# Red Hat OpenShift Service on AWS 4

## ROSA Classic 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: 2024-04-08

# Red Hat OpenShift Service on AWS 4 ROSA Classic 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

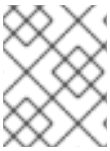


## 概要

このドキュメントでは、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。このドキュメントでは、クラスターへのアクセス方法、ID プロバイダーの設定方法、クラスターアクセスの取り消し方法、およびクラスターの削除方法についても詳しく説明します。

# 目次

# 第1章 デフォルトオプションを使用した STS を使用する ROSA クラスターの作成



**注記**

ROSA 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。

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、Red Hat OpenShift Service on AWS (ROSA) クラスターを迅速に作成します。Red Hat OpenShift Cluster Manager または ROSA CLI (**rosa**) を使用して、クラスターをデプロイすることができます。

このドキュメントの手順では、ROSA CLI (**rosa**) および OpenShift Cluster Manager 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 リソースをすぐに作成します。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。**manual** モードまたはカスタマイズを使用して ROSA クラスターをデプロイする手順については、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。

**次のステップ**

- AWS の前提条件 を満たしていることを確認してください。

**注記**

ROSA CLI 1.2.7 では、新しいクラスターの OIDC プロバイダーエンドポイント URL 形式に変更が導入されています。Red Hat OpenShift Service on AWS の OIDC プロバイダー URL は、リージョン別ではなくなりました。AWS CloudFront の実装により、アクセス速度と復元力が向上し、レイテンシーが短縮されます。

この変更は ROSA CLI 1.2.7 以降を使用して作成した新しいクラスターにのみ適用されるため、既存の OIDC プロバイダー設定の移行はサポートされていません。

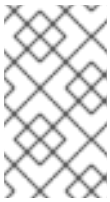
## 1.1. デフォルトのクラスター仕様の概要

デフォルトのインストールオプションを使用して、AWS 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について説明します。

**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**<br>• クラスター管理者ロールは作成されない |

| コンポーネント | デフォルトの仕様 |
| --- | --- |
| 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<br>• 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)<br>• ROSA CLI (**rosa**) を使用したインストールのデフォルトの AWS リージョン: **aws** CLI 設定によって定義されます。<br>• デフォルトの EC2 IMDS エンドポイント (v1 と v2 の両方) が有効になっています<br>• 可用性: データプレーンの単一ゾーン<br>• 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。<br>• 追加の etcd 暗号化が有効になっていません。<br>• 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)<br>• 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)<br>• 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)<br>• コンピュートノード数: 2<br>• 自動スケーリング: 無効<br>• 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<br>• クラスター全体のプロキシーは設定されていません。 |

| コンポーネント | デフォルトの仕様 |
| --- | --- |
| Classless Inter-Domain Routing (CIDR) の範囲 | • Machine CIDR: 10.0.0.0/16<br>• Service CIDR: 172.30.0.0/16<br>• Pod CIDR: 10.128.0.0/16<br>• 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**<br>  <br>**注記**<br>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。<br>• 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<br>• ノードドレインの 1 時間の猶予期間 |

## 1.2. AWS アカウントの関連付けについて

Red Hat Hybrid Cloud Console で Red Hat OpenShift Cluster Manager を使用して、AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する前に、AWS アカウントを Red Hat 組織に関連付ける必要があります。。次の IAM ロールを作成してリンクすることで、アカウントを関連付けることができます。

**OpenShift Cluster Manager ロール**

OpenShift Cluster Manager IAM ロールを作成し、Red Hat 組織にリンクします。
基本権限または管理権限を OpenShift Cluster Manager ロールに適用できます。基本パーミッションにより、OpenShift Cluster Manager を使用したクラスターのメンテナンスが可能になります。管理パーミッションにより、OpenShift Cluster Manager を使用して、クラスター固有の Operator ロールおよび OpenID Connect (OIDC) プロバイダーの自動デプロイが可能になります。

OpenShift Cluster Manager ロールで管理パーミッションを使用して、クラスターを迅速にデプロイできます。

**User role**

ユーザー IAM ロールを作成し、Red Hat ユーザーアカウントにリンクします。Red Hat ユーザーアカウントは、OpenShift Cluster Manager ロールにリンクされている Red Hat 組織に存在する必要があります。

ユーザーロールは、OpenShift Cluster Manager Hybrid Cloud Console を使用してクラスターと必要な STS リソースをインストールするときに、AWS Identity を確認するために Red Hat によって使用されます。

**関連情報**

- OpenShift Cluster Manager およびユーザー IAM ロールを作成してリンクする詳細な手順は、AWS アカウントを Red Hat 組織に関連付ける を参照してください。

## 1.3. PRIVATELINK ROSA クラスター以外の AMAZON VPC 要件

Amazon VPC を作成するには、以下が必要です。

- インターネットゲートウェイ
- NAT ゲートウェイ
- 必要なコンポーネントをインストールするためにインターネット接続のあるプライベートおよびパブリックサブネット。

Single-AZ クラスターには、少なくとも 1 つのプライベートサブネットとパブリックサブネットが必要で、Multi-AZ クラスターには 3 つ以上のプライベートサブネットとパブリックサブネットが必要です。

**関連情報**

- AWS クラスターに必要なデフォルトのコンポーネントの詳細は、AWS ドキュメントの Default VPCs を参照してください。
- AWS コンソールで VPC を作成する手順は、AWS ドキュメントの Create a VPC を参照してください。

## 1.4. OPENSHIFT CLUSTER MANAGER を使用してクラスターの迅速な作成

Red Hat OpenShift Cluster Manager を使用して AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する場合、デフォルトのオプションを選択してクラスターをすばやく作成できます。

OpenShift Cluster Manager を使用して STS を使用する ROSA クラスターをデプロイする前に、AWS アカウントを Red Hat 組織に関連付け、必要なアカウント全体の STS ロールおよびポリシーを作成する必要があります。

### 1.4.1. AWS アカウントを Red Hat 組織に関連付ける

Red Hat Hybrid Cloud Console で Red Hat OpenShift Cluster Manager を使用して、AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する前に、OpenShift Cluster Manager IAM ロールを作成し、そのロールを Red Hat 組織に関連付ける必要があります。次に、ユーザー IAM ロールを作成し、同じ Red Hat 組織内の Red Hat ユーザーアカウントにリンクします。

**前提条件**

- STS を使用する ROSA 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。

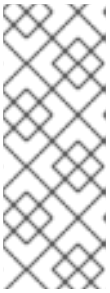
**注記**

ROSA クラスターを正常にインストールするには、最新バージョンの ROSA CLI を使用します。

- ROSA CLI を使用して Red Hat アカウントにログインしている。
- Red Hat 組織で組織管理者権限があります。

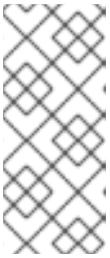
**手順**

1. OpenShift Cluster Manager ロールを作成し、Red Hat 組織にリンクします。



**注記**

OpenShift Cluster Manager Hybrid Cloud Console を使用してクラスター固有の Operator ロールと OpenID Connect (OIDC) プロバイダーの自動デプロイを有効にするには、ROSA クラスターの作成の **アカウントとロール** の手順で、**Admin OCM role** コマンドを選択して、ロールに管理権限を適用する必要があります。OpenShift Cluster Manager ロールの基本権限および管理権限の詳細については、**AWS アカウントの関連付けについて** を参照してください。



**注記**

OpenShift Cluster Manager Hybrid Cloud Console で ROSA クラスターを作成する **アカウントとロール** の手順で **Basic OCM role** コマンドを選択した場合は、手動モードを使用して ROSA クラスターをデプロイする必要があります。後のステップで、クラスター固有の Operator ロールと OpenID Connect (OIDC) プロバイダーを設定するように求められます。

```
$ rosa create ocm-role
```

ロールをすばやく作成してリンクするには、プロンプトでデフォルト値を選択します。

2. ユーザーロールを作成し、Red Hat ユーザーアカウントにリンクします。

```
$ rosa create user-role
```

ロールをすばやく作成してリンクするには、プロンプトでデフォルト値を選択します。

**注記**

Red Hat ユーザーアカウントは、OpenShift Cluster Manager ロールにリンクされている Red Hat 組織に存在する必要があります。

### 1.4.2. 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 Cluster Manager Hybrid Cloud Console を使用して AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) 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 STS ロールおよびポリシーを作成します。

**前提条件**

- STS を使用する ROSA 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。

**手順**

1. AWS アカウントで既存のロールとポリシーを確認します。

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

2. それらが AWS アカウントに存在しない場合は、アカウント全体の STS ロールとポリシーで必要なものを作成します。

```
$ rosa create account-roles
```

プロンプトでデフォルト値を選択して、ロールとポリシーをすばやく作成します。

### 1.4.3. OpenID Connect 設定の作成

Red Hat OpenShift Service on AWS 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) 設定を作成できます。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**

- 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**

- 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。

- 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
```

### 1.4.4. OpenShift Cluster Manager を使用してデフォルトオプションでクラスターを作成する

Red Hat Hybrid Cloud Console で Red Hat OpenShift Cluster Manager を使用して、AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する場

合、クラスターを迅速に作成するためのデフォルトのオプションを選択できます。管理 OpenShift Cluster Manager IAM ロールを使用して、クラスター固有の Operator ロールおよび OpenID Connect (OIDC) プロバイダーの自動デプロイメントを有効にすることもできます。

**前提条件**

- STS を使用する ROSA 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。
- 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。
- AWS アカウントを Red Hat 組織に関連付けました。アカウントを関連付けたときに、管理パーミッションを OpenShift Cluster Manager ロールに適用しました。詳細な手順については、**AWS アカウントを Red Hat 組織に関連付ける** を参照してください。
- 必要なアカウント全体の STS ロールとポリシーを作成しました。詳細な手順については、**アカウント全体の STS ロールおよびポリシーの作成** を参照してください。

**手順**

1. OpenShift Cluster Manager に移動し、**Create cluster**を選択します。
2. **Create an OpenShift cluster**ページの **Red Hat OpenShift Service on AWS (ROSA)**行で **Create cluster** を選択します。
3. AWS アカウント ID が **Associated AWS accounts** ドロップダウンメニューに表示されていること、およびインストーラー、サポート、ワーカー、およびコントロールプレーンのアカウントロールの Amazon Resource Names (ARN) が **Accounts and roles**ページに表示されていることを確認します。

**注記**

AWS アカウント ID が表示されていない場合は、AWS アカウントが Red Hat 組織に正常に関連付けられていることを確認してください。アカウントロール ARN が表示されていない場合は、必要なアカウント全体の STS ロールが AWS アカウントに存在することを確認してください。

4. **Next** をクリックします。
5. **Cluster details** ページで、**Cluster name** を入力します。残りのフィールドはデフォルト値のままにして、**Next** をクリックします。
6. クラスターをすばやくデプロイするには、**Cluster settings**、**Networking**、**Cluster roles and policies**、および **Cluster updates** ページのデフォルトのオプションをそのままにして、各ページで **Next** をクリックします。

7. **Review your ROSA cluster**確認ページで、選択内容の概要を確認し、**Create cluster** をクリックしてインストールを開始します。

**検証**

- クラスターの **概要** ページでインストールの進行状況を確認できます。同じページでインストールのログを表示できます。そのページの **Details** セクションの **Status** が **Ready** として表示されると、クラスターは準備が完了した状態になります。

**注記**

インストールが失敗するか、約 40 分経ってもクラスターの **状態** が **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。

## 1.5. CLI を使用してクラスターをすばやく作成する

Red Hat OpenShift Service on AWS (ROSA) の CLI (**rosa**) を使用して AWS Security Token Service (STS) を使用するクラスターを作成する場合、デフォルトのオプションを選択してクラスターをすばやく作成できます。

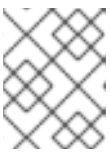
**前提条件**

- STS を使用する ROSA 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。
- 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. Operator ポリシーを含む、必要なアカウント全体のロールおよびポリシーを作成します。

```
$ rosa create account-roles --mode auto
```



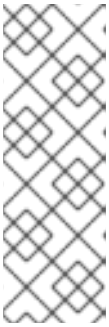
**注記**

**auto** モードを使用する場合は、任意で **-y** 引数を指定して対話式プロンプトを回避し、操作を自動的にチェックできます。

2. デフォルト設定を使用して、STS を使用するクラスターを作成します。デフォルトを使用する場合は、最新の安定した OpenShift バージョンがインストールされます。

```
$ rosa create cluster --cluster-name <cluster_name> \ 1
--sts --mode auto 2
```

1. **<cluster_name>** は、クラスター名に置き換えます。
2. **--mode auto** を指定すると、**rosa create cluster** コマンドは、クラスター固有の Operator IAM ロールおよび OIDC プロバイダーを自動的に作成します。Operator は、OIDC プロバイダーを利用して認証を行います。



**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。

3. クラスターのステータスを確認します。

```
$ rosa describe cluster --cluster <cluster_name|cluster_id>
```

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。

- **waiting (Waiting for OIDC configuration)**
- **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、約 40 分後に **State** フィールドが **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に関する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。

4. OpenShift インストーラーログを監視して、クラスター作成の進捗を追跡します。

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

1. **--watch** フラグを指定して、新規ログメッセージをインストールの進捗として監視します。この引数は任意です。

## 1.6. 次のステップ

- ROSA クラスターへのアクセス

## 1.7. 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。
- 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 カスタマイズを使用した STS を使用する ROSA クラスターの作成

カスタマイズを使用して、AWS Security Token Service (STS) で Red Hat OpenShift Service on AWS (ROSA) クラスターを作成します。Red Hat OpenShift Cluster Manager または ROSA CLI (**rosa**) を使用して、クラスターをデプロイすることができます。

このドキュメントの手順では、必要な AWS Identity and Access Management (IAM) リソースを作成するときに、**auto** モードと **manual** モードのどちらかを選択することもできます。

## 2.1. 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を理解する

AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターをインストールする場合、**auto** または **manual** モードを選択して、必要な AWS Identity and Access Management (IAM) リソースを作成できます。

**auto モード**

このモードでは、ROSA CLI (**rosa**) は必要な IAM ロールとポリシー、および AWS アカウントに OpenID Connect (OIDC) プロバイダーをすぐに作成します。

**手動 モード**

このモードでは、**rosa** は IAM リソースの作成に必要な **aws** コマンドを出力します。対応するポリシーの JSON ファイルも現在のディレクトリーに保存されます。**manual** モードを使用すると、生成された **aws** コマンドを手動で実行する前に確認できます。**manual** モードでは、コマンドを組織内の別の管理者またはグループに渡して、リソースを作成することもできます。

**重要**

**manual** モードを使用することを選択した場合、クラスターのインストールは、クラスター固有の Operator のロールと OIDC プロバイダーを手動で作成するまで待機します。リソースを作成した後、インストールが続行されます。詳細は、**OpenShift Cluster Manager を使用した Operator ロールと OIDC プロバイダーの作成**を参照してください。

STS で ROSA をインストールするために必要な AWS 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。

### 2.1.1. OpenShift Cluster Manager を使用した Operator ロールと OIDC プロバイダーの作成

Red Hat OpenShift Cluster Manager を使用してクラスターをインストールし、**manual** モードを使用して必要な AWS IAM Operator ロールと OIDC プロバイダーを作成することを選択した場合、リソースをインストールするために以下のいずれかの方法を選択するように求められます。組織のニーズに合ったリソース作成方法を選択できるようにするためのオプションが用意されています。

**AWS CLI (aws)**

この方法では、IAM リソースの作成に必要な **aws** コマンドとポリシーファイルを含むアーカイブファイルをダウンロードしてデプロイメントできます。ポリシーファイルを含むディレクトリーから提供された CLI コマンドを実行して、Operator ロールと OIDC プロバイダーを作成します。

**Red Hat OpenShift Service on AWS (ROSA) CLI (rosa)**

**rosa** を使用すると、提供されるコマンドを実行して、クラスターの Operator ロールと OIDC プロバイダーを作成できます。

**auto** モードを使用する場合、OpenShift Cluster Manager は、OpenShift Cluster Manager IAM ロールを通じて提供されるパーミッションを使用して、Operator ロールと OIDC プロバイダーを自動的に作成します。この機能を使用するには、ロールに管理者権限を適用する必要があります。

## 2.2. AWS アカウントの関連付けについて

Red Hat Hybrid Cloud Console で Red Hat OpenShift Cluster Manager を使用して、AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する前に、AWS アカウントを Red Hat 組織に関連付ける必要があります。。次の IAM ロールを作成してリンクすることで、アカウントを関連付けることができます。

**OpenShift Cluster Manager ロール**

OpenShift Cluster Manager IAM ロールを作成し、Red Hat 組織にリンクします。
基本権限または管理権限を OpenShift Cluster Manager ロールに適用できます。基本パーミッションにより、OpenShift Cluster Manager を使用したクラスターのメンテナンスが可能になります。管理パーミッションにより、OpenShift Cluster Manager を使用して、クラスター固有の Operator ロールおよび OpenID Connect (OIDC) プロバイダーの自動デプロイが可能になります。

OpenShift Cluster Manager ロールで管理パーミッションを使用して、クラスターを迅速にデプロイできます。

**User role**

ユーザー IAM ロールを作成し、Red Hat ユーザーアカウントにリンクします。Red Hat ユーザーアカウントは、OpenShift Cluster Manager ロールにリンクされている Red Hat 組織に存在する必要があります。
ユーザーロールは、OpenShift Cluster Manager Hybrid Cloud Console を使用してクラスターと必要な STS リソースをインストールするときに、AWS Identity を確認するために Red Hat によって使用されます。

**関連情報**

- OpenShift Cluster Manager とユーザー IAM ロールを作成してリンクする詳細な手順は、OpenShift Cluster Manager を使用してカスタマイズしたクラスターを作成する を参照してください。

## 2.3. IAM ロールとポリシーの ARN パスのカスタマイズ

AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターに必要な AWS IAM ロールとポリシーを作成するときに、カスタムの Amazon リソースネーム (ARN) パスを指定できます。これにより、組織のセキュリティー要件を満たすロールとポリシーの ARN パスを使用できます。

OCM ロール、ユーザーロール、およびアカウント全体のロールとポリシーを作成するときに、カスタム ARN パスを指定できます。

アカウント全体のロールとポリシーのセットを作成するときにカスタム ARN パスを定義すると、セット内のすべてのロールとポリシーに同じパスが適用されます。次の例は、アカウント全体のロールとポリシーのセットの ARN を示しています。この例では、ARN はカスタムパス **/test/path/dev/** とカスタムロール 接頭辞 **test-env** を使用します。

- **arn:aws:iam::<account_id>:role/test/path/dev/test-env-Worker-Role**
- **arn:aws:iam::<account_id>:role/test/path/dev/test-env-Support-Role**

- **arn:aws:iam::<account_id>:role/test/path/dev/test-env-Installer-Role**
- **arn:aws:iam::<account_id>:role/test/path/dev/test-env-ControlPlane-Role**
- **arn:aws:iam::<account_id>:policy/test/path/dev/test-env-Worker-Role-Policy**
- **arn:aws:iam::<account_id>:policy/test/path/dev/test-env-Support-Role-Policy**
- **arn:aws:iam::<account_id>:policy/test/path/dev/test-env-Installer-Role-Policy**
- **arn:aws:iam::<account_id>:policy/test/path/dev/test-env-ControlPlane-Role-Policy**

クラスター固有の Operator ロールを作成すると、関連するアカウント全体のインストーラーロールの ARN パスが自動的に検出され、Operator ロールに適用されます。

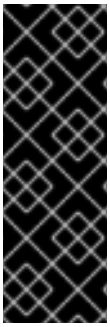
ARN パスの詳細は、AWS ドキュメントの Amazon リソースネーム (ARN) を参照してください。

**関連情報**

- Red Hat OpenShift Service on AWS クラスターを作成するときに IAM リソースのカスタム ARN パスを指定する手順については、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。

## 2.4. STS を使用する ROSA クラスターのサポートについての考慮事項

AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する方法でサポート対象なのは、この製品ドキュメントで説明されている手順を使用する方法です。



**重要**

ROSA CLI (**rosa**) で **manual** モードを使用し、STS リソースのインストールに必要な AWS Identity and Access Management (IAM) ポリシーファイルおよび **aws** コマンドを生成できます。

ファイルおよび **aws** コマンドは、レビュー目的でのみ生成され、いずれの方法でも変更しないでください。Red Hat は、変更したバージョンのポリシーファイルまたは **aws** コマンドを使用してデプロイした ROSA クラスターのサポートを提供しません。

## 2.5. PRIVATELINK ROSA クラスター以外の AMAZON VPC 要件

Amazon VPC を作成するには、以下が必要です。

- インターネットゲートウェイ
- NAT ゲートウェイ
- 必要なコンポーネントをインストールするためにインターネット接続のあるプライベートおよびパブリックサブネット。

Single-AZ クラスターには、少なくとも 1 つのプライベートサブネットとパブリックサブネットが必要で、Multi-AZ クラスターには 3 つ以上のプライベートサブネットとパブリックサブネットが必要です。

**関連情報**

- AWS クラスターに必要なデフォルトのコンポーネントの詳細は、AWS ドキュメントの Default VPCs を参照してください。
- AWS コンソールで VPC を作成する手順は、AWS ドキュメントの Create a VPC を参照してください。

## 2.6. OPENID CONNECT 設定の作成

Red Hat OpenShift Service on AWS 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) 設定を作成できます。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

- 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

- 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。

- 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
```

## 2.7. カスタマイズを使用したクラスターの作成

ご使用の環境のニーズに適した設定で、AWS Security Token Service (STS) クラスターを備えた Red Hat OpenShift Service on AWS (ROSA) をデプロイします。Red Hat OpenShift Cluster Manager または ROSA CLI (**rosa**) を使用して、カスタマイズを使用してクラスターをデプロイできます。

### 2.7.1. OpenShift Cluster Manager を使用してカスタマイズしたクラスターを作成する

AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する場合、Red Hat OpenShift Cluster Manager を使用して、インストールをインタラクティブにカスタマイズできます。

**重要**

STS では、パブリックおよび AWS PrivateLink クラスターのみがサポートされます。通常の プライベートクラスター (PrivateLink 以外) は STS では使用できません。

**前提条件**

- STS を使用する ROSA 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。
- 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。

- クラスター全体のプロキシーを設定する場合は、クラスターがインストールされている VPC からプロキシーにアクセスできることを確認している。プロキシーは VPC のプライベートサブネットからもアクセスできる必要があります。

**手順**

1. OpenShift Cluster Manager に移動し、**Create cluster**を選択します。
2. **Create an OpenShift cluster**ページの **Red Hat OpenShift Service on AWS (ROSA)**行で **Create cluster** を選択します。
3. AWS アカウントが自動的に検出されると、アカウント ID は **関連付けられた AWS アカウント** ドロップダウンメニューに表示されます。AWS アカウントが自動的に検出されない場合は、**Select an account→ Associate AWS account** をクリックして、次の手順に従います。

   a. **Authenticate** ページで、**rosa login** コマンドの横にあるコピーボタンをクリックします。このコマンドには、OpenShift Cluster Manager API ログイントークンが含まれます。

   **注記**

   OpenShift Cluster Manager の OpenShift Cluster Manager API Token ページで API トークンをロードすることもできます。

   b. CLI でコピーしたコマンドを実行して、ROSA アカウントにログインします。

   ```
   $ rosa login --token=<api_login_token> 1
   ```

   1 **<api_login_token>** を、コピーされたコマンドで提供されるトークンに置き換えます。

   **出力例**

   ```
   I: Logged in as '<username>' on 'https://api.openshift.com'
   ```

   c. OpenShift Cluster Manager の **Authenticate** ページで、**Next** をクリックします。

   d. **OCM role** ページで、**Basic OCM role** または **Admin OCM role** コマンドの横にあるコピーボタンをクリックします。
   基本ロールにより、OpenShift Cluster Manager は ROSA に必要な AWS IAM ロールとポリシーを検出できます。管理者ロールは、ロールとポリシーの検出も可能にします。さらに、管理者ロールを使用すると、OpenShift Cluster Manager を使用して、クラスター固有の Operator ロールと OpenID Connect (OIDC) プロバイダーを自動的にデプロイできます。

   e. コピーしたコマンドを CLI で実行し、プロンプトに従って OpenShift Cluster Manager IAM ロールを作成します。次の例では、デフォルトのオプションを使用して基本的な OpenShift Cluster Manager IAM ロールを作成します。

   ```
   $ rosa create ocm-role
   ```

   **出力例**

   ```
   I: Creating ocm role
   ```

```
? Role prefix: ManagedOpenShift 1
? Enable admin capabilities for the OCM role (optional): No 2
? Permissions boundary ARN (optional): 3
? Role Path (optional): 4
? Role creation mode: auto 5
I: Creating role using 'arn:aws:iam::<aws_account_id>:user/<aws_username>'
? Create the 'ManagedOpenShift-OCM-Role-<red_hat_organization_external_id>' role?
Yes
I: Created role 'ManagedOpenShift-OCM-Role-<red_hat_organization_external_id>' with
ARN 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-
<red_hat_organization_external_id>'
I: Linking OCM role
? OCM Role ARN: arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-
<red_hat_organization_external_id>
? Link the 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-
<red_hat_organization_external_id>' role with organization '<red_hat_organization_id>'?
Yes 6
I: Successfully linked role-arn 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-
OCM-Role-<red_hat_organization_external_id>' with organization account
'<red_hat_organization_id>'
```

1. OCM IAM ロール名に含める接頭辞を指定します。デフォルトは **ManagedOpenShift** です。Red Hat 組織の AWS アカウントごとに OCM ロールを 1 つだけ作成できます。
2. 管理者 OpenShift Cluster Manager IAM ロールを有効にします。これは、**--admin** 引数を指定するのと同じです。**自動** モードを使用して、OpenShift Cluster Manager を使用してクラスター固有の Operator ロールと OIDC プロバイダーを自動的にプロビジョニングする場合は、管理者ロールが必要です。
3. オプション: ロールのパーミッション境界 Amazon Resource Name (ARN) を指定します。詳細は、AWS ドキュメントの IAM エンティティーのアクセス許可の境界 を参照してください。
4. OCM ロールのカスタム ARN パスを指定します。パスには英数字のみを使用し、/ で開始および終了する必要があります (例: **/test/path/dev/**)。詳細は、**IAM ロールとポリシーの ARN パスのカスタマイズ** を参照してください。
5. ロール作成モードを選択します。**auto** モードを使用して、OpenShift Cluster Manager IAM ロールを自動的に作成し、それを Red Hat 組織アカウントにリンクすることができます。**manual** モードでは、ROSA CLI はロールの作成とリンクに必要な **aws** コマンドを生成します。**manual** モードでは、対応するポリシー JSON ファイルも現在のディレクトリーに保存されます。**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。
6. OpenShift Cluster Manager IAM ロールを Red Hat 組織アカウントにリンクします。

f. 上記のコマンドで OpenShift Cluster Manager IAM ロールを Red Hat 組織アカウントにリンクしないことを選択した場合は、OpenShift Cluster Manager **OCM role** ページから **rosa link** コマンドをコピーして実行します。

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

1. **<arn>** を、前のコマンドの出力に含まれている OpenShift Cluster Manager IAM の ARN に置き換えます。

g. OpenShift Cluster Manager **OCM role** ページで **Next** を選択します。

h. **User role** ページで、**User role** コマンドのコピーボタンをクリックし、CLI でコマンドを実行します。OpenShift Cluster Manager でクラスターおよび必要なリソースをインストールすると、Red Hat はユーザーロールを使用して AWS Identity を確認します。
プロンプトに従って、ユーザーロールを作成します。

```
$ rosa create user-role
```

**出力例**

```
I: Creating User role
? Role prefix: ManagedOpenShift 1
? Permissions boundary ARN (optional): 2
? Role Path (optional): [? for help] 3
? Role creation mode: auto 4
I: Creating ocm user role using 'arn:aws:iam::<aws_account_id>:user/<aws_username>'
? Create the 'ManagedOpenShift-User-<red_hat_username>-Role' role? Yes
I: Created role 'ManagedOpenShift-User-<red_hat_username>-Role' with ARN
'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-<red_hat_username>-
Role'
I: Linking User role
? User Role ARN: arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-
<red_hat_username>-Role
? Link the 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-
<red_hat_username>-Role' role with account '<red_hat_user_account_id>'? Yes 5
I: Successfully linked role ARN 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-
User-<red_hat_username>-Role' with account '<red_hat_user_account_id>'
```

1. ユーザーロール名に含める接頭辞を指定します。デフォルトは **ManagedOpenShift** です。

2. オプション: ロールのパーミッション境界 Amazon Resource Name (ARN) を指定します。詳細は、AWS ドキュメントの IAM エンティティーのアクセス許可の境界 を参照してください。

3. ユーザーロールのカスタム ARN パスを指定します。パスには英数字のみを使用し、/ で開始および終了する必要があります (例: **/test/path/dev/**)。詳細は、**IAM ロールとポリシーの ARN パスのカスタマイズ** を参照してください。

4. ロール作成モードを選択します。**auto** モードを使用して、ユーザーロールを自動的に作成し、OpenShift Cluster Manager ユーザーアカウントにリンクすることができます。**manual** モードでは、ROSA CLI はロールの作成とリンクに必要な **aws** コマンドを生成します。**manual** モードでは、対応するポリシー JSON ファイルも現在のディレクトリーに保存されます。**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。

5. ユーザーロールを OpenShift Cluster Manager ユーザーアカウントにリンクします。

i. 上記のコマンドでユーザーロールを OpenShift Cluster Manager ユーザーアカウントにリンクしないことを選択した場合は、OpenShift Cluster Manager **User role** ページから **rosa link** コマンドをコピーして実行します。

