# Red Hat OpenShift Service on AWS 4

## ROSA について

AWS アーキテクチャーでの Red Hat OpenShift サービスの概要

Last Updated: 2022-11-30

# Red Hat OpenShift Service on AWS 4 ROSA について

AWS アーキテクチャーでの Red Hat OpenShift サービスの概要

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

## 法律上の通知



## 概要

このドキュメントでは、Red Hat OpenShift Service on AWS (ROSA) のプラットフォームおよびアプリケーションアーキテクチャーの概要を説明します。

# 目次

# 第1章 ROSA の理解

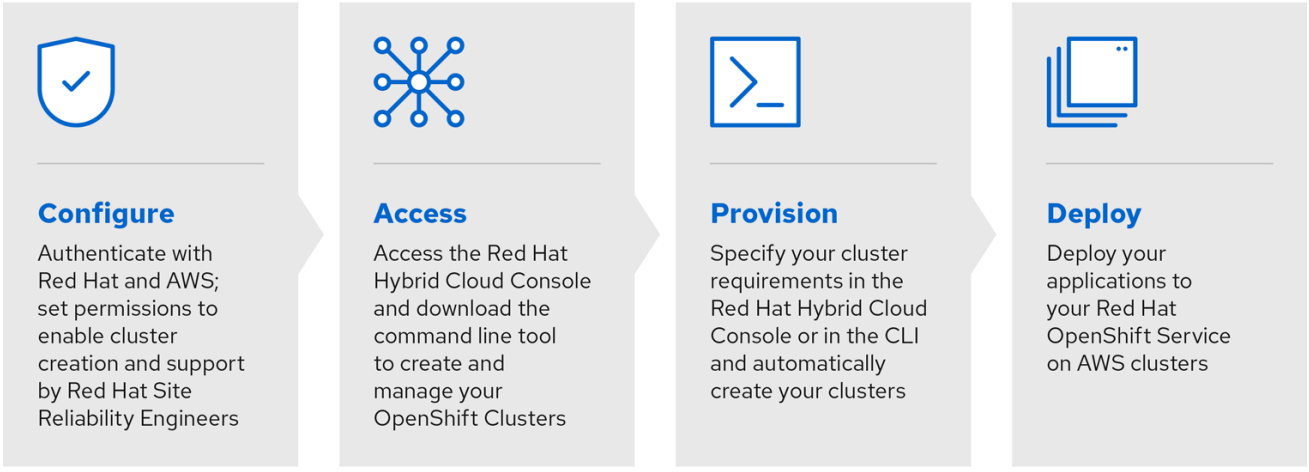
Red Hat OpenShift Service on AWS (ROSA)、Red Hat OpenShift Cluster Manager およびコマンドラインインターフェイス (CLI) ツールを使用した ROSA との対話、消費のしやすさ、および Amazon Web Services (AWS) サービスとの統合について理解します。

## 1.1. ROSA について

ROSA は、フルマネージドのターンキーアプリケーションプラットフォームであり、アプリケーションを構築してデプロイすることにより、お客様に価値を提供することに集中できます。Red Hat および AWS サイト信頼性エンジニアリング (SRE) のエキスパートが基盤となるプラットフォームを管理するため、インフラストラクチャー管理の複雑さを心配する必要はありません。ROSA は、幅広い AWS コンピュート、データベース、分析、機械学習、ネットワーク、モバイル、およびその他のサービスとのシームレスな統合を提供し、差別化されたエクスペリエンスの構築とお客様への提供をさらに加速します。

AWS アカウントから直接サービスに登録します。クラスターの作成後に、OpenShift Web コンソールまたは Red Hat OpenShift Cluster Manager でクラスターを操作できます。ROSA サービスは、OpenShift API およびコマンドラインインターフェイス (CLI) ツールも使用します。これらのツールは、標準化された OpenShift エクスペリエンスを提供し、既存のスキルおよびツールを使用できます。

OpenShift Container Platform との連携に必要な新規機能のリリースおよび共有される共通ソースを含む OpenShift の更新を受け取れます。ROSA では、バージョンの整合性を確保するために、Red Hat OpenShift Dedicated および OpenShift Container Platform と同じバージョンの OpenShift をサポートします。




## 1.2. 認証情報モード

### 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。

ROSA クラスターでサポートされている認証情報モードは 2 つあります。1 つは推奨される AWS Security Token Service (STS) を使用し、もう 1 つは Identity Access Management (IAM) ロールを使用します。

### 1.2.1. STS を使用した ROSA

AWS STS は、IAM または統合ユーザーに短期間の認証情報を提供するグローバル Web サービスです。STS を使用した ROSA は、ROSA クラスターに推奨される認証情報モードです。AWS STS と ROSA を使用して、コンポーネント固有の IAM ロールに一時的な制限付き特権の認証情報を割り当てることができます。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。

**rosa** CLI を使用して、STS を使用する ROSA クラスターに必要な IAM ロール、ポリシー、および ID リソースを作成できます。

AWS STS は、クラウドサービスのリソース管理における最小権限と安全なプラクティスの原則に準拠しています。**rosa** CLI は、固有のタスクに割り当てられた STS 認証情報を管理し、OpenShift 機能の一部として AWS リソースに対してアクションを実行します。STS を使用する際の制限の 1 つは、ROSA クラスターごとにロールを作成する必要があることです。

STS 認証情報モードは、次の理由でより安全です。

- 事前に作成した明示的で限定された一連のロールとポリシーをサポートし、要求されたすべてのパーミッションと使用されたすべてのロールを追跡します。
- サービスは、設定された権限に制限されています。
- サービスを実行すると、1 時間で有効期限が切れる認証情報を取得するため、認証情報をローテーションしたり取り消したりする必要はありません。有効期限は、有効期限が漏洩して再利用されるリスクも軽減します。

アカウント全体およびクラスターごとのロールのリストは、About IAM resources for ROSA clusters that use STS に記載されています。

### 1.2.2. STS なしの ROSA

このモードでは、アカウント内に **AdministratorAccess** を持つ事前に作成された IAM ユーザーを使用します。このユーザーは、必要に応じて他のロールとリソースを作成するための適切な権限を持っています。このアカウントを使用して、サービスはクラスターに必要なすべてのリソースを作成します。

## 1.3. 課金と課金設定

ROSA は AWS アカウントに直接請求されます。ROSA の価格設定は、消費量に応じて、年間契約や 3 年契約など、より割引率の高い契約が可能です。ROSA の総コストは、次の 2 つの要素で設定されます。

- ROSA サービス料
- AWS インフラストラクチャー料金

詳細は、AWS pricing page をご覧ください。

## 1.4. スタートガイド

クラスターのデプロイを開始するには、AWS アカウントが前提条件を満たしていること、Red Hat アカウントの準備ができていること、および Getting started with Red Hat OpenShift Service on AWS で概説されている手順に従うことを確認してください。

関連情報

- OpenShift Cluster Manager
- STS を使用する ROSA クラスターの IAM リソースについて
- Red Hat OpenShift Service on AWS の使用を開始する
- AWS pricing page

# 第2章 ROSA アーキテクチャー

## 2.1. アーキテクチャーの概念

Red Hat OpenShift Service on AWS アーキテクチャーで使用される OpenShift およびコンテナーの基本概念について説明します。

### 2.1.1. OpenShift

OpenShift は、エンタープライズワークロードを実行するための信頼できる環境を提供する Kubernetes コンテナープラットフォームです。これは、ビルトインソフトウェアで Kubernetes プラットフォームを拡張し、アプリケーションのライフサイクルの開発、操作、およびセキュリティーを強化します。OpenShift を使用すると、複数のハイブリッドクラウドプロバイダーおよび環境全体でワークロードを一貫した方法でデプロイできます。

### 2.1.2. Kubernetes

Red Hat OpenShift Service on AWS (ROSA) は、エンタープライズ Kubernetes プラットフォームである Red Hat OpenShift を使用します。Kubernetes は、コンテナー化されたワークロードおよびサービスを複数のホスト間で管理するためのオープンソースプラットフォームであり、手動の介入を最小限に抑えるか、または手動の介入なしにコンテナー化されたアプリケーションをのデプロイ、自動化、監視、スケーリングを行う管理ツールを提供します。Kubernetes の詳細は、Kubernetes ドキュメント を参照してください。

**クラスター、コンピュートノード、およびコンピュートノード**

Kubernetes クラスターは、コントロールプレーンおよび 1 つまたは複数のコンピュートノードで設定されます。コンピュートノードは、CPU、メモリー、オペレーティングシステム、割り当てられたディスクその他のプロパティーのタイプまたはプロファイルごとにコンピュートプールで整理されます。コンピュートノードは Kubernetes **Node** リソースに対応し、クラスター内のすべての Kubernetes リソースを制御し、監視する Kubernetes コントロールプレーンによって管理されます。
コンテナー化されたアプリケーションのリソースをデプロイする場合、Kubernetes コントロールプレーンは、デプロイメント要件およびクラスターで利用可能な容量を考慮して、これらのリソースをデプロイするコンピュートノードを判別します。Kubernetes リソースには、サービス、デプロイメント、および Pod が含まれます。

**namespace**

Kubernetes namespace は、クラスターを複数のチームと共有する場合などに、アプリケーションをデプロイし、アクセスを制限できる複数の領域にクラスターリソースを分割する方法です。たとえば、設定されるシステムリソースは、**kube-system** などの別の namespace に保持されます。
Kubernetes リソースの作成時に namespace を指定しない場合、リソースは **default** namespace に自動的に作成されます。

**Pod**

クラスターにデプロイされるコンテナー化アプリケーションはすべて、Pod と呼ばれる Kubernetes リソースによってデプロイされ、実行され、管理されます。Pod は、Kubernetes クラスターの小規模なデプロイ可能な単位を表し、単一の単位として処理する必要のあるコンテナーをグループ化するために使用されます。ほとんどの場合、各コンテナーは独自の Pod にデプロイされます。ただし、アプリケーションではコンテナーおよび他のヘルパーコンテナーを 1 つの Pod にデプロイして、それらのコンテナーを同じプライベート IP アドレスを使用して処理できるようにする必要がある場合があります。

**アプリケーション**

アプリケーションは、アプリケーションの完全なアプリケーションまたはアプリケーションのコンポーネントを指すことがあります。アプリケーションのコンポーネントを別の Pod にデプロイすることも、別のコンピュートノードにデプロイできます。

**サービス**

サービスは、Pod のセットをグループ化し、各 Pod の実際のプライベート IP アドレスを公開せずにこれらの Pod へのネットワーク接続を提供する Kubernetes リソースです。サービスを使用して、クラスター内またはパブリックインターネットでアプリケーションを利用できるようにすることができます。

**デプロイメント**

デプロイメントは、サービス、永続ストレージまたはアノテーションなどのアプリケーションの実行に必要な他のリソースまたは機能についての情報を指定できる Kubernetes リソースです。設定 YAML ファイルでデプロイメントを設定してから、これをクラスターに適用します。Kubernetes メインリソースを設定し、利用可能な容量を持つコンピュートノードの Pod にコンテナーをデプロイします。
ローリング更新時に追加する Pod の数や、同時に利用できない Pod 数などの、アプリケーションの更新ストラテジーを定義します。ローリング更新の実行時に、デプロイメントは更新が機能しているかどうかを確認し、障害の検出時にロールアウトを停止します。

デプロイメントは、Pod を管理するのに使用できるワークロードコントローラーの 1 つのタイプです。

### 2.1.3. コンテナー

コンテナーは、アプリケーションコード、設定、および依存関係を単一のユニットにパッケージ化する標準的な方法を提供します。コンテナーは、コンピュートホストで分離されたプロセスとして実行され、ホストオペレーティングシステムとそのハードウェアリソースを共有します。コンテナーは環境をまたがって移動でき、変更せずに実行できます。仮想マシンとは異なり、コンテナーはデバイス、そのオペレーティングシステム、および基礎となるハードウェアの仮想化を行いません。アプリケーションコード、ランタイム、システムツール、ライブラリーおよび設定のみがコンテナー内でパッケージ化されます。この方法により、コンテナーは仮想マシンと比較してより軽量で移植可能となり、より効率的になります。

OCI 準拠のコンテナーイメージは、既存の Linux コンテナーテクノロジー (LXC) 上にビルドされ、ソフトウェアをアプリケーションの実行に必要なすべての要素を含む標準化された単位にパッケージ化する方法についてのテンプレートを定義します。Red Hat OpenShift Service on AWS (ROSA) は CRI-O をコンテナーランタイムとして使用し、コンテナーをクラスターにデプロイします。

ROSA の Kubernetes でアプリケーションを実行するには、最初にコンテナーレジストリーに保存するコンテナーイメージを作成してアプリケーションをコンテナー化する必要があります。

**イメージ**

コンテナーイメージは、実行するすべてのコンテナーのベースです。コンテナーイメージは、イメージをビルドする方法を定義し、アプリケーション、アプリケーション設定、およびその依存関係などの追加するアーティファクトをビルドするテキストファイルの Dockerfile です。イメージは常に他のイメージからビルドされるため、迅速に設定できます。

**レジストリー**

イメージレジストリーは、コンテナーイメージを保存し、取得し、共有する場所です。レジストリーに保存されているイメージには、公開されている (パブリックレジストリー) か、小規模なユーザーのグループ (プライベートレジストリー) がアクセスできます。ROSA は、最初のコンテナー化されたアプリケーションを作成する際に使用できるパブリックイメージを提供します。エンタープライズアプリケーションの場合は、プライベートレジストリーを使用して、権限のないユーザーがイメージを使用できないようにすることができます。

## 2.2. アーキテクチャーモデル

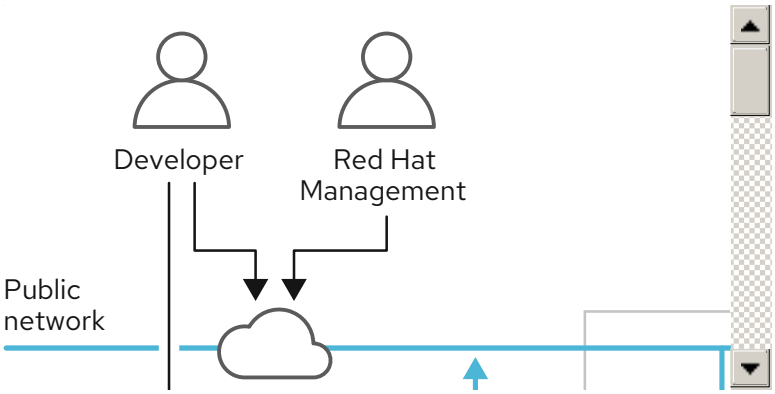
ROSA アーキテクチャーは、以下のネットワーク設定タイプをサポートします。

- パブリックネットワーク
- プライベートネットワーク
- AWS PrivateLink

### 2.2.1. パブリックおよびプライベートネットワークの ROSA アーキテクチャー

ROSA は、パブリックネットワークまたはプライベートネットワークのいずれかを使用してインストールできます。クラスター作成のプロセス中または作成後にプライベートクラスターおよびプライベートネットワーク接続を設定します。Red Hat は、パブリックネットワークを介したアクセスが限定されたクラスターを管理します。詳細は、サービス定義を参照してください。

**図2.1 パブリックおよびプライベートネットワークにデプロイされる ROSA**




または、プライベートサブネットでのみホストされる AWS PrivateLink を使用してクラスターをインストールします。

### 2.2.2. AWS PrivateLink アーキテクチャー

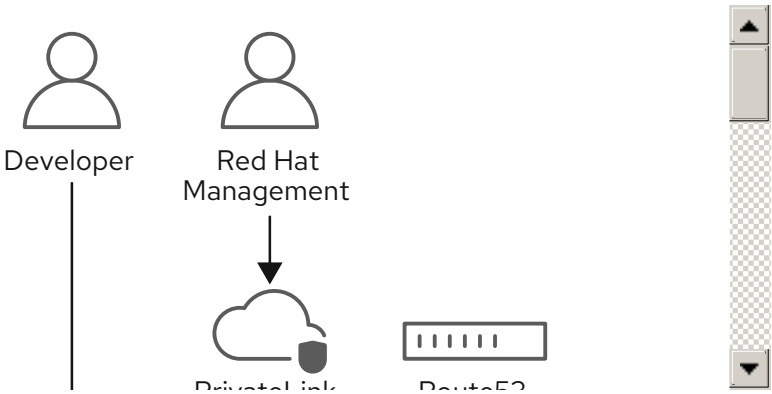
AWS PrivateLink クラスターを作成する Red Hat 管理対象インフラストラクチャーは、プライベートサブネットでホストされています。Red Hat とお客様によって提供されるインフラストラクチャー間の接続は、AWS PrivateLink VPC エンドポイント経由で作成されます。

**注記**

AWS PrivateLink は既存の VPC でのみサポートされます。

次の図は、PrivateLink クラスターのネットワーク接続を示しています。

図2.2 プライベートサブネットにデプロイされたマルチ AZ AWS PrivateLink クラスター




### 2.2.2.1. AWS リファレンスアーキテクチャー

AWS は、AWS PrivateLink を使用する設定の設定方法を計画する際に、お客様に役立つリファレンスアーキテクチャーを複数提供します。以下に 3 つの例を示します。

- プライベートサブネットおよび AWS Site-to-Site VPN アクセスを持つ VPC
  この設定により、ネットワークをインターネットに公開することなく、ネットワークをクラウドに拡張できます。

  Internet Protocol Security (IPsec) VPN トンネルを介してネットワークとの通信を有効にするために、この設定には、単一のプライベートサブネットと仮想プライベートゲートウェイを持つ仮想プライベートクラウド (VPC) が含まれます。インターネットを介した通信は、インターネットゲートウェイを使用しません。

  詳細は、AWS ドキュメントの VPC with a private subnet only and AWS Site-to-Site VPN access を参照してください。

- パブリックおよびプライベートサブネット (NAT) を持つ VPC
  この設定により、ネットワークを分離して、インターネットからパブリックサブネットに到達できるようにし、かつプライベートサブネットには到達できないようにすることができます。

  パブリックサブネットのみが送信トラフィックをインターネットに直接送信できます。プライベートサブネットは、パブリックサブネットにあるネットワークアドレス変換 (NAT) ゲートウェイを使用してインターネットにアクセスできます。これにより、データベースサーバーが NAT ゲートウェイを使用してソフトウェアの更新用にインターネットに接続できますが、インターネットからデータベースサーバーへ直接接続することはできません。

