Red Hat OpenShift Service on AWS 4

環境の準備

Red Hat OpenShift Service on AWS の計画、制限、およびスケーラビリティ

Last Updated: 2024-08-30

Red Hat OpenShift Service on AWS 4 環境の準備

Red Hat OpenShift Service on AWS の計画、制限、およびスケーラビリティ

法律上の通知

概要

このドキュメントでは、クラスターの制限やスケーラビリティーに関する情報など、Red Hat OpenShift Service on AWS (ROSA) クラスターのデプロイに関する計画上の考慮事項を説明します。

目次

第1章 STS を使用する ROSA をデプロイするための前提条件チェックリスト

これは、STS を使用して Red Hat OpenShift Service on AWS (ROSA) のクラシッククラスターを作成するために必要な前提条件のチェックリストです。

注記

このリストは一般的なチェックリストであり、実際の実装は異なる場合があります。

インストールプロセスの実行前に、アクセスできるマシンからこれをデプロイできることを確認します。

- プロビジョニングするクラウドの API サービス。
- **api.openshift.com**、**oidc.op1.openshiftapps.com**、**sso.redhat.com** へのアクセス。
- プロビジョニングするネットワーク上のホスト。
- インストールメディアを取得するインターネット。

重要

ROSA CLI のバージョン 1.2.7 以降、新しいクラスター上の OIDC プロバイダーのエンドポイント URL は、すべて Amazon CloudFront と oidc.op1.openshiftapps.com ドメインを使用します。この変更により、ROSA CLI 1.2.7 以降を使用して作成された新しいクラスターのアクセス速度の向上、遅延の減少、回復性の向上が実現されました。既存の OIDC プロバイダー設定に対してサポートされている移行パスはありません。

1.1. アカウントおよび CLI の前提条件

クラスターをデプロイするためにインストールする必要があるアカウントと CLI。

1.1.1. AWS アカウント

- 以下の情報を収集します。
  - AWS IAM User
  - AWS Access Key ID
  - AWS Secret Access Key
- ROSA の詳細な AWS 管理 IAM ポリシー と、STS を使用する ROSA クラスターの IAM リソース の詳細を参照して、適切なパーミッションがあることを確認してください。
- 詳細は、アカウント を参照してください。

1.1.2. AWS CLI (aws)

- まだインストールしていない場合は AWS コマンドラインインターフェイス からインストールします。

- CLI を設定します。
  1. ターミナルに **aws configure** と入力します。

     ```
     $ aws configure
     ```

  2. AWS Access Key ID を入力し、**enter** を押します。
  3. AWS Secret Access Key を入力し、**enter** を押します。
  4. デプロイするデフォルトのリージョンを入力します。
  5. 必要な出力形式として、“table” または “json” を入力します。
  6. 以下を実行して出力を確認します。

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

  7. 次のコマンドを実行して、ELB のサービスロールがすでに存在していることを確認します。

     ```
     $ aws iam get-role --role-name "AWSServiceRoleForElasticLoadBalancing"
     ```

     a. 存在しない場合は、以下を実行します。

     ```
     $ aws iam create-service-linked-role --aws-service-name
     "elasticloadbalancing.amazonaws.com"
     ```

1.1.3. Red Hat アカウント

- Red Hat Hybrid Cloud Console アカウントがない場合は作成します。

1.1.4. ROSA CLI (rosa)

1. まだ有効にしていない場合は、AWS console の AWS アカウントから ROSA を有効にします。
2. Red Hat OpenShift Service on AWS (ROSA) CLI から、または OpenShift コンソールの AWS コンソール から CLI をインストールします。
3. ターミナルで **rosa login** と入力すると、コンソールから トークンページ に移動するよう求められます。

   ```
   $ rosa login
   ```

4. Red Hat アカウントの認証情報でログインします。
5. **Load token** ボタンをクリックします。
6. トークンをコピーして CLI プロンプトに貼り付けて、**Enter** を押します。
   - あるいは、全 **$ rosa login --token=abc...** コマンドをコピーしてターミナルに貼り付けることもできます。

     ```
     $ rosa login --token=<abc..>
     ```

7. 以下を実行して認証情報を確認します。

```
$ rosa whoami
```

8. 次のコマンドを実行して、十分なクォータがあることを確認します。

```
$ rosa verify quota
```

- ROSA クラスター用にプロビジョニングされた AWS サービスの詳細は、プロビジョニングされた AWS インフラストラクチャー を参照してください。
- AWS サービスクォータの詳細は、必要な AWS サービスクォータ を参照してください。

1.1.5. OpenShift CLI (oc)

1. OpenShift CLI のスタートガイド または OpenShift コンソールの コマンドラインインターフェイス (CLI) ツール からインストールします。
2. 以下を実行して、OpenShift CLI が正しくインストールされていることを確認します。

```
$ rosa verify openshift-client
```

上記の前提条件をインストールして有効にしたら、次の手順に進みます。

1.2. SCP の前提条件

ROSA クラスターは、AWS 組織単位内の AWS アカウントでホストされます。Service Control Policy (SCP) が作成され、AWS サブアカウントのアクセスが許可されるサービスを管理する AWS Organizational Unit に適用されます。

- クラスターに必要なロールやポリシーよりも、組織の SCP の制限が厳しくないことを確認してください。
- コンソールから **Enable ROSA** を選択したときに、必要な **aws-marketplace:Subscribe** パーミッションを許可するように SCP が設定されていることを確認してください。詳細は AWS Organizations service control policy (SCP) is denying required AWS Marketplace permissions を参照してください。
- ROSA クラシッククラスターを作成すると、関連付けられた AWS OpenID Connect (OIDC) ID プロバイダーが作成されます。
  - この OIDC プロバイダー設定は、**us-east-1** AWS リージョンにある公開鍵に依存します。
  - AWS SCP をお持ちのお客様は、これらのクラスターが別のリージョンにデプロイされている場合でも **us-east-1** AWS リージョンを使用できるようにする必要があります。

1.3. ネットワークの前提条件

ネットワークの観点から必要とされる事項。

1.3.1. 最小帯域幅

Red Hat OpenShift Service on AWS では、クラスターをデプロイする際に、クラスターリソースとパブリックインターネットリソース間で 120 Mbps の最小帯域幅が必要です。ネットワーク接続が 120 Mbps

より遅い場合 (たとえば、プロキシー経由で接続している場合)、クラスターのインストールプロセスがタイムアウトし、デプロイメントが失敗します。

デプロイ後のネットワーク要件はワークロードに基づきます。ただし、最小帯域幅 120 Mbps は、クラスターと Operator を適切なタイミングで確実にアップグレードするために役立ちます。

1.3.2. ファイアウォール

- ファイアウォールを設定して、AWS ファイアウォールの前提条件 に記載されているドメインおよびポートへのアクセスを許可します。

1.3.3. 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。クラスターを作成する前に、次の前提条件を満たしていることを確認してください。

- 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。
- カスタムセキュリティーグループを、クラスターの作成に使用している VPC に関連付けます。カスタムセキュリティーグループを他の VPC に関連付けないでください。
- 場合によって、**Security groups per network interface** の AWS クォータの追加を要求する必要があります。

詳細は、セキュリティーグループ の詳細な要件を参照してください。

1.3.4. カスタム DNS

- カスタム DNS を使用する場合、ROSA インストーラーはローカルでホストを解決できるように、デフォルトの DHCP オプションで VPC DNS を使用できる必要があります。
  - これを行うには、**aws ec2 describe-dhcp-options** を実行し、VPC が VPC Resolver を使用しているかどうかを確認します。

    ```
    $ aws ec2 describe-dhcp-options
    ```

- それ以外の場合は、クラスターが内部 IP およびサービスを解決できるように、アップストリーム DNS はクラスタースコープをこの VPC に転送する必要があります。

1.4. PRIVATELINK の前提条件

PrivateLink クラスターをデプロイすることを選択した場合は、必ず既存の BYO VPC にクラスターをデプロイしてください。

- クラスターが使用する AZ ごとにパブリックおよびプライベートのサブネットを作成します。
  - または、インターネット用のトランジットゲートウェイを実装し、適切なルートで出力します。
- VPC の CIDR ブロックには、クラスターマシンの IP アドレスである **Networking.MachineCIDR** 範囲が含まれている必要があります。
  - サブネット CIDR ブロックは、指定したマシン CIDR に属している必要があります。

- **enableDnsHostnames** と **enableDnsSupport** の両方を **true** に設定します。
  - これにより、クラスターは VPC に割り当てられた Route 53 ゾーンを使用して、クラスターの内部 DNS レコードを解決できます。
- 以下を実行してルートテーブルを確認します。

```
----
$ aws ec2 describe-route-tables --filters "Name=vpc-id,Values=<vpc-id>"
----
```

  - クラスターがパブリックサブネットの NAT ゲートウェイまたはトランジットゲートウェイのいずれかを経由して出力できることを確認します。
  - フォローする UDR が設定されていることを確認してください。
- また、インストール中またはインストール後に、クラスター全体のプロキシーを設定することもできます。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。