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

(1) **<arn>** を、前のコマンドの出力に含まれているユーザーロールの ARN に置き換えます。

j. OpenShift Cluster Manager **User role** ページで、**Ok** をクリックします。

k. **Accounts and roles** ページの **Associated AWS accounts** ドロップダウンメニューに AWS アカウント ID が表示されていることを確認します。

l. 必要なアカウントロールが存在しない場合は、**Some account roles ARNs was not detected** という通知が表示されます。**rosa create account-roles** コマンドの横にあるコピーバッファーをクリックし、CLI でコマンドを実行することにより、Operator ポリシーを含む AWS アカウント全体のロールおよびポリシーを作成できます。

```
$ rosa create account-roles
```

**出力例**

```
I: Logged in as '<red_hat_username>' on 'https://api.openshift.com'
I: Validating AWS credentials...
I: AWS credentials are valid!
I: Validating AWS quota...
I: AWS quota ok. If cluster installation fails, validate actual AWS resource usage against
https://docs.openshift.com/rosa/rosa_getting_started/rosa-required-aws-service-
quotas.html
I: Verifying whether OpenShift command-line tool is available...
I: Current OpenShift Client Version: 4.0
I: Creating account roles
? Role prefix: ManagedOpenShift (1)
? Permissions boundary ARN (optional): (2)
? Path (optional): [? for help] (3)
? Role creation mode: auto (4)
I: Creating roles using 'arn:aws:iam::<aws_account_number>:user/<aws_username>'
? Create the 'ManagedOpenShift-Installer-Role' role? Yes (5)
I: Created role 'ManagedOpenShift-Installer-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Installer-Role'
? Create the 'ManagedOpenShift-ControlPlane-Role' role? Yes (6)
I: Created role 'ManagedOpenShift-ControlPlane-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-ControlPlane-Role'
? Create the 'ManagedOpenShift-Worker-Role' role? Yes (7)
I: Created role 'ManagedOpenShift-Worker-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Worker-Role'
? Create the 'ManagedOpenShift-Support-Role' role? Yes (8)
I: Created role 'ManagedOpenShift-Support-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Support-Role'
I: To create a cluster with these roles, run the following command:
rosa create cluster --sts
```

(1) OpenShift Cluster Manager IAM ロール名に含める接頭辞を指定します。デフォルトは **ManagedOpenShift** です。

**重要**

アカウントロールにカスタム ARN パスを使用する場合でも、AWS アカウント全体で一意のアカウント全体のロール 接頭辞を指定する必要があります。

2 オプション: ロールのパーミッション境界 Amazon Resource Name (ARN) を指定します。詳細は、AWS ドキュメントの IAM エンティティーのアクセス許可の境界 を参照してください。

3 アカウント全体のロールのカスタム ARN パスを指定します。パスには英数字のみを使用し、/ で開始および終了する必要があります (例: **/test/path/dev/**)。詳細は、**IAM ロールとポリシーの ARN パスのカスタマイズ** を参照してください。

4 ロール作成モードを選択します。**auto** モードを使用して、アカウント全体のロールとポリシーを自動的に作成できます。**manual** モードでは、ROSA CLI はロールとポリシーの作成に必要な **aws** コマンドを生成します。**manual** モードでは、対応するポリシー JSON ファイルも現在のディレクトリーに保存されます。**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。

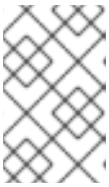
5 6 7 8 アカウント全体のインストーラー、コントロールプレーン、ワーカー、サポートロール、および対応する IAM ポリシーを作成します。詳細については、**アカウント全体の IAM ロールとポリシーリファレンス**を参照してください。

**注記**

このステップでは、ROSA CLI は、クラスター固有の Operator ポリシーによって使用されるアカウント全体の Operator IAM ポリシーも自動的に作成し、ROSA クラスター Operator がコア OpenShift 機能を実行できるようにします。詳細については、**アカウント全体の IAM ロールとポリシーリファレンス**を参照してください。

m. **Accounts and roles**ページで、**Refresh ARNs** をクリックし、インストーラー、サポート、ワーカー、およびコントロールプレーンのアカウントのロール ARN が表示されていることを確認します。
クラスターバージョンの AWS アカウントに複数のアカウントロールセットがある場合は、**インストーラーロール** ARN のドロップダウンリストが表示されます。クラスターで使用するインストーラーロールの ARN を選択します。クラスターは、選択したインストーラーロールに関連するアカウント全体のロールとポリシーを使用します。

4. **Next** をクリックします。



**注記**

**Accounts and roles**ページが更新された場合は、すべての前提条件を読んで完了したことを確認するために、チェックボックスの再選択が求められる場合があります。

5. **Cluster details** ページで、クラスターの名前を指定し、クラスターの詳細を指定します。

   a. **Cluster name** を追加します。

   b. **Version** ドロップダウンメニューからクラスターバージョンを選択します。

c. **Region** ドロップダウンメニューからクラウドプロバイダーのリージョンを選択します。

d. **Single zone** または **Multi-zone** 設定を選択し ます。

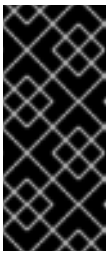
e. **Enable user workloads monitoring**を選択したままにして、Red Hat サイト信頼性エンジニアリング (SRE) プラットフォームメトリックから切り離して独自のプロジェクトをモニターします。このオプションはデフォルトで有効になっています。

f. オプション:etcd キー値の暗号化が必要な場合には、**Enable additional etcd encryption**を選択します。このオプションを使用すると、etcd キーの値は暗号化されますが、キーは暗号化されません。このオプションは、デフォルトで Red Hat OpenShift Service on AWS クラスター内の etcd ボリュームを暗号化するコントロールプレーンストレージ暗号化に追加されます。

**注記**

etcd のキー値の etcd 暗号化を有効にすると、約 20% のパフォーマンスのオーバーヘッドが発生します。このオーバーヘッドは、etcd ボリュームを暗号化するデフォルトのコントロールプレーンのストレージ暗号化に加えて、この 2 つ目の暗号化レイヤーの導入により生じます。お客様のユースケースで特に etcd 暗号化が必要な場合にのみ、暗号化を有効にすることを検討してください。

g. オプション: 独自の AWS Key Management Service (KMS) キーの Amazon Resource Name (ARN) を提供する場合は、**Encrypt persistent volumes with customer keys**を選択します。このキーは、クラスター内の永続ボリュームの暗号化に使用されます。

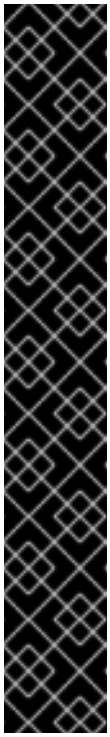


**重要**

デフォルトでは、デフォルトのストレージクラスから作成された永続ボリューム (PV) のみが暗号化されます。

他のストレージクラスを使用して作成された PV は、ストレージクラスが暗号化されるように設定されている場合にのみ暗号化されます。

i. オプション: 顧客管理の KMS キーを作成するには、対称暗号化 KMS キーの作成 の手順に従います。



**重要**

クラスターを正常に作成するには、アカウントのロールに加えて EBS Operator のロールが必要です。

このロールは、ROSA が Container Storage Interface (CSI) を通じてバックエンドストレージを管理するために必要な IAM ポリシーである **ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials** ポリシーに割り当てる必要があります。

クラスター Operator に必要なポリシーと権限の詳細は、**アカウント全体のロールを作成する方法** を参照してください。

**EBS Operator のロールの例**

**"arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-ebs-cloud-credent"**

Operator のロールを作成したら、AWS コンソールの **Key Management Service (KMS)** ページ で **キーポリシー** を編集して、ロールを追加する必要があります。

h. **Next** をクリックします。

6. **Default machine pool** ページで、**Compute node instance type**を選択します。

**注記**

クラスターの作成後、クラスター内のコンピュートノードの数を変更できますが、デフォルトのマシンプールのコンピュートノードインスタンスタイプは変更できません。使用可能なノードの数とタイプは、単一または複数のアベイラビリティーゾーンを使用するかどうかによって異なります。また、AWS アカウントと選択したリージョンで何が有効で利用可能かによっても異なります。

7. オプション: デフォルトのマシンプールの自動スケーリングを設定します。

a. **Enable autoscaling** を選択し、デプロイメントのニーズを満たすためにデフォルトのマシンプール内のマシン数を自動的にスケーリングします。

b. 自動スケーリングの最小および最大のノード数制限を設定します。Cluster Autoscaler は、指定する制限を超えてデフォルトのマシンプールノード数を減らしたり、増やしたりできません。

- 単一アベイラビリティーゾーンを使用してクラスターをデプロイした場合は、**最小**および**最大**のノード数 を設定します。これは、アベイラビリティーゾーンのコンピュートノードの最小および最大の制限を定義します。

- 複数のアベイラビリティーゾーンを使用してクラスターをデプロイした場合は、**Minimum nodes per zone**および **Maximum nodes per zone** を設定します。これは、ゾーンごとの最小および最大のコンピュート制限を定義します。

**注記**

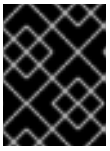
または、デフォルトのマシンプールの作成後にマシンプールの自動スケーリングを設定できます。

8. 自動スケーリングを有効にしなかった場合は、デフォルトのマシンプールのコンピュートノード数を選択します。

   - 単一アベイラビリティーゾーンを使用してクラスターをデプロイした場合は、ドロップダウンメニューから **コンピュートノード数** を選択します。これは、ゾーンのマシンプールにプロビジョニングするコンピュートノードの数を定義します。

   - 複数のアベイラビリティーゾーンを使用してクラスターをデプロイした場合は、ドロップダウンメニューから **コンピュートノードの数 (ゾーンごと)** を選択します。これは、ゾーンごとにマシンプールにプロビジョニングするコンピュートノードの数を定義します。

9. オプション: IMDSv2 の使用を強制するには、EC2 Instance Metadata Service (IMDS) 設定 (**optional** (デフォルト) または **required**) を選択します。IMDS の詳細は、AWS ドキュメントの Instance metadata and user data を参照してください。



**重要**

クラスターの作成後に Instance Metadata Service の設定を変更することはできません。

10. オプション: **Edit node labels** を展開してラベルをノードに追加します。**Add label** をクリックしてさらにノードラベルを追加し、**Next** を選選択します。

11. **Network configuration** ページの **Cluster privacy** セクションで、**Public** または **Private**を選択して、クラスターのパブリックまたはプライベート API エンドポイントとアプリケーションルートを使用します。

**重要**

クラスターの作成後、API エンドポイントをパブリックとプライベートの間で変更することはできません。

**パブリック API エンドポイント**

クラスターへのアクセスを制限しない場合は、**パブリック** を選択します。インターネットから Kubernetes API エンドポイントとアプリケーションルートにアクセスできます。

**プライベート API エンドポイント**

クラスターへのネットワークアクセスを制限する場合は、**Private** を選択します。Kubernetes API エンドポイントとアプリケーションルートには、直接のプライベート接続からのみアクセスできます。

**重要**

プライベート API エンドポイントを使用している場合、クラウドプロバイダーアカウントのネットワーク設定を更新するまでクラスターにはアクセスできません。

12. オプション: パブリック API エンドポイントを使用することを選択した場合は、デフォルトでクラスター用に新しい VPC が作成されます。代わりに既存の VPC にクラスターをインストールする場合は、**Install into an existing VPC** を選択します。

**警告**

OpenShift インストーラーによって作成された既存の VPC に ROSA クラスターをインストールすることはできません。このような VPC は、クラスターのデプロイ中に作成されたものであり、クラスターのプロビジョニング操作と削除操作が正しく機能するように、単一のクラスターにのみ関連付けられている必要があります。

VPC が OpenShift インストーラーによって作成されたものかどうかを確認するには、**kubernetes.io/cluster/<infra-id>** タグの **owned** 値を確認します。たとえば、**mycluster-12abc-34def** という名前の VPC のタグを確認したところ、**kubernetes.io/cluster/mycluster-12abc-34def** タグの値が **owned** であったとします。この VPC はインストーラーによって作成されたものであるため、管理者の方は変更しないでください。

**注記**

プライベート API エンドポイントを使用することを選択した場合は、既存の VPC と PrivateLink を使用する必要があり、**既存の VPC にインストールしてUse a PrivateLink** オプションが自動的に選択されます。これらのオプションを使用すると、Red Hat サイト信頼性エンジニアリング (SRE) チームはクラスターに接続して、AWS PrivateLink エンドポイントのみを使用してサポートを行うことができます。

13. オプション: クラスターを既存の VPC にインストールする場合は、**Configure a cluster-wide proxy** を選択して、HTTP または HTTPS プロキシーがクラスターからインターネットへの直接アクセスを拒否できるようにします。

14. **Next** をクリックします。

15. クラスターを既存の AWS VPC にインストールする場合、**Virtual Private Cloud (VPC) サブネット設定** を指定します。

**注記**

クラスターをインストールするアベイラビリティーゾーンごとに、VPC がパブリックおよびプライベートサブネットで設定されるようにする必要があります。PrivateLink を使用する場合には、プライベートサブネットのみが必要になります。

a. オプション: **Additional security groups** を展開し、デフォルトで作成されるマシンプール内のノードに適用する追加のカスタムセキュリティーグループを選択します。すでにセキュリティーグループを作成し、このクラスター用に選択した VPC にそのグループを関連付けている必要があります。クラスターを作成した後は、デフォルトのマシンプールにセキュリティーグループを追加または編集することはできません。
デフォルトでは、指定したセキュリティーグループがすべてのノードタイプに追加されます。ノードタイプごとに異なるセキュリティーグループを選択するには、**Apply the same security groups to all node types (control plane, infrastructure and worker)** チェックボックスをオフにします。

詳細は、**関連情報** の **セキュリティーグループ** の要件を参照してください。

16. クラスター全体のプロキシーを設定することを選択した場合は、**Cluster-wide proxy** ページでプロキシー設定の詳細を指定します。

    a. 次のフィールドの少なくとも 1 つに値を入力します。

    - 有効な **HTTP proxy URL** を指定します。
    - 有効な **HTTPS proxy URL** を指定します。
    - **Additional trust bundle** フィールドに、PEM でエンコードされた X.509 証明書バンドルを指定します。このバンドルはクラスターノードの信頼済み証明書ストアに追加されます。プロキシーのアイデンティティー証明書が Red Hat Enterprise Linux CoreOS (RHCOS) 信頼バンドルからの認証局によって署名されない限り、追加の信頼バンドルファイルが必要です。
      追加のプロキシー設定が必要ではなく、追加の認証局 (CA) を必要とする MITM の透過的なプロキシーネットワークを使用する場合には、MITM CA 証明書を指定する必要があります。

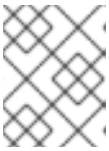
**注記**

HTTP または HTTPS プロキシー URL を指定せずに追加の信頼バンドルファイルをアップロードする場合、バンドルはクラスターに設定されますが、プロキシーで使用するように設定されていません。

    b. **Next** をクリックします。

Red Hat OpenShift Service on AWS を使用したプロキシーの設定に関する詳細は、**クラスター全体のプロキシーの設定** を参照してください。

17. **CIDR ranges** ダイアログで、カスタムの Classless Inter-Domain Routing (CIDR) 範囲を設定するか、提供されるデフォルトを使用して、**Next** を、クリックします。



**注記**

VPC にインストールする場合、**Machine CIDR** 範囲は VPC サブネットに一致する必要があります。

**重要**

CIDR 設定は後で変更することはできません。続行する前に、ネットワーク管理者と選択内容を確認してください。

18. **Cluster roles and policies** ページで、優先するクラスター固有の Operator の IAM ロールと OIDC プロバイダーの作成モードを選択します。
    **Manual** モードでは、**rosa** CLI コマンドまたは **aws** CLI コマンドのいずれかを使用して、クラスターに必要な Operator ロールと OIDC プロバイダーを生成できます。**手動** モードでは、優先オプションを使用して IAM リソースを手動で作成し、クラスターのインストールを完了する前に、詳細を確認できます。

    または、**Auto** モードを使用して、Operator のロールと OIDC プロバイダーを自動的に作成することもできます。**Auto** モードを有効にするには、OpenShift Cluster Manager IAM ロールに管理者機能が必要です。

**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、カスタムパスが自動的に検出され、Operator ロールに適用されます。カスタム ARN パスは、**Manual** モードまたは **Auto** モードのいずれかを使用して Operator ロールが作成されるときに適用されます。

19. オプション: クラスター固有の Operator IAM ロールの **カスタム Operator ロール接頭辞** を指定します。

**注記**

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。

20. **Next** を選択します。

21. **Cluster update strategy** ページで、更新設定を行います。

    a. クラスターの更新方法を選択します。

    - 各更新を個別にスケジュールする場合は、**Individual updates** を選択します。以下はデフォルトのオプションになります。
    - **Recurring updates** を選択して、更新が利用可能な場合に、希望の曜日と開始時刻にクラスターを更新します。

**重要**

定期的な更新を選択した場合でも、マイナーリリース間でクラスターをアップグレードする前に、アカウント全体およびクラスター固有の IAM リソースを更新する必要があります。

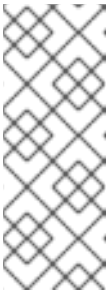
**注記**

保守終了日は、Red Hat OpenShift Service on AWS の更新ライフサイクルドキュメントで確認できます。詳細については、**Red Hat OpenShift Service on AWS 更新ライフサイクル** を参照してください。

    b. 繰り返し更新を選択した場合は、ドロップダウンメニューから希望の曜日およびアップグレード開始時刻 (UTC) を選択します。

    c. オプション: クラスターアップグレード時の **ノードのドレイン (解放)** の猶予期間を設定できます。デフォルトで **1 時間** の猶予期間が設定されています。

    d. **Next** をクリックします。



**注記**

クラスターのセキュリティーまたは安定性に大きく影響する重大なセキュリティー問題がある場合、Red Hat サイト信頼性エンジニアリング (SRE) は、影響を受けない最新の z ストリームバージョンへの自動更新をスケジュールする場合があります。更新は、お客様に通知された後、48 時間以内に適用されます。重大な影響を及ぼすセキュリティー評価の説明は、Red Hat セキュリティー評価について を参照してください。

22. 選択の概要を確認し、**Create cluster** をクリックしてクラスターのインストールを開始します。

23. **手動** モードを使用することを選択した場合は、クラスター固有の Operator のロールと OIDC プロバイダーを手動で作成して、インストールを続行します。

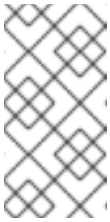
    a. **Action required to continue installation** ダイアログで、**AWS CLI** または **ROSA CLI** タブを選択し、リソースを手動で作成します。

    - **AWS CLI** メソッドを使用することを選択した場合は、**Download .zip** をクリックしてファイルを保存してから、AWS CLI コマンドとポリシーファイルをデプロイメントします。次に、CLI で提供されている **aws** コマンドを実行します。

**注記**

ポリシーファイルを含むディレクトリーで **aws** コマンドを実行する必要があります。

    - **ROSA CLI** メソッドを使用することを選択した場合は、**rosa create** コマンドの横にあるコピーボタンをクリックして、CLI で実行します。

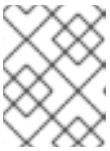


**注記**

関連付けられた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、これらの手動の方法を使用して Operator のロールを作成すると、カスタムパスが自動的に検出され、Operator のロールに適用されます。

    b. **Action required to continue installation** ダイアログで、**x** をクリックしてクラスターの **Overview** ページに戻ります。

    c. **Overview** ページの **Details** セクションで、クラスターの **Status** が **Waiting** から **Installing** に変更されていることを確認します。ステータスが変わるまでに約 2 分の短い遅延が発生する場合があります。



**注記**

**自動** モードの使用を選択した場合、OpenShift Cluster Manager は Operator ロールと OIDC プロバイダーを自動的に作成します。

**重要**

クラスターを正常に作成するには、アカウントのロールに加えて EBS Operator のロールが必要です。

このロールは、ROSA が Container Storage Interface (CSI) を通じてバックエンドストレージを管理するために必要な IAM ポリシーである **ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials** ポリシーに割り当てる必要があります。

クラスター Operator に必要なポリシーと権限の詳細は、**アカウント全体のロールを作成する方法** を参照してください。

**EBS Operator のロールの例**

**"arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-ebs-cloud-credent"**

Operator のロールを作成したら、AWS コンソールの Key Management Service (KMS) ページ で **キーポリシー** を編集して、ロールを追加する必要があります。

**検証**

- クラスターの **Overview** ページで、インストールの進捗をモニターできます。同じページでインストールのログを表示できます。そのページの **Details** セクションの **Status** が **Ready** として表示されると、クラスターは準備が完了した状態になります。

**注記**

インストールが失敗するか、約 40 分経ってもクラスターの **状態** が **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。

**関連情報**

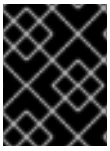
- **ROSA CLI を使用したオブジェクトの管理** の create cluster
- アカウント全体のロールを作成する方法

### 2.7.2. CLI を使用してカスタマイズしたクラスターを作成する

AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する場合は、インストールを対話的にカスタマイズできます。

**rosa create cluster --interactive** コマンドをクラスターの作成時に実行すると、デプロイメントのカスタマイズを可能にする一連の対話式プロンプトが表示されます。詳細は、**対話式クラスター作成モードリファレンス** を参照してください。

対話モードを使用したクラスターのインストールが完了すると、同じカスタム設定を使用してさらにクラスターをデプロイできるようにする単一のコマンドが出力に提供されます。



**重要**

STS では、パブリックおよび AWS PrivateLink クラスターのみがサポートされます。通常の プライベートクラスター (PrivateLink 以外) は STS では使用できません。

**前提条件**

- STS を使用する ROSA 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。
- 顧客管理の AWS Key Management Service (KMS) キーを暗号化に使用する場合は、対称 KMS キーを作成する必要があります。クラスターを作成するときに、Amazon Resource Name (ARN) を指定する必要があります。顧客管理の KMS キーを作成するには、対称暗号化 KMS キーの作成 の手順に従います。

**重要**

クラスターを正常に作成するには、アカウントのロールに加えて EBS Operator のロールが必要です。

このロールは、ROSA が Container Storage Interface (CSI) を通じてバックエンドストレージを管理するために必要な IAM ポリシーである **ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials** ポリシーに割り当てる必要があります。

クラスター Operator に必要なポリシーと権限の詳細は、**アカウント全体のロールを作成する方法** を参照してください。

**EBS Operator のロールの例**

**"arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-ebs-cloud-credent"**

Operator のロールを作成したら、AWS コンソールの **Key Management Service (KMS)** ページ で **キーポリシー** を編集して、ロールを追加する必要があります。

**手順**

1. Operator ポリシーを含む、必要なアカウント全体のロールおよびポリシーを作成します。
   a. 現在の作業ディレクトリーに IAM ポリシー JSON ファイルを作成し、確認用に **aws** CLI コマンドを実行します。

```
$ rosa create account-roles --interactive \ 1
                    --mode manual 2
```

1 **interactive** モードでは、インタラクティブプロンプトで設定オプションを指定できます。詳細は、**対話式クラスター作成モードリファレンス** を参照してください。

2 **manual** モードは、アカウント全体のロールおよびポリシーの作成に必要な **aws** CLI コマンドおよび JSON ファイルを生成します。確認後、手動でコマンドを実行してリ

### 出力例

```
I: Logged in as '<red_hat_username>' on 'https://api.openshift.com'
I: Validating AWS credentials...
I: AWS credentials are valid!
I: Validating AWS quota...
I: AWS quota ok. If cluster installation fails, validate actual AWS resource usage against
https://docs.openshift.com/rosa/rosa_getting_started/rosa-required-aws-service-
quotas.html
I: Verifying whether OpenShift command-line tool is available...
I: Current OpenShift Client Version: 4.0
I: Creating account roles
? Role prefix: ManagedOpenShift 1
? Permissions boundary ARN (optional): 2
? Path (optional): [? for help] 3
? Role creation mode: auto 4
I: Creating roles using 'arn:aws:iam::<aws_account_number>:user/<aws_username>'
? Create the 'ManagedOpenShift-Installer-Role' role? Yes 5
I: Created role 'ManagedOpenShift-Installer-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Installer-Role'
? Create the 'ManagedOpenShift-ControlPlane-Role' role? Yes 6
I: Created role 'ManagedOpenShift-ControlPlane-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-ControlPlane-Role'
? Create the 'ManagedOpenShift-Worker-Role' role? Yes 7
I: Created role 'ManagedOpenShift-Worker-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Worker-Role'
? Create the 'ManagedOpenShift-Support-Role' role? Yes 8
I: Created role 'ManagedOpenShift-Support-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Support-Role'
I: To create a cluster with these roles, run the following command:
rosa create cluster --sts
```

1 OpenShift Cluster Manager IAM ロール名に含める接頭辞を指定します。デフォルトは **ManagedOpenShift** です。

**重要**

アカウントロールにカスタム ARN パスを使用する場合でも、AWS アカウント全体で一意のアカウント全体のロール 接頭辞を指定する必要があります。

2 オプション: ロールのパーミッション境界 Amazon Resource Name (ARN) を指定します。詳細は、AWS ドキュメントの IAM エンティティーのアクセス許可の境界 を参照してください。

3 アカウント全体のロールのカスタム ARN パスを指定します。パスには英数字のみを使用し、/ で開始および終了する必要があります (例: **/test/path/dev/**)。詳細は、**IAM ロールとポリシーの ARN パスのカスタマイズ** を参照してください。

4 ロール作成モードを選択します。**auto** モードを使用して、アカウント全体のロールと

5 6 7 8 アカウント全体のインストーラー、コントロールプレーン、ワーカー、サポートロール、および対応する IAM ポリシーを作成します。詳細については、**アカ**

**注記**

このステップでは、ROSA CLI は、クラスター固有の Operator ポリシーによって使用されるアカウント全体の Operator IAM ポリシーも自動的に作成し、ROSA クラスター Operator がコア OpenShift 機能を実行できるようにします。詳細については、**アカウント全体の IAM ロールとポリシーリファレンス**を参照してください。

b. 確認後は、**aws** コマンドを手動で実行し、ロールおよびポリシーを作成します。または、**--mode auto** を使用して前述のコマンドを実行して、**aws** コマンドを即座に実行できます。

2. オプション: 独自の AWS KMS キーを使用してコントロールプレーン、インフラストラクチャー、ワーカーノードのルートボリューム、および永続ボリューム (PV) を暗号化する場合は、アカウント全体のインストーラーロールの ARN を KMS キーポリシーに追加します。

**重要**

デフォルトのストレージクラスから作成された永続ボリューム (PV) のみが、この特定のキーで暗号化されます。

他のストレージクラスを使用して作成された PV は引き続き暗号化されますが、ストレージクラスがこのキーを使用するように特別に設定されていない限り、PV はこのキーで暗号化されません。

a. KMS キーのキーポリシーをローカルマシンのファイルに保存します。次の例では、出力を現在の作業ディレクトリーの **kms-key-policy.json** に保存します。

```
$ aws kms get-key-policy --key-id <key_id_or_arn> --policy-name default --output text > kms-key-policy.json 1
```

1 **<key_id_or_arn>** を KMS キーの ID または ARN に置き換えます。

b. 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の ARN を、ファイルの **Statement.Principal.AWS** セクションに追加します。以下の例では、デフォルトの **ManagedOpenShift-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": "Allow ROSA use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Support-Role", (1)
                    "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Installer-Role",
                    "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role",
                    "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-ControlPlane-
Role",
                    "arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-
cluster-csi-drivers-ebs-cloud-credent" (2)
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Support-Role", (3)
                    "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Installer-Role",
                    "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role",
                    "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-ControlPlane-
Role",
                    "arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-
cluster-csi-drivers-ebs-cloud-credent" (4)
                ]
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        }
    ]
}
```

(1) (3) ROSA クラスターの作成時に使用されるアカウント全体のロールの ARN を指定する必要があります。セクションにリスト表示される ARN はコンマで区切る必要があります。

2 4 ROSA クラスターの作成時に使用する Operator ロールの ARN を指定する必要があります。セクションにリスト表示される ARN はコンマで区切る必要があります。

c. KMS キーポリシーに変更を適用します。

```
$ aws kms put-key-policy --key-id <key_id_or_arn> \ 1
  --policy file://kms-key-policy.json \ 2
  --policy-name default
```

1 **<key_id_or_arn>** を KMS キーの ID または ARN に置き換えます。

2 ローカルファイルでキーポリシーを参照する場合は、**file://** 接頭辞を含める必要があります。

次の手順でクラスターを作成すると、KMS キーの ARN を参照できます。

3. カスタムインストールオプションを使用して、STS を使用するクラスターを作成します。**--interactive** モードを使用して、カスタム設定を対話的に指定できます。

**警告**

OpenShift インストーラーによって作成された既存の VPC に ROSA クラスターをインストールすることはできません。このような VPC は、クラスターのデプロイ中に作成されたものであり、クラスターのプロビジョニング操作と削除操作が正しく機能するように、単一のクラスターにのみ関連付けられている必要があります。

VPC が OpenShift インストーラーによって作成されたものかどうかを確認するには、**kubernetes.io/cluster/<infra-id>** タグの **owned** 値を確認します。たとえば、**mycluster-12abc-34def** という名前の VPC のタグを確認したところ、**kubernetes.io/cluster/mycluster-12abc-34def** タグの値が **owned** であったとします。この VPC はインストーラーによって作成されたものであるため、管理者の方は変更しないでください。