  詳細は、AWS ドキュメントの VPC with public and private subnets (NAT) を参照してください。

- パブリックサブネットとプライベートサブネット、および AWS Site-to-Site VPN アクセスを持つ VPC
  この設定により、ネットワークをクラウドに拡張し、VPC からインターネットに直接アクセスすることができます。

  スケーラブルな Web フロントエンドを備えた多層アプリケーションをパブリックサブネットで実行し、IPsec AWS Site-to-Site VPN 接続によってネットワークに接続されているプライベートサブネットにデータを格納することができます。

  詳細は、AWS ドキュメントの VPC with public and private subnets and AWS Site-to-Site VPN access を参照してください。

# 第3章 ポリシーおよびサービス定義

## 3.1. RED HAT OPENSHIFT SERVICE ON AWS のサポート

可用性と障害を回避することは、どのアプリケーションプラットフォームでも非常に重要な要素です。Red Hat OpenShift Service on AWS (ROSA) は複数のレベルで障害に対する保護を提供しますが、お客様がデプロイするアプリケーションは高可用性を確保するために適切に設定される必要があります。クラウドプロバイダーで発生する可能性のある停止状態に対応するために、複数のアベイラビリティーゾーンにクラスターをデプロイしたり、フェイルオーバーメカニズムで複数のクラスターを維持したりするなどの追加のオプションを選択できます。

### 3.1.1. 潜在的な障害点

Red Hat OpenShift Service on AWS (ROSA) は、ダウンタイムに対してワークロードを保護するために多くの機能およびオプションを提供しますが、アプリケーションはこれらの機能を利用できるように適切に設計される必要があります。

ROSA は、Red Hat サイト信頼性エンジニアリング (SRE) サポートと、複数のアベイラビリティーゾーンクラスターをデプロイするオプションを追加することで、Kubernetes の数多くの一般的な問題からの保護を強化しますが、コンテナーまたはインフラストラクチャーが依然として失敗する多くの可能性があります。潜在的な障害点を把握することで、リスクを想定し、アプリケーションとクラスターの両方が特定のレベルで必要に応じて回復性を持つように設計できます。

**注記**

停止状態は、インフラストラクチャーおよびクラスターコンポーネントの複数の異なるレベルで生じる可能性があります。

#### 3.1.1.1. コンテナーまたは Pod の障害

設計上、Pod は短期間存在することが意図されています。アプリケーション Pod の複数のインスタンスが実行されている場合は、個別の Pod またはコンテナーの問題から保護できるようにサービスを適切にスケーリングします。OpenShift ノードスケジューラーは、回復性をさらに強化するために、これらのワークロードが異なるワーカーノードに分散するようにします。

Pod の障害に対応する場合は、ストレージがアプリケーションに割り当てられる方法も理解することが重要になります。単一 Pod に割り当てられる単一の永続ボリュームは、Pod のスケーリングを完全に活用できませんが、複製されるデータベース、データベースサービス、または共有ストレージはこれを活用できます。

アップグレードなどの計画メンテナーンス中にアプリケーションが中断されるのを防ぐには、Pod の Disruption Budget (停止状態の予算) を定義することが重要です。これらは Kubernetes API の一部であり、他のオブジェクトタイプと同様に **oc** コマンドで管理できます。この設定により、メンテナーンスのためのノードのドレイン (解放) などの操作時に Pod への安全面の各種の制約を指定できます。

#### 3.1.1.2. ワーカーノードの障害

ワーカーノードは、アプリケーション Pod が含まれる仮想マシンです。デフォルトで、ROSA クラスターには単一アベイラビリティーゾーンのクラスター用のワーカーノードが 2 つ以上含まれます。ワーカーノードに障害が発生した場合、Pod は、既存ノードに関する問題が解決するか、またはノードが置き換えられるまで、十分な容量がある限り、機能しているワーカーノードに移行します。ワーカーノードを追加することは、単一ノードの停止状態に対する保護策を強化することを意味し、ノードに障害が発生した場合に再スケジュールされる Pod の適切なクラスター容量を確保できます。

**注記**

ノードの障害に対応する場合、ストレージへの影響を把握することも重要になります。EFS ボリュームはノードの障害による影響を受けません。ただし、EBS ボリュームは、障害が発生するノードに接続されている場合はアクセスできません。

#### 3.1.1.3. クラスターの障害

ROSA クラスターには、選択したクラスターのタイプに応じて、単一ゾーンまたは複数のゾーンのいずれかで、高可用性を確保するために事前設定された 3 つ以上のコントロールプレーンノードと 3 つ以上のインフラストラクチャーノードがあります。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はワーカーノードと同じ耐障害性があり、この場合 Red Hat によって完全に管理される利点を活用できます。

コントロールプレーンが完全に停止する場合、OpenShift API は機能せず、既存のワーカーノード Pod は影響を受けません。ただし、Pod またはノードが同時に停止している場合は、コントロールプレーンのリカバリーが新規 Pod またはノードを追加される前、またはスケジュールする前に必要になります。

インフラストラクチャーノードで実行されるすべてのサービスは、高可用性を持ち、インフラストラクチャーノード間に分散されるように Red Hat によって設定されます。インフラストラクチャーが完全に停止すると、これらのサービスはこれらのノードが回復するまで利用できなくなります。

#### 3.1.1.4. ゾーンの障害

AWS のゾーン障害は、すべての仮想コンポーネント (ワーカーノード、ブロックまたは共有ストレージ、単一のアベイラビリティーゾーンに固有のロードバランサーなど) に影響を及ぼします。ゾーンの障害から保護するために、ROSA は複数のアベイラビリティーゾーンクラスターとして知られる 3 つのアベイラビリティーゾーンに分散するクラスターに関するオプションを提供します。既存のステートレスワークロードは、十分な容量がある限り、停止時に影響を受けないゾーンに再分散されます。

#### 3.1.1.5. ストレージの障害

ステートフルなアプリケーションをデプロイしている場合、ストレージは重要なコンポーネントであり、高可用性を検討する際に考慮に入れる必要があります。単一ブロックストレージ PV は、Pod レベルでも停止状態になった状態では実行できません。ストレージの可用性を維持する最適な方法として、複製されたストレージソリューション、停止による影響を受けない共有ストレージ、またはクラスターから独立したデータベースサービスを使用できます。

## 3.2. 責任分担マトリクス

以下では、Red Hat OpenShift Service on AWS (ROSA) マネージドサービスにおける Red Hat、クラウドプロバイダー、およびお客様のそれぞれの責任を説明します。

### 3.2.1. Red Hat OpenShift Service on AWS におけるロールの概要

Red Hat および Amazon Web Services (AWS) は Red Hat OpenShift Service on AWS サービスを管理し、お客様は特定のロールを共有します。Red Hat OpenShift Service on AWS サービスは、リモートでアクセスされ、パブリッククラウドリソースでホストされ、お客様が所有する AWS アカウントで作成され、Red Hat が所有する基礎となるプラットフォームおよびデータセキュリティーを持ちます。

**重要**

**cluster-admin** ロールがユーザーに追加される場合は、Red Hat Enterprise Agreement Appendix 4 (Online Subscription Services) の責任および除外事項について参照してください。

| リソース | インシデントおよびオペレーション管理 | 変更管理 | アイデンティティーおよびアクセス管理 | セキュリティーおよび規制コンプライアンス | 障害復旧 |
|---|---|---|---|---|---|
| お客様データ | お客様 | お客様 | お客様 | お客様 | お客様 |
| お客様のアプリケーション | お客様 | お客様 | お客様 | お客様 | お客様 |
| 開発者サービス | お客様 | お客様 | お客様 | お客様 | お客様 |
| プラットフォームモニタリング | Red Hat | Red Hat | Red Hat | Red Hat | Red Hat |
| ロギング | Red Hat | 共有 | 共有 | 共有 | Red Hat |
| アプリケーションのネットワーク | 共有 | 共有 | 共有 | Red Hat | Red Hat |
| クラスターネットワーク | Red Hat | 共有 | 共有 | Red Hat | Red Hat |
| 仮想ネットワーク | 共有 | 共有 | 共有 | 共有 | 共有 |

| リソース | インシデントおよびオペレーション管理 | 変更管理 | アイデンティティーおよびアクセス管理 | セキュリティーおよび規制コンプライアンス | 障害復旧 |
|---|---|---|---|---|---|
| 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 | Red Hat | Red Hat | Red Hat | Red Hat | Red Hat |
| ワーカーノード | Red Hat | Red Hat | Red Hat | Red Hat | Red Hat |
| クラスターのバージョン | Red Hat | 共有 | Red Hat | Red Hat | Red Hat |
| 容量の管理 | Red Hat | 共有 | Red Hat | Red Hat | Red Hat |
| 仮想ストレージ | Red Hat およびクラウドプロバイダー | Red Hat およびクラウドプロバイダー | Red Hat およびクラウドプロバイダー | Red Hat およびクラウドプロバイダー | Red Hat およびクラウドプロバイダー |
| 物理インフラストラクチャーおよびセキュリティー | クラウドプロバイダー | クラウドプロバイダー | クラウドプロバイダー | クラウドプロバイダー | クラウドプロバイダー |

### 3.2.2. 共有される責任のマトリクス

お客様、Red Hat、および Amazon Web Services (AWS) は、Red Hat OpenShift Service on AWS クラスターのモニターリングおよびメンテナーンスに関する責任を共有します。以下では、エリアおよびタスク別の責任について図示しています。

#### 3.2.2.1. インシデントおよびオペレーション管理

お客様は、お客様のアプリケーションデータ、およびお客様がクラスターネットワークまたは仮想ネットワークに設定した可能性のあるカスタムネットワークに関するインシデントおよびオペレーション管理を行います。

| リソース | Red Hat および AWS の責任 | お客様の責任 |
| --- | --- | --- |
| アプリケーションのネットワーク | クラウドロードバランサーおよびネイティブ OpenShift ルーターサービスを監視し、アラートに応答します。 | • サービ出力ドバランサーのエンドポイントの正常性を監視します。<br>• アプリケーションルート、およびその背後のエンドポイントの正常性を監視します。<br>• Red Hat に停電を報告します。 |
| 仮想ネットワーク | クラウドロードバランサー、サブネット、およびデフォルトのプラットフォームネットワークに必要なパブリッククラウドコンポーネントを監視し、アラートに応答します。 | 潜在的な問題やセキュリティーの脅威について、VPC から VPC 接続、VPN 接続、または直接接続を介して任意で設定されているネットワークトラフィックを監視します。 |

#### 3.2.2.2. 変更管理

Red Hat は、お客様が制御するクラスターインフラストラクチャーおよびサービスへの変更を有効にし、コントロールプレーンノード、インフラストラクチャーノードおよびサービス、ならびにワーカーノードのバージョンを維持します。お客様は、インフラストラクチャーの変更要求を開始し、クラスターでの任意のサービスおよびネットワーク設定のインストールおよび維持、およびお客様データおよびお客様のアプリケーションに対するすべての変更を行います。

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| ロギング | • プラットフォーム監査ログを一元的に集計し、監視します。<br>• ロギング Operator を提供し、これを維持して、お客様がデフォルトのアプリケーションロギングのロギングスタックをデプロイできるようにします。<br>• お客様のリクエストに対応して監査ログを提供します。 | • オプションのデフォルトアプリケーションロギング Operator をクラスターにインストールします。<br>• ロギングサイドカーコンテナーやサードパーティーロギングアプリケーションなどのオプションのアプリケーションロギングソリューションをインストール、設定し、維持します。<br>• ロギングスタックまたはクラスターの安定性に影響がある場合に、お客様のアプリケーションによって生成されるアプリケーションログのサイズおよび頻度を調整します。<br>• 特定のインシデントを調査するためにサポートケースを使用してプラットフォーム監査ログを要求します。 |

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| アプリケーションのネットワーク | • パブリッククラウドロードバランサーを設定します。プライベートロードバランサーを設定し、必要に応じて追加のロードバランサーを 1 つまで設定する機能を提供します。<br>• ネイティブ OpenShift ルーターサービスを設定します。ルーターをプライベートとして設定し、1 つのルーターシャードを追加する機能を提供します。<br>• デフォルトの内部 Pod トラフィック用に OpenShift SDN コンポーネントをインストールし、設定し、維持します。<br>• お客様が **NetworkPolicy** および **EgressNetworkPolicy** (ファイアウォール) オブジェクトを管理できる機能を提供します。 | • **NetworkPolicy** オブジェクトを使用して、プロジェクトおよび Pod ネットワーク、Pod ingress、および Pod egress のデフォルト以外の Pod ネットワークのパーミッションを設定します。<br>• OpenShift Cluster Manager を使用して、デフォルトのアプリケーションルートのプライベートロードバランサーを要求します。<br>• OpenShift Cluster Manager を使用して、追加の 1 つのパブリックまたはプライベートルーターシャードおよび対応するロードバランサーを設定します。<br>• 特定サービスの追加のサービス出力ドバランサーを要求し、設定します。<br>• 必要な DNS 転送ルールを設定します。 |
| クラスターネットワーク | • パブリックまたはプライベートサービスのエンドポイントや仮想ネットワークコンポーネントとの必要な統合などのクラスター管理コンポーネントを設定します。<br>• ワーカー、インフラストラクチャー、およびコントロールプレーンノード間の内部クラスター通信に必要な内部ネットワークコンポーネントを設定します。 | • クラスターのプロビジョニング時に OpenShift Cluster Manager で必要な場合は、マシン CIDR、サービス CIDR、および Pod CIDR の任意のデフォルト以外の IP アドレス範囲を指定します。<br>• クラスターの作成時または OpenShift Cluster Manager でクラスターの作成後に、API サービスエンドポイントをパブリックまたはプライベートにするように要求します。 |

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| 仮想ネットワーク | ● クラスターのプロビジョニングに必要な仮想ネットワークコンポーネント (仮想プライベートクラウド、サブネット、ロードバランサー、インターネットゲートウェイ、NAT ゲートウェイなど) をセットアップし、設定します。<br>● お客様が OpenShift Cluster Manager で必要に応じて、オンプレミスリソース、VPC 間の接続、および直接接続を管理できる機能を提供します。<br>● サービス出力ドバランサーと共に使用できるように、お客様がパブリッククラウドロードバランサーを作成およびデプロイできるようにします。 | ● VPC 間の接続、VPN 接続、直接接続などの任意のパブリッククラウドネットワークコンポーネントを設定し、維持します。<br>● 特定サービスの追加のサービス出力ドバランサーを要求し、設定します。 |
| クラスターのバージョン | ● アップグレードのスケジューリングプロセスを有効にします。<br>● アップグレードの進捗を監視し、発生した問題をすべて修正します。<br>● マイナーアップグレードおよびメンテナーンスアップグレードに関する変更ログおよびリリースノートを公開します。 | ● メンテナンスバージョンのアップグレードを即時、後日、または自動で行うようにスケジュールします。<br>● マイナーバージョンのアップグレードを確認し、スケジュールします。<br>● クラスターのバージョンがサポート範囲のマイナーバージョンであることを確認します。<br>● 互換性を確保するために、マイナーバージョンおよびメンテナーンスバージョンでお客様のアプリケーションをテストします。 |

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| 容量の管理 | • コントロールプレーンの使用を監視します。コントロールプレーンには、コントロールプレーンノードとインフラストラクチャーノードが含まれます。<br>• QoS (Quality of Service) を維持するために、コントロールプレーンノードをスケーリングし、サイズ変更します。 | • ワーカーノードの使用率を監視し、必要に応じて自動スケーリング機能を有効にします。<br>• クラスターのスケーリングストラテジーを決定します。マシンプールの詳細は、関連情報を参照してください。<br>• 提供される OpenShift Cluster Manager コントロールを使用して、必要に応じて追加のワーカーノードを追加または削除します。<br>• クラスターリソース要件に関する Red Hat の通知に対応します。 |

#### 3.2.2.3. アイデンティティーおよびアクセス管理

Identity and Access Management マトリックスには、クラスター、アプリケーション、およびインフラストラクチャーリソースへの承認されたアクセスを管理する責任が含まれます。これには、アクセス制御メカニズム、認証、および認可を提供し、リソースへのアクセスを管理するタスクが含まれます。

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| ロギング | • プラットフォーム監査ログについて、業界標準に基づく段階的な内部アクセスプロセスを順守します。<br>• ネイティブな OpenShift RBAC 機能を提供します。 | • プロジェクトへのアクセス、およびプロジェクトのアプリケーションログへのアクセスを制御するように OpenShift RBAC を設定します。<br>• サードパーティーまたはカスタムのアプリケーションロギングソリューションについては、お客様がアクセス管理を行います。 |

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| アプリケーションのネットワーク | ネイティブ OpenShift RBAC および **dedicated-admin** 機能を提供します。 | • OpenShift **dedicated-admin** および RBAC を、必要に応じてルート設定へのアクセスを制御するように設定します。<br>• Red Hat が OpenShift Cluster Manager へのアクセス権限を付与する組織管理者を管理します。クラスターマネージャーは、ルーターのオプションを設定し、サービ出力ドバランサーのクォータを提供するために使用されます。 |
| クラスターネットワーク | • OpenShift Cluster Manager を使用してお客様のアクセス制御を提供します。<br>• ネイティブ OpenShift RBAC および **dedicated-admin** 機能を提供します。 | • Red Hat アカウントの Red Hat 組織のメンバーシップを管理します。<br>• Red Hat が OpenShift Cluster Manager へのアクセス権限を付与する組織管理者を管理します。<br>• OpenShift **dedicated-admin** および RBAC を、必要に応じてルート設定へのアクセスを制御するように設定します。 |
| 仮想ネットワーク | OpenShift Cluster Manager を使用してお客様のアクセス制御を提供します。 | OpenShift Cluster Manager を使用してパブリッククラウドコンポーネントへの任意のユーザーアクセスを管理します。 |

#### 3.2.2.4. セキュリティーおよび規制コンプライアンス

以下は、コンプライアンスに関連する責任および管理について示しています。

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| ロギング | セキュリティーイベントについて分析するために、クラスターの監査ログを Red Hat SIEM に送信します。フォレンジック分析をサポートするために、定義された期間の監査ログを保持します。 | セキュリティーイベントのアプリケーションログを分析します。デフォルトのロギングスタックで指定されるよりも長い保持期間が必要な場合に、ロギングサイドカーコンテナーまたはサードパーティーのロギングアプリケーション経由でアプリケーションログを外部エンドポイントに送信します。 |
| 仮想ネットワーク | • 潜在的な問題やセキュリティーの脅威について、仮想ネットワークのコンポーネントを監視します。<br>• 追加のパブリッククラウドプロバイダーツールを活用して、追加の監視と保護を行います。 | • 潜在的な問題やセキュリティーの脅威について、オプションで設定される仮想ネットワークのコンポーネントを監視します。<br>• 必要に応じて、必要なファイアウォールルールまたはデータセンターの保護を設定します。 |

