# Red Hat OpenShift Service on AWS 4

## ROSA について

Red Hat OpenShift Service on AWS アーキテクチャーの概要

Last Updated: 2025-11-28

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

Red Hat OpenShift Service on AWS アーキテクチャーの概要

## Legal Notice



## Abstract

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。

# Table of Contents

# 第1章 RED HAT OPENSHIFT SERVICE ON AWS 4 ドキュメント

Red Hat OpenShift Service on AWS の公式ドキュメントへようこそ。ここでは、Red Hat OpenShift Service on AWS について学び、その機能を確認できます。

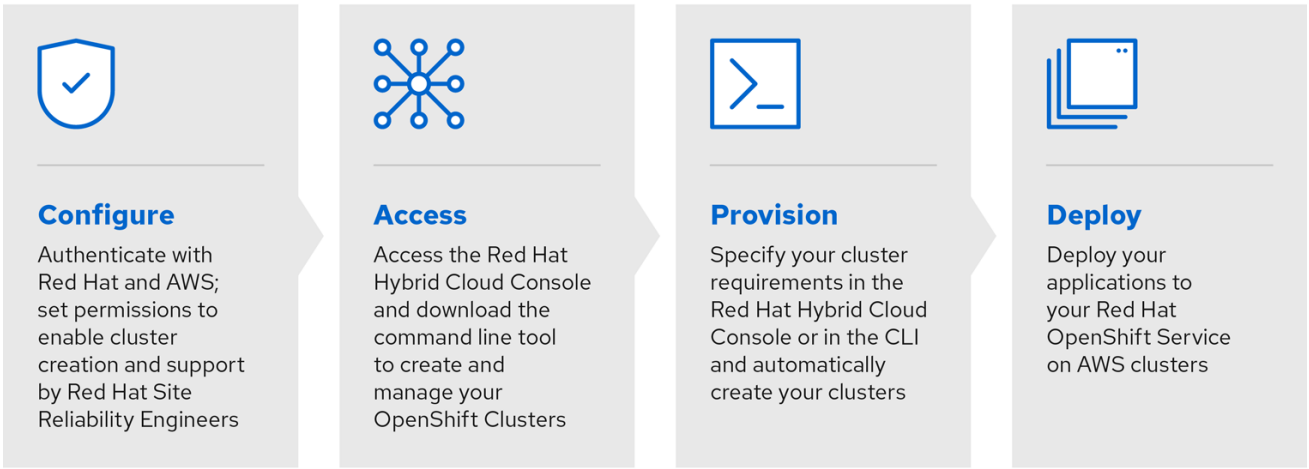
# 第2章 RED HAT OPENSHIFT SERVICE ON AWS の概要

Red Hat OpenShift Service on AWS 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す。これを利用すると、アプリケーションを構築およびデプロイして顧客に価値を提供するという、最も重要なことに集中できます。Red Hat と AWS の SRE 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、お客様がインフラストラクチャーの管理について心配する必要はありません。Red Hat OpenShift Service on AWS は、AWS のコンピュート、データベース、分析、機械学習、ネットワーク、モバイル、AI、その他の幅広い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。

Red Hat OpenShift Service on AWS は、効率性とセキュリティーを重視したマネージド Red Hat OpenShift Service on AWS クラスターを作成するための低コストのソリューションを提供します。新しいクラスターをすばやく作成し、数分でアプリケーションをデプロイできます。

AWS アカウントから直接サービスをサブスクライブします。クラスターを作成した後、OpenShift Web コンソール、**rosa** CLI、または Red Hat OpenShift Cluster Manager を使用してクラスターを操作できます。

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。Red Hat OpenShift Service on AWS は、バージョンの整合性を確保するために、Red Hat OpenShift Container Platform と同じバージョンの OpenShift をサポートしています。




Red Hat OpenShift Service on AWS は、AWS アカウントのインフラストラクチャー管理用の認証情報を取得するために、AWS IAM と AWS Security Token Service (STS) を使用します。AWS STS は、IAM ユーザー/ロールまたはフェデレーションされたユーザー/ロールの一時的な認証情報を作成するグローバル Web サービスです。Red Hat OpenShift Service on AWS はこれを使用して、特権が限られた短期間のセキュリティー認証情報を割り当てます。これらの認証情報は、AWS API 呼び出しを行う各コンポーネントに固有の IAM ロールに関連付けられます。この方法は、クラウドサービスのリソース管理における最小権限とセキュアなプラクティスの原則に沿ったものです。ROSA コマンドラインインターフェイス (CLI) ツールは、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。より詳細な説明は、AWS STS と Red Hat OpenShift Service on AWS の説明 を参照してください。

## 2.1. RED HAT OPENSHIFT SERVICE ON AWS の主な機能

- **クラスターノードのスケーリング:** Red Hat OpenShift Service on AWS は、最小限の 2 つのノードしか必要としないため、小規模なプロジェクトに最適でありながら、大規模なプロジェ

クトやエンタープライズをサポートするために拡張することもできます。リソースの需要に合わせてコンピュートノードを簡単に追加または削除できます。自動スケーリングを使用すると、現在のワークロードに基づいてクラスターのサイズを自動的に調整できます。詳細は、クラスター上のノードの自動スケーリングについて を参照してください。

- **フルマネージドの基盤となるコントロールプレーンインフラストラクチャー:** API サーバーや etcd データベースなどのコントロールプレーンコンポーネントは、Red Hat が所有する AWS アカウントでホストされます。
- **短いプロビジョニング時間:** プロビジョニング時間は約 10 分です。
- **アップグレード中の継続的なクラスター操作:** お客様はコントロールプレーンとマシンプールを個別にアップグレードできるため、アップグレードプロセス中にクラスターを確実に稼働し続けることができます。
- **ネイティブ AWS サービス:** AWS マネジメントコンソールから、セルフサービスのオンボーディングにより、オンデマンドで Red Hat OpenShift にアクセスし、使用できます。
- **柔軟な従量制の価格設定:** ビジネスニーズに合わせたスケールアップが可能で、柔軟な価格設定と時間単位または年単位のオンデマンド請求モデルに基づく従量課金制が導入されています。
- **Red Hat OpenShift と AWS の使用に対する一括請求書:** お客様は、Red Hat OpenShift と AWS の両方の使用に対して、AWS から単一の請求書を受け取ります。
- **完全に統合されたサポートエクスペリエンス:** 管理、メンテナンス、アップグレードは、Red Hat と Amazon の共同サポートと 99.95% のサービスレベルアグリーメント (SLA) に基づき、Red Hat Site Reliability Engineer (SRE) によって実行されます。詳細は、Red Hat OpenShift Service on AWS のサポートドキュメント を参照してください。
- **AWS サービスの統合:** AWS には、コンピュート、ストレージ、ネットワーク、データベース、分析、仮想化、AI などの強力なクラウドサービス群があります。これらのサービスはすべて、Red Hat OpenShift Service on AWS を通じて直接アクセスできます。これにより、使い慣れた管理インターフェイスを通じて、グローバルかつオンデマンドでの構築、運用、拡張が容易になります。
- **可用性の最大化:** サポート対象リージョン内の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て可用性を最大化し、最も要求の厳しいミッションクリティカルなアプリケーションとデータの高可用性を維持します。
- **最適化されたクラスター:** お客様のニーズに合わせて、EC2 インスタンスタイプ (メモリー最適化、コンピューティング最適化、汎用、高速コンピューティング) をクラスターのために選択できます。
- **世界中で利用可能:** Red Hat OpenShift Service on AWS が利用可能な世界の各地域を確認するには、製品の地域別提供状況ページ を参照してください。

## 2.2. 課金と課金設定

Red Hat OpenShift Service on AWS は Amazon Web Services (AWS) アカウントに直接請求されます。ROSA の価格は消費量に基づいており、年間契約または 3 年間の契約で割引率が高くなります。ROSA の総コストは、次の 2 つの要素で構成されます。

- ROSA サービス料
- AWS インフラストラクチャー料金

詳細は、AWS ウェブサイトの Red Hat OpenShift Service on AWS の料金 ページをご覧ください。

## 2.3. RED HAT OPENSHIFT SERVICE ON AWS の使用を開始する

次のセクションで、Red Hat OpenShift Service on AWS の学習と使用に役立つコンテンツを探してください。

### 2.3.1. アーキテクト

| Red Hat OpenShift Service on AWS について | Red Hat OpenShift Service on AWS のデプロイの計画 | 関連情報 |
|---|---|---|
| アーキテクチャーの概要 | バックアップと復元 | Red Hat OpenShift Service on AWS のライフサイクル |
| Red Hat OpenShift Service on AWS アーキテクチャー | プロセスとセキュリティーについて<br><br>Red Hat OpenShift Service on AWS のサービス定義<br><br>ライフサイクルの更新 | |
| サポートの利用 | | |

### 2.3.2. クラスター管理者

| Red Hat OpenShift Service on AWS について | Red Hat OpenShift Service on AWS のデプロイ | Red Hat OpenShift Service on AWS の管理 | 関連情報 |
|---|---|---|---|
| Red Hat OpenShift Service on AWS アーキテクチャー | Red Hat OpenShift Service on AWS のインストール | ロギング | サポートの利用 |
| OpenShift インタラクティブラーニングポータル | ストレージ | Red Hat OpenShift Service on AWS モニタリングについて<br><br>Red Hat OpenShift Service on AWS のライフサイクル<br><br>Red Hat OpenShift Service on AWS の責任に関する表 | バックアップと復元 |
| IAM リソースについて | Red Hat OpenShift Service on AWS roadmap | 提供状況について | アップグレード |

### 2.3.3. 開発者

| Red Hat OpenShift Service on AWS でのアプリケーション開発について | アプリケーションのデプロイ | 関連情報 |
|---|---|---|
| Red Hat Developers のサイト | アプリケーションのビルドの概要 | サポートの利用 |
| Red Hat OpenShift Dev Spaces (旧 Red Hat CodeReady Workspaces) | Operators の概要 | Red Hat OpenShift Service on AWS ロードマップ |
| | イメージ | |
| | 開発者向け CLI | |

### 2.3.4. 初めて Red Hat OpenShift Service on AWS クラスターを作成する前に

ROSA のインストールに関する追加情報について、Red Hat OpenShift Service on AWS のインストールのインタラクティブな説明 でプロセスの簡単な紹介を参照してください。

## 2.4. 関連情報

- Red Hat OpenShift Service on AWS 製品ページ
- AWS 製品ページ
- Red Hat カスタマーポータル
- OpenShift を理解する

# 第3章 AWS STS と ROSA WITH HCP の説明

Red Hat OpenShift Service on AWS は、AWS Identity Access Management (IAM) 用の AWS (Amazon Web Services) Security Token Service (STS) を使用して、AWS アカウント内のリソースとやり取りするのに必要な認証情報を取得します。

## 3.1. AWS STS 認証方法

ROSA with HCP の一環として、AWS アカウント内のインフラストラクチャーリソースを管理するのに必要な権限を Red Hat に付与する必要があります。ROSA with HCP の IAM STS ポリシーは、クラスターの自動化ソフトウェアに、AWS アカウント内のリソースへの限定的な短期アクセスを許可します。

STS 方式では、事前定義されたロールとポリシーを使用して、IAM ロールに一時的な最小限の権限を付与します。通常、認証情報は要求されてから 1 時間後に期限切れになります。有効期限が切れると、認証情報は AWS によって認識されなくなり、その認証情報を使用して API 要求を実行するためにアカウントにアクセスできなくなります。詳細は、AWS のドキュメント を参照してください。

AWS IAM の STS ロールは、ROSA クラスターごとに作成する必要があります。ROSA コマンドラインインターフェイス (CLI) (**rosa**) は、STS ロールを管理し、ROSA 固有の AWS 管理ポリシーを各ロールにアタッチするのに役立ちます。CLI には、ロールを作成し、AWS 管理ポリシーをアタッチするためのコマンドとファイル、および CLI が自動的にロールを作成してポリシーをアタッチできるようにするオプションが用意されています。または、ROSA CLI では、ロールを準備し、ROSA 固有の AWS 管理ポリシーをアタッチするためのコンテンツを利用することもできます。

## 3.2. AWS STS セキュリティー

AWS STS のセキュリティー機能には以下が含まれます。

- ユーザーが事前に作成する明示的かつ限定的なポリシーセット。
    - ユーザーは、プラットフォームに必要なすべての要求された権限を確認できます。
- サービスは、これらの権限以外の操作を一切行うことができません。
- 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。サービスは、操作を実行する必要が生じるたびに、1 時間以内に期限切れになる認証情報を取得します。
- 認証情報の有効期限により、認証情報の漏洩や再利用のリスクが軽減されます。
- ROSA 固有の AWS 管理ポリシーは、AWS API の制限内で、アカウント内の ROSA 固有の AWS リソースに対するアクションのみを許可するように厳密にスコープ指定されています。

ROSA のポリシーは、分離された特定の IAM ロールに対する短期的なセキュリティー認証情報を使用して、クラスターのソフトウェアコンポーネントに最小限の権限を付与します。認証情報は、AWS の API 呼び出しを実行する各コンポーネントおよびクラスターに固有の IAM ロールに関連付けられます。この方法は、クラウドサービスのリソース管理における最小権限とセキュアなプラクティスの原則に沿ったものです。

## 3.3. ROSA WITH HCP のコンポーネント

- **AWS インフラストラクチャー** - Amazon EC2 インスタンス、Amazon EBS ストレージ、ネットワークコンポーネントなど、クラスターに必要なインフラストラクチャー。AWS コンピュートタイプ を参照して、コンピュートノードでサポートされているインスタンスタイプを確認して

ください。クラウドリソース設定の詳細は、プロビジョニングされる AWS インフラストラクチャー を参照してください。

- **AWS STS** - 短期間の動的トークンを付与して、ユーザーに AWS アカウントのリソースを一時的に操作するために必要な権限を付与する方法。
- **OpenID Connect (OIDC)** - クラスター Operator が AWS で認証し、信頼ポリシーを通じてクラスターのロールを引き受け、必要な API 呼び出しを実行するために STS から一時的な認証情報を取得するためのメカニズム。
- **ロールとポリシー** - ROSA with HCP で使用するロールとポリシーは、アカウント全体のロールとポリシーと、Operator のロールとポリシーに分けられる。
  ポリシーは、各ロールに対して許可されるアクションを決定します。個々のロールとポリシーの詳細は、IAM リソースについて を参照してください。クラスターでこれらのリソースを準備する方法の詳細は、必要な IAM ロールとリソース を参照してください。
  - 次のアカウント全体のロールが必要です。
    - **<prefix>-HCP-ROSA-Worker-Role**
    - **<prefix>-HCP-ROSA-Support-Role**
    - **<prefix>-HCP-ROSA-Installer-Role**
  - 次のアカウント全体の AWS 管理ポリシーが必要です。
    - ROSAInstallerPolicy
    - ROSAWorkerInstancePolicy
    - ROSASRESupportPolicy
    - ROSAIngressOperatorPolicy
    - ROSAAmazonEBSCSIDriverOperatorPolicy
    - ROSACloudNetworkConfigOperatorPolicy
    - ROSAControlPlaneOperatorPolicy
    - ROSAImageRegistryOperatorPolicy
    - ROSAKMSProviderPolicy
    - ROSAKubeControllerPolicy
    - ROSAManageSubscription
    - ROSANodePoolManagementPolicy

**注記**

以下にリストされている特定のポリシーは、クラスター Operator ロールによって使用されます。Operator ロールは既存のクラスター名に依存しており、アカウント全体のロールと同時に作成できないため、2 番目のステップで作成されます。

- Operator のロールは次のとおりです。
  - <operator_role_prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
  - <operator_role_prefix>-openshift-cloud-network-config-controller-cloud-credentials
  - <operator_role_prefix>-openshift-machine-api-aws-cloud-credentials
  - <operator_role_prefix>-openshift-cloud-credential-operator-cloud-credentials
  - <operator_role_prefix>-openshift-image-registry-installer-cloud-credentials
  - <operator_role_prefix>-openshift-ingress-operator-cloud-credentials
- 信頼ポリシーは、アカウント全体のロールと Operator のロールごとに作成されます。

## 3.4. ROSA WITH HCP クラスターのデプロイ

ROSA with HCP クラスターのデプロイは、次の一般的な手順に従って行われます。

1. お客様がアカウント全体のロールを作成します。
2. お客様が Operator ロールを作成します。
3. Red Hat が AWS IAM STS を使用して、必要な権限を AWS に送信します。これにより、AWS は対応する AWS 管理の Operator ポリシーを作成してアタッチすることが可能になります。
4. お客様が OIDC プロバイダーを作成します。
5. お客様がクラスターを作成します。

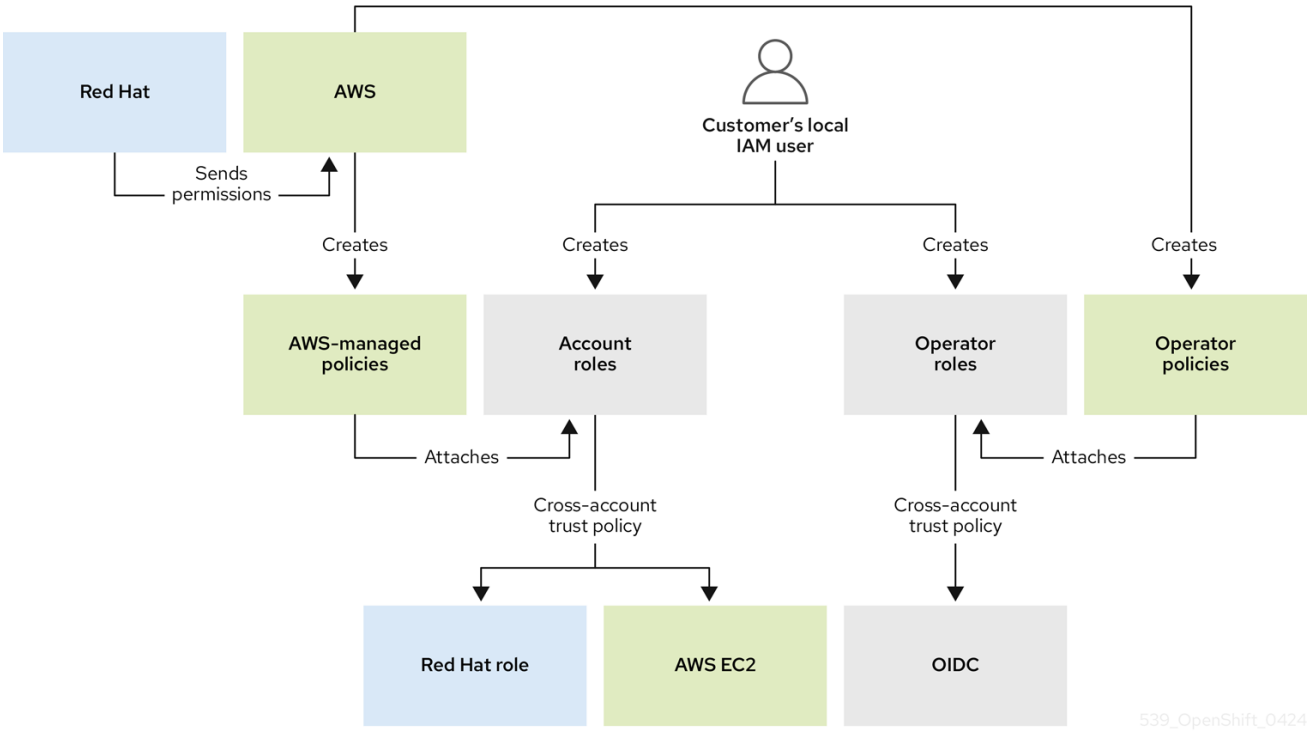
クラスターの作成プロセス中に、ROSA CLI は必要な JSON ファイルを作成し、必要なコマンドを出力します。必要に応じて、ROSA CLI でコマンドを実行することもできます。

ROSA CLI は自動的にロールを作成することも、**--mode manual** または **--mode auto** フラグを使用して手動で作成することもできます。デプロイメントの詳細は、カスタマイズによるクラスターの作成 を参照してください。

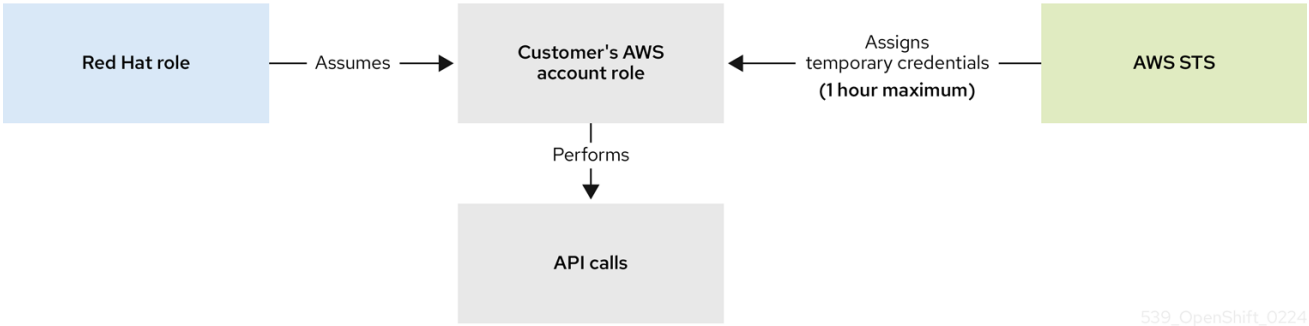
## 3.5. ROSA WITH HCP ワークフロー

ユーザーは、必要なアカウント全体のロールを作成します。ロールの作成時に、クロスアカウント信頼ポリシーという信頼ポリシーが作成されます。このポリシーは、Red Hat 所有のロールがこのロールを引き受けることを許可するものです。また、EC2 サービス用の信頼ポリシーも作成されます。このポリシーは、EC2 インスタンス上のワークロードがロールを引き受けて認証情報を取得することを許可するものです。AWS は各ロールに対応するアクセス許可ポリシーを割り当てます。