注記

PrivateLink 以外の ROSA クラスターを既存の BYO VPC にインストールできます。

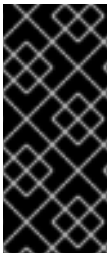
第2章 STS を使用する ROSA をデプロイするための詳細な要件

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。

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。

STS で ROSA をインストールする前に、以下の AWS 前提条件を満たしていることを確認してください。



重要

AWS STS を使用する ROSA クラスターを作成すると、関連付けられた AWS OpenID Connect(OIDC) アイデンティティープロバイダーも作成されます。この OIDC プロバイダー設定は、**us-east-1** AWS リージョンにある公開鍵に依存します。AWS SCP をお持ちのお客様は、これらのクラスターが別のリージョンにデプロイされている場合でも **us-east-1** AWS リージョンを使用できるようにする必要があります。

2.1. デプロイメントに STS を使用する場合のカスタマー要件

AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターをデプロイする前に、以下の前提条件を満たす必要があります。

2.1.1. アカウント

- 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する必要があります。CLI で **rosa verify quota** コマンドを実行すると、クラスターを実行するために必要なクォータがあることが検証されます。

注記

クォータの検証は AWS クォータを確認しますが、消費を AWS クォータと比較しません。詳細は、関連情報の「制限とスケーラビリティリンク」を参照してください。

- SCP ポリシーを適用し、強制される場合、これらのポリシーは、クラスターが必要とするロールおよびポリシーよりも制限的であってはなりません。
- AWS アカウントを Red Hat に譲渡できないようにする必要があります。
- Red Hat のアクティビティーに対する定義されたロールおよびポリシー以外に、追加の AWS 使用制限を課すことはできません。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。
- ネイティブ AWS サービスを同じ AWS アカウントにデプロイできます。
- Elastic Load Balancing (ELB) を設定するために必要なため、アカウントにはサービスにリンクされたロールが設定されている必要があります。以前に AWS アカウントでロードバランサー

を作成していない場合は、ELB のサービスにリンクされたロールを作成する方法について、関連情報の「Elastic Load Balancing (ELB) サービスにリンクされたロールの作成」を参照してください。

注記

Red Hat OpenShift Service on AWS およびその他の Red Hat がサポートするサービスをホストする VPC とは別に、仮想プライベートクラウド (VPC) にリソースをデプロイすることを推奨しますが、必須ではありません。

関連情報

- 制限およびスケーラビリティー
- Elastic Load Balancing (ELB) サービスにリンクされたロールの作成

2.1.2. アクセス要件

- 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。Red Hat は、このアクセスを保護および管理します。
- Red Hat OpenShift Service on AWS (ROSA) クラスター内で権限を昇格するために AWS アカウントを使用しないでください。
- 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、AWS アカウントで直接実行しないでください。
- ROSA クラスターをデプロイするために、事前に設定されたドメインは必要ありません。カスタムドメインを使用する場合は、追加のリソースを参照してください。

関連情報

- アプリケーションのカスタムドメインの設定 を参照してください。

2.1.3. 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許可をお客様から受けている場合があります。
- 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許可をお客様から受けている場合があります。
- 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 クラスターに関する制約、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。

2.1.4. セキュリティー要件

- 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、文書化されたドメインで egress を許可する必要があります。指定されたドメインは、「AWS 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。

関連情報

- AWS ファイアウォールの前提条件

2.1.5. OpenShift Cluster Manager を使用するための要件

以下のセクションでは、OpenShift Cluster Manager の要件を説明します。CLI ツールのみを使用する場合は、この要件を無視できます。

OpenShift Cluster Manager を使用するには、AWS アカウントをリンクする必要があります。このリンクの概念は、アカウントの関連付けとしても知られています。

2.1.5.1. AWS アカウントの関連付け

Red Hat OpenShift Service on AWS (ROSA) クラスタープロビジョニングタスクでは、Amazon リソースネーム (ARN) を使用して、IAM ロール **ocm-role** および **user-role** を AWS アカウントにリンクする必要があります。

ocm-role ARN は Red Hat 組織にラベルとして保存され、 **user-role** ARN は Red Hat ユーザーアカウント内にラベルとして保存されます。Red Hat は、これらの ARN ラベルを使用して、ユーザーが有効なアカウント所有者であり、AWS アカウントで必要なタスクを実行するための正しいアクセス許可が利用可能であることを確認します。

2.1.5.2. AWS アカウントのリンク

Red Hat OpenShift Service on AWS (ROSA) CLI、**rosa** を使用して、AWS アカウントを既存の IAM ロールにリンクできます。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager を使用してクラスターを作成しています。
- AWS アカウント全体のロールをインストールするために必要な権限がある。詳細は、このセクションの関連情報を参照してください。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成しましたが、まだ AWS アカウントにリンクしていません。次のコマンドを実行して、IAM ロールがすでにリンクされているかどうかを確認できます。

  ```
  $ rosa list ocm-role
  ```

  ```
  $ rosa list user-role
  ```

  両方のロールの **Linked** 列に **Yes** が表示されている場合、ロールはすでに AWS アカウントにリンクされています。

手順

1. CLI から、Amazon Resource Name (ARN) を使用して、**ocm-role** リソースを Red Hat 組織にリンクします。

注記

rosa link コマンドを実行するには、Red Hat Organization Administrator (組織管理者権限) が必要です。**ocm-role** リソースを AWS アカウントにリンクすると、組織内のすべてのユーザーに表示されます。

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

出力例

```
I: Linking OCM role
? Link the '<AWS ACCOUNT ID>` role with organization '<ORG ID>'? Yes
I: Successfully linked role-arn '<AWS ACCOUNT ID>' with organization account '<ORG ID>'
```

2. CLI から、Amazon Resource Name (ARN) を使用して、**user-role** リソースを Red Hat ユーザーアカウントにリンクします。

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

出力例

```
I: Linking User role
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125' role with
organization '<AWS ID>'? Yes
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125'
with organization account '<AWS ID>'
```

関連情報

- クラスターの作成に必要な IAM ロールのリストについては、アカウント全体の IAM ロールとポリシー参照 を参照してください。

2.1.5.3. 複数の AWS アカウントを Red Hat 組織に関連付ける

複数の AWS アカウントを Red Hat 組織に関連付けることができます。複数のアカウントを関連付けると、Red Hat 組織の関連付けられた AWS アカウントのいずれかに Red Hat OpenShift Service on AWS (ROSA) クラスターを作成できます。

この機能を使用すると、リージョンにバインドされた環境として複数の AWS プロファイルを使用することにより、さまざまな AWS リージョンにクラスターを作成できます。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager を使用してクラスターを作成しています。
- AWS アカウント全体のロールをインストールするために必要な権限がある。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成している。

手順

追加の AWS アカウントを関連付けるには、最初にローカル AWS 設定でプロファイルを作成します。次に、追加の AWS アカウントに **ocm-role**、user、および account のロールを作成して、アカウントを Red Hat 組織に関連付けます。

追加のリージョンでロールを作成するには、**rosa create** コマンドの実行時に **--profile <aws-profile>** パラメーターを指定し、**<aws_profile>** を追加のアカウントプロファイル名に置き換えます。

- OpenShift Cluster Manager ロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> ocm-role
```

- ユーザーロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> user-role
```

- アカウントロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> account-roles
```

注記

プロファイルを指定しない場合は、デフォルトの AWS プロファイルが使用されます。

2.2. オプトインリージョンでのクラスターデプロイの要件

AWS のオプトインリージョンは、デフォルトで有効になっていないリージョンです。オプトインリージョンで AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターをデプロイする場合には、以下の要件を満たす必要があります。

- リージョンは AWS アカウントで有効にする必要があります。オプトインリージョンの有効化の詳細は、AWS ドキュメント AWS リージョンの管理 を参照してください。
- AWS アカウントのセキュリティートークンバージョンは、バージョン 2 に設定する必要があります。オプトインリージョンにバージョン 1 セキュリティートークンを使用することはできません。

重要

セキュリティートークンのバージョン 2 に更新すると、トークンが長くなるため、トークンを保管するシステムに影響が出ることがあります。詳細は、the AWS documentation on setting STS preferences を参照してください。

2.2.1. AWS セキュリティートークンのバージョン設定

AWS のオプトインリージョンで AWS Security Token Service (STS) を使用して Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する場合は、AWS アカウントでセキュリティートークンのバージョンをバージョン 2 に設定する必要があります。

前提条件

- インストールホストに、最新の AWS CLI をインストールして設定している。

手順

1. AWS CLI の設定で定義されている AWS アカウントの ID をリスト表示します。

```
$ aws sts get-caller-identity --query Account --output json
```

出力が該当する AWS アカウントの ID と一致していることを確認します。

2. AWS アカウントに設定されているセキュリティートークンのバージョンを記載します。

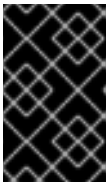
```
$ aws iam get-account-summary --query SummaryMap.GlobalEndpointTokenVersion --
output json
```

出力例