#### 3.2.2.5. 障害復旧

障害復旧には、データおよび設定のバックアップ、障害復旧環境へのデータおよび設定の複製、および障害イベント発生時のフェイルオーバーが含まれます。

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| 仮想ネットワーク | プラットフォームが機能するために必要な、影響を受けた仮想ネットワークコンポーネントを復元するか、再作成します。 | • パブリッククラウドプロバイダーが推奨されるように、障害に対する保護のために、可能な場合は複数のトンネルで仮想ネットワーク接続を設定します。<br>• 複数のクラスターでグローバルロードバランサーを使用する場合は、フェイルオーバー DNS および負荷分散を維持します。 |

#### 3.2.2.6. 関連情報

- マシンプールについて

### 3.2.3. データおよびアプリケーションに関するお客様の責任

お客様は、Red Hat OpenShift Service on AWS にデプロイするアプリケーション、ワークロード、およびデータに責任を負います。ただし、Red Hat は、お客様がプラットフォームでデータおよびアプリケーションを管理するのに役立つ各種ツールを提供します。

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| お客様データ | • データ暗号化のプラットフォームレベルの標準を維持します。<br>• シークレットなどのアプリケーションデータの管理に役立つ OpenShift コンポーネントを提供します。<br>• サードパーティーのデータサービス AWS RDS との統合を有効にし、クラスターおよびクラウドプロバイダー外のデータを保存し、管理します。 | プラットフォームに保存されるすべてのお客様データについて、またお客様のアプリケーションがこのデータを消費して公開する方法について責任を持ちます。 |

| リソース | Red Hat の責任 | お客様の責任 |
| --- | --- | --- |
| お客様のアプリケーション | ● お客様が OpenShift および Kubernetes API にアクセスし、コンテナー化されたアプリケーションをデプロイし、管理できるように、OpenShift コンポーネントと共にクラスターをプロビジョニングします。<br>● イメージプルシークレットでクラスターを作成し、お客様のデプロイメントで Red Hat Container Catalog レジストリーからイメージをプルできるようにします。<br>● お客様が Operator を設定してコミュニティー、サードパーティー、および Red Hat サービスをクラスターに追加するために使用できる OpenShift API へのアクセスを提供します。<br>● ストレージクラスとプラグインを提供し、お客様のアプリケーションで使用できるように永続ボリュームをサポートします。<br>● お客様がクラスター上にアプリケーションコンテナーイメージを安全に保存し、アプリケーションをデプロイおよび管理できるようにコンテナーイメージレジストリーを提供します。 | ● お客様およびサードパーティーのアプリケーション、データ、およびそれらの完全なライフサイクルに関する責任を持ちます。<br>● Operator または外部イメージを使用して Red Hat、コミュニティー、サードパーティー、独自のサービス、またはその他のサービスをクラスターに追加する際、お客様はこれらのサービスについて、単独、および Red Hat を含む適切なプロバイダーと連携して問題をトラブルシューティングする責任を負います。<br>● 提供されるツールおよび機能を使用して設定およびデプロイを行い、最新の状態を保ち、リソースの要求および制限を設定し、アプリケーションを実行するのに十分なリソースを持つようにクラスターのサイズを設定し、パーミッションを設定し、他のサービスと統合し、お客様がデプロイするイメージストリームまたはテンプレートを管理し、外部に提供し、保存し、バックアップし、データを復元し、さらに可用性と回復性が高いワークロードを管理します。<br>● メトリクスを収集し、アラートを作成するためにソフトウェアをインストールし、操作することを含め、Red Hat OpenShift Service on AWS で実行されるアプリケーションのモニターリングについての責任を持ちます。 |

## 3.3. RED HAT OPENSHIFT SERVICE ON AWS のサービス定義

本書では、Red Hat OpenShift Service on AWS (ROSA) マネージドサービスのサービス定義を説明します。

### 3.3.1. アカウント管理

このセクションでは、Red Hat OpenShift Service on AWS アカウント管理のサービス定義を説明します。

#### 3.3.1.1. 請求

Red Hat OpenShift Service on AWS についての請求は、サービス (ロードバランサー、ストレージ、EC2 インスタンス、他のコンポーネントなど)、および OpenShift サービスの Red Hat サブスクリプションで使用される AWS コンポーネントの使用状況に基づいて Amazon Web Services (AWS) で行われます。

追加の Red Hat ソフトウェアは別途購入する必要があります。

#### 3.3.1.2. クラスターのセルフサービス

お客様はクラスターをセルフサービスで利用できます。これには以下が含まれますが、これらに限定されません。

- クラスターの作成
- クラスターの削除
- アイデンティティープロバイダーの追加または削除
- 権限が昇格したグループからのユーザーの追加または削除
- クラスターのプライバシーの設定
- マシンプールの追加または削除、および自動スケーリングの設定
- アップグレードポリシーの定義

これらのタスクは、**rosa** CLI ユーティリティーを使用してセルフサービスで利用できます。

#### 3.3.1.3. インスタンスタイプ

単一アベイラビリティーゾーンのクラスターでは、少なくとも 3 つのコントロールプレーン、2 つのインフラストラクチャーノード、および 2 つのワーカーノードが単一のアベイラビリティーゾーンにデプロイされている必要があります。

複数のアベイラビリティーゾーンのクラスターでは、少なくとも 3 つのコントロールプレーン、3 つのインフラストラクチャーノード、および 3 つのワーカーノードが必要です。追加のノードを購入する場合は、ノードの適切な配分を維持できるように、3 の倍数単位で購入する必要があります。

すべての Red Hat OpenShift Service on AWS クラスターは、最大 180 ワーカーノードをサポートします。

**注記**

**Default** マシンプールのノードタイプは、クラスターの作成後に変更できません。

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は Red Hat によりデプロイされ、管理されます。クラウドプロバイダーコンソールを使用して基礎となるインフラストラクチャーをシャットダウンすることはサポートされておらず、データが失われる可能性があります。etcd および API 関連のワークロードを処理する 3 つ以上のコントロールプレーンノードが使用されます。メトリクス、ルーティング、Web コンソール、および他のワークロードを処理するインフラストラクチャーノードが少な

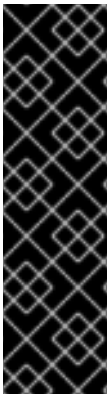
くとも 2 つあります。コントロールノードとインフラストラクチャーノードでワークロードを実行しないでください。実行する予定のワークロードはすべて、ワーカーノードにデプロイする必要があります。ワーカーノードにデプロイする必要がある Red Hat ワークロードの詳細については、以下の Red Hat Operator サポートセクションを参照してください。

**注記**

約 1 vCPU コアおよび 1 GiB のメモリーが各ワーカーノードで予約され、割り当て可能なリソースから削除されます。このリソースの予約は、基礎となるプラットフォームに必要なプロセスを実行するのに必要です。これらのプロセスには、udev、kubelet、コンテナーランタイムなどのシステムデーモンが含まれます。予約されるリソースは、カーネル予約も占めます。

監査ログの集計、メトリクスコレクション、DNS、イメージレジストリー、SDN などの OpenShift Container Platform コアシステムは、追加の割り当て可能なリソースを使用し、クラスターの安定性および保守性を確保できる可能性があります。消費される追加リソースは、使用方法によって異なる場合があります。

詳細は、Kubernetes のドキュメント を参照してください。



**重要**

Red Hat OpenShift Service on AWS バージョン 4.8.35、4.9.26、4.10.6 の時点で、Red Hat OpenShift Service on AWS におけるデフォルトの Pod ごとの PID 制限は **4096** です。この PID 制限を有効にする場合は、Red Hat OpenShift Service on AWS クラスターをこれらのバージョン以降にアップグレードする必要があります。以前のバージョンの Red Hat OpenShift Service on AWS クラスターでは、デフォルトの PID 制限である **1024** が使用されます。

Red Hat OpenShift Service on AWS クラスターで Pod ごとの PID 制限を設定することはできません。

**関連情報**

- Red Hat Operator のサポート

### 3.3.1.4. AWS インスタンスタイプ

Red Hat OpenShift Service on AWS は、次のワーカーノードインスタンスのタイプとサイズを提供します。

**例3.1 一般的用途**

- m5.metal (96† vCPU, 384 GiB)
- m5.xlarge (4 vCPU, 16 GiB)
- m5.2xlarge (8 vCPU, 32 GiB)
- m5.4xlarge (16 vCPU, 64 GiB)
- m5.8xlarge (32 vCPU, 128 GiB)
- m5.12xlarge (48 vCPU, 192 GiB)

- m5.16xlarge (64 vCPU, 256 GiB)
- m5.24xlarge (96 vCPU, 384 GiB)
- m5a.xlarge (4 vCPU, 16 GiB)
- m5a.2xlarge (8 vCPU, 32 GiB)
- m5a.4xlarge (16 vCPU, 64 GiB)
- m5a.8xlarge (32 vCPU, 128 GiB)
- m5a.12xlarge (48 vCPU, 192 GiB)
- m5a.16xlarge (64 vCPU, 256 GiB)
- m5a.24xlarge (96 vCPU, 384 GiB)
- m5ad.xlarge (4 vCPU, 16 GiB)
- m5ad.2xlarge (8 vCPU, 32 GiB)
- m5ad.4xlarge (16 vCPU, 64 GiB)
- m5ad.8xlarge (32 vCPU, 128 GiB)
- m5ad.12xlarge (48 vCPU, 192 GiB)
- m5ad.16xlarge (64 vCPU, 256 GiB)
- m5ad.24xlarge (96 vCPU, 384 GiB)
- m5d.metal (96† vCPU, 384 GiB)
- m5d.xlarge (4 vCPU、16 GiB)
- m5d.2xlarge (8 vCPU、32 GiB)
- m5d.4xlarge (16 vCPU、64 GiB)
- m5d.8xlarge (32 vCPU, 128 GiB)
- m5d.12xlarge (48 vCPU, 192 GiB)
- m5d.16xlarge (64 vCPU、256 GiB)
- m5d.24xlarge (96 vCPU、384 GiB)
- m5n.metal (96 vCPU, 384 GiB)
- m5n.xlarge (4 vCPU、16 GiB)
- m5n.2xlarge (8 vCPU、32 GiB)
- m5n.4xlarge (16 vCPU、64 GiB)
- m5n.8xlarge (32 vCPU、128 GiB)

- m5n.12xlarge (48 vCPU、192 GiB)
- m5n.16xlarge (64 vCPU、256 GiB)
- m5n.24xlarge (96 vCPU、384 GiB)
- m5dn.metal (96 vCPU、384 GiB)
- m5dn.xlarge (4 vCPU、16 GiB)
- m5dn.2xlarge (8 vCPU、32 GiB)
- m5dn.4xlarge (16 vCPU、64 GiB)
- m5dn.8xlarge (32 vCPU、128 GiB)
- m5dn.12xlarge (48 vCPU、192 GiB)
- m5dn.16xlarge (64 vCPU、256 GiB)
- m5dn.24xlarge (96 vCPU、384 GiB)
- m5zn.metal (48 vCPU、192 GiB)
- m5zn.xlarge (4 vCPU、16 GiB)
- m5zn.2xlarge (8 vCPU、32 GiB)
- m5zn.3xlarge (12 vCPU、48 GiB)
- m5zn.6xlarge (24 vCPU、96 GiB)
- m5zn.12xlarge (48 vCPU、192 GiB)
- m6i.metal (128 vCPU、512 GiB)
- m6i.xlarge (4 vCPU、16 GiB)
- m6i.2xlarge (8 vCPU、32 GiB)
- m6i.4xlarge (16 vCPU、64 GiB)
- m6i.8xlarge (32 vCPU、128 GiB)
- m6i.12xlarge (48 vCPU、192 GiB)
- m6i.16xlarge (64 vCPU、256 GiB)
- m6i.24xlarge (96 vCPU、384 GiB)
- m6i.32xlarge (128 vCPU、512 GiB)

† これらのインスタンスタイプは、48 個の物理コアで 96 個の論理プロセッサーを提供します。これらは、2 つの物理 Intel ソケットを備えた単一サーバー上で実行されます。

**例3.2 バースト可能な汎用目的**

- t3.xlarge (4 vCPU、16 GiB)
- t3.2xlarge (8 vCPU、32 GiB)
- t3a.xlarge (4 vCPU、16 GiB)
- t3a.2xlarge (8 vCPU、32 GiB)

**例3.3 メモリー集約型**

- x1.16xlarge (64 vCPU, 976 GiB)
- x1.32xlarge (128 vCPU, 1952 GiB)
- x1e.xlarge (4 vCPU, 122 GiB)
- x1e.2xlarge (8 vCPU, 244 GiB)
- x1e.4xlarge (16 vCPU, 488 GiB)
- x1e.8xlarge (32 vCPU, 976 GiB)
- x1e.16xlarge (64 vCPU, 1,952 GiB)
- x1e.32xlarge (128 vCPU, 3,904 GiB)
- x2idn.16xlarge (64 vCPU, 1024 GiB)
- x2idn.24xlarge (96 vCPU, 1536 GiB)
- x2idn.32xlarge (128 vCPU, 2048 GiB)
- x2iedn.xlarge (4 vCPU, 128 GiB)
- x2iedn.2xlarge (8 vCPU, 256 GiB)
- x2iedn.4xlarge (16 vCPU, 512 GiB)
- x2iedn.8xlarge (32 vCPU, 1024 GiB)
- x2iedn.16xlarge (64 vCPU, 2048 GiB)
- x2iedn.24xlarge (96 vCPU, 3072 GiB)
- x2iedn.32xlarge (128 vCPU, 4096 GiB)
- x2iezn.2xlarge (8 vCPU, 256 GiB)
- x2iezn.4xlarge (16vCPU, 512 GiB)
- x2iezn.6xlarge (24vCPU, 768 GiB)
- x2iezn.8xlarge (32vCPU, 1,024 GiB)
- x2iezn.12xlarge (48vCPU, 1,536 GiB)
- x2idn.metal (128vCPU, 2,048 GiB)

- x2iedn.metal (128vCPU, 4,096 GiB)
- x2iezn.metal (48 vCPU、1,536 GiB)

**例3.4 メモリー最適化**

- r4.xlarge (4 vCPU、30.5 GiB)
- r4.2xlarge (8 vCPU、61 GiB)
- r4.4xlarge (16 vCPU、122 GiB)
- r4.8xlarge (32 vCPU、244 GiB)
- r4.16xlarge (64 vCPU、488 GiB)
- r5.metal (96† vCPU, 768 GiB)
- r5.xlarge (4 vCPU, 32 GiB)
- r5.2xlarge (8 vCPU, 64 GiB)
- r5.4xlarge (16 vCPU, 128 GiB)
- r5.8xlarge (32 vCPU, 256 GiB)
- r5.12xlarge (48 vCPU, 384 GiB)
- r5.16xlarge (64 vCPU, 512 GiB)
- r5.24xlarge (96 vCPU, 768 GiB)
- r5a.xlarge (4 vCPU、32 GiB)
- r5a.2xlarge (8 vCPU、64 GiB)
- r5a.4xlarge (16 vCPU、128 GiB)
- r5a.8xlarge (32 vCPU、256 GiB)
- r5a.12xlarge (48 vCPU、384 GiB)
- r5a.16xlarge (64 vCPU、512 GiB)
- r5a.24xlarge (96 vCPU、768 GiB)
- r5ad.xlarge (4 vCPU、32 GiB)
- r5ad.2xlarge (8 vCPU、64 GiB)
- r5ad.4xlarge (16 vCPU、128 GiB)
- r5ad.8xlarge (32 vCPU、256 GiB)
- r5ad.12xlarge(48 vCPU、384 GiB)
- r5ad.16xlarge (64 vCPU、512 GiB)

- r5ad.24xlarge (96 vCPU、768 GiB)
- r5d.metal (96† vCPU, 768 GiB)
- r5d.xlarge (4 vCPU、32 GiB)
- r5d.2xlarge (8 vCPU、64 GiB)
- r5d.4xlarge (16 vCPU、128 GiB)
- r5d.8xlarge (32 vCPU、256 GiB)
- r5d.12xlarge (48 vCPU、384 GiB)
- r5d.16xlarge (64 vCPU、512 GiB)
- r5d.24xlarge (96 vCPU、768 GiB)
- r5n.metal (96 vCPU, 768 GiB)
- r5n.xlarge (4 vCPU、32 GiB)
- r5n.2xlarge (8 vCPU、64 GiB)
- r5n.4xlarge (16 vCPU、128 GiB)
- r5n.8xlarge (32 vCPU、256 GiB)
- r5n.12xlarge (48 vCPU、384 GiB)
- r5n.16xlarge (64 vCPU、512 GiB)
- r5n.24xlarge (96 vCPU、768 GiB)
- r5dn.metal (96 vCPU、768 GiB)
- r5dn.xlarge (4 vCPU、32 GiB)
- r5dn.2xlarge (8 vCPU、64 GiB)
- r5dn.4xlarge (16 vCPU、128 GiB)
- r5dn.8xlarge (32 vCPU、256 GiB)
- r5dn.12xlarge(48 vCPU, 384 GiB)
- r5dn.16xlarge (64 vCPU、512 GiB)
- r5dn.24xlarge (96 vCPU、768 GiB)
- r6i.metal (128 vCPU、1,024 GiB)
- r6i.xlarge (4 vCPU, 32 GiB)
- r6i.2xlarge (8 vCPU, 64 GiB)
- r6i.4xlarge (16 vCPU, 128 GiB)

- r6i.8xlarge (32 vCPU, 256 GiB)
- r6i.12xlarge (48 vCPU, 384 GiB)
- r6i.16xlarge (64 vCPU, 512 GiB)
- r6i.24xlarge (96 vCPU, 768 GiB)
- r6i.32xlarge (128 vCPU, 1,024 GiB)
- z1d.metal (48 vCPU, 384 GiB)
- z1d.xlarge (4 vCPU, 32 GiB)
- z1d.2xlarge (8 vCPU、64 GiB)
- z1d.3xlarge (12 vCPU、96 GiB)
- z1d.6xlarge (24 vCPU, 192 GiB)
- z1d.12xlarge (48 vCPU、384 GiB)

