "aws_region" {
  type    = string
  default = "us-east-2"
}

variable "default_aws_tags" {
  type        = map(string)
  description = "Default tags for AWS"
  default     = {}
}
EOF
```

3. 以下のコマンドを実行して **vpc.tf** ファイルを作成します。

```
$ cat<<-EOF>vpc.tf
#
# Copyright (c) 2023 Red Hat, Inc.
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#   http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#
module "vpc" {
  source  = "terraform-aws-modules/vpc/aws"
  version = "5.1.2"

  count = var.create_vpc ? 1 : 0
  name  = var.vpc_name
  cidr  = var.vpc_cidr_block

  azs             = local.region_azs
  private_subnets = var.multi_az ? var.private_subnet_cidrs : [var.private_subnet_cidrs[0]]
  public_subnets  = var.multi_az ? var.public_subnet_cidrs : [var.public_subnet_cidrs[0]]

  enable_nat_gateway   = true
  single_nat_gateway   = var.single_nat_gateway
```

```
  enable_dns_hostnames = true
  enable_dns_support   = true

  tags = var.additional_tags
}
EOF
```

これで Terraform を起動する準備ができました。

2.1.3.3. Terraform を使用した ROSA クラスターの作成

Terraform ファイルを作成した後、Terraform を起動して、必要な依存関係をすべて提供する必要があります。その後、Terraform プランを適用します。

重要

Terraform の状態ファイルは変更しないでください。詳細は、Terraform 使用時の考慮事項 を参照してください。

手順

1. Terraform ファイルに基づいてリソースを作成するように Terraform を設定し、次のコマンドを実行します。

```
$ terraform init
```

2. **オプション**: 次のコマンドを実行して、コピーした Terraform が正しいことを確認します。

```
$ terraform validate
```

出力例

```
Success! The configuration is valid.
```

3. 次のコマンドを実行して、Terraform を使用してクラスターを作成します。

```
$ terraform apply
```

Terraform インターフェイスでは、クラスターを作成するために次のような 2 つの質問が尋ねられます。

出力例

```
var.create_vpc
  If you would like to create a new VPC, set this value to 'true'. If you do not want to create a
new VPC, set this value to 'false'.

  Enter a value:

var.private_cluster
  If you want to create a private cluster, set this value to 'true'. If you want a publicly available
```

```
cluster, set this value to 'false'.

  Enter a value:
```

4. Terraform インターフェイスに作成または変更するリソースがリストされ、確認を求めるプロンプトが表示されたら、続行するには **yes** を、キャンセルするには **no** を入力します。

出力例

```
Plan: 63 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.
```

yes と入力すると、Terraform プランが開始され、AWS アカウントロール、Operator ロール、ROSA Classic クラスターが作成されます。

検証

1. 次のコマンドを実行して、クラスターが作成されたことを確認します。

```
$ rosa list clusters
```

クラスターの ID、名前、ステータスを示す出力例

```
ID                            NAME         STATE  TOPOLOGY
27c3snjsupa9obua74ba8se5kcj11269  rosa-tf-demo  ready  Classic (STS)
```

2. 次のコマンドを実行して、アカウントロールが作成されたことを確認します。

```
$ rosa list account-roles
```

出力例

```
I: Fetching account roles
ROLE NAME                              ROLE TYPE      ROLE ARN
OPENSHIFT VERSION  AWS Managed
ROSA-demo-Installer-Role                 Installer     arn:aws:iam::<ID>:role/ROSA-demo-
Installer-Role                4.14           No
ROSA-demo-Support-Role                   Support       arn:aws:iam::<ID>:role/ROSA-demo-
Support-Role                  4.14           No
ROSA-demo-Worker-Role                    Worker        arn:aws:iam::<ID>:role/ROSA-demo-
Worker-Role                   4.14           No
```

3. 次のコマンドを実行して、Operator ロールが作成されたことを確認します。

```
$ rosa list operator-roles
```

Terraform で作成された Operator ロールを示す出力例

```
I: Fetching operator roles
ROLE PREFIX    AMOUNT IN BUNDLE
rosa-demo      8
```

2.1.3.4. Terraform を使用した ROSA クラスターの削除

terraform destroy コマンドを使用して、**terraform apply** コマンドで作成したすべてのリソースを削除します。

注記

リソースを破棄する前に、Terraform の **.tf** ファイルを変更しないでください。これらの変数は削除対象のリソースと照合されます。

手順

1. **terraform apply** コマンドを実行してクラスターを作成したディレクトリーで、次のコマンドを実行してクラスターを削除します。

```
$ terraform destroy
```

Terraform インターフェイスでは、2 つの変数の入力を求められます。これらは、クラスターの作成時に指定した回答と一致する必要があります。

```
var.create_vpc
  If you would like to create a new VPC, set this value to 'true.' If you do not want to create a new VPC, set this value to 'false.'

  Enter a value:

var.private_cluster
  If you want to create a private cluster, set this value to 'true.' If you want a publicly available cluster, set this value to 'false.'

  Enter a value:
```

2. **yes** と入力して、ロールとクラスターの削除を開始します。

出力例

```
Plan: 0 to add, 0 to change, 63 to destroy.

Do you really want to destroy all resources?
  Terraform will destroy all your managed infrastructure, as shown above.
  There is no undo. Only 'yes' will be accepted to confirm.

  Enter a value: yes
```

検証

1. 次のコマンドを実行して、クラスターが破棄されたことを確認します。

```
$ rosa list clusters
```

```
-
```

クラスターがないことを示す出力例

```
I: No clusters available
```

2. 次のコマンドを実行して、アカウントロールが破棄されたことを確認します。

```
$ rosa list account-roles
```

Terraform で作成されたアカウントロールがないことを示す出力例

```
I: Fetching account roles
I: No account roles available
```

3. 次のコマンドを実行して、Operator ロールが破棄されたことを確認します。

```
$ rosa list operator-roles
```

Terraform で作成された Operator ロールがないことを示す出力例

```
I: Fetching operator roles
I: No operator roles available
```

2.1.4. 関連情報

- アカウント全体の IAM ロールおよびポリシー参照

第3章 カスタム AWS KMS 暗号鍵を使用した ROSA WITH HCP クラスターの作成

カスタムの AWS Key Management Service (KMS) キーを使用して、Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane クラスターを作成します。

3.1. ROSA WITH HCP の前提条件

ROSA with HCP クラスターを作成するには、次のものが必要です。

- 設定された仮想プライベートクラウド (VPC)
- アカウント全体のロール
- OIDC 設定
- オペレーターのロール

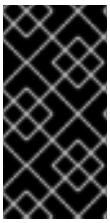
3.1.1. ROSA with HCP クラスター用の仮想プライベートクラウドの作成

ROSA with HCP クラスターを作成するには、Virtual Private Cloud (VPC) が必要です。次の方法を使用して VPC を作成できます。

- Terraform テンプレートを使用して VPC を作成する
- AWS コンソールで VPC リソースを手動で作成する

注記

Terraform の手順はテストとデモンストレーションを目的としています。独自のインストールでは、独自に使用するために VPC にいくつかの変更を加える必要があります。また、この Terraform スクリプトを使用するときは、クラスターをインストールする予定のリージョンと同じリージョンにあることを確認する必要があります。これらの例では、**us-east-2** を使用します。



重要

現在、ROSA with HCP では 複数の AWS アカウント間での VPC の共有 はサポートされていません。別の AWS アカウントから共有されているサブネットに ROSA with HCP クラスターをインストールしないでください。詳細は、"Are multiple ROSA clusters in a single VPC supported?" を参照してください。

Terraform を使用した Virtual Private Cloud の作成
Terraform は、確立されたテンプレートを使用してさまざまなリソースを作成できるツールです。次のプロセスでは、必要に応じてデフォルトのオプションを使用して、ROSA with HCP クラスターを作成します。Terraform の使用の詳細は、関連情報を参照してください。

前提条件

- マシンに Terraform バージョン 1.4.0 以降がインストールされている。
- マシンに Git がインストールされている。

手順

1. シェルプロンプトを開き、次のコマンドを実行して Terraform VPC リポジトリーのクローンを作成します。

```
$ git clone https://github.com/openshift-cs/terraform-vpc-example
```

2. 次のコマンドを実行して、作成したディレクトリーに移動します。

```
$ cd terraform-vpc-example
```

3. 次のコマンドを実行して、Terraform ファイルを開始します。

```
$ terraform init
```

このプロセスが完了すると、初期化を確認するメッセージが表示されます。

4. 既存の Terraform テンプレートに基づいて VPC Terraform プランを構築するには、**plan** コマンドを実行します。AWS リージョンを含める必要があります。クラスター名の指定を選択できます。**terraform plan** が完了すると、**rosa.tfplan** ファイルが **hypershift-tf** ディレクトリーに追加されます。オプションの詳細は、Terraform VPC リポジトリーの README ファイル を参照してください。

```
$ terraform plan -out rosa.tfplan -var region=<region>
```

5. 次のコマンドを実行して、このプランファイルを適用して VPC を構築します。

```
$ terraform apply rosa.tfplan
```

a. 任意: 次のコマンドを実行して、Terraform でプロビジョニングされたプライベート、パブリック、およびマシンプールのサブネット ID の値を環境変数としてキャプチャーし、ROSA with HCP クラスターを作成するときに使用できます。

```
$ export SUBNET_IDS=$(terraform output -raw cluster-subnets-string)
```

b. 次のコマンドを使用して、変数が正しく設定されたことを確認できます。

```
$ echo $SUBNET_IDS
```

出力例

```
$ subnet-0a6a57e0f784171aa,subnet-078e84e5b10ecf5b0
```

関連情報

- ニーズに合わせて VPC をカスタマイズするときに使用できるすべてのオプションの詳細なリストは、Terraform VPC リポジトリーを参照してください。

Virtual Private Cloud を手動で作成する

Terraform を使用する代わりに Virtual Private Cloud (VPC) を手動で作成することを選択した場合は、AWS コンソールの VPC ページ に移動します。VPC は、次の表に示す要件を満たしている必要があります。

表3.1 VPC の要件

要件	詳細
VPC 名	クラスターを作成するときは、特定の VPC 名と ID が必要です。
CIDR 範囲	VPC CIDR 範囲はマシンの CIDR と一致する必要があります。
アベイラビリティーゾーン	単一ゾーンの場合は 1 つの可用性ゾーンが必要で、複数ゾーンの場合は 3 つの可用性ゾーンが必要です。
パブリックサブネット	パブリッククラスターには、NAT ゲートウェイを備えたパブリックサブネットが 1 つ必要です。プライベートクラスターにはパブリックサブネットは必要ありません。
DNS ホスト名と解決	DNS ホスト名と解決が有効になっていることを確認する必要があります。

関連情報

- Get Started with Amazon VPC
- HashiCorp Terraform ドキュメント

3.1.2. アカウント全体の STS ロールおよびポリシーの作成

Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) を使用して、Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane クラスターを作成する前に、Operator ポリシーを含む、必要なアカウント全体のロールとポリシーを作成します。

注記

ROSA with HCP クラスターには、AWS 管理ポリシーがアタッチされたアカウントと Operator ロールが必要です。顧客管理のポリシーはサポートされていません。ROSA with HCP クラスターの AWS 管理ポリシーの詳細は、AWS managed policies for ROSA account roles を参照してください。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。
- 利用可能な AWS サービスクォータがある。
- AWS コンソールで ROSA サービスを有効にしている。
- インストールホストに、最新の ROSA CLI (**rosa**) をインストールして設定している。
- ROSA CLI を使用して Red Hat アカウントにログインしている。

手順

1. AWS アカウントに存在しない場合は、次のコマンドを実行して、必要なアカウント全体の STS ロールを作成し、ポリシーをアタッチします。