```
1
```

3. AWS アカウントの全リージョンのセキュリティートークンのバージョンをバージョン 2 に更新するには、以下のコマンドを実行します。

```
$ aws iam set-security-token-service-preferences --global-endpoint-token-version v2Token
```



重要

セキュリティートークンのバージョン 2 に更新すると、トークンが長くなるため、トークンを保管するシステムに影響が出ることがあります。詳細は、the AWS documentation on setting STS preferences を参照してください。

2.3. AWS の RED HAT 管理 IAM リファレンス

STS デプロイメントモデルでは、Red Hat は Amazon Web Services (AWS) IAM ポリシー、IAM ユーザー、または IAM ロールを作成し、管理しなくなります。これらのロールとポリシーの作成については、IAM ロールに関する以下のセクションを参照してください。

- **ocm** CLI を使用するには、**ocm-role** および **user-role** リソースが必要です。OpenShift Cluster Manager IAM ロールリソース を参照してください。
- クラスターが 1 つの場合は、アカウント全体の IAM ロールとポリシー参照 を参照してください。
- すべてのクラスターについて、必要な Operator ロールが必要です。クラスター固有の Operator IAM ロール参照 を参照してください。

2.4. 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。

2.4.1. 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。

2.4.2. 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。

2.4.3. 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 に関する ELB ドキュメント を参照してください。

2.4.4. 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。

2.4.5. 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。

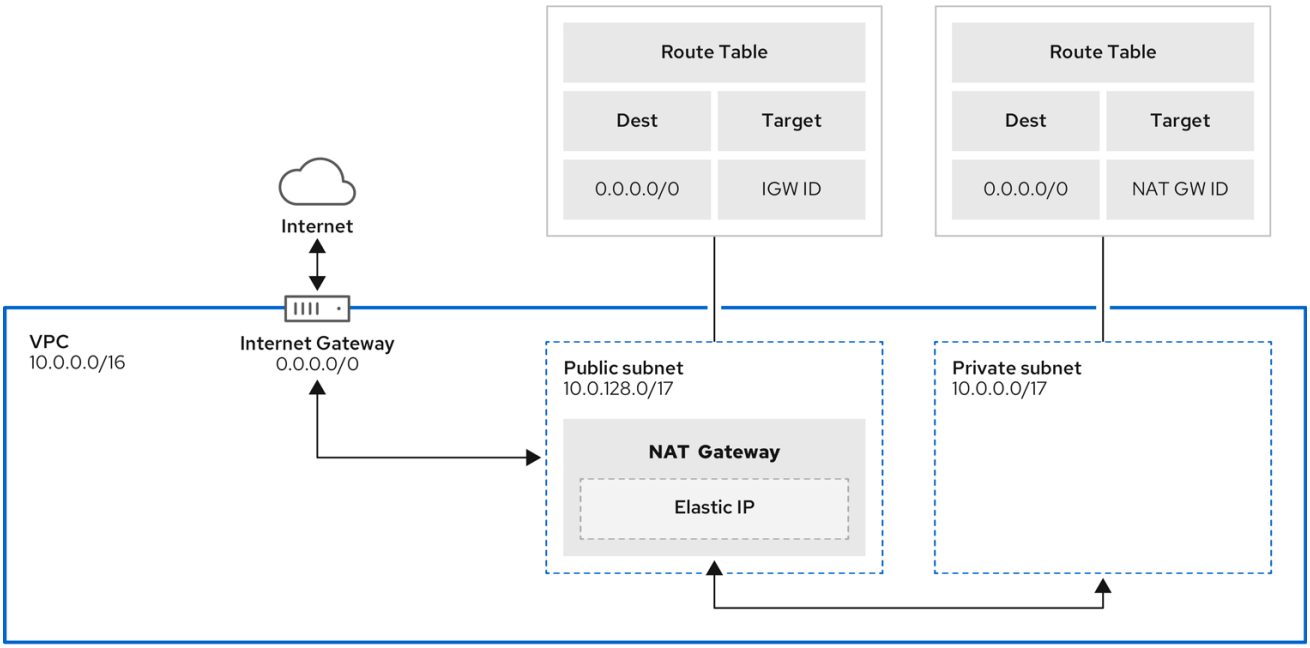
- **サブネット**: 単一アベイラビリティーゾーンがあるクラスターの 2 つのサブネット、または複数のアベイラビリティーゾーンがあるクラスターの 6 つのサブネット。

  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2.1 サンプル VPC アーキテクチャー



2.4.6. 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2.1 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::Security Group**	**icmp**	**0**
		tcp	**22**
		tcp	**6443**
		tcp	**22623**
WorkerSecurityGroup	**AWS::EC2::Security Group**	**icmp**	**0**
		tcp	**22**
BootstrapSecurityGroup	**AWS::EC2::Security Group**	**tcp**	**22**
		tcp	**19531**

2.4.6.1. 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。

2.5. ネットワークの前提条件

2.5.1. 最小帯域幅

Red Hat OpenShift Service on AWS では、クラスターをデプロイする際に、クラスターリソースとパブリックインターネットリソース間で 120 Mbps の最小帯域幅が必要です。ネットワーク接続が 120 Mbps より遅い場合 (たとえば、プロキシー経由で接続している場合)、クラスターのインストールプロセスがタイムアウトし、デプロイメントが失敗します。

デプロイ後のネットワーク要件はワークロードに基づきます。ただし、最小帯域幅 120 Mbps は、クラスターと Operator を適切なタイミングで確実にアップグレードするために役立ちます。

2.5.2. AWS ファイアウォールの前提条件

ファイアウォールを使用して Red Hat OpenShift Service on AWS からの Egress トラフィックを制御している場合は、以下の特定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 OpenShift 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。

2.5.2.1. ROSA Classic

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。

前提条件

- AWS Virtual Private Cloud (VPC) に Amazon S3 ゲートウェイエンドポイントを設定した。このエンドポイントは、クラスターから Amazon S3 サービスへのリクエストを完了するために必要です。

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。
cdn01.quay.io	443	コアコンテナーイメージを指定します。
cdn02.quay.io	443	コアコンテナーイメージを指定します。
cdn03.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	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。
access.redhat.com	443	必須。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。
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 [1]	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。
time-a-g.nist.gov	123 [2]	FedRAMP の NTP トラフィックを許可します。
time-a-wwv.nist.gov	123 [2]	FedRAMP の NTP トラフィックを許可します。

ドメイン	ポート	機能
time-a-b.nist.gov	123 [2]	FedRAMP の NTP トラフィックを許可します。

1. 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。
2. TCP ポートと UDP ポートの両方。

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	Telemetry と Red Hat Insights で必要です。
cloud.redhat.com/api/ingress	443	Telemetry と Red Hat Insights で必要です。
observatorium-mst.api.openshift.com	443	マネージド OpenShift 固有のテレメトリーに使用されます。
observatorium.api.openshift.com	443	マネージド 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の詳細は **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
ec2.amazonaws.com	443	AWS 環境でのクラスターのインストールおよび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および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および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および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および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および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 通知に関する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 通知に関する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. 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。

8. 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。

2.5.2.2. ROSA with HCP

前提条件

- AWS Virtual Private Cloud (VPC) に Amazon S3 ゲートウェイエンドポイントを設定した。このエンドポイントは、クラスターから Amazon S3 サービスへのリクエストを完了するために必要です。

手順

1. パッケージとツールのダウンロードとインストールに使用される次の URL を許可リストに追加します。

ドメイン	ポート	機能
quay.io	443	コアコンテナーイメージを指定します。
cdn01.quay.io	443	コアコンテナーイメージを指定します。
cdn02.quay.io	443	コアコンテナーイメージを指定します。
cdn03.quay.io	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。
registry.redhat.io	443	コアコンテナーイメージを指定します。
registry.access.redhat.com	443	必須。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。
access.redhat.com	443	必須。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。
api.openshift.com	443	必須。クラスターに利用可能な更新を確認するために使用されます。

ドメイン	ポート	機能
mirror.openshift.com	443	必須。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。

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
infogw.api.openshift.com	443	テレメトリーで必要です。
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	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。

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の詳細は **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
sts.<aws_region>.amazonaws.com [1]	443	必須。AWS Secure Token Service (STS) リージョンエンドポイントにアクセスするために使用されます。**<aws-region>** は、クラスターがデプロイされているリージョンに置き換えてください。

ドメイン	ポート	機能
sts.amazonaws.com [2]	443	脚注を参照してください。AWS Secure Token Service (STS) グローバルエンドポイントにアクセスするために使用されます。

1. これは、AWS Virtual Private Cloud (VPC) 内のプライベートインターフェイスエンドポイントをリージョンの AWS STS エンドポイントに設定することによっても実現できます。

2. AWS STS グローバルエンドポイントは、OpenShift 4.14.18 または 4.15.4 より前のバージョンを実行している場合にのみ許可する必要があります。ROSA HCP バージョン 4.14.18+、4.15.4+、および 4.16.0+ は、AWS STS リージョンエンドポイントを使用します。

4. 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	オプション: 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	オプション: **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	オプション: Sonatype Nexus、F5 Big IP Operator に必要です。

5. 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。

6. 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

2.6. 次のステップ

- 必要な AWS サービスクォータの確認

2.7. 関連情報

- SRE のすべての Red Hat OpenShift Service on AWS 4 クラスターへのアクセス

- アプリケーションのカスタムドメインの設定
- インスタンスタイプ

第3章 ROSA IAM ロールのリソース

Red Hat OpenShift Service on AWS (ROSA) Web UI では、OpenShift Cluster Manager および **rosa** コマンドラインインターフェイス (CLI) でエンドユーザーエクスペリエンスを提供するための信頼関係を作成する AWS アカウントに対する特定の権限が必要です。

この信頼関係は **ocm-role** AWS IAM ロールの作成と関連付けによって実現されます。このロールには、Red Hat アカウントを AWS アカウントにリンクする AWS インストーラーとの信頼ポリシーがあります。さらに、Web UI ユーザーごとに**user-role** AWS IAM ロールも必要です。これは、これらのユーザーを特定する役割を果たします。この **user-role** の AWS IAM ロールにはパーミッションがありません。

OpenShift Cluster Manager を使用するために必要な AWS IAM ロールは次のとおりです。

- **ocm-role**
- **user-role**

ROSA CLI (**rosa**) または OpenShift Cluster Manager Web UI のどちらを使用してクラスターを管理する場合でも ROSA CLI で **account-roles** と呼ばれるアカウント全体のロールを作成する必要があります。これらのアカウントのロールは最初のクラスターに必要であり、これらのロールは複数のクラスターで使用できます。これらの必要なアカウントロールは次のとおりです。

- **Worker-Role**
- **Support-Role**
- **Installer-Role**
- **ControlPlane-Role**

注記

ロールの作成では、AWS アクセスまたはシークレットキーは要求されません。このワークフローのベースとして、AWS Security Token Service (STS) が使用されます。AWS STS は、一時的な制限付きの認証情報を使用して認証を行います。

これらのロールの作成の詳細は、アカウント全体の IAM ロールとポリシー参照 を参照してください。

ROSA CLI では **operator-roles** と呼ばれるクラスター固有の Operator ロールは、バックエンドストレージ、Ingress、レジストリーの管理など、クラスター操作を実行するために必要な一時的なパーミッションを取得します。これらのロールは、作成するクラスターに必要です。これらの必要な Operator ロールは次のとおりです。

- **<cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credentials**
- **<cluster_name>-<hash>-openshift-cloud-network-config-controller-credentials**
- **<cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials**
- **<cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-credentials**
- **<cluster_name>-<hash>-openshift-image-registry-installer-cloud-credentials**
- **<cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials**

これらのロールの作成の詳細は、クラスター固有の Operator IAM ロール参照 を参照してください。

3.1. OCM-ROLE IAM リソースについて

ユーザーの Red Hat 組織が Red Hat OpenShift Service on AWS (ROSA) クラスターを作成できるようにするには **ocm-role** IAM リソースを作成する必要があります。AWS へのリンクのコンテキストでは、Red Hat 組織は OpenShift Cluster Manager 内の単一のユーザーです。

以下は、**ocm-role** IAM リソースに関するいくつかの考慮事項です。

- Red Hat 組織ごとに 1 つの **ocm-role** IAM ロールのみをリンクできますが、AWS アカウントごとに任意の数の **ocm-role** IAM ロールを指定できます。Web UI では、一度にリンクできるのはこれらのロールの内 1 つだけです。
- Red Hat 組織のすべてのユーザーは、**ocm-role** IAM リソースを作成してリンクできます。
- Red Hat Organization Administrator (組織管理者) のみが **ocm-role** IAM リソースのリンクを解除できます。この制限は、他の Red Hat 組織のメンバーが他のユーザーのインターフェイス機能を妨害しないように保護するためのものです。

  注記

  既存組織の一部ではない Red Hat アカウントを作成したばかりの場合、このアカウントは Red Hat Organization Administrator でもあります。

- 基本および管理 **ocm-role** IAM リソースの AWS アクセス許可ポリシーのリストについては、このセクションの関連情報の「OpenShift Cluster Manager ロールについて」を参照してください。

ROSA CLI (**rosa**) を使用すると、IAM リソースを作成するときにリンクできます。

注記

IAM リソースを AWS アカウントに "リンクする" または "関連付ける" ことは、**ocm-role** IAM ロールと Red Hat OpenShift Cluster Manager ロールを使用して信頼ポリシーを作成することを意味します。IAM リソースを作成してリンクすると、AWS の **ocm-role** IAM リソースと **arn:aws:iam::7333:role/RH-Managed-OpenShift-Installer** リソースとの信頼関係が表示されます。

Red Hat Organization Administrator (組織管理者) **ocm-role** IAM リソースを作成してリンクした後、すべての組織メンバーが独自の **user-role** IAM ロールを作成してリンクする場合もあります。この IAM リソースは、ユーザーごとに 1 回だけ作成およびリンクする必要があります。Red Hat 組織内の別のユーザーがすでに **ocm-role** IAM リソースを作成してリンクしている場合は、独自の **user-role** IAM ロールを作成してリンクしていることを確認する必要があります。

関連情報

- OpenShift Cluster Manager ロールについて を参照してください。

3.1.1. ocm-role IAM ロールの作成

ocm-role IAM ロールは、コマンドラインインターフェイス (CLI) を使用して作成します。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager 組織で Red Hat 組織管理者特権がある。
- AWS アカウント全体のロールをインストールするために必要な権限がある。
- 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

- 基本的な権限を持つ ocm-role IAM ロールを作成するには、次のコマンドを実行します。

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

- 管理者権限を持つ ocm-role IAM ロールを作成するには、次のコマンドを実行します。

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

このコマンドを使用すると、特定の属性を指定してロールを作成できます。次の出力例は、選択された "自動モード" を示しています。これにより、ROSA CLI (**rosa**) で Operator のロールとポリシーを作成できます。詳細は、関連情報の「アカウント全体のロールの作成方法」を参照してください。

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::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes (6)
I: Created role 'ManagedOpenShift-OCM-Role-182' with ARN  'arn:aws:iam::
<ARN>:role/ManagedOpenShift-OCM-Role-182'
I: Linking OCM role
? OCM Role ARN: arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182 (7)
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with organization
'<AWS ARN>'? Yes (8)
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' with
organization account '<AWS ARN>'
```