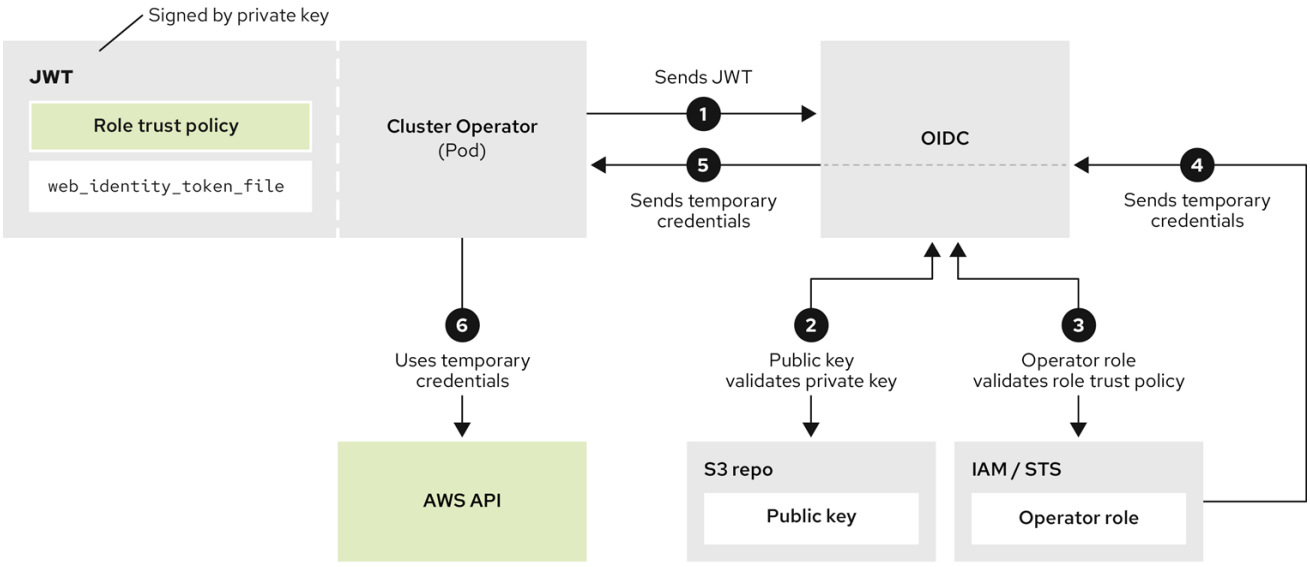
アカウント全体の Operator ロールとポリシーの両方を作成した後、ユーザーはクラスターを作成できます。この Operator ロールを、以前に作成された対応する権限ポリシーと、OIDC プロバイダーの信頼ポリシーに割り当てます。Operator ロールは、AWS リソースへのアクセスが必要なクラスター内の Pod を最終的に表すという点で、アカウント全体のロールとは異なります。ユーザーは IAM ロールを Pod に割り当てることができないため、Operator (ひいては Pod) が必要なロールにアクセスできるように、OIDC プロバイダーを使用して信頼ポリシーを作成する必要があります。




新しいロールが必要な場合は、現在 Red Hat のロールを使用しているワークロードが AWS アカウントのロールを引き受け、AWS STS から一時的な認証情報を取得し、引き受けたロールの権限ポリシーに従ってユーザーの AWS アカウント内の API 呼び出しを使用してアクションの実行を開始します。認証情報は一時的なもので、有効期間は最大 1 時間です。




Operator は、次のプロセスを使用して、タスクを実行するために必要な認証情報を取得します。各 Operator には、Operator のロール、権限ポリシー、および OIDC プロバイダーの信頼ポリシーが割り当てられます。Operator は、ロールとトークンファイル (**web_identity_token_file**) を含む JSON Web トークンを OIDC プロバイダーに渡してロールを引き受けます。OIDC プロバイダーは署名された鍵を公開鍵で認証します。公開鍵はクラスターの作成時に作成され、S3 バケットに保存されます。次に、Operator は、署名されたトークンファイル内のサブジェクトがロール信頼ポリシー内のロールと一致することを確認します。このロールは、OIDC プロバイダーが許可されたロールのみを取得できるようにするためのものです。その後、OIDC プロバイダーが一時的な認証情報を Operator に返し、Operator が AWS API 呼び出しを実行できるようにします。視覚的な説明は、次の図を参照してください。


Signed by private key
JWT
Role trust policy
web_identity_token_file
Cluster Operator
(Pod)
Sends JWT
1
5
Sends temporary
credentials
OIDC
4
Sends temporary
credentials
6
Uses temporary
credentials
2
Public key
validates private key
3
Operator role
validates role trust policy
AWS API
S3 repo
Public key
IAM / STS
Operator role
629_OpenShift_0424

# 第4章 アーキテクチャーモデル

Red Hat OpenShift Service on AWS には、次のクラスタートポロジーがあります。

Hosted Control Plane (HCP) - コントロールプレーンは Red Hat アカウントでホストされ、ワーカーノードは顧客の AWS アカウントにデプロイされます。

## 4.1. RED HAT OPENSHIFT SERVICE ON AWS と RED HAT OPENSHIFT SERVICE ON AWS (クラシックアーキテクチャー) の比較

**表4.1 Red Hat OpenShift Service on AWS と Red Hat OpenShift Service on AWS (クラシックアーキテクチャー) のアーキテクチャー比較表**

| | Hosted Control Plane (HCP) | Classic |
|---|---|---|
| **コントロールプレーンホスティング** | API サーバー etcd データベースなどのコントロールプレーンコンポーネントは、Red Hat が所有する AWS アカウントでホストされます。 | API サーバー etcd データベースなどのコントロールプレーンコンポーネントは、お客様が所有する AWS アカウントでホストされます。 |
| **Virtual Private Cloud (VPC)** | ワーカーノードは、AWS PrivateLink を介してコントロールプレーンと通信します。 | ワーカーノードおよびコントロールプレーンノードは、お客様の VPC にデプロイされます。 |
| **マルチゾーンデプロイメント** | コントロールプレーンは常に複数のアベイラビリティーゾーン (AZ) にデプロイされます。 | コントロールプレーンは、単一の AZ 内または複数の AZ にわたってデプロイできます。 |
| **マシンプール** | 各マシンプールは単一の AZ (プライベートサブネット) にデプロイされます。 | マシンプールは、単一の AZ または複数の AZ にデプロイできます。 |
| **インフラストラクチャーノード** | Ingress やイメージレジストリーなどのプラットフォームコンポーネントをホストするために専用のインフラストラクチャーノードは使用しません。 | プラットフォームコンポーネントをホストするために、2 つ (シングル AZ) または 3 つ (マルチ AZ) の専用インフラストラクチャーノードを使用します。 |
| **OpenShift ケーパビリティー** | プラットフォームモニタリング、イメージレジストリー、および Ingress コントローラーは、ワーカーノードにデプロイされます。 | プラットフォームモニタリング、イメージレジストリー、および Ingress コントローラーは、専用のインフラストラクチャーノードにデプロイされます。 |
| **クラスターのアップグレード** | コントロールプレーンと各マシンプールは個別にアップグレードできます。 | クラスター全体を同時にアップグレードする必要があります。 |
| **最小 EC2 フットプリント** | クラスターの作成には 2 つの EC2 インスタンスが必要です。 | クラスターを作成するには、7 個 (single-AZ) または 9 個 (multi-AZ) の EC2 インスタンスが必要です。 |

**関連情報**

- リージョンおよびアベイラビリティーゾーン

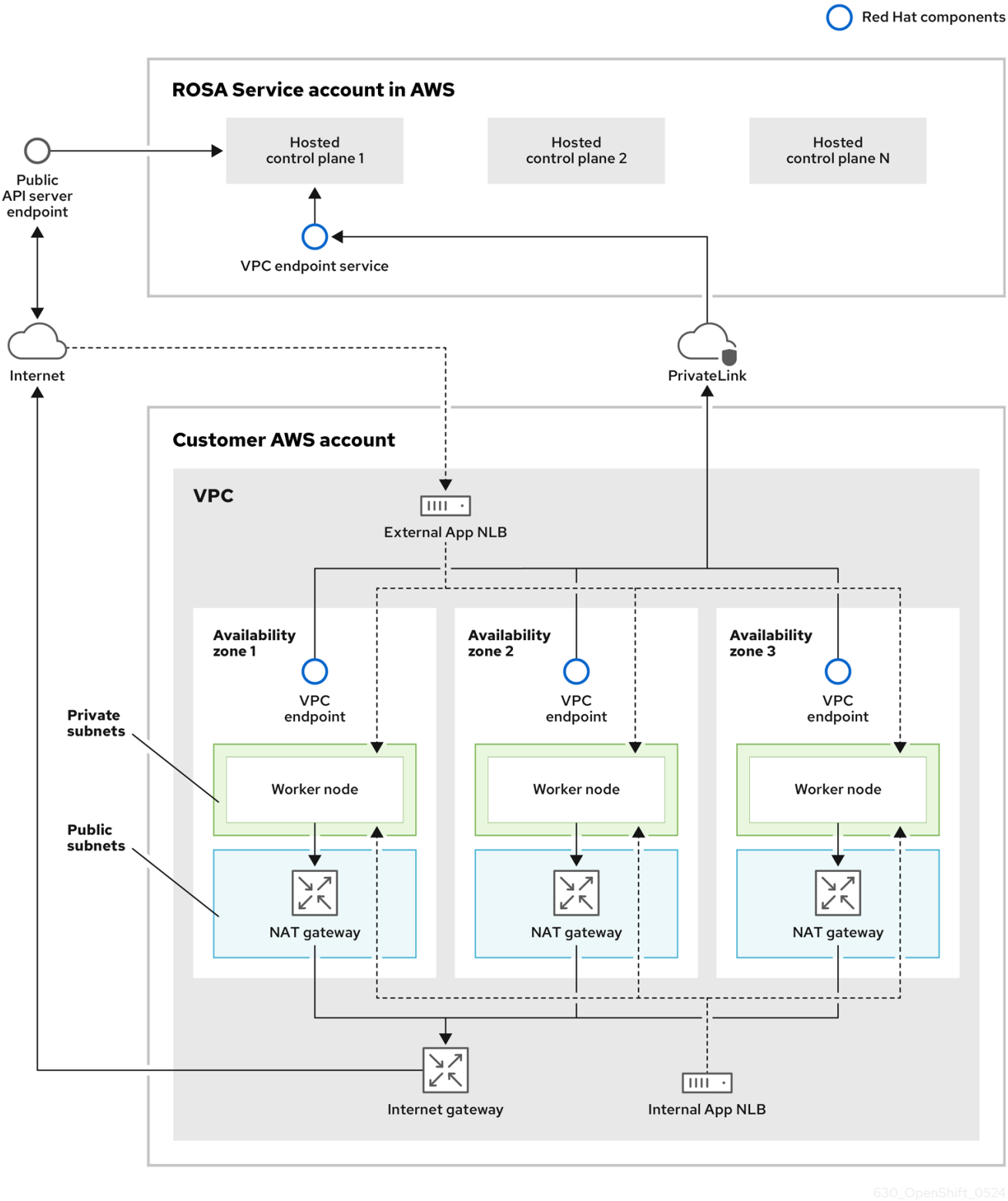
## 4.2. RED HAT OPENSHIFT SERVICE ON AWS WITH HCP のアーキテクチャー

Red Hat OpenShift Service on AWS は、高可用性を備えたシングルテナントの OpenShift コントロールプレーンをホストします。Hosted Control Plane は、2 つの API サーバーインスタンスと 3 つの etcd インスタンスを含む 3 つのアベイラビリティーゾーンにデプロイされます。

Red Hat OpenShift Service on AWS クラスターは、インターネットに公開された API サーバーを設置するかどうかを選択して作成できます。設置しない場合は "プライベート" クラスター、設置する場合は "パブリック" クラスターと見なされます。プライベート API サーバーには、VPC サブネットからのみアクセスできます。Hosted Control Plane には、API の公開設定にかかわらず、AWS PrivateLink エンドポイントを介してアクセスします。

ワーカーノードは AWS アカウントにデプロイされ、VPC プライベートサブネット上で実行されます。高可用性を確保するために、1 つ以上のアベイラビリティーゾーンから追加のプライベートサブネットを追加できます。ワーカーノードは、OpenShift コンポーネントとアプリケーションによって共有されます。Ingress コントローラー、イメージレジストリー、モニタリングなどの OpenShift コンポーネントは、VPC でホストされているワーカーノードにデプロイされます。

図4.1 Red Hat OpenShift Service on AWS アーキテクチャー




## 4.2.1. パブリックおよびプライベートネットワーク上の Red Hat OpenShift Service on AWS アーキテクチャー

Red Hat OpenShift Service on AWS を使用すると、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上にクラスターを作成できます。以下の図は、パブリックネットワークとプライベートネットワークの両方のアーキテクチャーを示しています。

図4.2 パブリックネットワーク上にデプロイされた Red Hat OpenShift Service on AWS

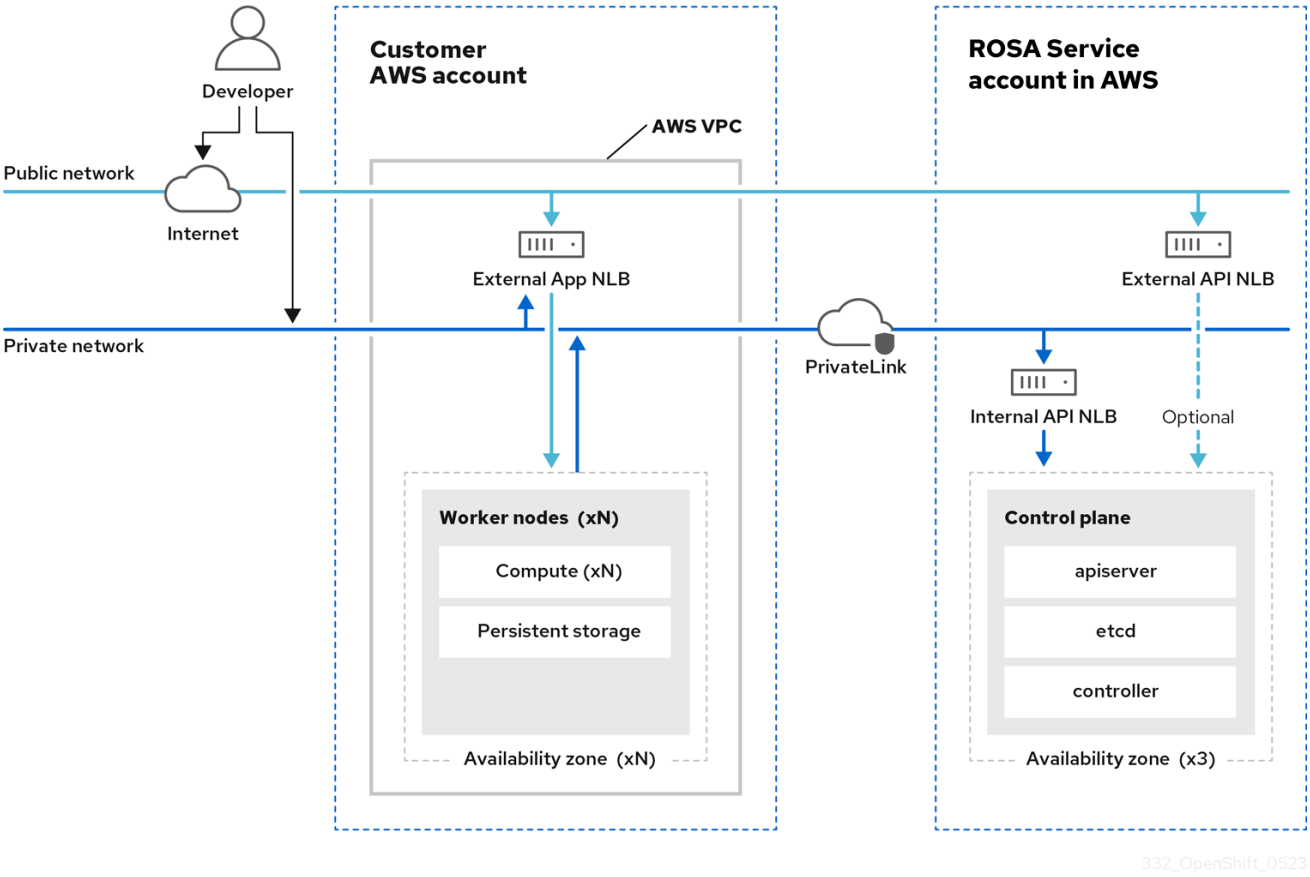
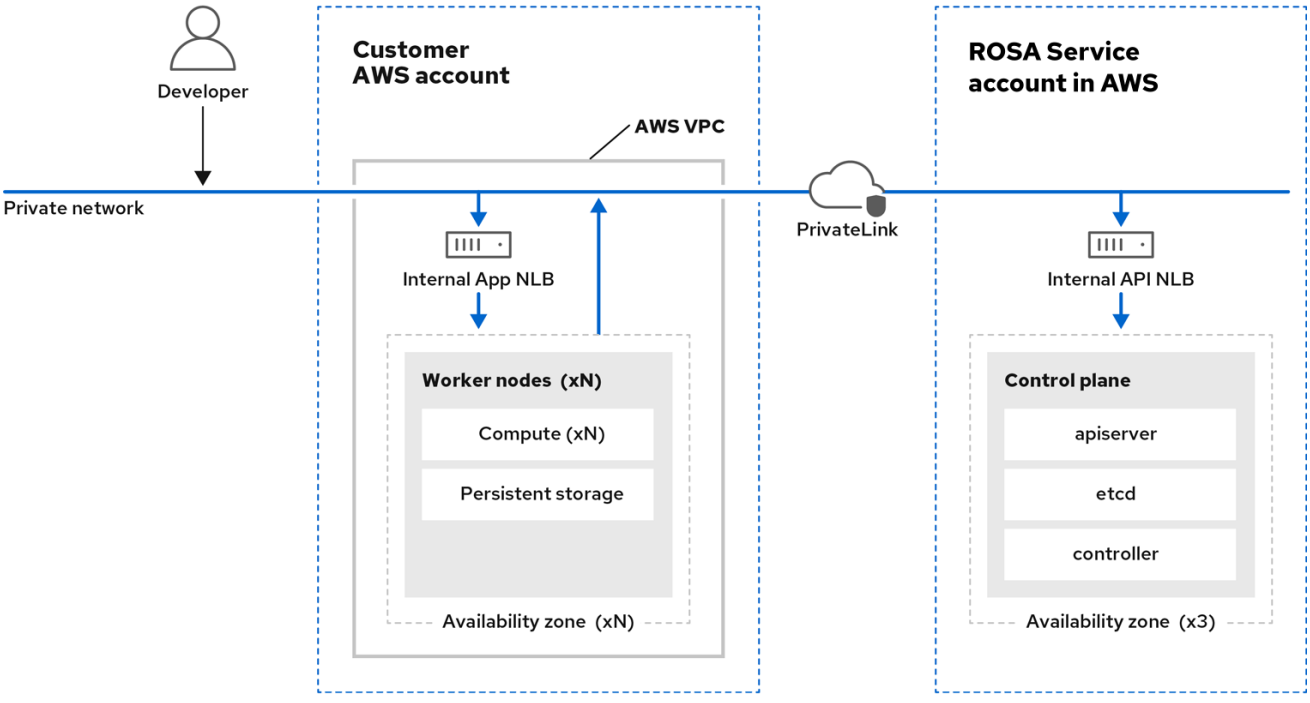



図4.3 プライベートネットワーク上にデプロイされた Red Hat OpenShift Service on AWS



# 第5章 ポリシーおよびサービス定義

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

可用性と障害回避は、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 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。

### 5.1.1. 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 の Site Reliability Engineering (SRE) によるサポートと、マシンプールを複数のアベイラビリティーゾーンにデプロイする方法を備えているため、多くの一般的な Kubernetes の問題に対する保護をさらに強化するのに役立ちます。しかし、それでもコンテナーやインフラストラクチャーに障害が発生する可能性のある状況はいくつかあります。潜在的な障害点を理解することで、リスクを理解し、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。

**重要**

ワーカーノードは永続性が保証されておらず、OpenShift の通常の運用および管理の一環として、いつでも置き換えられる可能性があります。ノードのライフサイクルの詳細は、**関連情報** を参照してください。

**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。

#### 5.1.1.1. コンテナーまたは Pod の障害

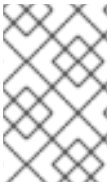
設計上、Pod は短期間存在することが意図されています。アプリケーション Pod の複数のインスタンスが実行されている場合は、個別の Pod またはコンテナーの問題から保護できるようにサービスを適切にスケーリングします。OpenShift ノードスケジューラーは、回復性をさらに強化するために、これらのワークロードが異なるワーカーノードに分散するようにします。

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、メンテナンスのためのノードの drain (Pod の退避) 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。

#### 5.1.1.2. 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 を含む仮想マシン (VM) です。デフォルトでは、ROSA クラスターにはクラスターごとに少なくとも 2 つのワーカーノードがあります。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、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は、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。

#### 5.1.1.3. 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。ゾーン障害から保護するために、ROSA は 3 つのアベイラビリティーゾーンにまたがってマシンプールをデプロイするオプションを提供しています。十分な容量がある限り、既存のステートレスワークロードが、障害発生時に影響を受けていないゾーンに再配布されます。

#### 5.1.1.4. 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。

**関連情報**

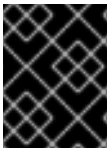
- ノードのライフサイクル

## 5.2. RED HAT OPENSHIFT SERVICE ON AWS におけるロールの概要

以下では、Red Hat OpenShift Service on AWS マネージドサービスにおける Red Hat、Amazon Web Services (AWS)、およびお客様のそれぞれの責任を説明します。

### 5.2.1. Red Hat OpenShift Service on AWS の責任共有

Red Hat と Amazon Web Services (AWS) が Red Hat OpenShift Service on AWS のサービスを管理している間、お客様には一定の責任があります。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を参照してください。

| 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 | アクセスとアイデンティティーの承認 | 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 |
| Logging | Red Hat | Red Hat とお客様 | Red Hat とお客様 | Red Hat とお客様 | Red Hat |
| アプリケーションのネットワーク | Red Hat とお客様 | Red Hat とお客様 | Red Hat とお客様 | Red Hat | Red Hat |
| クラスターネットワーク | Red Hat [1] | Red Hat とお客様 [2] | Red Hat とお客様 | Red Hat [1] | Red Hat [1] |
| 仮想ネットワーク管理 | Red Hat とお客様 | Red Hat とお客様 | Red Hat とお客様 | Red Hat とお客様 | Red Hat とお客様 |
| 仮想コンピューティング管理 (コントロールプレーン、インフラストラクチャー、およびワーカーノード) | Red Hat | Red Hat | Red Hat | Red Hat | Red Hat |

| 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 | アクセスとアイデンティティーの承認 | セキュリティーおよび規制コンプライアンス | 障害復旧 |
|---|---|---|---|---|---|
| クラスターのバージョン | Red Hat | Red Hat とお客様 | Red Hat | Red Hat | Red Hat |
| 容量の管理 | Red Hat | Red Hat とお客様 | Red Hat | Red Hat | Red Hat |
| 仮想ストレージ管理 | Red Hat | Red Hat | Red Hat | Red Hat | Red Hat |
| AWS ソフトウェア (パブリック AWS サービス) | AWS | AWS | AWS | AWS | AWS |
| ハードウェア/AWS グローバルインフラストラクチャー | AWS | AWS | AWS | AWS | AWS |