```
$ rosa create account-roles --hosted-cp
```

2. オプション: 次のコマンドを実行して、接頭辞を環境変数として設定します。

```
$ export ACCOUNT_ROLES_PREFIX=<account_role_prefix>
```

- 次のコマンドを実行して、変数の値を表示します。

```
$ echo $ACCOUNT_ROLES_PREFIX
```

出力例

```
ManagedOpenShift
```

ROSA の AWS 管理 IAM ポリシーの詳細は、AWS managed IAM policies for ROSA を参照してください。

3.1.3. OpenID Connect 設定の作成

ROSA with HCP クラスターを使用する場合は、クラスターを作成する前に OpenID Connect (OIDC) 設定を作成する必要があります。この設定は、OpenShift Cluster Manager で使用するために登録されています。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。
- Red Hat OpenShift Service on AWS の AWS 前提条件を完了している。
- インストールホストに、最新の Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールして設定している。

手順

1. AWS リソースと一緒に OIDC 設定を作成するには、次のコマンドを実行します。

```
$ rosa create oidc-config --mode=auto --yes
```

このコマンドは次の情報を返します。

出力例

```
? Would you like to create a Managed (Red Hat hosted) OIDC Configuration Yes
I: Setting up managed OIDC configuration
I: To create Operator Roles for this OIDC Configuration, run the following command and
remember to replace <user-defined> with a prefix of your choice:
 rosa create operator-roles --prefix <user-defined> --oidc-config-id 13cdr6b
If you are going to create a Hosted Control Plane cluster please include '--hosted-cp'
```

```
I: Creating OIDC provider using 'arn:aws:iam::4540112244:user/userName'
? Create the OIDC provider? Yes
I: Created OIDC provider with ARN 'arn:aws:iam::4540112244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/13cdr6b'
```

クラスターを作成するときは、OIDC 設定 ID を指定する必要があります。CLI 出力では、**--mode auto** のこの値が提供されます。それ以外の場合は、**--mode manual** の **aws** CLI 出力に基づいてこれらの値を決定する必要があります。

2. オプション: OIDC 設定 ID を変数として保存して、後で使用できます。次のコマンドを実行して変数を保存します。

```
$ export OIDC_ID=<oidc_config_id>
```
1

1 上記の出力例では、OIDC 設定 ID は 13cdr6b です。

- 次のコマンドを実行して、変数の値を表示します。

```
$ echo $OIDC_ID
```

出力例

```
13cdr6b
```

検証

- ユーザー組織に関連付けられているクラスターで使用できる可能な OIDC 設定をリストできます。以下のコマンドを実行します。

```
$ rosa list oidc-config
```

出力例

```
ID                               MANAGED  ISSUER URL
SECRET ARN
2330dbs0n8m3chkkr25gkkcd8pnj3lk2  true
https://dvbwgdztaeq9o.cloudfront.net/2330dbs0n8m3chkkr25gkkcd8pnj3lk2
233hvnrjoqu14jltk6lhbhf2tj11f8un  false    https://oidc-r7u1.s3.us-east-1.amazonaws.com
aws:secretsmanager:us-east-1:242819244:secret:rosa-private-key-oidc-r7u1-tM3MDN
```

3.1.4. Operator のロールとポリシーの作成

ROSA with HCP クラスターを使用する場合は、Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane (HCP) デプロイメントに必要な Operator IAM ロールを作成する必要があります。クラスター Operator は、Operator のロールを使用して、バックエンドストレージ、クラウドプロバイダーの認証情報、クラスターへの外部アクセスの管理など、クラスター操作を実行するために必要な一時的なアクセス許可を取得します。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。

- インストールホストに、最新の Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールして設定している。
- アカウント全体の AWS ロールを作成している。

手順

1. 次のコマンドを使用して、接頭辞名を環境変数に設定します。

```
$ export OPERATOR_ROLES_PREFIX=<prefix_name>
```

2. Operator ロールを作成するには、次のコマンドを実行します。

```
$ rosa create operator-roles --hosted-cp --prefix=$OPERATOR_ROLES_PREFIX --oidc-config-id=$OIDC_ID --installer-role-arn arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role
```

次の内訳は、Operator ロール作成のオプションを示しています。

```
$ rosa create operator-roles --hosted-cp
 --prefix=$OPERATOR_ROLES_PREFIX (1)
 --oidc-config-id=$OIDC_ID (2)
 --installer-role-arn
arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role (3)
```

(1) これらの Operator ロールを作成するときは、接頭辞を指定する必要があります。そうしないとエラーが発生します。演算子接頭辞は、このセクションの関連情報を参照してください。

(2) この値は、ROSA with HCP クラスター用に作成した OIDC 設定 ID です。

(3) この値は、ROSA アカウントロールの作成時に作成したインストーラーロールの ARN です。

ROSA with HCP クラスター用の正しいロールを作成するには、**--hosted-cp** パラメーターを含める必要があります。このコマンドは次の情報を返します。

出力例

```
? Role creation mode: auto
? Operator roles prefix: <pre-filled_prefix> (1)
? OIDC Configuration ID: 23soa2bgvpek9kmes9s7os0a39i13qm4 | https://dvbwgdztaeq9o.cloudfront.net/23soa2bgvpek9kmes9s7os0a39i13qm4 (2)
? Create hosted control plane operator roles: Yes
W: More than one Installer role found
? Installer role ARN: arn:aws:iam::4540112244:role/<prefix>-HCP-ROSA-Installer-Role
? Permissions boundary ARN (optional):
I: Reusable OIDC Configuration detected. Validating trusted relationships to operator roles:
I: Creating roles using 'arn:aws:iam::4540112244:user/<userName>'
I: Created role '<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials' with ARN 'arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials'
```

```
I: Created role '<prefix>-openshift-cloud-network-config-controller-cloud-credenti' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-controller-cloud-
credenti'
I: Created role '<prefix>-kube-system-kube-controller-manager' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager'
I: Created role '<prefix>-kube-system-capa-controller-manager' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager'
I: Created role '<prefix>-kube-system-control-plane-operator' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator'
I: Created role '<prefix>-kube-system-kms-provider' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider'
I: Created role '<prefix>-openshift-image-registry-installer-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-credentials'
I: Created role '<prefix>-openshift-ingress-operator-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials'
I: To create a cluster with these roles, run the following command:
 rosa create cluster --sts --oidc-config-id 23soa2bgvpek9kmes9s7os0a39i13qm4 --operator-
roles-prefix <prefix> --hosted-cp
```

1. このフィールドには、最初の作成コマンドで設定した接頭辞が事前に入力されます。
2. このフィールドでは、ROSA with HCP クラスター用に作成した OIDC 設定を選択する必要があります。

これで、Operator ロールが作成され、ROSA with HCP クラスターの作成に使用できるようになりました。

検証

- ROSA アカウントに関連付けられている Operator ロールをリスト表示できます。以下のコマンドを実行します。

```
$ rosa list operator-roles
```

出力例

```
I: Fetching operator roles
ROLE PREFIX  AMOUNT IN BUNDLE
<prefix>      8
? Would you like to detail a specific prefix Yes (1)
? Operator Role Prefix: <prefix>
ROLE NAME                                          ROLE ARN
VERSION  MANAGED
<prefix>-kube-system-capa-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager
4.13     No
<prefix>-kube-system-control-plane-operator
arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator
4.13     No
<prefix>-kube-system-kms-provider
arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider                    4.13
No
<prefix>-kube-system-kube-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager
```

```
4.13     No
<prefix>-openshift-cloud-network-config-controller-cloud-credenti
arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-controller-cloud-
credenti  4.13     No
<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
4.13     No
<prefix>-openshift-image-registry-installer-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-credentials
4.13     No
<prefix>-openshift-ingress-operator-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials
4.13     No
```

1 コマンドを実行すると、AWS アカウントに関連付けられているすべての接頭辞が表示され、この接頭辞に関連付けられているロールの数が記録されます。これらのロールとその詳細をすべて表示する必要がある場合は、詳細プロンプトで "Yes" と入力すると、これらのロールが詳細とともにリストされます。

3.1.5. カスタム AWS KMS キーを使用した ROSA クラスターの作成

ノードのルートボリューム、etcd データベース、またはその両方の暗号化に使用するお客様提供の KMS キーを使用して、Red Hat OpenShift Service on AWS (ROSA) クラスターを作成できます。両方にそれぞれ異なる KMS キー ARN を指定できます。

注記

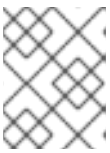
ROSA with HCP は、お客様提供の KMS キーを使用して永続ボリュームを暗号化するように **default** ストレージクラスを自動設定しません。これは、インストール後にクラスター内で設定できるものです。

手順

1. 次のコマンドを実行して、AWS の顧客管理のカスタム KMS キーを作成します。

```
$ KMS_ARN=$(aws kms create-key --region $AWS_REGION --description 'Custom ROSA
Encryption Key' --tags TagKey=red-hat,TagValue=true --query KeyMetadata.Arn --output
text)
```

このコマンドで、後の手順のために、このカスタムキーの Amazon リソースネーム (ARN) 出力が保存されます。



注記

お客様は、お客様の KMS キーに必要な **--tags TagKey=red-hat,TagValue=true** 引数を指定する必要があります。

2. 次のコマンドを実行して、KMS キーが作成されたことを確認します。

```
$ echo $KMS_ARN
```

3. AWS アカウント ID を環境変数に設定します。

```
$ AWS_ACCOUNT_ID=<aws_account_id>
```

4. 前述の手順で作成したアカウント全体のインストーラーロールと Operator ロールの ARN を、ファイルの **Statement.Principal.AWS** セクションに追加します。次の例では、デフォルトの **ManagedOpenShift-HCP-ROSA-Installer-Role** ロールの ARN が追加されます。

```
{
  "Version": "2012-10-17",
  "Id": "key-rosa-policy-1",
  "Statement": [
  {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
       {
            "Sid": "Installer Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:role/ManagedOpenShift-HCP-
ROSA-Installer-Role"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ROSA KubeControllerManager Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:role/<operator_role_prefix>-kube-
system-kube-controller-manager"

            },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "ROSA KMS Provider Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:role/<operator_role_prefix>-kube-
system-kms-provider"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "ROSA NodeManager Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:role/<operator_role_prefix>-kube-
system-capa-controller-manager"
            },
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:CreateGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

5. 次のコマンドを実行して、作成されたポリシーファイルの詳細を確認します。

```
$ cat rosa-key-policy.json
```

6. 次のコマンドを実行して、新しく生成されたキーポリシーをカスタム KMS キーに適用します。

```
$ aws kms put-key-policy --key-id $KMS_ARN \
--policy file://rosa-key-policy.json \
--policy-name default
```

7. 次のコマンドを実行してクラスターを作成します。

注記

クラスター名が 15 文字を超える場合、***.openshiftapps.com** にプロビジョニングされたクラスターのサブドメインとして自動生成されたドメイン接頭辞が含まれます。

サブドメインをカスタマイズするには、**--domain-prefix** フラグを使用します。ドメイン接頭辞は 15 文字を超えてはならず、一意である必要があり、クラスターの作成後に変更できません。

```
$ rosa create cluster --cluster-name <cluster_name> \
--subnet-ids <private_subnet_id>,<public_subnet_id> \
--sts \
--mode auto \
--machine-cidr 10.0.0.0/16 \
--compute-machine-type m5.xlarge \
--hosted-cp \
--region <aws_region> \
--oidc-config-id $OIDC_ID \
--kms-key-arn $KMS_ARN \ 1
--etcd-encryption-kms-arn $KMS_ARN \ 2
--operator-roles-prefix $OPERATOR_ROLES_PREFIX
```

