Red Hat OpenShift Service on AWS 4

ROSA について

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

Last Updated: 2024-09-17

Red Hat OpenShift Service on AWS 4 ROSA について

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

法律上の通知

概要

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

目次

第1章 ROSA の理解

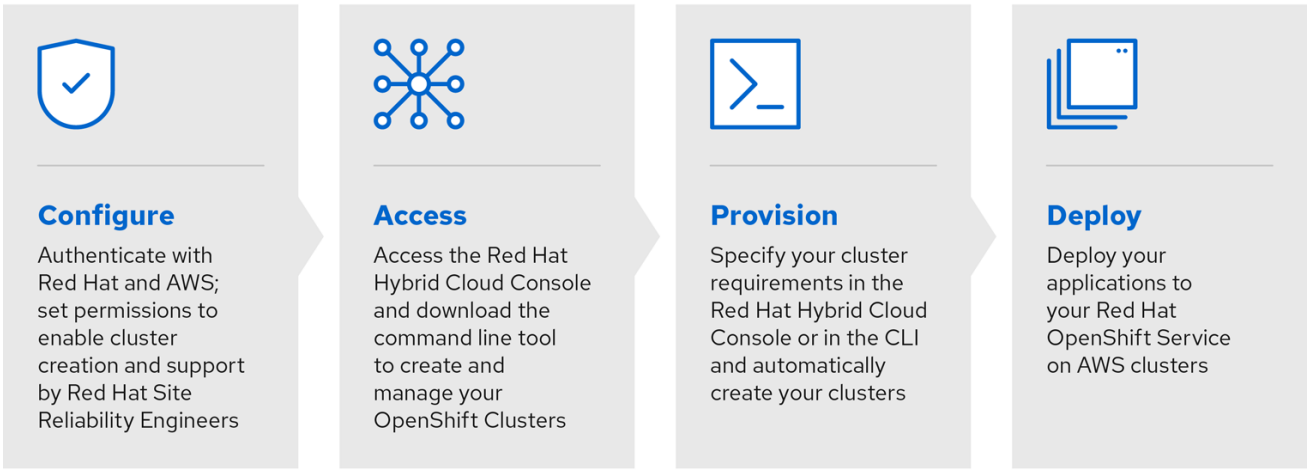
Red Hat OpenShift Service on AWS (ROSA)、Red Hat OpenShift Cluster Manager とコマンドラインインターフェイス (CLI) ツールを使用して ROSA と対話する方法、使用エクスペリエンス、Amazon Web Services (AWS) サービスとの統合を説明します。

1.1. ROSA について

ROSA は、フルマネージドのターンキーアプリケーションプラットフォームであり、アプリケーションを構築してデプロイすることにより、お客様に価値を提供することに集中できます。Red Hat Site Reliability Engineering (SRE) のエキスパートが基盤となるプラットフォームを管理するため、インフラストラクチャー管理の複雑さを心配する必要はありません。ROSA は、Amazon CloudWatch、AWS Identity and Access Management (IAM)、Amazon Virtual Private Cloud (VPC)、およびその他の幅広い AWS サービスとのシームレスな統合を提供し、顧客に対する差別化されたエクスペリエンスの構築と提供をさらに加速します。

AWS アカウントから直接サービス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。ROSA では、バージョンの整合性を確保するために、Red Hat OpenShift Dedicated および OpenShift Container Platform と同じバージョンの OpenShift をサポートします。



ROSA のインストールの詳細は、Red Hat OpenShift Service on AWS (ROSA) のインストールのインタラクティブな説明 を参照してください。

1.2. 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。

1.3. スタートガイド

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

関連情報

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

第2章 ポリシーおよびサービス定義

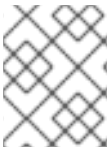
2.1. RED HAT OPENSHIFT SERVICE ON AWS のサポート

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

2.1.1. 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 Site Reliability Engineering (SRE) によるサポートと、複数のアベイラビリティゾーンクラスターをデプロイする方法をさらに備えており、多くの一般的な Kubernetes の問題からの保護を強化できますが、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は多数あります。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。



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。

2.1.1.1. 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ドレイン (解放) などの操作時に Pod への安全面の各種の制約を指定できます。

2.1.1.2. ワーカーノードの障害

ワーカーノードは、アプリケーション Pod が含まれる仮想マシンです。デフォルトで、ROSA クラスターには単一アベイラビリティーゾーンのクラスター用のワーカーノードが 2 つ以上含まれます。ワーカーノードに障害が発生した場合、Pod は、既存ノードに関する問題が解決するか、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。

2.1.1.3. クラスターの障害

シングル AZ ROSA クラスターには、プライベートサブネット内の同じアベイラビリティゾーン (AZ) に少なくとも 3 つのコントロールプレーンと 2 つのインフラストラクチャーノードがあります。

マルチ AZ ROSA クラスターには、選択したクラスターのタイプに応じて、少なくとも 3 つのコントロールプレーンノードと 3 つのインフラストラクチャーノードがあり、高可用性のために事前設定されています。コントロールプレーンおよびインフラストラクチャーノードはワーカーノードと同じ耐障害性があり、この場合は Red Hat によって完全に管理される利点を活用できます。

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

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

2.1.1.4. ゾーンの障害

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

2.1.1.5. ストレージの障害

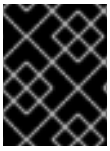
ステートフルなアプリケーションをデプロイしている場合、ストレージは重要なコンポーネントであり、高可用性を検討する際に考慮に入れる必要があります。単一ブロックストレージ PV は、Pod レベルでも停止状態になった状態では実行できません。ストレージの可用性を維持する最適な方法として、複製されたストレージソリューション、停止による影響を受けない共有ストレージ、またはクラスターから独立したデータベースサービスを使用できます。