1. 作成されたすべての AWS リソースの接頭辞値。この例では、**ManagedOpenShift** がすべての AWS リソースを付加します。
2. このロールに追加の管理者権限を付与するかどうかを選択します。

> **注記**
>
> **--admin** オプションを使用した場合、このプロンプトは表示されません。

3. パーミッション境界を設定するためのポリシーの Amazon Resource Name (ARN)。

4. ユーザー名の IAM パスを指定します。
5. AWS ロールの作成方法を選択します。**auto** を使用して、ROSA CLI はロールおよびポリシーを生成してリンクします。**auto** モードでは、AWS ロールを作成するためのいくつかの異なるプロンプトが表示されます。
6. **auto** メソッドは、接頭辞を使用して特定の **ocm-role** を作成するかどうかを尋ねます。
7. IAM ロールを OpenShift Cluster Manager に関連付けることを確認します。
8. 作成したロールを AWS 組織にリンクします。

3.2. USER-ROLE IAM ロールについて

Web UI ユーザーごとに **ユーザーロール** IAM ロールを作成して、これらのユーザーが ROSA クラスターを作成できるようにする必要があります。

user-role IAM ロールに関するいくつかの考慮事項は次のとおりです。

- Red Hat ユーザーアカウントごとに必要な **user-role** IAM ロールは 1 つだけですが、Red Hat 組織は IAM リソースの多くを持つことができます。
- Red Hat 組織のすべてのユーザーは、**user-role** IAM ロールを作成してリンクできます。
- Red Hat 組織の AWS アカウントごとに多数の **user-role** IAM ロールが存在する可能性があります。
- Red Hat は、**user-role** IAM ロールを使用してユーザーを識別します。この IAM リソースには AWS アカウントのパーミッションがありません。
- AWS アカウントは複数の **user-role** IAM ロールを指定できますが、各 IAM ロールを Red Hat 組織の各ユーザーにリンクする必要があります。ユーザーには、リンクされた **user-role** IAM ロールを複数指定できません。

注記

IAM リソースを AWS アカウントに "リンクする" または "関連付ける" ことは、**user-role** IAM ロールと Red Hat OpenShift Cluster Manager ロールを使用して信頼ポリシーを作成することを意味します。IAM リソースを作成してリンクすると、AWS の **user-role** IAM リソースと **arn:aws:iam::710019948333:role/RH-Managed-OpenShift-Installer** リソースとの信頼関係が表示されます。