1. お客様が独自の CNI プラグインを使用することを選択した場合、お客様に責任が移ります。
2. クラスターをプロビジョニングする前に、お客様はファイアウォールを設定して、必要な OpenShift および AWS ドメインとポートへのアクセスを許可する必要があります。詳細は、「AWS ファイアウォールの前提条件」を参照してください。

### 5.2.2. 領域ごとの責任共有のタスク

**関連情報**

Red Hat、AWS、および顧客はすべて、Red Hat OpenShift Service on AWS (ROSA) クラスターの監視、メンテナンス、および全体的な健全性に対して責任を共有します。このドキュメントでは、以下の表に示すように、リストされた各リソースの責任の概要を説明します。

### 5.2.3. クラスター通知の確認とアクション

クラスター通知 (サービスログと呼ばれることもあります) は、クラスターのステータス、健全性、またはパフォーマンスに関するメッセージです。

クラスター通知は、Red Hat Site Reliability Engineering (SRE) が管理対象クラスターの健全性をユーザーに通知する際に使用する主な方法です。Red Hat SRE は、クラスター通知を使用して、クラスターの問題を解決または防止するためのアクションを実行するように促すこともあります。

クラスターの所有者と管理者は、クラスターの健全性とサポート対象の状態を維持するために、クラスター通知を定期的に確認して対処する必要があります。

クラスターの通知は、Red Hat Hybrid Cloud Console のクラスターの **Cluster history** タブで表示できます。デフォルトでは、クラスターの所有者のみがクラスター通知をメールで受信します。他のユーザーがクラスター通知メールを受信する必要がある場合は、各ユーザーをクラスターの通知連絡先として追加します。

#### 5.2.3.1. クラスター通知ポリシー

クラスター通知は、クラスターの健全性とクラスターに大きな影響を与えるイベントに関する情報を常に提供できるように設計されています。

ほとんどのクラスター通知は、クラスターの問題や状態の重要な変更をすぐに通知するために、自動的に生成されて送信されます。

状況によっては、Red Hat Site Reliability Engineering (SRE) がクラスター通知を作成して送信し、複雑な問題に関する追加のコンテキストとガイダンスを提供します。

影響の少ないイベント、リスクの低いセキュリティー更新、日常的な運用とメンテナンス、または Red Hat SRE によってすぐに解決される軽微で一時的な問題は、クラスター通知が送信されません。

次の場合、Red Hat サービスが自動的に通知を送信します。

- リモートヘルスモニタリングまたは環境検証チェックにより、ワーカーノードのディスク領域不足など、クラスター内の問題が検出された場合。
- 重要なクラスターライフサイクルイベントが発生した場合。たとえば、スケジュールされたメンテナンスまたはアップグレードの開始時や、クラスター操作がイベントの影響を受けたが、お客様による介入は必要ない場合などです。
- クラスター管理に大きな変更が発生した場合。たとえば、クラスターの所有権または管理制御が 1 人のユーザーから別のユーザーに移行された場合などです。
- クラスターのサブスクリプションが変更または更新された場合。たとえば、Red Hat がサブスクリプションの条件やクラスターで利用可能な機能を更新した場合などです。

SRE は次の場合に通知を作成して送信します。

- インシデントにより、クラスターの可用性やパフォーマンスに影響を与えるデグレードや停止が発生した場合。たとえば、クラウドプロバイダーで地域的な停止が発生した場合などです。SRE は、インシデント解決の進行状況とインシデントが解決した時期を知らせる後続の通知を送信します。
- クラスターで、セキュリティー脆弱性、セキュリティー侵害、または異常なアクティビティーが検出された場合。
- お客様が行った変更によってクラスターが不安定になっているか、不安定になる可能性があることを Red Hat が検出した場合。
- ワークロードがクラスターのパフォーマンス低下や不安定化を引き起こしていることを Red Hat が検出した場合。

### 5.2.4. インシデントおよびオペレーション管理

Red Hat は、デフォルトのプラットフォームネットワーキングに必要なサービスコンポーネントを監督する責任があります。AWS は、AWS クラウドで提供されるすべてのサービスを実行するハードウェアインフラストラクチャーを保護する責任があります。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カスタムネットワークに関するインシデントおよび操作の管理を行います。

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| アプリケーションのネットワーク | **Red Hat**<br>● 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。 | ● 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>● 停止を Red Hat と AWS に報告します。 |
| クラスターネットワーク | **Red Hat**<br>● クラスター DNS、クラスターコンポーネント間のネットワークプラグイン接続、およびデフォルトの Ingress Controller に関連するインシデントを監視、警告、および対処します。 | ● オプションの Ingress コントローラー、ソフトウェアカタログを通じてインストールされた追加の Operator、およびデフォルトの OpenShift CNI プラグインを置き換えるネットワークプラグインに関連するインシデントを監視および対処します。 |
| 仮想ネットワーク管理 | **Red Hat**<br>● AWS ロードバランサー、Amazon VPC サブネット、デフォルトのプラットフォームネットワーキングに必要な AWS サービスコンポーネントを監視します。アラートに応答します。 | ● AWS ロードバランサーエンドポイントの健全性を監視します。<br>● Amazon VPC 間接続、AWS VPN 接続、または AWS Direct Connect を通じてオプションで設定されたネットワークトラフィックを監視し、潜在的な問題やセキュリティー上の脅威がないか確認します。 |
| 仮想ストレージ管理 | **Red Hat**<br>● クラスターノードに使用される Amazon EBS ボリュームと、ROSA サービスの組み込みコンテナーイメージレジストリーにアタッチされる Amazon S3 バケットを監視します。アラートに応答します。 | ● アプリケーションデータの健全性を監視します。<br>● 顧客管理の AWS KMS キーを使用する場合は、Amazon EBS 暗号化のキーのライフサイクルとキーのポリシーを作成して制御します。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| プラットフォームモニタリング | **Red Hat**<br>● すべての ROSA クラスターコンポーネント、サイトリライアビリティーエンジニア (SRE) サービス、および基盤となる AWS アカウントに対する集中監視およびアラートシステムを保守します。 | |
| インシデント管理 | **Red Hat**<br>● 既知のインシデントを提起して管理します。<br>● 根本原因分析 (RCA) の下書きを顧客と共有します。 | ● サポートケースを使用して、既知のインシデントを報告します。 |
| インフラストラクチャーとデータの回復力 | **Red Hat**<br>● STS を使用する ROSA クラスターで利用できる Red Hat 提供のバックアップ方法はありません。<br>● Red Hat は、RTO (Recovery Point Objective) または RTO (Recovery Time Objective) にコミットしません。 | ● データを定期的にバックアップし、Kubernetes のベストプラクティスに従ったワークロードを備えたマルチ 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します。<br>● クラウドリージョン全体が利用できない場合は、別のリージョンに新しいクラスターをインストールし、バックアップデータを使用してアプリを復元します。 |
| クラスター容量 | **Red Hat**<br>● クラスター上のすべてのコントロールプレーンとインフラストラクチャーノードの容量を管理します。<br>● アップグレード中およびクラスターのアラートへの対応時にクラスターの容量を評価します。 | |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| AWS ソフトウェア (パブリック AWS サービス) | **AWS**<br>● AWS インシデントと運用管理の詳細は、AWS ホワイトペーパーの AWS が運用上の回復力とサービスの継続性を維持する方法 を参照してください。 | ● 顧客アカウントの AWS リソースの健全性を監視します。<br>● IAM ツールを使用して、顧客アカウントの AWS リソースに適切なアクセス許可を適用します。 |
| ハードウェア/AWS グローバルインフラストラクチャー | **AWS**<br>● AWS インシデントと運用管理の詳細は、AWS ホワイトペーパーの How AWS maintains operational resilience and continuity of service を参照してください。 | ● 顧客のアプリケーションとデータを設定、管理、監視して、アプリケーションとデータのセキュリティー制御が適切に実施されていることを確認します。 |

#### 5.2.4.1. プラットフォームモニタリング

プラットフォームの監査ログは、一元的なセキュリティー情報およびイベント監視 (SIEM) システムにセキュアに転送されます。このシステムで、Red Hat SRE チームへの設定済みアラートがログによって起動されるほか、手動でのログのレビューも行われます。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。

#### 5.2.4.2. 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リングおよびアラートシステムから直接提出されるか、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関するアラートが送られ、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、復旧に関するすべての連絡と調整を管理します。
4. インシデントが解決されると、お客様が起票したサポートチケットにインシデントと解決策の簡単な概要が提供されます。この概要は、お客様がインシデントとその解決策を詳しく理解するのに役立ちます。

サポートチケットで提供される情報に加えて、さらに詳しい情報が必要な場合、お客様は次のワークフローをリクエストできます。

1. お客様は、インシデント解決後 5 営業日以内に追加情報をリクエストする必要があります。
2. Red Hat は、インシデントの重大度に応じて、サポートチケットで根本原因の概要または根本原因分析 (RCA) をお客様に提供する場合もあります。根本原因の概要に関する追加情報は、インシデント解決後 7 営業日以内に提供されます。根本原因分析に関する追加情報は、30 営業日以内に提供されます。

Red Hat は、サポートケースを通じて発生した顧客インシデントにも対応します。Red Hat は、次のような活動 (ただしこれに限定されません) を支援できます。

- 仮想コンピュートの分離を含むフォレンジック収集
- コンピュートイメージコレクションのガイド
- 収集された監査ログの提供

#### 5.2.4.3. クラスター容量

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。このようなアラートにより、通知がお客様に出される可能性があります。

**関連情報**

- クラスターの通知

### 5.2.5. 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を説明します。

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。AWS は、AWS クラウドで提供されるすべてのサービスを実行するハードウェアインフラストラクチャーを保護する責任があります。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、ならびに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。

#### 5.2.5.1. 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、またはそのグループ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、メンテナンスの除外を実装できます。

- 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、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。

#### 5.2.5.2. Red Hat が開始する変更

Red Hat Site Reliability Engineering (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ています。

許可された Red Hat SRE のレビュー担当者が、各ステップへの進行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。

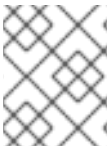
一部の変更は、段階的に実稼働環境にリリースされ、新機能の提供形態 (プライベートプレビューやパブリックプレビューなど) を管理するための機能フラグを使用して、指定のクラスターまたはお客様に提供されます。

#### 5.2.5.3. 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。

#### 5.2.5.4. 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**

必要な権限が 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、AWS 管理ポリシーが自動的に更新されます。

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。

#### 5.2.5.5. リソースに関するサービスおよびお客様の責任

次の表は、クラスターリソースに関する責任を定めたものです。

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| Logging | **Red Hat**<br>● 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>● サイドカーコンテナーのロギングやサードパーティーのロギングアプリケーションなど、任意のアプリロギングソリューションをインストール、設定、および保守します。<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 | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| アプリケーションのネットワーク | **Red Hat**<br>● パブリック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 トラフィック用の OVN-Kubernetes コンポーネントをインストール、設定、および保守します。<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ロー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。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| クラスターネットワーク | **Red Hat**<br>● 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 Amazon VPC 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>● ワーカークラスターとコントロールプレーン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セットアップします。 | ● クラスターをプロビジョニングする前に、必要な OpenShift および AWS ドメインとポートへのアクセスを許可するようにファイアウォールを設定します。詳細は、「AWS ファイアウォールの前提条件」を参照してください。<br>● 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。<br>● 追加のアプリケーションルートを公開するには、追加の Ingress Controller を作成します。<br>● デフォルトの OpenShift CNI プラグインなしでクラスターがインストールされている場合は、オプションの CNI プラグインをインストール、設定、およびアップグレードします。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| 仮想ネットワーク管理 | **Red Hat**<br>● 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、クラスターのプロビジョニングに必要な Amazon VPC コンポーネントをセットアップおよび設定します。<br>● オンプレミスリソースとの AWS VPN 接続、Amazon VPC 間の接続、および必要に応じて OpenShift Cluster Manager を介して AWS Direct Connect を管理できる機能を顧客が提供します。<br>● 顧客がサービスロードバランサーで使用する AWS 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。 | ● Amazon VPC 間接続、AWS VPN 接続、AWS Direct Connect などのオプションの Amazon VPC コンポーネントをセットアップおよび維持します。<br>● 特定サービスの追加のサービスロードバランサーを要求し、設定します。 |
| 仮想コンピューティング管理 | **Red Hat**<br>● クラスターのコンピューティングに Amazon EC2 インスタンスを使用するように ROSA コントロールプレーンとデータプレーンをセットアップおよび設定します。<br>● クラスター上の Amazon EC2 コントロールプレーンとインフラストラクチャーノードのデプロイメントを監視および管理します。 | ● OpenShift Cluster Manager または ROSA CLI (**rosa**) を使用してマシンプールを作成し、Amazon EC2 ワーカーノードを監視および管理します。<br>● 顧客が導入したアプリケーションとアプリケーションデータへの変更を管理します。 |
| クラスターのバージョン | **Red Hat**<br>● 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>● パッチリリースの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。 | ● 自動アップグレードを設定するか、パッチリリースアップグレードを直ちにまたは今後の予定として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>● パッチリリースで顧客のアプリケーションをテストし、互換性を確認します。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| 容量の管理 | **Red Hat**<br>● コントロールプレーンの使用を監視します。<br>● QoS (Quality of Service) を維持するために、コントロールプレーンのスケーリングおよびサイズ変更を行います。 | ● 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。 |
| 仮想ストレージ管理 | **Red Hat**<br>● Amazon EBS をセットアップして設定し、クラスターのローカルノードストレージと永続ボリュームストレージをプロビジョニングします。<br>● Amazon S3 バケットストレージを使用するように組み込みイメージレジストリーをセットアップおよび設定します。[1]<br>● Amazon S3 のイメージレジストリーリソースを定期的にプルーニングして、Amazon S3 の使用率とクラスターのパフォーマンスを最適化します。[2] | ● 必要に応じて、Amazon EBS CSI ドライバーまたは Amazon EFS CSI ドライバーを設定して、クラスター上に永続ボリュームをプロビジョニングします。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| AWS ソフトウェア (パブリック AWS サービス) | **AWS**<br><br>**コンピュート:** Amazon EC2 サービスを提供します。これは ROSA 関連リソースに使用されます。<br><br>**ストレージ:** Amazon EBS を提供します。これは、クラスターのローカルノードストレージと永続ボリュームストレージをプロビジョニングするために、ROSA によって使用されます。<br><br>**ストレージ:** Amazon S3 を提供します。これは ROSA の組み込みイメージレジストリーに使用されます。<br><br>**ネットワーク:** 次の AWS クラウドサービスを提供します。これらは、仮想ネットワークインフラストラクチャーのニーズを満たすために、ROSA によって使用されます。<br><br>● Amazon VPC<br>● Elastic Load Balancing<br>● AWS IAM<br>● AWS STS<br><br>**ネットワーク:** 次の AWS サービスを提供します。お客様はこれらのサービスを必要に応じて ROSA と統合できます。<br><br>● AWS VPN<br>● AWS Direct Connect<br>● AWS PrivateLink<br>● AWS Transit Gateway | ● IAM プリンシパルまたは STS 一時セキュリティー認証情報に関連付けられたアクセスキー ID とシークレットアクセスキーを使用して、リクエストに署名します。<br><br>● クラスターの作成時に使用するクラスターの VPC サブネットを指定します。<br><br>● オプションで、ROSA クラスターで使用するために顧客管理の VPC を設定します (PrivateLink クラスターと HCP クラスターに必要)。 |
| ハードウェア/AWS グローバルインフラストラクチャー | **AWS**<br><br>● AWS データセンターの管理コントロールの詳細は、AWS クラウドセキュリティーページの Our Controls を参照してください。<br><br>● 変更管理のベストプラクティスは、AWS ソリューションライブラリーの AWS での変更管理のガイダンス を参照してください。 | ● AWS Cloud でホストされている顧客のアプリケーションとデータに対して変更管理のベストプラクティスを実装します。 |

1. AWS STS の認証フローの詳細は、AWS STS の認証フロー を参照してください。
2. イメージのプルーニングの詳細は、イメージの自動プルーニング を参照してください。

**関連情報**

- Red Hat OpenShift Service on AWS のファイアウォールの前提条件

### 5.2.6. セキュリティーおよび規制コンプライアンス

次の表は、セキュリティーと規制遵守に関する責任の概要を示しています。

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| Logging | **Red Hat**<br>● セキュリティーイベントを分析するために、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。<br>● 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。 |
| 仮想ネットワーク管理 | **Red Hat**<br>● 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>● 追加の監視と保護には、パブリック AWS ツールを使用します。 | ● 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。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| 仮想ストレージ管理 | **Red Hat**<br>● 潜在的な問題やセキュリティー上の脅威がないか、仮想ストレージコンポーネントを監視します。<br>● 追加の監視と保護には、パブリック AWS ツールを使用します。<br>● Amazon EBS が提供する AWS 管理の Key Management Service (KMS) キーを使用して、デフォルトでコントロールプレーン、インフラストラクチャー、およびワーカーノードのボリュームデータを暗号化するように ROSA サービスを設定します。<br>● Amazon EBS が提供する AWS 管理の KMS キーを使用して、デフォルトのストレージクラスを使用する顧客の永続ボリュームを暗号化するように ROSA サービスを設定します。<br>● 顧客管理の AWS KMS キーを使用して永続ボリュームを暗号化できる機能を顧客が提供します。<br>● Amazon S3 管理キー (SSE-3) によるサーバー側の暗号化を使用して、定時時のイメージレジストリーデータを暗号化するようにコンテナーイメージレジストリーを設定します。<br>● 顧客がパブリックまたはプライベートの Amazon S3 イメージレジストリーを作成して、コンテナーイメージを不正なユーザーアクセスから保護できる機能を提供します。 | ● Amazon EBS ボリュームをプロビジョニングします。<br>● Amazon EBS ボリュームストレージを管理して、ROSA にボリュームとしてマウントできる十分なストレージを確保します。<br>● 永続ボリューム要求を作成し、OpenShift Cluster Manager を通じて永続ボリュームを生成します。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| 仮想コンピューティング管理 | **Red Hat**<br>● 仮想コンピューティングコンポーネントを監視して、潜在的な問題やセキュリティー上の脅威がないか確認します。<br>● 追加の監視と保護には、パブリック AWS ツールを使用します。 | ● 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。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| AWS ソフトウェア (パブリック AWS サービス) | **AWS**<br><br>**コンピュート:** セキュアな Amazon EC2。ROSA のコントロールプレーンとワーカーノードに使用されます。詳細は、Amazon EC2 ユーザーガイドの Amazon EC2 のインフラストラクチャーセキュリティー を参照してください。<br><br>**ストレージ:** セキュアな Amazon Elastic Block Store (EBS)。ROSA のコントロールプレーンとワーカーノードボリューム、および Kubernetes 永続ボリュームに使用されます。詳細は、Amazon EC2 ユーザーガイドの Amazon EC2 でのデータ保護 を参照してください。<br><br>**ストレージ:** AWS KMS を提供します。コントロールプレーン、ワーカーノードボリューム、および永続ボリュームを暗号化するために、ROSA によって使用されます。詳細は、Amazon EC2 ユーザーガイドの Amazon EBS 暗号化 を参照してください。<br><br>**Storage:** セキュアな Amazon S3。ROSA サービスの組み込みコンテナーイメージレジストリーに使用されます。詳細は、S3 ユーザーガイドの Amazon S3 セキュリティー を参照してください。<br><br>**Networking:** Amazon VPC に組み込まれたネットワークファイアウォール、プライベートまたは専用ネットワーク接続、AWS のセキュアな施設間の AWS グローバルおよび地域ネットワーク上のすべてのトラフィックの自動暗号化など、プライバシーを強化し、AWS グローバルインフラストラクチャー上のネットワークアクセスを制御するためのセキュリティー機能とサービスを提供します。詳細は、AWS セキュリティーの概要ホワイトペーパーの AWS Shared Responsibility Model と Infrastructure security を参照してください。 | • Amazon EC2 インスタンス上のデータを保護するために、セキュリティーのベストプラクティスと最小権限の原則に従っていることを確認します。詳細は、Infrastructure security in Amazon EC2 および Data protection in Amazon EC2 を参照してください。<br><br>• 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><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。<br><br>• オプションの顧客管理の KMS キーを作成し、KMS キーを使用して Amazon EBS 永続ボリュームを暗号化します。<br><br>• 仮想ストレージ内の顧客データを監視して、潜在的な問題やセキュリティー上の脅威がないか確認します。詳細は、責任共有モデル を参照してください。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| ハードウェア/AWS グローバルインフラストラクチャー | **AWS**<br>● ROSA がサービス機能を提供するために使用する AWS グローバルインフラストラクチャーを提供します。AWS のセキュリティー管理の詳細は、AWS ホワイトペーパーの AWS インフラストラクチャーのセキュリティー を参照してください。<br>● 顧客がコンプライアンスのニーズを管理し、AWS Artifact や AWS Security Hub などのツールを使用して AWS のセキュリティー状態を確認するためのドキュメントを提供します。詳細は、ROSA ユーザーガイドの ROSA のコンプライアンス検証 を参照してください。 | ● 顧客のアプリケーションとデータを設定、管理、監視して、アプリケーションとデータのセキュリティー制御が適切に実施されていることを確認します。<br>● IAM ツールを使用して、顧客アカウントの AWS リソースに適切なアクセス許可を適用します。 |

### 5.2.7. 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。

Red Hat OpenShift Service on AWS (ROSA) は、Pod レベル、ノードレベル、アベイラビリティーゾーンレベルで発生する障害に対する障害復旧を提供します。

どの障害復旧でも、必要な可用性のレベルを満たすには、可用性の高いアプリケーション、ストレージ、クラスターアーキテクチャー (複数のアベイラビリティーゾーンにまたがる複数のマシンプールなど) をデプロイするためのベストプラクティスをお客様が使用する必要があります。

単一のクラスターに単一のマシンプールしかない場合、アベイラビリティーゾーンまたはリージョンの障害が発生した際に、障害の回避や復旧を行うことはできません。複数のクラスターに単一のマシンプールがあり、お客様がフェイルオーバーを管理している場合は、ゾーンまたはリージョンレベルでの障害に対処できます。

単一のクラスターでは、複数のマシンプールが複数のアベイラビリティーゾーンにあっても、リージョン全体の障害が発生した際に、障害の回避や復旧を行うことはできません。複数のクラスターが複数のリージョンにあり、複数のマシンプールが複数のアベイラビリティーゾーンにあり、さらにお客様がフェイルオーバーを管理している場合は、リージョンレベルの障害に対処できます。