† これらのインスタンスタイプは、48 個の物理コアで 96 個の論理プロセッサーを提供します。これらは、2 つの物理 Intel ソケットを備えた単一サーバー上で実行されます。

これらのインスタンスタイプは、24 個の物理コアで 48 個の論理プロセッサーを提供します。

**例3.5 コンピュート最適化**

- c5.metal (96 vCPU、192 GiB)
- c5.xlarge (4 vCPU, 8 GiB)
- c5.2xlarge (8 vCPU、16 GiB)
- c5.4xlarge (16 vCPU、32 GiB)
- c5.9xlarge (36 vCPU、72 GiB)
- c5.12xlarge (48 vCPU、96 GiB)
- c5.18xlarge (72 vCPU、144 GiB)
- c5.24xlarge (96 vCPU、192 GiB)
- c5d.metal (96 vCPU、192 GiB)
- c5d.xlarge (4 vCPU、8 GiB)
- c5d.2xlarge (8 vCPU、16 GiB)
- c5d.4xlarge (16 vCPU、32 GiB)
- c5d.9xlarge (36 vCPU、72 GiB)
- c5d.12xlarge (48 vCPU、96 GiB)

- c5d.18xlarge(72 vCPU, 144 GiB)
- c5d.24xlarge (96 vCPU、192 GiB)
- c5a.xlarge (4 vCPU、8 GiB)
- c5a.2xlarge (8 vCPU、16 GiB)
- c5a.4xlarge (16 vCPU、32 GiB)
- c5a.8xlarge (32 vCPU、64 GiB)
- c5a.12xlarge (48 vCPU、96 GiB)
- c5a.16xlarge (64 vCPU、128 GiB)
- c5a.24xlarge (96 vCPU、192 GiB)
- c5ad.xlarge (4 vCPU、8 GiB)
- c5ad.2xlarge (8 vCPU、16 GiB)
- c5ad.4xlarge (16 vCPU、32 GiB)
- c5ad.8xlarge (32 vCPU、64 GiB)
- c5ad.12xlarge (48 vCPU、96 GiB)
- c5ad.16xlarge (64 vCPU、128 GiB)
- c5ad.24xlarge (96 vCPU、192 GiB)
- c5n.metal (72 vCPU、192 GiB)
- c5n.xlarge (4 vCPU、10.5 GiB)
- c5n.2xlarge (8 vCPU、21 GiB)
- c5n.4xlarge (16 vCPU、42 GiB)
- c5n.9xlarge (36 vCPU、96 GiB)
- c5n.18xlarge (72 vCPU、192 GiB)
- c6i.metal (128 vCPU、256 GiB)
- c6i.xlarge (4 vCPU、8 GiB)
- c6i.2xlarge (8 vCPU、16 GiB)
- c6i.4xlarge (16 vCPU、32 GiB)
- c6i.8xlarge (32 vCPU、64 GiB)
- c6i.12xlarge (48 vCPU、96 GiB)
- c6i.16xlarge (64 vCPU、128 GiB)

- c6i.24xlarge (96 vCPU、192 GiB)
- c6i.32xlarge (128 vCPU、256 GiB)

**例3.6 ストレージの最適化**

- i3.metal (72† vCPU, 512 GiB)
- i3.xlarge (4 vCPU, 30.5 GiB)
- i3.2xlarge (8 vCPU, 61 GiB)
- i3.4xlarge (16 vCPU, 122 GiB)
- i3.8xlarge (32 vCPU, 244 GiB)
- i3.16xlarge (64 vCPU, 488 GiB)
- i3en.metal (96 vCPU、768 GiB)
- i3en.xlarge (4 vCPU, 32 GiB)
- i3en.2xlarge (8 vCPU, 64 GiB)
- i3en.3xlarge (12 vCPU, 96 GiB)
- i3en.6xlarge (24 vCPU, 192 GiB)
- i3en.12xlarge (48 vCPU, 384 GiB)
- i3en.24xlarge (96 vCPU, 768 GiB)

† このインスタンスタイプは、36 個の物理コアで 72 個の論理プロセッサーを提供します。

**注記**

仮想インスタンスタイプは、.metal インスタンスタイプよりも速く初期化されます。

**関連情報**

- AWS インスタンスタイプ

### 3.3.1.5. リージョンおよびアベイラビリティーゾーン

以下の AWS リージョンは Red Hat OpenShift 4 でサポートされ、Red Hat OpenShift Service on AWS についてサポートされます。注: OpenShift 4 のサポートの有無にかかわらず、中国および GovCloud (US) リージョンはサポートされません。

- af-south-1 (Cape Town, AWS オプトインが必要)
- ap-east-1 (Hong Kong, AWS オプトインが必要)
- ap-northeast-1 (Tokyo)

- ap-northeast-2 (Seoul)
- ap-northeast-3 (Osaka)
- ap-south-1 (Mumbai)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ap-southeast-3 (Jakarta, AWS オプトインが必要)
- ca-central-1 (Central Canada)
- eu-central-1 (Frankfurt)
- eu-north-1 (Stockholm)
- eu-south-1 (Milan, AWS オプトインが必要)
- eu-west-1 (Ireland)
- eu-west-2 (London)
- eu-west-3 (Paris)
- me-south-1 (Bahrain, AWS オプトインが必要)
- sa-east-1 (São Paulo)
- us-east-1 (N. Virginia)
- us-east-2 (Ohio)
- us-west-1 (N. California)
- us-west-2 (Oregon)

複数のアベイラビリティーゾーンのクラスターは、少なくとも 3 つのアベイラビリティーゾーンのあるリージョンにのみデプロイできます。詳細は、AWS ドキュメントの Regions and Availability Zones セクションを参照してください。

新規 Red Hat OpenShift Service on AWS クラスターはそれぞれ、インストーラーで作成された Virtual Private Cloud (VPC)、または既存の Virtual Private Cloud (VPC) 内にインストールされます。オプションとして、単一アベイラビリティーゾーン (Single-AZ) または複数アベイラビリティーゾーン (Multi-AZ) にデプロイすることができます。これにより、クラスターレベルのネットワークおよびリソースの分離が行われ、VPN 接続や VPC ピアリングなどのクラウドプロバイダーの VPC 設定が有効になります。永続ボリューム (PV) は AWS Elastic Block Storage (EBS) によってサポートされ、それらがプロビジョニングされるアベイラビリティーゾーンに固有のものとして機能します。永続ボリューム要求 (PVC) は、Pod がスケジュールできなくなる状況を防ぐために、関連付けられた Pod リソースが特定のアベイラビリティーゾーンに割り当てられるまでボリュームにバインドされません。アベイラビリティーゾーン固有のリソースは、同一のアベイラビリティーゾーン内のリソースでのみ利用できます。

**警告**

リージョンおよびアベイラビリティーゾーンの単一または複数かの選択は、クラスターのデプロイ後に変更できません。

#### 3.3.1.6. サービスレベルアグリーメント (SLA)

サービス自体の SLA は、Red Hat Enterprise Agreement Appendix 4 (Online Subscription Services) で定義されています。

#### 3.3.1.7. 限定的なサポートのステータス

クラスターが **限定サポート** ステータスに移行すると、Red Hat はクラスターをプロアクティブに監視しなくなり、SLA は適用されなくなり、SLA に対して要求されたクレジットは拒否されます。製品サポートがなくなったという意味ではありません。場合によっては、違反要因を修正すると、クラスターが完全にサポートされた状態に戻ることがあります。ただし、それ以外の場合は、クラスターを削除して再作成する必要があります。

クラスターは、次のシナリオなど、さまざまな理由で限定サポートステータスに移行する場合があります。

**サポート終了日までにクラスターをサポートされるバージョンにアップグレードしない場合**

Red Hat は、サポート終了日以降のバージョンについて、ランタイムまたは SLA を保証しません。継続的なサポートを受けるには、サポートが終了する前に、クラスターを、サポートされているバージョンにアップグレードしてください。有効期限が切れる前にクラスターをアップグレードしない場合、クラスターは、サポートされているバージョンにアップグレードされるまで、限定サポートステータスに移行します。

Red Hat は、サポートされていないバージョンからサポートされているバージョンにアップグレードするための商業的に合理的なサポートを提供します。ただし、サポートされるアップグレードパスが利用できなくなった場合は、新規クラスターを作成し、ワークロードを移行することが必要になることがあります。

**ネイティブの Red Hat OpenShift Service on AWS コンポーネント、または Red Hat がインストールおよび管理するその他のコンポーネントを削除または置き換える場合**

クラスター管理者パーミッションを使用した場合、Red Hat は、インフラストラクチャーサービス、サービスの可用性、またはデータ損失に影響を与えるアクションを含む、ユーザーまたは認可されたユーザーのアクションに対して責任を負いません。Red Hat がそのようなアクションを検出した場合、クラスターは限定サポートステータスに移行する可能性があります。Red Hat はステータスの変更を通知します。アクションを元に戻すか、サポートケースを作成して、クラスターの削除と再作成が必要になる可能性のある修復手順を検討する必要があります。

クラスターが限定サポートステータスに移行する可能性のある特定のアクションについて質問がある場合、またはさらに支援が必要な場合は、サポートチケットを作成します。

#### 3.3.1.8. サポート

Red Hat OpenShift Service on AWS には Red Hat Premium サポートが含まれており、このサポートは Red Hat カスタマーポータル を使用して利用できます。

サポートの応答時間については、Red Hat OpenShift Service on AWS の SLA を参照してください。

AWS サポートは、AWS との既存のサポート契約に基づきます。

### 3.3.2. ロギング

Red Hat OpenShift Service on AWS は、Amazon (AWS) CloudWatch へのオプションの統合ログ転送を提供します。

#### 3.3.2.1. クラスター監査ロギング

クラスター監査ログは、インテグレーションが有効になっている場合に AWS CloudWatch 経由で利用できます。インテグレーションが有効でない場合は、サポートケースを作成して監査ログをリクエストできます。

#### 3.3.2.2. アプリケーションロギング

**STDOUT** に送信されるアプリケーションログは Fluentd によって収集され、クラスターロギングスタックで AWS CloudWatch に転送されます (インストールされている場合)。

### 3.3.3. モニターリング

このセクションでは、Red Hat OpenShift Service on AWS モニターリングのサービス定義を説明します。

#### 3.3.3.1. クラスターメトリクス

Red Hat OpenShift Service on AWS クラスターには、CPU、メモリー、ネットワークベースのメトリクスを含むクラスターモニターリングの統合された Prometheus スタックが同梱されます。これは Web コンソールからアクセスできます。また、これらのメトリクスは Red Hat OpenShift Service on AWS ユーザーによって提供される CPU またはメモリーメトリクスをベースとする Horizontal Pod Autoscaling を許可します。

#### 3.3.3.2. クラスターステータスの通知

Red Hat は、OpenShift Cluster Manager で利用可能なクラスターダッシュボードと、クラスターの初回デプロイで使用した連絡先、およびお客様が指定する追加の連絡先のメールアドレスに送信されるメール通知を使用して、Red Hat OpenShift Service on AWS クラスターの正常性およびステータスについて通信します。

### 3.3.4. ネットワーク

このセクションでは、Red Hat OpenShift Service on AWS ネットワークのサービス定義を説明します。

#### 3.3.4.1. アプリケーションのカスタムドメイン

ルートにカスタムホスト名を使用するには、正規名 (CNAME) レコードを作成して DNS プロバイダーを更新する必要があります。CNAME レコードでは、OpenShift の正規ルーターのホスト名をカスタムドメインにマップする必要があります。OpenShift の正規ルーターのホスト名は、ルートの作成後に **Route Details** ページに表示されます。または、ワイルドカード CNAME レコードを 1 度作成して、指定のホスト名のすべてのサブドメインをクラスターのルーターにルーティングできます。

#### 3.3.4.2. ドメイン検証証明書

Red Hat OpenShift Service on AWS には、クラスターの内部サービスと外部サービスの両方に必要な

TLS セキュリティー証明書が含まれます。外部ルートの場合は、各クラスターに提供され、インストールされる 2 つの別個の TLS ワイルドカード証明書があります。1 つは Web コンソールおよびルートのデフォルトホスト名用であり、もう 1 つは API エンドポイント用です。Let's Encrypt は証明書に使用される認証局です。内部の API エンドポイント などのクラスター内のルートでは、クラスターの組み込み認証局によって署名された TLS 証明書を使用し、TLS 証明書を信頼するためにすべての Pod で CA バンドルが利用可能である必要があります。

#### 3.3.4.3. ビルドのカスタム認証局

Red Hat OpenShift Service on AWS は、イメージレジストリーからイメージをプルする際にビルドによって信頼されるカスタム認証局の使用をサポートします。

#### 3.3.4.4. ロードバランサー

Red Hat OpenShift Service on AWS は、最大 5 つの異なるロードバランサーを使用します。

- クラスターの内部にあり、内部のクラスター通信のトラフィックのバランスを取るために使用される内部コントロールプレーンのロードバランサー。
- OpenShift および Kubernetes API へのアクセスに使用される外部コントロールプレーンのロードバランサー。このロードバランサーは OpenShift Cluster Manager で無効にできます。このロードバランサーが無効にされている場合、Red Hat は API DNS を内部コントロールプレーンのロードバランサーを参照するように再設定します。
- Red Hat によるクラスター管理用に予約される Red Hat の外部コントロールプレーンのロードバランサー。アクセスは厳密に制御され、ホワイトリストに登録されている bastion ホストからのみ通信が可能です。
- デフォルトのアプリケーションロードバランサーであるデフォルトの外部ルーター/ingress ロードバランサー (URL の **apps** で示される)。デフォルトのロードバランサーを OpenShift Cluster Manager で設定して、インターネット上で一般にアクセス可能にしたり、既存のプライベート接続でプライベートにのみアクセス可能にしたりできます。ロギング UI、メトリクス API、レジストリーなどのクラスターサービスを含む、クラスターのすべてのアプリケーションルートは、このデフォルトのルーターロードバランサーで公開されます。
- オプション: セカンダリーアプリケーションロードバランサーであるセカンダリールーター/ingress ロードバランサー (URL の **apps2** で示される)。セカンダリーロードバランサーを OpenShift Cluster Manager で設定して、インターネット上で一般にアクセス可能にしたり、既存のプライベート接続でプライベートにのみアクセス可能にしたりできます。**Label match** がこのルーターロードバランサーに設定されている場合は、このラベルに一致するアプリケーションルートのみがこのルーターロードバランサーで公開されます。それ以外の場合は、すべてのアプリケーションルートがこのルーターロードバランサーで公開されます。
- オプション: サービスのロードバランサー。サービスの非 HTTP/SNI トラフィックおよび非標準ポートを有効にします。これらのロードバランサーを Red Hat OpenShift Service on AWS で実行されているサービスにマップし、HTTP/SNI 以外のトラフィックや標準以外のポートの使用などの高度な ingress 機能を有効にできます。各 AWS アカウントには、各クラスター内で使用できる Classic Load Balancer の数を制限 するクォータがあります。

#### 3.3.4.5. クラスター ingress

プロジェクト管理者は、IP 許可リストによる ingress の制御など、さまざまな目的でルートアノテーションを追加できます。

Ingress ポリシーは、**ovs-networkpolicy** プラグインを使用する **NetworkPolicy** オブジェクトを使用して変更することもできます。これにより、同じクラスターの Pod 間や、同じ namespace にある Pod 間など、Ingress ネットワークポリシーを Pod レベルで完全に制御できます。

すべてのクラスター ingress トラフィックは定義されたロードバランサーを通過します。すべてのノードへの直接のアクセスは、クラウド設定によりブロックされます。

#### 3.3.4.6. クラスター egress

**EgressNetworkPolicy** オブジェクトでの Pod egress トラフィックの制御は、Red Hat OpenShift Service on AWS での送信トラフィックを防ぐか、またはこれを制限するために使用できます。

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からの公開される送信トラフィックは、クラスターイメージのセキュリティーおよびクラスターのモニターリングを維持するために必要です。これには、**0.0.0.0/0** ルートがインターネットゲートウェイにのみ属している必要があります。プライベート接続でこの範囲のルートをルーティングすることはできません。

OpenShift 4 クラスターは NAT ゲートウェイを使用して、クラスターからの公開される送信トラフィックのパブリック静的 IP を表示します。クラスターがデプロイされるそれぞれのアベイラビリティーゾーンは個別の NAT ゲートウェイを受信するため、最大 3 つの固有の静的 IP アドレスがクラスターの egress トラフィックについて存在する可能性があります。クラスター内に留まるトラフィックや、パブリックインターネットに送信されないトラフィックは NAT ゲートウェイを通過せず、トラフィックの送信元となるノードに属するソース IP アドレスを持ちます。ノード IP アドレスは動的であるため、お客様はプライベートリソースへのアクセス時に個々の IP アドレスをホワイトリストに入れることはできません。

お客様はクラスター上で Pod を実行し、外部サービスをクエリーすることで、パブリック静的 IP アドレスを判別できます。以下に例を示します。

```
$ oc run ip-lookup --image=busybox -i -t --restart=Never --rm -- /bin/sh -c "/bin/nslookup -type=a
myip.opendns.com resolver1.opendns.com | grep -E 'Address: [0-9.]+'"
```

#### 3.3.4.7. クラウドネットワーク設定

Red Hat OpenShift Service on AWS では、AWS で管理されるテクノロジーを使用したプライベートネットワーク接続の設定を可能にします。

- VPN 接続
- VPC ピアリング
- Transit Gateway
- Direct Connect

**重要**

Red Hat のサイト信頼性エンジニアリング (SRE) チームは、プライベートネットワーク接続を監視しません。これらの接続の監視は、お客様の責任で行われます。

#### 3.3.4.8. DNS 転送

プライベートクラウドネットワーク設定を持つ Red Hat OpenShift Service on AWS クラスターの場合、お客様はそのプライベート接続で利用可能な内部 DNS サーバーを指定でき、明示的に提供されるドメインについてこれをクエリーする必要があります。

### 3.3.5. ストレージ

このセクションでは、Red Hat OpenShift Service on AWS ストレージのサービス定義を説明します。

#### 3.3.5.1. 保存時に暗号化される (Encrypted-at-rest) OS およびノードストレージ

コントロールプレーンノードは、保存時に暗号化される (encrypted-at-rest) AWS Elastic Block Store (EBS) ストレージを使用します。