3.2.1. ユーザーロール IAM ロールの作成

コマンドラインインターフェイス (CLI) を使用して、**user-role** IAM ロールを作成できます。

前提条件

- AWS アカウントがある。
- 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

- 基本的な権限を持つ **user-role** IAM ロールを作成するには、次のコマンドを実行します。

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

このコマンドを使用すると、特定の属性を指定してロールを作成できます。次の出力例は、選択された "自動モード" を示しています。これにより、ROSA CLI (**rosa**) で Operator のロールとポリシーを作成できます。詳細は、関連情報の「自動および手動のデプロイメントモードについて」を参照してください。

出力例

```
I: Creating User role
? Role prefix: ManagedOpenShift (1)
? Permissions boundary ARN (optional): (2)
? Role Path (optional): (3)
? Role creation mode: auto (4)
I: Creating ocm user role using 'arn:aws:iam::2066:user'
? Create the 'ManagedOpenShift-User.osdocs-Role' role? Yes (5)
I: Created role 'ManagedOpenShift-User.osdocs-Role' with ARN
'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role'
I: Linking User role
? User Role ARN: arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role
? Link the 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' role with account '1AGE'?
Yes (6)
I: Successfully linked role ARN 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' with
account '1AGE'
```

1. 作成されたすべての AWS リソースの接頭辞値。この例では、**ManagedOpenShift** がすべての AWS リソースを付加します。
2. パーミッション境界を設定するためのポリシーの Amazon Resource Name (ARN)。
3. ユーザー名の IAM パスを指定します。
4. AWS ロールの作成方法を選択します。**auto** を使用して、ROSA CLI はロールおよびポリシーを生成してリンクします。**auto** モードでは、AWS ロールを作成するためのいくつかの異なるプロンプトが表示されます。
5. **auto** メソッドは、接頭辞を使用して特定の **user-role** を作成するかどうかを尋ねます。
6. 作成したロールを AWS 組織にリンクします。

重要

クラスターを削除する前に **user-role** IAM ロールのリンクを解除または削除すると、エラーが発生してクラスターを削除できなくなります。削除プロセスを続行するには、このロールを作成または再リンクする必要があります。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。

3.3. AWS アカウントの関連付け

Red Hat OpenShift Service on AWS (ROSA) クラスタープロビジョニングタスクでは、Amazon リソースネーム (ARN) を使用して、IAM ロール **ocm-role** および **user-role** を AWS アカウントにリンクする必要があります。

ocm-role ARN は Red Hat 組織にラベルとして保存され、 **user-role** ARN は Red Hat ユーザーアカウント内にラベルとして保存されます。Red Hat は、これらの ARN ラベルを使用して、ユーザーが有効なアカウント所有者であり、AWS アカウントで必要なタスクを実行するための正しいアクセス許可が利用可能であることを確認します。

3.3.1. AWS アカウントのリンク

Red Hat OpenShift Service on AWS (ROSA) CLI、**rosa** を使用して、AWS アカウントを既存の IAM ロールにリンクできます。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager を使用してクラスターを作成しています。
- AWS アカウント全体のロールをインストールするために必要な権限がある。詳細は、このセクションの関連情報を参照してください。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成しましたが、まだ AWS アカウントにリンクしていません。次のコマンドを実行して、IAM ロールがすでにリンクされているかどうかを確認できます。

```
$ rosa list ocm-role
```

```
$ rosa list user-role
```

両方のロールの **Linked** 列に **Yes** が表示されている場合、ロールはすでに AWS アカウントにリンクされています。

手順

1. CLI から、Amazon Resource Name (ARN) を使用して、**ocm-role** リソースを Red Hat 組織にリンクします。

> **注記**
>
> **rosa link** コマンドを実行するには、Red Hat Organization Administrator (組織管理者権限) が必要です。**ocm-role** リソースを AWS アカウントにリンクすると、組織内のすべてのユーザーに表示されます。

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

出力例

```
I: Linking OCM role
? Link the '<AWS ACCOUNT ID>` role with organization '<ORG ID>'? Yes
I: Successfully linked role-arn '<AWS ACCOUNT ID>' with organization account '<ORG ID>'
```

2. CLI から、Amazon Resource Name (ARN) を使用して、**user-role** リソースを Red Hat ユーザーアカウントにリンクします。

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

出力例

```
I: Linking User role
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125' role with
organization '<AWS ID>'? Yes
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125'
with organization account '<AWS ID>'
```

3.3.2. 複数の AWS アカウントを Red Hat 組織に関連付ける

複数の AWS アカウントを Red Hat 組織に関連付けることができます。複数のアカウントを関連付けると、Red Hat 組織の関連付けられた AWS アカウントのいずれかに Red Hat OpenShift Service on AWS (ROSA) クラスターを作成できます。

この機能を使用すると、リージョンにバインドされた環境として複数の AWS プロファイルを使用することにより、さまざまな AWS リージョンにクラスターを作成できます。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager を使用してクラスターを作成しています。
- AWS アカウント全体のロールをインストールするために必要な権限がある。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成している。

手順

追加の AWS アカウントを関連付けるには、最初にローカル AWS 設定でプロファイルを作成します。次に、追加の AWS アカウントに **ocm-role**、user、および account のロールを作成して、アカウントを Red Hat 組織に関連付けます。

追加のリージョンでロールを作成するには、**rosa create** コマンドの実行時に **--profile <aws-profile>** パラメーターを指定し、**<aws_profile>** を追加のアカウントプロファイル名に置き換えます。

- OpenShift Cluster Manager ロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> ocm-role
```

- ユーザーロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> user-role
```

- アカウントロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> account-roles
```

注記

プロファイルを指定しない場合は、デフォルトの AWS プロファイルが使用されます。

3.4. インストーラーロールのパーミッション境界

インストーラーロールの **パーミッション境界** としてポリシーを適用できます。AWS 管理ポリシーまたはカスタマー管理ポリシーを使用して、Amazon Web Services (AWS) アイデンティティーおよびアクセス管理 (IAM) エンティティー (ユーザーまたはロール) の境界を設定できます。ポリシーと境界ポリシーの組み合わせにより、ユーザーまたはロールが最大限アクセスできるパーミッションを制限できます。インストーラーポリシー自体の変更がサポートされていないため、ROSA には、インストーラーロールの権限を制限できる 3 つの準備されたパーミッション境界ポリシーファイルのセットが含まれています。

注記

この機能は、Red Hat OpenShift Service on AWS (クラシックアーキテクチャー) クラスターでのみサポートされます。

パーミッション境界ポリシーファイルは以下のとおりです。

- **Core** 境界ポリシーファイルには、ROSA (クラシックアーキテクチャー) インストーラーが Red Hat OpenShift Service on AWS クラスターをインストールするために必要な最小限の権限が含まれています。インストーラーには、仮想プライベートクラウド (VPC) または PrivateLink (PL) を作成する権限がありません。VPC を指定する必要があります。

- **VPC** 境界ポリシーファイルには、ROSA (クラシックアーキテクチャー) インストーラーが VPC を作成/管理するために必要最小限の権限が含まれています。PL またはコアインストールのアクセス許可は含まれません。インストーラーがクラスターをインストールして VPC を作成/管理するのに十分な権限を持つクラスターをインストールする必要があり、PL を設定する必要がない場合は、インストーラーロールとともにコアファイルと VPC 境界ファイルを使用します。

- **PrivateLink (PL)** 境界ポリシーファイルには、ROSA (クラシックアーキテクチャー) インストーラーがクラスターを使用して AWS PL を作成するために必要最小限の権限が含まれています。VPC またはコアのインストールの権限は含まれません。インストール中に、すべての PL クラスターに対して事前に作成された VPC を提供します。

パーミッション境界ポリシーファイルを使用する場合は、以下の組み合わせが適用されます。

- パーミッション境界ポリシーがない場合、完全なインストーラーポリシー権限がクラスターに適用されます。

- **Core** は、インストーラーロールに対して最も限定的な権限だけを設定します。VPC および PL 権限は **Core only** の境界ポリシーに含まれません。

  - インストーラーは VPC または PL を作成または管理できません。
  - 顧客が提供する VPC が必要であり、PrivateLink (PL) は利用できません。
- **Core + VPC** は、インストーラーロールのコアおよび VPC パーミッションを設定します。
  - インストーラーは PL を作成または管理できません。
  - カスタム/BYO-VPC を使用していないことを前提としています。
  - インストーラーが VPC を作成して管理することを前提としています。
- **Core + PrivateLink (PL)**は、インストーラーが PL インフラストラクチャーをプロビジョニングできることを意味します。
  - お客様が提供する VPC が必要です。
  - これは、PL のプライベートクラスター用です。

この例の手順は、ROSA の **Core** インストーラーのパーミッション境界ポリシーのみを使用して、権限が最も制限されたインストーラーロールおよびポリシーに適用できます。これは、AWS コンソールまたは AWS CLI を使用して実行できます。この例では、AWS CLI と次のポリシーを使用します。

例3.1 sts_installer_core_permission_boundary_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
  "autoscaling:DescribeAutoScalingGroups",
  "ec2:AllocateAddress",
  "ec2:AssociateAddress",
  "ec2:AttachNetworkInterface",
  "ec2:AuthorizeSecurityGroupEgress",
  "ec2:AuthorizeSecurityGroupIngress",
  "ec2:CopyImage",
  "ec2:CreateNetworkInterface",
  "ec2:CreateSecurityGroup",
  "ec2:CreateTags",
  "ec2:CreateVolume",
  "ec2:DeleteNetworkInterface",
  "ec2:DeleteSecurityGroup",
  "ec2:DeleteSnapshot",
  "ec2:DeleteTags",
  "ec2:DeleteVolume",
  "ec2:DeregisterImage",
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeAddresses",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeDhcpOptions",
  "ec2:DescribeImages",
  "ec2:DescribeInstanceAttribute",
  "ec2:DescribeInstanceCreditSpecifications",
  "ec2:DescribeInstances",
  "ec2:DescribeInstanceStatus",
```

```
"ec2:DescribeInstanceTypeOfferings",
"ec2:DescribeInstanceTypes",
"ec2:DescribeInternetGateways",
"ec2:DescribeKeyPairs",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePrefixLists",
"ec2:DescribeRegions",
"ec2:DescribeReservedInstancesOfferings",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolumes",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcClassicLink",
"ec2:DescribeVpcClassicLinkDnsSupport",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcs",
"ec2:GetConsoleOutput",
"ec2:GetEbsDefaultKmsKeyId",
"ec2:ModifyInstanceAttribute",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ReleaseAddress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"elasticloadbalancing:AddTags",
"elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
"elasticloadbalancing:AttachLoadBalancerToSubnets",
"elasticloadbalancing:ConfigureHealthCheck",
"elasticloadbalancing:CreateListener",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing:CreateLoadBalancerListeners",
"elasticloadbalancing:CreateTargetGroup",
"elasticloadbalancing:DeleteLoadBalancer",
"elasticloadbalancing:DeleteTargetGroup",
"elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
"elasticloadbalancing:DeregisterTargets",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:ModifyLoadBalancerAttributes",
"elasticloadbalancing:ModifyTargetGroup",
"elasticloadbalancing:ModifyTargetGroupAttributes",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
```

```
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
"iam:AddRoleToInstanceProfile",
"iam:CreateInstanceProfile",
"iam:DeleteInstanceProfile",
"iam:GetInstanceProfile",
"iam:TagInstanceProfile",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:ListAttachedRolePolicies",
"iam:ListInstanceProfiles",
"iam:ListInstanceProfilesForRole",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:PassRole",
"iam:RemoveRoleFromInstanceProfile",
"iam:SimulatePrincipalPolicy",
"iam:TagRole",
"iam:UntagRole",
"route53:ChangeResourceRecordSets",
"route53:ChangeTagsForResource",
"route53:CreateHostedZone",
"route53:DeleteHostedZone",
"route53:GetAccountLimit",
"route53:GetChange",
"route53:GetHostedZone",
"route53:ListHostedZones",
"route53:ListHostedZonesByName",
"route53:ListResourceRecordSets",
"route53:ListTagsForResource",
"route53:UpdateHostedZoneComment",
"s3:CreateBucket",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:GetAccelerateConfiguration",
"s3:GetBucketAcl",
"s3:GetBucketCORS",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketPolicy",
"s3:GetBucketRequestPayment",
"s3:GetBucketTagging",
"s3:GetBucketVersioning",
"s3:GetBucketWebsite",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetObject",
"s3:GetObjectAcl",
"s3:GetObjectTagging",
"s3:GetObjectVersion",
"s3:GetReplicationConfiguration",
"s3:ListBucket",
```

```
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectTagging",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "sts:AssumeRole",
        "sts:AssumeRoleWithWebIdentity",
        "sts:GetCallerIdentity",
        "tag:GetResources",
        "tag:UntagResources",
        "kms:DescribeKey",
        "cloudwatch:GetMetricData",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:ModifyVpcEndpointServicePermissions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

重要

パーミッション境界を使用するには、パーミッション境界ポリシーを準備し、AWS IAM の関連するインストーラーロールに追加する必要があります。ROSA (**rosa**) CLI は、パーミッション境界機能を提供しますが、これはインストーラーロールだけでなくすべてのロールに適用されるため、提供されているパーミッション境界ポリシー (インストーラーロールのみ対象) では機能しません。

前提条件

- AWS アカウントがある。
- AWS のロールとポリシーの管理に必要な権限がある。
- ワークステーションに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- インストーラーロールと対応するポリシーを含む ROSA アカウント全体のロールがすでに準備されている。これらが AWS アカウントに存在しない場合は、**関連情報** の「アカウント全体の STS ロールとポリシーの作成」を参照してください。

手順

1. **rosa** CLI で次のコマンドを入力して、ポリシーファイルを準備します。

```
$ curl -o ./rosa-installer-core.json https://raw.githubusercontent.com/openshift/managed-cluster-config/master/resources/sts/4.16/sts_installer_core_permission_boundary_policy.json
```

2. 次のコマンドを入力して、AWS でポリシーを作成し、Amazon Resource Name (ARN) を収集します。

```
$ aws iam create-policy \
--policy-name rosa-core-permissions-boundary-policy \
--policy-document file://./rosa-installer-core.json \
--description "ROSA installer core permission boundary policy, the minimum permission set, allows BYO-VPC, disallows PrivateLink"
```

出力例

```
{
    "Policy": {
        "PolicyName": "rosa-core-permissions-boundary-policy",
        "PolicyId": "<Policy ID>",
        "Arn": "arn:aws:iam::<account ID>:policy/rosa-core-permissions-boundary-policy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "<CreateDate>",
        "UpdateDate": "<UpdateDate>"
    }
}
```

3. 次のコマンドを入力して、制限するインストーラーロールにアクセス許可境界ポリシーを追加します。

```
$ aws iam put-role-permissions-boundary \
--role-name ManagedOpenShift-Installer-Role \
--permissions-boundary arn:aws:iam::<account ID>:policy/rosa-core-permissions-boundary-policy
```

4. **rosa** CLI で次のコマンドを入力して、インストーラーロールを表示し、添付されたポリシー (パーミッション境界を含む) を検証します。

```
$ aws iam get-role --role-name ManagedOpenShift-Installer-Role \
--output text | grep PERMISSIONSBOUNDARY
```

出力例

```
PERMISSIONSBOUNDARY arn:aws:iam::<account ID>:policy/rosa-core-permissions-boundary-policy Policy
```

PL および VPC パーミッション境界ポリシーのその他の例については、以下を参照してください。

例3.2 sts_installer_privatelink_permission_boundary_policy.json

```
{
"Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "route53:ListHostedZonesByVPC",
        "route53:CreateVPCAssociationAuthorization",
        "route53:AssociateVPCWithHostedZone",
        "route53:DeleteVPCAssociationAuthorization",
        "route53:DisassociateVPCFromHostedZone",
        "route53:ChangeResourceRecordSets"
      ],
      "Resource": "*"
    }
  ]
}
```

例3.3 sts_installer_vpc_permission_boundary_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
      "ec2:AssociateDhcpOptions",
      "ec2:AssociateRouteTable",
      "ec2:AttachInternetGateway",
      "ec2:CreateDhcpOptions",
      "ec2:CreateInternetGateway",
      "ec2:CreateNatGateway",
      "ec2:CreateRouteTable",
      "ec2:CreateSubnet",
      "ec2:CreateVpc",
      "ec2:DeleteDhcpOptions",
      "ec2:DeleteInternetGateway",
      "ec2:DeleteNatGateway",
```

```
            "ec2:DeleteRouteTable",
            "ec2:DeleteSubnet",
            "ec2:DeleteVpc",
            "ec2:DetachInternetGateway",
            "ec2:DisassociateRouteTable",
            "ec2:ModifySubnetAttribute",
            "ec2:ModifyVpcAttribute",
            "ec2:ReplaceRouteTableAssociation"
                ],
                "Resource": "*"
            }
        ]
    }
```

3.5. 関連情報

- Permissions boundaries for IAM entities (AWS ドキュメント) を参照してください。
- アカウント全体の STS ロールとポリシーの作成 を参照してください。
- IAM ロールのトラブルシューティング を参照してください。
- クラスターの作成に必要な IAM ロールのリストについては、アカウント全体の IAM ロールとポリシー参照 を参照してください。

第4章 制限およびスケーラビリティー

このドキュメントでは、Red Hat OpenShift Service on AWS (ROSA) クラスターでテストされたクラスターの最大値について、最大値のテストに使用されたテスト環境と設定に関する情報とともに詳しく説明します。コントロールプレーンとインフラストラクチャーノードのサイズ設定とスケーリングに関する情報も提供されます。