```
$ rosa create cluster --interactive --sts
```

**出力例**

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Cluster name: <cluster_name>
? Domain prefix: <domain_prefix> 1
? Deploy cluster with Hosted Control Plane (optional): No
? Create cluster admin user: Yes 2
? Username: user-admin 3
? Password: [? for help] ********** 4
? OpenShift version: 4.15.0 5
```

```
? Configure the use of IMDSv2 for ec2 instances optional/required (optional): 6
I: Using arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Installer-Role for the
Installer role 7
I: Using arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-ControlPlane-Role for the
ControlPlane role
I: Using arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role for the Worker
role
I: Using arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Support-Role for the
Support role
? External ID (optional): 8
? Operator roles prefix: <cluster_name>-<random_string> 9
? Deploy cluster using pre registered OIDC Configuration ID:
? Tags (optional) 10
? Multiple availability zones (optional): No 11
? AWS region: us-east-1
? PrivateLink cluster (optional): No
? Install into an existing VPC (optional): Yes 12
? Select availability zones (optional): No
? Enable Customer Managed key (optional): No 13
? Compute nodes instance type (optional):
? Enable autoscaling (optional): No
? Compute nodes: 2
? Additional Security Group IDs (optional): 14
? > [*]  sg-0e375ff0ec4a6cfa2 ('sg-1')
? > [ ]  sg-0e525ef0ec4b2ada7 ('sg-2')
? Machine CIDR: 10.0.0.0/16
? Service CIDR: 172.30.0.0/16
? Pod CIDR: 10.128.0.0/14
? Host prefix: 23
? Encrypt etcd data (optional): No 15
? Disable Workload monitoring (optional): No
I: Creating cluster '<cluster_name>'
I: To create this cluster again in the future, you can run:
   rosa create cluster --cluster-name <cluster_name> --role-arn arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Installer-Role --support-role-arn arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Support-Role --master-iam-role arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-ControlPlane-Role --worker-iam-role
arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role --operator-roles-prefix
<cluster_name>-<random_string> --region us-east-1 --version 4.15.0 --additional-compute-
security-group-ids sg-0e375ff0ec4a6cfa2 --additional-infra-security-group-ids sg-
0e375ff0ec4a6cfa2 --additional-control-plane-security-group-ids sg-0e375ff0ec4a6cfa2 --
replicas 2 --machine-cidr 10.0.0.0/16 --service-cidr 172.30.0.0/16 --pod-cidr 10.128.0.0/14 --
host-prefix 23 16
I: To view a list of clusters and their status, run 'rosa list clusters'
I: Cluster '<cluster_name>' has been created.
I: Once the cluster is installed you will need to add an Identity Provider before you can login
into the cluster. See 'rosa create idp --help' for more information.
...
```

1 オプション: クラスターを作成するときに、**--domain-prefix** フラグを使用して ***.openshiftapps.com** 上のクラスターのサブドメインをカスタマイズできます。このフラグの値は組織内で一意である必要があり、15 文字を超えてはならず、クラスターの作成後に変更できません。フラグが指定されていない場合は、クラスター名の長さに応じて自動生成された値が作成されます。クラスター名が 15 文字以下の場合、その名前がドメイン接

頭辞に使用されます。クラスター名が 15 文字を超える場合、ドメイン接頭辞は 15 文字の文字列にランダムに生成されます。

2 3 4 クラスターの作成時に、クラスターのローカル管理者ユーザーを作成できます。**Yes** を選択すると、クラスター管理者のユーザー名とパスワードを作成するように求められます。ユーザー名には、/、**:**、または **%** を含めることはできません。パスワードは空白を含まない 14 文字以上 (ASCII 標準) である必要があります。このプロセスでは、htpasswd ID プロバイダーが自動的に設定されます。

5 クラスターの作成時にリストされる **OpenShift version** オプションには、メジャー、マイナー、パッチバージョン (例: **4.15.0**) が含まれます。

6 オプション: EC2 Instance Metadata Service (IMDS) の v1 エンドポイントと v2 エンドポイントの両方を使用するようにすべての EC2 インスタンスを設定するには、optional を指定します。これはデフォルト値です。すべての EC2 インスタンスが IMDSv2 のみを使用するように設定するには、required を指定します。

**重要**

クラスターの作成後に Instance Metadata Service の設定を変更することはできません。

7 クラスターバージョンの AWS アカウントに複数のアカウントロールセットがある場合は、オプションのインタラクティブなリストが表示されます。

8 オプション: アカウントのロールが引き受けられるときに、Red Hat OpenShift Service on AWS および OpenShift インストーラーによって渡される一意の識別子を指定します。このオプションは、外部 ID を予想されるカスタムアカウントロールにのみ必要です。

9 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、**Operator IAM ロール接頭辞の定義**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。

10 オプション: Red Hat OpenShift Service on AWS が作成した AWS 内のすべてのリソースで使用するタグを指定します。タグは、AWS 内のリソースの管理、識別、整理、検索、フィルタリングに使用できます。タグはコンマで区切られます。例: "key value, data input"。

**重要**

Red Hat OpenShift Service on AWS は、クラスター作成時に Red Hat OpenShift リソースへのカスタムタグのみをサポートします。タグを追加すると、削除したり編集したりすることはできません。Red Hat が追加したタグは、クラスターが Red Hat の実稼働サービスレベルアグリーメント (SLA) への準拠を維持するために必要です。これらのタグは削除してはいけません。

Red Hat OpenShift Service on AWS では、ROSA クラスターマネージドリソース以外へのタグの追加はサポートされていません。AWS リソースが ROSA クラスターによって管理されている場合、これらのタグが失われる可能性があります。このような場合、タグを調整してそのままの状態に保つためのカスタムソリューションまたはツールが必要になる可能性があります。

11 オプション: 実稼働環境のワークロードには、複数のアベイラビリティーゾーンの使用が推奨されます。デフォルトは単一のアベイラビリティーゾーンです。

12 オプション: 既存の VPC にクラスターを作成することも、使用する新しい VPC を ROSA で作成することもできます。

**警告**

OpenShift インストーラーによって作成された既存の VPC に ROSA クラスターをインストールすることはできません。このような VPC は、クラスターのデプロイ中に作成されたものであり、クラスターのプロビジョニング操作と削除操作が正しく機能するように、単一のクラスターにのみ関連付けられている必要があります。

VPC が OpenShift インストーラーによって作成されたものかどうかを確認するには、**kubernetes.io/cluster/<infra-id>** タグの **owned** 値を確認します。たとえば、**mycluster-12abc-34def** という名前の VPC のタグを確認したところ、**kubernetes.io/cluster/mycluster-12abc-34def** タグの値が **owned** であったとします。この VPC はインストーラーによって作成されたものであるため、管理者の方は変更しないでください。

13 オプション: 独自の AWS KMS キーを使用してコントロールプレーン、インフラストラクチャー、ワーカーノードのルートボリューム、および PV を暗号化する場合は、このオプションを有効にします。前述の手順でアカウント全体のロール ARN を追加した KMS キーの ARN を指定します。

**重要**

デフォルトのストレージクラスから作成された永続ボリューム (PV) のみが、この特定のキーで暗号化されます。

他のストレージクラスを使用して作成された PV は引き続き暗号化されますが、ストレージクラスがこのキーを使用するように特別に設定されていない限り、PV はこのキーで暗号化されません。

14 オプション: クラスターで使用する追加のカスタムセキュリティーグループを選択できます。すでにセキュリティーグループを作成し、このクラスター用に選択した VPC にそのグループを関連付けている必要があります。マシンプールを作成した後に、デフォルトのマシンプールのセキュリティーグループを追加または編集することはできません。詳細は、**関連情報** の **セキュリティーグループ** の要件を参照してください。

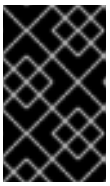
15 オプション: このオプションを有効にするのは、デフォルトで etcd ボリュームを暗号化するコントロールプレーンストレージ暗号化に加えて、etcd キー値の暗号化が必要なユースケースの場合のみです。このオプションを使用すると、etcd キーの値は暗号化されますが、キーは暗号化されません。

**重要**

etcd のキー値の etcd 暗号化を有効にすると、約 20% のパフォーマンスのオーバーヘッドが発生します。このオーバーヘッドは、etcd ボリュームを暗号化するデフォルトのコントロールプレーンのストレージ暗号化に加えて、この 2 つ目の暗号化レイヤーの導入により生じます。Red Hat は、お客様のユースケースで特に etcd 暗号化が必要な場合にのみ有効にすることを推奨します。

16 この出力には、今後も同じ設定でクラスターを作成するのに実行できるカスタムコマンドが含まれます。

**--interactive** モードを使用する代わりに、**rosa create cluster** コマンドの実行時にカスタマイズオプションを直接指定できます。**rosa create cluster --help** コマンドを実行して利用可能な CLI オプションのリストを表示するか、**ROSA CLI を使用したオブジェクトの管理** の **クラスターの作成** を参照してください。



**重要**

Operator IAM ロールおよび OpenID Connect (OIDC) プロバイダーを作成し、クラスターの状態を **ready** に移行するには、以下の手順を実行する必要があります。

4. クラスター固有の Operator IAM ロールを作成します。

   a. 現在の作業ディレクトリーに Operator IAM ポリシー JSON ファイルを作成し、確認用に **aws** CLI コマンドを実行します。

```
$ rosa create operator-roles --mode manual --cluster <cluster_name|cluster_id> 1
```

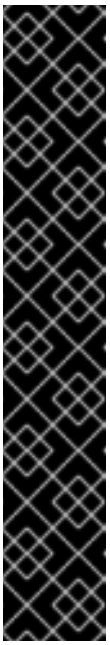
   1 **manual** モードは、Operator ロールの作成に必要な **aws** CLI コマンドおよび JSON ファイルを生成します。確認後、手動でコマンドを実行してリソースを作成する必要があります。

b. 確認後は、**aws** コマンドを手動で実行し、Operator IAM ロールを作成し、マネージド Operator ポリシーをそれらに割り当てます。または、**--mode auto** を使用して前述のコマンドを実行して、**aws** コマンドを即座に実行できます。

**注記**

前の手順で接頭辞を指定した場合、カスタム接頭辞が Operator ロール名に適用されます。

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、カスタムパスが自動的に検出され、Operator ロールに適用されます。



**重要**

クラスターを正常に作成するには、アカウントのロールに加えて EBS Operator のロールが必要です。

このロールは、ROSA が Container Storage Interface (CSI) を通じてバックエンドストレージを管理するために必要な IAM ポリシーである **ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials** ポリシーに割り当てる必要があります。

クラスター Operator に必要なポリシーと権限の詳細は、**アカウント全体のロールを作成する方法** の EBS Operator ロールの例 **"arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-ebs-cloud-credent"** を参照してください。

Operator のロールを作成したら、AWS コンソールの Key Management Service (KMS) ページ で **キーポリシー** を編集して、ロールを追加する必要があります。

5. クラスター Operator が認証に使用する OpenID Connect (OIDC) プロバイダーを作成します。

```
$ rosa create oidc-provider --mode auto --cluster <cluster_name|cluster_id> 1
```

1 **auto** モードは、OIDC プロバイダーを作成する **aws** CLI コマンドを即時実行します。

6. クラスターのステータスを確認します。

```
$ rosa describe cluster --cluster <cluster_name|cluster_id>
```

**出力例**

```
Name:                  <cluster_name>
ID:                  <cluster_id>
External ID:           <external_id>
OpenShift Version:       <version>
Channel Group:           stable
DNS:                 <cluster_name>.xxxx.p1.openshiftapps.com
AWS Account:           <aws_account_id>
API URL:               https://api.<cluster_name>.xxxx.p1.openshiftapps.com:6443
Console URL:           https://console-openshift-console.apps.
```

```
<cluster_name>.xxxx.p1.openshiftapps.com
Region:                  <aws_region>
Multi-AZ:                false
Nodes:
 - Master:               3
 - Infra:                2
 - Compute:              2
Network:
 - Service CIDR:         172.30.0.0/16
 - Machine CIDR:         10.0.0.0/16
 - Pod CIDR:             10.128.0.0/14
 - Host Prefix:          /23
STS Role ARN:            arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Installer-
Role
Support Role ARN:        arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Support-
Role
Instance IAM Roles:
 - Master:               arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-ControlPlane-
Role
 - Worker:               arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role
Operator IAM Roles:
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-ingress-operator-
cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-
ebs-cloud-credent
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-machine-api-aws-
cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cloud-credential-
operator-cloud-crede
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-image-registry-
installer-cloud-creden
Ec2 Metadata Http Tokens:   optional
State:                   ready
Private:                 No
Created:                 Oct  1 2021 08:12:25 UTC
Details Page:            https://console.redhat.com/openshift/details/s/<subscription_id>
OIDC Endpoint URL:       https://oidc.op1.openshiftapps.com/<cluster_id>|<oidc_config_id>
\ 1
```

1. エンドポイント URL は、BYO OIDC 設定によって異なります。OIDC 設定を事前に作成している場合、URL の末尾が **<oidc_config_id>** 値になります。それ以外の場合、URL の末尾は **<cluster-ID>** 値です。

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。

- **waiting (Waiting for OIDC configuration)**
- **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、約 40 分後に **State** フィールドが **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に関する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。

7. OpenShift インストーラーログを監視して、クラスター作成の進捗を追跡します。

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

1 1 **--watch** フラグを指定して、新規ログメッセージをインストールの進捗として監視します。この引数は任意です。

**関連情報**

- セキュリティーグループ
- アカウント全体のロールを作成する方法

## 2.8. 次のステップ

- ROSA クラスターへのアクセス

## 2.9. 関連情報

- 共有 Virtual Private Cloud (VPC) 内での ROSA クラスター設定について、詳細は ROSA クラスターの共有 VPC の設定 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。
- インタラクティブモードを使用して AWS IAM リソースとクラスターを作成するときに表示されるオプションの概要は、インタラクティブクラスター作成モードのリファレンス 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。
- 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。
- etcd 暗号化の詳細は、etcd 暗号化サービスの定義 を参照してください。
- ROSA を使用したプロキシーの設定に関する詳細は、クラスター全体のプロキシーの設定 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、クラスターデプロイメント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3章 TERRAFORM を使用した STS を使用する ROSA クラスターの作成

## 3.1. TERRAFORM を使用したデフォルトの ROSA CLASSIC 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。

**注記**

- ROSA のクイックスタートガイドについては、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。
- CLI または OpenShift Cluster Manager を使用して、デフォルトオプションを使用した ROSA クラスターをインストールするには、デフォルトオプションを使用した STS を使用する ROSA クラスターの作成 を参照してください。
- **manual** モードまたはカスタマイズを使用して ROSA クラスターをデプロイする手順については、カスタマイズを使用した STS を使用する ROSA クラスターの作成 を参照してください。

以下で説明するクラスター作成プロセスでは、次のリソースを備えた ROSA Classic AWS Security Token Service (STS) 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** を使用する OIDC プロバイダー
- 必須の Operator ロールとポリシー
- IAM アカウントロールとポリシー
- 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

**前提条件**

- STS を使用する ROSA をデプロイするための詳細な要件 を完了している。
- Terraform の前提条件 を完了している。

### 3.1.1. デフォルトのクラスター仕様の概要

**表3.1 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>**<br>• クラスター管理者ロールは作成されない |

| コンポーネント | デフォルトの仕様 |
| --- | --- |
| クラスター設定 | • デフォルトのクラスターバージョン: **4.15.0**<br>• クラスター名: **rosa-<6-digit-alphanumeric-string>**<br>• 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)<br>• ROSA CLI (**rosa**) を使用したインストールのデフォルトの AWS リージョン: **aws** CLI 設定によって定義されます。<br>• デフォルトの EC2 IMDS エンドポイント (v1 と v2 の両方) が有効になっています<br>• 可用性: データプレーンの単一ゾーン<br>• 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。<br>• 追加の etcd 暗号化が有効になっていません。<br>• 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)<br>• 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)<br>• 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)<br>• コンピュートノード数: 2<br>• 自動スケーリング: 無効<br>• 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<br>• クラスター全体のプロキシーは設定されていません。 |

| コンポーネント | デフォルトの仕様 |
| --- | --- |
| Classless Inter-Domain Routing (CIDR) の範囲 | • Machine CIDR: 10.0.0.0/16<br>• Service CIDR: 172.30.0.0/16<br>• Pod CIDR: 10.128.0.0/14<br>• 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**<br>  <br>**注記**<br>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。<br>• 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<br>• ノードドレインの 1 時間の猶予期間 |

### 3.1.2. 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。

#### 3.1.2.1. 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**

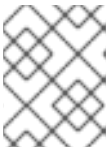
1. **オプション**: この手順の実行中、現在のディレクトリーに Terraform ファイルが作成されます。次のコマンドを実行すると、これらのファイルを保存する新しいディレクトリーを作成してそこに移動できます。

```
$ 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
```

#### 3.1.2.2. 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、**account-roles.tf** ファイルを作成します。

```
$ cat<<-EOF>account-roles.tf
data "rhcs_policies" "all_policies" {}

data "rhcs_versions" "all" {}

module "create_account_roles" {
  source  = "terraform-redhat/rosa-sts/aws"
  version = ">=0.0.15"

  create_account_roles  = true
  create_operator_roles = false

  account_role_prefix    = local.cluster_name
  path                   = var.path
  rosa_openshift_version = regex("^[0-9]+\\.[0-9]+", var.rosa_openshift_version)
  account_role_policies  = data.rhcs_policies.all_policies.account_role_policies
  all_versions           = data.rhcs_versions.all
  operator_role_policies = data.rhcs_policies.all_policies.operator_role_policies
  tags                   = var.additional_tags
}

resource "time_sleep" "wait_10_seconds" {
  depends_on = [module.create_account_roles]

  create_duration = "10s"
}
EOF
```

2. 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 = ">= 1.5.0"
      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/"]
  }
}

data "aws_availability_zones" "available" {}

locals {
  # Extract availability zone names for the specified region, limit it to 1
  region_azs = 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 {
  path = coalesce(var.path, "/")
  sts_roles = {
    role_arn         =
"arn:aws:iam::\${data.aws_caller_identity.current.account_id}:role\${local.path}\${local.cluster_n
ame}-Installer-Role",
    support_role_arn =
"arn:aws:iam::\${data.aws_caller_identity.current.account_id}:role\${local.path}\${local.cluster_n
ame}-Support-Role",
    instance_iam_roles = {
      master_role_arn =
"arn:aws:iam::\${data.aws_caller_identity.current.account_id}:role\${local.path}\${local.cluster_n
ame}-ControlPlane-Role",
      worker_role_arn =
"arn:aws:iam::\${data.aws_caller_identity.current.account_id}:role\${local.path}\${local.cluster_n
ame}-Worker-Role"
    },
    operator_role_prefix = local.cluster_name,
    oidc_config_id       = rhcs_rosa_oidc_config.oidc_config.id
  }
  worker_node_replicas = coalesce(var.worker_node_replicas, 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}")
}

data "aws_caller_identity" "current" {
}

resource "rhcs_cluster_rosa_classic" "rosa_sts_cluster" {
  name                 = local.cluster_name
  cloud_region         = var.aws_region
  multi_az             = false
  aws_account_id       = data.aws_caller_identity.current.account_id
  availability_zones   = ["us-east-1a"]
  tags                 = var.additional_tags
  version              = var.rosa_openshift_version
  compute_machine_type = var.machine_type
  replicas             = local.worker_node_replicas
  autoscaling_enabled  = false
  sts                  = local.sts_roles
  properties = {
    rosa_creator_arn = data.aws_caller_identity.current.arn
  }
  machine_cidr     = var.vpc_cidr_block

  lifecycle {
    precondition {
      condition     = can(regex("^[a-z][-a-z0-9]{0,13}[a-z0-9]\$", local.cluster_name))
      error_message = "ROSA cluster name must be less than 16 characters, be lower case
alphanumeric, with only hyphens."
    }
  }

  depends_on = [time_sleep.wait_10_seconds]
}
```

```
resource "rhcs_cluster_wait" "wait_for_cluster_build" {
  cluster = rhcs_cluster_rosa_classic.rosa_sts_cluster.id
  # timeout in minutes
  timeout = 60
}
EOF
```

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

```
$ cat<<-EOF>oidc-provider.tf
resource "rhcs_rosa_oidc_config" "oidc_config" {
  managed = true
}

data "rhcs_rosa_operator_roles" "operator_roles" {
  operator_role_prefix = local.cluster_name
  account_role_prefix  = local.cluster_name
}

module "oidc_provider" {
  source  = "terraform-redhat/rosa-sts/aws"
  version = "0.0.15"

  create_operator_roles = false
  create_oidc_provider  = true

  cluster_id                = ""
  rh_oidc_provider_thumbprint = rhcs_rosa_oidc_config.oidc_config.thumbprint
  rh_oidc_provider_url      = rhcs_rosa_oidc_config.oidc_config.oidc_endpoint_url
  tags                      = var.additional_tags
  path                      = var.path
}
EOF
```

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

```
$ cat<<-EOF>operator-roles.tf
module "operator_roles" {
  source  = "terraform-redhat/rosa-sts/aws"
  version = "0.0.15"

  create_operator_roles = true
  create_oidc_provider  = false

  rh_oidc_provider_thumbprint = rhcs_rosa_oidc_config.oidc_config.thumbprint
  rh_oidc_provider_url      = rhcs_rosa_oidc_config.oidc_config.oidc_endpoint_url
  operator_roles_properties   =
data.rhcs_rosa_operator_roles.operator_roles.operator_iam_roles
  tags                      = var.additional_tags
  path                      = var.path
}
EOF
```

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

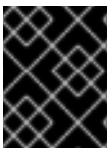
```
$ cat<<-EOF>variables.tf
variable "rosa_openshift_version" {
  type        = string
  default     = "4.15.0"
  description = "Desired version of OpenShift for the cluster, for example '4.15.0'. If version is
greater than the currently running version, an upgrade will be scheduled."
}

variable "account_role_policies" {
  description = "account role policies details for account roles creation"
  type = object({
    sts_installer_permission_policy             = string
    sts_support_permission_policy               = string
    sts_instance_worker_permission_policy       = string
    sts_instance_controlplane_permission_policy = string
  })
  default = null
}

variable "operator_role_policies" {
  description = "operator role policies details for operator roles creation"
  type = object({
    openshift_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy =
string
    openshift_cloud_network_config_controller_cloud_credentials_policy              = string
    openshift_cluster_csi_drivers_ebs_cloud_credentials_policy                      = string
    openshift_image_registry_installer_cloud_credentials_policy                    = string
    openshift_ingress_operator_cloud_credentials_policy                            = string
    openshift_machine_api_aws_cloud_credentials_policy                             = string
  })
  default = null
}

# ROSA Cluster info
variable "cluster_name" {
  default     = null
  type        = string
  description = "Provide the name of your ROSA cluster."
}

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

variable "path" {
  description = "(Optional) The arn path for the account/operator roles as well as their
policies."
  type        = string
  default     = null
}

variable "machine_type" {
```

```
  description = "The AWS instance type used for your default worker pool."
  type        = string
  default     = "m5.xlarge"
}

variable "worker_node_replicas" {
  default     = 2
  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 "autoscaling_enabled" {
  description = "Enables autoscaling. This variable requires you to set a maximum and
minimum replicas range using the 'max_replicas' and 'min_replicas' variables. If the
autoscaling_enabled is 'true', you cannot configure the worker_node_replicas."
  type        = string
  default     = "false"
}

#VPC Info
variable "vpc_cidr_block" {
  type        = string
  description = "The value of the IP address block for machines or cluster nodes for the VPC."
  default     = "10.0.0.0/16"
}

#AWS Info
variable "aws_region" {
  type    = string
  default = "us-east-1"
}
EOF
```

これで Terraform を起動する準備ができました。

#### 3.1.2.3. 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
```

4. Terraform インターフェイスに、作成または変更されるリソースがリストされ、確認のプロンプトが表示されます。続行するには **yes** を入力し、キャンセルするには **no** を入力します。

**出力例**

```
Plan: 39 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.

  Enter a value: yes
```

**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、および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-ControlPlane-Role               Control plane  arn:aws:iam::<ID>:role/ROSA-
demo-ControlPlane-Role               4.14             No
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      6
```

#### 3.1.2.4. 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
```

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。

**Terraform の確認の出力例:**

```
Plan: 0 to add, 0 to change, 39 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
```

# 第4章 インタラクティブなクラスター作成モードリファレンス

このセクションでは、インタラクティブモードで、ROSA CLI (**rosa**) を使用して OCM ロール、ユーザーロール、および Red Hat OpenShift Service on AWS (ROSA) クラスターを作成するときに表示されるオプションの概要を説明します。

## 4.1. 対話型 OCM およびユーザーロール作成モードのオプション

Red Hat OpenShift Cluster Manager で、OCM とユーザーロールを作成してリンクすることで、AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する前に、AWS アカウントを Red Hat 組織に関連付ける必要があります。**rosa create ocm-role** コマンドまたは **rosa create user-role** コマンドの実行時に **--interactive** オプションを指定することで、インタラクティブモードを有効にできます。

次の表に、対話型 OCM ロール作成モードのオプションを示します。

**表4.1 --interactive OCM ロール作成モードオプション**

| フィールド | 説明 |
|---|---|
| **Role prefix** | OCM IAM ロール名に含める接頭辞を指定します。デフォルトは **ManagedOpenShift** です。Red Hat 組織の AWS アカウントごとに OCM ロールを 1 つだけ作成できます。 |
| **OCM ロールの管理者機能の有効化 (オプション)** | admin OCM IAM ロールの有効化 (**--admin** 引数を指定するのと同等)**auto** モードで、OpenShift Cluster Manager を使用してクラスター固有の Operator ロールと OIDC プロバイダーを自動的にプロビジョニングする場合は、管理者ロールが必要です。 |
| **パーミッション境界 ARN (オプション)** | OCM ロールのパーミッション境界 Amazon Resource Name (ARN) を指定します。詳細は、AWS ドキュメントの IAM エンティティーのアクセス許可の境界 を参照してください。 |
| **ロールのパス (オプション)** | OCM ロールのカスタム ARN パスを指定します。パスには英数字のみを使用し、/ で開始および終了する必要があります (例: **/test/path/dev/**)。詳細は、**IAM ロールとポリシーの ARN パスのカスタマイズ** を参照してください。 |
| **ロール作成モード** | ロール作成モードを選択します。**auto** モードを使用して OCM ロールを自動的に作成し、それを Red Hat 組織アカウントにリンクできます。**manual** モードでは、**rosa** CLI はロールの作成とリンクに必要な **aws** コマンドを生成します。**manual** モードでは、対応するポリシー JSON ファイルも現在のディレクトリーに保存されます。**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。 |
| **<ocm_role_name> ロールを作成しますか?** | OCM ロールを作成するかどうかを確認します。 |
| **<ocm_role_arn> ロールを組織 <red_hat_organization_id> にリンクしますか?** | OCM ロールを Red Hat 組織にリンクするかどうかを確認します。 |

次の表では、インタラクティブなユーザーロール作成モードのオプションについて説明します。

**表4.2 --interactive ユーザーロール作成モードオプション**

| フィールド | 説明 |
| --- | --- |
| **Role prefix** | ユーザーロール名に含める接頭辞を指定します。デフォルトは **ManagedOpenShift** です。 |
| **パーミッション境界 ARN (オプション)** | ユーザーロールのパーミッション境界 Amazon Resource Name (ARN) を指定します。詳細は、AWS ドキュメントの IAM エンティティーのアクセス許可の境界 を参照してください。 |
| **ロールのパス (オプション)** | ユーザーロールのカスタム ARN パスを指定します。パスには英数字のみを使用し、/ で開始および終了する必要があります (例: **/test/path/dev/**)。詳細は、**IAM ロールとポリシーの ARN パスのカスタマイズ** を参照してください。 |
| **ロール作成モード** | ロール作成モードを選択します。**auto** モードを使用して、ユーザーロールを自動的に作成し、OpenShift Cluster Manager ユーザーアカウントにリンクすることができます。**manual** モードでは、ROSA CLI はロールの作成とリンクに必要な **aws** コマンドを生成します。**manual** モードでは、対応するポリシー JSON ファイルも現在のディレクトリーに保存されます。**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。 |
| **<user_role_name> ロールを作成しますか?** | ユーザーロールを作成するかどうかを確認します。 |
| **<user_role_arn> ロールを <red_hat_user_account_id> アカウントにリンクしますか?** | ユーザーロールを Red Hat ユーザーアカウントにリンクするかどうかを確認します。 |

## 4.2. 対話型クラスター作成モードのオプション

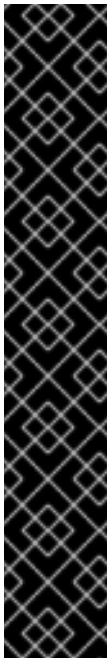
インタラクティブモードを使用して AWS Security Token Service (STS) で Red Hat OpenShift Service on AWS クラスターを作成できます。**rosa create cluster** コマンドの実行時に **--interactive** オプションを指定することで、モードを有効にできます。