2.2. 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 (ROSA) 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。

2.2.1. 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
ロギング	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
Cluster networking	Red Hat [1]	Red Hat およびお客様 [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

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
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
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
Capacity management	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、責任はお客様へと移行します。

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。

関連情報

- AWS ファイアウォールの前提条件

2.2.2. 領域ごとの責任共有のタスク

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。

2.2.3. 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。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。

2.2.3.1. 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 SRE によってすぐに解決される軽微で一時的な問題については、クラスター通知は送信されません。

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。

2.2.4. 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** ● 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。 ● 停止を Red Hat と AWS に報告します。
Cluster networking	**Red Hat** ● 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の接続、およびデフォルトの Ingress コントローラーに関連するインシデントの監視、アラート、および対処します。	● オプションの Ingress コントローラー、OperatorHub を介し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応します。

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** ● 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。 ● 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** ● 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。 ● 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。
プラットフォームモニタリング	**Red Hat** ● 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** ● 既知のインシデントを提起して管理します。 ● 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。

リソース	サービスの責任	お客様の責任
インフラストラクチャーとデータの回復力	**Red Hat** ● 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。 ● 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。 ● 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** ● 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。 ● 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。	
AWS ソフトウェア (パブリック AWS サービス)	**AWS** ● 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。 ● 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** ● 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。

2.2.4.1. プラットフォームモニタリング

プラットフォーム監査ログは、一元化された SIEM (security information and event monitoring) システムに安全に転送されます。これにより、SRE チームに対して設定されたアラートがトリガーされる場合は手動によるレビューの対象となります。監査ログは SIEM システムに 1 年間保持されます。指定され

たクラスターの監査ログは、クラスターの削除時に削除されません。

2.2.4.2. 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 (担当者) が割り当てられます。
3. インシデントのリードは、関連する通知やサポートケースの更新など、リカバリーに関するすべての通信および調整を管理します。
4. インシデントの復旧が行われます。
5. インシデントが文書化され、Root Cause Analysis (根本原因分析 (RCA)) がインシデント発生後 5 営業日以内に実行されます。
6. RCA のドラフト文書は、インシデント発生後 7 日以内にお客様に共有されます。

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

2.2.4.3. 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。

2.2.5. 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。

2.2.5.1. 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
- ID プロバイダーの追加、変更、または削除
- 昇格されたグループからのユーザーの追加、変更、または削除
- アドオンのインストールまたは削除
- クラスターネットワーク設定の変更
- マシンプールの追加、変更、または削除
- ユーザーワークロードの監視の有効化または無効化
- アップグレードの開始

重要

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

2.2.5.2. 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ます。

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

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

2.2.5.3. 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。

2.2.5.4. 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

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

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

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
ロギング	**Red Hat** ● 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。 ● 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。 ● 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。 ● 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。 ● 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。 ● 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。
アプリケーションのネットワーク	**Red Hat** ● 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。 ● 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。 ● デフォルトの内部 Pod トラフィック (バージョン 4.11 より前に作成されたクラスターの場合) 用に OpenShift SDN コンポーネントをインストール、設定、および保守します。 ● 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。 ● 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。 ● 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。 ● 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。 ● 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
Cluster networking	**Red Hat** ● 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。 ● ワーカー、インフラストラクチャー、およびコントロールプレーンノード間の内部クラスター通信に必要な内部ネットワークコンポーネントを設定します。	● クラスター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。 ● 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。 ● 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。 ● 追加の Ingress コントローラーを作成して、追加のアプリケーションルートを公開します。 ● 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、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** ● 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。 ● 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。 ● 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。 ● 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** ● 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。 ● 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。 ● 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** ● 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。 ● 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。 ● 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。 ● 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。 ● 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
Capacity management	**Red Hat** ● コントロールプレーンの使用を監視します。コントロールプレーンには、コントロールプレーンノードとインフラストラクチャーノードが含まれます。 ● QoS (Quality of Service) を維持するために、コントロールプレーンノードをスケーリングし、サイズ変更します。	● ワーカーノードの使用率を監視し、必要に応じて自動スケーリング機能を有効にします。 ● 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。 ● 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。 ● 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** ● 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。 ● 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。 ● 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。	● 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** **Compute:** ROSA コントロールプレーン、インフラストラクチャー、ワーカーノードに使用される Amazon EC2 サービスを提供します。 **Storage:** ROSA がクラスターに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できるようにするために使用される Amazon EBS を提供します。 **Storage:** ROSA サービスの組み込みイメージレジストリーに Amazon S3 を提供します。 **Networking:** ROSA 仮想ネットワーキングインフラストラクチャーのニーズを満たすために、次の AWS Cloud サービスを提供します。 ● Amazon VPC ● Elastic Load Balancing ● AWS IAM **Networking:** 次の AWS サービスを提供します。これは、オプションで ROSA と統合できます。 ● AWS VPN ● AWS Direct Connect ● AWS PrivateLink ● 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。 ● 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。 ● 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** ● 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。 ● 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。