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| 仮想ネットワーク管理 | **Red Hat**<br>● 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。 |
| 仮想ストレージ管理 | **Red Hat** | ● 顧客の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を作成します。 |
| 仮想コンピューティング管理 | **Red Hat** - 障害が発生したワーカーノードをお客様が手動または自動で交換できるようにします。 | ● OpenShift Cluster Manager または ROSA CLI を通じてマシンプール設定を編集して、障害が発生した Amazon EC2 ワーカーノードを置き換えます。 |
| AWS ソフトウェア (パブリック AWS サービス) | **AWS**<br><br>**Compute:** Amazon EBS スナップショットや Amazon EC2 Auto Scaling などのデータ復元力をサポートする Amazon EC2 機能を提供します。詳細は、EC2 ユーザーガイドの Amazon EC2 の復元力 を参照してください。<br><br>**Storage:** ROSA サービスと顧客が、Amazon EBS ボリュームのスナップショットを通じてクラスター上の Amazon EBS ボリュームをバックアップできる機能を提供します。<br><br>**Storage:** データの復元力をサポートする Amazon S3 の機能は、Resilience in Amazon S3 を参照してください。<br><br>**Networking:** データ復元力をサポートする Amazon VPC 機能の詳細は、Amazon VPC ユーザーガイドの Resilience in Amazon Virtual Private Cloud を参照してください。 | ● フォールトトレランスとクラスターの可用性を向上させるために、複数のアベイラビリティーゾーンにわたる複数のマシンプールを使用して ROSA クラスターを設定します。<br>● Amazon EBS CSI ドライバーを使用して永続ボリュームをプロビジョニングし、ボリュームスナップショットを有効にします。<br>● Amazon EBS 永続ボリュームの CSI ボリュームスナップショットを作成します。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| ハードウェア/AWS グローバルインフラストラクチャー | **AWS**<br>● ROSA がアベイラビリティーゾーン全体でノードをスケーリングできるようにする AWS グローバルインフラストラクチャーを提供します。この機能により、ROSA は中断することなくゾーン間の自動フェイルオーバーを調整できるようになります。<br>● 災害復旧のベストプラクティスの詳細は、AWS Well-Architected フレームワークの Disaster recovery options in the cloud を参照してください。 | ● フォールトトレランスとクラスターの可用性を向上させるために、複数のアベイラビリティーゾーンにわたる複数のマシンプールを使用して ROSA クラスターを設定します。 |

**関連情報**

- マシンプールについて

### 5.2.8. データおよびアプリケーションに関する追加のお客様の責任

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 と AWS は、お客様がプラットフォーム上のデータとアプリケーションを管理できるようにするさまざまなツールを提供しています。

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

| リソース | Red Hat と AWS | お客様の責任 |
| --- | --- | --- |
| お客様データ | **Red Hat**<br>● 業界のセキュリティーおよびコンプライアンス標準で定義されている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>● Amazon RDS などのデータサービスとの統合を有効にして、クラスターや AWS の外部にデータを保存および管理します。<br>**AWS**<br>● Amazon RDS を提供すると、顧客はクラスターや AWS の外部でデータを保存および管理できるようになります。 | ● プラットフォームに保存されるすべてのお客様データと、お客様のアプリケーションがこのデータを使用し、公開する方法に関する責任を持ちます。 |

| リソース | Red Hat と AWS | お客様の責任 |
| --- | --- | --- |
| お客様のアプリケーション | **Red Hat**<br>● 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セキュアに保存し、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。<br>**AWS**<br>● 顧客のアプリケーションで使用する永続ボリュームをサポートする Amazon EBS を提供します。<br>● コンテナーイメージレジストリーの Red Hat プロビジョニングをサポートするために Amazon S3 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>● Red Hat OpenShift Service on AWS で実行するアプリケーションを監視する責任を持ちます。これには、メトリクスの収集、アラートの作成、アプリケーション内のシークレットの保護を行うソフトウェアのインストールと操作が含まれます。 |

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

このドキュメントでは、Red Hat OpenShift Service on AWS マネージドサービスのサービス定義の概要を説明します。

### 5.3.1. 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。

#### 5.3.1.1. 課金と課金設定

Red Hat OpenShift Service on AWS は Amazon Web Services (AWS) アカウントに直接請求されます。ROSA の価格は消費量に基づいており、年間契約または 3 年間の契約で割引率が高くなります。ROSA の総コストは、次の 2 つの要素で構成されます。

- ROSA サービス料
- AWS インフラストラクチャー料金

詳細は、AWS ウェブサイトの Red Hat OpenShift Service on AWS の料金 ページをご覧ください。

#### 5.3.1.2. 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

これらのセルフサービスタスクは、Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) を使用して実行できます。

**関連情報**

- Red Hat Operator のサポート

#### 5.3.1.3. インスタンスタイプ

ROSA with HCP クラスターにはすべて、少なくとも 2 つのワーカーノードが必要です。クラウドプロバイダーコンソールを使用して基盤となる (EC2 インスタンス) インフラストラクチャーをシャットダウンすることは、サポート対象外の操作であり、データの損失やその他のリスクにつながる可能性があります。

**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。

監査ログの集約、メトリクスの収集、DNS、イメージレジストリー、CNI/OVN-Kubernetes などの OpenShift/ROSA コアシステムは、クラスターの安定性と保守性を維持するために、追加の割り当て可能なリソースを消費す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。

**関連情報**

- Red Hat OpenShift Service on AWS インスタンスタイプ

#### 5.3.1.4. リージョンおよびアベイラビリティーゾーン

現在、ROSA with HCP では、次の AWS リージョンが利用可能です。

**注記**

中国のリージョンは、OpenShift Container Platform でのサポートの有無にかかわらず、サポートされていません。

**注記**

GovCloud (US) リージョンの場合は、Access request for Red Hat OpenShift Service on AWS (ROSA) FedRAMP を送信する必要があります。

**表5.1 AWS リージョン**

| リージョン | ロケーション | 最小要件 ROSA バージョン | AWS オプトインが必要 |
|---|---|---|---|
| us-east-1 | N.Virginia | 4.14 | いいえ |
| us-east-2 | Ohio | 4.14 | いいえ |
| us-west-2 | Oregon | 4.14 | いいえ |
| af-south-1 | Cape Town | 4.14 | はい |
| ap-east-1 | Hong Kong | 4.14 | はい |
| ap-south-2 | Hyderabad | 4.14 | はい |
| ap-southeast-3 | Jakarta | 4.14 | はい |

| リージョン | ロケーション | 最小要件 ROSA バージョン | AWS オプトインが必要 |
|---|---|---|---|
| ap-southeast-4 | Melbourne | 4.14 | はい |
| ap-southeast-5 | Malaysia | 4.16.34; 4.17.15 | はい |
| ap-southeast-7 | Thailand | 4.18 | はい |
| ap-south-1 | Mumbai | 4.14 | いいえ |
| ap-northeast-3 | Osaka | 4.14 | いいえ |
| ap-northeast-2 | Seoul | 4.14 | いいえ |
| ap-southeast-1 | Singapore | 4.14 | いいえ |
| ap-southeast-2 | シドニー | 4.14 | いいえ |
| ap-northeast-1 | Tokyo | 4.14 | いいえ |
| ca-central-1 | Central Canada | 4.14 | いいえ |
| eu-central-1 | Frankfurt | 4.14 | いいえ |
| mx-central-1 | Mexico | 4.18 | はい |
| eu-north-1 | Stockholm | 4.14 | いいえ |
| eu-west-1 | Ireland | 4.14 | いいえ |
| eu-west-2 | London | 4.14 | いいえ |
| eu-south-1 | Milan | 4.14 | はい |
| eu-west-3 | Paris | 4.14 | いいえ |
| eu-south-2 | Spain | 4.14 | はい |
| eu-central-2 | Zurich | 4.14 | はい |
| me-south-1 | Bahrain | 4.14 | はい |
| me-central-1 | UAE | 4.14 | はい |
| sa-east-1 | São Paulo | 4.14 | いいえ |

| リージョン | ロケーション | 最小要件 ROSA バージョン | AWS オプトインが必要 |
|---|---|---|---|
| il-central-1 | Tel Aviv | 4.15 | はい |
| ca-west-1 | Calgary | 4.14 | はい |

クラスターは、3 つ以上のアベイラビリティーゾーンを持つ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。

HCP を備えた新しい ROSA クラスターはそれぞれ、単一リージョンの既存の Virtual Private Cloud (VPC) 内にインストールされます。必要に応じて、そのリージョンのアベイラビリティゾーンの合計数までデプロイできます。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 Amazon Elastic Block Storage (Amazon 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、同じ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**

クラスターのデプロイ後にリージョンを変更することはできません。

**関連情報**

- Red Hat OpenShift Service on AWS エンドポイントとクォータ

#### 5.3.1.5. Local Zones

Red Hat OpenShift Service on AWS は AWS Local Zones の使用をサポートしていません。

#### 5.3.1.6. 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。

#### 5.3.1.7. 限定サポートステータス

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。

**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関する質問がある場合、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。

#### 5.3.1.8. 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は、Red Hat 製品サポートのサービスレベルアグリーメント 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。

### 5.3.2. 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。

#### 5.3.2.1. 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。

#### 5.3.2.2. 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)。

### 5.3.3. モニタリング

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

#### 5.3.3.1. 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により、ROSA ユーザーが提供する CPU またはメモリーメトリクスに基づく水平 Pod 自動スケーリングが可能になります。

#### 5.3.3.2. クラスターの通知

クラスター通知 (サービスログと呼ばれることもあります) は、クラスターのステータス、健全性、またはパフォーマンスに関するメッセージです。

クラスター通知は、Red Hat Site Reliability Engineering (SRE) が管理対象クラスターの健全性をユーザーに通知する際に使用する主な方法です。Red Hat SRE は、クラスター通知を使用して、クラスターの問題を解決または防止するためのアクションを実行するように促すこともあります。

クラスターの所有者と管理者は、クラスターの健全性とサポート対象の状態を維持するために、クラスター通知を定期的に確認して対処する必要があります。

クラスターの通知は、Red Hat Hybrid Cloud Console のクラスターの **Cluster history** タブで表示できます。デフォルトでは、クラスターの所有者のみがクラスター通知をメールで受信します。他のユーザーがクラスター通知メールを受信する必要がある場合は、各ユーザーをクラスターの通知連絡先として追加します。

### 5.3.4. ネットワーク

このセクションでは、ROSA ネットワークのサービス定義に関する情報を提供します。

#### 5.3.4.1. アプリケーションのカスタムドメイン

**警告**

Red Hat OpenShift Service on AWS 4.14 以降、Custom Domain Operator は非推奨になりました。ROSA 4.14 以降で Ingress を管理するには、Ingress Operator を使用してください。

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。

#### 5.3.4.2. ドメイン検証証明書

ROSA には、クラスター上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ています。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。

#### 5.3.4.3. ビルド用のカスタム認証局

ROSA は、イメージレジストリーからイメージをプルするときに、ビルドによって信頼されるカスタム認証局を使用することをサポートしています。

#### 5.3.4.4. ロードバランサー

Red Hat OpenShift Service on AWS は、デフォルトの Ingress コントローラーからのみロードバランサーをデプロイします。お客様は、他のすべてのロードバランサーを、セカンダリー Ingress コントローラーやサービスロードバランサー用に、必要に応じてデプロイできます。

#### 5.3.4.5. 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。

#### 5.3.4.6. クラスター egress

**EgressNetworkPolicy** オブジェクトによる Pod の Egress トラフィック制御を使用すると、ROSA with Hosted Control Plane (HCP) の送信トラフィックを防止または制限できます。

#### 5.3.4.7. クラウドネットワーク設定

Red Hat OpenShift Service on AWS では、次のような AWS 管理のテクノロジーを使用してプライベートネットワーク接続を設定できます。

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

**重要**

Red Hat Site Reliability Engineer (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。このような接続の監視はお客様の責任です。

#### 5.3.4.8. DNS 転送

プライベートクラウドネットワーク設定を持つ ROSA クラスターの場合、お客様は、明示的に指定されたドメインの問い合わせ先として、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ます。

#### 5.3.4.9. ネットワークの検証

ROSA クラスターを既存の Virtual Private Cloud (VPC) にデプロイするか、クラスターとって新しいサブネットを持つマシンプールを追加で作成すると、ネットワーク検証チェックが自動的に実行されます。このチェックによりネットワーク設定が検証され、エラーが強調表示されるため、デプロイメント前に設定の問題を解決できます。

ネットワーク検証チェックを手動で実行して、既存のクラスターの設定を検証することもできます。

**関連情報**

- ネットワークの検証

### 5.3.5. 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。

#### 5.3.5.1. 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

ワーカーノードは、保存時に暗号化される Amazon Elastic Block Store (Amazon EBS) ストレージを使用します。

#### 5.3.5.2. 暗号化された保存時の 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。

#### 5.3.5.3. ブロックストレージ (RWO)

永続ボリューム (PV) は、Read-Write-Once の Amazon Elastic Block Store (Amazon EBS) によってサポートされています。

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。

#### 5.3.5.4. 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、Amazon Elastic File Storage Setup for Red Hat OpenShift Service on AWS を参照してください。

### 5.3.6. プラットフォーム

このセクションでは、Red Hat OpenShift Service on AWS プラットフォームのサービス定義について説明します。

#### 5.3.6.1. 自動スケーリング

ROSA with HCP ではノードの自動スケーリングが利用できます。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。

#### 5.3.6.2. 複数のアベイラビリティーゾーン

コントロールプレーンのコンポーネントは、お客様のワーカーノード設定に関係なく、常に複数のアベイラビリティゾーンにデプロイされます。

#### 5.3.6.3. 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 ROSA with HCP 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。

#### 5.3.6.4. ノードのライフサイクル

ワーカーノードは永続性が保証されておらず、OpenShift の通常の運用および管理の一環として、いつでも置き換えられる可能性があります。

次のような状況では、ワーカーノードが置き換えられる可能性があります。

- クラスターをスムーズに運用するために、マシンヘルスチェックがデプロイされており、**NotReady** ステータスのワーカーノードを置き換えるように設定されている場合。
- インスタンスをホストする基盤ハードウェアの修復不可能な障害が AWS で検出された場合、AWS EC2 インスタンスが終了されることがあります。
- アップグレード中、まずアップグレードされたノードが新しく作成され、クラスターに参加します。前述の自動ヘルスチェックによってこの新しいノードがクラスターに正常に統合されると、古いノードがクラスターから削除されます。

Kubernetes ベースのシステムで実行されるすべてのコンテナー化されたワークロードでは、ノードの置き換えに対して耐性を持つようにアプリケーションを設定することがベストプラクティスです。

#### 5.3.6.5. クラスターバックアップポリシー

Red Hat は、オブジェクトレベルのバックアップソリューションを ROSA クラスターに使用することを推奨しています。OpenShift API for Data Protection (OADP) は OpenShift に含まれていますが、デフォルトでは有効になっていません。お客様は、クラスター上で OADP を設定して、オブジェクトレベルのバックアップおよび復元機能を実現できます。

Red Hat はお客様のアプリケーションまたはアプリケーションデータをバックアップしません。お客様はアプリケーションとそのデータに対して単独で責任を負い、独自のバックアップおよび復元機能を導入する必要があります。

**警告**

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と復元はお客様の責任です。お客様の責任の詳細は、「責任共有マトリックス」を参照してください。

#### 5.3.6.6. OpenShift のバージョン

ROSA with HCP はサービスとして実行されます。ライフサイクル終了 (EOL) に達すると、Red Hat の SRE チームが強制的にアップグレードを実行します。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。

#### 5.3.6.7. アップグレード

アップグレードは、ROSA CLI、**rosa**、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。

#### 5.3.6.8. Windows コンテナー

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。代わりに、ROSA クラスター上で稼働する OpenShift Virtualization 上で Windows ベースの仮想マシンを実行することがサポートされています。

#### 5.3.6.9. コンテナーエンジン

ROSA with HCP は、OpenShift 4 上で稼働し、唯一利用可能なコンテナーエンジン (コンテナーランタイムインターフェイス) である CRI-O を使用します。

#### 5.3.6.10. オペレーティングシステム

ROSA with HCP は、OpenShift 4 上で稼働し、すべてのクラスターノードのオペレーティングシステムとして Red Hat CoreOS (RHCOS) を使用します。

#### 5.3.6.11. 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
- OpenShift Virtualization

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

ソフトウェアカタログマーケットプレイスにリストされている Operator はすべて、インストールに使用できる必要があります。これらの Operator はお客様のワークロードと見なされ、Red Hat SRE によって監視または管理されません。Red Hat によって作成された Operator は Red Hat によってサポートされます。

### 5.3.7. 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。

#### 5.3.7.1. 認証プロバイダー

クラスターの認証は、OpenShift Cluster Manager またはクラスター作成プロセスを使用するか、ROSA CLI **rosa** を使用して設定できます。ROSA 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
- htpasswd

#### 5.3.7.2. 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。

#### 5.3.7.3. お客様管理者ユーザー

Red Hat OpenShift Service on AWS は、通常のユーザーに加えて、ROSA with HCP 固有のグループにアクセスを提供します。このグループは **dedicated-admin** と呼ばれます。**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は、

- クラスターで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権を持ちます。
- クラスターのリソースクォータと制限を管理できます。
- **NetworkPolicy** オブジェクトを追加および管理できます。
- 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ます。
- クラスター上の予約された **dedicated-admin** プロジェクトにアクセスできます。これにより、昇格された権限を持つサービスアカウントの作成が可能になり、クラスター上のプロジェクトのデフォルトの制限とクォータを更新できるようになります。
- ソフトウェアカタログから Operator をインストールし、すべての ***.operators.coreos.com** API グループのすべての動詞を実行できます。