次の表では、対話型クラスター作成モードのオプションについて説明します。

**表4.3 --interactive クラスター作成モードオプション**

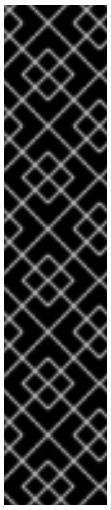
| フィールド | 説明 |
| --- | --- |
| **Cluster name** | クラスターの名前を入力します (例: **my-rosa-cluster**)。 |
| **Domain prefix** | クラスターのサブドメインのドメイン接頭辞の名前を入力します (例: **my-rosa-cluster)**。 |

| フィールド | 説明 |
| --- | --- |
| **Deploy cluster with Hosted Control Plane (optional)** | Hosted Control Plane の使用を有効にします。 |
| **Create cluster admin user** | htpasswd ID プロバイダーを使用してクラスターを作成するときに、クラスター管理者ユーザーを作成します。ユーザー名には、/、**:**、または **%** を含めることはできません。パスワードは空白を含まない 14 文字以上 (ASCII 標準) である必要があります。 |
| **Deploy cluster using AWS STS** | AWS Security Token Service (STS) を使用して、コンポーネント固有の AWS Identity and Access Management (IAM) ロールについて一時的な制限付き権限の認証情報を割り当てる OpenShift クラスターを作成します。サービスを使用すると、クラスターコンポーネントはセキュアなクラウドリソース管理プラクティスを使用して AWS API 呼び出しを実行できます。デフォルトは **Yes** です。 |
| **OpenShift のバージョン** | インストールする OpenShift のバージョンを選択します (例: 4)。デフォルトは最新のバージョンです。 |
| **Configure the use of IMDSv2 for ec2 instances optional/required (optional)** | すべての EC2 インスタンスが EC2 Instance Metadata Service (IMDS) の v1 と v2 エンドポイントの両方を使用する (オプション) か、IMDSv2 のみを使用する (必須) かを指定します。 |
| **Installer role ARN** | クラスターバージョンの AWS アカウントに複数のアカウントロールセットがある場合は、インストーラーロール ARN のリストが表示されます。クラスターで使用するインストーラーロールの ARN を選択します。クラスターは、選択したインストーラーロールに関連するアカウント全体のロールとポリシーを使用します。 |
| **External ID (optional)** | アカウントロールが仮定される際に OpenShift Cluster Manager および OpenShift インストーラーによって渡される一意の識別子を指定します。このオプションは、外部 ID を予想されるカスタムアカウントロールにのみ必要です。 |
| **Operator roles prefix** | クラスター固有の Operator IAM ロールに割り当てる接頭辞を入力します。デフォルトはクラスターの名前であり、4 桁のランダムな文字列です (例: **my-rosa-cluster-a0b1**)。 |
| **Deploy cluster using pre registered OIDC Configuration ID** | 事前設定された OIDC 設定を使用するか、クラスター作成プロセスの一部として新しい OIDC 設定を作成するかを指定します。 |

| フィールド | 説明 |
| --- | --- |
| **Tags (optional)** | Red Hat OpenShift Service on AWS が作成した AWS 内のすべてのリソースで使用するタグを指定します。タグは、AWS 内のリソースの管理、識別、整理、検索、フィルタリングに使用できます。タグはコンマで区切られます (例: "key value、foo bar")。<br>  <br>**重要**<br>Red Hat OpenShift Service on AWS は、クラスター作成時に Red Hat OpenShift リソースへのカスタムタグのみをサポートします。タグを追加すると、削除したり編集したりすることはできません。Red Hat が追加したタグは、クラスターが Red Hat の実稼働サービスレベルアグリーメント (SLA) への準拠を維持するために必要です。これらのタグは削除してはいけません。<br>Red Hat OpenShift Service on AWS では、ROSA クラスターマネージドリソース以外へのタグの追加はサポートされていません。AWS リソースが ROSA クラスターによって管理されている場合、これらのタグが失われる可能性があります。このような場合、タグを調整してそのままの状態に保つためのカスタムソリューションまたはツールが必要になる可能性があります。 |
| **Multiple availability zones (optional)** | クラスターを AWS リージョンの複数のアベイラビリティーゾーンにデプロイします。デフォルトは **No** で、クラスターは単一のアベイラビリティーゾーンにデプロイされます。クラスターを複数のアベイラビリティーゾーンにデプロイする場合、AWS リージョンには少なくとも 3 つのアベイラビリティーゾーンが必要です。実稼働環境のワークロードには、複数のアベイラビリティーゾーンの使用が推奨されます。 |
| **AWS region** | クラスターをデプロイする AWS リージョンを指定します。これにより、**AWS_REGION** 環境変数が上書きされます。 |
| **PrivateLink cluster (optional)** | AWS PrivateLink を使用してクラスターを作成します。このオプションは、トラフィックをパブリックインターネットに公開することなく、Virtual Private Cloud (VPC)、AWS サービス、およびオンプレミスネットワーク間のプライベート接続を提供します。サポートを提供するために、Red Hat Site Reliability Engineering (SRE) は AWS PrivateLink Virtual Private Cloud (VPC) エンドポイントを使用してクラスターに接続できます。このオプションは、クラスターの作成後に変更できません。デフォルトは **No** です。 |

| フィールド | 説明 |
| --- | --- |
| **Machine CIDR** | マシン (クラスターノード) の IP アドレス範囲を指定します。この IP アドレス範囲は、VPC サブネットのすべての CIDR アドレス範囲を包含する必要があります。サブネットは連続している必要があります。単一のアベイラビリティーゾーンデプロイメントでは、サブネット接頭辞 **/25** を使用した 128 アドレスの最小 IP アドレス範囲がサポートされます。サブネット接頭辞 **/24** を使用する最小アドレス範囲 256 アドレスの範囲は、複数のアベイラビリティーゾーンを使用するデプロイメントでサポートされます。デフォルトは **10.0.0.0/16** です。この範囲は、接続されているネットワークと競合しないようにする必要があります。 |
| **Service CIDR** | サービスの IP アドレス範囲を指定します。必須ではありませんが、クラスター間でアドレスブロックを同じにすることが推奨されます。これにより、IP アドレスの競合が発生することはありません。範囲は、ワークロードに対応するのに十分な大きさである必要があります。アドレスブロックは、クラスター内からアクセスする外部サービスと重複してはいけません。デフォルトは **172.30.0.0/16** です。 |
| **Pod CIDR** | Pod の IP アドレス範囲を指定します。必須ではありませんが、クラスター間でアドレスブロックを同じにすることが推奨されます。これにより、IP アドレスの競合が発生することはありません。範囲は、ワークロードに対応するのに十分な大きさである必要があります。アドレスブロックは、クラスター内からアクセスする外部サービスと重複してはいけません。デフォルトは **10.128.0.0/14** です。 |
| **Install into an existing VPC (optional)** | クラスターを既存の AWS VPC にインストールします。このオプションを使用するには、VPC にはクラスターをインストールする各アベイラビリティーゾーンの 2 つのサブネットが必要です。デフォルトは **No** です。 |
| **Select availability zones (optional)** | 既存の AWS VPC にインストールするときに使用するアベイラビリティーゾーンを指定します。コンマ区切りのリストを使用して、可用性ゾーンを提供します。**No** を指定すると、インストーラーは可用性ゾーンを自動的に選択します。 |
| **Enable customer managed key (optional)** | このオプションを有効にすると、特定の AWS Key Management Service (KMS) キーを永続データの暗号化キーとして使用できます。このキーは、コントロールプレーン、インフラストラクチャー、およびワーカーノードのルートボリュームの暗号化キーとして使用されます。キーは、デフォルトのストレージクラスで作成された永続ボリュームが特定の KMS キーで暗号化されるように、デフォルトのストレージクラスでも設定されます。これを無効にすると、永続データが常に暗号化されるように、指定されたリージョンのアカウント KMS キーがデフォルトで使用されます。デフォルトは **No** です。 |

| フィールド | 説明 |
| --- | --- |
| **Compute nodes instance type** | コンピュートノードのインスタンスタイプを選択します。デフォルトは **m5.xlarge** です。 |
| **Enable autoscaling (optional)** | コンピュートノードの自動スケーリングを有効にします。Autoscaler は、デプロイメントの需要に合わせてクラスターのサイズを調整します。デフォルトは **No** です。 |
| **Additional Compute Security Group IDs (optional)** | クラスターと一緒に作成される標準マシンプールで使用する追加のカスタムセキュリティーグループの ID を選択します。デフォルトでは何も選択されていません。選択した VPC に関連付けられたセキュリティーグループのみが表示されます。追加のセキュリティーグループを最大 5 つ選択できます。 |
| **Additional Infra Security Group IDs (optional)** | クラスターと一緒に作成されるインフラノードで使用する追加のカスタムセキュリティーグループの ID を選択します。デフォルトでは何も選択されていません。選択した VPC に関連付けられたセキュリティーグループのみが表示されます。追加のセキュリティーグループを最大 5 つ選択できます。 |
| **Additional Control Plane Security Group IDs (optional)** | クラスターと一緒に作成されるコントロールプレーンノードで使用する追加のカスタムセキュリティーグループの ID を選択します。デフォルトでは何も選択されていません。選択した VPC に関連付けられたセキュリティーグループのみが表示されます。追加のセキュリティーグループを最大 5 つ選択できます。 |
| **Compute nodes** | 各アベイラビリティーゾーンにプロビジョニングするコンピュートノードの数を指定します。単一アベイラビリティーゾーンにデプロイされたクラスターには、2 つ以上のノードが必要です。複数のゾーンにデプロイされるクラスターには 3 つ以上のノードが必要です。ワーカーノードの最大数は 180 ノードです。デフォルト値は **2** です。 |
| **Default machine pool labels (optional)** | デフォルトのマシンプールのラベルを指定します。ラベルの形式は、キーと値のペアのコンマ区切りリストにする必要があります。このリストは、ノードのラベルに継続的に加えられた変更を上書きします。 |
| **Host prefix** | 個々のマシンにスケジューリングされた Pod に割り当てるサブネット接頭辞の長さを指定します。ホスト接頭辞は、各マシンの Pod IP アドレスプールを決定します。例えば、ホスト接頭辞を **/23** に設定した場合、各マシンには Pod CIDR アドレス範囲から **/23** のサブネットが割り当てられます。デフォルトは **/23** で、クラスターノード数は 512、ノードあたりの Pod 数は 512 となっていますが、いずれも当社がサポートする最大値を超えています。サポートされている最大値については、以下の関連情報のセクションを参照してください。 |

| フィールド | 説明 |
| --- | --- |
| **Machine pool root disk size (GiB or TiB)** | マシンプールのルートディスクのサイズを指定します。この値には、GiB や TiB などの単位接尾辞を含める必要があります (デフォルト値の **300GiB** など)。 |
| **Enable FIPS support (optional)** | FIPS モードを有効または無効にします。デフォルトは **false** (無効) です。FIPS モードが有効になっている場合、Red Hat OpenShift Service on AWS が実行される Red Hat Enterprise Linux CoreOS (RHCOS) マシンは、デフォルトの Kubernetes 暗号化スイートをバイパスし、代わりに RHCOS で提供される暗号化モジュールを使用します。<br><br>  <br>**重要**<br><br>クラスターで FIPS モードを有効にするには、FIPS モードで動作するように設定された {op-system-base-full} コンピューターからインストールプログラムを実行する必要があります。RHEL での FIPS モードの設定の詳細は、FIPS モードでのシステムのインストール を参照してください。FIPS モードでブートされた {op-system-base-full} または Red Hat Enterprise Linux CoreOS (RHCOS) を実行する場合、Red Hat OpenShift Service on AWS コアコンポーネントは、x86_64、ppc64le、および s390x アーキテクチャーのみで、FIPS 140-2/140-3 検証のために NIST に提出された {op-system-base} 暗号化ライブラリーを使用します。 |
| **Encrypt etcd data (optional)** | Red Hat Open Shift Service on AWS では、コントロールプレーンストレージはデフォルトで静止時に暗号化され、これには etcd ボリュームの暗号化も含まれます。さらに、**Encrypt etcd data** オプションを有効にすると、鍵ではなく、etcd 内の一部のリソースの鍵の値を暗号化することができます。<br><br>  <br>**重要**<br><br>etcd のキー値の etcd 暗号化を有効にすると、約 20% のパフォーマンスのオーバーヘッドが発生します。このオーバーヘッドは、etcd ボリュームを暗号化するデフォルトのコントロールプレーンのストレージ暗号化に加えて、この 2 つ目の暗号化レイヤーの導入により生じます。Red Hat は、お客様のユースケースで特に etcd 暗号化が必要な場合にのみ有効にすることを推奨します。 |
| **ワークロードの監視を無効にする (オプション)** | ユーザー定義プロジェクトの監視を無効にします。ユーザー定義プロジェクトの監視はデフォルトで有効にされます。 |

| フィールド | 説明 |
| --- | --- |
| **Route Selector for ingress (optional)** | Ingress のルートセレクターを指定します。形式は、キーと値のペアのコンマ区切りリストにする必要があります。ラベルを指定しない場合、すべてのルートは両方のルーターで公開されます。従来の Ingress サポートの場合、これらのラベルは包含ラベルです。それ以外の場合は、除外ラベルとして扱われます。 |
| **Excluded namespaces for ingress (optional)** | Ingress の除外された namespace を指定します。形式はコンマ区切りのリスト **value1、value2...** である必要があります。値を指定しない場合、すべての namespace が公開されます。 |
| **Wildcard Policy (任意: 'Skip' で選択を省略します。デフォルト値は入力されています)** | Ingress のワイルドカードポリシーを選択します。オプションは **WildcardsDisallowed** および **WildcardsAllowed** です。デフォルトは **WildcardsDisallowed** です。 |
| **Namespace Ownership Policy (任意: 'Skip' で選択を省略します。デフォルト値は入力されています)** | Ingress の namespace 所有権ポリシーを選択します。オプションは **Strict** および **InterNamespaceAllowed** です。デフォルトは **Strict** です。 |

## 4.3. 関連情報

- OCM ロール、ユーザーロール、およびアカウント全体のロールにカスタム ARN パスを使用する方法の詳細は、IAM ロールおよびポリシーの ARN パスのカスタマイズ を参照してください。
- サポートされている最大値のリストについては、ROSA tested cluster maximums を参照してください。
- AWS IAM リソースを含め、STS を使用する ROSA クラスターをすばやく作成するための詳細な手順は、デフォルトオプションを使用した STS を使用する ROSA クラスターの作成 を参照してください。
- AWS IAM リソースを含め、STS を使用する ROSA クラスターをカスタマイズを使用して作成する詳細な手順は、カスタマイズを使用した STS を使用する ROSA クラスターの作成 を参照してください。
- etcd 暗号化の詳細は、etcd 暗号化サービスの定義 を参照してください。
- VPC アーキテクチャーの例は、こちらのサンプル VPC アーキテクチャー を参照してください。

# 第5章 ROSA での AWS PRIVATELINK クラスターの作成

本書では、AWS PrivateLink を使用して ROSA クラスターを作成する方法を説明します。

## 5.1. AWS PRIVATELINK について

Red Hat OpenShift Service on AWS クラスターは、パブリックサブネット、インターネットゲートウェイ、またはネットワークアドレス変換 (NAT) ゲートウェイに要件なしに作成できます。この設定では、Red Hat は AWS PrivateLink を使用してクラスターを管理および監視し、すべてのパブリック Ingress ネットワークトラフィックを回避します。パブリックサブネットがないと、アプリケーションルーターをパブリックとして設定することはできません。プライベートアプリケーションルーターを設定することが唯一のオプションです。

詳細は、AWS の Web サイトの AWS PrivateLink を参照してください。

**重要**

PrivateLink クラスターは、インストール時にのみ作成できます。インストール後にクラスターを PrivateLink に変更することはできません。

## 5.2. AWS PRIVATELINK クラスターの使用要件

AWS PrivateLink クラスターの場合は、インターネットゲートウェイ、NAT ゲートウェイ、およびパブリックサブネットは必要ありませんが、必要なコンポーネントをインストールするには、プライベートサブネットにインターネット接続が必要です。Single-AZ クラスターと Multi-AZ クラスターには、それぞれにプライベートサブネットが少なくとも 1 つまたは 3 つ必要です。以下の表は、インストールを成功させるために必要な AWS リソースを示しています。

**表5.1 必要な AWS リソース**

| コンポーネント | AWS タイプ | 説明 |
| --- | --- | --- |
| VPC | • AWS::EC2::VPC<br>• AWS::EC2::VPCEndpoint | 使用するクラスターの VPC を指定する必要があります。 |

<table>
<tr><th>コンポーネント</th><th>AWS タイプ</th><th>説明</th></tr>
<tr><td>ネットワークアクセス制御</td><td><ul><li>AWS::EC2::NetworkAcl</li><li>AWS::EC2::NetworkAclEntry</li></ul></td><td>以下のポートへのアクセスを許可する必要があります。<table><tr><th>ポート</th><th>理由</th></tr><tr><td>80</td><td>受信 HTTP トラフィック</td></tr><tr><td>443</td><td>受信 HTTPS トラフィック</td></tr><tr><td>22</td><td>受信 SSH トラフィック</td></tr><tr><td>1024-65535</td><td>受信一時 (ephemeral) トラフィック</td></tr><tr><td>0-65535</td><td>送信一時 (ephemeral) トラフィック</td></tr></table></td></tr>
<tr><td>プライベートサブネット</td><td><ul><li>AWS::EC2::Subnet</li><li>AWS::EC2::RouteTable</li><li>AWS::EC2::SubnetRouteTableAssociation</li></ul></td><td>VPC には、Single-AZ デプロイメントの場合は 1 つのアベイラビリティーゾーン、Multi-AZ デプロイメントの場合は 3 つのアベイラビリティーゾーンに、プライベートサブネットが必要です。適切なルートおよびルートテーブルを指定する必要があります。</td></tr>
</table>

## 5.3. AWS PRIVATELINK クラスターの作成

Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) を使用して AWS PrivateLink クラスターを作成できます。

**注記**

AWS PrivateLink は既存の VPC でのみサポートされます。

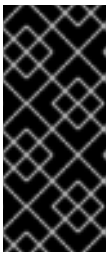
**前提条件**

- 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**

クラスターの作成には最長で 40 分かかる場合があります。

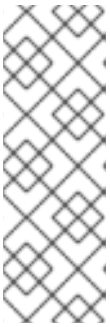
1. AWS PrivateLink を使用すると、1 つのアベイラビリティーゾーン (Single-AZ) または複数のアベイラビリティーゾーン (Multi-AZ) でクラスターを作成できます。いずれの場合も、マシンのクラスレスのドメイン内ルーティング (CIDR) は、仮想プライベートクラウドの CIDR と一致させる必要があります。詳細は、独自の VPC を使用するための要件 および VPC 検証 を参照してください。



**重要**

ファイアウォールを使用する場合は、Red Hat OpenShift Service on AWS が機能するために必要なサイトにアクセスできるように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。



**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。

- Single-AZ クラスターを作成するには、以下を実行します。

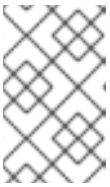
```
$ rosa create cluster --private-link --cluster-name=<cluster-name> [--machine-cidr=<VPC CIDR>/16] --subnet-ids=<private-subnet-id>
```

- Multi-AZ クラスターを作成するには、以下を実行します。

```
$ rosa create cluster --private-link --multi-az --cluster-name=<cluster-name> [--machine-cidr=<VPC CIDR>/16] --subnet-ids=<private-subnet-id1>,<private-subnet-id2>,<private-subnet-id3>
```

2. 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。クラスターの作成時に、出力の **State** フィールドは **pending** から **installing** に移行し、最終的に **ready** に移行します。

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



**注記**

インストールが失敗した場合や、40 分後に **State** フィールドが **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に関するドキュメントで詳細を確認してください。

3. 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
```

## 5.4. AWS PRIVATELINK DNS 転送の設定

AWS PrivateLink クラスターを使用すると、パブリックホストゾーンとプライベートホストゾーンが Route53 に作成されます。プライベートホストゾーンでは、ゾーン内のレコードは、割り当てられている VPC 内からのみ解決できます。

**Let's Encrypt DNS-01** 検証では、ドメインに対して有効で公的に信頼されている証明書を発行できるように、パブリックゾーンが必要です。**Let's Encrypt** の検証が完了すると、検証レコードは削除されます。ただし、これらの証明書を発行および更新するには、ゾーンが引き続き必要です。これらの証明書は通常、60 日ごとに必要です。これらのゾーンは通常空のように見えますが、検証プロセスで重要なロールを果たしています。

プライベートホストゾーンの詳細は、AWS プライベートホストゾーンのドキュメント を参照してください。パブリックホストゾーンの詳細は、AWS パブリックホストゾーンのドキュメント を参照してください。

**前提条件**

- 企業ネットワークまたは他の VPC に接続性がある。
- UDP ポート 53 と TCP ポート 53 は、DNS クエリーを可能にするためにネットワーク全体で有効になっている。
- Red Hat OpenShift Service on AWS を使用して AWS PrivateLink クラスターを作成している。

**手順**

1. **api.<cluster_domain>**、***.apps.<cluster_domain>** などのレコードが VPC の外部で解決できるようにするには、Route 53 Resolver Inbound Endpoint を設定 します。
2. インバウンドエンドポイントを設定するときは、クラスターの作成時に使用された VPC とプライベートサブネットを選択します。
3. エンドポイントが動作可能になり、関連付けられたら、DNS クエリーを **drow-pl-01.htno.p1.openshiftapps.com** などの最上位クラスタードメインの IP アドレスに転送するように企業ネットワークを設定します。
4. ある VPC から別の VPC に DNS クエリーを転送する場合は、転送ルールを設定 します。
5. リモートネットワーク DNS サーバーを設定している場合は、特定の DNS サーバーのドキュメントを参照して、インストールされているクラスタードメインの選択的 DNS 転送を設定してください。

## 5.5. 次のステップ

アイデンティティープロバイダーの設定

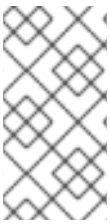
## 5.6. 関連情報

- 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

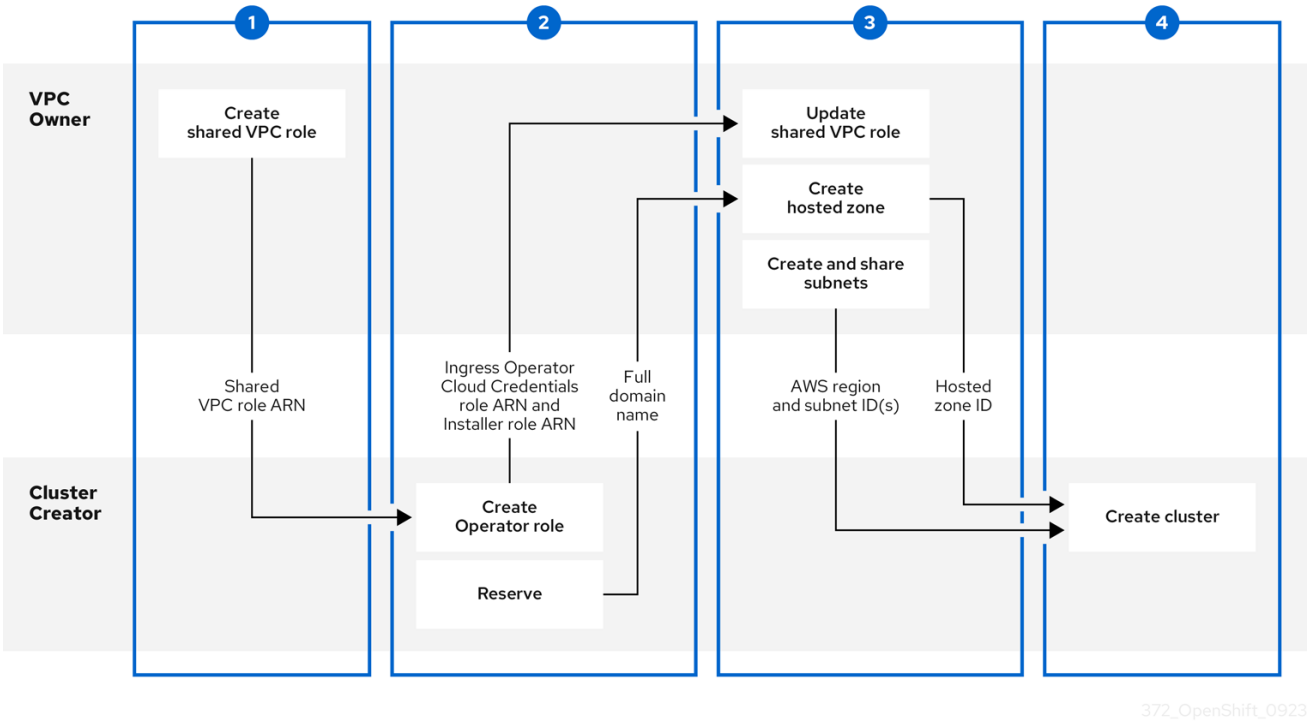
# 第6章 ROSA クラスターの共有 VPC の設定

一元管理された共有 AWS Virtual Private Cloud (VPC) 内に Red Hat OpenShift Service on AWS (ROSA) クラスターを作成できます。



**注記**

このプロセスには、同じ AWS 組織に属する **2 つの別々の** AWS アカウントが必要です。1 つのアカウントは VPC 所有の AWS アカウント (**VPC Owner**) として機能し、もう 1 つのアカウントはクラスターを作成する AWS アカウント (**Cluster Creator**) でクラスターを作成します。




### VPC Owner の前提条件

- ロールを作成し、リソースを共有するための適切な権限を持つ AWS アカウントがある。
- **Cluster Creator** の AWS アカウントは、**VPC Owner** の AWS アカウントとは別である。
- どちらの AWS アカウントも、同じ AWS 組織に属している。
- 組織の管理アカウントからのリソース共有を有効にしている。
- AWS console にアクセスできる。

### Cluster Creator の前提条件

- ROSA CLI (**rosa**) 1.2.26 以降がインストールされている。
- クラスター作成に必要な ROSA アカウントロール をすべて作成している。
- **Cluster Creator** の AWS アカウントは、**VPC Owner** の AWS アカウントとは別である。

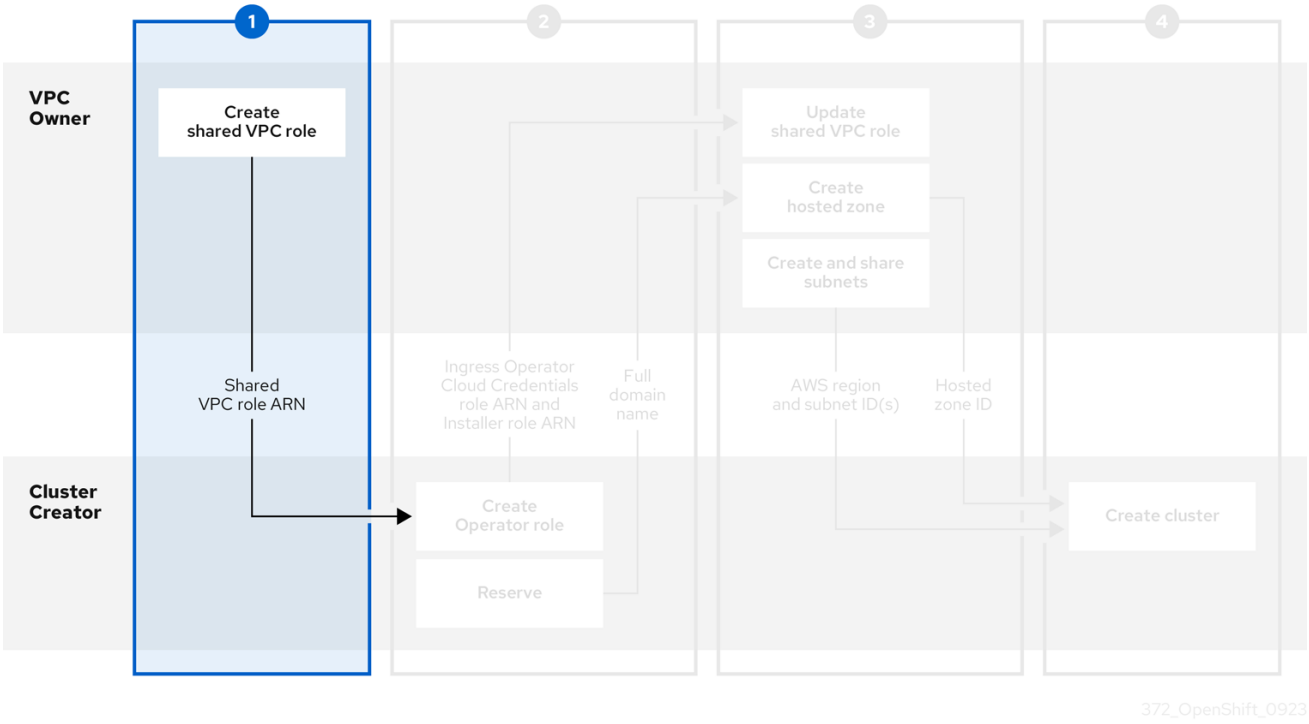
- どちらの AWS アカウントも、同じ AWS 組織に属している。

**注記**

共有 VPC へのクラスターのインストールは、OpenShift 4.12.34 以降、4.13.10 以降、および今後の全 4.y ストリームでのみサポートされます。

## 6.1. ステップ 1: VPC OWNER: AWS 組織内で共有するための VPC の設定

アカウントが現在の AWS 組織内にある場合、設定済みの VPC 内のサブネットを別の AWS ユーザーアカウントで共有できます。




**手順**

1. AWS コンソールの VPC セクション で、仕様に合わせて VPC を作成または変更します。
2. **SharedVPCPolicy という** 名前を使用する必要な共有 VPC 権限を許可するカスタムポリシーファイルを作成します。

```
$ cat <<EOF > /tmp/shared-vpc-policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:ChangeResourceRecordSets",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53:ChangeTagsForResource",
                "route53:GetAccountLimit",
```