関連情報

- AWS ファイアウォールの前提条件

2.2.6. 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
ロギング	**Red Hat** ● セキュリティーイベントについて分析するために、クラスターの監査ログを Red Hat SIEM に送信します。フォレンジック分析をサポートするために、定義された期間の監査ログを保持します。	● セキュリティーイベントのアプリケーションログを分析します。 ● デフォルトのロギングスタックで指定されるよりも長い保持期間が必要な場合に、ロギングサイドカーコンテナーまたはサードパーティーのロギングアプリケーション経由でアプリケーションログを外部エンドポイントに送信します。
仮想ネットワーク管理	**Red Hat** ● 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。 ● 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。 ● 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** ● 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。 ● 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。 ● 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。 ● 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。 ● 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。 ● 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。 ● 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。 ● 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。 ● 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** ● 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。 ● 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。 ● 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** **Compute:** ROSA コントロールプレーン、インフラストラクチャー、ワーカーノードに使用される安全な Amazon EC2。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。 **Storage:** ROSA コントロールプレーン、インフラストラクチャー、ワーカーノードボリューム、および Kubernetes 永続ボリュームに使用されるセキュアな Amazon Elastic Block Store (EBS)。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。 **Storage:** ROSA がコントロールプレーン、インフラストラクチャー、ワーカーノードのボリューム、および永続ボリュームを暗号化するために使用する AWS KMS を提供します。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。 **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。 **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 の安全な施設間の 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。 - 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。 - 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。 - 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。 - 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** ● 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。 ● 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。 ● 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。

関連情報

- お客様や責任共有の詳細は、ROSA のセキュリティー に関する文書を参照してください。

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

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

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

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

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** ● プラットフォームが機能するために必要な、影響を受けた仮想ネットワークコンポーネントを復元するか、再作成します。	● パブリッククラウドプロバイダーが推奨されるように、障害に対する保護のために、可能な場合は複数のトンネルで仮想ネットワーク接続を設定します。 ● 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** ● IAM ユーザー認証情報を使用して作成された ROSA クラスターの場合は、時間ごと、日ごと、週ごとのボリュームスナップショットを通じて、クラスター上のすべての Kubernetes オブジェクトをバックアップします。1時間ごとのバックアップは 24 時間 (1 日) 保持され、毎日のバックアップは 168 時間 (1 週間) 保持され、毎週のバックアップは 720 時間 (30 日間) 保持されます。	● 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** ● クラスターを監視し、障害が発生した Amazon EC2 コントロールプレーンまたはインフラストラクチャーノードを交換します。 ● 障害が発生したワーカーノードを手動または自動で交換できる機能を顧客に提供します。	● 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。

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** **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。 **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。 **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。 **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。	• ROSA マルチ AZ クラスターを設定して、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ます。 • 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。 • 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。
ハードウェア/AWS グローバルインフラストラクチャー	**AWS** • ROSA がアベイラビリティーゾーン全体でコントロールプレーン、インフラストラクチャー、ワーカーノードを拡張できるようにする 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。 • 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。	• ROSA マルチ AZ クラスターを設定して、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ます。

関連情報

- マシンプールについて

2.2.8. 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
お客様データ	**Red Hat** ● 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。 ● 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。 ● 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。 **AWS** ● 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** ● 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。 ● 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。 ● 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。 ● 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。 ● お客様がクラスター上にアプリケーションコンテナーイメージを安全に保存し、アプリケーションをデプロイおよび管理できるようにコンテナーイメージレジストリーを提供します。 **AWS** ● 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。 ● 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。 ● 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。 ● 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。 ● 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、メトリックの収集、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のためのソフトウェアのインストールと操作が含まれます。

2.2.9. 関連情報

- Red Hat Site Reliability Engineering (SRE) チームによるアクセスの詳細は、アイデンティティーおよびアクセス管理 を参照してください。

2.3. 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 (ROSA) マネージドサービスのサービス定義を説明します。

2.3.1. 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。

2.3.1.1. 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。

2.3.1.2. 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

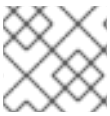
- Red Hat Operator のサポート
- PID 制限の設定

2.3.1.3. インスタンスタイプ

サポートされているインスタンスタイプの詳細は、Red Hat OpenShift Service on AWS インスタンスタイプ を参照してください。

2.3.1.4. リージョンおよびアベイラビリティーゾーン

現在、以下の AWS リージョンが Red Hat OpenShift 4 で利用可能であり、Red Hat OpenShift Service on AWS でサポートされています。



注記

OpenShift 4 のサポートの有無にかかわらず、中国リージョンはサポートされません。

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。

GovCloud (US) リージョンは、ROSA Classic クラスターでのみサポートされます。

例2.1 AWS リージョン

- us-east-1 (N. Virginia)
- us-east-2 (Ohio)
- us-west-1 (N. California)
- us-west-2 (Oregon)
- af-south-1 (Cape Town、AWS オプトインが必要)
- ap-east-1 (Hong Kong、AWS オプトインが必要)
- ap-south-2 (Hyderabad、AWS オプトインが必要)
- ap-southeast-3 (Jakarta、AWS オプトインが必要)
- ap-southeast-4 (Melbourne、AWS オプトインが必要)
- ap-south-1 (Mumbai)
- ap-northeast-3 (Osaka)
- ap-northeast-2 (Seoul)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ap-northeast-1 (Tokyo)
- ca-central-1 (Central Canada)
- eu-central-1 (Frankfurt)
- eu-north-1 (Stockholm)
- eu-west-1 (Ireland)

- eu-west-2 (London)
- eu-south-1 (Milan、AWS オプトインが必要)
- eu-west-3 (Paris)
- eu-south-2 (Spain)
- eu-central-2 (Zurich、AWS オプトインが必要)
- me-south-1 (Bahrain、AWS オプトインが必要)
- me-central-1 (UAE、AWS オプトインが必要)
- sa-east-1 (São Paulo)
- us-gov-east-1 (AWS GovCloud - 米国東部)
- us-gov-west-1 (AWS GovCloud - 米国西部)