1. この KMS キー ARN は、すべてのワーカーノードのルートボリュームを暗号化するために使用します。etcd データベースの暗号化のみが必要な場合は必要ありません。
2. この KMS キー ARN は、etcd データベースの暗号化に使用します。etcd データベースは、デフォルトでは常に AES 暗号ブロックを使用して暗号化されますが、代わりに KMS キーを使用して暗号化することもできます。ノードのルートボリュームの暗号化のみが必要な場合は必要ありません。

検証

OpenShift Cluster Manager を使用して、KMS キーが機能することを確認できます。

1. OpenShift Cluster Manager に移動し、**Instances** を選択します。
2. インスタンスを選択します。
3. **Storage** タブをクリックします。
4. **KMS key ID** をコピーします。
5. **Key Management Service** を検索して選択します。
6. コピーした **KMS key ID** を **Filter** フィールドに入力します。

3.2. 次のステップ

- ROSA クラスターへのアクセス

3.3. 関連情報

- CLI を使用してクラスターを作成する方法については、CLI を使用した ROSA with HCP クラスターの作成 を参照してください。
- 手動モードを使用して ROSA クラスターをデプロイする手順は、カスタマイズを使用したクラスターの作成 を参照してください。
- STS を使用する Red Hat OpenShift Service on AWS をデプロイするのに必要な AWS Identity Access Management (IAM) リソースの詳細は、STS を使用するクラスターの IAM リソースについて を参照してください。
- オプションで Operator ロール名接頭辞を設定する方法の詳細は、カスタム Operator IAM ロール接頭辞について を参照してください。
- STS を使用する ROSA をインストールするための前提条件の詳細は、STS を使用する ROSA の AWS の前提条件 を参照してください。
- **auto** モードと **manual** モードを使用して必要な STS リソースを作成する方法の詳細は、自動デプロイメントモードと手動デプロイメントモードについて を参照してください。
- AWS IAM での OpenID Connect (OIDC) ID プロバイダーの使用の詳細は、Creating OpenID Connect (OIDC) identity providers を参照してください。
- ROSA クラスターのインストールのトラブルシューティングの詳細は、インストールのトラブルシューティング を参照してください。

- Red Hat サポートにサポートを依頼する手順は、Red Hat OpenShift Service on AWS のサポートを受ける を参照してください。

第4章 ROSA WITH HCP でのプライベートクラスターの作成

パブリックインターネットアクセスを必要としない Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane (HCP) ワークロードの場合は、プライベートクラスターを作成できます。

4.1. ROSA CLI を使用したプライベート ROSA WITH HCP クラスターの作成

ROSA コマンドラインインターフェイス (CLI) **rosa** を使用して、ROSA with HCP に複数のアベイラビリティーゾーン (Multi-AZ) を持つプライベートクラスターを作成できます。

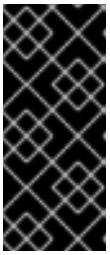
前提条件

- 利用可能な AWS サービスクォータがある。
- AWS コンソールで ROSA サービスを有効にしている。
- インストールホストに、最新バージョンの ROSA CLI をインストールして設定している。

手順

Hosted Control Plane を使用したクラスターの作成には、10 分ほどかかる場合があります。

1. 少なくとも 1 つのプライベートサブネットを持つ VPC を作成します。マシンの Classless Inter-Domain Routing (CIDR) が、仮想プライベートクラウドの CIDR と一致していることを確認します。詳細は、独自の VPC を使用するための要件 および VPC 検証 を参照してください。



重要

ファイアウォールを使用する場合は、ROSA が機能するのに必要なサイトにアクセスできるようにファイアウォールを設定する必要があります。

詳細は、「AWS PrivateLink ファイアウォールの前提条件」セクションを参照してください。

2. 次のコマンドを実行して、アカウント全体の IAM ロールを作成します。

```
$ rosa create account-roles --hosted-cp
```

3. 次のコマンドを実行して、OIDC 設定を作成します。

```
$ rosa create oidc-config --mode=auto --yes
```

OIDC 設定の ID を保存します。Operator ロールの作成に必要なためです。

出力例

```
I: Setting up managed OIDC configuration
I: To create Operator Roles for this OIDC Configuration, run the following command and remember to replace <user-defined> with a prefix of your choice:
 rosa create operator-roles --prefix <user-defined> --oidc-config-id 28s4avcdt2l318r1jbk3ifmimkurk384
If you are going to create a Hosted Control Plane cluster please include '--hosted-cp'
```

```
I: Creating OIDC provider using 'arn:aws:iam::46545644412:user/user'
I: Created OIDC provider with ARN 'arn:aws:iam::46545644412:oidc-
provider/oidc.op1.openshiftapps.com/28s4avcdt2l318r1jbk3ifmimkurk384'
```

4. 次のコマンドを実行して、Operator ロールを作成します。

```
$ rosa create operator-roles --hosted-cp --prefix <operator_roles_prefix> --oidc-config-id
<oidc_config_id> --installer-role-arn
arn:aws:iam::$<account_roles_prefix>:role/$<account_roles_prefix>-HCP-ROSA-Installer-
Role
```

5. 次のコマンドを実行して、ROSA with HCP プライベートクラスターを作成します。

```
$ rosa create cluster --private --cluster-name=<cluster-name> --sts --mode=auto --hosted-cp
--operator-roles-prefix <operator_role_prefix> --oidc-config-id <oidc_config_id> [--machine-
cidr=<VPC CIDR>/16] --subnet-ids=<private-subnet-id1>[,<private-subnet-id2>,<private-
subnet-id3>]
```

6. 以下のコマンドを実行して Pod のステータスを確認します。クラスターの作成中、出力の **State** フィールドは **pending** から **installing** に移行し、最後に **ready** に移行します。

```
$ rosa describe cluster --cluster=<cluster_name>
```

注記

インストールが失敗する場合や、10 分経っても **State** フィールドが **ready** に変わらない場合は、関連情報セクションの「Red Hat OpenShift Service on AWS のインストールのトラブルシューティング」ドキュメントを参照してください。

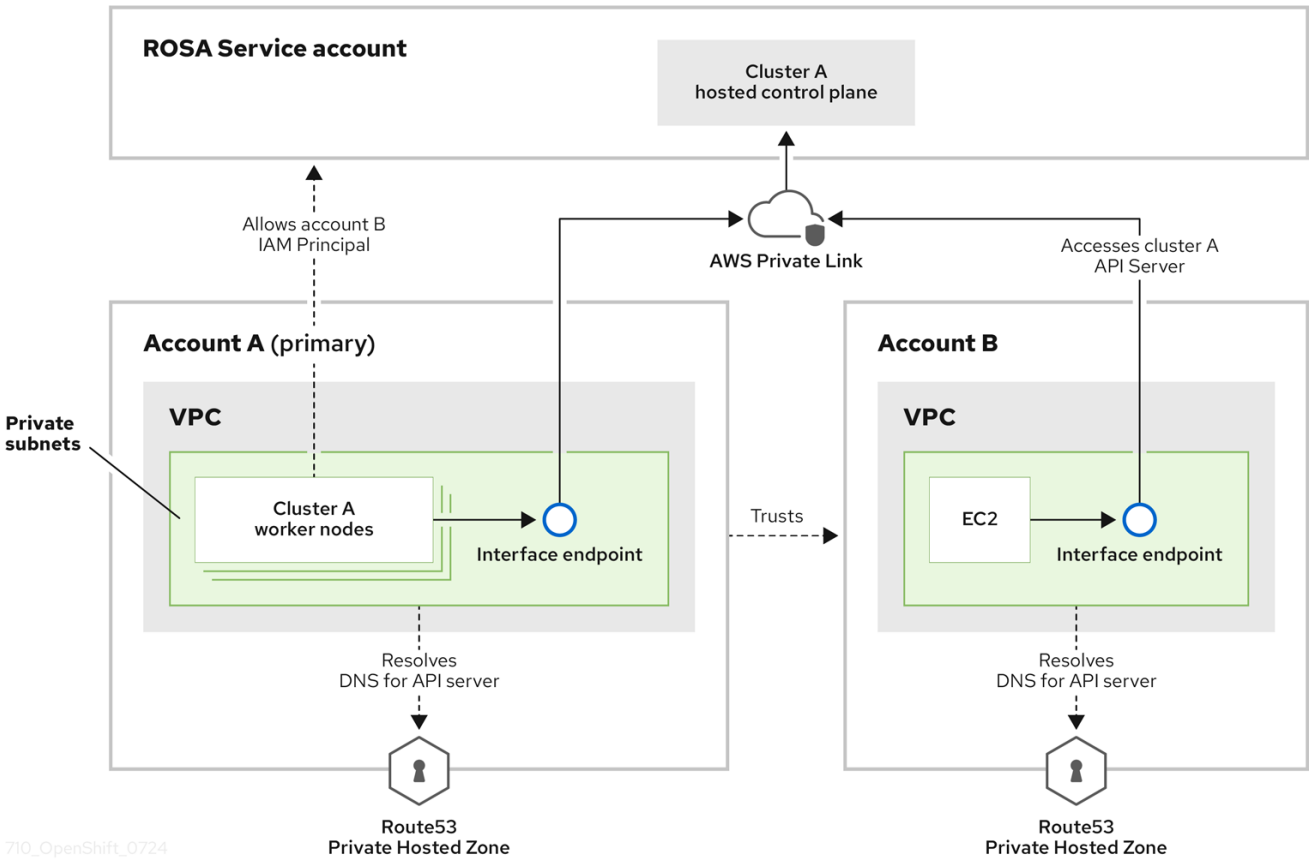
7. 以下のコマンドを実行して、OpenShift インストーラーのログでクラスターの進捗を追跡します。

```
$ rosa logs install --cluster=<cluster_name> --watch
```

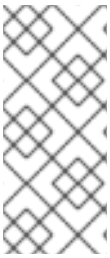
4.2. ROSA WITH HCP クラスター上の追加のプリンシパル

クラスターのプライベート API サーバーエンドポイントに接続するための追加プリンシパルとして、AWS Identity and Access Management (IAM) ロールを許可できます。

パブリックインターネットまたは VPC プライベートサブネット内で作成されたインターフェイスエンドポイントから、ROSA with HCP クラスターの API サーバーエンドポイントにアクセスできます。デフォルトでは、**-kube-system-kube-controller-manager** Operator ロールを使用して、ROSA with HCP API サーバーへのプライベートアクセスが可能です。クラスターがインストールされているプライマリーアカウントを使用せずに、別のアカウントから直接 ROSA with HCP API サーバーにアクセスできるようにするには、追加のプリンシパルとして、クロスアカウント IAM ロールを含める必要があります。この機能を使用すると、ピアリングを回避したり、クロスアカウント VPC をクラスターの VPC にアタッチしたりして、ネットワークアーキテクチャーを簡素化し、データ転送コストを削減できます。



この図では、クラスターを作成するクラスターが Account A として指定されています。このアカウントは、別のアカウントである Account B に API サーバーへのアクセス権が必要であることを指定します。



注記

追加の許可済みプリンシパルを設定した後、クロスアカウント ROSA with HCP API サーバーにアクセスする VPC にインターフェイス VPC エンドポイントを作成する必要があります。次に、Route53 にプライベートホストゾーンを作成し、クロスアカウント ROSA with HCP API サーバーへの呼び出しを、作成された VPC エンドポイントを通過するようにルーティングします。