```
                "route53:GetChange",
                "route53:GetHostedZone",
                "route53:ListTagsForResource",
                "route53:UpdateHostedZoneComment",
                "tag:GetResources",
                "tag:UntagResources"
            ],
            "Resource": "*"
        }
    ]
}
EOF
```

3. AWS でポリシーを作成します。

```
$ aws iam create-policy \
    --policy-name SharedVPCPolicy \
    --policy-document file:///tmp/shared-vpc-policy.json
```

このポリシーを、共有 VPC 権限に必要なロールに割り当てます。

4. ロールを引き受けるパーミッションを付与するカスタム信頼ポリシーファイルを作成します。

```
$ cat <<EOF > /tmp/shared-vpc-role.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<Account-ID>:root"  (1)
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
```

(1) **Cluster Creator** が必要なクラスターロールを作成した後、プリンシパルのスコープを減らして設定されます。作成時に、**クラスター作成者の** AWS アカウント ID を **arn:aws:iam::{Account}:root** として使用して、root ユーザープレースホルダーを作成する必要があります。

5. IAM ロールを作成します。

```
$ aws iam create-role --role-name <role_name> \  (1)
    --assume-role-policy-document file:///tmp/shared-vpc-role.json
```

(1) **<role_name>** は、作成するロールの名前に置き換えます。

6. カスタムの **SharedVPPColicy** パーミッションポリシーを割り当てます。

```
$ aws iam attach-role-policy --role-name <role_name> --policy-arn \ 1
  arn:aws:iam::<AWS_account_ID>:policy/SharedVPCPolicy 2
```

1. **<role_name>** は、作成したロールの名前に置き換えます。
2. **<AWS_account_ID>** は、**VPC Owner** の AWS アカウント ID に置き換えます。

7. **SharedVPCRole** ARN を **Cluster Creator** に指定して、設定を続行します。

**関連情報**

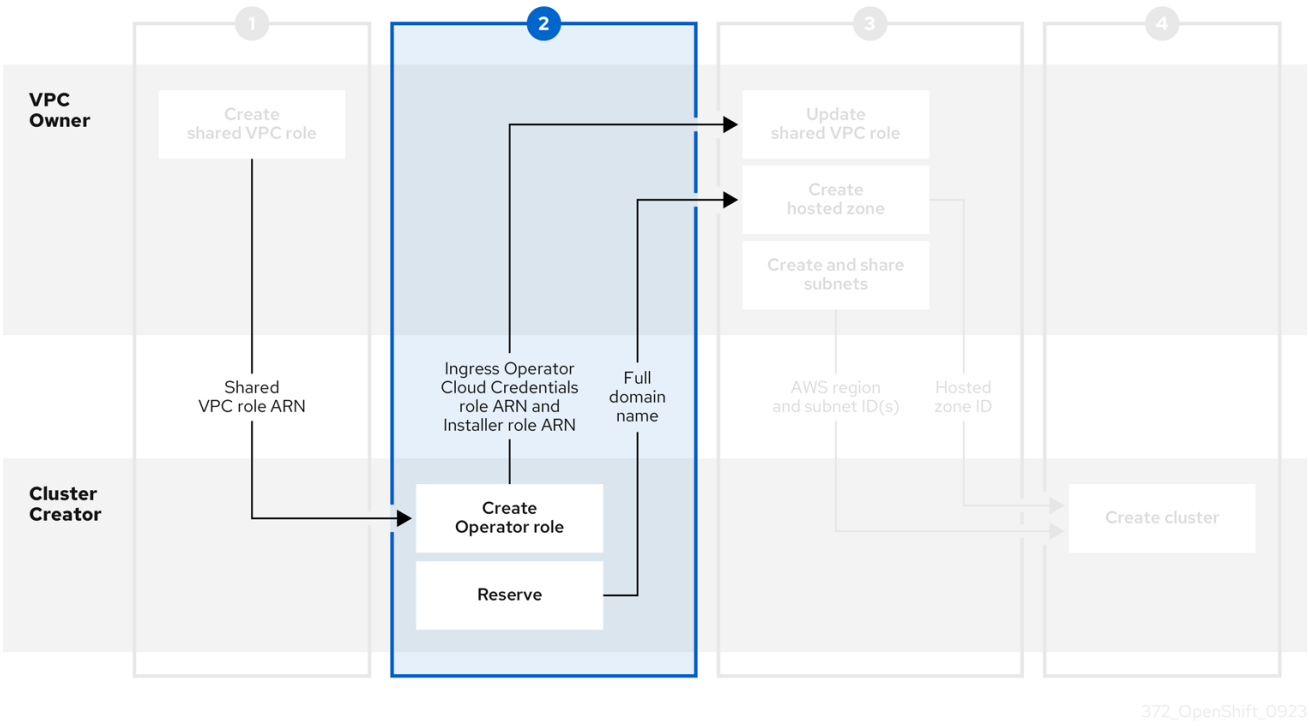
- AWS リソースの共有 については、AWS のドキュメントを参照してください。

## 6.2. ステップ 2: CLUSTER CREATOR: DNS の予約およびクラスター OPERATOR ロールの作成

**VPC Owner** が VPC リソースを共有するための仮想プライベートクラウド、サブネット、および IAM ロールを作成した後、**openshiftapps.com** DNS ドメインを予約し、**VPC Owner** に通信するための Operator ロールを作成します。

**注記**

共有 VPC クラスターの場合は、クラスター作成手順の後に Operator ロールを作成することもできます。クラスターは、Ingress Operator のロール ARN が共有 VPC ロールの信頼関係に追加されるまで **waiting** 状態になります。




**前提条件**

- **VPC Owner** から IAM ロールの **SharedVPCRole** ARN を取得している。

**手順**

1. 以下のコマンドを使用して **openshiftapps.com** DNS ドメインを予約します。

```
$ rosa create dns-domain
```

このコマンドは、予約済みの **openshiftapps.com** DNS ドメインを作成します。

```
I: DNS domain '14eo.p1.openshiftapps.com' has been created.
I: To view all DNS domains, run 'rosa list dns-domains'
```

2. OIDC 設定を作成します。
OIDC 設定プロセス の詳細は、この記事を確認してください。次のコマンドは、必要な OIDC 設定 ID を生成します。

```
$ rosa create oidc-config
```

コマンドが OIDC 設定を作成したことを確認します。

```
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
25tu67hq45rto1am3slpf5lq6jargg
```

3. 次のコマンドを入力して、Operator ロールを作成します。

```
$ rosa create operator-roles --oidc-config-id <oidc-config-ID> (1)
   --installer-role-arn <Installer_Role> (2)
   --shared-vpc-role-arn <Created_VPC_Role_Arn> (3)
   --prefix <operator-prefix> (4)
```

(1) 前の手順で作成した OIDC 設定 ID を指定します。

(2) **rosa create account-roles** プロセスの一部として作成されたインストーラー ARN を指定します。

(3) **VPC Owner** が作成したロールの ARN を指定します。

(4) Operator ロールの接頭辞を指定します。

**注記**

インストーラーアカウントのロールと共有 VPC ロールには 1 対 1 の関係が必要です。複数の共有 VPC ロールを作成する場合は、共有 VPC ロールごとに 1 セットのアカウントロールを作成する必要があります。

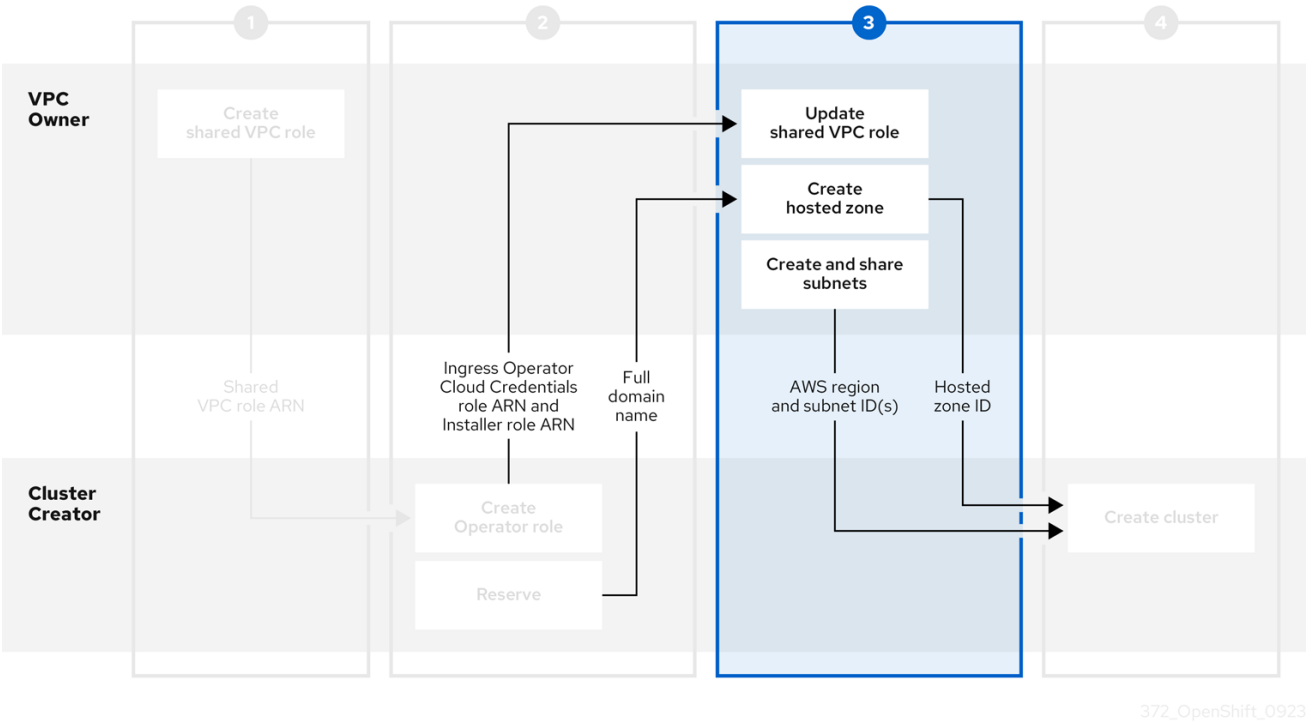
4. Operator ロールを作成したら、**<intended_cluster_name>.<reserved_dns_domain>** と指定して作成された完全なドメイン名、**Ingress Operator Cloud Credentials** ロールの ARN、および **Installer** ロールの ARN を **VPC Owner** と共有して、設定を続行します。
共有情報は、以下のようになります。

- **my-rosa-cluster.14eo.p1.openshiftapps.com**

- **arn:aws:iam::111122223333:role/ManagedOpenShift-Installer-Role**
- **arn:aws:iam::111122223333:role/my-rosa-cluster-openshift-ingress-operator-cloud-credentials**

## 6.3. ステップ 3: VPC OWNER: 共有 VPC ロールの更新とホストゾーンの作成

**Cluster Creator** が DNS ドメインと IAM ロールを指定した後に、プライベートホストゾーンを作成し、VPC を共有するために作成された IAM ロールの信頼ポリシーを更新します。




**前提条件**

- **Cluster Creator** からの完全なドメイン名を取得している。
- **Ingress Operator Cloud Credentials** ロールの ARN を **Cluster Creator** から取得している。
- **インストーラー** ロールの ARN を **Cluster Creator** から取得している。

**手順**

1. AWS console の Resource Access Manager で、**Cluster Creator** の AWS アカウント ID を使用して、以前に作成したパブリックおよびプライベートサブネットを共有するリソース共有を作成します。
2. VPC 共有 IAM ロールを更新し、**Installer** および **Ingress Operator Cloud Credentials** ロールを信頼ポリシーの principal セクションに追加します。

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

```
    "Sid": "Statement1",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
           "arn:aws:iam::<Cluster-Creator's-AWS-Account-ID>:role/<prefix>-ingress-operator-
cloud-credentials",
           "arn:aws:iam::<Cluster-Creator's-AWS-Account-ID>:role/<prefix>-Installer-Role"
         ]
    },
    "Action": "sts:AssumeRole"
  }
   ]
}
```

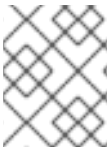
3. AWS console の Route 53 セクション でプライベートホストゾーンを作成します。ホストゾーン設定でのドメイン名は **<cluster_name>.<reserved_dns_domain>** です。プライベートホストゾーンは、作成された VPC に関連付ける必要があります。

4. ホストゾーンが作成され、VPC に関連付けられたら、**Cluster Creator** に以下を提供して設定を続行します。

   - ホストゾーン ID
   - AWS リージョン
   - サブネット ID

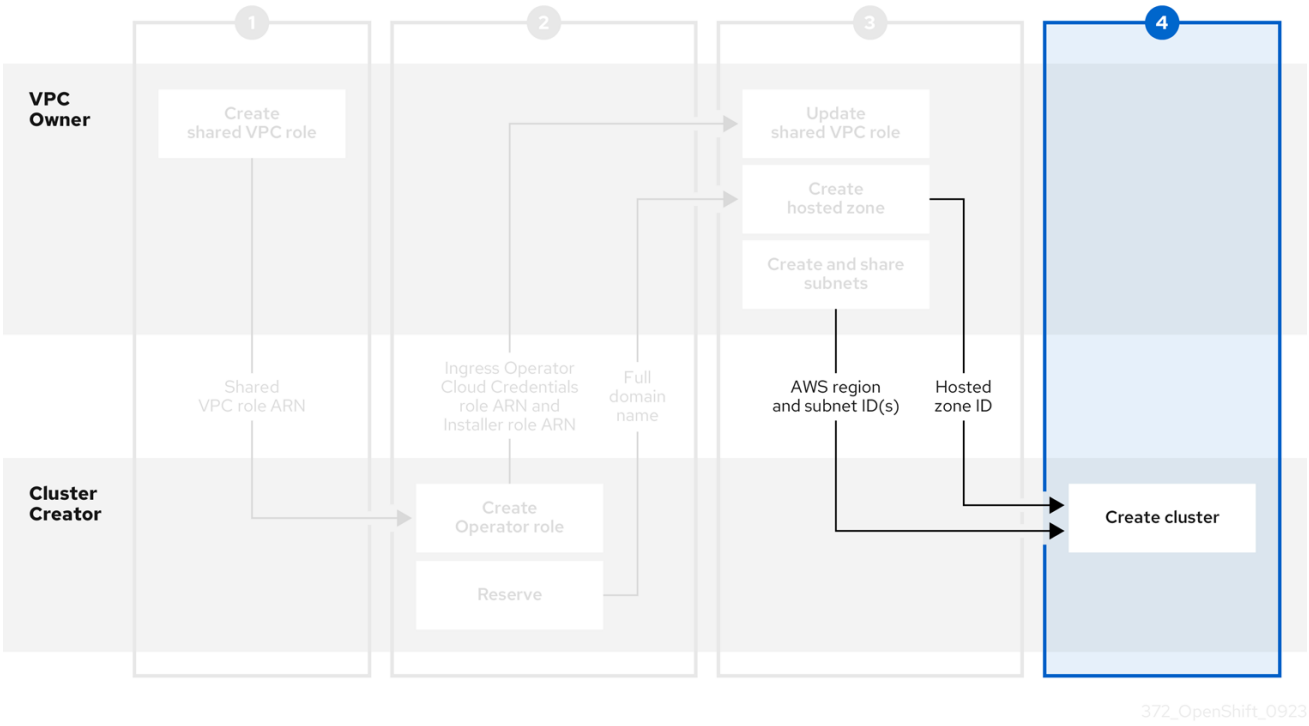
## 6.4. ステップ 4: CLUSTER CREATOR: 共有 VPC でのクラスターの作成

共有 VPC にクラスターを作成するには、次の手順を実行します。



**注記**

共有 VPC へのクラスターのインストールは、OpenShift 4.12.34 以降、4.13.10 以降、および今後の全 4.y ストリームでのみサポートされます。




**前提条件**

- **VPC Owner** からホストゾーン ID を取得している。
- **VPC Owner** から AWS リージョンを取得している。
- **VPC Owner** からサブネット ID を取得している。
- **VPC Owner** から **SharedVPCRole** ARN を取得している。

**手順**

- ターミナルで次のコマンドを入力して、共有 VPC を作成します。

```
rosa create cluster --cluster-name <cluster_name> --sts --operator-roles-prefix <prefix> --oidc-config-id <oidc_config_id> --region us-east-1 --subnet-ids <subnet_ids> --private-hosted-zone-id <hosted_zone_ID> --shared-vpc-role-arn <vpc-role-arn> --base-domain <dns-domain>
```

**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。

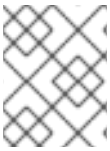
# 第7章 ROSA クラスターへのアクセス

アイデンティティープロバイダー (IDP) アカウントを使用して Red Hat OpenShift Service on AWS (ROSA) クラスターにアクセスすることが推奨されます。ただし、クラスターを作成したクラスター管理者は、クイックアクセス手順を使用してこれにアクセスできます。

本書では、クラスターにアクセスし、ROSA CLI (**rosa**) を使用して IDP を設定する方法を説明します。または、OpenShift Cluster Manager コンソールを使用して IDP アカウントを作成できます。

## 7.1. クラスターへの迅速なアクセス

この迅速なクイックアクセスを実行する手順を使用してクラスターにログインできます。



**注記**

ベストプラクティスとして、IDP アカウントを代わりに使用してクラスターにアクセスできます。

**手順**

1. 以下のコマンドを実行します。

```
$ rosa create admin --cluster=<cluster_name>
```

**出力例**

```
W: It is recommended to add an identity provider to login to this cluster. See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'cluster_name'. It may take up to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.cluster-name.t6k4.i1.oragnization.org:6443 \ (1)
--username cluster-admin \
--password FWGYL-2mkJI-3ZTTZ-rINns
```

(1) Hosted Control Plane (HCP) クラスターを使用する Red Hat OpenShift Service on AWS (ROSA) の場合、ポート番号は **443** である必要があります。

2. 直前のコマンドの出力の **oc login** コマンド、ユーザー名、およびパスワードを入力します。

**出力例**

```
$ oc login https://api.cluster_name.t6k4.i1.oragnization.org:6443 \ (1)
>  --username cluster-admin \
>  --password FWGYL-2mkJI-3ZTTZ-rINns
Login successful.
You have access to 77 projects, the list has been suppressed. You can list all projects with ' projects'
```

(1) ROSA with HCP クラスターの場合、ポート番号は **443** である必要があります。

3. デフォルトプロジェクトを使用して、この **oc** コマンドを実行してクラスター管理者のアクセスが作成されていることを確認します。

```
$ oc whoami
```

**出力例**

```
cluster-admin
```

## 7.2. IDP アカウントでのクラスターへのアクセス

クラスターにログインするには、アイデンティティープロバイダー (IDP) を設定できます。この手順では、IDP の例として GitHub を使用します。サポートされている他の IDP を表示するには、**rosa create idp --help** コマンドを実行します。

**注記**

または、クラスターを作成したユーザーとして、クイックアクセス手順を使用できます。

**手順**

IDP アカウントを使用してクラスターにアクセスするには、以下を実行します。

1. IDP を追加します。
   a. 以下のコマンドは、GitHub がサポートする IDP を作成します。コマンドを実行後に、出力の対話式プロンプトに従って GitHub 開発者の設定 にアクセスし、新しい OAuth アプリケーションを設定します。

```
$ rosa create idp --cluster=<cluster_name> --interactive
```

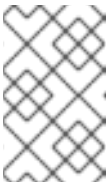
   b. 以下の値を設定します。
      - アイデンティティープロバイダーのタイプ: **github**
      - メンバーの制限: **organizations** (GitHub Organization がない場合は作成可能)
      - GitHub Organization: **rh-test-org** (組織の名前を入力)

**出力例**

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Restrict to members of: organizations
? GitHub organizations: rh-test-org
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/rh-rosa-test-cluster/settings/applications/new?
oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-openshift.apps.rh-
rosa-test-cluster.z7v0.s1.devshift.org%2Foauth2callback%2Fgithub-
1&oauth_application%5Bname%5D=rh-rosa-test-cluster-
stage&oauth_application%5Burl%5D=https%3A%2F%2Fconsole-openshift-
```

```
console.apps.rh-rosa-test-cluster.z7v0.s1.devshift.org
  - Click on 'Register application'
...
```

c. 出力された URL に従い、**Register application** を選択すると、Git Hub の組織に新しい OAuth アプリケーションが登録されます。アプリケーションを登録することで、ROSA に内蔵されている OAuth サーバーが GitHub 組織のメンバーをクラスターに認証することができるようになります。



**注記**

**Register a new OAuth application** GitHub フォームのフィールドには、Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) で定義される URL を介して、必要な値が自動的に入力されます。

d. 作成した GitHub アプリケーションの情報を使用し、プロンプトを続行します。以下の値を設定します。

- クライアント ID: **<my_github_client_id>**
- クライアントシークレット: [? for help] **<my_github_client_secret>**
- ホスト名: (オプション。現在のところ空白のままにすることが可能)
- マッピング方法: **claim**

**出力例 (続き)**

```
...
? Client ID: <my_github_client_id>
? Client Secret: [? for help] <my_github_client_secret>
? Hostname:
? Mapping method: claim
I: Configuring IDP for cluster 'rh_rosa_test_cluster'
I: Identity Provider 'github-1' has been created. You need to ensure that there is a list of cluster administrators defined. See 'rosa create user --help' for more information. To login into the console, open https://console-openshift-console.apps.rh-test-org.z7v0.s1.devshift.org and click on github-1
```

IDP は、クラスター内で設定するのに 1 - 2 分かかる場合があります。

e. 以下のコマンドを実行して、IDP が正しく設定されていることを確認します。

```
$ rosa list idps --cluster=<cluster_name>
```

**出力例**

```
NAME        TYPE      AUTH URL
github-1    GitHub    https://oauth-openshift.apps.rh-rosa-test-cluster1.j9n4.s1.devshift.org/oauth2callback/github-1
```

2. クラスターにログインします。

a. 以下のコマンドを実行して、クラスターの **Console URL** を取得します。

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

**出力例**

```
Name:         rh-rosa-test-cluster1
ID:           1de87g7c30g75qechgh7l5b2bha6r04e
External ID: 34322be7-b2a7-45c2-af39-2c684ce624e1
API URL:      https://api.rh-rosa-test-cluster1.j9n4.s1.devshift.org:6443 (1)
Console URL: https://console-openshift-console.apps.rh-rosa-test-
cluster1.j9n4.s1.devshift.org
Nodes:        Master: 3, Infra: 3, Compute: 4
Region:       us-east-2
State:        ready
Created:      May 27, 2020
```

(1) Hosted Control Plane (HCP) クラスターを使用する Red Hat OpenShift Service on AWS (ROSA) の場合、ポート番号は **443** である必要があります。

b. **Console URL** に移動し、Github 認証情報を使用してログインします。

c. OpenShift コンソールの右上で、名前をクリックして **Copy Login Command** をクリックします。

d. 追加した IDP の名前 (この場合は **github-1**) を選択し、**Display Token** をクリックします。

e. **oc** ログインコマンドをコピーし、これをターミナルに貼り付けます。

```
$ oc login --token=z3sgOGVDk0k4vbqo_wFqBQQTnT-nA-nQLb8XEmWnw4X --
server=https://api.rh-rosa-test-cluster1.j9n4.s1.devshift.org:6443 (1)
```

(1) ROSA with HCP クラスターの場合は、ポート番号 **443** を使用します。

**出力例**

```
Logged into "https://api.rh-rosa-cluster1.j9n4.s1.devshift.org:6443" as "rh-rosa-test-user"
using the token provided. (1)

You have access to 67 projects, the list has been suppressed. You can list all projects
with 'oc projects'

Using project "default".
```

(1) ROSA with HCP クラスターの場合、ポート番号は **443** である必要があります。

f. 単純な **oc** コマンドを実行して、すべての設定が適切でログインしていることを確認します。

```
$ oc version
```

**出力例**

```
```

```
Client Version: 4.4.0-202005231254-4a4cd75
Server Version: 4.3.18
Kubernetes Version: v1.16.2
```

## 7.3. CLUSTER-ADMIN アクセス権限の付与

クラスターを作成したユーザーは、**cluster-admin** ユーザーロールをアカウントに追加して、最大管理者権限を割り当てます。これらの権限は、クラスターの作成時に自動的にユーザーアカウントに割り当てられることはありません。

さらに、クラスターを作成したユーザーのみが、他の **cluster-admin** または **dedicated-admin** ユーザーにクラスターアクセスを付与できます。**dedicated-admin** アクセスを持つユーザーの権限は少なくなります。ベストプラクティスとして、**cluster-admin** ユーザーの数をできるだけ少なく制限できます。

**前提条件**

- アイデンティティープロバイダー (IDP) をクラスターに追加している。
- 作成するユーザーの IDP ユーザー名がある。
- クラスターにログインしている。

**手順**

1. ユーザーに **cluster-admin** 権限を付与します。

```
$ rosa grant user cluster-admin --user=<idp_user_name> --cluster=<cluster_name>
```

2. ユーザーがクラスター管理者としてリスト表示されていることを確認します。

```
$ rosa list users --cluster=<cluster_name>
```

**出力例**

```
GROUP            NAME
cluster-admins   rh-rosa-test-user
dedicated-admins rh-rosa-test-user
```

3. 以下のコマンドを実行して、ユーザーが **cluster-admin** アクセスを持つことを確認します。クラスター管理者はエラーを出さずにこのコマンドを実行できますが、専用の管理者は実行できません。

```
$ oc get all -n openshift-apiserver
```

**出力例**

```
NAME                READY   STATUS    RESTARTS   AGE
pod/apiserver-6ndg2   1/1     Running   0          17h
pod/apiserver-lrmxs   1/1     Running   0          17h
pod/apiserver-tsqhz   1/1     Running   0          17h
NAME          TYPE        CLUSTER-IP     EXTERNAL-IP   PORT(S)   AGE
service/api   ClusterIP   172.30.23.241   <none>        443/TCP   18h
```

```
NAME                    DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE
SELECTOR                  AGE
daemonset.apps/apiserver   3         3         3       3            3           node-
role.kubernetes.io/master=   18h
```

**関連情報**

- クラスター管理ロール

## 7.4. DEDICATED-ADMIN アクセスの取り消し

クラスターを作成したユーザーのみが、他の **cluster-admin** または **dedicated-admin** ユーザーにクラスターアクセスを付与できます。**dedicated-admin** アクセスを持つユーザーの権限は少なくなります。ベストプラクティスとして、**dedicated-admin** アクセスをほとんどの管理者に付与することができます。

**前提条件**

- アイデンティティープロバイダー (IDP) をクラスターに追加している。
- 作成するユーザーの IDP ユーザー名がある。
- クラスターにログインしている。

**手順**

1. 以下のコマンドを実行して、ユーザーを **dedicated-admin** にプロモートします。

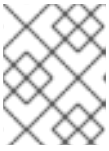
```
$ rosa grant user dedicated-admin --user=<idp_user_name> --cluster=<cluster_name>
```

2. 以下のコマンドを実行して、ユーザーに **dedicated-admin** アクセスがあることを確認します。

```
$ oc get groups dedicated-admins
```

**出力例**

```
NAME              USERS
dedicated-admins   rh-rosa-test-user
```



**注記**

**Forbidden** エラーは、**dedicated-admin** 権限を持たないユーザーがこのコマンドを実行する場合に表示されます。

**関連情報**

- お客様管理者ユーザー

## 7.5. 関連情報

- Red Hat OpenShift Cluster Manager コンソールを使用したアイデンティティープロバイダーの設定

- STS を使用する ROSA のデプロイメントワークフローについて

# 第8章 STS のアイデンティティープロバイダーの設定

Red Hat OpenShift Service on AWS (ROSA) クラスターの作成後に、アイデンティティープロバイダーを設定して、ユーザーがクラスターにアクセスする方法を判別する必要があります。

以下のトピックでは、OpenShift Cluster Manager コンソールを使用してアイデンティティープロバイダーを設定する方法を説明します。または、ROSA CLI (**rosa**) を使用してアイデンティティープロバイダーを設定し、クラスターにアクセスできます。

## 8.1. アイデンティティープロバイダーについて

Red Hat OpenShift Service on AWS には、ビルトイン OAuth サーバーが含まれます。開発者および管理者は OAuth アクセストークンを取得して、API に対して認証します。管理者は、クラスターのインストール後に、OAuth をアイデンティティープロバイダーを指定するように設定できます。アイデンティティープロバイダーを設定すると、ユーザーはログインし、クラスターにアクセスできます。

### 8.1.1. サポートされるアイデンティティープロバイダー

以下の種類のアイデンティティープロバイダーを設定できます。

| アイデンティティープロバイダー | 説明 |
| --- | --- |
| GitHub または GitHub Enterprise | GitHub または GitHub Enterprise の OAuth 認証サーバーに対して、ユーザー名とパスワードを検証するように Github アイデンティティープロバイダーを設定します。 |
| GitLab | GitLab.com またはその他の GitLab インスタンスをアイデンティティープロバイダーとして使用するように GitLab アイデンティティープロバイダーを設定します。 |
| Google | Google の OpenID Connect 統合機能を使用して Google アイデンティティープロバイダーを設定します。 |
| LDAP | 単純なバインド認証を使用して、LDAPv3 サーバーに対してユーザー名とパスワードを検証するように LDAP アイデンティティープロバイダーを設定します。 |
| OpenID Connect | Authorization Code Flow を使用して OpenID Connect アイデンティティープロバイダーと統合するように OpenID Connect (OIDC) アイデンティティープロバイダーを設定します。 |
| htpasswd | 単一の静的管理ユーザー用に htpasswd アイデンティティープロバイダーを設定します。問題のトラブルシューティングを行うには、ユーザーとしてクラスターにログインできます。<br><br>  <br>**重要**<br><br>htpasswd ID プロバイダーオプションは、単一の静的管理ユーザーを作成できるようにするためだけに含まれています。htpasswd は、Red Hat OpenShift Service on AWS の汎用 ID プロバイダーとしてはサポートされていません。単一ユーザーを設定する手順は、**htpasswd アイデンティティープロバイダーの設定** を参照してください。 |