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

新規 Red Hat OpenShift Service on AWS クラスターはそれぞれ、インストーラーで作成された Virtual Private Cloud (VPC)、または既存の Virtual Private Cloud (VPC) 内にインストールされます。オプションとして、単一アベイラビリティーゾーン (Single-AZ) または複数アベイラビリティーゾーン (Multi-AZ) にデプロイすることができます。これにより、クラスターレベルのネットワークおよびリソースの分離が行われ、VPN 接続や VPC ピアリングなどのクラウドプロバイダーの VPC 設定が有効になります。永続ボリューム (PV) は 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

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

関連情報

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

2.3.1.5. Local Zones

Red Hat OpenShift Service on AWS は、顧客がレイテンシーの影響を受けやすいアプリケーションのワークロードを配置できる大都市集中型のアベイラビリティーゾーンである AWS Local Zones の使用をサポートします。Local Zones は、独自のインターネット接続を持つ AWS リージョンの拡張です。

AWS Local Zones の詳細は、AWS ドキュメント How Local Zones work を参照してください。

AWS Local Zones を有効にして Local Zone をマシンプールに追加する手順は、マシンプール用のローカルゾーンの設定 を参照してください。

2.3.1.6. Service Level Agreement (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。

2.3.1.7. 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。

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

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

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

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

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

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

2.3.1.8. サポート

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

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

AWS サポートは、AWS との既存のサポート契約に基づきます。

2.3.2. Logging

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。

2.3.2.1. 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。

2.3.2.2. 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)。

2.3.3. 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。

2.3.3.1. クラスターメトリック

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、これらのメトリックは Red Hat OpenShift Service on AWS ユーザーによって提供される CPU またはメモリーメトリックをベースとする Horizontal Pod Autoscaling を許可します。

2.3.3.2. クラスターの通知

クラスター通知は、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。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。

2.3.4. ネットワーク

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

2.3.4.1. 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。Red Hat OpenShift Service on AWS 4.14 以降で Ingress を管理するには、Ingress Operator を使用します。Red Hat OpenShift Service on AWS 4.13 以前のバージョンでは機能に変更はありません。

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。

2.3.4.2. ドメイン検証証明書

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

2.3.4.3. ビルドのカスタム認証局

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

2.3.4.4. ロードバランサー

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

- クラスターの内部にあり、内部のクラスター通信のトラフィックのバランスを取るために使用される内部コントロールプレーンのロードバランサー。
- OpenShift および Kubernetes API へのアクセスに使用される外部コントロールプレーンのロードバランサー。このロードバランサーは OpenShift Cluster Manager で無効にできます。このロードバランサーが無効にされている場合、Red Hat は API DNS を内部コントロールプレーンのロードバランサーを参照するように再設定します。
- Red Hat によるクラスター管理用に予約される Red Hat の外部コントロールプレーンのロードバランサー。アクセスは厳密に制御され、ホワイトリストに登録されている bastion ホストからのみ通信が可能です。
- デフォルトのアプリケーションロードバランサーであるデフォルトの外部ルーター/ingress ロードバランサー (URL の **apps** で示される)。デフォルトのロードバランサーを OpenShift Cluster Manager で設定して、インターネット上で一般にアクセス可能にしたり、既存のプライベート接続でプライベートにのみアクセス可能にしたりできます。ロギング UI、メトリック API、レジストリーなどのクラスターサービスを含む、クラスターのすべてのアプリケーションルートは、このデフォルトのルーターロードバランサーで公開されます。

- オプション: セカンダリーアプリケーションロードバランサーであるセカンダリールーター/ingress ロードバランサー (URL の **apps2** で示される)。セカンダリーロードバランサーを OpenShift Cluster Manager で設定して、インターネット上で一般にアクセス可能にしたり、既存のプライベート接続でプライベートにのみアクセス可能にしたりできます。**Label match** がこのルーターロードバランサーに設定されている場合は、このラベルに一致するアプリケーションルートのみがこのルーターロードバランサーで公開されます。それ以外の場合は、すべてのアプリケーションルートがこのルーターロードバランサーで公開されます。

- オプション: サービスのロードバランサー。サービスの非 HTTP/SNI トラフィックおよび非標準ポートを有効にします。これらのロードバランサーを Red Hat OpenShift Service on AWS で実行されているサービスにマップし、HTTP/SNI 以外のトラフィックや標準以外のポートの使用などの高度な ingress 機能を有効にできます。各 AWS アカウントには、各クラスター内で使用できる Classic Load Balancer の数を制限 するクォータがあります。

2.3.4.5. 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。

2.3.4.6. クラスター egress

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

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

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

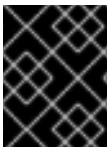
お客様はクラスター上で Pod を実行し、外部サービスをクエリーすることで、パブリック静的 IP アドレスを判別できます。以下に例を示します。

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

2.3.4.7. 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。これらの接続の監視は、お客様の責任で行われます。

2.3.4.8. DNS 転送

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

2.3.4.9. ネットワークの検証

Red Hat OpenShift Service on AWS クラスターを既存の Virtual Private Cloud (VPC) にデプロイするとき、またはクラスターに新しいサブネットを持つ追加のマシンプールを作成するときに、ネットワーク検証チェックが自動的に実行します。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

- ネットワーク検証チェックの詳細は、ネットワーク検証 を参照してください。

2.3.5. 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。

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

コントロールプレーン、インフラストラクチャー、およびワーカーノードは、保存時に暗号化された Amazon Elastic Block Store (Amazon EBS) ストレージを使用します。