4.1. クラスターの最大数

Red Hat OpenShift Service on AWS (ROSA) クラスターのインストールを計画するときは、以下のテスト済みオブジェクトの最大値を考慮してください。この表は、(ROSA) クラスターでテストされた各タイプの最大制限を示しています。

これらのガイドラインは、複数のアベイラビリティーゾーン設定の 180 コンピューティング（ワーカーとも呼ばれる）ノードのクラスターに基づいています。小規模なクラスターの場合、最大値はこれより低くなります。

表4.1 テスト済みのクラスターの最大値

最大値のタイプ	4.x テスト済みの最大値
Pod 数 [1]	25,000
ノードあたりの Pod 数	250
コアあたりの Pod 数	デフォルト値はありません。
namespace 数 [2]	5,000
namespace あたりの Pod 数 [3]	25,000
サービス数 [4]	10,000
namespace あたりのサービス数	5,000
サービスあたりのバックエンド数	5,000
namespace あたりのデプロイメント数 [3]	2,000

1. ここで表示される Pod 数はテスト用の Pod 数です。実際の Pod 数は、アプリケーションのメモリー、CPU、ストレージ要件により異なります。

2. 有効なプロジェクトが多数ある場合は、キースペースが過度に大きくなり、スペースのクォータを超過すると、etcd はパフォーマンスの低下による影響を受ける可能性があります。etcd ストレージを利用できるようにするには、デフラグを含む etcd の定期的なメンテナンスを行うことが強く推奨されます。

3. システムには、状態遷移への対応として、指定された namespace 内のすべてのオブジェクトに対して反復処理する必要がある制御ループがいくつかあります。単一の namespace にタイプのオブジェクトの数が多くなると、ループのコストが上昇し、状態変更を処理する速度が低下し

ます。この制限については、アプリケーションの各種要件を満たすのに十分な CPU、メモリー、およびディスクがシステムにあることが前提となっています。

4. 各サービスポートと各サービスのバックエンドには、**iptables** の対応するエントリーがあります。特定のサービスのバックエンド数は、エンドポイントのオブジェクトサイズに影響があり、その結果、システム全体に送信されるデータサイズにも影響を与えます。

4.2. OPENSHIFT CONTAINER PLATFORM テスト環境および設定

以下の表は、AWS クラウドプラットフォームについてクラスターの最大値をテストする OpenShift Container Platform 環境および設定をリスト表示しています。

ノード	タイプ	仮想 CPU	RAM(GiB)	ディスクタイプ	ディスクサイズ (GiB)/IOPS	数	リージョン
コントロールプレーン/etcd [1]	m5.4xlarge	16	64	gp3	350 / 1,000	3	us-west-2
インフラストラクチャーノード [2]	r5.2xlarge	8	64	gp3	300 / 900	3	us-west-2
ワークロード [3]	m5.2xlarge	8	32	gp3	350 / 900	3	us-west-2
Compute nodes	m5.2xlarge	8	32	gp3	350 / 900	102	us-west-2

1. io1 ディスクは、4.10 より前のすべてのバージョンでコントロールプレーン/etcd ノードに使用されます。

2. Prometheus は使用状況パターンに応じて大量のメモリーを要求できるため、インフラストラクチャーノードはモニタリングコンポーネントをホストするために使用されます。

3. ワークロードノードは、パフォーマンスとスケーラビリティーのワークロードジェネレーターを実行するための専用ノードです。

より大きなクラスターサイズとより多くのオブジェクト数に到達できる可能性があります。ただし、インフラストラクチャーノードのサイズによって、Prometheus で利用できるメモリー量が制限されます。オブジェクトの作成、変更、または削除時に、Prometheus はメトリックをそのメモリーに保存してから、ディスクでメトリックを永続化する前に 3 時間保存されます。オブジェクトの作成、変更、削除のレートが高すぎると、Prometheus はメモリーリソースがないために負荷がかかり、失敗する可能性があります。

4.3. コントロールプレーンとインフラストラクチャーノードのサイズ設定とスケーリング

Red Hat OpenShift Service on AWS (ROSA) クラスターをインストールすると、コントロールプレーンとインフラストラクチャーノードのサイズは、コンピュートノードの数によって自動的に決定されます。

インストール後にクラスター内のコンピュートノードの数を変更した場合、Red Hat Site Reliability Engineer (SRE) チームは、クラスターの安定性を維持するために、必要に応じてコントロールプレーンとインフラストラクチャーノードをスケーリングします。

4.3.1. インストール中のノードのサイズ設定

インストールプロセス中に、コントロールプレーンとインフラストラクチャーノードのサイズが動的に計算されます。サイズ計算は、クラスター内のコンピュートノードの数に基づいています。

次の表に、インストール中に適用されるコントロールプレーンとインフラストラクチャーノードのサイズを示します。

コンピュートノードの数	コントロールプレーンのサイズ	インフラストラクチャーノードのサイズ
1 から 25	m5.2xlarge	r5.xlarge
26 から 100	m5.4xlarge	r5.2xlarge
101 から 180	m5.8xlarge	r5.4xlarge

注記

ROSA のコンピュートノードの最大数は 180 です。

4.3.2. インストール後のノードのスケーリング

インストール後にコンピュートノードの数を変更した場合、コントロールプレーンとインフラストラクチャーノードは、必要に応じて Red Hat Site Reliability Engineer (SRE) チームによってスケーリングされます。ノードは、プラットフォームの安定性を維持するためにスケーリングされます。

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のインストール後のスケーリング要件は、ケースごとに評価されます。ノードリソースの消費および受信アラートの考慮が行われます。

コントロールプレーンノードのサイズ変更のアラートのルール

サイズ変更アラートは、次の状況が発生した場合に、クラスター内のコントロールプレーンノードに対してトリガーされます。

- コントロールプレーンノードは、クラシック ROSA クラスターで平均 66% 以上の使用率を維持します。

注記

ROSA のコンピュートノードの最大数は 180 です。

インフラストラクチャーノードのサイズ変更アラートのルール

CPU またはメモリーの使用率が継続して高い場合、クラスター内のインフラストラクチャーノードに対してサイズ変更アラートがトリガーされます。このように継続して使用率が高い状態が続いているのは、以下の場合です。

- インフラストラクチャーノードは、2 つのインフラストラクチャーノードを使用するアベイラビリティーゾーンが 1 つあるクラシック ROSA クラスターで、平均 50% 以上の使用率を維持します。
- インフラストラクチャーノードは、3 つのインフラストラクチャーノードを使用するアベイラビリティーゾーンが複数あるクラシック ROSA クラスターで、平均 66% 以上の使用率を維持します。

注記

ROSA のコンピュートノードの最大数は 180 です。

サイズ変更アラートは、使用率が高い状態が継続した場合にのみ表示されます。ノードが一時的にダウンして他のノードがスケールアップするなど、短期間に使用量が急増した場合には、これらのアラートはトリガーされません。

SRE チームは、ノードでのリソース消費の増加を管理するなど、追加の理由でコントロールプレーンとインフラストラクチャーノードをスケーリングする場合があります。

スケーリングが適用されると、サービスログエントリーを通じて顧客に通知されます。サービスログの詳細は、**ROSA クラスターのサービスログへのアクセス** を参照してください。

4.3.3. 大規模なクラスターのサイズに関する考慮事項

大規模なクラスターの場合、インフラストラクチャーノードのサイズ設定はスケーラビリティーに大きな影響を与える要因になる可能性があります。指定のしきい値に影響を与える要因には、etcd バージョンやストレージデータ形式などの多数の要因があります。

これらの制限を超えても、クラスターが障害が発生するとは限りません。ほとんど場合、これらの制限値を超えると、パフォーマンスが全体的に低下します。

4.4. 次のステップ

- 環境のプランニング

4.5. 関連情報

- Red Hat Hybrid Cloud Console を使用したクラスター通知の表示

第5章 環境のプランニング

5.1. テスト済みのクラスターの最大値に基づく環境計画

このドキュメントでは、テスト済みのクラスターの最大値に基づいて、AWS での Red Hat OpenShift Service 環境をプランニングする方法を説明します。

ノード上で物理リソースを過剰にサブスクライブすると、Kubernetes スケジューラーが Pod の配置時に行うリソースの保証に影響が及びます。メモリースワップを防ぐために実行できる処置について確認してください。

一部のテスト済みの最大値については、単一のディメンションが作成するオブジェクトでのみ変更されます。これらの制限はクラスター上で数多くのオブジェクトが実行されている場合には異なります。

このドキュメントに記載されている数は、Red Hat のテスト方法、セットアップ、設定、およびチューニングに基づいています。これらの数は、独自のセットアップおよび環境に応じて異なります。

環境の計画時に、以下の式を使用して、ノードに配置できる Pod の数を判別します。

```
required pods per cluster / pods per node = total number of nodes needed
```