### 8.1.2. アイデンティティープロバイダーパラメーター

以下のパラメーターは、すべてのアイデンティティープロバイダーに共通するパラメーターです。

| パラメーター | 説明 |
| --- | --- |
| **name** | プロバイダー名は、プロバイダーのユーザー名に接頭辞として付加され、アイデンティティー名が作成されます。 |
| **mappingMethod** | 新規アイデンティティーがログイン時にユーザーにマップされる方法を定義します。以下の値のいずれかを入力します。<br><br>**claim**<br>デフォルトの値です。アイデンティティーの推奨ユーザー名を持つユーザーをプロビジョニングします。そのユーザー名を持つユーザーがすでに別のアイデンティティーにマッピングされている場合は失敗します。<br>**lookup**<br>既存のアイデンティティー、ユーザーアイデンティティーマッピング、およびユーザーを検索しますが、ユーザーまたはアイデンティティーの自動プロビジョニングは行いません。これにより、クラスター管理者は手動で、または外部のプロセスを使用してアイデンティティーとユーザーを設定できます。この方法を使用する場合は、ユーザーを手動でプロビジョニングする必要があります。<br>**add**<br>アイデンティティーの推奨ユーザー名を持つユーザーをプロビジョニングします。推奨ユーザー名を持つユーザーがすでに存在する場合、アイデンティティーは既存のユーザーにマッピングされ、そのユーザーの既存のアイデンティティーマッピングに追加されます。これは、同じユーザーセットを識別して同じユーザー名にマッピングするアイデンティティープロバイダーが複数設定されている場合に必要です。 |

**注記**

**mappingMethod** パラメーターを **add** に設定すると、アイデンティティープロバイダーの追加または変更時に新規プロバイダーのアイデンティティーを既存ユーザーにマッピングできます。

## 8.2. GITHUB アイデンティティープロバイダーの設定

GitHub または GitHub Enterprise の OAuth 認証サーバーに対してユーザー名とパスワードを検証し、Red Hat OpenShift Service on AWS クラスターにアクセスするように GitHub アイデンティティープロバイダーを設定します。OAuth は Red Hat OpenShift Service on AWS と GitHub または GitHub Enterprise 間のトークン交換フローを容易にします。

**警告**

GitHub 認証を設定することによって、ユーザーは GitHub 認証情報を使用して Red Hat OpenShift Service on AWS にログインできます。GitHub ユーザー ID を持つすべてのユーザーが Red Hat OpenShift Service on AWS クラスターにログインできないようにするために、アクセスを特定の GitHub 組織のユーザーに制限する必要があります。

**前提条件**

- OAuth アプリケーションを、GitHub 組織管理者によって GitHub 組織設定 内に直接作成している。
- GitHub 組織またはチーム が GitHub アカウントに設定されている。

**手順**

1. OpenShift Cluster Manager から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。

**注記**

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **GitHub** を選択します。
5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することができません。
   - **OAuth callback URL** が指定のフィールドに自動的に生成されます。これを使用して GitHub アプリケーションを登録します。

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     以下に例を示します。

     ```
     https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/github
     ```

6. アプリケーションを GitHub に登録します。
7. Red Hat OpenShift Service on AWS に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。

8. GitHub から提供される **Client ID** および **Client secret** を入力します。
9. **hostname** を入力します。GitHub Enterprise のホステッドインスタンスを使用する場合は、ホスト名を入力する必要があります。
10. オプション: 認証局 (CA) ファイルを使用して、設定された GitHub Enterprise URL のサーバー証明書を検証できます。**Browse** をクリックして **CA ファイル** を見つけ、これをアイデンティティープロバイダーに割り当てます。
11. **Use organizations** または **Use teams** を選択し、アクセスを特定の GitHub 組織または GitHub チームに制限します。
12. アクセスを制限する組織またはチームの名前を入力します。**Add more** をクリックして、ユーザーが所属できる複数の組織またはチームを指定します。
13. **Confirm** をクリックします。

**検証**

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

## 8.3. GITLAB アイデンティティープロバイダーの設定

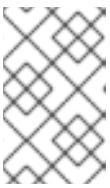
GitLab.com またはその他の GitLab インスタンスをアイデンティティープロバイダーとして使用するように GitLab アイデンティティープロバイダーを設定します。

**前提条件**

- GitLab バージョン 7.7.0 から 11.0 を使用する場合は、OAuth 統合 を使用して接続します。GitLab バージョン 11.1 以降の場合は、OAuth ではなく OpenID Connect (OIDC) を使用して接続します。

**手順**

1. OpenShift Cluster Manager から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。



**注記**

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **GitLab** を選択します。
5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することができません。
    - **OAuth callback URL** が指定のフィールドに自動的に生成されます。この URL を GitLab に指定します。

```
https://oauth-openshift.apps.<cluster_name>.
<cluster_domain>/oauth2callback/<idp_provider_name>
```

以下に例を示します。

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/gitlab
```

6. GitLab に新規アプリケーションを追加します。
7. Red Hat OpenShift Service on AWS に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。
8. GitLab から提供される **Client ID** および **Client secret** を入力します。
9. GitLab プロバイダーの **URL** を入力します。
10. オプション: 認証局 (CA) ファイルを使用して、設定された GitLab URL のサーバー証明書を検証できます。**Browse** をクリックして **CA ファイル** を見つけ、これをアイデンティティープロバイダーに割り当てます。
11. **Confirm** をクリックします。

**検証**

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

## 8.4. GOOGLE アイデンティティープロバイダーの設定

ユーザーが Google 認証情報で認証できるように Google アイデンティティープロバイダーを設定します。

**警告**

Google をアイデンティティープロバイダーとして使用することで、Google ユーザーはサーバーに対して認証されます。**hostedDomain** 設定属性を使用して、特定のホストドメインのメンバーに認証を限定することができます。

**手順**

1. OpenShift Cluster Manager から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。

**注記**

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **Google** を選択します。
5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することができません。
   - **OAuth callback URL** が指定のフィールドに自動的に生成されます。この URL を Google に指定します。

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     以下に例を示します。

     ```
     https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/google
     ```
6. Google の OpenID Connect 統合機能 を使用して Google アイデンティティープロバイダーを設定します。
7. Red Hat OpenShift Service on AWS に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。
8. 登録済みの Google プロジェクトの **Client ID** と、Google が発行する **Client secret** を入力します。
9. ホストされたドメインを入力して、ユーザーを Google Apps ドメインに制限します。
10. **Confirm** をクリックします。

**検証**

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

## 8.5. LDAP アイデンティティープロバイダーの設定

単純なバインド認証を使用して LDAPv3 サーバーに対してユーザー名とパスワードを検証するように LDAP アイデンティティープロバイダーを設定します。

**前提条件**

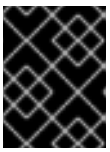
- LDAP アイデンティティープロバイダーを設定する場合は、設定済みの **LDAP URL** を入力する必要があります。設定される URL は、LDAP ホストと使用する検索パラメーターを指定する RFC 2255 URL です。URL の構文は以下のようになります。

  ```
  ldap://host:port/basedn?attribute?scope?filter
  ```

| URL コンポーネント | 説明 |
|---|---|
| **ldap** | 通常の LDAP の場合は、文字列 **ldap** を使用します。セキュアな LDAP (LDAPS) の場合は、代わりに **ldaps** を使用します。 |
| **host:port** | LDAP サーバーの名前とポートです。デフォルトは、ldap の場合は **localhost:389**、LDAPS の場合は **localhost:636** です。 |
| **basedn** | すべての検索が開始されるディレクトリーのブランチの DN です。これは少なくともディレクトリーツリーの最上位になければなりませんが、ディレクトリーのサブツリーを指定することもできます。 |
| **attribute** | 検索対象の属性です。RFC 2255 はコンマ区切りの属性のリストを許可しますが、属性をどれだけ指定しても最初の属性のみが使用されます。属性を指定しない場合は、デフォルトで **uid** が使用されます。使用しているサブツリーのすべてのエントリー間で一意の属性を選択することを推奨します。 |
| **scope** | 検索の範囲です。**one** または **sub** のいずれかを指定できます。範囲を指定しない場合は、デフォルトの範囲として **sub** が使用されます。 |
| **filter** | 有効な LDAP 検索フィルターです。指定しない場合、デフォルトは **(objectClass=*)** です。 |

検索の実行時に属性、フィルター、指定したユーザー名が組み合わされて以下のような検索フィルターが作成されます。

```
(&(<filter>)(<attribute>=<username>))
```

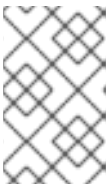


**重要**

LDAP ディレクトリーの検索に認証が必要な場合は、エントリー検索の実行に使用する **bindDN** と **bindPassword** を指定します。

**手順**

1. OpenShift Cluster Manager から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。



**注記**

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **LDAP** を選択します。

5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することができません。
6. ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。
7. **LDAP URL** を入力して、使用する LDAP 検索パラメーターを指定します。
8. オプション: **Bind DN** および **Bind password** を入力します。
9. LDAP 属性をアイデンティティーにマップする属性を入力します。
   - 値をユーザー ID として使用する **ID** 属性を入力します。**Add more** をクリックして、複数の ID 属性を追加します。
   - オプション: 表示名の値として使用する **Preferred username** 属性を入力します。**Add more** をクリックして、優先する複数のユーザー名属性を追加します。
   - オプション: メールアドレスの値として使用する **Email** 属性を入力します。**Add more** をクリックして、複数のメール属性を追加します。
10. オプション: **Show advanced Options** をクリックし、認証局 (CA) ファイルを LDAP アイデンティティープロバイダーに追加し、設定された URL のサーバー証明書を検証します。**Browse** をクリックして **CA ファイル** を見つけ、これをアイデンティティープロバイダーに割り当てます。
11. オプション: 高度なオプションで、LDAP プロバイダーを **非セキュア** にするよう選択できます。このオプションを選択すると、CA ファイルは使用できません。

**重要**

非セキュアな LDAP 接続 (ldap:// またはポート 389) を使用している場合は、設定ウィザードで **で Insecure** オプションを確認する必要があります。

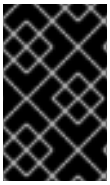
12. **Confirm** をクリックします。

**検証**

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

## 8.6. OPENID アイデンティティープロバイダーの設定

Authorization Code Flow を使用して OpenID Connect アイデンティティープロバイダーに統合するように OpenID アイデンティティープロバイダーを設定します。



**重要**

Red Hat OpenShift Service on AWS の認証 Operator では、設定済みの OpenID Connect アイデンティティープロバイダーが OpenID Connect Discovery 仕様を実装する必要があります。

要求は、OpenID アイデンティティープロバイダーから返される JWT **id_token** から読み取られ、指定される場合は発行者 URL によって返される JSON から読み取られます。

1 つ以上の要求をユーザーのアイデンティティーを使用するように設定される必要があります。

また、どの要求をユーザーの推奨ユーザー名、表示名およびメールアドレスとして使用するか指定することができます。複数の要求が指定されている場合は、値が入力されている最初の要求が使用されます。標準の要求は以下の通りです。

| 要求 | 説明 |
| --- | --- |
| **preferred_username** | ユーザーのプロビジョニング時に優先されるユーザー名です。**janedoe** などのユーザーを参照する際に使用する省略形の名前です。通常は、ユーザー名またはメールなどの、認証システムのユーザーのログインまたはユーザー名に対応する値です。 |
| **email** | メールアドレス。 |
| **name** | 表示名。 |

詳細は、OpenID claim のドキュメント を参照してください。

**前提条件**

- OpenID Connect を設定する前に、Red Hat OpenShift Service on AWS クラスターで使用する Red Hat 製品またはサービスのインストール前提条件を確認してください。

**手順**

1. OpenShift Cluster Manager から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。

**注記**

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **OpenID** を選択します。
5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することができません。
   - **OAuth callback URL** が指定のフィールドに自動的に生成されます。

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     以下に例を示します。

     ```
     https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/openid
     ```

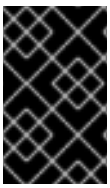
6. 認可リクエストを作成する 手順に従って、新しい OpenID Connect クライアントを OpenID ID プロバイダーに登録します。
7. Red Hat OpenShift Service on AWS に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合は、**Claim** の使用が推奨されます。
8. OpenID から提供される **Client ID** および **Client secret** を入力します。
9. **Issuer URL** を入力します。これは、OpenID プロバイダーが発行者 ID としてアサートする URL です。URL クエリーパラメーターまたはフラグメントのない https スキームを使用する必要があります。
10. メールアドレスの値として使用する **Email** 属性を入力します。**Add more** をクリックして、複数のメール属性を追加します。
11. 優先するユーザー名の値として使用する **Name** 属性を入力します。**Add more** をクリックして、優先する複数のユーザー名を追加します。
12. 表示名の値として使用する **Preferred username** 属性を入力します。**Add more** をクリックして、複数の表示名を追加します。
13. オプション: **Show advanced Options** をクリックし、認証局 (CA) ファイルを OpenID アイデンティティープロバイダーに追加します。
14. オプション: 高度なオプションから、**追加のスコープ** を追加できます。デフォルトでは、**OpenID** の範囲が要求されます。
15. **Confirm** をクリックします。

**検証**

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

## 8.7. HTPASSWD アイデンティティープロバイダーの設定

クラスター管理者権限で単一の静的ユーザーを作成するように htpasswd アイデンティティープロバイダーを設定します。問題のトラブルシューティングを行うには、ユーザーとしてクラスターにログインできます。



**重要**

htpasswd ID プロバイダーオプションは、単一の静的管理ユーザーを作成できるようにするためだけに含まれています。htpasswd は、Red Hat OpenShift Service on AWS の汎用 ID プロバイダーとしてはサポートされていません。

**手順**

1. OpenShift Cluster Manager から、**Clusters** ページに移動し、クラスターを選択します。
2. **Access control → Identity providers** の順に選択します。
3. **Add identity provider** をクリックします。
4. **Identity Provider** ドロップダウンメニューから **HTPasswd** を選択します。

5. アイデンティティープロバイダーの **Name** フィールドに一意の名前を追加します。

6. 静的ユーザーに推奨されるユーザー名およびパスワードを使用するか、独自のユーザー名およびパスワードを作成します。

**注記**

この手順で定義した認証情報は、以下の手順で **Add** を選択した後に表示されません。認証情報を失った場合は、アイデンティティープロバイダーを再作成し、認証情報を再度定義する必要があります。

7. **Add** を選択して htpasswd アイデンティティープロバイダーおよび単一の静的ユーザーを作成します。

8. クラスターを管理する静的ユーザーにパーミッションを付与します。

   a. **Access control → Cluster Roles and Access** で、**Add user** を選択します。

   b. 前のステップで作成した静的ユーザーの **User ID** を入力します。

   c. **グループ** を選択します。**dedicated-admins** グループのユーザーには、Red Hat OpenShift Service on AWS の標準の管理者権限があります。**cluster-admins** グループのユーザーには、クラスターへの完全な管理アクセス権限があります。

   d. **Add user** を選択して、管理者権限をユーザーに付与します。

**検証**

- 設定された htpasswd アイデンティティープロバイダーは、**Access control → Identity providers** ページに表示されます。

**注記**

アイデンティティープロバイダーの作成後に、同期は通常 2 分以内に完了します。htpasswd アイデンティティープロバイダーが利用可能になると、ユーザーとしてクラスターにログインできます。

- 管理ユーザーは、**Access control → Cluster Roles and Access** ページで確認できます。ユーザーの管理グループメンバーシップも表示されます。

## 8.8. 関連情報

- クラスターへのアクセス
- STS を使用する ROSA のデプロイメントワークフローについて

# 第9章 ROSA クラスターへのアクセスの取り消し

IDP (アイデンティティプロバイダー) は、Red Hat OpenShift Service on AWS (ROSA) クラスターへのアクセスを制御します。ユーザーのクラスターへのアクセスを取り消すには、認証用に設定された IDP 内で設定する必要があります。

## 9.1. ROSA CLI を使用した管理者アクセスの取り消し

ユーザーの管理者権限を取り消して、管理者権限がなくてもクラスターにアクセスできるようにすることができます。ユーザーの管理者アクセスを削除するには、**dedicated-admin** または **cluster-admin** の権限を取り消す必要があります。Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) または OpenShift Cluster Manager コンソールを使用して管理者権限を取り消すことができます。

### 9.1.1. ROSA CLI を使用した **dedicated-admin** アクセスの取り消し

**dedicated-admin** ユーザーのアクセス権を取り消すことができるのは、自分がクラスターを作成したユーザー、組織管理者ユーザー、またはスーパー管理者ユーザーの場合です。

**前提条件**

- アイデンティティープロバイダー (IDP) をクラスターに追加している。
- 取り消す権限を持つユーザーの IDP ユーザー名がある。
- クラスターにログインしている。

**手順**

1. ユーザーの **dedicated-admin** アクセスを取り消すには、次のコマンドを入力してください。

```
$ rosa revoke user dedicated-admin --user=<idp_user_name> --cluster=<cluster_name>
```

2. 以下のコマンドを実行して、ユーザーに **dedicated-admin** アクセスがなくなったことを確認します。出力には、取り消したユーザーが表示されません。

```
$ oc get groups dedicated-admins
```

### 9.1.2. ROSA CLI を使用した **cluster-admin** アクセス権の取り消し

クラスターを作成したユーザーのみが、**cluster-admin** ユーザーのアクセスを取り消すことができます。

**前提条件**

- アイデンティティープロバイダー (IDP) をクラスターに追加している。
- 取り消す権限を持つユーザーの IDP ユーザー名がある。
- クラスターにログインしている。

**手順**

1. ユーザーの **cluster-admin** アクセスを取り消すには、次のコマンドを入力してください。

```
$ rosa revoke user cluster-admins --user=myusername --cluster=mycluster
```

2. 次のコマンドを入力して、そのユーザーが **cluster-admin** アクセス権を失ったことを確認します。出力には、取り消したユーザーが表示されません。

```
$ oc get groups cluster-admins
```

## 9.2. OPENSHIFT CLUSTER MANAGER コンソールを使用した管理者アクセスの取り消し

OpenShift Cluster Manager のコンソールから、ユーザーの **dedicated-admin** または **cluster-admin** アクセスを取り消すことができます。ユーザーは、管理者権限がなくてもクラスターにアクセスできるようになります。

**前提条件**

- アイデンティティープロバイダー (IDP) をクラスターに追加している。
- 取り消す権限を持つユーザーの IDP ユーザー名がある。
- クラスターの作成に使用した OpenShift Cluster Manager アカウント、組織の管理者ユーザー、またはスーパーユーザーを使用して OpenShift Cluster Manager コンソールにログインしている。

**手順**

1. OpenShift Cluster Manager の **Clusters** タブで、クラスターの名前を選択し、クラスターの詳細を表示します。
2. **Access control** > **Cluster Roles and Access** を選択します。
3. 削除するユーザーについて、ユーザーとグループの組み合わせの右にある **Options** メニュー

をクリックし、**Delete** をクリックします。

# 第10章 ROSA クラスターの削除

このドキュメントでは、AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを削除する手順について説明します。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。

## 10.1. 前提条件

- Red Hat OpenShift Service on AWS が VPC を作成した場合は、クラスターを正常に削除する前に、クラスターから次のアイテムを削除する必要があります。
  - VPN 設定や VPC ピアリング接続などのネットワーク設定
  - VPC に追加された追加サービス

これらの設定とサービスが残っている場合、クラスターは適切に削除されません。

## 10.2. ROSA クラスターとクラスター固有の IAM リソースの削除

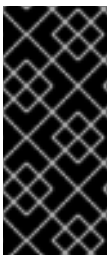
ROSA CLI (**rosa**) または Red Hat OpenShift Cluster Manager を使用して、AWS Security Token Service (STS) クラスターを備えた Red Hat OpenShift Service on AWS (ROSA) を削除できます。

クラスターを削除した後、ROSA CLI (**rosa**) を使用して、AWS アカウントのクラスター固有の Identity and Access Management (IAM) リソースをクリーンアップできます。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。



**重要**

インストール時に VPC を作成したクラスターが削除されると、関連するインストールプログラムで作成された VPC も削除され、同じ VPC を使用しているすべてのクラスターが失敗します。さらに、インストールプログラムによって作成されるリソースと同じ **tagSet** のキーと値のペアで作成され、**owned** の値でラベルが付いたリソースも削除されます。

**前提条件**

- ROSA クラスターをインストールしました。
- 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. クラスター ID、クラスター固有 Operator ロールの Amazon Resource Names (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> 1
```

1 **<cluster_name>** は、クラスター名に置き換えます。

**出力例**

```
Name:                       mycluster
ID:                         1s3v4x39lhs8sm49m90mi0822o34544a 1
...
Operator IAM Roles: 2
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-machine-api-aws-cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cloud-credential-operator-cloud-crede
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-image-registry-installer-cloud-creden
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-ingress-operator-cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cluster-csi-drivers-ebs-cloud-credent
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cloud-network-config-controller-cloud
State:                      ready
Private:                    No
Created:                    May 13 2022 11:26:15 UTC
Details Page:
https://console.redhat.com/openshift/details/s/296kyEFwzoy1CREQicFRdZybrc0
OIDC Endpoint URL:          https://oidc.op1.openshiftapps.com/<oidc_config_id> 3
```

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**

クラスターが削除された後、ROSA CLI (**rosa**) 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 が必要です。

2. クラスターを削除します。

- Red Hat OpenShift Cluster Manager を使用してクラスターを削除するには:

  a. OpenShift Cluster Manager に移動します。

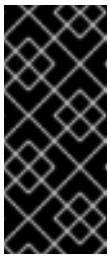
  b. クラスターの横にあるオプションメニュー  をクリックし、**Delete cluster** を選択します。

c. プロンプトでクラスターの名前を入力し、**Delete** をクリックします。

- ROSA CLI (**rosa**) を使用してクラスターを削除するには:

a. 以下のコマンドを実行してクラスターを削除し、ログを監視し、**<my-cluster>** 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のを待つ必要があります。クラスター固有の Operator ロールは、OpenShift Operator によって作成されるリソースをクリーンアップするために必要です。Operator は、OIDC プロバイダーを利用して認証を行います。

3. クラスター Operator が認証に使用する OIDC プロバイダーを削除します。

```
$ rosa delete oidc-provider -c <cluster_id> --mode auto
```
(1)

(1) **<cluster_id>** をクラスターの ID に置き換えてください。

**注記**

**-y** オプションを使用すると、プロンプトに対して自動的にはいと答えることができます。

4. オプション: クラスター固有の Operator IAM ロールを削除します。

**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。

```
$ rosa delete operator-roles -c <cluster_id> --mode auto
```
(1)

(1) **<cluster_id>** をクラスターの ID に置き換えてください。

### 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。

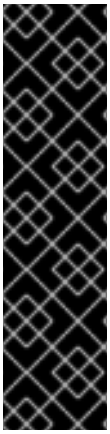
**関連情報**

- アカウント全体の IAM ロールとポリシーを削除する手順は、アカウント全体の IAM ロールとポリシーの削除 を参照してください。
- OpenShift Cluster Manager およびユーザー IAM ロールを削除する手順は、OpenShift Cluster Manager およびユーザー IAM ロールの解除と削除 を参照してください。

## 10.3. 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 AWS Security Token Services (STS) クラスターを使用してすべての Red Hat OpenShift Service on AWS (ROSA) を削除した後、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 STS 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 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とされていない場合に限り、リソースを削除する必要があります。

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して管理し、削除する場合は、OpenShift Cluster Manager とユーザー IAM ロールが必要です。OpenShift Cluster Manager を使用してアカウントに ROSA 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、ロールを削除する必要があります。削除された場合のクラスターの修復についてはその他のリソースセクションを削除前に参照してください。

### 10.3.1. 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、STS を使用する ROSA 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について説明します。アカウント全体の AWS Identityentityand Access Management (IAM) のロールとポリシーを削除できるのは、それらに依存する AWS Security Token Services (STS) クラスターを備えたすべての Red Hat OpenShift Service on AWS (ROSA) を削除した後でのみです。

**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 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とされていない場合に限り、ロールを削除する必要があります。

**前提条件**

- ROSA クラスターをインストールしました。
- 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. 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
```

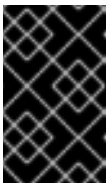
**出力例**

```
I: Fetching account roles
ROLE NAME                          ROLE TYPE      ROLE ARN
OPENSHIFT VERSION
ManagedOpenShift-ControlPlane-Role  Control plane  arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-ControlPlane-Role  4.10
ManagedOpenShift-Installer-Role     Installer      arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Installer-Role     4.10
ManagedOpenShift-Support-Role       Support        arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Support-Role       4.10
ManagedOpenShift-Worker-Role        Worker         arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Worker-Role        4.10
```

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。

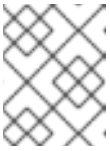


**重要**

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、ロールを削除する必要があります。

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。

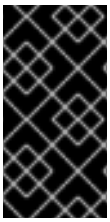
b. AWS IAM Console を使用して、アカウント全体のインラインポリシーと Operator ポリシーを削除します。AWS IAM コンソールを使用して IAM ポリシーを削除する方法の詳細は、AWS ドキュメントの IAM ポリシーの削除 を参照してください。

**重要**

アカウント全体のインラインおよび Operator IAM ポリシーは、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、ロールを削除する必要があります。

### 10.3.2. 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 Red Hat OpenShift Service on AWS (ROSA) クラスターをインストールした場合は、OpenShift Cluster Manager とユーザー ID およびアクセス管理 (IAM) のロールを作成し、それらを RedHat 組織にリンクしました。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 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、ロールを削除する必要があります。

**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 組織にリンクしました。
- 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。
- Red Hat 組織で組織管理者権限があります。

**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
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
```

   b. OpenShift Cluster Manager IAM ロールが上記のコマンドの出力に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 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。前の例では、ARN の形式は **arn:aws:iam::<aws_account_external_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。

## 10.4. 関連情報

- STS を使用する ROSA クラスターの AWS IAM リソースは、STS を使用する ROSA クラスターの IAM リソースについて を参照してください。
- IAM ロールの欠落によるクラスターエラーの詳細は、削除できないクラスターの修復 を参照してください。

# 第11章 AWS STS を使用しない ROSA のデプロイ

## 11.1. ROSA の AWS の前提条件

Red Hat OpenShift Service on AWS (ROSA) は、Red Hat によるクラスターのお客様の既存 Amazon Web Service (AWS) アカウントへのデプロイを可能にするモデルを提供します。

ROSA をインストールする前に、前提条件を満たしていることを確認する必要があります。この要件は、AWS Security Token Service (STS) には適用されません。STS を使用している場合は、STS 固有の要件 を参照してください。

### ヒント

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

### 11.1.1. お客様の要件

Red Hat OpenShift Service on AWS (ROSA) クラスターは、デプロイする前に複数の前提条件を満たす必要があります。

**注記**

クラスターを作成するには、ユーザーは予想されるロールまたは STS ユーザーとしてではなく、IAM ユーザーとしてログインする必要があります。

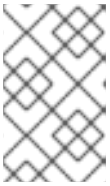
#### 11.1.1.1. アカウント

- お客様は、お客様の AWS アカウント内にプロビジョニングされる Red Hat OpenShift Service on AWS をサポートするのに十分な AWS 制限 が設定されていることを確認します。
- お客様の AWS アカウントは、該当するサービスコントロールポリシー (SCP) が適用されたお客様の AWS Organizations 組織にある必要があります。

**注記**

お客様のアカウントが AWS Organizations 内にあることや SCP を適用することは要件ではありませんが、Red Hat が制限なしで SCP にリスト表示されるすべてのアクションを実行できるようにする必要があります。

- お客様の AWS アカウントは、Red Hat に譲渡することはできません。
- お客様は、Red Hat の各種アクティビティーに対して AWS の使用についての制限を課すことができない場合があります。制限を課すことにより、Red Hat のインシデントへの対応が大幅に妨げられます。
- お客様は、同じ AWS アカウント内にネイティブ AWS サービスをデプロイすることができます。

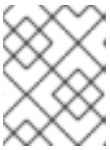


**注記**

Red Hat OpenShift Service on AWS やその他の Red Hat がサポートするサービスをホストする VPC とは別の Virtual Private Cloud (VPC) でリソースをデプロイすることが推奨されますが、これは義務ではありません。

#### 11.1.1.2. アクセス要件

- Red Hat OpenShift Service on AWS サービスを適切に管理するには、Red Hat では **AdministratorAccess** ポリシーを管理者ロールに常に適用する必要があります。AWS Security Token Service (STS) を使用している場合、この要件は **適用されません**。



**注記**

このポリシーは、お客様が指定する AWS アカウントのリソースを変更するためのパーミッションおよび機能を Red Hat に提供します。

- Red Hat には、顧客が提供した AWS アカウントへの AWS コンソールアクセス権が必要です。このアクセスは、Red Hat により保護され、管理されます。
- お客様は AWS アカウントを使用して Red Hat OpenShift Service on AWS クラスター内でパーミッションを昇格させることはできません。
- Red Hat OpenShift Service on AWS (ROSA) CLI、**rosa**、または OpenShift Cluster Manager コンソールで利用可能なアクションは、お客様の AWS アカウントで直接実行しないでください。