2.3.5.2. 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。

2.3.5.3. 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 の数について独自の制限があります。詳細は、AWS インスタンスタイプの制限 を参照してください。

2.3.5.4. 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 OpenShift Dedicated and Red Hat OpenShift Service on AWS を参照してください。

2.3.6. プラットフォーム

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

2.3.6.1. 自動スケーリング

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

関連情報

- クラスターでのノードの自動スケーリングについて

2.3.6.2. デーモンセット

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

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

2.3.6.3. 複数のアベイラビリティーゾーン

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

2.3.6.4. ノードラベル

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

2.3.6.5. クラスターバックアップポリシー

重要

Red Hat は、STS を使用した ROSA クラスターのバックアップ方法を提供していません。お客様がアプリケーションとアプリケーションデータのバックアップ計画を立てることが重要です。

アプリケーションおよびアプリケーションデータのバックアップは Red Hat OpenShift Service on AWS サービスの一部として行われません。

以下の表は、非 STS クラスターにのみ適用されます。以下のコンポーネントは、Red Hat によってやむを得ない状況で使用されます。

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

2.3.6.6. OpenShift version

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

2.3.6.7. Upgrades

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。

2.3.6.8. Windows Container

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。

2.3.6.9. コンテナーエンジン

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

2.3.6.10. オペレーティングシステム

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

2.3.6.11. 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

2.3.6.12. Kubernetes Operator のサポート

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

2.3.7. 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。

2.3.7.1. 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

2.3.7.2. 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。

2.3.7.3. 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、**dedicated-admin** と呼ばれる ROSA 固有のグループへのアクセスを提供します。**dedicated-admin** グループのメンバーであるクラスターのすべてのユーザーは、以下を実行できます。

- 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。
- OperatorHub 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。