4.2.1. ROSA with HCP クラスター作成時にプリンシパルを追加する

他のロールを介したアクセスを許可するには、**--additional-allowed-principals** 引数を使用します。

手順

1. 次の例のように、**rosa create cluster** コマンドに **--additional-allowed-principals** 引数を追加します。

```
$ rosa create cluster [...] --additional-allowed-principals <arn_string>
```

arn:aws:iam::account_id:role/role_name を使用して、特定のロールを承認できます。

2. クラスター作成コマンドを実行すると、**--additional-allowed-principals** が指定されたクラスター概要が表示されます。

出力例

```
-
```

```
Name:                       mycluster
Domain Prefix:              mycluster
Display Name:               mycluster
ID:                         <cluster-id>
External ID:                <cluster-id>
Control Plane:              ROSA Service Hosted
OpenShift Version:          4.15.17
Channel Group:              stable
DNS:                        Not ready
AWS Account:                <aws_id>
AWS Billing Account:        <aws_id>
API URL:
Console URL:
Region:                     us-east-2
Availability:
 - Control Plane:           MultiAZ
 - Data Plane:              SingleAZ

Nodes:
 - Compute (desired):       2
 - Compute (current):       0
Network:
 - Type:                    OVNKubernetes
 - Service CIDR:            172.30.0.0/16
 - Machine CIDR:            10.0.0.0/16
 - Pod CIDR:                10.128.0.0/14
 - Host Prefix:             /23
 - Subnets:                 subnet-453e99d40, subnet-666847ce827
EC2 Metadata Http Tokens:   optional
Role (STS) ARN:             arn:aws:iam::<aws_id>:role/mycluster-HCP-ROSA-Installer-Role
Support Role ARN:           arn:aws:iam::<aws_id>:role/mycluster-HCP-ROSA-Support-Role
Instance IAM Roles:
 - Worker:                  arn:aws:iam::<aws_id>:role/mycluster-HCP-ROSA-Worker-Role
Operator IAM Roles:
 - arn:aws:iam::<aws_id>:role/mycluster-kube-system-control-plane-operator
 - arn:aws:iam::<aws_id>:role/mycluster-openshift-cloud-network-config-controller-cloud-
creden
 - arn:aws:iam::<aws_id>:role/mycluster-openshift-image-registry-installer-cloud-credentials
 - arn:aws:iam::<aws_id>:role/mycluster-openshift-ingress-operator-cloud-credentials
 - arn:aws:iam::<aws_id>:role/mycluster-openshift-cluster-csi-drivers-ebs-cloud-credentials
 - arn:aws:iam::<aws_id>:role/mycluster-kube-system-kms-provider
 - arn:aws:iam::<aws_id>:role/mycluster-kube-system-kube-controller-manager
 - arn:aws:iam::<aws_id>:role/mycluster-kube-system-capa-controller-manager
Managed Policies:           Yes
State:                      waiting (Waiting for user action)
Private:                    No
Delete Protection:          Disabled
Created:                    Jun 25 2024 13:36:37 UTC
User Workload Monitoring:   Enabled
Details Page:               https://console.redhat.com/openshift/details/s/Bvbok4O79q1Vg8
OIDC Endpoint URL:          https://oidc.op1.openshiftapps.com/vhufi5lap6vbl3jlq20e
(Managed)
Audit Log Forwarding:       Disabled
External Authentication:    Disabled
Additional Principals:      arn:aws:iam::<aws_id>:role/additional-user-role
```

4.2.2. 既存の ROSA with HCP クラスターにプリンシパルを追加する

コマンドラインインターフェイス (CLI) を使用して、クラスターにプリンシパルをさらに追加できます。

手順

- 次のコマンドを実行してクラスターを編集し、このクラスターのエンドポイントにアクセスできる追加のプリンシパルを追加します。

```
$ rosa edit cluster -c <cluster_name> --additional-allowed-principals <arn_string>
```

arn:aws:iam::account_id:role/role_name を使用して、特定のロールを承認できます。

4.3. 次のステップ

アイデンティティープロバイダーの設定

4.4. 関連情報

- AWS PrivateLink ファイアウォールの前提条件
- STS を使用する ROSA のデプロイメントワークフローの概要
- ROSA クラスターの削除
- ROSA アーキテクチャーモデル
- Red Hat OpenShift Service on AWS のインストールのトラブルシューティング

第5章 外部認証を使用した ROSA WITH HCP クラスターの作成

組み込みの OpenShift OAuth サーバーを置き換えて、外部の OpenID Connect (OIDC) アイデンティティープロバイダーを使用して認証用のトークンを発行する Hosted Control Plane (HCP) クラスターを使用して、Red Hat OpenShift Service on AWS (ROSA) を作成できます。組み込みの OpenShift OAuth サーバーは、外部 OIDC アイデンティティープロバイダーを含むさまざまなアイデンティティープロバイダーとの統合をサポートしていますが、OAuth サーバー自体の機能に制限されています。CLI などのマシン間ワークフローを容易にし、組み込みの OpenShift OAuth サーバーを使用するときには利用できない追加機能を提供するために、外部の OIDC アイデンティティープロバイダーを ROSA with HCP クラスターに直接統合できます。

重要

既存の ROSA クラスターを Hosted Control Plane アーキテクチャーにアップグレードまたは変換することはできないため、ROSA with HCP の機能を使用するには新しいクラスターを作成する必要があります。また、外部認証プロバイダーを使用するように作成されたクラスターを、内部 OAuth2 サーバーを使用するように変換することもできません。新しいクラスターも作成する必要があります。

重要

現在、ROSA with HCP では 複数の AWS アカウント間での VPC の共有 はサポートされていません。別の AWS アカウントから共有されているサブネットに ROSA with HCP クラスターをインストールしないでください。詳細は、"Are multiple ROSA clusters in a single VPC supported?" を参照してください。

注記

ROSA with HCP クラスターは、Security Token Service (STS) 認証のみをサポートします。

関連資料

- ROSA CLI を使用して自動モードで ROSA with HCP の使用を開始する方法 については、AWS ドキュメントを参照してください。

5.1. ROSA WITH HCP の前提条件

ROSA with HCP クラスターを作成するには、次の手順を完了する必要があります。

- AWS の前提条件 を満たしている。
- 仮想プライベートクラウド (VPC) を設定している。
- アカウント全体のロール を作成している。
- OIDC 設定 を作成している。
- Operator ロール を作成している。

5.2. 外部認証プロバイダーを使用する ROSA WITH HCP クラスターの作成

外部認証サービスを使用するクラスターを作成するには、ROSA CLI で **--external-auth-providers-enabled** フラグを使用します。

注記

ROSA with HCP クラスターを作成する場合、デフォルトのマシン Classless Inter-Domain Routing (CIDR) は **10.0.0.0/16** です。これが VPC サブネットの CIDR 範囲に対応していない場合は、次のコマンドに **--machine-cidr <address_block>** を追加します。

手順

- **OIDC_ID**、**SUBNET_IDS**、および **OPERATOR_ROLES_PREFIX** 変数を使用して環境を準備した場合は、これらの変数をクラスターの作成時にも引き続き使用できます。たとえば、以下のコマンドを実行します。

```
$ rosa create cluster --hosted-cp --subnet-ids=$SUBNET_IDS \
  --oidc-config-id=$OIDC_ID --cluster-name=<cluster_name> \
  --operator-roles-prefix=$OPERATOR_ROLES_PREFIX \
  --external-auth-providers-enabled
```

- 環境変数を設定していない場合は、以下のコマンドを実行します。

```
$ rosa create cluster --cluster-name=<cluster_name> --sts --mode=auto \
   --hosted-cp --operator-roles-prefix <operator-role-prefix> \
   --oidc-config-id <ID-of-OIDC-configuration> \
   --external-auth-providers-enabled \
   --subnet-ids=<public-subnet-id>,<private-subnet-id>
```

検証

- 次のコマンドを実行して、クラスターの詳細で外部認証が有効になっていることを確認します。

```
$ rosa describe cluster --cluster=<cluster_name>
```

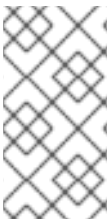
```
Name:                       rosa-ext-test
Display Name:               rosa-ext-test
ID:                         <cluster_id>
External ID:                <cluster_ext_id>
Control Plane:              ROSA Service Hosted
OpenShift Version:          4.17.0
Channel Group:              stable
DNS:                        <dns>
AWS Account:                <AWS_id>
AWS Billing Account:        <AWS_id>
API URL:                    <ocm_api>
Console URL:
Region:                     us-east-1
Availability:
 - Control Plane:           MultiAZ
 - Data Plane:              SingleAZ

Nodes:
 - Compute (desired):       2
 - Compute (current):       0
Network:
 - Type:                    OVNKubernetes
```

```
 - Service CIDR:          <service_cidr>
 - Machine CIDR:          <machine_cidr>
 - Pod CIDR:              <pod_cidr>
 - Host Prefix:           /23
 - Subnets:               <subnet_ids>
EC2 Metadata Http Tokens:   optional
Role (STS) ARN:             arn:aws:iam::<AWS_id>:role/<account_roles_prefix>-HCP-ROSA-
Installer-Role
Support Role ARN:           arn:aws:iam::<AWS_id>:role/<account_roles_prefix>-HCP-ROSA-
Support-Role
Instance IAM Roles:
 - Worker:                  arn:aws:iam::<AWS_id>:role/<account_roles_prefix>-HCP-ROSA-
Worker-Role
Operator IAM Roles:
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-openshift-cloud-network-config-
controller-clo
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-kube-system-capa-controller-
manager
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-kube-system-control-plane-operator
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-kube-system-kms-provider
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-kube-system-kube-controller-
manager
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-openshift-image-registry-installer-
cloud-cred
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-openshift-ingress-operator-cloud-
credentials
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-openshift-cluster-csi-drivers-ebs-
cloud-crede
Managed Policies:           Yes
State:                      ready
Private:                    No
Created:                    Mar 29 2024 14:25:52 UTC
User Workload Monitoring:   Enabled
Details Page:               https://<url>
OIDC Endpoint URL:          https://<endpoint> (Managed)
Audit Log Forwarding:       Disabled
External Authentication:    Enabled (1)
```

(1) **External Authentication** フラグが有効になり、外部認証プロバイダーを作成できるようになりました。

5.3. 外部認証プロバイダーの作成

外部認証プロバイダーのオプションを有効にして ROSA with HCP クラスターを作成した後、ROSA CLI を使用してプロバイダーを作成する必要があります。



注記

ROSA CLI の **rosa create|delete|list idp[s]** コマンドと同様に、**rosa create external-auth-provider** を使用して作成した既存のアイデンティティープロバイダーを編集できません。代わりに、外部認証プロバイダーを削除して、新しい認証プロバイダーを作成する必要があります。

次の表は、外部認証プロバイダーを作成するときに使用できる CLI フラグを示しています。

CLI フラグ	説明
--cluster	クラスターの名前または ID。
--name	外部認証プロバイダーを参照するために使用される名前。
--console-client-secret	この文字列は、アカウントをアプリケーションに関連付けるために使用されるクライアントシークレット。クライアントシークレットを含めない場合、このコマンドはパブリック OIDC OAuthClient を使用します。
--issuer-audiences	これは、トークンオーディエンスのコンマ区切りリストです。
--issuer-url	トークン発行者の URL。
--claim-mapping-username-claim	クラスターアイデンティティーのユーザー名を構築するために使用されるクレームの名前。
--claim-mapping-groups-claim	クラスターアイデンティティーのグループー名を構築するために使用されるクレームの名前。

手順

- 対話型コマンドインターフェイスを使用するには、次のコマンドを実行します。

```
$ rosa create external-auth-provider -c <cluster_name>
```

```
I: Enabling interactive mode
? Name: 1
? Issuer audiences: 2
? The serving url of the token issuer: 3
? CA file path (optional): 4
? Claim mapping username: 5
? Claim mapping groups: 6
? Claim validation rule (optional): 7
? Console client id (optional): 8
```