#### 5.3.7.4. 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。

#### 5.3.7.5. 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
```

#### 5.3.7.6. 規制コンプライアンス

最新のコンプライアンス情報は、**ROSA のプロセスとセキュリティー** の **コンプライアンス** テーブルを参照してください。

#### 5.3.7.7. 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、ROSA で使用されるすべての公開ロードバランサーに対して、最も一般的なレベル 3 および 4 の攻撃に対する 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、追加の保護を提供するために接続が切断されます。

#### 5.3.7.8. etcd 暗号化

Red Hat OpenShift Service on AWS では、etcd ボリュームの暗号化を含め、コントロールプレーンのストレージが保存時にデフォルトで暗号化されます。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。

お客様は、ビルド時に etcd データベースを暗号化することも、etcd データベースを暗号化するために独自のカスタム AWS KMS キーを提供することもできます。

etcd 暗号化では、次の Kubernetes API サーバーおよび OpenShift API サーバーのリソースが暗号化されます。

- シークレット
- config map
- ルート
- OAuth アクセストークン
- OAuth 認証トークン

### 5.3.8. 関連情報

- Red Hat OpenShift Service on AWS のセキュリティーについて

- Red Hat OpenShift Service on AWS のライフサイクル

## 5.4. RED HAT OPENSHIFT SERVICE ON AWS インスタンスタイプ

ROSA with HCP は、次のワーカーノードのインスタンスタイプおよびサイズを提供します。

**注記**

現在、ROSA with HCP は最大 500 個のワーカーノードをサポートしています。

### 5.4.1. AWS x86 ベースのインスタンスタイプ

**例5.1 一般的用途**

- 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)
- m5.metal (96 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 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します。
- 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)
- m5dn.metal (96 vCPU、384 GiB)
- m5zn.metal (48 vCPU、192 GiB)
- m5d.metal (96† vCPU、384 GiB)
- m5n.metal (96 vCPU、384 GiB)
- m6a.xlarge (4 vCPU、16 GiB)

- m6a.2xlarge (8 vCPU、32 GiB)
- m6a.4xlarge (16 vCPU、64 GiB)
- m6a.8xlarge (32 vCPU、128 GiB)
- m6a.12xlarge (48 vCPU、192 GiB)
- m6a.16xlarge (64 vCPU、256 GiB)
- m6a.24xlarge (96 vCPU、384 GiB)
- m6a.32xlarge (128 vCPU、512 GiB)
- m6a.48xlarge (192 vCPU、768 GiB)
- m6a.metal (192 vCPU、768 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)
- m6i.metal (128 vCPU、512 GiB)
- m6id.xlarge (4 vCPU、16 GiB)
- m6id.2xlarge (8 vCPU、32 GiB)
- m6id.4xlarge (16 vCPU、64 GiB)
- m6id.8xlarge (32 vCPU、128 GiB)
- m6id.12xlarge (48 vCPU、192 GiB)
- m6id.16xlarge (64 vCPU、256 GiB)
- m6id.24xlarge (96 vCPU、384 GiB)
- m6id.32xlarge (128 vCPU、512 GiB)
- m6id.metal (128 vCPU、512 GiB)
- m6idn.xlarge (4 vCPU、16 GiB)
- m6idn.2xlarge (8 vCPU、32 GiB)

- m6idn.4xlarge (16 vCPU、64 GiB)
- m6idn.8xlarge (32 vCPU、128 GiB)
- m6idn.12xlarge (48 vCPU、192 GiB)
- m6idn.16xlarge (64 vCPU、256 GiB)
- m6idn.24xlarge (96 vCPU、384 GiB)
- m6idn.32xlarge (128 vCPU、512 GiB)
- m6in.xlarge (4 vCPU、16 GiB)
- m6in.2xlarge (8 vCPU、32 GiB)
- m6in.4xlarge (16 vCPU、64 GiB)
- m6in.8xlarge (32 vCPU、128 GiB)
- m6in.12xlarge (48 vCPU、192 GiB)
- m6in.16xlarge (64 vCPU、256 GiB)
- m6in.24xlarge (96 vCPU、384 GiB)
- m6in.32xlarge (128 vCPU、512 GiB)
- m7a.xlarge (4 vCPU、16 GiB)
- m7a.2xlarge (8 vCPU、32 GiB)
- m7a.4xlarge (16 vCPU、64 GiB)
- m7a.8xlarge (32 vCPU、128 GiB)
- m7a.12xlarge (48 vCPU、192 GiB)
- m7a.16xlarge (64 vCPU、256 GiB)
- m7a.24xlarge (96 vCPU、384 GiB)
- m7a.32xlarge (128 vCPU、512 GiB)
- m7a.48xlarge (192 vCPU、768 GiB)
- m7a.metal-48xl (192 vCPU、768 GiB)
- m7i-flex.2xlarge (8 vCPU、32 GiB)
- m7i-flex.4xlarge (16 vCPU、64 GiB)
- m7i-flex.8xlarge (32 vCPU、128 GiB)
- m7i-flex.xlarge (4 vCPU、16 GiB)
- m7i.xlarge (4 vCPU、16 GiB)

- m7i.2xlarge (8 vCPU、32 GiB)
- m7i.4xlarge (16 vCPU、64 GiB)
- m7i.8xlarge (32 vCPU、128 GiB)
- m7i.12xlarge (48 vCPU、192 GiB)
- m7i.16xlarge (64 vCPU、256 GiB)
- m7i.24xlarge (96 vCPU、384 GiB)
- m7i.48xlarge (192 vCPU、768 GiB)
- m7i.metal-24xl (96 vCPU、384 GiB)
- m7i.metal-48xl (192 vCPU、768 GiB)

**例5.2 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5.3 メモリー集約型**

- u7i-6tb.112xlarge (448 vCPU、6,144 GiB)
- u7i-8tb.112xlarge (448 vCPU、6,144 GiB)
- u7i-12tb.224xlarge (896 vCPU、12,288 GiB)
- u7in-16tb.224xlarge (896 vCPU、16,384 GiB)
- u7in-24tb.224xlarge (896 vCPU、24,576 GiB)
- u7in-32tb.224xlarge (896 vCPU、32,768 GiB)
- u7inh-32tb.480xlarge (1920 vCPU、32,768 GiB)
- x1.16xlarge (64 vCPU、976 GiB)
- x1.32xlarge (128 vCPU、1,952 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、1,024 GiB)
- x2idn.24xlarge (96 vCPU、1,536 GiB)
- x2idn.32xlarge (128 vCPU、2,048 GiB)
- x2iedn.xlarge (4 vCPU、128 GiB)
- x2iedn.2xlarge (8 vCPU、256 GiB)
- x2iedn.4xlarge (16 vCPU、512 GiB)
- x2iedn.8xlarge (32 vCPU、1,024 GiB)
- x2iedn.16xlarge (64 vCPU、2,048 GiB)
- x2iedn.24xlarge (96 vCPU、3,072 GiB)
- x2iedn.32xlarge (128 vCPU、4,096 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)
- x2iezn.metal (48 vCPU、1,536 GiB)
- x2idn.metal (128vCPU、2,048 GiB)
- x2iedn.metal (128vCPU、4,096 GiB)

**例5.4 最適化されたメモリー**

- 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.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)
- r5.metal (96 vCPU、768 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します。
- 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)
- r5b.xlarge (4 vCPU、32 GiB)
- r5b.2xlarge (8 vCPU、364 GiB)
- r5b.4xlarge (16 vCPU、3,128 GiB)
- r5b.8xlarge (32 vCPU、3,256 GiB)
- r5b.12xlarge (48 vCPU、3,384 GiB)
- r5b.16xlarge (64 vCPU、3,512 GiB)
- r5b.24xlarge (96 vCPU、3,768 GiB)
- r5b.metal (96 768 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)
- r5d.metal (96 vCPU、768 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します。
- 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)
- r5n.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)
- r5dn.metal (96 vCPU、768 GiB)
- r6a.xlarge (4 vCPU、32 GiB)
- r6a.2xlarge (8 vCPU、64 GiB)
- r6a.4xlarge (16 vCPU、128 GiB)
- r6a.8xlarge (32 vCPU、256 GiB)
- r6a.12xlarge (48 vCPU、384 GiB)

- r6a.16xlarge (64 vCPU、512 GiB)
- r6a.24xlarge (96 vCPU、768 GiB)
- r6a.32xlarge (128 vCPU、1,024 GiB)
- r6a.48xlarge (192 vCPU、1,536 GiB)
- r6a.metal (192 vCPU、1,536 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)
- r6i.metal (128 vCPU、1,024 GiB)
- r6id.xlarge (4 vCPU、32 GiB)
- r6id.2xlarge (8 vCPU、64 GiB)
- r6id.4xlarge (16 vCPU、128 GiB)
- r6id.8xlarge (32 vCPU、256 GiB)
- r6id.12xlarge (48 vCPU、384 GiB)
- r6id.16xlarge (64 vCPU、512 GiB)
- r6id.24xlarge (96 vCPU、768 GiB)
- r6id.32xlarge (128 vCPU、1,024 GiB)
- r6id.metal (128 vCPU、1,024 GiB)
- r6idn.12xlarge (48 vCPU、384 GiB)
- r6idn.16xlarge (64 vCPU、512 GiB)
- r6idn.24xlarge (96 vCPU、768 GiB)
- r6idn.2xlarge (8 vCPU、64 GiB)
- r6idn.32xlarge (128 vCPU、1,024 GiB)
- r6idn.4xlarge (16 vCPU、128 GiB)

- r6idn.8xlarge (32 vCPU、256 GiB)
- r6idn.xlarge (4 vCPU、32 GiB)
- r6in.12xlarge (48 vCPU、384 GiB)
- r6in.16xlarge (64 vCPU、512 GiB)
- r6in.24xlarge (96 vCPU、768 GiB)
- r6in.2xlarge (8 vCPU、64 GiB)
- r6in.32xlarge (128 vCPU、1,024 GiB)
- r6in.4xlarge (16 vCPU、128 GiB)
- r6in.8xlarge (32 vCPU、256 GiB)
- r6in.xlarge (4 vCPU、32 GiB)
- r7a.xlarge (4 vCPU、32 GiB)
- r7a.2xlarge (8 vCPU、64 GiB)
- r7a.4xlarge (16 vCPU、128 GiB)
- r7a.8xlarge (32 vCPU、256 GiB)
- r7a.12xlarge (48 vCPU、384 GiB)
- r7a.16xlarge (64 vCPU、512 GiB)
- r7a.24xlarge (96 vCPU、768 GiB)
- r7a.32xlarge (128 vCPU、1024 GiB)
- r7a.48xlarge (192 vCPU、1536 GiB)
- r7a.metal-48xl (192 vCPU、1536 GiB)
- r7i.xlarge (4 vCPU、32 GiB)
- r7i.2xlarge (8 vCPU、64 GiB)
- r7i.4xlarge (16 vCPU、128 GiB)
- r7i.8xlarge (32 vCPU、256 GiB)
- r7i.12xlarge (48 vCPU、384 GiB)
- r7i.16xlarge (64 vCPU、512 GiB)
- r7i.24xlarge (96 vCPU、768 GiB)
- r7i.metal-24xl (96 vCPU、768 GiB)
- r7iz.xlarge (4 vCPU、32 GiB)

- r7iz.2xlarge (8 vCPU、64 GiB)
- r7iz.4xlarge (16 vCPU、128 GiB)
- r7iz.8xlarge (32 vCPU、256 GiB)
- r7iz.12xlarge (48 vCPU、384 GiB)
- r7iz.16xlarge (64 vCPU、512 GiB)
- r7iz.32xlarge (128 vCPU、1024 GiB)
- r7iz.metal-16xl (64 vCPU、512 GiB)
- r7iz.metal-32xl (128 vCPU、1,024 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)
- z1d.metal (48 vCPU、384 GiB)こ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5.5 高速コンピューティング**

- p3.2xlarge (8 vCPU、61 GiB)
- p3.8xlarge (32 vCPU、244 GiB)
- p3.16xlarge (64 vCPU、488 GiB)
- p3dn.24xlarge (96 vCPU、768 GiB)
- p4d.24xlarge (96 vCPU、1,152 GiB)
- p4de.24xlarge (96 vCPU、1,152 GiB)
- p5.48xlarge (192 vCPU、2,048 GiB)
- p5e.48xlarge (192 vCPU、2,048 GiB)
- p5en.48xlarge (192 vCPU、2,048 GiB)
- g4ad.xlarge (4 vCPU、16 GiB)
- g4ad.2xlarge (8 vCPU、32 GiB)
- g4ad.4xlarge (16 vCPU、64 GiB)
- g4ad.8xlarge (32 vCPU、128 GiB)

- g4ad.16xlarge (64 vCPU、256 GiB)
- g4dn.xlarge (4 vCPU、16 GiB)
- g4dn.2xlarge (8 vCPU、32 GiB)
- g4dn.4xlarge (16 vCPU、64 GiB)
- g4dn.8xlarge (32 vCPU、128 GiB)
- g4dn.12xlarge (48 vCPU、192 GiB)
- g4dn.16xlarge (64 vCPU、256 GiB)
- g4dn.metal (96 vCPU、384 GiB)
- g5.xlarge (4 vCPU、16 GiB)
- g5.2xlarge (8 vCPU、32 GiB)
- g5.4xlarge (16 vCPU、64 GiB)
- g5.8xlarge (32 vCPU、128 GiB)
- g5.16xlarge (64 vCPU、256 GiB)
- g5.12xlarge (48 vCPU、192 GiB)
- g5.24xlarge (96 vCPU、384 GiB)
- g5.48xlarge (192 vCPU、768 GiB)
- dl1.24xlarge (96 vCPU、768 GiB) Intel 固有で、Nvidia では対応していません。
- g6.xlarge (4 vCPU、16 GiB)
- g6.2xlarge (8 vCPU、32 GiB)
- g6.4xlarge (16 vCPU、64 GiB)
- g6.8xlarge (32 vCPU、128 GiB)
- g6.12xlarge (48 vCPU、192 GiB)
- g6.16xlarge (64 vCPU、256 GiB)
- g6.24xlarge (96 vCPU、384 GiB)
- g6.48xlarge (192 vCPU、768 GiB)
- g6e.xlarge (4 vCPU、32 GiB)
- g6e.2xlarge (8 vCPU、64 GiB)
- g6e.4xlarge (16 vCPU、128 GiB)
- g6e.8xlarge (32 vCPU、256 GiB)

- g6e.12xlarge (48 vCPU、384 GiB)
- g6e.16xlarge (64 vCPU、512 GiB)
- g6e.24xlarge (96 vCPU、768 GiB)
- g6e.48xlarge (192 vCPU、1,536 GiB)
- gr6.4xlarge (16 vCPU、128 GiB)
- gr6.8xlarge (32 vCPU、256 GiB)
- p6-b200.48xlarge (192 vCPU、2,048 GiB)

GPU インスタンスタイプソフトウェアスタックのサポートは AWS によって提供されます。AWS サービスクォータが必要な GPU インスタンスタイプに対応できることを確認します。

**例5.6 高速コンピューティング - AWS Trainium と Inferentia**

**警告**

AWS Trainium および Inferentia インスタンスタイプの詳細は、Inferentia & Trainium instances on ROSA を参照してください。

- trn1.2xlarge (8 vCPU、32 GiB)
- trn1.32xlarge (128 vCPU、512 GiB)
- trn1n.32xlarge (128 vCPU、512 GiB)
- trn2.48xlarge (192 vCPU、2048 GiB)
- trn2u.48xlarge (192 vCPU、2048 GiB)
- inf1.xlarge (4 vCPU、8 GiB)
- inf1.2xlarge (8 vCPU、16 GiB)
- inf1.6xlarge (24 vCPU、48 GiB)
- inf1.24xlarge (96 vCPU、192 GiB)
- inf2.xlarge (4 vCPU、16 GiB)
- inf2.8xlarge (32 vCPU、128 GiB)
- inf2.24xlarge (96 vCPU、384 GiB)
- inf2.48xlarge (192 vCPU、768 GiB)

**例5.7 最適化されたコンピュート**

- 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)
- c5.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)
- c5d.metal (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.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)
- c5n.metal (72 vCPU、192 GiB)
- c6a.xlarge (4 vCPU、8 GiB)
- c6a.2xlarge (8 vCPU、16 GiB)
- c6a.4xlarge (16 vCPU、32 GiB)
- c6a.8xlarge (32 vCPU、64 GiB)
- c6a.12xlarge (48 vCPU、96 GiB)
- c6a.16xlarge (64 vCPU、128 GiB)
- c6a.24xlarge (96 vCPU、192 GiB)
- c6a.32xlarge (128 vCPU、256 GiB)
- c6a.48xlarge (192 vCPU、384 GiB)
- c6a.metal (192 vCPU、384 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)
- c6i.metal (128 vCPU、256 GiB)
- c6id.xlarge (4 vCPU、8 GiB)
- c6id.2xlarge (8 vCPU、16 GiB)

- c6id.4xlarge (16 vCPU、32 GiB)
- c6id.8xlarge (32 vCPU、64 GiB)
- c6id.12xlarge (48 vCPU、96 GiB)
- c6id.16xlarge (64 vCPU、128 GiB)
- c6id.24xlarge (96 vCPU、192 GiB)
- c6id.32xlarge (128 vCPU、256 GiB)
- c6id.metal (128 vCPU、256 GiB)
- c6in.12xlarge (48 vCPU、96 GiB)
- c6in.16xlarge (64 vCPU、128 GiB)
- c6in.24xlarge (96 vCPU、192 GiB)
- c6in.2xlarge (8 vCPU、16 GiB)
- c6in.32xlarge (128 vCPU、256 GiB)
- c6in.4xlarge (16 vCPU、32 GiB)
- c6in.8xlarge (32 vCPU、64 GiB)
- c6in.xlarge (4 vCPU、8 GiB)
- c7a.xlarge (4 vCPU、8 GiB)
- c7a.2xlarge (8 vCPU、16 GiB)
- c7a.4xlarge (16 vCPU、32 GiB)
- c7a.8xlarge (32 vCPU、64 GiB)
- c7a.12xlarge (48 vCPU、96 GiB)
- c7a.16xlarge (64 vCPU、128 GiB)
- c7a.24xlarge (96 vCPU、192 GiB)
- c7a.32xlarge (128 vCPU、256 GiB)
- c7a.48xlarge (192 vCPU、384 GiB)
- c7a.metal-48xl (192 vCPU、384 GiB)
- c7i.xlarge (4 vCPU、8 GiB)
- c7i.2xlarge (8 vCPU、16 GiB)
- c7i.4xlarge (16 vCPU、32 GiB)
- c7i.8xlarge (32 vCPU、64 GiB)

- c7i.12xlarge (48 vCPU、96 GiB)
- c7i.16xlarge (64 vCPU、128 GiB)
- c7i.24xlarge (96 vCPU、192 GiB)
- c7i.48xlarge (192 vCPU、384 GiB)
- c7i-flex.xlarge (4 vCPU、8 GiB)
- c7i-flex.2xlarge (8 vCPU、16 GiB)
- c7i-flex.4xlarge (16 vCPU、32 GiB)
- c7i-flex.8xlarge (32 vCPU、64 GiB)
- c7i.metal-24xl (96 vCPU、192 GiB)
- c7i.metal-48xl (192 vCPU、384 GiB)
- hpc6a.48xlarge (96 vCPU、384 GiB)
- hpc6id.32xlarge (64 vCPU、1024 GiB)
- hpc7a.12xlarge (24 vCPU、768 GiB)
- hpc7a.24xlarge (48 vCPU、768 GiB)
- hpc7a.48xlarge (96 vCPU、768 GiB)
- hpc7a.96xlarge (192 vCPU、768 GiB)
- m5zn.12xlarge (48 vCPU、192 GiB)
- m5zn.2xlarge (8 vCPU、32 GiB)
- m5zn.3xlarge (16 vCPU、48 GiB)
- m5zn.6xlarge (32 vCPU、96 GiB)
- m5zn.xlarge (4 vCPU、16 GiB)

**例5.8 最適化されたストレージ**

- c5ad.12xlarge (48 vCPU、96 GiB)
- c5ad.16xlarge (64 vCPU、128 GiB)
- c5ad.24xlarge (96 vCPU、192 GiB)
- c5ad.2xlarge (8 vCPU、16 GiB)
- c5ad.4xlarge (16 vCPU、32 GiB)
- c5ad.8xlarge (32 vCPU、64 GiB)
- c5ad.xlarge (4 vCPU、8 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)
- i3.metal (72 vCPU、512 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。
- 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)
- i3en.metal (96 vCPU、768 GiB)
- i4i.xlarge (4 vCPU、32 GiB)
- i4i.2xlarge (8 vCPU、64 GiB)
- i4i.4xlarge (16 vCPU、128 GiB)
- i4i.8xlarge (32 vCPU、256 GiB)
- i4i.12xlarge (48 vCPU、384 GiB)
- i4i.16xlarge (64 vCPU、512 GiB)
- i4i.24xlarge (96 vCPU、768 GiB)
- i4i.32xlarge (128 vCPU、1,024 GiB)
- i4i.metal (128 vCPU、1,024 GiB)
- i7i.xlarge (4 vCPU、32 GiB)
- i7i.2xlarge (8 vCPU、64 GiB)
- i7i.4xlarge (16 vCPU、128 GiB)
- i7i.8xlarge (32 vCPU、256 GiB)
- i7i.12xlarge (48 vCPU、384 GiB)
- i7i.16xlarge (64 vCPU、512 GiB)
- i7i.24xlarge (96 vCPU、768 GiB)

- i7i.48xlarge (192 vCPU、1,536 GiB)
- i7i.metal-24xl (96 vCPU、768 GiB)
- i7i.metal-48xl (192 vCPU、1,536 GiB)
- i7ie.xlarge (4 vCPU、32 GiB)
- i7ie.2xlarge (8 vCPU、64 GiB)
- i7ie.3xlarge (12 vCPU、96 GiB)
- i7ie.6xlarge (24 vCPU、192 GiB)
- i7ie.12xlarge (48 vCPU、384 GiB)
- i7ie.18xlarge (72 vCPU、576 GiB)
- i7ie.24xlarge (96 vCPU、768 GiB)
- i7ie.48xlarge (192 vCPU、1,536 GiB)
- i7ie.metal-24xl (96 vCPU、768 GiB)
- i7ie.metal-48xl (192 vCPU、1,536 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.xlarge (4 vCPU、16 GiB)
- m5d.2xlarge (8 vCPU、32 GiB)
- m5d.4xlarge (16 vCPU、64 GiB)
- m5d.8xlarge (32 vCPU、28 GiB)
- m5d.12xlarge (48 vCPU、192 GiB)
- m5d.16xlarge (64 vCPU、256 GiB)
- m5d.24xlarge (96 vCPU、384 GiB)

**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。

**例5.9 高メモリー**

- u-3tb1.56xlarge (224 vCPU、3,072 GiB)
- u-6tb1.56xlarge (224 vCPU、6,144 GiB)
- u-6tb1.112xlarge (448 vCPU、6,144 GiB)
- u-6tb1.metal (448 vCPU、6,144 GiB)
- u-9tb1.112xlarge (448 vCPU、9,216 GiB)
- u-9tb1.metal (448 vCPU、9,216 GiB)
- u-12tb1.112xlarge (448 vCPU、12,288 GiB)
- u-12tb1.metal (448 vCPU、12,288 GiB)
- u-18tb1.metal (448 vCPU、18,432 GiB)
- u-24tb1.metal (448 vCPU、24,576 GiB)
- u-24tb1.112xlarge (448 vCPU、24,576 GiB)

**例5.10 最適化されたネットワーク**

- 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)
- 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)
- m5n.12xlarge (48 vCPU、192 GiB)

- m5n.16xlarge (64 vCPU、256 GiB)
- m5n.24xlarge (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)

### 5.4.2. AWS Arm ベースの Graviton インスタンスタイプ

x86 ベースのアーキテクチャーに加えて、ROSA with HCP は次の Arm ベースの Graviton ワーカーノードインスタンスタイプとサイズを提供します。

**注記**

Graviton インスタンスタイプは、2024 年 7 月 24 日以降に作成された新しいクラスターでのみ使用できます。

**例5.11 一般的用途**

- a1.xlarge (2 vCPU、4 GiB)
- a1.2xlarge (4 vCPU、8 GiB)
- a1.4xlarge (8 vCPU、16 GiB)
- a1.metal (16 vCPU、32 GiB)
- m6g.xlarge (2 vCPU、8 GiB)
- m6g.2xlarge (4 vCPU、16 GiB)
- m6g.4xlarge (8 vCPU、32 GiB)
- m6g.8xlarge (32 vCPU、128 GiB)
- m6g.12xlarge (48 vCPU、192 GiB)
- m6g.16xlarge (64 vCPU、256 GiB)
- m6g.metal (64 vCPU、256 GiB)
- m6gd.xlarge (2 vCPU、8 GiB)
- m6gd.2xlarge (4 vCPU、16 GiB)
- m6gd.4xlarge (8 vCPU、32 GiB)
- m6gd.8xlarge (32 vCPU、128 GiB)
- m6gd.12xlarge (48 vCPU、192 GiB)

- m6gd.16xlarge (64 vCPU、256 GiB)
- m6gd.metal (64 vCPU、256 GiB)
- m7g.xlarge (2 vCPU、8 GiB)
- m7g.2xlarge (4 vCPU、16 GiB)
- m7g.4xlarge (8 vCPU、32 GiB)
- m7g.8xlarge (32 vCPU、128 GiB)
- m7g.12xlarge (48 vCPU、192 GiB)
- m7g.16xlarge (64 vCPU、256 GiB)
- m7g.metal (64 vCPU、256 GiB)
- m7gd.2xlarge (4 vCPU、16 GiB)
- m7gd.4xlarge (8 vCPU、32 GiB)
- m7gd.8xlarge (32 vCPU、128 GiB)
- m7gd.12xlarge (48 vCPU、192 GiB)
- m7gd.16xlarge (64 vCPU、256 GiB)
- m7gd.xlarge (2 vCPU、8 GiB)
- m7gd.metal (64 vCPU、256 GiB)
- m8g.xlarge (4 vCPU、16 GiB)
- m8g.2xlarge (8 vCPU、32 GiB)
- m8g.4xlarge (16 vCPU、64 GiB)
- m8g.8xlarge (32 vCPU、128 GiB)
- m8g.12xlarge (48 vCPU、192 GiB)
- m8g.16xlarge (64 vCPU、256 GiB)
- m8g.24xlarge (96 vCPU、384 GiB)
- m8g.48xlarge (192 vCPU、768 GiB)
- m8g.metal-24xl (96 vCPU、384 GiB)
- m8g.metal-48xl (192 vCPU、768 GiB)

**例5.12 バースト可能な汎用目的**

- t4g.xlarge (4 vCPU、16 GiB)
- t4g.2xlarge (8 vCPU、32 GiB)

**例5.13 メモリー集約型**

- x2gd.xlarge (2 vCPU、64 GiB)
- x2gd.2xlarge (4 vCPU、128 GiB)
- x2gd.4xlarge (8 vCPU、256 GiB)
- x2gd.8xlarge (16 vCPU、512 GiB)
- x2gd.12xlarge (32 vCPU、768 GiB)
- x2gd.16xlarge (64 vCPU、1,024 GiB)
- x2gd.metal (64 vCPU、1,024 GiB)
- x8g.xlarge (4 vCPU、64 GiB)
- x8g.2xlarge (8 vCPU、128 GiB)
- x8g.4xlarge (16 vCPU、256 GiB)
- x8g.8xlarge (32 vCPU、512 GiB)
- x8g.12xlarge (48 vCPU、768 GiB)
- x8g.16xlarge (64 vCPU、1,024 GiB)
- x8g.24xlarge (96 vCPU、1,536 GiB)
- x8g.48xlarge (192 vCPU、3,072 GiB)
- x8g.metal-24xl (96 vCPU、1,536 GiB)
- x8g.metal-48xl (192 vCPU、3,072 GiB)

**例5.14 最適化されたメモリー**

- r6g.xlarge (4 vCPU、32 GiB)
- r6g.2xlarge (8 vCPU、64 GiB)
- r6g.4xlarge (16 vCPU、128 GiB)
- r6g.8xlarge (32 vCPU、256 GiB)
- r6g.12xlarge (48 vCPU、384 GiB)
- r6g.16xlarge (64 vCPU、512 GiB)
- r6g.metal (64 vCPU、512 GiB)
- r6gd.xlarge (4 vCPU、32 GiB)

- r6gd.2xlarge (8 vCPU、64 GiB)
- r6gd.4xlarge (16 vCPU、128 GiB)
- r6gd.8xlarge (32 vCPU、256 GiB)
- r6gd.12xlarge (48 vCPU、384 GiB)
- r6gd.16xlarge (64 vCPU、512 GiB)
- r6gd.metal (64 vCPU、512 GiB)
- r7g.xlarge (4 vCPU、32 GiB)
- r7g.2xlarge (8 vCPU、64 GiB)
- r7g.4xlarge (16 vCPU、128 GiB)
- r7g.8xlarge (32 vCPU、256 GiB)
- r7g.12xlarge (48 vCPU、384 GiB)
- r7g.16xlarge (64 vCPU、512 GiB)
- r7g.metal (64 vCPU、512 GiB)
- r7gd.xlarge (4 vCPU、32 GiB)
- r7gd.2xlarge (8 vCPU、64 GiB)
- r7gd.4xlarge (16 vCPU、128 GiB)
- r7gd.8xlarge (32 vCPU、256 GiB)
- r7gd.12xlarge (48 vCPU、384 GiB)
- r7gd.16xlarge (64 vCPU、512 GiB)
- r7gd.metal (64 vCPU、512 GiB)
- r8g.xlarge (4 vCPU、32 GiB)
- r8g.2xlarge (8 vCPU、64 GiB)
- r8g.4xlarge (16 vCPU、128 GiB)
- r8g.8xlarge (32 vCPU、256 GiB)
- r8g.12xlarge (48 vCPU、384 GiB)
- r8g.16xlarge (64 vCPU、512 GiB)
- r8g.24xlarge (96 vCPU、768 GiB)
- r8g.48xlarge (192 vCPU、1,536 GiB)
- r8g.metal-24xl (96 vCPU、768 GiB)

- r8g.metal-48xl (192 vCPU、1,536 GiB)

**例5.15 高速コンピューティング**

- g5g.xlarge (4 vCPU、8 GiB)
- g5g.2xlarge (8 vCPU、16 GiB)
- g5g.4xlarge (16 vCPU、32 GiB)
- g5g.8xlarge (32 vCPU、64 GiB)
- g5g.16xlarge (64 vCPU、128 GiB)