2.3.7.4. 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。

2.3.7.5. 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
```

2.3.7.6. 規制コンプライアンス

最新のコンプライアンス情報については、**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。

2.3.7.7. ネットワークセキュリティー

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

2.3.7.8. etcd 暗号化

Red Hat OpenShift Service on AWS では、コントロールプレーンストレージはデフォルトで静止時に暗号化され、これには etcd ボリュームの暗号化も含まれます。このストレージレベルの暗号化は、クラウドプロバイダーのストレージ層を介して提供されます。

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

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

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

重要

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

2.3.8. 関連情報

- 最新のコンプライアンス情報は、ROSA のプロセスおよびセキュリティーについて を参照してください。
- ROSA のライフサイクル を参照してください。

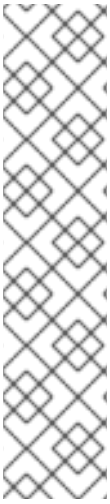
2.4. RED HAT OPENSHIFT SERVICE ON AWS インスタンスタイプ

アベイラビリティゾーンが 1 つのクラスターには、1 つのアベイラビリティゾーンにデプロイされた 3 つ以上のコントロールプレーンノード、2 つ以上のインフラストラクチャーノード、および 2 つ以上のワーカーノードが必要です。

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

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

コントロールプレーンおよびインフラストラクチャーノードは Red Hat によりデプロイされ、管理されます。クラウドプロバイダーコンソールを使用して基礎となるインフラストラクチャーをシャットダウンすることはサポートされておらず、データが失われる可能性があります。etcd および API 関連のワークロードを処理する 3 つ以上のコントロールプレーンノードが使用されます。メトリック、ルーティング、Web コンソール、および他のワークロードを処理するインフラストラクチャーノードが少なくとも 2 つあります。コントロールノードとインフラストラクチャーノードでワークロードを実行しないでください。実行する予定のワークロードはすべて、ワーカーノードにデプロイする必要があります。ワーカーノードにデプロイする必要がある Red Hat ワークロードの詳細は、以下の Red Hat Operator サポートセクションを参照してください。



注記

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

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

詳細は、Kubernetes のドキュメント を参照してください。

2.4.1. AWS x86 ベースのインスタンスタイプ

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

例2.2 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)
- 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)

† これらのインスタンスタイプは、48 個の物理コア上で 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。

例2.3 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2.4 メモリー集約型

- 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2.5 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)
- 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)
- 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)
- 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)
- 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)

† これらのインスタンスタイプは、48 個の物理コア上で 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。

‡ このインスタンスタイプは、24 個の物理コア上に 48 個の論理プロセッサーを提供します。

例2.6 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)
- 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 で対応していません。

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2.7 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)
- 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)
- 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)

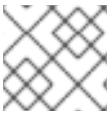
例2.8 最適化されたストレージ

- 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)
- 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)
- 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)

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



注記

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

例2.9 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2.10 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)

関連情報

- AWS インスタンスタイプ

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

2.5.1. 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 のマネージドインスタンスであり、独立したリリーススケジュールを維持します。マネージドオファリングの詳細は、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

2.5.2. 定義

表2.1 バージョン参照

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

メジャーリリースまたは X リリース

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

例

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

マイナーリリースまたは Y リリース

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

例

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

パッチリリースまたは Z リリース

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

例

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

2.5.3. 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。

2.5.4. マイナーバージョン (x.Y.z)

4.8 OpenShift Container Platform 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が一般公開されてから 16 か月間以上、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、サポート対象の最も古いマイナーバージョンの最新の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、クラスターが "限定サポート" ステータスになります。

例

1. 現時点で、お客様のクラスターは 4.13.8 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、クラスターに "限定サポート" ステータスのフラグが設定されます。

関連情報

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

2.5.5. 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、あるパッチリリースが非推奨になる可能性があります。この場合は、そのリリースのインストールができなくなり、そのリリースからの強制的なアップグレードが必要となります。

例

1. 4.7.6 に重要な CVE が含まれることが確認されるとします。
2. CVE の影響を受けるすべてのリリースは、サポートされるパッチリリースの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。

2.5.6. 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。

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

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

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

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

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

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

2.5.7. 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。

2.5.8. 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。

2.5.9. 必須アップグレード

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

極端な状況下では、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安全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、クラスターを最新の安全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。

2.5.10. ライフサイクルの日付

バージョン	一般公開	ライフサイクルの終了日
4.16	2024 年 7 月 2 日	2025 年 11 月 2 日
4.15	2024 年 2 月 27 日	2025 年 6 月 30 日
4.14	2023 年 10 月 31 日:	2025 年 2 月 28 日
4.13	2023 年 5 月 17 日	2024 年 9 月 17 日
4.12	2023 年 1 月 17 日	2024 年 7 月 17 日
4.11	2022 年 8 月 10 日	2023 年 12 月 10 日
4.10	2022 年 3 月 10 日	2023 年 9 月 10 日
4.9	2021 年 10 月 18 日	2022 年 12 月 18 日
4.8	2021 年 7 月 27 日	2022 年 9 月 27 日

2.6. HOSTED CONTROL PLANE (HCP) を備えた RED HAT OPENSHIFT SERVICE ON AWS (ROSA) のサービス定義

このドキュメントでは、Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) のマネージドサービスのサービス定義を説明します。

2.6.1. 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。

2.6.1.1. 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。

2.6.1.2. 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

2.6.1.3. インスタンスタイプ

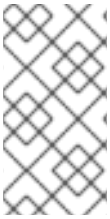
サポートされているインスタンスタイプの詳細は、ROSA with HCP インスタンスタイプ を参照してください。

2.6.1.4. 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

OpenShift 4 のサポートの有無にかかわらず、中国リージョンはサポートされません。



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。

GovCloud (US) リージョンは、ROSA Classic クラスターでのみサポートされます。

例2.11 AWS リージョン

- us-east-1 (N. Virginia)
- us-east-2 (Ohio)
- us-west-2 (Oregon)
- af-south-1 (Cape Town、AWS オプトインが必要)
- ap-east-1 (Hong Kong、AWS オプトインが必要)
- ap-south-2 (Hyderabad、AWS オプトインが必要)

- ap-southeast-3 (Jakarta、AWS オプトインが必要)
- ap-southeast-4 (Melbourne、AWS オプトインが必要)
- ap-south-1 (Mumbai)
- ap-northeast-3 (Osaka)
- ap-northeast-2 (Seoul)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ap-northeast-1 (Tokyo)
- ca-central-1 (Central Canada)
- eu-central-1 (Frankfurt)
- eu-north-1 (Stockholm)
- eu-west-1 (Ireland)
- eu-west-2 (London)
- eu-south-1 (Milan、AWS オプトインが必要)
- eu-west-3 (Paris)
- eu-south-2 (Spain)
- eu-central-2 (Zurich、AWS オプトインが必要)
- me-south-1 (Bahrain、AWS オプトインが必要)
- me-central-1 (UAE、AWS オプトインが必要)
- sa-east-1 (São Paulo)

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

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

2.6.1.5. Local Zones

Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) では、AWS Local Zones を使用できません。

2.6.1.6. Service Level Agreement (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。

2.6.1.7. 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ついて質問がある場合、またはさらに支援が必要な場合は、サポートチケットを作成します。

2.6.1.8. サポート

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

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

AWS サポートは、AWS との既存のサポート契約に基づきます。

2.6.2. Logging

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。

2.6.2.1. 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。

2.6.2.2. 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)。

2.6.3. 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。

2.6.3.1. クラスターメトリック

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、これらのメトリックは Red Hat OpenShift Service on AWS ユーザーによって提供される CPU またはメモリーメトリックをベースとする Horizontal Pod Autoscaling を許可します。

2.6.3.2. クラスターの通知

クラスター通知は、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。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。

2.6.4. ネットワーク

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

2.6.4.1. 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。Red Hat OpenShift Service on AWS 4.14 以降で Ingress を管理するには、Ingress Operator を使用します。Red Hat OpenShift Service on AWS 4.13 以前のバージョンでは機能に変更はありません。

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。

2.6.4.2. ドメイン検証証明書

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

2.6.4.3. ビルドのカスタム認証局

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

2.6.4.4. ロードバランサー

Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) 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。

2.6.4.5. 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。

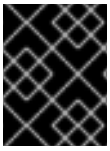
2.6.4.6. クラスター egress

EgressNetworkPolicy オブジェクトでの Pod egress トラフィックの制御は、Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS での送信トラフィックを防ぐか、これを制限するために使用できます。

2.6.4.7. 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。これらの接続の監視は、お客様の責任で行われます。

2.6.4.8. DNS 転送

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

2.6.4.9. ネットワークの検証

Red Hat OpenShift Service on AWS クラスターを既存の Virtual Private Cloud (VPC) にデプロイするとき、またはクラスターに新しいサブネットを持つ追加のマシンプールを作成するときに、ネットワーク検証チェックが自動的に実行します。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。
:!rosa-with-hcp:

関連情報

- ネットワーク検証チェックの詳細は、ネットワーク検証 を参照してください。

2.6.5. ストレージ

このセクションでは、Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) のストレージのサービス定義に関する情報を提供します。

2.6.5.1. 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。

2.6.5.2. 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。

2.6.5.3. 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 の数について独自の制限があります。詳細は、AWS インスタンスタイプの制限 を参照してください。

2.6.5.4. 共有ストレージ (RWX)

AWS CSI ドライバーを使用すると、Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) に RWX サポートを提供できます。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 OpenShift Dedicated and Red Hat OpenShift Service on AWS を参照してください。

2.6.6. プラットフォーム

このセクションでは、Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) のプラットフォームのサービス定義に関する情報を提供します。

2.6.6.1. 自動スケーリング

Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) では、ノードの自動スケーリングを利用できます。オートスケーラーオプションを設定して、クラスター内のマシンの数を自動的にスケーリングできます。

関連情報

- クラスターでのノードの自動スケーリングについて

2.6.6.2. デーモンセット

Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) では、デーモンセットを作成して実行できます。

2.6.6.3. 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。

2.6.6.4. 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、Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) では変更できません。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。

2.6.6.5. クラスターバックアップポリシー

重要

Red Hat は、STS を使用した ROSA クラスターのバックアップ方法を提供していません。お客様がアプリケーションとアプリケーションデータのバックアップ計画を立てることが重要です。

アプリケーションおよびアプリケーションデータのバックアップは、Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) の一部ではありません。

2.6.6.6. OpenShift version

Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) は、サービスとして実行され、OpenShift Container Platform の最新バージョンで最新の状態に保たれます。最新バージョンへのアップグレードのスケジューリング機能を利用できます。

2.6.6.7. Upgrades

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。

2.6.6.8. Windows Container

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。

2.6.6.9. コンテナーエンジン

Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) は、OpenShift 4 で実行し、唯一の利用可能なコンテナーエンジンとして CRI-O を使用します。

2.6.6.10. オペレーティングシステム

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

2.6.6.11. 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

2.6.6.12. Kubernetes Operator のサポート

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

2.6.7. セキュリティー

このセクションでは、Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) のセキュリティーのサービス定義に関する情報を提供します。

2.6.7.1. 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

2.6.7.2. 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。

2.6.7.3. お客様管理者ユーザー

Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) は、通常のユーザーに加えて、**dedicated-admin** と呼ばれる HCP 固有のグループを持つ ROSA へのアクセスを提供します。**dedicated-admin** グループのメンバーであるクラスターのすべてのユーザーは、以下を実行できます。

- 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。
- OperatorHub 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。

2.6.7.4. クラスター管理ロール

Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) の管理者には、組織のクラスターの **cluster-admin** ロールへのデフォルトアクセス権があります。**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。

2.6.7.5. 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
```