#### 3.3.5.2. 保存時に暗号化される (encrypted-at-rest) PV

PV に使用される EBS ボリュームはデフォルトで保存時に暗号化されます。

#### 3.3.5.3. ブロックストレージ (RWO)

永続ボリューム (PV) は Read-Write-Once で、AWS EBS によってサポートされます。

PV は一度に 1 つのノードにのみ割り当てられ、それらがプロビジョニングされるアベイラビリティーゾーンに固有のものです。ただし、PV はそのアベイラビリティーゾーンの任意のノードに割り当てることができます。

各クラウドプロバイダーには、1 つのノードに割り当てることのできる PV の数について独自の制限があります。詳細は、AWS インスタンスタイプの制限 を参照してください。

#### 3.3.5.4. 共有ストレージ (RWX)

AWS CSI ドライバーは、Red Hat OpenShift Service on AWS の RWX サポートを提供するのに使用できます。コミュニティー Operator は、設定を簡素化するために提供されます。詳細は、AWS EFS Setup for OpenShift Dedicated and Red Hat OpenShift Service on AWS を参照してください。

### 3.3.6. プラットフォーム

このセクションでは、Red Hat OpenShift Service on AWS (ROSA) プラットフォームのサービス定義を説明します。

#### 3.3.6.1. クラスターバックアップポリシー

**重要**

お客様がアプリケーションとアプリケーションデータのバックアップ計画を立てることが重要です。

アプリケーションおよびアプリケーションデータのバックアップは Red Hat OpenShift Service on AWS サービスの一部として行われません。次の表に、クラスターバックアップポリシーの概要を示します。

| コンポーネント | スナップショットの頻度 | 保持期間 | 注記 |
|---|---|---|---|
| 完全なオブジェクトストアのバックアップ、すべてのクラスターの永続ボリューム (PV) | 毎日 | 7 日 | これは、etcd などのすべての Kubernetes オブジェクトとクラスター内のすべての PV の完全バックアップです。 |
| | 週次 | 30 日 | |

| コンポーネント | スナップショットの頻度 | 保持期間 | 注記 |
| --- | --- | --- | --- |
| 完全なオブジェクトストアのバックアップ | 毎時 | 24 時間 | これは、etcd などのすべての Kubernetes オブジェクトの完全バックアップです。このバックアップスケジュールでは、PV はバックアップされません。 |
| ノードのルートボリューム | なし | 該当なし | ノードは短期的なものと見なされます。ノードのルートボリュームには、何も保存できません。 |

#### 3.3.6.2. 自動スケーリング

ノードの自動スケーリングは Red Hat OpenShift Service on AWS で利用できます。オートスケーラーオプションを設定して、クラスター内のマシンの数を自動的にスケーリングできます。

**関連情報**

- クラスターでのノードの自動スケーリングについて

#### 3.3.6.3. デーモンセット

Red Hat OpenShift Service on AWS でデーモンセットを作成し、実行できます。デーモンセットをワーカーノードでのみの実行に制限するには、以下の **nodeSelector** を使用します。

```
...
spec:
  nodeSelector:
    role: worker
...
```

#### 3.3.6.4. 複数のアベイラビリティゾーン

複数アベイラビリティーゾーンのクラスターでは、コントロールプレーンノードは複数のアベイラビリティーゾーンに分散され、各アベイラビリティーゾーンに 1 つ以上のワーカーノードが必要になります。

#### 3.3.6.5. ノードラベル

カスタムノードラベルはノードの作成時に Red Hat によって作成され、現時点では Red Hat OpenShift Service on AWS クラスターで変更することはできません。ただし、カスタムラベルは新規マシンプールの作成時にサポートされます。

#### 3.3.6.6. OpenShift バージョン

Red Hat OpenShift Service on AWS はサービスとして実行され、最新の OpenShift Container Platform バージョンで最新の状態に維持されます。最新バージョンへのアップグレードのスケジューリング機能を利用できます。

#### 3.3.6.7. アップグレード

アップグレードは、**rosa** CLI ユーティリティーまたは OpenShift Cluster Manager を使用してスケジュールできます。

アップグレードポリシーおよび手順についての詳細は、Red Hat OpenShift Service on AWS のライフサイクル を参照してください。

#### 3.3.6.8. Windows Containers

現時点では、Windows コンテナーに対する Red Hat OpenShift のサポートは Red Hat OpenShift Service on AWS では利用できません。

#### 3.3.6.9. コンテナーエンジン

Red Hat OpenShift Service on AWS は OpenShift 4 で実行され、唯一の利用可能なコンテナーエンジンとして CRI-O を使用します。

#### 3.3.6.10. オペレーティングシステム

Red Hat OpenShift Service on AWS は OpenShift 4 で実行され、すべてのコントロールプレーンおよびワーカーノードのオペレーティングシステムとして Red Hat CoreOS を使用します。

#### 3.3.6.11. Red Hat Operator のサポート

通常、Red Hat ワークロードは、Operator Hub を通じて利用できる Red Hat 提供の Operator を指します。Red Hat ワークロードは Red Hat SRE チームによって管理されないため、ワーカーノードにデプロイする必要があります。これらの Operator は、追加の Red Hat サブスクリプションが必要になる場合があり、追加のクラウドインフラストラクチャーコストが発生する場合があります。これらの Red Hat 提供の Operator の例は次のとおりです。

- Red Hat Quay
- Red Hat Advanced Cluster Management
- Red Hat Advanced Cluster Security
- Red Hat OpenShift Service Mesh
- OpenShift Serverless
- Red Hat OpenShift Logging
- Red Hat OpenShift Pipelines

#### 3.3.6.12. Kubernetes Operator のサポート

Operator Hub Marketplace に一覧表示されるすべての Operator はインストールに利用できるはずです。これらの Operator はお客様のワークロードと見なされるため、Red Hat SRE の監視の対象外です。

### 3.3.7. セキュリティー

このセクションでは、Red Hat OpenShift Service on AWS セキュリティーのサービス定義を説明します。

#### 3.3.7.1. 認証プロバイダー

クラスターの認証は、OpenShift Cluster Manager Hybrid Cloud Console またはクラスター作成プロセス、または **rosa** CLI を使用して設定できます。Red Hat OpenShift Service on AWS はアイデンティティープロバイダーではないため、クラスターへのアクセスすべてが統合ソリューションの一部としてお客様によって管理される必要があります。同時にプロビジョニングされる複数のアイデンティティープロバイダーの使用がサポートされます。以下のアイデンティティープロバイダーがサポートされます。

- GitHub または GitHub Enterprise
- GitLab
- Google
- LDAP
- OpenID Connect

#### 3.3.7.2. 特権付きコンテナー

特権付きコンテナーは、**cluster-admin** ロールを持つユーザーが利用できます。特権付きコンテナーを **cluster-admin** として使用する場合、これは Red Hat Enterprise Agreement Appendix 4 (Online Subscription Services) の責任および除外事項に基づいて使用されます。

#### 3.3.7.3. お客様側の管理者ユーザー

通常ユーザーのほかに、Red Hat OpenShift Service on AWS は **dedicated-admin** という Red Hat OpenShift Service on AWS 固有のグループへのアクセスを提供します。**dedicated-admin** グループのメンバーであるクラスターのすべてのユーザーには、以下が該当します。

- クラスターのお客様が作成したすべてのプロジェクトへの管理者アクセスがある。
- クラスターのリソースクォータおよび制限を管理できる。
- **NetworkPolicy** オブジェクトを追加し、管理できる。
- スケジューラー情報を含む、クラスター内の特定のノードおよび PV に関する情報を表示できる。
- クラスターの予約された **dedicated-admin** プロジェクトにアクセスできる。これにより、昇格した権限を持つサービスアカウントの作成が可能になり、クラスターのプロジェクトのデフォルトの制限およびクォータを更新する機能も提供されます。

#### 3.3.7.4. クラスター管理ロール

Red Hat OpenShift Service on AWS の管理者には、組織のクラスターについて **cluster-admin** ロールへのデフォルトアクセスがあります。**cluster-admin** ロールを持つアカウントにログインしている場合、ユーザーのパーミッションは、特権付きセキュリティーコンテキストを実行するために拡大します。

#### 3.3.7.5. プロジェクトのセルフサービス

デフォルトで、すべてのユーザーはプロジェクトを作成し、更新し、削除することができます。これは、**dedicated-admin** グループのメンバーが認証されたユーザーから **self-provisioner** ロールを削除すると制限されます。

```
$ oc adm policy remove-cluster-role-from-group self-provisioner system:authenticated:oauth
```

以下を適用すると、制限を元に戻すことができます。

```
$ oc adm policy add-cluster-role-to-group self-provisioner system:authenticated:oauth
```

#### 3.3.7.6. 法規制コンプライアンス

最新のコンプライアンス情報は、Red Hat OpenShift Service on AWS のプロセスおよびセキュリティーについてを参照してください。

#### 3.3.7.7. ネットワークセキュリティー

Red Hat OpenShift Service on AWS では、AWS は AWS Shield と呼ばれる標準の DDoS 保護をすべてのロードバランサーで提供します。これにより、Red Hat OpenShift Service on AWS に使用されるすべてのパブリック向けロードバランサーで最も一般的に使用されるレベル 3 および 4 攻撃に対し、95% の保護が提供されます。応答を受信するために **haproxy** ルーターに送信される HTTP 要求に 10 秒のタイムアウトが追加されるか、または追加の保護を提供するために接続が切断されます。

#### 3.3.7.8. etcd 暗号化

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。このストレージレベルの暗号化は、クラウドプロバイダーのストレージ層を介して提供されます。

etcd 暗号化を有効にして、キーではなく etcd のキーの値を暗号化することもできます。etcd 暗号化を有効にすると、以下の Kubernetes API サーバーおよび OpenShift API サーバーリソースが暗号化されます。

- シークレット
- 設定マップ
- ルート
- OAuth アクセストークン
- OAuth 認証トークン

etcd 暗号化機能はデフォルトで有効にされず、これはクラスターのインストール時にのみ有効にできます。etcd 暗号化が有効にされている場合でも、コントロールプレーンノードにアクセスできるユーザーまたは **cluster-admin** 権限を持つユーザーは、etcd キーの値にアクセスできます。

**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。

### 3.3.8. 関連情報

- 最新のコンプライアンス情報は、Understanding process and security for ROSA を参照してください。
- ROSA life cycle を参照してください。

## 3.4. RED HAT OPENSHIFT SERVICE ON AWS 更新ライフサイクル

### 3.4.1. 概要

Red Hat は、Red Hat OpenShift Service on AWS の製品ライフサイクルを公開しています。これにより、お客様およびパートナー様は、プラットフォーム上で実行されるアプリケーションの計画、デプロイ、サポートを効果的に行えます。Red Hat は、可能な限りの透明性を実現するためにこのライフサイクルを公開していますが、問題が発生した場合はこれらのポリシーに例外を設ける場合もあります。

Red Hat OpenShift Service on AWS は Red Hat OpenShift のマネージドインスタンスであり、独立したリリーススケジュールを維持します。マネージドオファリングについての詳細は、Red Hat OpenShift Service on AWS のサービス定義を参照してください。特定バージョンのセキュリティーアドバイザリーおよびバグ修正アドバイザリーは、Red Hat OpenShift Container Platform のライフサイクルポリシーに基づいて利用可能となり、Red Hat OpenShift Service on AWS のメンテナーンススケジュールに基づいて提供されます。

**関連情報**

- Red Hat OpenShift Service on AWS のサービス定義

### 3.4.2. 定義

**表3.1 バージョン参照**

| バージョンの形式 | メジャー | マイナー | パッチ | major.minor.patch |
|---|---|---|---|---|
| | x | y | z | x.y.z |
| 例 | 4 | 5 | 21 | 4.5.21 |

**メジャーリリースまたは X リリース**

**メジャーリリース** または **X リリース** (X.y.z) としてのみ言及されます。

**例**

- "メジャーリリース 5" → 5.y.z
- "メジャーリリース 4" → 4.y.z
- "メジャーリリース 3" → 3.y.z

**マイナーリリースまたは Y リリース**

**マイナーリリース** または **Y リリース** (x.Y.z) としてのみ言及されます。

**例**

- "マイナーリリース 4" → 4.4.z
- "マイナーリリース 5" → 4.5.z
- "マイナーリリース 6" → 4.6.z

**パッチリリースまたは Z リリース**

**パッチリリース** または **Z リリース** (x.y.Z) としてのみ言及されます。

**例**

- "マイナーリリース 5 のパッチリリース 14" → 4.5.14
- "マイナーリリース 5 のパッチリリース 25" → 4.5.25
- "マイナーリリース 6 のパッチリリース 26" → 4.6.26

### 3.4.3. メジャーバージョン (X.y.z)

Red Hat OpenShift Service on AWS のメジャーバージョン (バージョン 4 など) は、後続のメジャーバージョンのリリースまたは製品の終了後 1 年間サポートされます。

**例**

- Red Hat OpenShift Service on AWS についてバージョン 5 が 1 月 1 日に利用可能になる場合、バージョン 4 は 12 月 31 日までの 12 カ月間、マネージドクラスターで実行を継続することができます。その後、クラスターはアップグレード、またはバージョン 5 に移行する必要があります。

### 3.4.4. マイナーバージョン (x.Y.z)

OpenShift Container Platform 4.8 のマイナーバージョン以降、Red Hat は、該当のマイナーバージョンの一般提供後 14 カ月間、すべてのマイナーバージョンをサポートします。パッチバージョンは、14 か月のサポート期間の影響を受けません。

14 カ月間の終了 60 日、30 日、および 15 日前に、お客様は通知を受けます。クラスターは 14 カ月間が終了する前にサポート対象のマイナーバージョンにアップグレードする必要があります。アップグレードしないと、クラスターは限定的なサポートのステータスになります。

**例**

1. 現時点で、お客様のクラスターは 4.8.14 で実行しているとします。4.8 マイナーバージョンは、2021 年 7 月 27 日に一般提供されました。
2. 2022 年 7 月 29 日、8 月 28 日、および 9 月 12 日に、クラスターがまだサポート対象のマイナーバージョンにアップグレードされていない場合、2022 年 9 月 27 日にクラスターが「制限付きサポート」ステータスになることがお客様に通知されます。
3. クラスターは、2022 年 9 月 27 日までに 4.9 以降にアップグレードする必要があります。
4. アップグレードが実行されていない場合、クラスターには限定的なサポートのステータスのフラグが設定されます。

**関連情報**

- Red Hat OpenShift Service on AWS サポートの制限付きステータス (limited supported status)

### 3.4.5. パッチバージョン (x.y.Z)

マイナーバージョンがサポートされる期間中、とくに指定がない限り、Red Hat はすべての OpenShift Container Platform パッチバージョンをサポートします。

プラットフォームのセキュリティーおよび安定性の理由から、あるパッチリリースが非推奨になる可能性があります。この場合は、そのリリースのインストールができなくなり、そのリリースからの強制的なアップグレードが必要となります。

**例**

1. 4.7.6 に重要な CVE が含まれることが確認されるとします。
2. CVE の影響を受けるすべてのリリースは、サポートされるパッチリリースの一覧から削除されます。さらに、4.7.6 を実行するクラスターについては、自動アップグレードのスケジュールが 48 時間以内に行われます。

### 3.4.6. 限定的なサポートのステータス

クラスターが **限定サポート** ステータスに移行すると、Red Hat はクラスターをプロアクティブに監視しなくなり、SLA は適用されなくなり、SLA に対して要求されたクレジットは拒否されます。製品サポートがなくなったという意味ではありません。場合によっては、違反要因を修正すると、クラスターが完全にサポートされた状態に戻ることがあります。ただし、それ以外の場合は、クラスターを削除して再作成する必要があります。

クラスターは、次のシナリオなど、さまざまな理由で限定サポートステータスに移行する場合があります。

**サポート終了日までにクラスターをサポートされるバージョンにアップグレードしない場合**

Red Hat は、サポート終了日以降のバージョンについて、ランタイムまたは SLA を保証しません。継続的なサポートを受けるには、サポートが終了する前に、クラスターを、サポートされているバージョンにアップグレードしてください。有効期限が切れる前にクラスターをアップグレードしない場合、クラスターは、サポートされているバージョンにアップグレードされるまで、限定サポートステータスに移行します。

Red Hat は、サポートされていないバージョンからサポートされているバージョンにアップグレードするための商業的に合理的なサポートを提供します。ただし、サポートされるアップグレードパスが利用できなくなった場合は、新規クラスターを作成し、ワークロードを移行することが必要になることがあります。

**ネイティブの Red Hat OpenShift Service on AWS コンポーネント、または Red Hat がインストールおよび管理するその他のコンポーネントを削除または置き換える場合**

クラスター管理者パーミッションを使用した場合、Red Hat は、インフラストラクチャーサービス、サービスの可用性、またはデータ損失に影響を与えるアクションを含む、ユーザーまたは認可されたユーザーのアクションに対して責任を負いません。Red Hat がそのようなアクションを検出した場合、クラスターは限定サポートステータスに移行する可能性があります。Red Hat はステータスの変更を通知します。アクションを元に戻すか、サポートケースを作成して、クラスターの削除と再作成が必要になる可能性のある修復手順を検討する必要があります。

クラスターが限定サポートステータスに移行する可能性のある特定のアクションについて質問がある場合、またはさらに支援が必要な場合は、サポートチケットを作成します。

### 3.4.7. サポート対象バージョンの例外ポリシー

Red Hat は、事前通知なしに新規または既存のバージョンを追加または削除したり、実稼働環境に影響を与える重要なバグまたはセキュリティーの問題があることが確認された今後のマイナーリリースバージョンを遅延させる権利を留保します。

### 3.4.8. インストールポリシー

Red Hat では、最新のサポートリリースのインストールを推奨していますが、Red Hat OpenShift Service on AWS は前述のポリシーに記載されているサポート対象のリリースのインストールをサポートします。

### 3.4.9. 必須アップグレード

Critical (重大) または Important (重要) の CVE、または Red Hat が特定するその他のバグが、クラスターのセキュリティーまたは安定性に大幅に影響を与える場合、お客様は 2 営業日 以内にサポート対象の次のパッチリリースにアップグレードする必要があります。

極端な場合、また Red Hat による CVE の環境に対する重大度の評価に基づき、次のサポート対象のパッチリリースへのアップグレードが通知後 2 営業日 以内に実行されていない場合に、セキュリティー違反または不安定な状態が発生する可能性を軽減するために、クラスターは最新のパッチリリースに自動的に更新されます。