1. 外部認証プロバイダーの名前。この名前は、数字とダッシュが含まれる小文字である必要があります。
2. この認証プロバイダーがトークンを発行するオーディエンス ID。
3. トークンを提供する発行者の URL。
4. オプション: リクエストを行うときに使用する証明書ファイル。
5. **メール** の使用など、クラスターアイデンティティーのユーザー名を構築するために使用されるクレームの名前。

6 **グループ** の使用など、ID トークンをクラスターアイデンティティーに変換する方法。

7 オプション: ユーザーを認証するトークン要求を検証するのに役立つルール。このフィールドは、**:<required_value>** の形式にする必要があります。

8 オプション: アプリ登録でコンソールに使用するアプリケーションまたはクライアント ID。

- 次のコマンドを使用して、外部認証プロバイダーを作成するために必要な ID を含めることができます。

```
rosa create external-auth-provider --cluster=<cluster_id> \
  --name=<provider_name> --issuer-url=<issuing_url> \
  --issuer-audiences=<audience_id> \
  --claim-mapping-username-claim=email \
  --claim-mapping-groups-claim=groups \
  --console-client-id=<client_id_for_app_registration> \
  --console-client-secret=<client_secret>
```

出力例

```
I: Successfully created an external authentication provider for cluster '<cluster_id>'
```

検証

- 外部認証プロバイダーを確認するには、次のいずれかのオプションを実行します。
  - 次のコマンドを使用して、指定されたクラスターの外部認証設定をリスト表示します。

```
$ rosa list external-auth-provider -c <cluster_name>
```

出力例

次の例は、設定された Microsoft Entra ID 外部認証プロバイダーを示しています。

```
NAME       ISSUER URL
m-entra-id  https://login.microsoftonline.com/<group_id>/v2.0
```

  - 次のコマンドを使用して、指定されたクラスターの外部認証設定を表示します。

```
$ rosa describe external-auth-provider \
    -c <cluster_name> --name <name_of_external_authentication>
```

出力例

```
ID:                         ms-entra-id
Cluster ID:                 <cluster_id>
Issuer audiences:
                          - <audience_id>
Issuer Url:                 https://login.microsoftonline.com/<group_id>/v2.0
Claim mappings group:       groups
Claim mappings username:    email
```

関連情報

- IDP 用に Entra ID を設定する方法の詳細は、Azure ドキュメントの What is Microsoft Entra ID? または Microsoft Entra ID (旧称 Azure Active Directory) のアイデンティティープロバイダーとしての設定 ドキュメントのチュートリアルセクションを参照してください。

5.4. ROSA WITH HCP の BREAK GLASS 認証情報の作成

ROSA with HCP クラスターの所有者は、break glass 認証情報を使用して一時的な管理クライアント認証情報を作成し、カスタム OpenID Connect (OIDC) トークン発行者を指定して設定されたクラスターにアクセスできます。Break Glass 認証情報を作成すると、新しい cluster-admin **kubeconfig** ファイルが生成されます。**kubeconfig** ファイルには、CLI がクライアントを正しいクラスターと API サーバーに接続するために使用するクラスターに関する情報が含まれています。新しく生成された **kubeconfig** ファイルを使用して、ROSA with HCP クラスターへのアクセスを許可できます。

前提条件

- 外部認証を有効にした ROSA with HCP クラスターが作成されている。詳細は、**外部認証プロバイダーを使用する HCP クラスターを使用した ROSA with HCP の作成** を参照してください。
- 外部認証プロバイダーが作成されている。詳細は、**外部認証プロバイダーの作成** を参照してください。
- **cluster admin** 権限が割り当てられたアカウントがある。

手順

1. 次のいずれかのコマンドを使用して、Break Glass 認証情報を作成します。
   - 対話型コマンドインターフェイスを使用してカスタム設定を対話的に指定し、ブレークグラス認証情報を作成するには、次のコマンドを実行します。

     ```
     $ rosa create break-glass-credential -c <cluster_name> -i (1)
     ```

     (1) <cluster_name> は、クラスターの名前に置き換えます。

     このコマンドは、対話型 CLI プロセスを開始します。

     出力例

     ```
     I: Enabling interactive mode
     ? Username (optional): (1)
     ? Expiration duration (optional): (2)
     I: Successfully created a break glass credential for cluster 'ac-hcp-test'.
     ```

     (1) 空白のままにすると、**username** の値は無作為に生成されたユーザー名の値になります。

     (2) break glass 認証情報の最小有効期間は 10 分、最大有効期間は 24 時間です。空白のままにすると、有効期限の値はデフォルトで 24 時間になります。

   - 指定された値を使用して、**mycluster** というクラスターの Break Glass 認証情報を作成するには以下を実行します。

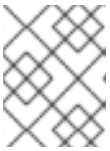
```
$ rosa create break-glass-credential -c mycluster --username test-username --expiration
1h
```

2. 次のコマンドを実行して、**mycluster** というクラスターで使用可能な Break Glass 認証情報 ID、ステータス、および関連ユーザーをリスト表示します。

```
$ rosa list break-glass-credential -c mycluster
```

出力例

```
ID                           USERNAME    STATUS
2a7jli9n4phe6c02ul7ti91djtv2o51d  test-user   issued
```



注記

コマンドに **-o json** 引数を追加することで、JSON 出力で認証情報を表示することもできます。

3. break glass 認証情報のステータスを表示するには、<break_glass_credential_id> をブレークグラス認証情報 ID に置き換えて、次のコマンドを実行します。

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c <cluster_name>
```

出力例

```
ID:                          2a7jli9n4phe6c02ul7ti91djtv2o51d
Username:                         test-user
Expire at:                    Dec 28 2026 10:23:05 EDT
Status:                      issued
```

Status フィールドで使用可能な値のリストは次のとおりです。

- **issued** break glass 認証情報が発行され、使用できる状態になりました。
- **expired** ブレークグラス認証情報の有効期限が切れているため、使用できなくなりました。
- **failed** ブレークグラス認証情報の作成に失敗しました。この場合、失敗の詳細を示すサービスログが送信されます。サービスログの詳細は、**Red Hat OpenShift Service on AWS クラスターのサービスログへのアクセス** を参照してください。Red Hat サポートに問い合わせる手順については、**サポート** を参照してください。
- **awaiting_revocation** break glass 認証情報は現在取り消されているため、使用できません。
- **revoked** break glass 認証情報は取り消されており、使用できなくなりました。

4. **kubeconfig** を取得するには、次のコマンドを実行します。
   - **kubeconfig** ディレクトリーを作成します。

```
$ mkdir ~/kubeconfigs
```

- 新しく生成された **kubeconfig** ファイルをエクスポートします。<cluster_name> はクラスターの名前に置き換えます。

```
$ export CLUSTER_NAME=<cluster_name> && export
KUBECONFIG=~/kubeconfigs/break-glass-${CLUSTER_NAME}.kubeconfig
```

- **kubeconfig** を表示します。

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c mycluster --
kubeconfig
```

出力例

```
apiVersion: v1
clusters:
- cluster:
    server: <server_url>
  name: cluster
contexts:
- context:
    cluster: cluster
    namespace: default
    user: test-username
  name: admin
current-context: admin
kind: Config
preferences: {}
users:
- name: test-user
  user:
    client-certificate-data: <client-certificate-data> (1)
    client-key-data: <client-key-data> (2)
```

(1) クライアント証明書には、Kubernetes 証明局 (CA) によって署名されたユーザーの証明書が含まれています。

(2) client-key には、クライアント証明書に署名したキーが含まれます。

5. オプション: **kubeconfig** を保存するには、次のコマンドを実行します。

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c mycluster --
kubeconfig > $KUBECONFIG
```

関連情報

- 外部認証を有効にした ROSA with HCP クラスターの作成の詳細は、外部認証プロバイダーを使用する ROSA with HCP クラスターの作成 を参照してください。

5.5. BREAK GLASS 認証情報を使用した ROSA WITH HCP クラスターへのアクセス

Break Glass 認証情報から新しい **kubeconfig** を使用して、ROSA with HCP クラスターへの一時的な管理者アクセス権を取得します。

前提条件

- 外部認証が有効になっている ROSA with HCP クラスターにアクセスできる。詳細は、**外部認証プロバイダーを使用する ROSA with HCP クラスターの作成** を参照してください。
- **oc** および **kubectl** CLI がインストールされている。
- 新しい **kubeconfig** が設定されている。詳細は、**ROSA with HCP クラスターの Break Glass 認証情報の作成** を参照してください。

手順

1. クラスターの詳細にアクセスします。

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c <cluster_name>  --
kubeconfig > $KUBECONFIG
```

2. クラスターからノードを一覧表示します。

```
$ oc get nodes
```

出力例

```
NAME                         STATUS   ROLES   AGE   VERSION
ip-10-0-0-27.ec2.internal   Ready    worker  8m    v1.28.7+f1b5f6c
ip-10-0-0-67.ec2.internal   Ready    worker  9m    v1.28.7+f1b5f6c
```

3. 適切な認証情報があることを確認します。

```
$ kubectl auth whoami
```

出力例

```
ATTRIBUTE    VALUE
Username     system:customer-break-glass:test-user
Groups       [system:masters system:authenticated]
```

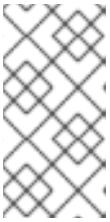
4. 外部 OIDC プロバイダーで定義されたグループに **ClusterRoleBinding** を適用します。**ClusterRoleBinding** は、Microsoft Entra ID で作成された **rosa-hcp-admins** グループを ROSA with HCP クラスター内のグループにマップします。

```
$ oc apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: rosa-hcp-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
```

```
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: f715c264-ab90-45d5-8a29-2e91a609a895
EOF
```

出力例

```
clusterrolebinding.rbac.authorization.k8s.io/rosa-hcp-admins created
```



注記

ClusterRoleBinding が適用されると、ROSA with HCP クラスターが設定され、**rosa** CLI と Red Hat Hybrid Cloud Console が外部 OpenID Connect (OIDC) プロバイダーを通じて認証されます。ロールの割り当てとクラスターでのアプリケーションのデプロイを開始できるようになりました。

関連情報

- クラスターロールバインディングの詳細は、RBAC を使用したパーミッションの定義および適用 を参照してください。

5.6. ROSA WITH HCP クラスターの BREAK GLASS 認証情報の取り消し

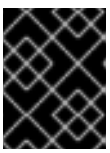
revoke break-glass-credentials コマンドを使用すると、プロビジョニングした Break Glass 認証情報へのアクセスをいつでも取り消すことができます。

前提条件

- break glass 認証情報が作成されている。
- クラスターの所有者である。

手順

- 次のコマンドを実行して、ROSA with HCP クラスターの Break Glass 認証情報を取り消します。



重要

このコマンドを実行すると、クラスターに関連するすべての Break Glass 認証情報へのアクセスが取り消されます。

```
$ rosa revoke break-glass-credentials -c <cluster_name> 1
```

1 <cluster_name> は、クラスターの名前に置き換えます。

出力例

```
? Are you sure you want to revoke all the break glass credentials on cluster 'my-cluster'?: Yes
I: Successfully requested revocation for all break glass credentials from cluster 'my-cluster'
```

検証

- 失効処理には数分かかる場合があります。次のいずれかのコマンドを実行すると、クラスターの Break Glass 認証情報が取り消されたことを確認できます。
  - すべての Break Glass 認証情報をリスト表示し、それぞれのステータスを確認します。

```
$ rosa list break-glass-credential -c <cluster_name>
```