#### 11.1.1.3. サポート要件

- Red Hat では、お客様が少なくとも AWS の ビジネスサポート を用意することを推奨します。
- Red Hat は、お客様の代わりに AWS サポートをリクエストする権限をお客様から受けます。
- Red Hat は、お客様のアカウントで AWS リソース制限の引き上げをリクエストする権限をお客様から受けます。
- Red Hat は、この要件に関するセクションで指定されていない場合に、すべての Red Hat OpenShift Service on AWS クラスターについての制約、制限、予想される内容およびデフォルトの内容を管理します。

#### 11.1.1.4. セキュリティー要件

- ボリュームスナップショットは、お客様の AWS アカウントおよびお客様が指定するリージョン内に残ります。
- Red Hat には、許可リストにある IP アドレスから EC2 ホストおよび API サーバーへの ingress アクセスが必要です。
- Red Hat では、Red Hat が管理する中央ロギングスタックにシステムおよび監査ログを転送できるようにするために egress が必要です。

### 11.1.2. 必要なお客様の手順

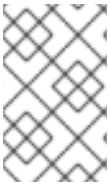
Red Hat OpenShift Service on AWS (ROSA) をデプロイする前に、以下の手順を実行します。

**手順**

1. お客様が AWS Organizations を使用している場合は、組織内の AWS アカウントを使用するか、新規アカウントを作成 する必要があります。
2. Red Hat が必要なアクションを実行できるようにするには、Service Control Policy (SCP) を作成するか、AWS アカウントに適用されているものがないことを確認する必要があります。
3. SCP を AWS アカウントに 割り当て ます。
4. 環境を設定するには、ROSA の手順に従います。

#### 11.1.2.1. Service Control Policy (SCP) の有効なパーミッションの最小セット

Service Control Policy (SCP) は、組織内のパーミッションを管理する組織ポリシーの一種です。SCP は、組織内のアカウントを、定義されたアクセス制御ガイドラインの範囲内にとどめるためのものです。これらのポリシーは、AWS Organizations で維持され、接続された AWS アカウント内で利用可能なサービスを制御します。SCP の管理はお客様の責任です。



**注記**

AWS セキュリティートークンサービス (STS) を使用する場合は、最小 SCP 要件が適用されません。STS の詳細は、STS を使用する ROSA の AWS の前提条件 について参照してください。

Service Control Policy (SCP) がこれらの必要なパーミッションを制限していないことを確認します。

| | サービス | アクション | 効果 |
|---|---|---|---|
| 必須 | Amazon EC2 | すべて | 許可 |
| | Amazon EC2 Auto Scaling | すべて | 許可 |
| | Amazon S3 | すべて | 許可 |
| | アイデンティティーおよびアクセス管理 | すべて | 許可 |
| | Elastic Load Balancing | すべて | 許可 |
| | Elastic Load Balancing V2 | すべて | 許可 |
| | Amazon CloudWatch | すべて | 許可 |
| | Amazon CloudWatch Events | すべて | 許可 |
| | Amazon CloudWatch Logs | すべて | 許可 |

| | サービス | アクション | 効果 |
|---|---|---|---|
| | AWS EC2 Instance Connect | SendSerialConsoleSSHPublicKey | 許可 |
| | AWS Support | すべて | 許可 |
| | AWS Key Management Service | すべて | 許可 |
| | AWS Security Token Service | すべて | 許可 |
| | AWS Tiro | CreateQuery<br>GetQueryAnswer<br>GetQueryExplanation | 許可 |
| | AWS Marketplace | サブスクライブ<br>サブスクライブ解除<br>サブスクリプションの表示 | 許可 |
| | AWS Resource Tagging | すべて | 許可 |
| | AWS Route53 DNS | すべて | 許可 |
| | AWS Service Quotas | ListServices<br>GetRequestedServiceQuotaChange<br>GetServiceQuota<br>RequestServiceQuotaIncrease<br>ListServiceQuotas | 許可 |
| オプション | AWS Billing | ViewAccount<br>Viewbilling<br>ViewUsage | 許可 |
| | AWS Cost and Usage Report | すべて | 許可 |

| | サービス | アクション | 効果 |
|---|---|---|---|
| | AWS Cost Explorer Services | すべて | 許可 |

**関連情報**

- Service Control Policy
- パーミッションに対する SCP の影響

### 11.1.3. AWS の Red Hat 管理 IAM リファレンス

Red Hat は、IAM ポリシー、IAM ユーザー、および IAM ロールなどの以下の Amazon Web Services (AWS) リソースを作成し、管理します。

#### 11.1.3.1. IAM ポリシー

**注記**

IAM ポリシーは、Red Hat OpenShift Service on AWS の機能の変更に伴って変更されることがあります。

- **AdministratorAccess** ポリシーは管理ロールによって使用されます。このポリシーは、お客様の AWS アカウントで Red Hat OpenShift Service on AWS (ROSA) クラスターを管理するために必要なアクセスを Red Hat に提供します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

#### 11.1.3.2. IAM ユーザー

**osdManagedAdmin** ユーザーは、ROSA をお客様の AWS アカウントにインストール後すぐに作成されます。

### 11.1.4. プロビジョニングされる AWS インフラストラクチャー

以下は、デプロイされた Red Hat OpenShift Service on AWS (ROSA) クラスターでプロビジョニングされる Amazon Web Services (AWS) コンポーネントの概要です。プロビジョニングされたすべての AWS コンポーネントの詳細なリストは、OpenShift Container Platform ドキュメント を参照してください。

#### 11.1.4.1. EC2 インスタンス

AWS EC2 インスタンスは、AWS パブリッククラウドに ROSA のコントロールプレーンおよびデータプレーン機能をデプロイするために必要です。

インスタンスタイプは、ワーカーノードの数に応じてコントロールプレーンおよびインフラストラクチャーノードによって異なる場合があります。少なくとも、以下の EC2 インスタンスがデプロイされます。

- 3 つの **m5.2xlarge** コントロールプレーンノード
- 2 つの **r5.xlarge** インフラストラクチャーノード
- 2 つの **m5.xlarge** カスタマイズ可能なワーカーノード

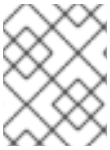
ワーカーノード数の詳細なガイダンスは、このページの関連情報セクションに一覧表示されている「制限およびスケーラビリティー」トピックの初期計画に関する考慮事項に関する情報を参照してください。

#### 11.1.4.2. Amazon Elastic Block Store ストレージ

Amazon Elastic Block Store (Amazon EBS) ブロックストレージは、ローカルノードストレージと永続ボリュームストレージの両方に使用されます。

各 EC2 インスタンスのボリューム要件:

- コントロールプレーンボリューム
  - サイズ: 350GB
  - タイプ: gp3
  - 1 秒あたりの I/O 処理数: 1000
- インフラストラクチャーボリューム
  - サイズ: 300GB
  - タイプ: gp3
  - 1 秒あたりの入出力操作: 900
- ワーカーボリューム
  - サイズ: 300GB
  - タイプ: gp3
  - 1 秒あたりの入出力操作: 900



**注記**

OpenShift Container Platform 4.11 のリリースより前にデプロイされたクラスターは、デフォルトで gp2 タイプのストレージを使用します。

#### 11.1.4.3. Elastic Load Balancing

API 用に最大 2 つのネットワークロードバランサー、アプリケーションルーター用に最大 2 つのクラシックロードバランサー。詳細は、AWS についての ELB ドキュメント を参照してください。

#### 11.1.4.4. S3 ストレージ

イメージレジストリーは、AWS S3 ストレージによって支えられています。S3 の使用およびクラスターのパフォーマンスを最適化するために、リソースのプルーニングを定期的に実行します。

**注記**

通常のサイズがそれぞれ 2TB の 2 つのバケットが必要です。

#### 11.1.4.5. VPC

お客様はクラスターごとに 1 つの VPC を確認できるはずです。さらに、VPC には以下の設定が必要です。

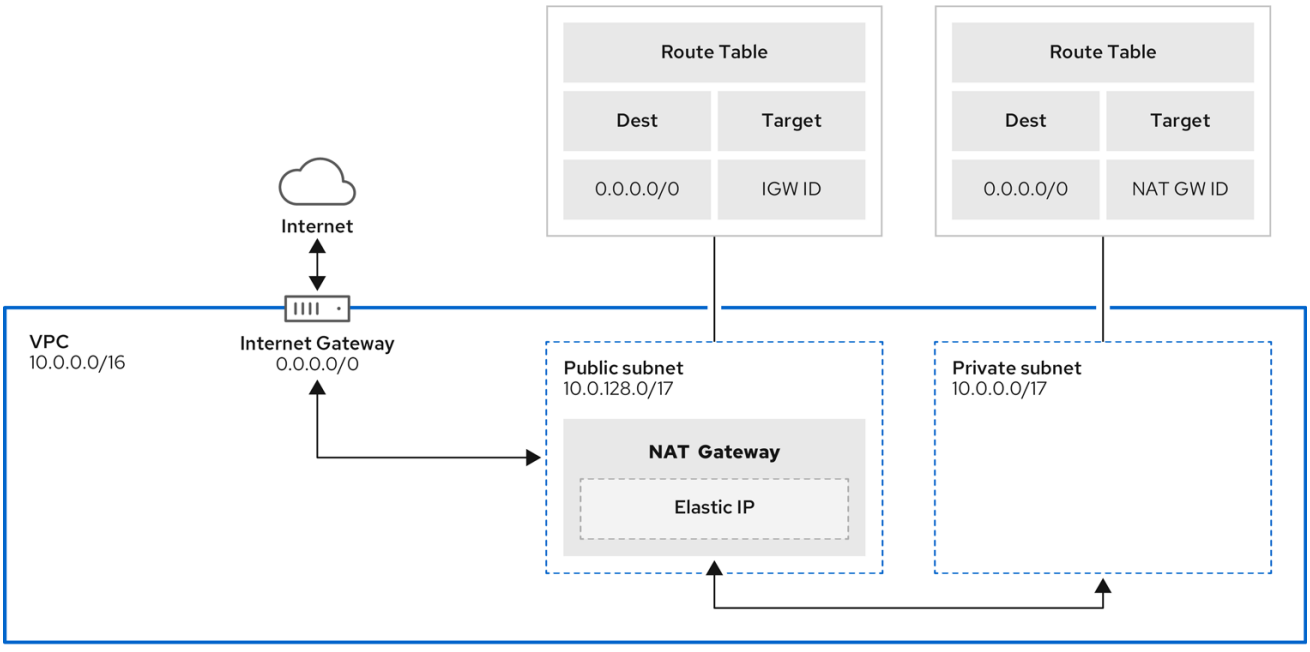
- **サブネット**: 単一アベイラビリティーゾーンがあるクラスターの 2 つのサブネット、または複数のアベイラビリティーゾーンがあるクラスターの 6 つのサブネット。

**注記**

**パブリックサブネット** は、インターネットゲートウェイを介してインターネットに直接接続します。**プライベートサブネット** は、ネットワークアドレス変換 (NAT) ゲートウェイを介してインターネットに接続します。

- **ルートテーブル**: プライベートサブネットごとに 1 つのルートテーブルと、クラスターごとに 1 つの追加テーブル。
- **インターネットゲートウェイ**: クラスターごとに 1 つのインターネットゲートウェイ。
- **NAT ゲートウェイ**: パブリックサブネットごとに 1 つの NAT ゲートウェイ。

**図11.1 サンプル VPC アーキテクチャー**




#### 11.1.4.6. セキュリティーグループ

AWS セキュリティーグループは、プロトコルおよびポートアクセスレベルでセキュリティーを提供します。これらは EC2 インスタンスおよび Elastic Load Balancing (ELB) ロードバランサーに関連付けられます。各セキュリティーグループには、1 つ以上の EC2 インスタンスの送受信トラフィックをフィルタリングする一連のルールが含まれます。OpenShift インストールに必要なポートがネットワーク上で開いており、ホスト間のアクセスを許可するよう設定されていることを確認する必要があります。

**表11.1 デフォルトのセキュリティーグループに必要なポート**

| グループ | タイプ | IP プロトコル | ポート範囲 |
|---|---|---|---|
| MasterSecurityGroup | **AWS::EC2::SecurityGroup** | **icmp** | **0** |
| | | **tcp** | **22** |
| | | **tcp** | **6443** |
| | | **tcp** | **22623** |
| WorkerSecurityGroup | **AWS::EC2::SecurityGroup** | **icmp** | **0** |
| | | **tcp** | **22** |
| BootstrapSecurityGroup | **AWS::EC2::SecurityGroup** | **tcp** | **22** |
| | | **tcp** | **19531** |

#### 11.1.4.6.1. 追加のカスタムセキュリティーグループ

既存の管理対象外の VPC を使用してクラスターを作成する場合、クラスターの作成中に追加のカスタムセキュリティーグループを追加できます。カスタムセキュリティーグループには次の制限があります。

- クラスターを作成する前に、AWS でカスタムセキュリティーグループを作成する必要があります。詳細は、Amazon EC2 security groups for Linux instances を参照してください。
- カスタムセキュリティーグループを、クラスターのインストール先の VPC に関連付ける必要があります。カスタムセキュリティーグループを別の VPC に関連付けることはできません。
- カスタムセキュリティーグループを追加する場合は、VPC の追加クォータをリクエストする必要がある場合があります。ROSA の AWS クォータ要件については、**環境の準備** の **必要な AWS サービスクォータ** を参照してください。AWS クォータ引き上げのリクエストについては、Requesting a quota increase を参照してください。

### 11.1.5. AWS ファイアウォールの前提条件

**重要**

PrivateLink でデプロイメントされた ROSA クラスターのみが、ファイアウォールを使用して出力トラフィックを制御できます。

このセクションでは、Red Hat OpenShift Service on AWS クラスターからの出力トラフィックを制御で

きるようにするために必要な詳細を提供します。ファイアウォールを使用して出力トラフィックを制御している場合は、以下のドメインとポートの組み合わせへのアクセスを許可するようにファイアウォールを設定する必要があります。Red Hat OpenShift Service on AWS は、フルマネージド Open Shift サービスを提供するためにこのアクセスを必要とします。

**手順**

1. パッケージとツールのインストールおよびダウンロードに使用される以下の URL を許可リストに指定します。

| ドメイン | ポート | 機能 |
|---|---|---|
| **registry.redhat.io** | 443 | コアコンテナーイメージを指定します。 |
| **quay.io** | 443 | コアコンテナーイメージを指定します。 |
| **.quay.io** | 443 | コアコンテナーイメージを指定します。 |
| **sso.redhat.com** | 443 | 必須。**https://console.redhat.com/openshift** サイトでは、**sso.redhat.com** からの認証を使用してプルシークレットをダウンロードし、Red Hat SaaS ソリューションを使用してサブスクリプション、クラスターインベントリー、チャージバックレポートなどのモニタリングを行います。 |
| **quay-registry.s3.amazonaws.com** | 443 | コアコンテナーイメージを指定します。 |
| **ocm-quay-production-s3.s3.amazonaws.com** | 443 | コアコンテナーイメージを指定します。 |
| **quayio-production-s3.s3.amazonaws.com** | 443 | コアコンテナーイメージを指定します。 |
| **cart-rhcos-ci.s3.amazonaws.com** | 443 | Red Hat Enterprise Linux CoreOS (RHCOS) イメージを提供します。 |
| **openshift.org** | 443 | Red Hat Enterprise Linux CoreOS (RHCOS) イメージを提供します。 |
| **registry.access.redhat.com** [1] | 443 | Red Hat Ecosytem Catalog に保存されているすべてのコンテナーイメージをホストします。さらに、レジストリーは、開発者が OpenShift および Kubernetes 上で構築するのに役立つ **odo** CLI ツールへのアクセスを提供します。 |
| **registry.connect.redhat.com** | 443 | すべてのサードパーティーのイメージと認定 Operator に必要です。 |

| ドメイン | ポート | 機能 |
|---|---|---|
| **console.redhat.com** | 443 | 必須。クラスターと OpenShift Console Manager との間の対話が、スケジューリングアップグレードなどの機能を有効にすることを許可します。 |
| **sso.redhat.com** | 443 | **https://console.redhat.com/openshift** サイトは、**sso.redhat.com** からの認証を使用します。 |
| **pull.q1w2.quay.rhcloud.com** | 443 | quay.io が利用できない場合のフォールバックとして、コアコンテナーイメージを提供します。 |
| **.q1w2.quay.rhcloud.com** | 443 | quay.io が利用できない場合のフォールバックとして、コアコンテナーイメージを提供します。 |
| **www.okd.io** | 443 | **openshift.org** サイトは **www.okd.io** にリダイレクトされます。 |
| **www.redhat.com** | 443 | **sso.redhat.com** サイトは **www.redhat.com** にリダイレクトされます。 |
| **aws.amazon.com** | 443 | **iam.amazonaws.com** および **sts.amazonaws.com** サイトは **aws.amazon.com** にリダイレクトされます。 |
| **catalog.redhat.com** | 443 | **registry.access.redhat.com** および **https://registry.redhat.io** サイトは **catalog.redhat.com** にリダイレクトされます。 |
| **dvbwgdztaeq9o.cloudfront.net** [2] | 443 | マネージド OIDC 設定を使用した STS 実装で、 ROSA が使用します。 |

1. ファイアウォール環境では、**access.redhat.com** リソースが許可リストに含まれていることを確認してください。このリソースは、コンテナークライアントが **registry.access.redhat.com** からイメージを取得するときにイメージを検証するために必要な署名ストアをホストします。

2. リソースのリダイレクトが必要な大規模なクラウドフロントの停止が発生した場合、**cloudfront.net** の前の英数字の文字列が変更される可能性があります。

**quay.io** などのサイトを許可リストに追加するには、**.quay.io** などのワイルドカードエントリーを拒否リストに加えないでください。ほとんどの場合、イメージレジストリーはコンテンツ配信ネットワーク (CDN) を使用してイメージを提供します。ファイアウォールがアクセスを

ブロックすると、初回のダウンロード要求が **cdn01.quay.io** などのホスト名にリダイレクトされると、イメージのダウンロードが拒否されます。

**cdn01.quay.io** などの CDN ホスト名は、許可リストに **.quay.io** などのワイルドカードエントリーを追加する場合に説明されます。

2. 次のテレメトリー URL を許可リストします。

| ドメイン | ポート | 機能 |
|---|---|---|
| **cert-api.access.redhat.com** | 443 | テレメトリーで必要です。 |
| **api.access.redhat.com** | 443 | テレメトリーで必要です。 |
| **infogw.api.openshift.com** | 443 | テレメトリーで必要です。 |
| **console.redhat.com** | 443 | テレメトリーと Red Hat Insights で必要です。 |
| **cloud.redhat.com/api/ingress** | 443 | テレメトリーと Red Hat Insights で必要です。 |
| **observatorium-mst.api.openshift.com** | 443 | Managed OpenShift 固有のテレメトリーに使用されます。 |
| **observatorium.api.openshift.com** | 443 | Managed OpenShift 固有のテレメトリーに使用されます。 |

マネージドクラスターでは、テレメトリーを有効にして、Red Hat が問題に迅速に対応し、顧客をより適切にサポートし、製品のアップグレードがクラスターに与える影響をよりよく理解できるようにする必要があります。Red Hat によるリモートヘルスモニタリングデータの使用方法について、詳細は **関連情報** セクションの **リモートヘルスモニタリングについて** を参照してください。

3. 次の Amazon Web Services (AWS) API URI を許可リストします。

| ドメイン | ポート | 機能 |
|---|---|---|
| **.amazonaws.com** | 443 | AWS サービスおよびリソースへのアクセスに必要です。 |

または、Amazon Web Services (AWS) API にワイルドカードを使用しない場合は、次の URL を許可リストに追加する必要があります。

| ドメイン | ポート | 機能 |
|---|---|---|

| ドメイン | ポート | 機能 |
| --- | --- | --- |
| **ec2.amazonaws.com** | 443 | AWS 環境でのクラスターのインストールや管理に使用されます。 |
| **events.<aws_region>.amazonaws.com** | 443 | AWS 環境でのクラスターのインストールや管理に使用されます。 |
| **iam.amazonaws.com** | 443 | AWS 環境でのクラスターのインストールや管理に使用されます。 |
| **route53.amazonaws.com** | 443 | AWS 環境でのクラスターのインストールや管理に使用されます。 |
| **sts.amazonaws.com** | 443 | AWS STS のグローバルエンドポイントを使用するように設定されたクラスターの場合は、AWS 環境にクラスターをインストールおよび管理するために使用されます。 |
| **sts.<aws_region>.amazonaws.com** | 443 | AWS STS の地域化されたエンドポイントを使用するように設定されたクラスターの場合は、AWS 環境にクラスターをインストールおよび管理するために使用されます。詳細は、AWS STS の地域化されたエンドポイント を参照してください。 |
| **tagging.us-east-1.amazonaws.com** | 443 | AWS 環境でのクラスターのインストールや管理に使用されます。このエンドポイントは、クラスターがデプロイメントされているリージョンに関係なく、常に us-east-1 です。 |
| **ec2.<aws_region>.amazonaws.com** | 443 | AWS 環境でのクラスターのインストールや管理に使用されます。 |
| **elasticloadbalancing.<aws_region>.amazonaws.com** | 443 | AWS 環境でのクラスターのインストールや管理に使用されます。 |
| **servicequotas.<aws_region>.amazonaws.com** | 443 | 必須。サービスをデプロイするためのクォータを確認するのに使用されます。 |
| **tagging.<aws_region>.amazonaws.com** | 443 | タグの形式で AWS リソースに関するメタデータを割り当てることができます。 |

4. 以下の OpenShift URL を許可リストします。

| ドメイン | ポート | 機能 |
| --- | --- | --- |
| **mirror.openshift.com** | 443 | ミラーリングされたインストールのコンテンツおよびイメージへのアクセスに使用されます。Cluster Version Operator (CVO) には単一の機能ソースのみが必要ですが、このサイトはリリースイメージ署名のソースでもあります。 |
| **storage.googleapis.com/openshift-release** (推奨) | 443 | mirror.openshift.com/ の代替サイト。quay.io からプルするイメージを把握するのにクラスターが使用するプラットフォームリリース署名をダウンロードするのに使用されます。 |
| **api.openshift.com** | 443 | クラスターに更新が利用可能かどうかを確認するのに使用されます。 |

5. 次のサイトリライアビリティーエンジニアリング (SRE) および管理 URL を許可リストします。

| ドメイン | ポート | 機能 |
| --- | --- | --- |
| **api.pagerduty.com** | 443 | このアラートサービスは、クラスター内の alertmanager が使用します。これにより、Red Hat SRE に対してイベントの SRE 通知についてのアラートが送信されます。 |
| **events.pagerduty.com** | 443 | このアラートサービスは、クラスター内の alertmanager が使用します。これにより、Red Hat SRE に対してイベントの SRE 通知についてのアラートが送信されます。 |
| **api.deadmanssnitch.com** | 443 | Red Hat OpenShift Service on AWS がクラスターが使用可能で実行中であるかどうかを示す定期的な ping を送信するために使用するアラートサービス。 |
| **nosnch.in** | 443 | Red Hat OpenShift Service on AWS がクラスターが使用可能で実行中であるかどうかを示す定期的な ping を送信するために使用するアラートサービス。 |

| ドメイン | ポート | 機能 |
| --- | --- | --- |
| **.osdsecuritylogs.splunkcloud.com** または **inputs1.osdsecuritylogs.splunkcloud.cominputs2.osdsecuritylogs.splunkcloud.cominputs4.osdsecuritylogs.splunkcloud.cominputs5.osdsecuritylogs.splunkcloud.cominputs6.osdsecuritylogs.splunkcloud.cominputs7.osdsecuritylogs.splunkcloud.cominputs8.osdsecuritylogs.splunkcloud.cominputs9.osdsecuritylogs.splunkcloud.cominputs10.osdsecuritylogs.splunkcloud.cominputs11.osdsecuritylogs.splunkcloud.cominputs12.osdsecuritylogs.splunkcloud.cominputs13.osdsecuritylogs.splunkcloud.cominputs14.osdsecuritylogs.splunkcloud.cominputs15.osdsecuritylogs.splunkcloud.com** | 9997 | **splunk-forwarder-operator** によって使用され、ログベースのアラートについて Red Hat SRE が使用するロギング転送エンドポイントとして使用されます。 |
| **http-inputs-osdsecuritylogs.splunkcloud.com** | 443 | 必須。**splunk-forwarder-operator** によって使用され、ログベースのアラートについて Red Hat SRE が使用するロギング転送エンドポイントとして使用されます。 |
| **sftp.access.redhat.com** (推奨) | 22 | **must-gather-operator** が、クラスターに関する問題のトラブルシューティングに役立つ診断ログをアップロードするのに使用される SFTP サーバー。 |

6. オプションのサードパーティーコンテンツに対する次の URL を許可リストに追加します。

| ドメイン | ポート | 機能 |
| --- | --- | --- |
| **registry.connect.redhat.com** | 443 | すべてのサードパーティーのイメージと認定 Operator に必要です。 |
| **rhc4tp-prod-z8cxf-image-registry-us-east-1-evenkyleffocxqvofrk.s3.dualstack.us-east-1.amazonaws.com** | 443 | **registry.connect.redhat.com** でホストされているコンテナーイメージにアクセスできます |
| **oso-rhc4tp-docker-registry.s3-us-west-2.amazonaws.com** | 443 | Sonatype Nexus、F5 Big IP Operator に必要です。 |

7. Amazon Web Services (AWS) API のワイルドカードを許可しなかった場合は、内部 OpenShift レジストリーに使用される S3 バケットも許可する必要があります。そのエンドポイントを取得するには、クラスターが正常にプロビジョニングされた後に次のコマンドを実行します。

```
$ oc -n openshift-image-registry get pod -l docker-registry=default -o json | jq
'.items[].spec.containers[].env[] | select(.name=="REGISTRY_STORAGE_S3_BUCKET")'
```

S3 エンドポイントは次の形式にする必要があります。

```
'<cluster-name>-<random-string>-image-registry-<cluster-region>-<random-
string>.s3.dualstack.<cluster-region>.amazonaws.com'.
```

8. ビルドに必要な言語またはフレームワークのリソースを提供するサイトを許可リストに指定します。
9. OpenShift で使用される言語およびフレームワークに依存するアウトバウンド URL を許可リストに指定します。ファイアウォールまたはプロキシーで許可できる推奨 URL のリストは、OpenShift Outbound URLs to Allow を参照してください。

**関連情報**

- リモートヘルスモニタリングについて
- セキュリティーグループ
- 必要な AWS サービスクォータ

### 11.1.6. 次のステップ

- 必要な AWS サービスクォータの確認

### 11.1.7. 関連情報

- 制限およびスケーラビリティー
- SRE のすべての Red Hat OpenShift Service on AWS 4 クラスターへのアクセス
- ROSA デプロイメントワークフローを理解する

## 11.2. ROSA デプロイメントワークフローを理解する

Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する前に、AWS の前提条件を満たし、必要な AWS サービスクォータが利用可能であることを確認し、環境をセットアップする必要があります。

このドキュメントでは、ROSA のワークフローステージの概要と、各ステージの詳細なリソースを説明します。

**ヒント**

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

### 11.2.1. ROSA デプロイメントワークフローの概要

このセクションで説明されているワークフローステージに従い、Red Hat OpenShift Service on AWS (ROSA) クラスターを設定し、アクセスできます。

1. AWS の前提条件の実行。ROSA クラスターをデプロイするには、AWS アカウントが前提条件を満たしている必要があります。
2. 必要な AWS サービスクォータの確認。クラスターのデプロイメントを準備するには、ROSA クラスターの実行に必要な AWS サービスクォータを確認します。
3. AWS アカウントの設定。ROSA クラスターを作成する前に、AWS アカウントで ROSA を有効にし、AWS CLI (**aws**) ツールをインストールして設定し、AWS CLI ツールの設定を確認する必要があります。
4. ROSA および Open Shift CLI ツールのインストールと、AWS サービスクォータの確認 。ROSA CLI (**rosa**)、OpenShift CLI (**oc**) をインストールし、設定します。ROSA CLI を使用して、必要な AWS リソースクォータが利用可能かどうかを確認できます。
5. ROSA クラスターの作成 か AWS PrivateLink を使用した ROSA クラスターの作成 。ROSA CLI (**rosa**) を使用してクラスターを作成します。オプションで、AWS PrivateLink を使用して ROSA クラスターを作成できます。
6. クラスターへのアクセス。アイデンティティープロバイダーを設定し、必要に応じてクラスター管理者権限をアイデンティティープロバイダーユーザーに付与できます。**cluster-admin** ユーザーを設定して、新たにデプロイされたクラスターにすばやくアクセスすることもできます。
7. ユーザーの ROSA クラスターへのアクセスを取り消す。ROSA CLI または Web コンソールを使用して、ROSA クラスターへのアクセス権をユーザーから取り消すことができます。
8. ROSA クラスターの削除。ROSA CLI (**rosa**) を使用して、ROSA クラスターを削除できます。

### 11.2.2. 関連情報

- ROSA デプロイメントワークフローを使用して AWS Security Token Service (STS) を使用するクラスターを作成する方法については、STS を使用する ROSA のデプロイメントワークフローについて を参照してください。
- アイデンティティープロバイダーの設定
- クラスターの削除
- クラスターへのアクセスの削除
- クラスターおよびユーザーを作成するためのコマンドのクイックリファレンス

## 11.3. 必要な AWS サービスクォータ

Red Hat OpenShift Service on AWS クラスターの実行に必要な Amazon Web Service (AWS) サービスクォータのリストを確認します。

**ヒント**

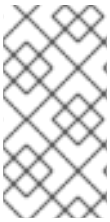
AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