### 3.4.10. ライフサイクルの日付

| バージョン | 一般公開 | ライフサイクルの終了日 |
|---|---|---|
| 4.11 | 2022 年 8 月 10 日 | 2023 年 10 月 10 日 |
| 4.10 | 2022 年 3 月 10 日 | 2023 年 5 月 10 日 |
| 4.9 | 2021 年 10 月 18 日 | 2022 年 12 月 18 日 |
| 4.8 | 2021 年 7 月 27 日 | 2022 年 9 月 27 日 |

## 3.5. RED HAT OPENSHIFT SERVICE ON AWS のプロセスおよびセキュリティーについて

以下では、管理対象の Red Hat OpenShift Service on AWS (ROSA) における Red Hat の責任について説明します。

**頭字語および用語**

- **AWS** - Amazon Web Services
- **CEE** - Customer Experience and Engagement (Red Hat サポート)
- **CI/CD** - 継続的インテグレーション/継続的デリバリー
- **CVE** - 共通脆弱性識別子 (Common Vulnerabilities and Exposures)

- **PV** - 永続ボリューム
- **ROSA** - Red Hat OpenShift Service on AWS
- **SRE** - Red Hat のサイト信頼性エンジニアリング (Site Reliability Engineering)
- **VPC** - Virtual Private Cloud

### 3.5.1. インシデントおよびオペレーション管理

以下では、Red Hat OpenShift Service on AWS (ROSA) マネージドサービスにおける Red Hat の責任について詳しく説明します。

#### 3.5.1.1. プラットフォームモニタリング

Red Hat のサイト信頼性エンジニアリング (SRE) チームは、すべての ROSA クラスターコンポーネント、SRE サービス、および基礎となる AWS アカウントに関する一元的なモニターリングおよびアラートシステムを維持します。プラットフォーム監査ログは、一元化された SIEM (security information and event monitoring) システムに安全に転送されます。これにより、SRE チームに対して設定されたアラートがトリガーされる場合は手動によるレビューの対象となります。監査ログは SIEM システムに 1 年間保持されます。指定されたクラスターの監査ログは、クラスターの削除時に削除されません。

#### 3.5.1.2. インシデント管理

インシデントは、1 つ以上の Red Hat サービスの低下や停止をもたらすイベントです。インシデントは、お客様または CEE (Customer Experience and Engagement) のメンバーがサポートケースを通して報告されるか、一元化されたモニターリングおよびアラートシステムから直接提出されるか、または SRE チームのメンバーから直接提出される場合があります。

サービスおよびお客様への影響に応じて、インシデントは 重大度 に基づいて分類されます。

新たなインシデントを管理する際に、Red Hat では以下の一般的なワークフローを使用します。

1. SRE の最初に応答するメンバーには新たなインシデントについてのアラートが送られ、最初の調査が開始されます。
2. 初回の調査後、インシデントには復旧作業を調整するインシデントのリード (担当者) が割り当てられます。
3. インシデントのリードは、関連する通知やサポートケースの更新など、リカバリーに関するすべての通信および調整を管理します。
4. インシデントの復旧が行われます。
5. インシデントが文書化され、Root Cause Analysis (根本原因分析 (RCA)) がインシデント発生後 5 営業日以内に実行されます。
6. RCA のドラフト文書は、インシデント発生後 7 日以内にお客様に共有されます。

#### 3.5.1.3. 通知

プラットフォーム通知は、メールを使用して設定されます。一部のお客様への通知はアカウントの対応 Red Hat アカウントチーム (テクニカルアカウントマネージャーを含む) にも送信されます。

以下のアクティビティーで通知をトリガーできます。

- プラットフォームのインシデント
- パフォーマンスの低下
- クラスター容量に関する警告
- 重大な脆弱性および解決
- アップグレードのスケジュール

#### 3.5.1.4. STS を使用した ROSA クラスターのバックアップおよび復元

STS の ROSA クラスターで利用可能なバックアップ方法はありません。

#### 3.5.1.5. バックアップおよび復元

OpenShift Cluster Manager からのすべての Red Hat OpenShift Service on AWS クラスターメタデータは、Red Hat によって安全にバックアップされます。次の表に、バックアップおよびリカバリーの戦略の概要を示します。

| コンポーネント | スナップショットの頻度 | 保持期間 | 注記 |
|---|---|---|---|
| 完全なオブジェクトストアのバックアップ、すべてのクラスターの永続ボリューム (PV) | 毎日 | 7 日 | これは、etcd などのすべての Kubernetes オブジェクトとクラスター内のすべての PV の完全バックアップです。 |
| | 週次 | 30 日 | |
| 完全なオブジェクトストアのバックアップ | 毎時 | 24 時間 | これは、etcd などのすべての Kubernetes オブジェクトの完全バックアップです。このバックアップスケジュールでは、PV はバックアップされません。 |
| ノードのルートボリューム | なし | 該当なし | ノードは短期的なものと見なされます。ノードのルートボリュームには、何も保存できません。 |

- Red Hat は、RTO (Recovery Point Objective) または RTO (Recovery Time Objective) にコミットしません。
- お客様はデータのバックアップを定期的に行う必要があります。
- お客様は、Kubernetes のベストプラクティスに従ったワークロードでマルチ AZ クラスターをデプロイして、リージョン内の高可用性を確保する必要があります。
- クラウドリージョン全体が利用できない場合、お客様は新しいクラスターを異なるリージョンにインストールし、バックアップデータを使用してアプリケーションを復元する必要があります。

#### 3.5.1.6. クラスター容量

クラスター容量の評価および管理に関する責任は、Red Hat とお客様との間で共有されます。Red Hat SRE は、クラスター上のすべての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容量に関する責任を負います。

Red Hat SRE はアップグレード時に、またクラスターのアラートへの対応としてクラスター容量の評価も行います。クラスターアップグレードの容量に与える影響は、アップグレードのテストプロセスの一部として評価され、容量がクラスターへの新たな追加内容の影響を受けないようにします。クラスターのアップグレード時にワーカーノードが追加され、クラスターの容量全体がアップグレードプロセス時に維持されるようにします。

Red Hat SRE チームによる容量評価は、使用状況のしきい値が一定期間超過した後のクラスターからのアラートへの対応として行われます。このアラートにより、通知がお客様に出されます。

### 3.5.2. 変更管理

このセクションでは、クラスターおよび設定変更、パッチ、およびリリースの管理方法に関するポリシーについて説明します。

#### 3.5.2.1. お客様が開始する変更

クラスターデプロイメント、ワーカーノードのスケーリング、またはクラスターの削除などのセルフサービス機能を使用して変更を開始できます。

変更履歴は、OpenShift Cluster Manager の **概要タブ** の **クラスター履歴** セクションにキャプチャーされ、表示できます。変更履歴には、以下の変更のログが含まれますが、これに限定されません。

- アイデンティティープロバイダーの追加または削除
- **dedicated-admins** グループへの/からのユーザーの追加または削除
- クラスターコンピュートノードのスケーリング
- クラスターロードバランサーのスケーリング
- クラスター永続ストレージのスケーリング
- クラスターのアップグレード

以下のコンポーネントの OpenShift Cluster Manager での変更を回避することで、メンテナーンスの除外を実装できます。

- クラスターの削除
- ID プロバイダーの追加、変更、または削除
- 昇格されたグループからのユーザーの追加、変更、または削除
- アドオンのインストールまたは削除
- クラスターネットワーク設定の変更
- マシンプールの追加、変更、または削除
- ユーザーワークロードの監視の有効化または無効化
- アップグレードの開始

**重要**

メンテナンスの除外を適用するには、マシンプールの自動スケーリングまたは自動アップグレードポリシーが無効になっていることを確認してください。メンテナンスの除外が解除されたら、必要に応じてマシンプールの自動スケーリングまたは自動アップグレードポリシーを有効にします。

#### 3.5.2.2. Red Hat が開始する変更

Red Hat サイト信頼性エンジニアリング (SRE) は、GitOps ワークフローと完全に自動化された CI/CD パイプラインを使用して、Red Hat OpenShift Service on AWS のインフラストラクチャー、コード、および設定を管理します。このプロセスにより、Red Hat は、お客様に悪影響を与えることなく、継続的にサービスの改善を安全に導入できます。

提案されるすべての変更により、チェック時にすぐに一連の自動検証が実行されます。変更は、自動統合テストが実行されるステージング環境にデプロイされます。最後に、変更は実稼働環境にデプロイされます。各ステップは完全に自動化されます。

認可された SRE レビュー担当者は、各ステップに進む前にこれを承認する必要があります。変更を提案した個人がレビュー担当者になることはできません。すべての変更および承認は、GitOps ワークフローの一部として完全に監査可能です。

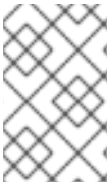
一部の変更は、機能フラグを使用して指定されたクラスターまたはお客様に対する新機能の可用性を制御することで、段階的にリリースされます。

#### 3.5.2.3. パッチ管理

OpenShift Container Platform ソフトウェアおよび基礎となるイミュータブルな Red Hat CoreOS (RHCOS) オペレーティングシステムイメージには、通常の z-stream アップグレードのバグおよび脆弱性のパッチが適用されます。OpenShift Container Platform ドキュメントの RHCOS アーキテクチャー を参照してください。

#### 3.5.2.4. リリース管理

Red Hat はクラスターを自動的にアップグレードしません。OpenShift Cluster Manager Web コンソールを使用して、クラスターの更新を定期的に (定期的なアップグレード) または 1 回だけ (個別にアップグレード) 行うようにスケジュールできます。クラスターが重大な影響を与える CVE の影響を受ける場合にのみ、Red Hat はクラスターを新しい z-stream バージョンに強制的にアップグレードする可能性があります。



**注記**

必要な権限は y-stream リリース間で変更される可能性があるため、アップグレードを実行する前にポリシー更新が必要になる場合があります。したがって、STS を使用する ROSA クラスターで定期的なアップグレードをスケジュールすることはできません。

お客様は OpenShift Cluster Manager Web コンソールで、すべてのクラスターアップグレードイベントの履歴を確認できます。リリースの詳細は、ライフサイクルポリシー を参照してください。

### 3.5.3. アイデンティティーおよびアクセス管理

Red Hat Site Reliability Engineering (SRE) チームによるアクセスのほとんどは、自動化された設定管理によりクラスター Operator を使用して行われます。

#### 3.5.3.1. サブプロセッサー

利用可能なサブプロセスの一覧は、Red Hat カスタマーポータルの Red Hat Subprocessor List を参照してください。

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

SRE は、Web コンソールまたはコマンドラインツールを使用して Red Hat OpenShift Service on AWS クラスターにアクセスします。認証には、パスワードの複雑さおよびアカウントのロックアウトに関する業界標準の要件が適用されるマルチファクター認証 (MFA) が必要です。SRE は、監査可能性を確保するために個人として認証する必要があります。すべての認証試行は、セキュリティー情報およびイベント管理 (SIEM) システムに記録されます。

SRE は、暗号化された HTTP 接続を使用してプライベートクラスターにアクセスします。接続は、IP 許可リストまたはプライベートクラウドプロバイダーのリンクを使用して、セキュアな Red Hat ネットワークからのみ許可されます。

#### 3.5.3.3. Red Hat OpenShift Service on AWS での特権アクセスの制御

SRE は、Red Hat OpenShift Service on AWS および AWS コンポーネントにアクセスする際に最小権限の原則に従います。手動による SRE アクセスには、基本的に以下の 4 つのカテゴリーがあります。

- 通常の 2 要素認証を使用するが、権限の昇格のない Red Hat ポータル経由での SRE の管理者アクセス。
- 通常の 2 要素認証を使用するが、権限の昇格のない Red Hat の企業 SSO を使用した SRE の管理者アクセス。
- OpenShift の昇格。これは Red Hat SSO を使用した手動による昇格です。アクセスは 2 時間に制限され、完全に監査対象となり、管理者承認が必要になります。
- AWS アクセスまたは昇格。AWS コンソールまたは CLI アクセスの手動による昇格です。アクセスは 60 分間に制限され、完全に監査されます。

これらのアクセスタイプのそれぞれには、コンポーネントへの異なるレベルのアクセスがあります。

| コンポーネント | 通常の SRE 管理者アクセス (Red Hat ポータル) | 通常の SRE 管理者アクセス (Red Hat SSO) | OpenShift の昇格 | クラウドプロバイダーのアクセスまたは昇格 |
|---|---|---|---|---|
| OpenShift Cluster Manager | R/W | アクセスなし | アクセスなし | アクセスなし |
| OpenShift コンソール | アクセスなし | R/W | R/W | アクセスなし |
| ノードのオペレーティングシステム | アクセスなし | 昇格した OS およびネットワークのパーミッションの一覧。 | 昇格した OS およびネットワークのパーミッションの一覧。 | アクセスなし |

| コンポーネント | 通常の SRE 管理者アクセス (Red Hat ポータル) | 通常の SRE 管理者アクセス (Red Hat SSO) | OpenShift の昇格 | クラウドプロバイダーのアクセスまたは昇格 |
|---|---|---|---|---|
| AWS コンソール | アクセスなし | アクセスはありませんが、これはクラウドプロバイダーのアクセスを要求するために使用されるアカウントです。 | アクセスなし | SRE アイデンティティーを使用したすべてのクラウドプロバイダーのパーミッション。 |

#### 3.5.3.4. SRE の AWS アカウントへのアクセス

Red Hat の担当者は、通常の Red Hat OpenShift Service on AWS 操作では AWS アカウントにアクセスしません。緊急のトラブルシューティングが必要な場合に、SRE にはクラウドインフラストラクチャーアカウントにアクセスするための明確に定義された監査可能な手順があります。

SRE は、AWS Security Token Service (STS) を使用して確保したロールの有効期間の短い AWS アクセストークンを生成します。STS トークンへのアクセスは監査ログに記録され、個別のユーザーまでトレースできます。STS および非 STS クラスターはいずれも、SRE アクセスに AWS STS サービスを使用します。STS 以外のクラスターの場合、**BYOCAdminAccess** ロールには **AdministratorAccess** IAM ポリシーが割り当てられ、このロールは管理に使用されます。STS クラスターの場合、**ManagedOpenShift-Support-Role** には **ManagedOpenShift-Support-Access** ポリシーが割り当てられており、このロールは管理に使用されます。

#### 3.5.3.5. Red Hat サポートのアクセス

通常、Red Hat の CEE (Customer Experience and Engagement) チームは、クラスターの各部分への読み取り専用アクセスを持ちます。とくに、CEE にはコアおよび製品の namespace への制限されたアクセスがありますが、お客様の namespace へのアクセスはありません。

| ロール | コア namespace | 階層化した製品 namespace | お客様の namespace | AWS アカウント* |
|---|---|---|---|---|
| OpenShift SRE | 読み取り: All<br>書き込み: Very 限定的[1] | 読み取り: All<br>書き込み: None | 読み取り: None[2]<br>書き込み: None | 読み取り: All [3]<br>書き込み: All [3] |
| CEE | 読み取り: All<br>書き込み: None | 読み取り: All<br>書き込み: None | 読み取り: None[2]<br>書き込み: None | 読み取り: None<br>書き込み: None |
| お客様管理者 | 読み取り: None<br>書き込み: None | 読み取り: None<br>書き込み: None | 読み取り: All<br>書き込み: All | 読み取り: All<br>書き込み: All |

| ロール | コア namespace | 階層化した製品 namespace | お客様の namespace | AWS アカウント* |
|---|---|---|---|---|
| お客様ユーザー | 読み取り: None<br>書き込み: None | 読み取り: None<br>書き込み: None | 読み取り: Limited[4]<br>書き込み: Limited[4] | 読み取り: None<br>書き込み: None |
| 上記以外 | 読み取り: None<br>書き込み: None | 読み取り: None<br>書き込み: None | 読み取り: None<br>書き込み: None | 読み取り: None<br>書き込み: None |

1. デプロイメントの失敗、クラスターのアップグレード、および正しくないワーカーノードの置き換えなどの一般的なユースケースに対応することに限定されます。
2. Red Hat は、デフォルトではお客様のデータにアクセスできません。
3. SRE は AWS アカウントに、文書化されたインシデントの発生時の例外的なトラブルシューティングのための緊急手順としてアクセスします。
4. お客様管理者によって RBAC で許可されるものや、ユーザーが作成した namespace に限定されます。

#### 3.5.3.6. お客様のアクセス

お客様のアクセスは、お客様によって作成される namespace、およびお客様管理者ロールによって RBAC を使用して付与されるパーミッションに限定されます。基礎となるインフラストラクチャーまたは製品 namespace へのアクセスは通常、**cluster-admin** アクセスなしでは許可されません。お客様のアクセスと認証について詳細は、本書の認証についてのセクションを参照してください。

#### 3.5.3.7. アクセスの承認およびレビュー

新規の SRE ユーザーアクセスには、管理者の承認が必要です。分離された SRE アカウントまたは転送された SRE アカウントは、自動化されたプロセスで認可されたユーザーとして削除されます。さらに、SRE は、認可されたユーザー一覧の管理者の署名を含む、定期的なアクセスのレビューを実行します。

### 3.5.4. セキュリティーおよび規制コンプライアンス

セキュリティーおよび規制コンプライアンスには、セキュリティー管理の実装やコンプライアンス認定などのタスクが含まれます。

#### 3.5.4.1. データの分類

Red Hat は、データの機密性を判断し、収集、使用、送信、保存、処理中にデータの機密性と整合性に対する固有のリスクを特定するためにデータ分類の標準を定義し、これに従います。お客様が所有するデータは、最高レベルの機密性と処理要件を持つものとして分類されます。

#### 3.5.4.2. データ管理

Red Hat OpenShift Service on AWS (ROSA) は、AWS Key Management Service (KMS) を使用して、暗号化されたデータのキーを安全に管理します。これらのキーは、デフォルトで暗号化されるコントロールプレーンのデータボリュームに使用されます。お客様のアプリケーションの永続ボリューム (PV)

は、キー管理に AWS KMS を使用します。

お客様が ROSA クラスターを削除すると、コントロールプレーンのデータボリュームや、永続ボリューム (PV) などのお客様のアプリケーションデータボリュームを含め、すべてのクラスターのデータが永久に削除されます。

#### 3.5.4.3. 脆弱性管理

Red Hat は業界標準ツールを使用して ROSA の定期的な脆弱性スキャンを実行します。特定される脆弱性は、重大度に基づくタイムラインに応じて修復されるまで追跡されます。コンプライアンス認定監査の過程で、脆弱性スキャンと修復のアクティビティーが文書化され、サードパーティーの評価者による検証が行われます。