2.6.7.6. 規制コンプライアンス

最新のコンプライアンス情報については、**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。

2.6.7.7. ネットワークセキュリティー

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

2.6.7.8. etcd 暗号化

Hosted Control Plane (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA) では、コントロールプレーンストレージがデフォルトで保存時に暗号化されます。これには etcd ボリュームの暗号化も含まれます。このストレージレベルの暗号化は、クラウドプロバイダーのストレージ層を介して提供されます。

etcd データベースはデフォルトで常に暗号化されます。お客様は、etcd データベースを暗号化する目的で、独自のカスタム AWS KMS キーを指定できます。

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

2.6.8. 関連情報

- 最新のコンプライアンス情報は、ROSA のプロセスおよびセキュリティーについて を参照してください。
- ROSA のライフサイクル を参照してください。

2.7. ROSA WITH HCP 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礎となるインフラストラクチャーをシャットダウンすることはサポートされておらず、データが失われる可能性があります。

注記

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

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

詳細は、Kubernetes のドキュメント を参照してください。

2.7.1. AWS x86 ベースのインスタンスタイプ

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

例2.12 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)
- 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)

† これらのインスタンスタイプは、48 個の物理コア上で 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。

例2.13 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2.14 メモリー集約型

- 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2.15 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)
- 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)
- 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)
- 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)
- 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)

† これらのインスタンスタイプは、48 個の物理コア上で 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。

‡ このインスタンスタイプは、24 個の物理コア上に 48 個の論理プロセッサーを提供します。

例2.16 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)
- 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 で対応していません。

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2.17 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)
- 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)
- 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2.18 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)
- 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)
- 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)

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

注記

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

例2.19 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2.20 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)

2.7.2. 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2.21 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)

例2.22 バースト可能な汎用目的

- t4g.xlarge (4 vCPU、16 GiB)

- t4g.2xlarge (8 vCPU、32 GiB)

例2.23 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、1024 GiB)
- x2gd.metal (64 vCPU、1024 GiB)

例2.24 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)

例2.25 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2.26 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)

例2.27 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2.28 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)

注記

現在、ROSA with HCP は最大 90 個のワーカーノードをサポートしています。

関連情報

- AWS インスタンスタイプ

2.8. HCP を備えた ROSA の更新ライフサイクル

2.8.1. 概要

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

Red Hat OpenShift Service on AWS は Red Hat OpenShift のマネージドインスタンスであり、独立したリリーススケジュールを維持します。マネージドオファリングの詳細は、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

2.8.2. 定義

表2.2 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

2.8.3. 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。

2.8.4. マイナーバージョン (x.Y.z)

4.8 OpenShift Container Platform 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が一般公開されてから 16 か月間以上、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

2.8.5. パッチバージョン (x.y.Z)

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

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

例

1. 4.7.6 に重要な CVE が含まれることが確認されるとします。
2. CVE の影響を受けるすべてのリリースは、サポートされるパッチリリースの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。

2.8.6. 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について質問がある場合、またはさらに支援が必要な場合は、サポートチケットを作成します。

2.8.7. 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。

2.8.8. 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。

2.8.9. 必須アップグレード

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

極端な状況下では、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安全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安全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。