- g5g.metal (64 vCPU、128 GiB)

**例5.16 最適化されたコンピュート**

- c6g.xlarge (4 vCPU、8 GiB)
- c6g.2xlarge (8 vCPU、16 GiB)
- c6g.4xlarge (16 vCPU、32 GiB)
- c6g.8xlarge (32 vCPU、64 GiB)
- c6g.12xlarge (48 vCPU、96 GiB)
- c6g.16xlarge (64 vCPU、128 GiB)
- c6g.metal (64 vCPU、128 GiB)
- c6gd.xlarge (4 vCPU、8 GiB)
- c6gd.2xlarge (8 vCPU、16 GiB)
- c6gd.4xlarge (16 vCPU、32 GiB)
- c6gd.8xlarge (32 vCPU、64 GiB)
- c6gd.12xlarge (48 vCPU、96 GiB)
- c6gd.16xlarge (64 vCPU、128 GiB)
- c6gd.metal (64 vCPU、128 GiB)
- c6gn.xlarge (4 vCPU、8 GiB)
- c6gn.2xlarge (8 vCPU、16 GiB)
- c6gn.4xlarge (16 vCPU、32 GiB)
- c6gn.8xlarge (32 vCPU、64 GiB)
- c6gn.12xlarge (48 vCPU、96 GiB)

- c6gn.16xlarge (64 vCPU、128 GiB)
- c7g.xlarge (4 vCPU、8 GiB)
- c7g.2xlarge (4 vCPU、8 GiB)
- c7g.4xlarge (16 vCPU、32 GiB)
- c7g.8xlarge (32 vCPU、64 GiB)
- c7g.12xlarge (48 vCPU、96 GiB)
- c7g.16xlarge (64 vCPU、128 GiB)
- c7g.metal (64 vCPU、128 GiB)
- c7gd.xlarge (4 vCPU、8 GiB)
- c7gd.2xlarge (4 vCPU、8 GiB)
- c7gd.4xlarge (16 vCPU、32 GiB)
- c7gd.8xlarge (32 vCPU、64 GiB)
- c7gd.12xlarge (48 vCPU、96 GiB)
- c7gd.16xlarge (64 vCPU、128 GiB)
- c7gd.metal (64 vCPU、128 GiB)
- c7gn.xlarge (4 vCPU、8 GiB)
- c7gn.2xlarge (8 vCPU、16 GiB)
- c7gn.4xlarge (16 vCPU、32 GiB)
- c7gn.8xlarge (32 vCPU、64 GiB)
- c7gn.12xlarge (48 vCPU、96 GiB)
- c7gn.16xlarge (64 vCPU、128 GiB)
- c7gn.metal (64 vCPU、128 GiB)
- c8g.xlarge (4 vCPU、8 GiB)
- c8g.2xlarge (8 vCPU、16 GiB)
- c8g.4xlarge (16 vCPU、32 GiB)
- c8g.8xlarge (32 vCPU、64 GiB)
- c8g.12xlarge (48 vCPU、96 GiB)
- c8g.16xlarge (64 vCPU、128 GiB)
- c8g.24xlarge (96 vCPU、192 GiB)

- c8g.48xlarge (192 vCPU、384 GiB)
- c8g.metal-24xl (96 vCPU、192 GiB)
- c8g.metal-48xl (192 vCPU、384 GiB)

**例5.17 最適化されたストレージ**

- i4g.xlarge (4 vCPU、32 GiB)
- i4g.2xlarge (8 vCPU、64 GiB)
- i4g.4xlarge (16 vCPU、128 GiB)
- i4g.8xlarge (32 vCPU、256 GiB)
- i4g.16xlarge (64 vCPU、512 GiB)
- is4gen.xlarge (4 vCPU、16 GiB)
- is4gen.2xlarge (8 vCPU、32 GiB)
- is4gen.4xlarge (16 vCPU、64 GiB)
- is4gen.8xlarge (32 vCPU、128 GiB)
- im4gn.xlarge (4 vCPU、16 GiB)
- im4gn.2xlarge (8 vCPU、32 GiB)
- im4gn.4xlarge (16 vCPU、64 GiB)
- im4gn.8xlarge (32 vCPU、128 GiB)
- im4gn.16xlarge (64 vCPU、256 GiB)

**例5.18 高性能コンピューティング (HPC)**

- hpc7g.4xlarge (16 vCPU、128 GiB)
- hpc7g.8xlarge (32 vCPU、128 GiB)
- hpc7g.16xlarge (64 vCPU、128 GiB)

**関連情報**

- AWS インスタンスタイプ

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

### 5.5.1. 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 のマネージドデプロイメントであり、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

### 5.5.2. 定義

**表5.2 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

### 5.5.3. 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。

### 5.5.4. 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、特定のマイナーバージョンの一般提供が開始してから 16 カ月間以上、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、サポート期間の影響を受けません。

サポート期間が終了する 60 日前、30 日前、および 15 日前に、お客様に通知されます。サポート期間が終了する前に、クラスターをサポート対象の最も古いマイナーバージョンの最新パッチバージョンにクラスターを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、コントロールプレーンが次のサポート対象のマイナーバージョンに Red Hat によって自動的にアップグレードされます。

**例**

1. 現時点で、お客様のクラスターは 4.13.8 で実行しているとします。4.13 マイナーバージョンは、2023 年 5 月 17 日に一般提供されました。
2. 2024 年 7 月 19 日、8 月 16 日、および 9 月 2 日に、クラスターがサポート対象のマイナーバージョンにまだアップグレードされていない場合、2024 年 9 月 17 日にクラスターが "限定サポート" 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、2024 年 9 月 17 日までに 4.14 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、クラスターのコントロールプレーンが自動的に 4.14.26 にアップグレードされます。クラスターのワーカーノードへの自動アップグレードは行われません。

**関連情報**

- Red Hat OpenShift Service on AWS の限定サポートステータス

### 5.5.5. 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、あるバ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リストから削除されます。さらに、4.7.6 を実行するクラスターは、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。

### 5.5.6. 限定サポートステータス

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。

**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を質問がある場合、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。

### 5.5.7. 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。

### 5.5.8. 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。

### 5.5.9. 削除ポリシー

Red Hat は、対処が必要なサービス通知が対処されない場合、15 日以内に Red Hat OpenShift Service on AWS クラスターを削除する権利を留保します。この対処には、クラスターをサポート対象の OpenShift バージョンにアップグレードすることや、クラスターの健全性の問題を解決して、サービスがクラスターをサポート対象の OpenShift バージョンに自動アップグレードできるようにすることが含まれます。

Red Hat OpenShift Service on AWS のサービスは、クラスターが健全でない場合や OpenShift バージョンが EOL に近づいている場合にお客様に通知します。

**重要**

削除保護が有効に設定された Red Hat OpenShift Service on AWS クラスターであっても、削除ポリシーに基づいて削除される場合があります。

Red Hat OpenShift Service on AWS クラスターが削除されると、クラスター上でホストされているすべてのアプリケーションやビジネスに影響が出ます。さらに、クラスターの削除後もクラウドリソースが AWS アカウントに残る場合があり、引き続きコストが発生します。

### 5.5.10. 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。

極端な状況下では、環境に対する CVE の重要性に関する Red Hat の評価に基づいて、Red Hat はお客様に対して、2 営業日 以内にクラスターを最新のセキュアなパッチリリースに更新するようスケジュールするか手動で更新するよう通知します。2 営業日 が経過しても、更新が実行されない場合、Red Hat は潜在的なセキュリティー違反や不安定性を軽減するために、クラスターのコントロールプレーンを最新のセキュアなパッチリリースに自動的に更新します。Red Hat は、サポートケース を通じてお客様からリクエストがあった場合、当社の判断で自動更新を一時的に延期することがあります。

### 5.5.11. ライフサイクルの日付

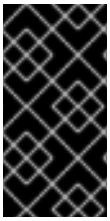
| バージョン | 一般提供 | メンテナンスサポートの終了日 | Extended Update Support Add-On - Term 1 終了 |
|---|---|---|---|
| 4.20 | 2025 年 10 月 21 日 | 2027 年 4 月 21 日 | 2027 年 10 月 21 日 |
| 4.19 | 2025 年 6 月 17 日 | 2026 年 12 月 17 日 | |
| 4.18 | 2025 年 2 月 25 日 | 2026 年 8 月 25 日 | 2027 年 2 月 25 日 |
| 4.17 | 2024 年 10 月 1 日 | 2026 年 4 月 1 日 | |
| 4.16 | 2024 年 6 月 27 日 | 2025 年 12 月 27 日 | 2026 年 6 月 27 日 |
| 4.15 | 2024 年 2 月 27 日 | 2025 年 8 月 27 日 | |

Extended Update Support Add-On - Term 1 は、4.16 以降の偶数バージョンを使用している Red Hat OpenShift Service on AWS を利用するお客様に提供され、Red Hat OpenShift Service on AWS サブスクリプションに追加費用なしで含まれています。

Extended Update Support Add-On - Term 1 の主な利点は、対象となるマイナーリリースのサポートライフサイクルを 18 カ月から合計 24 カ月に延長できることです。この 6 カ月の延長により、組織は完全なバージョンアップグレードを行うことなく、重要なセキュリティー更新や緊急度の高いバグ修正を継

続的に適用できます。これにより、ミッションクリティカルなアプリケーションの安定性を確保し、複雑な規制検証スケジュールに対応しながら、限られた保守期間を効率的に活用することが可能になります。

Red Hat OpenShift Service on AWS クラスターに Extended Update Support Add-On - Term 1 を適用するには、チャネルグループを **eus** に更新する必要があります。クラスターチャネルグループの更新の詳細は、**関連情報** セクションの **クラスターの編集** を参照してください。Extended Update Support Add-On - Term 1 の詳細は、Extended Update Support Add-On を参照してください。



**重要**

クラスターをバージョン 4.16 からバージョン 4.18 にアップグレードする前に、コントロールプレーンとマシンプールがバージョン 4.16 を使用していることを確認してください。詳細は、**関連情報** セクションの **Red Hat OpenShift Service on AWS クラスターのアップグレードオプション** を参照してください。

**関連情報**

- ROSA CLI コマンドリファレンス
- Red Hat OpenShift Service on AWS クラスターのアップグレードオプション

## 5.6. SRE およびサービスアカウントのアクセス

Red Hat Site Reliability Engineering (SRE) による Red Hat OpenShift Service on AWS クラスターへのアクセスについて、アイデンティティーおよびアクセス管理の観点から説明します。

### 5.6.1. アイデンティティーおよびアクセス管理

Red Hat 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。

#### 5.6.1.1. サブプロセッサー

利用可能なサブプロセスのリストは、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。

### 5.6.2. SRE クラスターアクセス

Red Hat SRE による Red Hat OpenShift Service on AWS クラスターへのアクセスは、複数の必要な認証階層を通じて制御され、すべて厳格な企業ポリシーによって管理されます。クラスターにアクセスするすべての認証試行とクラスター内で行われた変更は、それらのアクションを担当する SRE の特定のアカウント ID とともに監査ログに記録されます。これらの監査ログは、SRE がお客様のクラスターに加えたすべての変更が、Red Hat のマネージドサービスに関するガイドラインで規定されている厳格なポリシーと手順に準拠していることを確認するのに役立ちます。

以下に示す情報は、SRE がお客様のクラスターにアクセスするために実行する必要があるプロセスの概要です。

- Red Hat SRE が、Red Hat SSO (クラウドサービス) から更新された ID トークンを要求します。このリクエストは認証されます。トークンは 15 分間有効です。トークンの有効期限が切れたら、トークンを再度更新して新しいトークンを受け取ることができます。新規トークンへの更新機能には期限はありません。ただし、新しいトークンに更新する機能は、非アクティブな状態が 30 日間続くと無効になります。

- Red Hat SRE が Red Hat VPN に接続します。VPN への認証は、Red Hat Corporate Identity and Access Management (RH IAM) システムによって行います。RH IAM を使用すると、SRE は多要素になり、グループおよび既存のオンボーディングおよびオフボーディングプロセスによって組織ごとに内部管理できるようになります。SRE が認証されて接続されると、SRE はクラウドサービスフリート管理プレーンにアクセスできるようになります。クラウドサービスフリート管理プレーンの変更には何層にもわたる承認が必要であり、厳格な企業ポリシーによって維持されます。

- 承認が完了すると、SRE はフリート管理プレーンにログインし、フリート管理プレーンが作成したサービスアカウントトークンを受け取ります。トークンは 15 分間有効です。トークンは無効になると、削除されます。

- フリート管理プレーンにアクセスが許可されると、SRE はネットワーク設定に応じてさまざまな方法を使用してクラスターにアクセスします。

    - プライベートまたはパブリッククラスターへのアクセス: リクエストは、ポート 6443 で暗号化された HTTP 接続を使用して、特定のネットワークロードバランサー (NLB) 経由で送信されます。

    - PrivateLink クラスターへのアクセス: リクエストは Red Hat Transit Gateway に送信されます。ゲートウェイは各リージョンの Red Hat の VPC に接続します。リクエストを受信する VPC は、ターゲットとなるプライベートクラスターのリージョンによって決まります。VPC 内には、顧客の PrivateLink クラスターへの PrivateLink エンドポイントを含むプライベートサブネットがあります。

### 5.6.3. 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。特に、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 にはアクセスできません。

| 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 - 通常操作 [1] | 読み取り: All<br>書き込み: Very limited | 読み取り: All<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 |
| OpenShift SRE - 昇格されたアクセス [2] (承認されたアクセスによって制御) | 読み取り: All<br>書き込み: All | 読み取り: All<br>書き込み: All | 読み取り: All<br>書き込み: All | 読み取り: All<br>書き込み: All |
| 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<br>書き込み: None | 読み取り: None<br>書き込み: None |

| 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 |
| 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 [3]<br>書き込み: Limited [3] | 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、および適切で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. アクセスが昇格されたことで、SRE に **cluster-admin** ロールのアクセスレベルが付与され、承認済みアクセスによって制御されます。詳細は、「デフォルトのクラスターロール」および「承認されたアクセス」を参照してください。
3. 顧客管理者によって RBAC で許可される内容と、ユーザーが作成した namespace に限定されます。

**関連情報**

- Approved Access
- デフォルトのクラスターロール

### 5.6.4. 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の詳細は、このドキュメントの「認証について」セクションを参照してください。

### 5.6.5. アクセスの承認およびレビュー

Red Hat SRE による新しい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リスト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。

アクセスとアイデンティティーの認可表には、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済み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 | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| Logging | **Red Hat**<br>● 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は、お客様がアクセス管理を行います。 |
| アプリケーションのネットワーク | **Red Hat**<br>● 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、サービスロー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 | **Red Hat**<br>● 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。 |
| 仮想ネットワーク管理 | **Red Hat**<br>● 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 を介して、AWS コンポーネントへのオプションのユーザーアクセスを管理します。 |

| リソース | サービスの責任 | お客様の責任 |
| --- | --- | --- |
| 仮想ストレージ管理 | **Red Hat**<br>● Red Hat 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 を介して、AWS コンポーネントへのオプションのユーザーアクセスを管理します。<br>● ROSA サービスへのアクセスを有効にするために必要な AWS IAM ロールとアタッチされたポリシーを作成します。 |
| 仮想コンピューティング管理 | **Red Hat**<br>● Red Hat 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 を介して、AWS コンポーネントへのオプションのユーザーアクセスを管理します。<br>● ROSA サービスへのアクセスを有効にするために必要な AWS IAM ロールとアタッチされたポリシーを作成します。 |
| AWS ソフトウェア (パブリック AWS サービス) | **AWS**<br>**コンピュート:** Amazon EC2 サービスを提供します。これは ROSA のコントロールプレーンとワーカーノードに使用されます。<br>**ストレージ:** Amazon EBS を提供します。これは、クラスターのローカルノードストレージと永続ボリュームストレージをプロビジョニングするために、ROSA によって使用されます。<br>**ストレージ:** Amazon S3 を提供します。これはサービスの組み込みイメージレジストリーに使用されます。<br>**ネットワーク:** AWS Identity and Access Management (IAM) を提供します。これは、お客様のアカウントで実行されている ROSA リソースへのアクセスを制御するために、お客様が使用します。 | ● ROSA サービスへのアクセスを有効にするために必要な AWS IAM ロールとアタッチされたポリシーを作成します。<br>● IAM ツールを使用して、顧客アカウントの AWS リソースに適切なアクセス許可を適用します。<br>● AWS 組織全体で ROSA を有効にするには、お客様が AWS Organizations 管理者を管理する責任があります。<br>● AWS 組織全体で ROSA を有効にするには、お客様が AWS License Manager を使用して ROSA エンタイトルメント付与を配布する責任があります。 |
| ハードウェアと AWS グローバルインフラストラクチャー | **AWS**<br>● AWS データセンターの物理的なアクセス制御に関する詳細は、AWS クラウドセキュリティーページの Our Controls を参照してください。 | ● お客様は AWS グローバルインフラストラクチャーに対して責任を負いません。 |

### 5.6.6. サービスアカウントが SRE 所有のプロジェクトで AWS IAM ロールを引き受ける方法

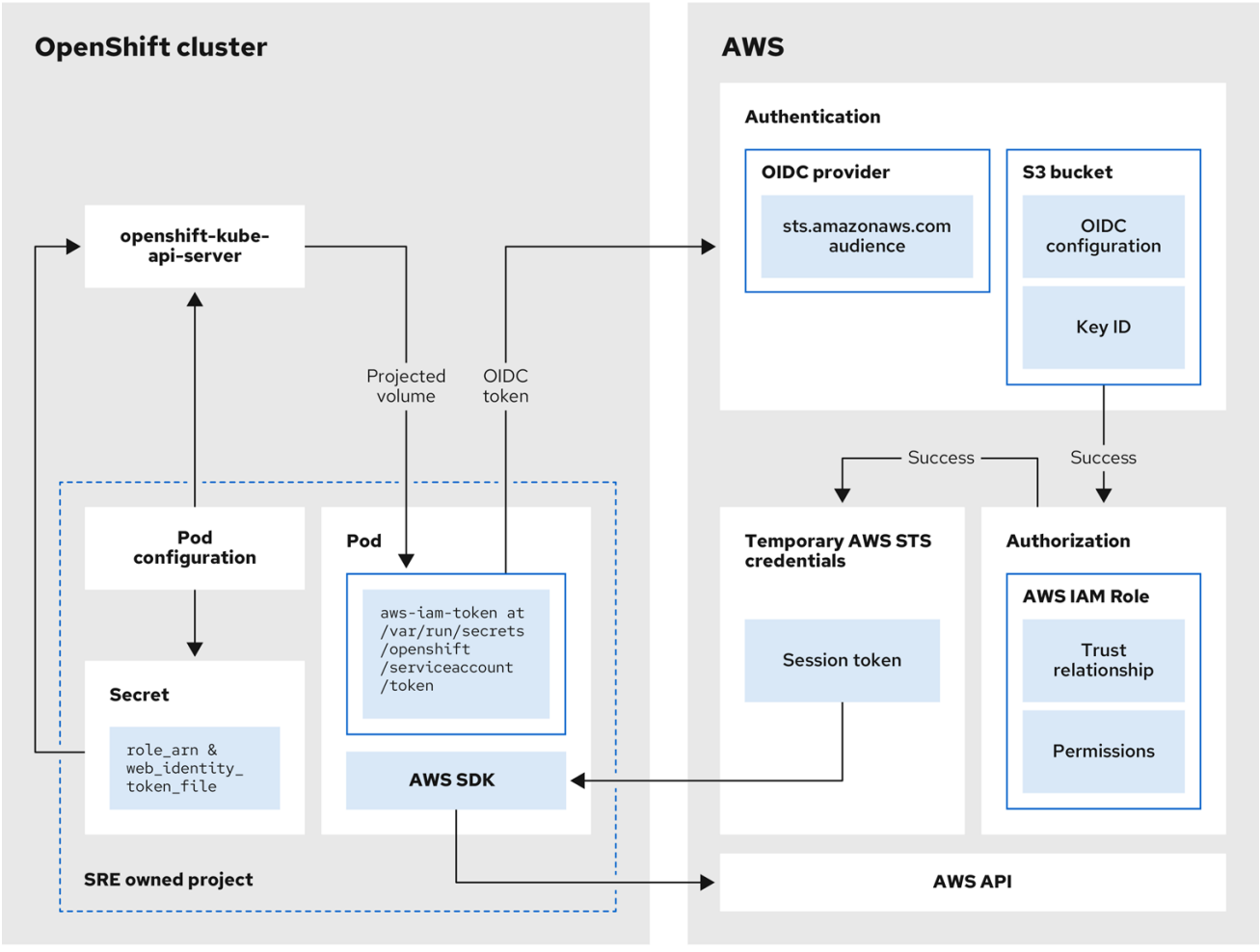
Red Hat OpenShift Service on AWS クラスターをインストールすると、クラスター固有の Operator AWS Identity and Access Management (IAM) ロールが作成されます。これらの IAM ロールにより、ROSA cluster Operator がコア OpenShift 機能を実行できるようになります。

クラスター Operator はサービスアカウントを使用して IAM ロールを引き受けます。サービスアカウントが IAM ロールを引き受けると、クラスター Operator の Pod でサービスアカウントが使用する一時的な AWS STS 認証情報が提供されます。引き受けたロールに必要な AWS 権限がある場合、サービスアカウントは Pod で AWS SDK 操作を実行できます。

#### 5.6.6.1. Red Hat SRE が所有するプロジェクトで AWS IAM ロールを引き受けるためのワークフロー

次の図は、SRE が所有するプロジェクトで AWS IAM ロールを引き受けるためのワークフローを示しています。

**図5.1 SRE 所有プロジェクトで AWS IAM ロールを引き受けるワークフロー**



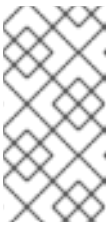

ワークフローには次の段階があります。

1. クラスター Operator が実行する各プロジェクト内で、Operator のデプロイメント仕様には、投影されたサービスアカウントトークンのボリュームマウントと、Pod の AWS 認証情報設定が含まれるシークレットがあります。トークンは、オーディエンスおよび時間の制限がありま

す。ROSA は 1 時間ごとに新しいトークンを生成し、AWS SDK は AWS 認証情報の設定を含むマウントされたシークレットを読み取ります。この設定には、マウントされたトークンと AWS IAM ロール ARN へのパスが含まれています。シークレットの認証情報設定には次のものが含まれます。

- AWS SDK オペレーションの実行に必要なパーミッションを持つ IAM ロールの ARN を含む **$AWS_ARN_ROLE** 変数。
- サービスアカウントの OpenID Connect (OIDC) トークンへの Pod 内のフルパスを含む **$AWS_WEB_IDENTITY_TOKEN_FILE** 変数。完全パスは **/var/run/secrets/openshift/serviceaccount/token** です。

2. クラスター Operator が AWS サービス (EC2 など) にアクセスするために AWS IAM ロールを引き受ける必要がある場合、Operator で実行される AWS SDK クライアントコードは **AssumeRoleWithWebIdentity** API を呼び出します。
3. OIDC トークンは、Pod から OIDC プロバイダーに渡されます。次の要件が満たされている場合は、プロバイダーがサービスアカウント ID を認証します。
   - ID 署名は有効であり、秘密鍵によって署名されています。
   - **sts.amazonaws.com** オーディエンスは OIDC トークンにリストされており、OIDC プロバイダーで設定されたオーディエンスと一致します。

     **注記**

     STS クラスターを使用する ROSA では、インストール中に OIDC プロバイダーが作成され、デフォルトでサービスアカウント発行者として設定されます。**sts.amazonaws.com** オーディエンスは、デフォルトで OIDC プロバイダーに設定されています。

   - OIDC トークンの有効期限が切れていません。
   - トークン内の発行者の値には、OIDC プロバイダーの URL が含まれています。
4. プロジェクトとサービスアカウントが、引き受ける IAM ロールの信頼ポリシーのスコープ内にある場合は、認可が成功します。
5. 認証と認可が成功すると、AWS アクセストークン、秘密鍵、セッショントークンの形式で一時的な AWS STS 認証情報が Pod に渡され、サービスアカウントで使用されます。認証情報を使用することで、IAM ロールで有効になっている AWS アクセス許可がサービスアカウントに一時的に付与されます。
6. クラスター Operator が実行されると、Pod で AWS SDK を使用している Operator は、投影されたサービスアカウントへのパスが含まれるシークレットと AWS IAM ロール ARN を OIDC プロバイダーに対して認証するためのシークレットを消費します。OIDC プロバイダーは、AWS API に対する認証に使用できるように、一時的な STS 認証情報を返します。

**関連情報**

- クラスター固有の Operator IAM ロール参照
- アカウント全体のロールを作成する方法

## 5.7. RED HAT OPENSHIFT SERVICE ON AWS のセキュリティーについて

このドキュメントでは、Red Hat、Amazon Web Services (AWS)、および管理対象の Red Hat OpenShift Service on AWS に対するお客様のセキュリティーに関する責任を詳しく説明します。

**表5.3 頭字語および用語**

| 略語 | 定義 |
| --- | --- |
| **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** | Common Vulnerabilities and Exposures |
| * **PV** | 永続ボリューム |
| * **SRE** | Red Hat Site Reliability Engineering |
| * **VPC** | 仮想プライベートクラウド |

### 5.7.1. 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。

#### 5.7.1.1. 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、処理中にそのデータの機密性および整合性に対する固有のリスクを強調表示するために、データ分類標準を定義し、フォローします。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に分類されます。

#### 5.7.1.2. 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セキュアに管理します。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、インフラストラクチャー、およびワーカー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。

#### 5.7.1.3. 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。特定された脆弱性は、重大度に基づくタイムラインに応じて修復で追跡されます。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。

#### 5.7.1.4. ネットワークセキュリティー

##### 5.7.1.4.1. 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。

##### 5.7.1.4.2. 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。

##### 5.7.1.4.3. クラスターのネットワークアクセス制御

**NetworkPolicy** オブジェクトと OVN-Kubernetes CNI を使用すると、お客様はプロジェクトごとにきめ細かなネットワークアクセス制御ルールを設定できます。

#### 5.7.1.5. 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。

#### 5.7.1.6. Compliance

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5.4 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**

| Compliance | Red Hat OpenShift Service on AWS |
|---|---|
| HIPAA Qualified[1] | はい |
| ISO 27001 | はい |
| ISO 27017 | はい |
| ISO 27018 | はい |
| PCI DSS 4.0 | はい |
| SOC 1 タイプ 2 | はい |
| SOC 2 タイプ 2 | はい |

| Compliance | Red Hat OpenShift Service on AWS |
| --- | --- |
| SOC 3 | はい |
| FedRAMP High[2] | いいえ |

1. Red Hat の HIPAA 認定 ROSA サービスの詳細は、HIPAA Overview を参照してください。
2. ROSA on GovCloud の詳細は、FedRAMP Marketplace ROSA Agency および ROSA JAB listings を参照してください。

**関連情報**

- Red Hat Subprocessor List
- ROSA の責任
- ROSA with HCP サービス定義
- IP ベースの AWS ロールを引き受けるための追加制約を追加する

# 第6章 IAM リソースについて

Red Hat OpenShift Service on AWS は、AWS Security Token Service (STS) を使用して、権限が制限された一時的な認証情報をクラスターに提供します。そのため、クラスターをデプロイする前に、次の AWS Identity Access Management (IAM) リソースを作成する必要があります。

- ROSA のサポート、インストール、コンピュート機能に必要な STS 権限を提供する、カウント全体の特定の IAM ロールとポリシー。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 を使用してクラスターをデプロイおよび管理する場合は、次の関連情報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。

このドキュメントでは、ROSA with HCP クラスターを作成するときにデプロイする必要がある IAM リソースに関するリファレンス情報を提供します。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**

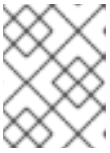
- ROSA with HCP クラスターの迅速な作成

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

OpenShift Cluster Manager 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。詳細は、AWS アカウントの関連付け を参照してください。

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 (**user-role**) は、Red Hat が顧客の 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。

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

OpenShift Cluster Manager 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。

#### 6.1.1.1. 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6.1 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リスト表示できます。 |
| **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リスト表示できます。 |
| **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。 |

| リソース | 説明 |
| --- | --- |
| **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6.2 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) をサポートするアイデンティティープロバイダーを記述するリソースを作成します。この権限を使用して OIDC プロバイダーを作成すると、このプロバイダーがプロバイダーと AWS の間に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リスト表示できます。 |
| **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リスト表示できます。 |
| **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アクセス許可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

### 6.1.2. ocm-role IAM ロールの作成

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

**前提条件**

- AWS アカウントがある。
- OpenShift Cluster Manager 組織で Red Hat 組織管理者特権がある。
- AWS アカウント全体のロールをインストールするために必要な権限がある。
- インストールホストに最新の ROSA CLI **rosa** をインストールして設定した。

**手順**

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

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

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

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

このコマンドを使用すると、特定の属性を指定してロールを作成できます。次の出力例は、選択された "自動モード" を示しています。これにより、ROSA CLI (**rosa**) で Operator のロールとポリシーを作成できます。詳細は、「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。以下の例は、作成フローを示しています。