出力例

```
ID                            USERNAME    STATUS
2330dbs0n8m3chkkr25gkkcd8pnj3lk2  test-user   awaiting_revocation
```

  - 個々の認証情報をチェックしてステータスを確認することもできます。

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c <cluster_name>
```

出力例

```
ID:                         2330dbs0n8m3chkkr25gkkcd8pnj3lk2
Username:                       test-user
Expire at:                   Dec 28 2026 10:23:05 EDT
Status:                     issued
Revoked at:                     Dec 27 2026 15:30:33 EDT
```

5.7. 外部認証プロバイダーの削除

ROSA CLI を使用して外部認証プロバイダーを削除します。

手順

1. 次のコマンドを実行して、クラスター上の外部認証プロバイダーを表示します。

```
$ rosa list external-auth-provider -c <cluster_name>
```

出力例

```
NAME        ISSUER URL
entra-test  https://login.microsoftonline.com/<group_id>/v2.0
```

2. 次のコマンドを実行して、外部認証プロバイダーを削除します。

```
$ rosa delete external-auth-provider <name_of_provider> -c <cluster_name>
```

出力例

```
? Are you sure you want to delete external authentication provider entra-test on cluster rosa-ext-test? Yes
I: Successfully deleted external authentication provider 'entra-test' from cluster 'rosa-ext-test'
```

検証

1. 次のコマンドを実行して、クラスター上の外部認証プロバイダーを照会します。

```
$ rosa list external-auth-provider -c <cluster_name>
```

出力例

```
E: there are no external authentication providers for this cluster
```

5.8. 関連情報

- オプションで Operator ロール名接頭辞を設定する方法の詳細は、カスタム Operator IAM ロール接頭辞について を参照してください。
- STS を使用する ROSA をインストールするための前提条件の詳細は、STS を使用する ROSA の AWS の前提条件 を参照してください。
- **auto** モードと **manual** モードを使用して必要な STS リソースを作成する方法の詳細は、自動デプロイメントモードと手動デプロイメントモードについて を参照してください。
- AWS IAM で OpenID Connect (OIDC) アイデンティティープロバイダーの使用に関する詳細は、AWS ドキュメントの Creating OpenID Connect (OIDC) identity providers を参照してください。
- ROSA クラスターのインストールのトラブルシューティングの詳細は、インストールのトラブルシューティング を参照してください。
- Red Hat サポートにサポートを依頼する手順は、Red Hat OpenShift Service on AWS のサポートを受ける を参照してください。

第6章 CNI プラグインなしの ROSA WITH HCP クラスター

Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane (HCP) クラスターを作成するときに、独自の Container Network Interface (CNI) プラグインを使用できます。CNI なしで ROSA with HCP クラスターを作成し、クラスターの作成後に独自の CNI プラグインをインストールできます。

重要

独自の CNI を使用する場合、CNI プラグインのサポートの責任は、選択した CNI ベンダーとの連携のもと、お客様が負うことになります。

ROSA with HCP のデフォルトのプラグインは、OVN-Kubernetes ネットワークプラグイン です。このプラグインは、Red Hat がサポートする ROSA with HCP 用の唯一の CNI プラグインです。

ROSA with HCP クラスターに独自の CNI を使用する場合は、クラスターを作成する前にプラグインベンダーから商用サポートを受けることを強く推奨します。Red Hat サポートは、独自の CNI を使用することを選択したお客様に、Pod 間トラフィックなどの CNI 関連の問題に関するサポートを提供できません。CNI 以外のすべての問題については、Red Hat は引き続きサポートを提供します。Red Hat からの CNI 関連のサポートが必要な場合は、デフォルトの OVN-Kubernetes ネットワークプラグインを使用してクラスターをインストールする必要があります。詳細は、責任マトリックス を参照してください。

6.1. CNI プラグインなしで ROSA WITH HCP クラスターを作成する

6.1.1. 前提条件

- AWS の前提条件 を満たしていることを確認する。
- Virtual Private Cloud (VPC) が設定されていることを確認する。

6.1.2. アカウント全体の STS ロールおよびポリシーの作成

Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) を使用して、Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane クラスターを作成する前に、Operator ポリシーを含む、必要なアカウント全体のロールとポリシーを作成します。

注記

ROSA with HCP クラスターには、AWS 管理ポリシーがアタッチされたアカウントと Operator ロールが必要です。顧客管理のポリシーはサポートされていません。ROSA with HCP クラスターの AWS 管理ポリシーの詳細は、AWS managed policies for ROSA account roles を参照してください。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。
- 利用可能な AWS サービスクォータがある。
- AWS コンソールで ROSA サービスを有効にしている。
- インストールホストに、最新の ROSA CLI (**rosa**) をインストールして設定している。
- ROSA CLI を使用して Red Hat アカウントにログインしている。

手順

1. AWS アカウントに存在しない場合は、次のコマンドを実行して、必要なアカウント全体の STS ロールを作成し、ポリシーをアタッチします。

```
$ rosa create account-roles --hosted-cp
```

2. オプション: 次のコマンドを実行して、接頭辞を環境変数として設定します。

```
$ export ACCOUNT_ROLES_PREFIX=<account_role_prefix>
```

- 次のコマンドを実行して、変数の値を表示します。

```
$ echo $ACCOUNT_ROLES_PREFIX
```

出力例

```
ManagedOpenShift
```

ROSA の AWS 管理 IAM ポリシーの詳細は、AWS managed IAM policies for ROSA を参照してください。

6.1.3. OpenID Connect 設定の作成

ROSA with HCP クラスターを使用する場合は、クラスターを作成する前に OpenID Connect (OIDC) 設定を作成する必要があります。この設定は、OpenShift Cluster Manager で使用するために登録されています。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。
- Red Hat OpenShift Service on AWS の AWS 前提条件を完了している。
- インストールホストに、最新の Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールして設定している。

手順

1. AWS リソースと一緒に OIDC 設定を作成するには、次のコマンドを実行します。

```
$ rosa create oidc-config --mode=auto --yes
```

このコマンドは次の情報を返します。

出力例

```
? Would you like to create a Managed (Red Hat hosted) OIDC Configuration Yes
I: Setting up managed OIDC configuration
I: To create Operator Roles for this OIDC Configuration, run the following command and
remember to replace <user-defined> with a prefix of your choice:
 rosa create operator-roles --prefix <user-defined> --oidc-config-id 13cdr6b
If you are going to create a Hosted Control Plane cluster please include '--hosted-cp'
```

```
I: Creating OIDC provider using 'arn:aws:iam::4540112244:user/userName'
? Create the OIDC provider? Yes
I: Created OIDC provider with ARN 'arn:aws:iam::4540112244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/13cdr6b'
```

クラスターを作成するときは、OIDC 設定 ID を指定する必要があります。CLI 出力では、**--mode auto** のこの値が提供されます。それ以外の場合は、**--mode manual** の **aws** CLI 出力に基づいてこれらの値を決定する必要があります。

2. オプション: OIDC 設定 ID を変数として保存して、後で使用できます。次のコマンドを実行して変数を保存します。

```
$ export OIDC_ID=<oidc_config_id>
```
1

1 上記の出力例では、OIDC 設定 ID は 13cdr6b です。

- 次のコマンドを実行して、変数の値を表示します。

```
$ echo $OIDC_ID
```

出力例

```
13cdr6b
```

検証

- ユーザー組織に関連付けられているクラスターで使用できる可能な OIDC 設定をリストできます。以下のコマンドを実行します。

```
$ rosa list oidc-config
```

出力例

```
ID                               MANAGED  ISSUER URL
SECRET ARN
2330dbs0n8m3chkkr25gkkcd8pnj3lk2  true
https://dvbwgdztaeq9o.cloudfront.net/2330dbs0n8m3chkkr25gkkcd8pnj3lk2
233hvnrjoqu14jltk6lhbhf2tj11f8un  false    https://oidc-r7u1.s3.us-east-1.amazonaws.com
aws:secretsmanager:us-east-1:242819244:secret:rosa-private-key-oidc-r7u1-tM3MDN
```

6.1.4. Operator のロールとポリシーの作成

ROSA with HCP クラスターを使用する場合は、Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane (HCP) デプロイメントに必要な Operator IAM ロールを作成する必要があります。クラスター Operator は、Operator のロールを使用して、バックエンドストレージ、クラウドプロバイダーの認証情報、クラスターへの外部アクセスの管理など、クラスター操作を実行するために必要な一時的なアクセス許可を取得します。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。

- インストールホストに、最新の Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールして設定している。
- アカウント全体の AWS ロールを作成している。

手順

1. 次のコマンドを使用して、接頭辞名を環境変数に設定します。

```
$ export OPERATOR_ROLES_PREFIX=<prefix_name>
```

2. Operator ロールを作成するには、次のコマンドを実行します。

```
$ rosa create operator-roles --hosted-cp --prefix=$OPERATOR_ROLES_PREFIX --oidc-config-id=$OIDC_ID --installer-role-arn arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role
```

次の内訳は、Operator ロール作成のオプションを示しています。

```
$ rosa create operator-roles --hosted-cp
 --prefix=$OPERATOR_ROLES_PREFIX (1)
 --oidc-config-id=$OIDC_ID (2)
 --installer-role-arn
arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role (3)
```

(1) これらの Operator ロールを作成するときは、接頭辞を指定する必要があります。そうしないとエラーが発生します。演算子接頭辞は、このセクションの関連情報を参照してください。

(2) この値は、ROSA with HCP クラスター用に作成した OIDC 設定 ID です。

(3) この値は、ROSA アカウントロールの作成時に作成したインストーラーロールの ARN です。

ROSA with HCP クラスター用の正しいロールを作成するには、**--hosted-cp** パラメーターを含める必要があります。このコマンドは次の情報を返します。

出力例

```
? Role creation mode: auto
? Operator roles prefix: <pre-filled_prefix> (1)
? OIDC Configuration ID: 23soa2bgvpek9kmes9s7os0a39i13qm4 | https://dvbwgdztaeq9o.cloudfront.net/23soa2bgvpek9kmes9s7os0a39i13qm4 (2)
? Create hosted control plane operator roles: Yes
W: More than one Installer role found
? Installer role ARN: arn:aws:iam::4540112244:role/<prefix>-HCP-ROSA-Installer-Role
? Permissions boundary ARN (optional):
I: Reusable OIDC Configuration detected. Validating trusted relationships to operator roles:
I: Creating roles using 'arn:aws:iam::4540112244:user/<userName>'
I: Created role '<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials' with ARN 'arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials'
```

```
I: Created role '<prefix>-openshift-cloud-network-config-controller-cloud-credenti' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-controller-cloud-
credenti'
I: Created role '<prefix>-kube-system-kube-controller-manager' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager'
I: Created role '<prefix>-kube-system-capa-controller-manager' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager'
I: Created role '<prefix>-kube-system-control-plane-operator' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator'
I: Created role '<prefix>-kube-system-kms-provider' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider'
I: Created role '<prefix>-openshift-image-registry-installer-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-credentials'
I: Created role '<prefix>-openshift-ingress-operator-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials'
I: To create a cluster with these roles, run the following command:
 rosa create cluster --sts --oidc-config-id 23soa2bgvpek9kmes9s7os0a39i13qm4 --operator-
roles-prefix <prefix> --hosted-cp
```

1. このフィールドには、最初の作成コマンドで設定した接頭辞が事前に入力されます。
2. このフィールドでは、ROSA with HCP クラスター用に作成した OIDC 設定を選択する必要があります。

これで、Operator ロールが作成され、ROSA with HCP クラスターの作成に使用できるようになりました。

検証

- ROSA アカウントに関連付けられている Operator ロールをリスト表示できます。以下のコマンドを実行します。