### 11.3.1. 必要な AWS サービスクォータ

以下の表は、1 つの Red Hat OpenShift Service on AWS クラスターを作成して実行するために必要な AWS サービスのクォータとレベルを示しています。ほとんどのデフォルト値は大抵のワークロードに適していますが、次の場合には追加クォータのリクエストが必要になることがあります。

- ROSA クラスターには少なくとも 100 個の vCPU が必要ですが、Running On-Demand Standard の Amazon EC2 インスタンスに割り当てられる vCPU のデフォルトの最大値は **5** です。したがって、以前に同じ AWS アカウントを使用して ROSA クラスターを作成したことがない場合は、**Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances** を実行するための追加の EC2 クォータをリクエストする必要があります。

- カスタムセキュリティーグループなど、一部のオプションのクラスター設定機能により、追加クォータのリクエストが必要になることがあります。たとえば、ROSA はデフォルトで 1 つのセキュリティーグループをワーカーマシンプールのネットワークインターフェイスに関連付けますが、**Security groups per network interface** のデフォルトのクォータは **5** であるため、5 つのカスタムセキュリティーグループを追加するには、追加のクォータをリクエストする必要があります。セキュリティーグループを追加すると、ワーカーのネットワークインターフェイス上のセキュリティーグループが、合計 6 つになるためです。



**注記**

AWS SDK を使用すると、ROSA はクォータをチェックできますが、AWS SDK の計算では、既存の使用量が考慮されません。そのため、クォータチェックが AWS SDK で合格しても、クラスターの作成が失敗する可能性があります。この問題を修正するには、クォータを増やします。

特定のクォータを変更または増やす必要がある場合は、Amazon のドキュメントの requesting a quota inscrease を参照してください。大きなクォータリクエストはレビューのために Amazon サポートに送信され、承認されるまでに時間がかかります。クォータリクエストが緊急の場合は、AWS サポートにお問い合わせください。

**表11.2 ROSA に必要なサービスクォータ**

| クォータ名 | サービスコード | クォータコード | AWS のデフォルト | 最小要件 | 説明 |
|---|---|---|---|---|---|

| クォータ名 | サービスコード | クォータコード | AWS のデフォルト | 最小要件 | 説明 |
|---|---|---|---|---|---|
| Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances | ec2 | L-1216C47A | 5 | 100 | オンデマンド標準 (A、C、D、H、I、M、R、T、Z) インスタンスの実行に割り当てられる vCPU の最大数。<br><br>デフォルト値の 5 vCPU は、ROSA クラスターを作成するには不十分です。ROSA では、クラスター作成に必要な vCPU は最低 100 個です。 |
| Storage for General Purpose SSD (gp2) volume storage in TiB | ebs | L-D18FCD1D | 50 | 300 | このリージョンの汎用 SSD (gp2) ボリューム全体にプロビジョニングできるストレージの最大集計量 (TiB 単位)。 |
| Storage for General Purpose SSD (gp3) volume storage in TiB | ebs | L-7A658B76 | 50 | 300 | このリージョンの汎用 SSD (gp3) ボリューム全体にプロビジョニングできるストレージの最大集計量 (TiB 単位)。<br><br>最適なパフォーマンスを得るには、300 TiB のストレージが最低限必要です。 |

| クォータ名 | サービスコード | クォータコード | AWS のデフォルト | 最小要件 | 説明 |
|---|---|---|---|---|---|
| Storage for Provisioned IOPS SSD (io1) volumes in TiB | ebs | L-FD252861 | 50 | 300 | このリージョンのプロビジョンド IOPS SSD (io1) ボリューム全体にプロビジョニングできるストレージの最大集計量 (TiB 単位)。<br><br>最適なパフォーマンスを得るには、300 TiB のストレージが最低限必要です。 |

**表11.3 一般的な AWS サービスクォータ**

| クォータ名 | サービスコード | クォータコード | AWS のデフォルト | 最小要件 | 説明 |
|---|---|---|---|---|---|
| EC2-VPC Elastic IPs | ec2 | L-0263D0A3 | 5 | 5 | このリージョンで EC2-VPC に割り当てることができる Elastic IP アドレスの最大数。 |
| VPCs per Region | vpc | L-F678F1CE | 5 | 5 | リージョンあたりの VPC の最大数。このクォータは、リージョンあたりのインターネットゲートウェイの最大数に直接関係しています。 |

| クォータ名 | サービスコード | クォータコード | AWS のデフォルト | 最小要件 | 説明 |
|---|---|---|---|---|---|
| Internet gateways per Region | vpc | L-A4707A72 | 5 | 5 | リージョンあたりのインターネットゲートウェイの最大数。このクォータは、リージョンあたりの VPC の最大数に直接関係しています。このクォータを増やすには、リージョンあたりの VPC の数を増やします。 |
| Network interfaces per Region | vpc | L-DF5E4CA3 | 5,000 | 5,000 | リージョンあたりのネットワークインターフェイスの最大数。 |
| Security groups per network interface | vpc | L-2AFB9258 | 5 | 5 | ネットワークインターフェイスごとのセキュリティーグループの最大数。セキュリティーグループごとのルール数のクォータとこのクォータを掛けた値が 1000 を超えることはできません。 |
| Snapshots per Region | ebs | L-309BACF6 | 10,000 | 10,000 | リージョンあたりのスナップショットの最大数 |

| クォータ名 | サービスコード | クォータコード | AWS のデフォルト | 最小要件 | 説明 |
|---|---|---|---|---|---|
| IOPS for Provisioned IOPS SSD (Io1) volumes | ebs | L-B3A130E6 | 300,000 | 300,000 | このリージョンのプロビジョンド IOPS SSD (io1) ボリューム全体にプロビジョニングできる IOPS の最大集計数。 |
| Application Load Balancers per Region | elasticloadbalancing | L-53DA6B97 | 50 | 50 | 各リージョンに存在できる Application Load Balancer の最大数。 |
| Classic Load Balancers per Region | elasticloadbalancing | L-E9E9831D | 20 | 20 | 各リージョンに存在できる Classic Load Balancer の最大数。 |

#### 11.3.1.1. 関連情報

- AWS CLI コマンドを使用して、サービスクォータの引き上げリクエストをリクエスト、表示、および管理する方法
- ROSA サービスクォータ
- クォータの引き上げをリクエストする

### 11.3.2. 次のステップ

- AWS アカウントの設定

### 11.3.3. 関連情報

- ROSA デプロイメントワークフローを理解する

## 11.4. AWS アカウントの設定

AWS の前提条件が完了したら、AWS アカウントを設定し、Red Hat OpenShift Service on AWS (ROSA) サービスを有効にします。

**ヒント**

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

### 11.4.1. AWS アカウントの設定

AWS アカウントを ROSA サービスを使用するように設定するには、以下の手順を実行します。

**前提条件**

- デプロイメントの前提条件およびポリシーを確認し、完了している。
- Red Hat アカウント がない場合は作成している。次に、確認リンクについてのメールを確認する。ROSA をインストールするには認証情報が必要です。

**手順**

1. 使用する Amazon Web Services (AWS) アカウントにログインします。
実稼働クラスターを実行するには、専用の AWS アカウントを使用することが推奨されます。
AWS Organizations を使用している場合は、組織内の AWS アカウントを使用するか、アカウントを新規作成 できます。

   AWS Organizations を使用しており、使用する予定の AWS アカウントにサービスコントロールポリシー (SCP) を適用する必要がある場合は、最小限必要な SCP についての詳細を AWS 前提条件で確認してください。

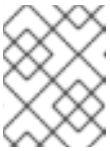
   クラスター作成プロセスの一環として、**rosa** は **osdCcsAdmin** IAM ユーザーを作成します。このユーザーは、AWS CLI の設定時に指定する IAM 認証情報を使用します。

   **注記**

   このユーザーは **Programmatic** アクセスを有効にしており、**AdministratorAccess** ポリシーがこれに割り当てられています。

2. AWS コンソールで ROSA サービスを有効にします。
   a. AWS アカウント にサインインします。
   b. ROSA を有効にするには、ROSA service に移動し、**Enable OpenShift** を選択します。
3. AWS CLI をインストールし、設定します。
   a. AWS コマンドラインインターフェイスのドキュメントを参照し、オペレーティングシステムの AWS CLI を インストール し、設定 します。
   **.aws/credentials** ファイルで正しい **aws_access_key_id** および **aws_secret_access_key** を指定します。AWS ドキュメントの AWS 設定の基本 を参照してください。
   b. デフォルトの AWS リージョンを設定します。

   **注記**

   環境変数を使用してデフォルトの AWS リージョンを設定することが推奨されます。

   ROSA は以下の優先順位でリージョンを評価します。

   i. **--region** フラグを指定して **rosa** コマンドを実行する際に指定されるリージョン。

ii. **AWS_DEFAULT_REGION** 環境変数に設定されるリージョン。AWS ドキュメントの Environment variables to configure the AWS CLI を参照してください。

iii. AWS 設定ファイルで設定されるデフォルトのリージョン。AWS ドキュメントの Quick configuration with aws configure を参照してください。

c. オプション: AWS の名前付きプロファイルを使用して AWS CLI 設定および認証情報を設定します。**rosa** は以下の優先順位で AWS の名前付きプロファイルを評価します。

i. **rosa** コマンドを **--profile** フラグを指定して実行する場合に指定されるプロファイル。

ii. **AWS_PROFILE** 環境変数に設定されるプロファイル。AWS ドキュメントの Named profiles を参照してください。

d. 以下のコマンドを実行して AWS API をクエリーし、AWS CLI がインストールされ、正しく設定されていることを確認します。

```
$ aws sts get-caller-identity --output text
```

**出力例**

```
<aws_account_id>  arn:aws:iam::<aws_account_id>:user/<username>  <aws_user_id>
```

これらの手順を完了したら、ROSA をインストールします。

### 11.4.2. 次のステップ

- ROSA CLI のインストール

### 11.4.3. 関連情報

- AWS 前提条件
- 必要な AWS サービスクォータおよび要求の増加
- ROSA デプロイメントワークフローを理解する

## 11.5. RED HAT OPENSHIFT SERVICE ON AWS (ROSA) CLI (ROSA) のインストール

AWS アカウントを設定したら、Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールし、設定します。

### ヒント

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

### 11.5.1. ROSA CLI のインストールと設定

Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールし、設定します。OpenShift CLI (**oc**) をインストールし、ROSA CLI (**rosa**) を使用して、必要な AWS リソースクォータが利用可能かどうかを確認することもできます。

**前提条件**

- AWS の前提条件および ROSA ポリシーを確認し、完了している。
- Red Hat アカウント がない場合は作成している。次に、確認リンクについてのメールを確認する。ROSA をインストールするには認証情報が必要です。
- AWS アカウントを設定し、AWS アカウントに ROSA サービスを有効にしている。

**手順**

1. Red Hat OpenShift Service on AWS コマンドラインインターフェイス (CLI) の **rosa** をインストールします。
   a. お使いのオペレーティングシステム用の ROSA CLI の 最新リリース をダウンロードします。
   b. オプション: **rosa** にダウンロードした実行可能ファイルの名前を変更します。本書では、**rosa** を使用して実行可能ファイルを参照します。
   c. オプション: **rosa** をパスに追加します。

      **例**

      ```
      $ mv rosa /usr/local/bin/rosa
      ```

   d. 以下のコマンドを実行して、インストールを確認します。

      ```
      $ rosa
      ```

      **出力例**

      ```
      Command line tool for Red Hat OpenShift Service on AWS.
      For further documentation visit https://access.redhat.com/documentation/ja-jp/red_hat_openshift_service_on_aws

      Usage:
        rosa [command]

      Available Commands:
        completion  Generates completion scripts
        create      Create a resource from stdin
        delete      Delete a specific resource
        describe    Show details of a specific resource
        download    Download necessary tools for using your cluster
        edit        Edit a specific resource
        grant       Grant role to a specific resource
        help        Help about any command
        init        Applies templates to support Red Hat OpenShift Service on AWS
        install     Installs a resource into a cluster
        link        Link a ocm/user role from stdin
      ```

```
  list        List all resources of a specific type
  login       Log in to your Red Hat account
  logout      Log out
  logs        Show installation or uninstallation logs for a cluster
  revoke      Revoke role from a specific resource
  uninstall   Uninstalls a resource from a cluster
  unlink      UnLink a ocm/user role from stdin
  upgrade     Upgrade a resource
  verify      Verify resources are configured correctly for cluster install
  version     Prints the version of the tool
  whoami      Displays user account information

Flags:
      --color string   Surround certain characters with escape sequences to display them in
color on the terminal. Allowed options are [auto never always] (default "auto")
      --debug          Enable debug mode.
  -h, --help           help for rosa

Use "rosa [command] --help" for more information about a command.
```

e. オプション: ROSA CLI のコマンド補完スクリプトを生成します。以下の例では、Linux マシン用の Bash 補完スクリプトを生成します。

```
$ rosa completion bash | sudo tee /etc/bash_completion.d/rosa
```

f. オプション: 既存のターミナルから ROSA CLI のコマンド補完を有効にします。次の例では、Linux マシン上の既存のターミナルで **rosa** の Bash 補完を有効にします。

```
$ source /etc/bash_completion.d/rosa
```

2. **rosa** で Red Hat アカウントにログインします。

a. 以下のコマンドを入力します。

```
$ rosa login
```

b. **<my_offline_access_token>** をトークンに置き換えます。

**出力例**

```
To login to your Red Hat account, get an offline access token at
https://console.redhat.com/openshift/token/rosa
? Copy the token and paste it here: <my-offline-access-token>
```

**出力例**

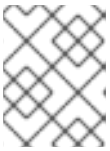
```
I: Logged in as 'rh-rosa-user' on 'https://api.openshift.com'
```

3. 以下のコマンドを実行して、AWS アカウントに必要なパーミッションがあることを確認します。

```
$ rosa verify permissions
```

**出力例**

```
I: Validating SCP policies...
I: AWS SCP policies ok
```



**注記**

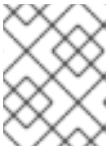
このコマンドは、AWS Security Token Service(STS) を使用しない ROSA クラスターに対してのみパーミッションを検証します。

4. AWS アカウントに、Red Hat OpenShift Service on AWS クラスターにデプロイするのに必要なクォータがあることを確認します。

```
$ rosa verify quota --region=us-west-2
```

**出力例**

```
I: Validating AWS quota...
I: AWS quota ok
```



**注記**

AWS クォータはリージョンによって異なる場合があります。エラーが発生した場合は、別のリージョンを試してください。

クォータを増やす必要がある場合は、AWS コンソール に移動し、失敗したサービスについてクォータの増加を要求します。

パーミッションとクォータの両方のチェックにパスしたら、次のステップに進みます。

5. クラスターデプロイメント用に AWS アカウントを準備します。

   a. 以下のコマンドを実行して、Red Hat および AWS の認証情報が正しく設定されていることを確認します。AWS アカウント ID、デフォルトのリージョンおよび ARN が予想される内容と一致していることを確認します。現時点では、**OCM** で始まる行を安全に無視できます。

```
$ rosa whoami
```

**出力例**

```
AWS Account ID:               000000000000
AWS Default Region:           us-east-2
AWS ARN:                      arn:aws:iam::000000000000:user/hello
OCM API:                      https://api.openshift.com
OCM Account ID:               1DzGIdIhqEWyt8UUXQhSoWaaaaa
OCM Account Name:             Your Name
OCM Account Username:         you@domain.com
OCM Account Email:            you@domain.com
OCM Organization ID:          1HopHfA2hcmhup5gCr2uH5aaaaa
OCM Organization Name:        Red Hat
OCM Organization External ID: 0000000
```

b. AWS アカウントを初期化します。この手順では、クラスターのデプロイメントおよび管理用に AWS アカウントを準備するために CloudFormation テンプレートを実行します。このステップには通常、完了までに 1 - 2 分の時間がかかります。

```
$ rosa init
```

**出力例**

```
I: Logged in as 'rh-rosa-user' on 'https://api.openshift.com'
I: Validating AWS credentials...
I: AWS credentials are valid!
I: Validating SCP policies...
I: AWS SCP policies ok
I: Validating AWS quota...
I: AWS quota ok
I: Ensuring cluster administrator user 'osdCcsAdmin'...
I: Admin user 'osdCcsAdmin' created successfully!
I: Verifying whether OpenShift command-line tool is available...
E: OpenShift command-line tool is not installed.
Run 'rosa download oc' to download the latest version, then add it to your PATH.
```

6. ROSA CLI から OpenShift CLI (**oc**) をインストールします。

a. 以下のコマンドを入力して、最新バージョンの **oc** CLI をダウンロードします。

```
$ rosa download oc
```

b. **oc** CLI をダウンロードした後に、これをデプロイメントし、パスに追加します。

c. 以下のコマンドを実行して、**oc** CLI が正常にインストールされていることを確認します。

```
$ rosa verify oc
```

ROSA のインストール後に、クラスターを作成する準備が整います。

### 11.5.2. 次のステップ

- ROSA クラスターを作成 するか、ROSA で AWS PrivateLink クラスターを作成 します。

### 11.5.3. 関連情報

- AWS 前提条件
- 必要な AWS サービスクォータおよび要求の増加
- ROSA デプロイメントワークフローを理解する

## 11.6. AWS STS を使用せずに ROSA クラスターの作成

環境を設定して Red Hat OpenShift Service on AWS (ROSA) をインストールした後に、クラスターを作成します。

本書では、ROSA クラスターを設定する方法を説明します。または、AWS PrivateLink を使用して ROSA クラスターを作成できます。

### ヒント

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

## 11.6.1. クラスターの作成

ROSA CLI (**rosa**) を使用して Red Hat OpenShift Service on AWS (ROSA) クラスターを作成できます。

### 前提条件

Red Hat OpenShift Service on AWS がインストールされている。

**注記**

現時点で、AWS 共有 VPC は ROSA インストールではサポートされていません。

### 手順

1. デフォルト設定を使用するか、対話モードでカスタム設定を指定してクラスターを作成できます。クラスターの作成時に他のオプションを表示するには、**rosa create cluster --help** コマンドを入力します。
   クラスターの作成には最長で 40 分かかる場合があります。

**注記**

実稼働環境のワークロードには、複数のアベイラビリティーゾーン (AZ) の使用が推奨されます。デフォルトは単一のアベイラビリティーゾーンです。**--help** を使用してこのオプションを手動で設定する方法の例を確認するか、この設定に関するプロンプトを表示する対話モードを使用します。

- デフォルトのクラスター設定でクラスターを作成するには、以下を実行します。

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

**出力例**

```
I: Creating cluster with identifier '1de87g7c30g75qechgh7l5b2bha6r04e' and name 'rh-rosa-test-cluster1'
I: To view list of clusters and their status, run `rosa list clusters`
I: Cluster 'rh-rosa-test-cluster1' has been created.
I: Once the cluster is 'Ready' you will need to add an Identity Provider and define the list of cluster administrators. See `rosa create idp --help` and `rosa create user --help` for more information.
I: To determine when your cluster is Ready, run `rosa describe cluster rh-rosa-test-cluster1`.
```

- 対話式プロンプトを使用してクラスターを作成するには、以下を実行します。

```
$ rosa create cluster --interactive
```

- ネットワーク IP 範囲を設定するには、以下のデフォルト範囲を使用できます。manual モードを使用する場合の詳細は、**rosa create cluster --help | grep cidr** コマンドを使用します。対話モードでは、設定の入力を求めるプロンプトが出されます。
  - ノード CIDR: 10.0.0.0/16
  - Service CIDR: 172.30.0.0/16
  - Pod CIDR: 10.128.0.0/14

2. 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。クラスターの作成時に、出力の **State** フィールドは **pending** から **installing** に移行し、最終的に **ready** に移行します。

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

**出力例**

```
Name: rh-rosa-test-cluster1
OpenShift Version: 4.6.8
DNS: *.example.com
ID: uniqueidnumber
External ID: uniqueexternalidnumber
AWS Account: 123456789101
API URL: https://api.rh-rosa-test-cluster1.example.org:6443
Console URL: https://console-openshift-console.apps.rh-rosa-test-cluster1.example.or
Nodes: Master: 3, Infra: 2, Compute: 2
Region: us-west-2
Multi-AZ: false
State: ready
Channel Group: stable
Private: No
Created: Jan 15 2021 16:30:55 UTC
Details Page: https://console.redhat.com/examplename/details/idnumber
```

**注記**

インストールが失敗した場合や、40 分後に **State** フィールドが **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に関するドキュメントで詳細を確認してください。

3. OpenShift インストーラーログを監視して、クラスター作成の進捗を追跡します。

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

### 11.6.2. 次のステップ

アイデンティティープロバイダーの設定

### 11.6.3. 関連情報

- ROSA デプロイメントワークフローを理解する

- ROSA クラスターの削除
- ROSA アーキテクチャー

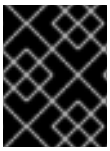
## 11.7. プライベートクラスターの設定

Red Hat OpenShift Service on AWS クラスターをプライベートにし、内部アプリケーションを企業ネットワーク内でホストできるようにします。さらに、プライベートクラスターは、セキュリティーを強化するために内部 API エンドポイントのみを持つように設定できます。

プライバシー設定は、クラスターの作成時またはクラスターの設定後に設定できます。

### 11.7.1. 新規クラスターでのプライベートクラスターの有効化

新規 Red Hat OpenShift Service on AWS クラスターの作成時にプライベートクラスター設定を有効にすることができます。



**重要**

プライベートクラスターは AWS セキュリティートークンサービス (STS) と併用できません。ただし、STS は AWS PrivateLink クラスターをサポートします。

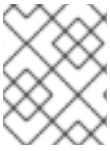
**前提条件**

AWS VPC ピアリング、VPN、DirectConnect、または TransitGateway がプライベートアクセスを許可するよう設定されている。

**手順**

以下のコマンドを入力して新規プライベートクラスターを作成します。

```
$ rosa create cluster --cluster-name=<cluster_name> --private
```



**注記**

または、各クラスターオプションについて **--interactive** を使用してプロンプトを表示します。

### 11.7.2. 既存クラスターでのプライベートクラスターの有効化

クラスターを作成したら、後でクラスターをプライベートにすることができます。

**重要**

プライベートクラスターは AWS セキュリティートークンサービス (STS) と併用できません。ただし、STS は AWS PrivateLink クラスターをサポートします。

**前提条件**

AWS VPC ピアリング、VPN、DirectConnect、または TransitGateway がプライベートアクセスを許可するよう設定されている。

**手順**

以下のコマンドを実行して、既存のクラスターで **--private** オプションを有効にします。

```
$ rosa edit cluster --cluster=<cluster_name> --private
```

**注記**

クラスターをプライベートとパブリックの間で移行するには、完了までに数分の時間がかかる場合があります。

### 11.7.3. 関連情報

- ROSA での AWS PrivateLink クラスターの作成

## 11.8. ROSA クラスターへのアクセスの削除

**rosa** コマンドラインを使用して Red Hat OpenShift Service on AWS (ROSA) クラスターへのアクセスを削除します。

**ヒント**

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

### 11.8.1. ROSA CLI を使用した dedicated-admin アクセスの取り消し

**dedicated-admin** ユーザーのアクセス権を取り消すことができるのは、自分がクラスターを作成したユーザー、組織管理者ユーザー、またはスーパー管理者ユーザーの場合です。

**前提条件**

- アイデンティティープロバイダー (IDP) をクラスターに追加している。
- 取り消す権限を持つユーザーの IDP ユーザー名がある。
- クラスターにログインしている。

**手順**

1. ユーザーの **dedicated-admin** アクセスを取り消すには、次のコマンドを入力してください。

```
$ rosa revoke user dedicated-admin --user=<idp_user_name> --cluster=<cluster_name>
```

2. 以下のコマンドを実行して、ユーザーに **dedicated-admin** アクセスがなくなったことを確認します。出力には、取り消したユーザーが表示されません。

```
$ oc get groups dedicated-admins
```

### 11.8.2. ROSA CLI を使用した cluster-admin アクセス権の取り消し

クラスターを作成したユーザーのみが、**cluster-admin** ユーザーのアクセスを取り消すことができます。

**前提条件**

- アイデンティティープロバイダー (IDP) をクラスターに追加している。
- 取り消す権限を持つユーザーの IDP ユーザー名がある。
- クラスターにログインしている。

**手順**

1. ユーザーの **cluster-admin** アクセスを取り消すには、次のコマンドを入力してください。

```
$ rosa revoke user cluster-admins --user=myusername --cluster=mycluster
```

2. 次のコマンドを入力して、そのユーザーが **cluster-admin** アクセス権を失ったことを確認します。出力には、取り消したユーザーが表示されません。

```
$ oc get groups cluster-admins
```

## 11.9. ROSA クラスターの削除

**rosa** コマンドラインを使用して Red Hat OpenShift Service on AWS (ROSA) クラスターを削除します。

**ヒント**

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

### 11.9.1. 前提条件

- Red Hat OpenShift Service on AWS が VPC を作成した場合は、クラスターを正常に削除する前に、クラスターから次のアイテムを削除する必要があります。
  - VPN 設定や VPC ピアリング接続などのネットワーク設定
  - VPC に追加された追加サービス

これらの設定とサービスが残っている場合、クラスターは適切に削除されません。

### 11.9.2. ROSA クラスターとクラスター固有の IAM リソースの削除

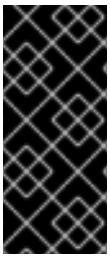
ROSA CLI (**rosa**) または Red Hat OpenShift Cluster Manager を使用して、AWS Security Token Service (STS) クラスターを備えた Red Hat OpenShift Service on AWS (ROSA) を削除できます。

クラスターを削除した後、ROSA CLI (**rosa**) を使用して、AWS アカウントのクラスター固有の Identity and Access Management (IAM) リソースをクリーンアップできます。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。



**重要**

インストール時に VPC を作成したクラスターが削除されると、関連するインストールプログラムで作成された VPC も削除され、同じ VPC を使用しているすべてのクラスターが失敗します。さらに、インストールプログラムによって作成されるリソースと同じ **tagSet** のキーと値のペアで作成され、**owned** の値でラベルが付いたリソースも削除されます。

**前提条件**

- ROSA クラスターをインストールしました。
- 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. クラスター ID、クラスター固有 Operator ロールの Amazon Resource Names (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>
```
(1)

(1) **<cluster_name>** は、クラスター名に置き換えます。

**出力例**

```
Name:                       mycluster
ID:                         1s3v4x39lhs8sm49m90mi0822o34544a
...
Operator IAM Roles:
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-machine-api-aws-cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cloud-credential-operator-cloud-crede
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-image-registry-installer-cloud-creden
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-ingress-operator-cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cluster-csi-drivers-ebs-cloud-credent
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cloud-network-config-controller-cloud
State:                      ready
Private:                    No
Created:                    May 13 2022 11:26:15 UTC
Details Page:
https://console.redhat.com/openshift/details/s/296kyEFwzoy1CREQicFRdZybrc0
OIDC Endpoint URL:          https://oidc.op1.openshiftapps.com/<oidc_config_id>
```
(1) (2) (3)

(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::**

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**

クラスターが削除された後、ROSA CLI (**rosa**) 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 が必要です。

2. クラスターを削除します。

- Red Hat OpenShift Cluster Manager を使用してクラスターを削除するには:

  a. OpenShift Cluster Manager に移動します。

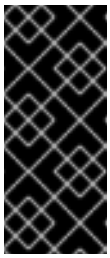
  b. クラスターの横にあるオプションメニュー  をクリックし、**Delete cluster** を選択します。

  c. プロンプトでクラスターの名前を入力し、**Delete** をクリックします。

- ROSA CLI (**rosa**) を使用してクラスターを削除するには:

  a. 以下のコマンドを実行してクラスターを削除し、ログを監視し、**<my-cluster>** 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
```



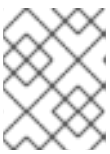
**重要**

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のを待つ必要があります。クラスター固有の Operator ロールは、OpenShift Operator によって作成されるリソースをクリーンアップするために必要です。Operator は、OIDC プロバイダーを利用して認証を行います。

3. クラスター Operator が認証に使用する OIDC プロバイダーを削除します。

```
$ rosa delete oidc-provider -c <cluster_id> --mode auto 1
```

1 **<cluster_id>** をクラスターの ID に置き換えてください。



**注記**

**-y** オプションを使用すると、プロンプトに対して自動的にはいと答えることができます。

4. オプション: クラスター固有の Operator IAM ロールを削除します。

**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。

```
$ rosa delete operator-roles -c <cluster_id> --mode auto 1
```

1 **<cluster_id>** をクラスターの ID に置き換えてください。

**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。

## 11.10. クラスターおよびユーザーを作成するためのコマンドのクイックリファレンス

### ヒント

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

### 11.10.1. コマンドクイックリファレンスのリスト

最初のクラスターおよびユーザーがすでに作成されている場合、このリストは追加のクラスターおよびユーザーの作成時のコマンドクイックリファレンスのリストとして機能します。

```
## Configures your AWS account and ensures everything is setup correctly
$ rosa init

## Starts the cluster creation process (~30-40minutes)
$ rosa create cluster --cluster-name=<cluster_name>

## Connect your IDP to your cluster
$ rosa create idp --cluster=<cluster_name> --interactive

## Promotes a user from your IDP to dedicated-admin level
$ rosa grant user dedicated-admin --user=<idp_user_name> --cluster=<cluster_name>

## Checks if your install is ready (look for State: Ready),
## and provides your Console URL to login to the web console.
$ rosa describe cluster --cluster=<cluster_name>
```

### 11.10.2. 関連情報

- ROSA デプロイメントワークフローを理解する