```
I: Creating ocm role
? Role prefix: ManagedOpenShift
? Enable admin capabilities for the OCM role (optional): No
? Permissions boundary ARN (optional):
? Role Path (optional):
? Role creation mode: auto
I: Creating role using 'arn:aws:iam::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes
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
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with
organization '<AWS ARN>'? Yes
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182'
with organization account '<AWS ARN>'
```

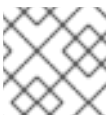
ここでは、以下のようになります。

**Role prefix**

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。

**OCM ロールの管理者機能の有効化 (オプション)**

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。

**パーミッション境界 ARN (オプション)**

アクセス許可境界を設定するためのポリシーの Amazon Resource Name (ARN)。

**ロールのパス (オプション)**

ユーザー名の IAM パスを指定します。

**ロール作成モード**

AWS ロールの作成方法を選択します。**auto** を使用して、ROSA CLI はロールおよびポリシーを生成してリンクします。**auto** モードでは、AWS ロールを作成するためのいくつかの異なるプロンプトが表示されます。

**'ManagedOpenShift-OCM-Role-182' ロールを作成しますか？**

**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。

**OCM Role ARN**

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

**'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' ロールを組織 '<AWS ARN>' にリンクしますか？**

作成したロールを AWS 組織にリンクします。

**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

## 6.2. アカウント全体の IAM ロールとポリシーのリファレンス

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、Red Hat OpenShift Service on AWS のマイナーリリースバージョン (例: Red Hat OpenShift Service on AWS 4) に固有であり、以前のバージョンと互換性があります。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。

### 6.2.1. アカウント全体のロールを作成する方法

Red Hat OpenShift Service on AWS (ROSA) CLI、**rosa**、または OpenShift Cluster Manager の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。ロールは、手動で作成することも、これらのロールと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作成することもできます。

#### 6.2.1.1. 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。

#### 6.2.1.2. 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、この管理 **ocm-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。

**表6.3 ROSA Manage Subscription のポリシーおよびポリシーファイル**

| リソース | 説明 |
|---|---|
| **ROSAManageSubscription** | このポリシーは、必要なアクセス権をパッケージ化することで権限の設定を簡素化し、過剰な権限の付与を防ぎながら、ROSA サブスクリプションに対する適切な制御権をエンティティーに与えます。 |

**表6.4 ROSA インストーラーのロール、ポリシー、およびポリシーファイル**

| リソース | 説明 |
|---|---|
| **HCP-ROSA-Installer-Role** | ROSA インストーラーによって使用される IAM ロール。 |
| ROSAInstallerPolicy | 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。 |
| **HCP-ROSA-Installer-Role** 信頼ポリシー | Red Hat OpenShift Service on AWS クラスターを設定するという目的のためだけに、Red Hat インストーラーに AWS アカウント内で操作する一時的な権限を付与します。 |

**例6.1 sts_hcp_installer_permission_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
```

```
            "ec2:DescribeSecurityGroupRules",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcAttribute",
            "ec2:DescribeVpcs",
            "ec2:DescribeInstanceTypeOfferings",
            "ec2:DescribeCapacityReservations",
            "elasticloadbalancing:DescribeAccountLimits",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:GetOpenIDConnectProvider",
            "iam:GetRole",
            "route53:GetHostedZone",
            "route53:ListHostedZones",
            "route53:ListHostedZonesByName",
            "route53:ListResourceRecordSets",
            "route53:GetAccountLimit",
            "servicequotas:GetServiceQuota"
        ],
        "Resource": "*"
    },
    {
        "Sid": "PassRoleToEC2",
        "Action": [
            "iam:PassRole"
        ],
        "Resource": [
            "arn:*:iam::*:role/*-ROSA-Worker-Role"
        ],
        "Effect": "Allow",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    },
    {
        "Sid": "ManageInstanceProfiles",
        "Effect": "Allow",
        "Action": [
            "iam:AddRoleToInstanceProfile",
            "iam:RemoveRoleFromInstanceProfile",
            "iam:DeleteInstanceProfile",
            "iam:GetInstanceProfile"
        ],
        "Resource": [
            "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
        ]
    },
    {
        "Sid": "CreateInstanceProfiles",
        "Effect": "Allow",
        "Action": [
            "iam:CreateInstanceProfile",
            "iam:TagInstanceProfile"
        ],
```

```
            "Resource": [
                "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "GetSecretValue",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "Route53ManageRecords",
            "Effect": "Allow",
            "Action": [
                "route53:ChangeResourceRecordSets"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringLike": {
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames": [
                        "*.openshiftapps.com",
                        "*.devshift.org",
                        "*.hypershift.local",
                        "*.openshiftusgov.com",
                        "*.devshiftusgov.com"
                    ]
                }
            }
        },
        {
            "Sid": "Route53Manage",
            "Effect": "Allow",
            "Action": [
                "route53:ChangeTagsForResource",
                "route53:CreateHostedZone",
                "route53:DeleteHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateTags",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "RunInstances"
                    ]
                }
            }
        },
        {
            "Sid": "RunInstancesNoCondition",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:snapshot/*"
            ]
        },
        {
            "Sid": "RunInstancesRestrictedRequestTag",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "RunInstancesRedHatOwnedAMIs",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Owner": [
                        "531415883065",
                        "251351625822",
                        "210686502322"
                    ]
```

```
            }
        }
    },
    {
        "Sid": "ManageInstancesRestrictedResourceTag",
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances",
            "ec2:GetConsoleOutput"
        ],
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/red-hat-managed": "true"
            }
        }
    },
    {
        "Sid": "CreateGrantRestrictedResourceTag",
        "Effect": "Allow",
        "Action": [
            "kms:CreateGrant"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/red-hat": "true"
            },
            "StringLike": {
                "kms:ViaService": "ec2.*.amazonaws.com"
            },
            "Bool": {
              "kms:GrantIsForAWSResource": true
            }
        }
    },
    {
        "Sid": "ManagedKMSRestrictedResourceTag",
        "Effect": "Allow",
        "Action": [
            "kms:DescribeKey",
            "kms:GenerateDataKeyWithoutPlaintext"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/red-hat": "true"
            }
        }
    },
    {
        "Sid": "CreateSecurityGroups",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateSecurityGroup"
        ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:security-group*/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "DeleteSecurityGroup",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:security-group*/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "SecurityGroupIngressEgress",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:security-group*/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "CreateSecurityGroupsVPCNoCondition",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ]
        },
        {
            "Sid": "CreateTagsRestrictedActions",
            "Effect": "Allow",
            "Action": [
```

```
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:security-group/*"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction": [
                    "CreateSecurityGroup"
                ]
            }
        }
    },
    {
        "Sid": "CreateTagsK8sSubnet",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:subnet/*"
        ],
        "Condition": {
            "ForAllValues:StringLike": {
                "aws:TagKeys": [
                    "kubernetes.io/cluster/*"
                ]
            }
        }
    },
    {
        "Sid": "DeleteTagsK8sSubnet",
        "Effect": "Allow",
        "Action": [
            "ec2:DeleteTags"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:subnet/*"
        ],
        "Condition": {
            "Null": {
                "aws:TagKeys": "false"
            },
            "ForAllValues:StringLike": {
                "aws:TagKeys": [
                    "kubernetes.io/cluster/*"
                ]
            }
        }
    },
    {
        "Sid": "ListPoliciesAttachedToRoles",
        "Effect": "Allow",
        "Action": [
            "iam:ListAttachedRolePolicies",
            "iam:ListRolePolicies"
```

```
            ],
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

**例6.2 sts_hcp_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"
        }
    ]
}
```

**表6.5 ROSA ワーカーノードのロール、ポリシー、およびポリシーファイル**

| リソース | 説明 |
|---|---|
| **HCP-ROSA-Worker-Role** | 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。 |
| ROSAWorkerInstancePolicy | 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。 |
| **HCP-ROSA-Worker-Role** 信頼ポリシー | ワーカーノード上の重要なソフトウェアに対して、Red Hat がリモートで管理するクラスターのコントロールプレーンにセキュアに接続して通信することを許可します。 |

**例6.3 sts_hcp_worker_instance_permission_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2DescribeInstancesRegions",
            "Effect": "Allow",
            "Action": ["ec2:DescribeInstances", "ec2:DescribeRegions"],
            "Resource": "*"
        },
```

```
        {
            "Sid": "ECRGetAuthorizationToken",
            "Effect": "Allow",
            "Action": ["ecr:GetAuthorizationToken"],
            "Resource": "*"
        },
        {
            "Sid": "ECRReadOnlyAccessRedHatManaged",
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:ListImages",
                "ecr:DescribeImages",
                "ecr:BatchGetImage",
                "ecr:ListTagsForResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

**例6.4 sts_hcp_worker_instance_trust_policy.json**

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

**表6.6 ROSA サポートのロール、ポリシー、およびポリシーファイル**

| リソース | 説明 |
| --- | --- |
| **HCP-ROSA-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。 |

| リソース | 説明 |
| --- | --- |
| ROSASRESupportPolicy | 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。 |
| **HCP-ROSA-Support-Role** 信頼ポリシー | 許可された Red Hat Site Reliability Engineers (SRE) がクラスターで診断およびサポート機能を実行するためのセキュアなメカニズムを提供します。 |

**例6.5 sts_hcp_support_permission_policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Route53",
      "Effect": "Allow",
      "Action": [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "DecribeIAMRoles",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "EC2DescribeInstance",
      "Effect": "Allow",
      "Action": [
```

```
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeIamInstanceProfileAssociations",
      "ec2:DescribeReservedInstances",
      "ec2:DescribeScheduledInstances"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "VPCNetwork",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSubnets",
      "ec2:DescribeRouteTables"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "Cloudtrail",
    "Effect": "Allow",
    "Action": [
      "cloudtrail:DescribeTrails",
      "cloudtrail:LookupEvents"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "Cloudwatch",
    "Effect": "Allow",
    "Action": [
      "cloudwatch:GetMetricData",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:ListMetrics"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "DescribeVolumes",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeVolumes",
      "ec2:DescribeVolumesModifications",
      "ec2:DescribeVolumeStatus"
    ],
    "Resource": [
      "*"
```

```
    ]
  },
  {
    "Sid": "DescribeLoadBalancers",
    "Effect": "Allow",
    "Action": [
      "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"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "DescribeVPC",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeVpcEndpointConnections",
      "ec2:DescribeVpcEndpoints"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "DescribeSecurityGroups",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeSecurityGroupReferences",
      "ec2:DescribeSecurityGroupRules",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeStaleSecurityGroups"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DescribeAddressesAttribute",
    "Effect": "Allow",
    "Action": "ec2:DescribeAddressesAttribute",
    "Resource": "arn:aws:ec2:*:*:elastic-ip/*"
  },
  {
    "Sid": "DescribeInstance",
    "Effect": "Allow",
```

```
      "Action": [
        "iam:GetInstanceProfile"
      ],
      "Resource": "arn:aws:iam::*:instance-profile/*",
      "Condition": {
        "StringEquals": {
            "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "DescribeSpotFleetInstances",
      "Effect": "Allow",
      "Action": "ec2:DescribeSpotFleetInstances",
      "Resource": "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "DescribeVolumeAttribute",
      "Effect": "Allow",
      "Action": "ec2:DescribeVolumeAttribute",
      "Resource": "arn:aws:ec2:*:*:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "ManageInstanceLifecycle",
      "Effect": "Allow",
      "Action": [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    }
  ]
}
```

**例6.6 sts_hcp_support_trust_policy.json**

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::710019948333:role/RH-Technical-Support-15234082"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

**表6.7 ROSA Kube Controller Operator のポリシーおよびポリシーファイル**

| リソース | 説明 |
| --- | --- |
| **openshift-hcp-kube-controller-manager-credentials** | Amazon EC2、Elastic Load Balancing、AWS KMS リソースを管理するための権限を kube コントローラーに付与する IAM ポリシー。 |

**例6.7 openshift-hcp_kube-controller-manager-credentials-policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeLoadBalancerPolicies"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "KMSDescribeKey",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": [
```

```
      "*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/red-hat": "true"
      }
    }
  },
  {
    "Sid": "LoadBalanacerManagement",
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:ConfigureHealthCheck",
      "elasticloadbalancing:CreateLoadBalancerPolicy",
      "elasticloadbalancing:DeleteLoadBalancer",
      "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
      "elasticloadbalancing:ModifyLoadBalancerAttributes",
      "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
      "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "CreateTargetGroup",
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:CreateTargetGroup"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/red-hat-managed": "true"
      }
    }
  },
  {
    "Sid": "LoadBalanacerManagementResourceTag",
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:DeleteListener",
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:ModifyTargetGroup",
      "elasticloadbalancing:DeleteTargetGroup",
      "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
      "elasticloadbalancing:CreateLoadBalancerListeners",
      "elasticloadbalancing:DeleteLoadBalancerListeners",
      "elasticloadbalancing:AttachLoadBalancerToSubnets",
      "elasticloadbalancing:DetachLoadBalancerFromSubnets",
      "elasticloadbalancing:ModifyListener",
      "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
    ],
```

```
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "CreateListeners",
      "Effect": "Allow",
      "Action": [
          "elasticloadbalancing:CreateListener"
      ],
      "Resource": [
          "*"
      ],
      "Condition": {
          "StringEquals": {
              "aws:RequestTag/red-hat-managed": "true",
              "aws:ResourceTag/red-hat-managed": "true"
          }
      }
  },
    {
      "Sid": "CreateSecurityGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "CreateSecurityGroupVpc",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid": "CreateLoadBalancer",
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:CreateLoadBalancer"
      ],
```

```
      "Resource": [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "ModifySecurityGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "CreateTagsSecurityGroups",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateSecurityGroup"
        }
      }
    }
  ]
}
```


表6.8 ROSA Control Plane Operator のポリシーおよびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **openshift-hcp-control-plane-operator-credentials-policy** | Amazon EC2 および Route 53 リソースを管理するために必要な権限を Control Plane Operator に付与する IAM ポリシー。 |