#### 3.5.4.4. ネットワークセキュリティー

##### 3.5.4.4.1. ファイアウォールおよび DDoS 保護

各 ROSA クラスターは、AWS セキュリティーグループのファイアウォールルールを使用してセキュアなネットワーク設定で保護されます。ROSA のお客様は、AWS Shield Standard により DDoS 攻撃に対して保護されます。

##### 3.5.4.4.2. プライベートクラスターおよびネットワーク接続

お客様はオプションとして、Web コンソール、API、アプリケーションルーターなどの ROSA クラスターエンドポイントをプライベートに設定し、クラスターのコントロールプレーンおよびアプリケーションがインターネットからアクセスされないようにすることができます。Red Hat SRE には、IP 許可リストを使用して保護されるインターネットアクセス可能なエンドポイントが必要です。

AWS のお客様は、AWS VPC のピアリング、AWS VPN、AWS Direct Connect などのテクノロジーを使用して、ROSA クラスターへのプライベートネットワーク接続を設定できます。

##### 3.5.4.4.3. クラスターネットワークのアクセス制御

粒度の細かいネットワークアクセス制御ルールは、お客様が **NetworkPolicy** オブジェクトおよび OpenShift SDN を使用してプロジェクトごとに設定できます。

#### 3.5.4.5. ペネトレーションテスト

Red Hat は、ROSA に対して定期的なペネトレーションテストを実行します。テストは、業界標準ツールやベストプラクティスを使用して独立した内部チームによって実行されます。

検出される可能性のある問題は、重大度に基づいて優先付けされます。オープンソースプロジェクトに属する問題が確認される場合は、解決に向けてコミュニティーに共有されます。

#### 3.5.4.6. コンプライアンス

Red Hat OpenShift Service on AWS は、セキュリティーおよび管理に関する一般的な業界のベストプラクティスに従います。認定の概要を以下の表に示します。

**表3.2 Red Hat OpenShift Service on AWS のセキュリティーおよび管理に関する認定**

| 認定 | Red Hat OpenShift Service on AWS |
| --- | --- |
| ISO 27001 | はい |
| PCI DSS | はい |
| SOC 2 タイプ 2 | はい |

**関連情報**

- SRE の常駐に関する詳細は、Red Hat Subprocessor List を参照してください。

### 3.5.5. 障害復旧

Red Hat OpenShift Service on AWS (ROSA) は、Pod、ワーカーノード、インフラストラクチャーノード、コントロールプレーンノード、およびアベイラビリティーゾーンレベルで発生する障害について障害復旧を行います。

すべての障害復旧では、必要な可用性レベルを確保するために、単一ゾーンのデプロイメントまたは複数ゾーンのデプロイメントなど、高可用性アプリケーション、ストレージ、およびクラスターアーキテクチャーのデプロイにベストプラクティスを採用する必要があります。

単一ゾーンクラスターは、アベイラビリティーゾーンまたはリージョンの停止時に障害を防止したり、リカバリーを行ったりしません。お客様によってメンテナーンスされるフェイルオーバーが設定される複数の単一ゾーンクラスターは、ゾーンまたはリージョンレベルで停止に対応できます。

1 つの複数ゾーンクラスターは、リージョンが完全に停止した場合に障害を防止したり、リカバリーを行ったりしません。お客様によってメンテナーンスされるフェイルオーバーが設定される複数の複数ゾーンクラスターは、リージョンレベルで停止に対応できます。

### 3.5.6. 関連情報

- お客様や共有される責任についての詳細は、ROSA の責任 についての文書を参照してください。
- ROSA およびそのコンポーネントについての詳細は、ROSA サービス定義 を参照してください。

# 第4章 STS を使用する ROSA クラスターの IAM リソースについて

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には、以下の AWS Identity Access Management (IAM) リソースを作成する必要があります。

- ROSA サポート、インストール、コントロールプレーン、およびコンピュート機能に必要な STS パーミッションを提供する特定のアカウント全体の IAM ロールおよびポリシー。これには、アカウント全体の Operator ポリシーが含まれます。
- ROSA クラスター Operator がコア OpenShift 機能を実行できるようにするクラスター固有の Operator IAM ロール。
- クラスター Operator が認証に使用する OpenID Connect (OIDC) プロバイダー。
- OpenShift Cluster Manager を使用して ROSA をデプロイする場合は、追加のリソースを作成する必要があります。
  - クラスターへのインストールを完了するための OpenShift Cluster Manager IAM ロール。
  - AWS アカウント ID を確認するための権限のないユーザーロール。

本書では、STS を使用する ROSA クラスターの作成時にデプロイする必要のある IAM リソースについての参考情報を提供します。また、**rosa create** コマンドで **manual** モードを使用する場合に生成される **aws** CLI コマンドも含まれます。

**関連情報**

- AWS IAM リソースを含む STS を使用して 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 を使用した ROSA クラスターの作成 を参照してください。
- AWS IAM リソースを含むカスタマイズを使用して STS で ROSA クラスターを作成する手順は、カスタマイズを使用して STS を使用する ROSA クラスターの作成 を参照してください。

## 4.1. OPENSHIFT CLUSTER MANAGER のロールおよび権限

OpenShift Cluster Manager Hybrid Cloud Console を使用して ROSA クラスターを作成する場合、以下の AWS IAM ロールを AWS アカウントにリンクしてクラスターを作成し、管理する必要があります。IAM ロールを AWS アカウントにリンクする方法は、AWS アカウントの関連付け を参照してください。

**ヒント**

**rosa** CLI ツールのみを使用する場合は、これらの IAM ロールを作成する必要はありません。

これらの AWS IAM ロールは以下のとおりです。

- ROSA ユーザーロールは、お客様の AWS アイデンティティーを検証するために使用する AWS ロールです。このロールには追加のパーミッションがなく、ロールには Red Hat インストーラーアカウントとの信頼関係があります。
- **ocm-role** リソースは、OpenShift Cluster Manager での ROSA クラスターのインストールに必要なパーミッションを付与します。基本的なパーミッションまたは管理パーミッションを **ocm-role** リソースに適用できます。管理用 **ocm-role** リソースを作成する場合、OpenShift Cluster

Manager は必要な AWS Operator ロールと OpenID Connect (OIDC) プロバイダーを作成できます。この IAM ロールは、Red Hat インストーラーアカウントとも信頼関係を構築します。

**注記**

**ocm-role** IAM リソースは、IAM ロールと、作成される必要なポリシーの組み合わせを指します。

OpenShift Cluster Manager で auto モードを使用して Operator ロールポリシーおよび OIDC プロバイダーを作成する場合は、このユーザーロールと管理 **ocm-role** リソースを作成する必要があります。

### 4.1.1. OpenShift Cluster Manager ロールについて

OpenShift Cluster Manager Hybrid Cloud Console で ROSA クラスターを作成するには、**ocm-role** IAM ロールが必要です。基本的な **ocm-role** IAM ロールのパーミッションにより、OpenShift Cluster Manager 内でクラスターのメンテナーンスを実行できます。Operator ロールおよび OpenID Connect(OIDC) プロバイダーを自動的に作成するには、**--admin** オプションを **rosa create** コマンドに追加する必要があります。このコマンドは、管理タスクに必要な追加のパーミッションを持つ **ocm-role** リソースを作成します。

**注記**

この昇格された IAM ロールにより、OpenShift Cluster Manager はクラスターの作成時にクラスター固有の Operator ロールおよび OIDC プロバイダーを自動的に作成できるようになりました。このロールおよびポリシーの自動作成の詳細については、関連情報のアカウント全体のロールの作成方法リンクを参照してください。

#### 4.1.1.1. ユーザーロールについて

**ocm-role** IAM ロールのほかにも、Red Hat OpenShift Service on AWS が AWS アイデンティティーを検証できるようにユーザーロールを作成する必要があります。このロールにはパーミッションがなく、インストーラーアカウントと **ocm-role** リソース間の信頼関係の作成にのみ使用されます。

以下の表は、**ocm-role** リソースの関連付けられた基本および管理パーミッションを示しています。

**表4.1 基本的な ocm-role リソースの関連パーミッション**

| リソース | 説明 |
|---|---|
| **iam:GetOpenIDConnectProvider** | この権限により、基本ロールは指定された OpenID Connect (OIDC) プロバイダーに関する情報を取得できます。 |
| **iam:GetRole** | このパーミッションにより、基本ロールは指定されたロールの情報を取得できます。返されるデータには、ロールのパス、GUID、ARN、およびロールを想定するパーミッションを付与するロールの信頼ポリシーが含まれます。 |
| **iam:ListRoles** | このパーミッションにより、基本ロールはパス接頭辞内のロールを一覧表示できます。 |
| **iam:ListRoleTags** | このパーミッションにより、基本ロールは指定されたロールのタグを一覧表示できます。 |

| リソース | 説明 |
| --- | --- |
| **ec2:DescribeRegions** | このパーミッションにより、基本ロールはアカウントの有効なすべてのリージョンに関する情報を返すことができます。 |
| **ec2:DescribeRouteTables** | このパーミッションにより、基本ロールはすべてのルートテーブルに関する情報を返すことができます。 |
| **ec2:DescribeSubnets** | このパーミッションにより、基本ロールはすべてのサブネットに関する情報を返すことができます。 |
| **ec2:DescribeVpcs** | このパーミッションにより、基本ロールは仮想プライベートクラウド (VPC) に関する情報を返すことができます。 |
| **sts:AssumeRole** | このパーミッションにより、基本ロールは一時的なセキュリティー認証情報を取得して、通常のパーミッション以外の AWS リソースにアクセスできます。 |
| **sts:AssumeRoleWithWebIdentity** | このパーミッションにより、基本ロールは web アイデンティティープロバイダーでアカウントを認証されたユーザーの一時的なセキュリティー認証情報を取得できます。 |

表4.2 admin **ocm-role リソースの追加パーミッション**

| リソース | 説明 |
| --- | --- |
| **iam:AttachRolePolicy** | このパーミッションにより、admin ロールは指定されたポリシーを必要な IAM ロールに割り当てることができます。 |
| **iam:CreateOpenIDConnectProvider** | この権限は、OpenID Connect (OIDC) をサポートする ID プロバイダーを説明するリソースを作成します。このパーミッションで OIDC プロバイダーを作成すると、このプロバイダーはプロバイダーと AWS 間の信頼関係を確立します。 |
| **iam:CreateRole** | このパーミッションにより、admin ロールは AWS アカウントのロールを作成できます。 |
| **iam:ListPolicies** | このパーミッションにより、admin ロールは AWS アカウントに関連付けられたポリシーを一覧表示できます。 |
| **iam:ListPolicyTags** | このパーミッションにより、admin ロールは指定されたポリシーのタグを一覧表示できます。 |
| **iam:PutRolePermissionsBoundary** | このパーミッションにより、admin ロールは指定されたポリシーに基づいてユーザーのパーミッション境界を変更できます。 |
| **iam:TagRole** | このパーミッションにより、admin ロールは IAM ロールにタグを追加できます。 |

**関連情報**

- アカウント全体のロールを作成する方法

### OpenShift Cluster Manager 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、OpenShift Cluster Manager IAM ロールを作成します。

**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ります。
- 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。

**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
```

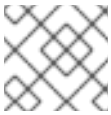
このコマンドを使用すると、特定の属性を指定してロールを作成できます。次の出力例は、選択された自動モードを示しています。これにより、**rosa** CLI で Operator のロールとポリシーを作成できます。詳細については、関連情報のアカウント全体のロールの作成方法を参照してください。

**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 creation mode: auto 4
I: Creating role using 'arn:aws:iam::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes 5
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 6
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with organization
'<AWS ARN'? Yes 7
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 AWS ロールを作成する方法を選択します。**auto** を使用して、**rosa** CLI ツール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 **ocm-role** を作成するかどうかを尋ねます。

6 IAM ロールを OpenShift Cluster Manager に関連付けることを確認します。

7 作成したロールを AWS 組織にリンクします。

AWS IAM ロールは AWS アカウントにリンクして、クラスターを作成および管理します。IAM ロールを AWS アカウントにリンクする方法は、AWS アカウントの関連付け を参照してください。

**関連情報**

- AWS Identity and Access Management Data Types
- Amazon Elastic Computer Cloud Data Types
- AWS Token Security Service Data Types
- アカウント全体のロールを作成する方法

## 4.2. アカウント全体の IAM ロールおよびポリシー参照

このセクションでは、Operator ポリシーを含む、STS を使用する ROSA デプロイメントに必要なアカウント全体の IAM ロールおよびポリシーに関する詳細を提供します。また、ポリシーを定義する JSON ファイルも含まれます。

アカウント全体のロールおよびポリシーは、OpenShift マイナーリリースバージョン (OpenShift 4.8 など) に固有であり、後方互換性があります。パッチバージョンに関係なく、同じマイナーバージョンの複数のクラスターにアカウント全体のロールおよびポリシーを再利用することで、必要な STS リソースを最小限に抑えることができます。

### 4.2.1. アカウント全体のロールを作成する方法

**rosa** CLI ツールまたは OpenShift Cluster Manager Hybrid Cloud Console ガイド付きインストールを使用して、アカウント全体のロールを作成できます。手動で、またはこれらのロールおよびポリシーに事前定義された名前を使用する自動プロセスを使用して、ロールを作成できます。

**rosa** CLI ツールを使用して、アカウント全体のロールを作成できます。手動で、またはこれらのロールおよびポリシーに事前定義された名前を使用する自動プロセスを使用して、ロールを作成できます。

**手動 ocm-role リソースの作成**
システムでこれらのロールを作成するのに必要な CLI アクセスがある場合は、手動作成方法を使用できます。このオプションは、目的の CLI ツールまたは OpenShift Cluster Manager から実行できます。手

動作成プロセスを開始すると、CLI は、ロールを作成して必要なポリシーにリンクする一連のコマンドを実行するために表示します。

**自動 ocm-role リソースの作成**
管理者権限で **ocm-role** リソースを作成した場合は、OpenShift Cluster Manager からの自動作成方法を使用できます。**rosa** CLI では、これらのロールとポリシーを自動的に作成するために、この **adminocm-role** IAM リソースが必要です。この方法を選択すると、デフォルト名を使用するロールおよびポリシーが作成されます。

OpenShift Cluster Manager で ROSA ガイド付きインストールを使用する場合は、ガイド付きクラスターインストールの最初のステップで、管理者権限を持つ **ocm-role** リソースを作成しておく必要があります。このロールがないと、Operator ロールおよびポリシーの自動作成オプションを使用できませんが、クラスターと、そのロールおよびポリシーを手動プロセスで作成することはできます。

**注記**

**sts_installer_trust_policy.json** および **sts_support_trust_policy.json** サンプルに存在するアカウント番号は、必要なロールを引き受けることが許可されている Red Hat アカウントを表します。

**表4.3 ROSA インストーラーロール、ポリシー、およびポリシーファイル**

| リソース | 説明 |
|---|---|
| **ManagedOpenShift-Installer-Role** | ROSA インストーラーによって使用される IAM ロール。 |
| **ManagedOpenShift-Installer-Role-Policy** | クラスターのインストールタスクを完了するのに必要なパーミッションを持つ ROSA インストーラーを提供する IAM ポリシー。 |

**例4.1 sts_installer_trust_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::710019948333:role/RH-Managed-OpenShift-Installer"
                ]
            },
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

**例4.2 sts_installer_permission_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:AssociateDhcpOptions",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CopyImage",
                "ec2:CreateDhcpOptions",
                "ec2:CreateInternetGateway",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteDhcpOptions",
                "ec2:DeleteInternetGateway",
                "ec2:DeleteNatGateway",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteSubnet",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeleteVpc",
                "ec2:DeleteVpcEndpoints",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
```

```
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:DetachInternetGateway",
                "ec2:DisassociateRouteTable",
                "ec2:GetConsoleOutput",
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVpcAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRouteTableAssociation",
                "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: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: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:GetBucketReplication",
"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",
                "ec2:CreateVpcEndpointServiceConfiguration",
                "ec2:DeleteVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:ModifyVpcEndpointServicePermissions"
                "kms:DescribeKey",
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        }
    ]
}
```

**表4.4 ROSA コントロールプレーンのロール、ポリシー、およびポリシーファイル**

| リソース | 説明 |
|---|---|
| **ManagedOpenShift-ControlPlane-Role** | ROSA コントロールプレーンによって使用される IAM ロール。 |
| **ManagedOpenShift-ControlPlane-Role-Policy** | コンポーネントの管理に必要なパーミッションを持つ ROSA コントロールプレーンを提供する IAM ポリシー。 |

**例4.3 sts_instance_controlplane_trust_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

**例4.4 sts_instance_controlplane_permission_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteVolume",
                "ec2:Describe*",
                "ec2:DetachVolume",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyVolume",
                "ec2:RevokeSecurityGroupIngress",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerPolicy",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteLoadBalancerListeners",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:Describe*",
                "elasticloadbalancing:DetachLoadBalancerFromSubnets",
                "elasticloadbalancing:ModifyListener",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

表4.5 ROSA コンピュートノードロール、ポリシー、およびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **ManagedOpenShift-Worker-Role** | ROSA コンピュートインスタンスによって使用される IAM ロール。 |
| **ManagedOpenShift-Worker-Role-Policy** | コンポーネントの管理に必要なパーミッションを持つ ROSA コンピュートインスタンスを提供する IAM ポリシー。 |

**例4.5 sts_instance_worker_trust_policy.json**

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": [
               "ec2.amazonaws.com"
            ]
         },
         "Action": [
            "sts:AssumeRole"
         ]
      }
   ]
}
```

**例4.6 sts_instance_worker_permission_policy.json**

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeInstances"
            "ec2:DescribeRegions"
         ],
         "Resource": "*"
      }
   ]
}
```

表4.6 ROSA サポートロール、ポリシー、およびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **ManagedOpenShift-Support-Role** | Red Hat Site Reliability Engineering (SRE) サポートチームによって使用される IAM ロール。 |
| **ManagedOpenShift-Support-Role-Policy** | ROSA クラスターをサポートするために必要なパーミッションを持つ Red Hat SRE サポートチームを提供する IAM ポリシー。 |

**例4.7 sts_support_trust_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::710019948333:role/RH-Technical-Support-Access"
                ]
            },
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

**例4.8 sts_support_permission_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:LookupEvents",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:CopySnapshot",
                "ec2:CreateNetworkInsightsPath",
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:DeleteTags",
                "ec2:DescribeAccountAttributes",
```