```
$ rosa list operator-roles
```

出力例

```
I: Fetching operator roles
ROLE PREFIX  AMOUNT IN BUNDLE
<prefix>      8
? Would you like to detail a specific prefix Yes 1
? Operator Role Prefix: <prefix>
ROLE NAME                                          ROLE ARN
VERSION  MANAGED
<prefix>-kube-system-capa-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager
4.13     No
<prefix>-kube-system-control-plane-operator
arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator
4.13     No
<prefix>-kube-system-kms-provider
arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider                    4.13
No
<prefix>-kube-system-kube-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager
```

```
4.13     No
<prefix>-openshift-cloud-network-config-controller-cloud-credenti
arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-controller-cloud-
credenti  4.13     No
<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
4.13     No
<prefix>-openshift-image-registry-installer-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-credentials
4.13     No
<prefix>-openshift-ingress-operator-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials
4.13     No
```

1. コマンドを実行すると、AWS アカウントに関連付けられているすべての接頭辞が表示され、この接頭辞に関連付けられているロールの数が記録されます。これらのロールとその詳細をすべて表示する必要がある場合は、詳細プロンプトで "Yes" と入力すると、これらのロールが詳細とともにリストされます。

関連情報

- オペレーター接頭辞については、カスタム Operator IAM ロール接頭辞 を参照してください。

6.2. クラスターの作成

Red Hat OpenShift Service on AWS (ROSA) コマンドラインインターフェイス (CLI) **rosa** を使用してクラスターを作成する場合、オプションのフラグ **--no-cni** を追加すると、CNI プラグインなしでクラスターを作成できます。

前提条件

- ROSA with HCP の AWS の前提条件を完了している。
- 利用可能な AWS サービスクォータがある。
- AWS コンソールで ROSA サービスを有効にしている。
- インストールホストに、最新の ROSA CLI (**rosa**) をインストールして設定している。**rosa version** を実行して、現在インストールされている ROSA CLI のバージョンを確認します。新しいバージョンが利用可能な場合、CLI はこのアップグレードをダウンロードするためのリンクを提供します。
- ROSA CLI を使用して Red Hat アカウントにログインしている。
- OIDC 設定が作成されている。
- AWS Elastic Load Balancing (ELB) サービスロールが AWS アカウントに存在することを確認している。

手順

1. 次のコマンドのいずれかを使用して、ROSA with HCP クラスターを作成できます。

注記

ROSA with HCP クラスターを作成する場合、デフォルトのマシン Classless Inter-Domain Routing (CIDR) は **10.0.0.0/16** です。これが VPC サブネットの CIDR 範囲に対応していない場合は、次のコマンドに **--machine-cidr <address_block>** を追加します。Red Hat OpenShift Service on AWS のデフォルト CIDR 範囲の詳細は CIDR 範囲の定義 を参照してください。

- 単一の初期マシンプール、パブリックに利用可能な API、およびパブリックに利用可能な Ingress を備え、CNI プラグインのないクラスターを作成するには、次のコマンドを実行します。

```
$ rosa create cluster --cluster-name=<cluster_name> \
    --sts --mode=auto --hosted-cp --operator-roles-prefix <operator-role-prefix> \
    --oidc-config-id <ID-of-OIDC-configuration> --subnet-ids=<public-subnet-id>,<private-subnet-id> --no-cni
```

- 単一の初期マシンプール、プライベートに利用可能な API、およびプライベートに利用可能な Ingress を備え、CNI プラグインのないクラスターを作成するには、次のコマンドを実行します。

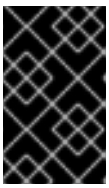
```
$ rosa create cluster --private --cluster-name=<cluster_name> \
    --sts --mode=auto --hosted-cp --subnet-ids=<private-subnet-id> --no-cni
```

- **OIDC_ID**、**SUBNET_IDS**、および **OPERATOR_ROLES_PREFIX** 変数を使用して環境を準備した場合は、CNI プラグインなしでクラスターを作成するときに、それらの変数を引き続き使用できます。たとえば、以下のコマンドを実行します。

```
$ rosa create cluster --hosted-cp --subnet-ids=$SUBNET_IDS --oidc-config-id=$OIDC_ID --cluster-name=<cluster_name> --operator-roles-prefix=$OPERATOR_ROLES_PREFIX --no-cni
```

2. 次のコマンドを実行して、クラスターのステータスを確認します。

```
$ rosa describe cluster --cluster=<cluster_name>
```



重要

クラスターが **ready** 状態に達してから初めてログインする場合、独自の CNI プラグインをインストールするまで、ノードは **not ready** 状態のままです。CNI のインストール後、ノードは **ready** に変わります。

以下の **State** フィールドの変更は、クラスターインストールの進捗として出力に表示されます。

- **pending (Preparing account)**
- **installing (DNS setup in progress)**
- **installing**
- **ready**

注記

インストールが失敗した場合や、**State** フィールドが 10 分以上 **ready** に変わらない場合は、インストールのトラブルシューティングのドキュメントで詳細を確認してください。詳細は、**インストールのトラブルシューティング**を参照してください。Red Hat サポートにサポートを依頼する手順は、**Red Hat OpenShift Service on AWS のサポートを受ける**を参照してください。

3. Red Hat OpenShift Service on AWS インストールプログラムのログを監視して、クラスター作成の進行状況を追跡します。ログを確認するには、次のコマンドを実行します。

```
$ rosa logs install --cluster=<cluster_name> --watch 1
```

1 オプション: インストールの進行中に新しいログメッセージを監視するには、**--watch** 引数を使用します。

6.2.1. CNI プラグインがないクラスターの予想される動作

ROSA with HCP クラスターのインストールが完了しても、CNI プラグインがないとクラスターは動作しません。ノードが準備ができていないため、ワークロードをデプロイできません。たとえば、Red Hat OpenShift Service on AWS クラスターの Web コンソールを利用できないため、クラスターにログインするには OpenShift CLI (**oc**) を使用する必要があります。さらに、HAProxy ベースの Ingress Controller、イメージレジストリー、Prometheus ベースのモニタリングスタックなど、その他の OpenShift コンポーネントが実行されていません。これは、CNI プロバイダーをインストールするまでの予想される動作です。

6.3. 次のステップ

- CNI プラグインをインストールします。その後、ノードが **not ready** 状態から **ready** 状態に変わります。
- ROSA クラスターへのアクセス ドキュメントを使用して、ROSA クラスターにアクセスします。

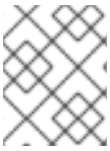
第7章 ROSA WITH HCP クラスターの削除

Red Hat OpenShift Service on AWS (ROSA) with hosted control planes (HCP) クラスターを削除する場合は、Red Hat OpenShift Cluster Manager または ROSA コマンドラインインターフェイス (CLI) (**rosa**) のいずれかを使用できます。クラスターを削除した後、クラスターで使用されている AWS Identity and Access Management (IAM) リソースを削除することもできます。

7.1. ROSA WITH HCP クラスターとクラスター固有の IAM リソースの削除

ROSA コマンドラインインターフェイス (CLI) (**rosa**) または Red Hat OpenShift Cluster Manager を使用して、ROSA with HCP クラスターを削除できます。

クラスターを削除した後、ROSA CLI を使用して、AWS アカウント内のクラスター固有のアイデンティティーおよびアクセス管理 (IAM) リソースを消去できます。クラスター固有のリソースには、Operator ロールと OpenID Connect (OIDC) プロバイダーが含まれます。



注記

IAM リソースは、クラスターの削除およびクリーンアップのプロセスで使用されるため、クラスターの削除は、IAM リソースを削除する前に完了する必要があります。

アドオンがインストールされている場合、クラスターの削除前にアドオンをアンインストールするため、削除により多くの時間がかかります。所要時間は、アドオンの数とサイズによって異なります。

前提条件

- ROSA with HCP クラスターをインストールした。
- インストールホストに、最新の ROSA CLI (**rosa**) をインストールして設定している。

手順

1. 次のコマンドを実行して、クラスター ID、クラスター固有の Operator ロールの Amazon リソース名 (ARN)、および OIDC プロバイダーのエンドポイント URL を取得します。

```
$ rosa describe cluster --cluster=<cluster_name>
```

出力例

```
Name:                  test_cluster
Domain Prefix:         test_cluster
Display Name:          test_cluster
ID:                    <cluster_id> 1
External ID:           <external_id>
Control Plane:         ROSA Service Hosted
OpenShift Version:     4.17.0
Channel Group:         stable
DNS:                   test_cluster.l3cn.p3.openshiftapps.com
AWS Account:           <AWS_id>
AWS Billing Account:   <AWS_id>
API URL:               https://api.test_cluster.l3cn.p3.openshiftapps.com:443
Console URL:
Region:                us-east-1
```

```
Availability:
 - Control Plane:          MultiAZ
 - Data Plane:             SingleAZ

Nodes:
 - Compute (desired):      2
 - Compute (current):      0
Network:
 - Type:                   OVNKubernetes
 - Service CIDR:           172.30.0.0/16
 - Machine CIDR:           10.0.0.0/16
 - Pod CIDR:               10.128.0.0/14
 - Host Prefix:            /23
 - Subnets:                <subnet_ids>
EC2 Metadata Http Tokens:  optional
Role (STS) ARN:            arn:aws:iam::<AWS_id>:role/test_cluster-HCP-ROSA-Installer-Role
Support Role ARN:          arn:aws:iam::<AWS_id>:role/test_cluster-HCP-ROSA-Support-
Role
Instance IAM Roles:
 - Worker:                 arn:aws:iam::<AWS_id>:role/test_cluster-HCP-ROSA-Worker-Role
Operator IAM Roles: 2
 - arn:aws:iam::<AWS_id>:role/test_cluster-openshift-cloud-network-config-controller-cloud-
crede
 - arn:aws:iam::<AWS_id>:role/test_cluster-openshift-image-registry-installer-cloud-
credentials
 - arn:aws:iam::<AWS_id>:role/test_cluster-openshift-ingress-operator-cloud-credentials
 - arn:aws:iam::<AWS_id>:role/test_cluster-kube-system-kube-controller-manager
 - arn:aws:iam::<AWS_id>:role/test_cluster-kube-system-capa-controller-manager
 - arn:aws:iam::<AWS_id>:role/test_cluster-kube-system-control-plane-operator
 - arn:aws:iam::<AWS_id>:role/hcpcluster-kube-system-kms-provider
 - arn:aws:iam::<AWS_id>:role/test_cluster-openshift-cluster-csi-drivers-ebs-cloud-
credentials
Managed Policies:          Yes
State:                     ready
Private:                   No
Created:                   Apr 16 2024 20:32:06 UTC
User Workload Monitoring:  Enabled
Details Page:              https://console.redhat.com/openshift/details/s/<cluster_id>
OIDC Endpoint URL:         https://oidc.op1.openshiftapps.com/<cluster_id> (Managed) 3
Audit Log Forwarding:      Disabled
External Authentication:   Disabled
```

1. クラスター ID をリスト表示します。
2. クラスター固有の Operator ロールの ARN を指定します。たとえば、サンプル出力では、Machine Config Operator に必要なロールの ARN は **arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-machine-api-aws-cloud-credentials** です。
3. クラスター固有の OIDC プロバイダーのエンドポイント URL が表示されます。

重要

クラスターを削除した後、ROSA CLI を使用してクラスター固有の STS リソースを削除するには、クラスター ID が必要になります。

2. OpenShift Cluster Manager または ROSA CLI (**rosa**) を使用してクラスターを削除します。
   - OpenShift Cluster Manager を使用してクラスターを削除するには、以下を実行します。
     a. OpenShift Cluster Manager に移動します。
     b. クラスターの横にあるオプションメニュー  をクリックし、**Delete cluster** を選択します。
     c. プロンプトにクラスターの名前を入力し、**Delete** をクリックします。
   - ROSA CLI を使用してクラスターを削除するには:
     a. 次のコマンドを実行します。**<cluster_name>** は、クラスターの名前または ID に置き換えます。