ノードあたりの現在の Pod の最大数は 250 です。ただし、ノードに適合する Pod 数はアプリケーション自体によって異なります。**アプリケーション要件を基にした環境計画** で説明されているように、アプリケーションのメモリー、CPU、およびストレージ要件を検討してください。

シナリオ例

クラスターごとに 2200 の Pod のあるクラスターのスコープを設定する場合、ノードごとに最大 250 の Pod があることを前提として、最低でも 9 つのノードが必要になります。

```
2200 / 250 = 8.8
```

ノード数を 20 に増やす場合は、Pod 配分がノードごとに 110 の Pod に変わります。

```
2200 / 20 = 110
```

ここでは、以下のようになります。

```
required pods per cluster / total number of nodes = expected pods per node
```

5.2. アプリケーション要件に基づく環境計画

このドキュメントでは、アプリケーション要件に応じて AWS 上の Red Hat OpenShift Service 環境をプランニングする方法を説明します。

アプリケーション環境の例を考えてみましょう。

Pod タイプ	Pod 数	最大メモリー	CPU コア数	永続ストレージ
apache	100	500 MB	0.5	1 GB

Pod タイプ	Pod 数	最大メモリー	CPU コア数	永続ストレージ
node.js	200	1 GB	1	1 GB
postgresql	100	1 GB	2	10 GB
JBoss EAP	100	1 GB	1	1 GB

推定要件: CPU コア 550 個、メモリー 450 GB、および 1.4 TB ストレージ

ノードのインスタンスサイズは、希望に応じて増減を調整できます。ノードのリソースはオーバーコミットされることが多く、デプロイメントシナリオでは、小さいノードで数を増やしたり、大きいノードで数を減らしたりして、同じリソース量を提供することもできます。このデプロイメントシナリオでは、小さいノードで数を増やしたり、大きいノードで数を減らしたりして、同じリソース量を提供することもできます。運用上の敏捷性やインスタンスあたりのコストなどの要因を考慮する必要があります。

ノードのタイプ	数量	CPU	RAM (GB)
ノード (オプション 1)	100	4	16
ノード (オプション 2)	50	8	32
ノード (オプション 3)	25	16	64

アプリケーションによってはオーバーコミットの環境に適しているものもあれば、そうでないものもあります。たとえば、Java アプリケーションや Huge Page を使用するアプリケーションの多くは、オーバーコミットに対応できません。対象のメモリーは、他のアプリケーションに使用できません。上記の例では、環境は一般的な比率として約 30 % オーバーコミットされています。

アプリケーション Pod は環境変数または DNS のいずれかを使用してサービスにアクセスできます。環境変数を使用する場合、それぞれのアクティブなサービスについて、変数が Pod がノードで実行される際に kubelet によって挿入されます。クラスター対応の DNS サーバーは、Kubernetes API で新規サービスの有無を監視し、それぞれに DNS レコードのセットを作成します。DNS がクラスター全体で有効にされている場合、すべての Pod は DNS 名でサービスを自動的に解決できるはずです。DNS を使用したサービス検出は、5000 サービスを超える使用できる場合があります。サービス検出に環境変数を使用し、namespace で 5000 サービスを超える場合に引数のリストが許可される長さを超えると、Pod およびデプロイメントが失敗し始めます。

デプロイメントのサービス仕様ファイルのサービスリンクを無効にして、以下を解消します。

例

```
Kind: Template
apiVersion: template.openshift.io/v1
metadata:
  name: deploymentConfigTemplate
  creationTimestamp:
  annotations:
    description: This template will create a deploymentConfig with 1 replica, 4 env vars and a service.
    tags: ''
```

```
objects:
  - kind: DeploymentConfig
    apiVersion: apps.openshift.io/v1
    metadata:
      name: deploymentconfig${IDENTIFIER}
    spec:
      template:
        metadata:
          labels:
            name: replicationcontroller${IDENTIFIER}
        spec:
          enableServiceLinks: false
          containers:
          - name: pause${IDENTIFIER}
            image: "${IMAGE}"
            ports:
            - containerPort: 8080
              protocol: TCP
            env:
            - name: ENVVAR1_${IDENTIFIER}
              value: "${ENV_VALUE}"
            - name: ENVVAR2_${IDENTIFIER}
              value: "${ENV_VALUE}"
            - name: ENVVAR3_${IDENTIFIER}
              value: "${ENV_VALUE}"
            - name: ENVVAR4_${IDENTIFIER}
              value: "${ENV_VALUE}"
            resources: {}
            imagePullPolicy: IfNotPresent
            capabilities: {}
            securityContext:
              capabilities: {}
              privileged: false
          restartPolicy: Always
          serviceAccount: ''
      replicas: 1
      selector:
        name: replicationcontroller${IDENTIFIER}
      triggers:
      - type: ConfigChange
      strategy:
        type: Rolling
  - kind: Service
    apiVersion: v1
    metadata:
      name: service${IDENTIFIER}
    spec:
      selector:
        name: replicationcontroller${IDENTIFIER}
      ports:
      - name: serviceport${IDENTIFIER}
        protocol: TCP
        port: 80
        targetPort: 8080
      portalIP: ''
      type: ClusterIP
```

```
      sessionAffinity: None
    status:
      loadBalancer: {}
  parameters:
  - name: IDENTIFIER
    description: Number to append to the name of resources
    value: '1'
    required: true
  - name: IMAGE
    description: Image to use for deploymentConfig
    value: gcr.io/google-containers/pause-amd64:3.0
    required: false
  - name: ENV_VALUE
    description: Value to use for environment variables
    generate: expression
    from: "[A-Za-z0-9]{255}"
    required: false
  labels:
template: deploymentConfigTemplate
```

namespace で実行できるアプリケーション Pod の数は、環境変数がサービス検出に使用される場合にサービスの数およびサービス名の長さによって異なります。システムの **ARG_MAX** は、新規プロセスの引数の最大の長さを定義し、デフォルトで 2097152 バイト (2 MiB) に設定されます。kubelet は、以下を含む namespace で実行するようにスケジュールされる各 Pod に環境変数を挿入します。

- **<SERVICE_NAME>_SERVICE_HOST=<IP>**
- **<SERVICE_NAME>_SERVICE_PORT=<PORT>**
- **<SERVICE_NAME>_PORT=tcp://<IP>:<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP=tcp://<IP>:<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_PROTO=tcp**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_PORT=<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_ADDR=<ADDR>**

引数の長さが許可される値を超え、サービス名の文字数がこれに影響を及ぼす場合は、namespace の Pod が起動に失敗し始めます。

第6章 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。

6.1. 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 (クラシックアーキテクチャー) クラスターでは、クラスターの作成、可用性、およびアップグレードを提供するために、最低 100 vCPU の AWS EC2 サービスクォータが必要です。実行中のオンデマンド標準 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 increase 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6.1 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。 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)。 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)。 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6.2 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。

6.1.1. 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

6.2. 次のステップ

- 環境の設定および ROSA のインストール

第7章 STS を使用するための環境の設定

AWS の前提条件を満たしていることを確認した後に、環境を設定し、Red Hat OpenShift Service on AWS (ROSA) をインストールします。

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。

7.1. STS のための環境の設定

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、次の手順を実行して環境をセットアップします。

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、確認リンクに関するメールを確認する。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、これらのポリシーは、クラスターが必要とするロールおよびポリシーよりも制限的なものである必要はありません。

2. AWS マネジメントコンソールで 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 リージョンを設定できます。

      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
```

4. ROSA CLI の最新バージョン (**rosa**) をインストールします。

a. 使用している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ファイルの名前を変更し、ファイルを実行可能にします。このドキュメントでは、**rosa** を使用して実行可能ファイルを参照します。

```
$ chmod +x rosa
```

c. オプション: **rosa** をパスに追加します。

```
$ 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. 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. 既存のターミナルから **rosa** コマンドの補完を可能にするためのスクリプトを作成します。以下の例では、Linux マシン上で **rosa** の Bash 補完スクリプトをソースとして使用しています。

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

5. ROSA CLI 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'
```

6. AWS アカウントに ROSA クラスターをデプロイするために必要なクォータがあることを確認します。

```
$ rosa verify quota [--region=<aws_region>]
```

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 管理コンソール に移動して、失敗したサービスのクォータの増加をリクエストします。

クォータの確認に成功したら、次のステップに進みます。

7. 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. 次のコマンドを実行して、Red Hat および AWS 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、OpenShift Cluster Manager で始まる行は無視しても問題ありません。

```
$ rosa whoami
```

出力例

```
AWS Account ID:               000000000000
AWS Default Region:           us-east-1
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
```

8. ROSA (**rosa**) CLI から OpenShift CLI (**oc**) バージョン 4.7.9 以降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 openshift-client
```

   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 openshift-client
```

ロールの作成

これらの手順を完了したら、IAM および OIDC アクセスベースのロールをセットアップできます。

7.2. 次のステップ

- STS をすばやく使用して ROSA クラスターを作成 するか、カスタマイズを使用してクラスターを作成 します。

7.3. 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