**例6.8 openshift_hcp_control_plane_operator_credentials_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadPermissions",
            "Action": [
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:DescribeSecurityGroups",
                "route53:ListHostedZones"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "CreateSecurityGroups",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:security-group*/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "DeleteSecurityGroup",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:security-group*/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "SecurityGroupIngressEgress",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:security-group*/*"
            ],
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "CreateSecurityGroupsVPCNoCondition",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ]
        },
        {
            "Sid": "ListResourceRecordSets",
            "Action": [
                "route53:ListResourceRecordSets"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "ChangeResourceRecordSetsRestrictedRecordNames",
            "Action": [
                "route53:ChangeResourceRecordSets"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ],
            "Condition": {
                "ForAllValues:StringLike": {
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames": [
                        "*.hypershift.local"
                    ]
                }
            }
        },
        {
            "Sid": "VPCEndpointWithCondition",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/red-hat-managed": "true"
                }
```

```
            }
        },
        {
            "Sid": "VPCEndpointResourceTagCondition",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:security-group*/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "VPCEndpointNoCondition",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:route-table/*"
            ]
        },
        {
            "Sid": "ManageVPCEndpointWithCondition",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        },
        {
            "Sid": "ModifyVPCEndpoingNoCondition",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
```

```
            "Sid": "CreateTagsRestrictedActions",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc-endpoint/*",
                "arn:aws:ec2:*:*:security-group/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateVpcEndpoint",
                        "CreateSecurityGroup"
                    ]
                }
            }
        }
    ]
}
```

表6.9 ROSA Node Pool Management Operator のポリシーおよびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **openshift-hcp-capa-controller-manager-credentials-policy** | ワーカーノードとして管理される Amazon EC2 インスタンスの情報取得、実行、終了を行うために必要な権限を NodePool コントローラーに付与する IAM ポリシー。このポリシーは、AWS KMS キーを使用したワーカーノードのルートボリュームのディスク暗号化を許可する権限と、ワーカーノードに接続されている Elastic Network Interface にタグを付ける権限も付与します。 |

例6.9 **openshift_hcp_capa_controller_manager_credentials_policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadPermissions",
      "Action": [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect": "Allow",
      "Resource": [
```

```
        "*"
      ]
    },
    {
      "Sid": "CreateServiceLinkedRole",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:*:iam::*:role/aws-service-
role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid": "PassWorkerRole",
      "Action": [
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": [
              "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "NetworkInterfaces",
      "Effect": "Allow",
      "Action": [
```

```
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/red-hat-managed": "true"
      }
    }
  },
  {
    "Sid": "NetworkInterfacesNoCondition",
    "Effect": "Allow",
    "Action": [
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:vpc/*"
    ]
  },
  {
    "Sid": "TerminateInstances",
    "Effect": "Allow",
    "Action": [
      "ec2:TerminateInstances"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/red-hat-managed": "true"
      }
    }
  },
  {
    "Sid": "CreateTags",
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition": {
      "StringEquals": {
          "ec2:CreateAction": [
              "RunInstances"
          ]
      }
    }
```

```
    },
    {
      "Sid": "CreateTagsCAPAControllerReconcileNetworkInterface",
      "Effect": "Allow",
      "Action": [
          "ec2:CreateTags"
      ],
      "Resource": [
          "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition": {
        "StringEquals": {
            "aws:RequestTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "CreateTagsCAPAControllerReconcileInstance",
      "Effect": "Allow",
      "Action": [
          "ec2:CreateTags"
      ],
      "Resource": [
          "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
          "StringEquals": {
              "aws:ResourceTag/red-hat-managed": "true"
          }
      }
    },
    {
      "Sid": "CreateTagsCAPAControllerReconcileVolume",
      "Effect": "Allow",
      "Action": [
          "ec2:CreateTags"
      ],
      "Resource": [
          "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
          "StringEquals": {
              "aws:RequestTag/red-hat-managed": "true"
          }
      }
    },
    {
      "Sid": "RunInstancesRequest",
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
```

```
      "StringEquals": {
        "aws:RequestTag/red-hat-managed": "true"
      }
    }
  },
  {
    "Sid": "RunInstancesNoCondition",
    "Effect": "Allow",
    "Action": [
      "ec2:RunInstances"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:capacity-reservation/*"
    ]
  },
  {
    "Sid": "RunInstancesRedHatAMI",
    "Effect": "Allow",
    "Action": [
      "ec2:RunInstances"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:image/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:Owner": [
          "531415883065",
          "251351625822"
        ]
      }
    }
  },
  {
    "Sid": "ManagedKMSRestrictedResourceTag",
    "Effect": "Allow",
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "aws:ResourceTag/red-hat": "true"
      }
    }
  },
  {
    "Sid": "CreateGrantRestricted",
    "Effect": "Allow",
    "Action": [
      "kms:CreateGrant"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        },
        "StringEquals": {
          "aws:ResourceTag/red-hat": "true"
        },
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

表6.10 ROSA Image Registry Operator のポリシーおよびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **openshift-hcp-image-registry-operator-permission-policy** | ROSA クラスター内のイメージレジストリーと依存サービス (S3 を含む) のリソースをプロビジョニングおよび管理するために必要な権限を Image Registry Operator に付与する IAM ポリシー。これは、Operator が ROSA クラスターの内部レジストリーをインストールおよび保守できるようにするために必要です。 |

例6.10 **openshift_hcp_image_registry_operator_permission_policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListBuckets",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowSpecificBucketActions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
```

```
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
      ]
    },
    {
      "Sid": "AllowSpecificObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
  ]
}
```

**表6.11 ROSA Amazon EBSCI Driver Operator のポリシーおよびポリシーファイル**

| リソース | 説明 |
|---|---|
| **openshift-hcp-cluster-csi-driver-ebs-operator-cloud-credentials-policy** | ROSA クラスターに Amazon EBS CSI ドライバーをインストールおよび保守するために必要な権限を Amazon EBS CSI Driver Operator に付与する IAM ポリシー。 |

**例6.11 openshift_hcp_cluster_csi_driver_ebs_operator_cloud_credentials_policy.json**

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

```
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVolume"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/red-hat-managed": "true"
        }
      }
    },
    {
      "Sid": "CreateVolumeFromSnapshot",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVolume"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
```

```
    "Sid": "CreateSnapshotResourceTag",
    "Effect": "Allow",
    "Action": [
      "ec2:CreateSnapshot"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/red-hat-managed": "true"
      }
    }
  },
  {
    "Sid": "CreateSnapshotRequestTag",
    "Effect": "Allow",
    "Action": [
      "ec2:CreateSnapshot"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/red-hat-managed": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DeleteSnapshot"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/red-hat-managed": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": [
          "CreateVolume",
```

```
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

表6.12 ROSA Cloud Network Config Operator のポリシーおよびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **openshift-hcp-cloud-network-config-cloud-credentials-permission-policy** | ROSA クラスターに Amazon EBS CSI ドライバーをインストールおよび保守するために必要な権限を Amazon EBS CSI Driver Operator に付与する IAM ポリシー。 |

例6.12 **openshift_hcp_cloud_network_config_cloud_credentials_permission_policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceStatus",
            "ec2:DescribeInstanceTypes",
            "ec2:DescribeSubnets",
            "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
            "ec2:UnassignPrivateIpAddresses",
            "ec2:AssignPrivateIpAddresses",
            "ec2:UnassignIpv6Addresses",
            "ec2:AssignIpv6Addresses"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/red-hat-managed": "true"
        }
      }
    }
  ]
}
```

表6.13 ROSA Ingress Operator のポリシーおよびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **openshift-hcp-cluster-ingress-operator-cloud-credentials-policy** | クラスターへの外部アクセスを管理するために必要な権限を ROSA Ingress Operator に提供する IAM ポリシー。 |

例6.13 **openshift_hcp_cluster_ingress_operator_cloud_credentials_policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "route53:ChangeResourceRecordSets"
        ],
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringLike": {
                "route53:ChangeResourceRecordSetsNormalizedRecordNames": [
                  "*.openshiftapps.com",
                  "*.devshift.org",
                  "*.openshiftusgov.com",
                  "*.devshiftusgov.com"
                ]
            }
        }
    }
  ]
}
```

表6.14 ROSA KMS Provider Operator のポリシーおよびポリシーファイル

| リソース | 説明 |
| --- | --- |
| **openshift-hcp-kms-provider-credential-policy.** | etcd データ暗号化をサポートする AWS KMS キーを管理するために必要な権限を組み込みの AWS Encryption Provider に付与する IAM ポリシー。このポリシーは、AWS Encryption Provider が提供する KMS キーを使用して etcd データを暗号化および復号することを Amazon EC2 に許可します。 |

**例6.14 openshift_hcp_kms_provider_credential_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "VolumeEncryption",
        "Effect": "Allow",
        "Action": [
          "kms:Encrypt",
          "kms:Decrypt",
          "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
          "StringEquals": {
            "aws:ResourceTag/red-hat": "true"
          }
        }
      }
    ]
}
```

**関連情報**

- HCP を備えた ROSA の更新ライフサイクル

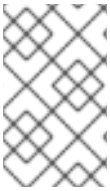
### 6.2.2. アカウント全体の IAM ロールおよびポリシー AWS CLI リファレンス

このセクションでは、**rosa** コマンドが端末で生成する **aws** CLI コマンドをリスト表示します。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。

#### 6.2.2.1. 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。このプロセスは次のコマンドで開始します。**<openshift_version>** は、Red Hat OpenShift Service on AWS (ROSA) のバージョン (**4** など) を指します。

```
$ 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 \
```

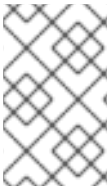
```
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=rosa_role_type,Value=installer

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=<openshift_version>
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=<openshift_version>
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=<openshift_version>
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=<openshift_version>
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=<openshift_version>
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=<openshift_version>
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=<openshift_version>
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=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=operator_namespace,Value=openshift-image-
registry Key=operator_name,Value=installer-cloud-credentials
```

#### 6.2.2.2. 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、Red Hat OpenShift Service on AWS (ROSA) CLI ( **rosa**) はロールと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
```

**関連情報**

- AWS documentation about permissions boundaries for IAM entities
- アカウント全体のロールとポリシーの作成

## 6.3. クラスター固有の OPERATOR IAM ロール参照

Operator ロールは、バックエンドストレージ、クラウド Ingress コントローラー、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権限を取得するために使用されます。

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。AWS が管理する Operator ポリシーは、AWS IAM でバージョン管理されます。最新バージョンの AWS 管理ポリシーが常に使用されるため、ROSA with HCP で使用される AWS 管理ポリシーのアップグレードを管理したりスケジュールしたりする必要はありません。

**注記**

Operator ロールに一致するポリシーがアカウントに複数ある場合は、ロールの作成時に選択肢のリストが表示されます。

**表6.15 ROSA with HCP に必要な Operator ロールと AWS 管理ポリシー**

| ロール名 | AWS 管理ポリシー名 | ロールの説明 |
|---|---|---|
| **openshift-cloud-network-config-controller-credentials** | **ROSACloudNetworkConfigOperatorPolicy** | クラスターのクラウドネットワーク認証情報を管理するために、クラウドネットワーク設定コントローラーが必要とする IAM ロール。 |
| **openshift-image-registry-installer-cloud-credentials** | **ROSAImageRegistryOperatorPolicy** | ROSA Image Registry Operator がクラスターの AWS S3 内の OpenShift イメージレジストリーストレージを管理するために必要な IAM ロール。 |
| **kube-system-kube-controller-manager** | **ROSAKubeControllerPolicy** | HCP クラスター上の OpenShift の管理に必要な IAM ロール。 |

| ロール名 | AWS 管理ポリシー名 | ロールの説明 |
| --- | --- | --- |
| **kube-system-capa-controller-manager** | **ROSANodePoolManagementPolicy** | HCP クラスター上のノードの管理に必要な IAM ロール。 |
| **kube-system-control-plane-operator** | **ROSAControlPlaneOperatorPolicy** | HCP クラスター上のコントロールプレーンの管理に必要な IAM ロール。 |
| **kube-system-kms-provider** | **ROSAKMSProviderPolicy** | HCP クラスター上の OpenShift の管理に必要な IAM ロール。 |
| **openshift-ingress-operator-cloud-credentials** | **ROSAIngressOperatorPolicy** | 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。 |
| **openshift-cluster-csi-drivers-ebs-cloud-credentials** | **ROSAAmazonEBSCSIDriverOperatorPolicy** | 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。 |

### 6.3.1. 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 コマンドをリスト表示します。

```
$ 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=<openshift_version>
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=<openshift_version>
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=<openshift_version>
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=<openshift_version>
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=<openshift_version>
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。

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

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 Ingress Cloud Credentials Operator IAM ロールのデフォルト名は、**mycluster-<hash>-openshift-ingress-operator-cloud-credentials** です。**<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は、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 Ingress Cloud Credentials Operator ロールの名前は、**mycluster-dev-openshift-ingress-operator-cloud-credenti** です。

**注記**

ロール名は 64 文字に切り捨てられます。

## 6.4. OPERATOR 認証のための OPEN ID CONNECT (OIDC) 要件

STS を使用する ROSA インストールの場合は、クラスター Operator が認証するために使用するクラスター固有の OIDC プロバイダーを作成するか、独自の OIDC プロバイダー用に独自の OIDC 設定を作成する必要があります。

### 6.4.1. CLI を使用した OIDC プロバイダーの作成

Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) を使用して、AWS アカウントでホストされる OIDC プロバイダーを作成できます。

**前提条件**

- ROSA CLI の最新バージョンがインストールされている。

**手順**

- 未登録または登録済みの OIDC 設定を使用して OIDC プロバイダーを作成する方法
  - 未登録の OIDC 設定では、クラスターを通じて OIDC プロバイダーを作成する必要があります。次のコマンドを実行して OIDC プロバイダーを作成します。

```
$ 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://oidc.op1.openshiftapps.com/<oidc_config_id> \ 1
 --client-id-list openshift sts.<aws_region>.amazonaws.com \
 --thumbprint-list <thumbprint> 2
```

1 クラスターの作成後に OpenID Connect (OIDC) アイデンティティープロバイダーにアクセスするために使用する URL。

2 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) 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の詳細は、AWS ドキュメント を参照してください。

- 登録された OIDC 設定は、OIDC 設定 ID を使用します。OIDC 設定 ID を指定して次のコマンドを実行します。

```
$ rosa create oidc-provider --oidc-config-id <oidc_config_id> --mode auto -y
```

**コマンド出力**

```
I: Creating OIDC provider using 'arn:aws:iam::4540112244:user/userName'
I: Created OIDC provider with ARN 'arn:aws:iam::4540112244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/241rh9ql5gpu99d7leokhvkp8icnalpf'
```

## 6.4.2. OpenID Connect 設定の作成

Red Hat がホストするクラスターを使用する場合は、Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) を使用して、マネージドまたはアンマネージド OpenID Connect (OIDC) 設定を作成できます。マネージド OIDC 設定は Red Hat の AWS アカウント内に保存されますが、生成されたアンマネージド OIDC 設定は AWS アカウント内に保存されます。OIDC 設定は、OpenShift Cluster Manager で使用するために登録されています。アンマネージド OIDC 設定を作成する場合、CLI は秘密キーを提供します。

### 6.4.2.1. OpenID Connect 設定の作成

Red Hat OpenShift Service on AWS クラスターを作成する際に、クラスターを作成する前に OpenID Connect (OIDC) 設定を作成できます。この設定は、OpenShift Cluster Manager で使用するために登録されています。

**前提条件**

- Red Hat OpenShift Service on AWS の AWS 前提条件を満たしている。
- インストールホストに最新の ROSA コマンドラインインターフェイス (CLI) (**rosa**) をインストールして設定した。

**手順**

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

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

このコマンドは次の情報を返します。

以下に例を示します。

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

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

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

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

**<oidc_config_id>**

この出力例では、OIDC 設定 ID は **13cdr6b** です。

- 次のコマンドを実行して、変数の値を表示します。

```
$ echo $OIDC_ID
```

以下に例を示します。

```
13cdr6b
```

**検証**

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

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

以下に例を示します。

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

#### 6.4.2.2. 独自の OpenID Connect 設定を作成するためのパラメーターオプション

次のオプションを **rosa create oidc-config** コマンドに追加できます。これらのパラメーターはすべてオプションです。パラメーターを指定せずに **rosa create oidc-config** コマンドを実行すると、アンマネージドの OIDC 設定が作成されます。

**注記**

OpenShift Cluster Manager を通じて **/oidc_configs** にリクエストを送信して、アンマネージド OIDC 設定を登録する必要があります。応答で ID を受け取ります。この ID を使用してクラスターを作成します。

##### 6.4.2.2.1. 生ファイル

RSA 秘密キーの生ファイルを提供できます。このキーの名前は **rosa-private-key-oidc-<random_label_of_length_4>.key** です。また、**discovery-document-oidc-<random_label_of_length_4>.json** という名前の検出ドキュメントと、**jwks-oidc-<random_label_of_length_4>.json** という名前の JSON Web キーセットも受け取ります。

これらのファイルを使用してエンドポイントを設定します。このエンドポイントは、**/.well-known/openid-configuration** に対して検出ドキュメントで応答し、**keys.json** に対して JSON Web キーセットで応答します。秘密キーは、Amazon Web Services (AWS) Secrets Manager Service (SMS) に平文として保存されます。

**例**

```
$ rosa create oidc-config --raw-files
```

##### 6.4.2.2.2. モード

OIDC 設定を作成するモードを指定できます。**manual** オプションを使用すると、S3 バケット内で OIDC 設定をセットアップする AWS コマンドを受け取ります。このオプションでは、秘密キーを Secrets Manager に保存します。**manual** オプションの場合、OIDC エンドポイント URL は S3 バケットの URL になります。OIDC 設定を OpenShift Cluster Manager に登録するには、Secrets Manager ARN を取得する必要があります。

**auto** オプションを使用すると、**manual** モードと同じ OIDC 設定と AWS リソースを受け取ります。2 つのオプションの大きな違いは、**auto** オプションを使用すると ROSA が AWS を呼び出すため、それ以上のアクションを行う必要がないことです。OIDC エンドポイント URL は、S3 バケットの URL です。CLI は Secrets Manager ARN を取得し、OIDC 設定を OpenShift Cluster Manager に登録し、ユーザーが STS クラスターの作成を続行するために実行できる 2 番目の **rosa** コマンドを報告します。

**例**

```
$ rosa create oidc-config --mode=<auto|manual>
```

#### 6.4.2.2.3. managed

Red Hat の AWS アカウントでホストされる OIDC 設定を作成します。このコマンドは、STS クラスターの作成時に使用する OIDC 設定 ID で直接応答する秘密キーを作成します。

**例**

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

**出力例**

```
W: For a managed OIDC Config only auto mode is supported. However, you may choose the
provider creation mode
? OIDC Provider creation mode: auto
I: Setting up managed OIDC configuration
I: Please run the following command to create a cluster with this oidc config
rosa create cluster --sts --oidc-config-id 233jnu62i9aphpucsj9kueqlkr1vcgra
I: Creating OIDC provider using 'arn:aws:iam::242819244:user/userName'
? Create the OIDC provider? Yes
I: Created OIDC provider with ARN 'arn:aws:iam::242819244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/233jnu62i9aphpucsj9kueqlkr1vcgra'
```

## 6.5. SERVICE CONTROL POLICY (SCP) の有効なパーミッションの最小セット

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

**注記**

AWS Security Token Service (STS) を使用する場合は、Service Control Policy が次のリソースをブロックしないようにする必要があります。

- **ec2:{}**
- **iam:{}**
- **tag:***

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

| | Service | アクション | 効果 |
|---|---|---|---|
| 必須 | Amazon EC2 | すべて | 許可 |

| | Service | アクション | 効果 |
|---|---|---|---|
| | Amazon EC2 Auto Scaling | すべて | 許可 |
| | Amazon S3 | すべて | 許可 |
| | アイデンティティーおよびアクセス管理 | すべて | 許可 |
| | Elastic Load Balancing | すべて | 許可 |
| | Elastic Load Balancing V2 | すべて | 許可 |
| | Amazon CloudWatch | すべて | 許可 |
| | Amazon CloudWatch Events | すべて | 許可 |
| | Amazon CloudWatch Logs | すべて | 許可 |
| | AWS EC2 Instance Connect | SendSerialConsoleSSHPublicKey | 許可 |
| | AWS Support | すべて | 許可 |
| | AWS Key Management Service | すべて | 許可 |
| | AWS Security Token Service | すべて | 許可 |
| | AWS Tiro | CreateQuery<br>GetQueryAnswer<br>GetQueryExplanation | 許可 |
| | AWS Marketplace | サブスクライブ<br>サブスクライブ解除<br>サブスクリプションの表示 | 許可 |
| | AWS Resource Tagging | すべて | 許可 |
| | AWS Route53 DNS | すべて | 許可 |

| | Service | アクション | 効果 |
|---|---|---|---|
| | AWS Service Quotas | ListServices<br>GetRequestedServiceQuotaChange<br>GetServiceQuota<br>RequestServiceQuotaIncrease<br>ListServiceQuotas | 許可 |
| 任意 | AWS Billing | ViewAccount<br>Viewbilling<br>ViewUsage | 許可 |
| | AWS Cost and Usage Report | すべて | 許可 |
| | AWS Cost Explorer Services | すべて | 許可 |

**関連情報**

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

## 6.6. 顧客管理のポリシー

Red Hat OpenShift Service on AWS (ROSA) ユーザーは、ROSA クラスターの実行と保守に必要な IAM ロールに顧客管理ポリシーを割り当てることができます。この機能は、AWS IAM ロールでは珍しいことではありません。これらのポリシーを ROSA 固有の IAM ロールにアタッチする機能により、ROSA クラスターのアクセス許可機能が拡張されます。たとえば、クラスターコンポーネントが、ROSA 固有の IAM ポリシーの一部ではない追加の AWS リソースにアクセスできるようにすることができます。

顧客管理ポリシーに依存する重要な顧客アプリケーションがクラスターまたはロールのアップグレード中に変更されないようにするために、ROSA は、**ListAttachedRolesPolicies** 権限を使用してロールから権限ポリシーのリストを取得し、**ListRolePolicies** 権限を使用して ROSA 固有のロールからポリシーのリストを取得します。この情報により、クラスターイベント中に顧客管理ポリシーが影響を受けないようになり、Red Hat SRE は ROSA 固有の IAM ロールに関連付けられた ROSA および顧客管理ポリシーの両方を監視できるようになり、クラスターの問題をより効果的にトラブルシューティング機能が向上します。

**警告**

ROSA 固有のポリシーを制限する IAM ロールにアクセス許可境界ポリシーをアタッチすることはサポートされていません。これらのポリシーにより、ROSA クラスターを正常に実行および維持するために必要な基本的なアクセス許可の機能が中断される可能性があるためです。ROSA (クラシックアーキテクチャー) インストーラーロールには、アクセス許可境界ポリシーが用意されています。詳細は、関連情報セクションを参照してください。

**関連情報**

- Permissions boundaries for IAM entities