```
$ rosa delete cluster --cluster=<cluster_name> --watch
```

重要

Operator ロールと OIDC プロバイダーを削除する前に、クラスターの削除が完了するまで待つ必要があります。

3. 次のコマンドを実行して、クラスター固有の Operator IAM ロールを削除します。

```
$ rosa delete operator-roles --prefix <operator_role_prefix>
```

4. 次のコマンドを実行して OIDC プロバイダーを削除します。

```
$ rosa delete oidc-provider --oidc-config-id <oidc_config_id>
```

トラブルシューティング

- IAM ロールが欠落しているためにクラスターを削除できない場合は、削除できないクラスターの修復 を参照してください。
- 他の理由でクラスターを削除できない場合:
  - Hybrid Cloud Console で保留中のクラスターのアドオンがないことを確認します。
  - Amazon Web Console で、すべての AWS リソースと依存関係が削除されていることを確認します。

7.2. アカウント全体の IAM リソースを削除する

アカウント全体の AWS Identity and Access Management (IAM) リソースに依存する Red Hat OpenShift Service on AWS (ROSA) with Hosted Control Plane (HCP) クラスターを削除したら、アカウント全体のリソースを削除できます。

Red Hat OpenShift Cluster Manager を使用して HCP クラスターで ROSA をインストールする必要がなくなった場合は、OpenShift Cluster Manager とユーザー IAM ロールを削除することもできます。

重要

アカウント全体の IAM ロールおよびポリシーは、同じ AWS アカウントの他の ROSA with HCP クラスターによって使用される可能性があります。他のクラスターで必要でない場合にのみリソースを削除します。

OpenShift Cluster Manager を使用して同じ AWS アカウント内の他の Red Hat OpenShift Service on AWS クラスターをインストール、管理、および削除する場合は、OpenShift Cluster Manager とユーザーの IAM ロールが必要です。OpenShift Cluster Manager を使用してアカウントに Red Hat OpenShift Service on AWS クラスターをインストールする必要がなくなった場合にのみ、ロールを削除してください。削除前にこれらのロールが削除された場合にクラスターを修復する方法は、**クラスターのデプロイメントのトラブルシューティング** の「削除できないクラスターの修復」を参照してください。

関連情報

- 削除できないクラスターの修復

7.2.1. アカウント全体の IAM ロールとポリシーの削除

このセクションでは、ROSA with HCP のデプロイ用に作成したアカウント全体の IAM ロールおよびポリシーを、アカウント全体の Operator ポリシーとともに削除する手順を説明します。アカウント全体の AWS アイデンティティーおよびアクセス管理 (IAM) ロールとポリシーは、それらに依存するすべての ROSA with HCP クラスターを削除した後にのみ削除できます。

重要

アカウント全体の IAM ロールとポリシーは、同じ AWS アカウント内の他の Red Hat OpenShift Service on AWS によって使用される可能性があります。他のクラスターで必要とされていない場合に限り、ロールだけを削除します。

前提条件

- 削除するアカウント全体の IAM ロールがある。
- インストールホストに、最新の ROSA CLI (**rosa**) をインストールして設定している。

手順

1. アカウント全体のロールを削除します。
   a. ROSA CLI (**rosa**) を使用して、AWS アカウントのアカウント全体のロールをリスト表示します。

```
$ rosa list account-roles
```

出力例

```
I: Fetching account roles
ROLE NAME                                ROLE TYPE      ROLE ARN
OPENSHIFT VERSION  AWS Managed
ManagedOpenShift-HCP-ROSA-Installer-Role  Installer      arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-HCP-ROSA-Installer-Role  4.17              Yes
ManagedOpenShift-HCP-ROSA-Support-Role    Support        arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-HCP-ROSA-Support-Role    4.17
Yes
ManagedOpenShift-HCP-ROSA-Worker-Role     Worker         arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-HCP-ROSA-Worker-Role     4.17
Yes
```

b. アカウント全体のロールを削除します。

```
$ rosa delete account-roles --prefix <prefix> --mode auto (1)
```

(1) その際、**--<prefix>** 引数を含める必要があります。**<prefix>** を削除するアカウント全体のロールの接頭辞に置き換えてください。アカウント全体のロールを作成したときにカスタム接頭辞を指定しなかった場合は、デフォルトの接頭辞である **ManagedOpenShift** を指定します。

重要

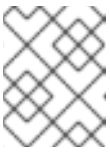
アカウント全体の IAM ロールは、同じ AWS アカウント内の他の ROSA クラスターによって使用される場合があります。他のクラスターで必要とされていない場合に限り、ロールだけを削除します。

出力例

```
W: There are no classic account roles to be deleted
I: Deleting hosted CP account roles
? Delete the account role 'delete-rosa-HCP-ROSA-Installer-Role'? Yes
I: Deleting account role 'delete-rosa-HCP-ROSA-Installer-Role'
? Delete the account role 'delete-rosa-HCP-ROSA-Support-Role'? Yes
I: Deleting account role 'delete-rosa-HCP-ROSA-Support-Role'
? Delete the account role 'delete-rosa-HCP-ROSA-Worker-Role'? Yes
I: Deleting account role 'delete-rosa-HCP-ROSA-Worker-Role'
I: Successfully deleted the hosted CP account roles
```

2. アカウント全体のインラインポリシーと Operator ポリシーを削除します。

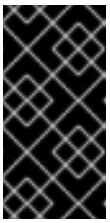
a. AWS IAM Console の **Policies** ページで、アカウント全体のロールとポリシーを作成したときに指定した接頭辞でポリシーのリストをフィルタリングします。



注記

アカウント全体のロールを作成したときにカスタム接頭辞を指定しなかった場合は、デフォルトの接頭辞である **ManagedOpenShift** を検索します。

b. AWS IAM Console を使用して、アカウント全体のインラインポリシーと Operator ポリシーを削除します。AWS IAM コンソールを使用して IAM ポリシーを削除する方法の詳細は、AWS ドキュメントの IAM ポリシーの削除 を参照してください。



重要

アカウント全体のインライン IAM ポリシーと Operator IAM ポリシーは、同じ AWS アカウント内の他の ROSA with HCP によって使用される可能性があります。他のクラスターで必要とされていない場合に限り、ロールだけを削除します。

関連情報

- STS を使用する ROSA クラスターの IAM リソースについて

7.2.2. OpenShift Cluster Manager およびユーザー IAM ロールのリンク解除と削除

Red Hat OpenShift Cluster Manager を使用して ROSA with HCP クラスターをインストールすると、OpenShift Cluster Manager と、Red Hat 組織にリンクするユーザーアイデンティティーおよびアクセス管理 (IAM) ロールも作成されます。クラスターを削除した後、ROSA CLI (**rosa**) を使用して、ロールのリンクを解除して削除できます。

重要

OpenShift Cluster Manager を使用して同じ AWS アカウントに他の ROSA クラスターをインストールおよび管理する場合は、OpenShift Cluster Manager とユーザー IAM ロールが必要です。OpenShift Cluster Manager を使用して ROSA with HCP クラスターをインストールする必要がなくなった場合にのみ、ロールを削除してください。

前提条件

- OpenShift Cluster Manager とユーザー IAM ロールを作成し、それらを Red Hat 組織にリンクしている。
- インストールホストに、最新の ROSA CLI (**rosa**) をインストールして設定している。
- Red Hat 組織で組織管理者権限がある。

手順

1. Red Hat 組織から OpenShift Cluster Manager IAM ロールのリンクを解除し、ロールを削除します。

   a. AWS アカウントで OpenShift Cluster Manager IAM ロールをリスト表示します。

```
$ rosa list ocm-roles
```

出力例

```
I: Fetching ocm roles
ROLE NAME                                   ROLE ARN
LINKED  ADMIN  AWS Managed
```

```
ManagedOpenShift-OCM-Role-<red_hat_organization_external_id>  arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-OCM-Role-
<red_hat_organization_external_id>  Yes      Yes     Yes
```

b. 上記のコマンドの出力で OpenShift Cluster Manager IAM ロールがリンク済みとしてリストされている場合は、次のコマンドを実行して、Red Hat 組織からロールのリンクを解除します。

```
$ rosa unlink ocm-role --role-arn <arn> 1
```

1 **<arn>** を OpenShift Cluster Manager IAM ロールの Amazon Resource Name (ARN) に置き換えます。ARN は、前のコマンドの出力で指定されます。上記の例では、ARN の形式は **arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-<red_hat_organization_external_id>** です。

出力例

```
I: Unlinking OCM role
? Unlink the 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-
<red_hat_organization_external_id>' role from organization '<red_hat_organization_id>'?
Yes
I: Successfully unlinked role-arn 'arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-OCM-Role-
<red_hat_organization_external_id>' from organization account
'<red_hat_organization_id>'
```

c. OpenShift Cluster Manager IAM のロールとポリシーを削除します。

```
$ rosa delete ocm-role --role-arn <arn>
```

出力例

```
I: Deleting OCM role
? OCM Role ARN: arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-
<red_hat_organization_external_id>
? Delete 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-
<red_hat_organization_external_id>' ocm role? Yes
? OCM role deletion mode: auto 1
I: Successfully deleted the OCM role
```

1 削除モードを指定します。**auto** モードを使用して、OpenShift Cluster Manager IAM ロールとポリシーを自動的に削除できます。**manual** モードでは、ROSA CLI はロールとポリシーを削除するために必要な **aws** コマンドを生成します。**manual** モードでは、**aws** コマンドを手動で実行する前に詳細を確認することができます。

2. Red Hat 組織からユーザー IAM ロールのリンクを解除し、ロールを削除します。

a. AWS アカウントのユーザー IAM ロールをリスト表示します。

```
$ rosa list user-roles
```

出力例

```
I: Fetching user roles
ROLE NAME                              ROLE ARN
LINKED
ManagedOpenShift-User-<ocm_user_name>-Role  arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-User-<ocm_user_name>-Role  Yes
```

b. 上記のコマンドの出力にユーザー IAM ロールがリンクされていると表示されている場合は、Red Hat 組織からロールのリンクを解除します。

```
$ rosa unlink user-role --role-arn <arn> (1)
```

(1) **<arn>** をユーザー IAM ロールの Amazon Resource Name (ARN) に置き換えます。ARN は、前のコマンドの出力で指定されます。前の例では、ARN の形式は **arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-<ocm_user_name>-Role** です。

出力例

```
I: Unlinking user role
? Unlink the 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-
<ocm_user_name>-Role' role from the current account '<ocm_user_account_id>'? Yes
I: Successfully unlinked role ARN 'arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-User-<ocm_user_name>-Role' from account
'<ocm_user_account_id>'
```

c. ユーザー IAM ロールを削除します。

```
$ rosa delete user-role --role-arn <arn>
```

出力例

```
I: Deleting user role
? User Role ARN: arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-
<ocm_user_name>-Role
? Delete the 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-
<ocm_user_name>-Role' role from the AWS account? Yes
? User role deletion mode: auto (1)
I: Successfully deleted the user role
```

(1) 削除モードを指定します。**auto** モードを使用して、ユーザー IAM ロールを自動的に削除できます。**manual** モードでは、ROSA CLI はロールを削除するために必要な **aws** コマンドを生成します。**manual** モードでは、**aws** コマンドを手動で実行する前に詳細を確認できます。