```
                "ec2:DescribeAddresses",
                "ec2:DescribeAddressesAttribute",
                "ec2:DescribeAggregateIdFormat",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeCarrierGateways",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeCoipPools",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeIdFormat",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLocalGatewayRouteTables",
                "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
                "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
                "ec2:DescribeLocalGateways",
                "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
                "ec2:DescribeLocalGatewayVirtualInterfaces",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInsightsAnalyses",
                "ec2:DescribeNetworkInsightsPaths",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePlacementGroups",
                "ec2:DescribePrefixLists",
                "ec2:DescribePrincipalIdFormat",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeRouteTables",
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshotAttribute",
                "ec2:DescribeSnapshots",
```

```
"ec2:DescribeSpotFleetInstances",
"ec2:DescribeStaleSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayConnectPeers",
"ec2:DescribeTransitGatewayConnects",
"ec2:DescribeTransitGatewayMulticastDomains",
"ec2:DescribeTransitGatewayPeeringAttachments",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGateways",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeVolumeAttribute",
"ec2:DescribeVolumeStatus",
"ec2:DescribeVolumes",
"ec2:DescribeVolumesModifications",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcClassicLink",
"ec2:DescribeVpcClassicLinkDnsSupport",
"ec2:DescribeVpcEndpointConnectionNotifications",
"ec2:DescribeVpcEndpointConnections",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcEndpointServicePermissions",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetAssociatedIpv6PoolCidrs",
"ec2:GetConsoleOutput",
"ec2:GetManagedPrefixListEntries",
"ec2:GetSerialConsoleAccessStatus",
"ec2:GetTransitGatewayAttachmentPropagations",
"ec2:GetTransitGatewayMulticastDomainAssociations",
"ec2:GetTransitGatewayPrefixListReferences",
"ec2:GetTransitGatewayRouteTableAssociations",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:ModifyInstanceAttribute",
"ec2:RebootInstances",
"ec2:RunInstances",
"ec2:SearchLocalGatewayRoutes",
"ec2:SearchTransitGatewayMulticastGroups",
"ec2:SearchTransitGatewayRoutes",
"ec2:StartInstances",
"ec2:StartNetworkInsightsAnalysis",
"ec2:StopInstances",
"ec2:TerminateInstances",
"elasticloadbalancing:ConfigureHealthCheck",
"elasticloadbalancing:DescribeAccountLimits",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeListenerCertificates",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
```

```
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeRules",
                "elasticloadbalancing:DescribeSSLPolicies",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GetRole",
                "iam:ListRoles",
                "kms:CreateGrant",
                "route53:GetHostedZone",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "s3:GetBucketTagging",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListAllMyBuckets"
                "sts:DecodeAuthorizationMessage",
                "tiros:CreateQuery",
                "tiros:GetQueryAnswer",
                "tiros:GetQueryExplanation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::managed-velero*",
                "arn:aws:s3:::*image-registry*"
            ]
        }
    ]
}
```

**表4.7 ROSA Ingress Operator IAM ポリシーおよびポリシーファイル**

| リソース | 説明 |
| --- | --- |
| **ManagedOpenShift-openshift-ingress-operator-cloud-credentials** | クラスターへの外部アクセスを管理するために必要なパーミッションを持つ ROSA Ingress Operator を提供する IAM ポリシー。 |

**例4.9 openshift_ingress_operator_cloud_credentials_policy.json**

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

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "route53:ChangeResourceRecordSets",
        "tag:GetResources"
      ],
      "Resource": "*"
    }
  ]
}
```

**表4.8 ROSA バックエンドストレージ IAM ポリシーおよびポリシーファイル**

| リソース | 説明 |
| --- | --- |
| **ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials** | Container Storage Interface (CSI) でバックエンドストレージを管理するのに ROSA が必要とする IAM ポリシー。 |

**例4.10 openshift_cluster_csi_drivers_ebs_cloud_credentials_policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DetachVolume",
        "ec2:ModifyVolume"
      ],
      "Resource": "*"
    }
  ]
}
```

**表4.9 ROSA Machine Config Operator ポリシーおよびポリシーファイル**

| リソース | 説明 |
| --- | --- |
| **ManagedOpenShift-openshift-machine-api-aws-cloud-credentials** | コアクラスター機能の実行に必要なパーミッションと共に ROSA Machine Config Operator を提供する IAM ポリシー。 |

**例4.11 openshift_machine_api_aws_cloud_credentials_policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "iam:PassRole",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlainText",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:RevokeGrant",
        "kms:CreateGrant",
        "kms:ListGrants"
      ],
```

```
      "Resource": "*",
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}
```

表4.10 ROSA Cloud Credential Operator ポリシーおよびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **ManagedOpenShift-openshift-cloud-credential-operator-cloud-credentials** | クラウドプロバイダーの認証情報の管理に必要なパーミッションと共に ROSA Cloud Credential Operator を提供する IAM ポリシー。 |

例4.12 **openshift_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json**

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

表4.11 ROSA Image Registry Operator ポリシーおよびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **ManagedOpenShift-openshift-image-registry-installer-cloud-credentials** | クラスターの AWS S3 で内部レジストリーストレージを管理するために必要なパーミッションを持つ ROSA イメージレジストリー Operator を提供する IAM ポリシー。 |

例4.13 **openshift_image_registry_installer_cloud_credentials_policy.json**

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

```
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketTagging",
        "s3:GetBucketTagging",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetBucketPublicAccessBlock",
        "s3:PutEncryptionConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": "*"
    }
  ]
}
```

**関連情報**

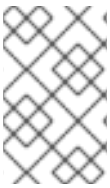
- OpenShift のメジャー、マイナー、およびパッチバージョンの定義については、Red Hat OpenShift Service on AWS の更新ライフサイクル を参照してください。

### 4.2.2. アカウント全体の IAM ロールおよびポリシー AWS CLI リファレンス

このセクションでは、**rosa** コマンドが端末で生成する **aws** CLI コマンドを一覧表示します。コマンドは、手動モードまたは自動モードのいずれかで実行できます。

**アカウントロールの作成に手動モードを使用する**
手動のロール作成モードでは、確認して実行するための **aws** コマンドが生成されます。次のコマンドは、そのプロセスを開始します。

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



**注記**

提供されているコマンドの例には、**ManagedOpenShift** 接頭辞が含まれています。**--prefix** オプションを使用してカスタム接頭辞を指定しない場合は、**ManagedOpenShift** 接頭辞がデフォルト値です。

**コマンド出力**

```
aws iam create-role \
```

```
 --role-name ManagedOpenShift-Installer-Role \
 --assume-role-policy-document file://sts_installer_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=rosa_role_type,Value=installer

aws iam put-role-policy \
 --role-name ManagedOpenShift-Installer-Role \
 --policy-name ManagedOpenShift-Installer-Role-Policy \
 --policy-document file://sts_installer_permission_policy.json

aws iam create-role \
 --role-name ManagedOpenShift-ControlPlane-Role \
 --assume-role-policy-document file://sts_instance_controlplane_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=rosa_role_type,Value=instance_controlplane

aws iam put-role-policy \
 --role-name ManagedOpenShift-ControlPlane-Role \
 --policy-name ManagedOpenShift-ControlPlane-Role-Policy \
 --policy-document file://sts_instance_controlplane_permission_policy.json

aws iam create-role \
 --role-name ManagedOpenShift-Worker-Role \
 --assume-role-policy-document file://sts_instance_worker_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=rosa_role_type,Value=instance_worker

aws iam put-role-policy \
 --role-name ManagedOpenShift-Worker-Role \
 --policy-name ManagedOpenShift-Worker-Role-Policy \
 --policy-document file://sts_instance_worker_permission_policy.json

aws iam create-role \
 --role-name ManagedOpenShift-Support-Role \
 --assume-role-policy-document file://sts_support_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=rosa_role_type,Value=support

aws iam put-role-policy \
 --role-name ManagedOpenShift-Support-Role \
 --policy-name ManagedOpenShift-Support-Role-Policy \
 --policy-document file://sts_support_permission_policy.json

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-ingress-operator-cloud-credentials \
 --policy-document file://openshift_ingress_operator_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-ingress-operator Key=operator_name,Value=cloud-
credentials

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credent \
 --policy-document file://openshift_cluster_csi_drivers_ebs_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-cluster-csi-drivers Key=operator_name,Value=ebs-cloud-
credentials
```

```
aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-machine-api-aws-cloud-credentials \
 --policy-document file://openshift_machine_api_aws_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-machine-api Key=operator_name,Value=aws-cloud-
credentials

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-cloud-credential-operator-cloud-crede \
 --policy-document
file://openshift_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-cloud-credential-operator
Key=operator_name,Value=cloud-credential-operator-iam-ro-creds

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-image-registry-installer-cloud-creden \
 --policy-document file://openshift_image_registry_installer_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-image-registry Key=operator_name,Value=installer-
cloud-credentials
```

**ロール作成に自動モードを使用する**

**--mode auto** 引数を追加すると、**rosa** CLI ツールがロールおよびポリシーを作成します。次のコマンドは、そのプロセスを開始します。

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

**注記**

提供されているコマンドの例には、**ManagedOpenShift** 接頭辞が含まれています。**--prefix** オプションを使用してカスタム接頭辞を指定しない場合は、**ManagedOpenShift** 接頭辞がデフォルト値です。

**コマンド出力**

```
I: Creating roles using 'arn:aws:iam::<ARN>:user/<UserID>'
? Create the 'ManagedOpenShift-Installer-Role' role? Yes
I: Created role 'ManagedOpenShift-Installer-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-Installer-Role'
? Create the 'ManagedOpenShift-ControlPlane-Role' role? Yes
I: Created role 'ManagedOpenShift-ControlPlane-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-ControlPlane-Role'
? Create the 'ManagedOpenShift-Worker-Role' role? Yes
I: Created role 'ManagedOpenShift-Worker-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-Worker-Role'
? Create the 'ManagedOpenShift-Support-Role' role? Yes
I: Created role 'ManagedOpenShift-Support-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-Support-Role'
? Create the operator policies? Yes
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-machine-api-
aws-cloud-credentials'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-cloud-
```

```
credential-operator-cloud-crede'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-image-registry-installer-cloud-creden'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-ingress-operator-cloud-credentials'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credent'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-cloud-network-config-controller-cloud'
I: To create a cluster with these roles, run the following command:
rosa create cluster --sts
```

## 4.3. クラスター固有の OPERATOR IAM ロール参照

このセクションでは、STS を使用する Red Hat OpenShift Service on AWS (ROSA) デプロイメントに必要な Operator IAM ロールの詳細を提供します。クラスター Operator は、Operator のロールを使用して、バックエンドストレージ、クラウドプロバイダーの資格情報、クラスターへの外部アクセスの管理など、クラスター操作を実行するために必要な一時的なアクセス許可を取得します。

Operator ロールを作成する場合、一致するクラスターバージョンの Operator ポリシーはロールに割り当てられます。Operator ポリシーは、互換性のある Operator およびバージョンにタグ付けされます。Operator ロールの適切なポリシーは、タグを使用して決定されます。

**注記**

Operator ロールのアカウントで複数のマッチングポリシーが利用可能な場合は、Operator の作成時にオプションのインタラクティブな一覧が提供されます。

**表4.12 ROSA クラスター固有の Operator ロール**

| リソース | 説明 |
|---|---|
| **<cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credentials** | Container Storage Interface (CSI) でバックエンドストレージを管理するのに ROSA で必要な IAM ロール。 |
| **<cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials** | コアクラスター機能を実行するのに ROSA Machine Config Operator で必要な IAM ロール。 |
| **<cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-credentials** | クラウドプロバイダーの認証情報を管理するために ROSA Cloud Credential Operator で必要な IAM ロール。 |
| **<cluster_name>-<hash>-openshift-cloud-network-config-controller-credentials** | クラスターのクラウドネットワーク設定を管理するために、クラウドネットワーク設定コントローラーで必要な IAM ロール。 |
| **<cluster_name>-<hash>-openshift-image-registry-installer-cloud-credentials** | クラスターの AWS S3 で内部レジストリーストレージを管理するのに ROSA Image Registry Operator で必要な IAM ロール。 |

| リソース | 説明 |
| --- | --- |
| **<cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials** | クラスターへの外部アクセスを管理するのに ROSA Ingress Operator で必要な IAM ロール。 |

### 4.3.1. Operator IAM ロール AWS CLI リファレンス

このセクションでは、**manual** モードを使用して以下の **rosa** コマンドを実行する際にターミナルに表示される **aws** CLI コマンドを一覧表示します。

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

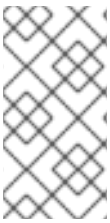
**注記**

**manual** モードを使用すると、**aws** コマンドは確認用に端末に出力されます。**aws** コマンドを確認したら、手動で実行する必要があります。または、**rosa create** コマンドで **--mode auto** を指定して、**aws** コマンドを即時に実行することができます。

**コマンド出力**

```
aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credent \
 --assume-role-policy-document file://operator_cluster_csi_drivers_ebs_cloud_credentials_policy.json
\
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-cluster-csi-drivers
Key=operator_name,Value=ebs-cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credent \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-cluster-csi-drivers-
ebs-cloud-credent

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials \
 --assume-role-policy-document file://operator_machine_api_aws_cloud_credentials_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-machine-api
Key=operator_name,Value=aws-cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-machine-api-aws-
cloud-credentials

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-crede \
 --assume-role-policy-document
file://operator_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-cloud-credential-operator
```

```
Key=operator_name,Value=cloud-credential-operator-iam-ro-creds

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-crede \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-cloud-credential-operator-cloud-crede

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-image-registry-installer-cloud-creden \
 --assume-role-policy-document file://operator_image_registry_installer_cloud_credentials_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-image-registry Key=operator_name,Value=installer-cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-image-registry-installer-cloud-creden \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-image-registry-installer-cloud-creden

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials \
 --assume-role-policy-document file://operator_ingress_operator_cloud_credentials_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=4.8 Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-ingress-operator Key=operator_name,Value=cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-ingress-operator-cloud-credentials
```



**注記**

テーブルで提供されているコマンドの例には、**ManagedOpenShift** 接頭辞を使用する Operator ロールが含まれます。Operator ポリシーを含む、アカウント全体のロールおよびポリシーの作成時にカスタム接頭辞を定義する場合は、Operator ロールの作成時に **--prefix <prefix_name>** オプションを使用してこれを参照する必要があります。

### 4.3.2. カスタム Operator IAM ロールの接頭辞について

AWS Security Token Service (STS) を使用する各 Red Hat OpenShift Service on AWS (ROSA) クラスターには、クラスター固有の Operator IAM ロールが必要です。

デフォルトでは、Operator ロール名の前にクラスター名とランダムな 4 桁のハッシュが付けられます。たとえば、**mycluster** という名前のクラスターの Cloud Credential OperatorIAM ロールのデフォルト名は **mycluster-<hash>-openshift-cloud-credential-operator-cloud-credentials** です。ここで、**<hash>** はランダムな 4 桁の文字列です。

このデフォルトの命名規則により、AWS アカウントのクラスターの Operator IAM ロールを簡単に識別できます。

クラスターの Operator ロールを作成する場合、オプションで、**<cluster_name>-<hash>** の代わりに使用するカスタム接頭辞を指定できます。カスタム接頭辞を使用すると、環境の要件を満たすために、Operator ロール名の前に論理識別子を追加できます。たとえば、クラスター名と環境タイプ

(**mycluster-dev** など) の接頭辞を付けることができます。この例では、カスタム接頭辞が付いた CloudCredentialOperator のロール名は **mycluster-dev-openshift-cloud-credential-operator-cloud-credenti** です。

**注記**

ロール名は 64 文字に切り捨てられます。

**関連情報**

- カスタム接頭辞を使用してクラスター固有の Operator IAM ロールを作成する手順は、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 または CLI を使用してカスタマイズしたクラスターを作成する 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。

## 4.4. OPERATOR 認証用の OIDC プロバイダー要件

STS を使用する ROSA インストールの場合は、認証を行うためにクラスター Operator によって使用されるクラスター固有の OIDC プロバイダーを作成する必要があります。

### 4.4.1. OIDC プロバイダー AWS CLI リファレンス

このセクションでは、**manual** モードを使用して以下の **rosa** コマンドを実行する際にターミナルに表示される **aws** CLI コマンドを一覧表示します。

```
$ rosa create oidc-provider --mode manual --cluster <cluster_name>
```

**注記**

**manual** モードを使用すると、**aws** コマンドはレビュー用に端末に出力されます。**aws** コマンドを確認したら、手動で実行する必要があります。または、**rosa create** コマンドで **--mode auto** を指定して、**aws** コマンドを即時に実行することができます。

**コマンド出力**

```
aws iam create-open-id-connect-provider \
 --url https://rh-oidc.s3.<aws_region>.amazonaws.com/<cluster_id> \
 --client-id-list openshift sts.amazonaws.com \
 --thumbprint-list <thumbprint> 1
```

1 サムプリントは、**rosa create oidc-provider** コマンドの実行時に自動的に生成されます。AWS Identity and Access Management (IAM) OpenID Connect (OIDC) アイデンティティープロバイダーでサムプリントを使用する方法は、AWS ドキュメント を参照してください。

# 第5章 RED HAT OPENSHIFT SERVICE ON AWS のサポート

Red Hat OpenShift Service on AWS (ROSA) のサポート

## 5.1. サポート

本書で説明されている手順で問題が発生した場合は、Red Hat カスタマーポータル にアクセスしてください。カスタマーポータルから、以下を行うことができます。

- Red Hat 製品に関する技術サポート記事の Red Hat ナレッジベースの検索またはブラウズ。
- 他の製品ドキュメントへのアクセス。
- Red Hat サポートに対するサポートケースの送信。
    a. **ケースを作成します** をクリックします。
    b. **Defect/Bug** または **Account/Customer Service Request** など、ケース作成の理由を選択します。
    c. **Product** フィールドに **OpenShift** と入力し、リストを絞り込みます。ドロップダウンメニューから **Red Hat OpenShift Service on AWS** およびバージョンを選択します。
    d. 残りのフィールドを完了させます。
    e. **Review** ページで、サポートへの問い合わせの対象である正しいクラスター ID を選択し、**Submit** をクリックします。

有効な AWS サポート契約がある限り、AWS サポート のサポートを受けることもできます。

本書の改善への提案がある場合、またはエラーを見つけた場合は、最も関連性の高いドキュメントコンポーネントの Jira Issue を送信してください。セクション名や Red Hat OpenShift Service on AWS のバージョンなど、具体的な情報を提供してください。