2.8.10. ライフサイクルの日付

バージョン	一般公開	ライフサイクルの終了日
4.16	2024 年 7 月 2 日	2025 年 11 月 2 日
4.15	2024 年 2 月 27 日	2025 年 6 月 30 日
4.14	2023 年 12 月 4 日	2025 年 2 月 28 日

2.9. 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 (ROSA) に対するお客様のセキュリティーに関する責任について詳しく説明します。

頭字語および用語

- **AWS** - Amazon Web Services
- **CEE** - Customer Experience and Engagement (Red Hat サポート)
- **CI/CD** - 継続的インテグレーション/継続的デリバリー
- **CVE** - 共通脆弱性識別子 (Common Vulnerabilities and Exposures)
- **PV** - 永続ボリューム
- **ROSA** - Red Hat OpenShift Service on AWS
- **SRE** - Red Hat Site Reliability Engineering
- **VPC** - Virtual Private Cloud

2.9.1. 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。

2.9.1.1. 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。

2.9.1.2. 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安全に管理します。これらのキーは、デフォルトで暗号化されるコントロールプレーン、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。

2.9.1.3. 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。

2.9.1.4. ネットワークセキュリティー

2.9.1.4.1. 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。

2.9.1.4.2. 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。

2.9.1.4.3. クラスターネットワークのアクセス制御

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

2.9.1.5. 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。

2.9.1.6. コンプライアンス

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

表2.3 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

コンプライアンス	Red Hat OpenShift Service on AWS (ROSA)	ホスト型コントロールプレーン (HCP) を備えた Red Hat OpenShift Service on AWS (ROSA)
HIPAA Qualified	はい	いいえ
ISO 27001	はい	はい
ISO 27017	はい	はい
ISO 27018	はい	はい
PCI DSS	はい	はい
SOC 1 タイプ 2	はい	はい
SOC 2 タイプ 2	はい	はい
SOC 3	はい	はい
FedRAMP High[1]	はい (GovCloud の要件)	いいえ

1. 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

- SRE の常駐に関する詳細は、Red Hat Subprocessor List を参照してください。
- お客様や責任共有の詳細は、ROSA の各種の責任 に関する文書を参照してください。
- ROSA およびそのコンポーネントの詳細は、ROSA サービス定義 を参照してください。

2.10. 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 (ROSA) 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。

2.10.1. 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。

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。

2.10.2. SRE クラスターアクセス

SRE による Red Hat OpenShift Service on AWS (ROSA) 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 によって顧客のクラスターに加えられたすべての変更が、Red Hat のマネージドサービスガイドラインを構成す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 が顧客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。

- SRE は、Red Hat SSO (クラウドサービス) に更新された 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。

- SRE は Red Hat VPN に接続します。VPN への認証は、Red Hat Corporate Identity and Access Management システム (RH IAM) 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。

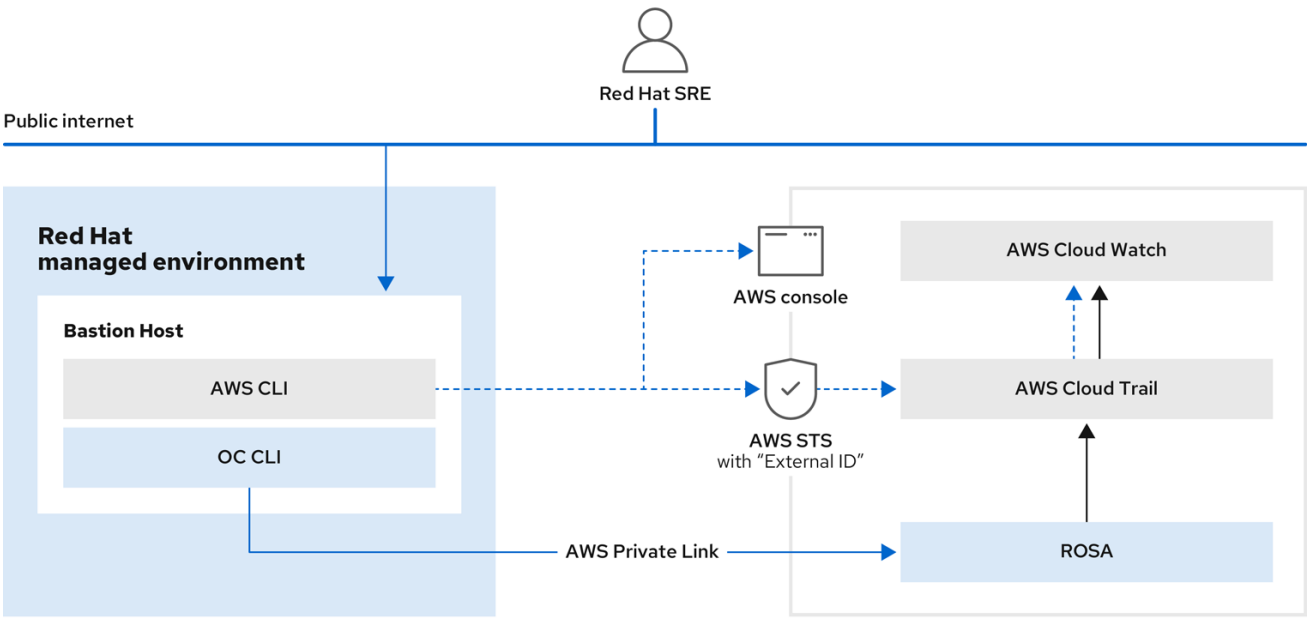
    - プライベートまたはパブリッククラスターへのアクセス: リクエストは、ポート 6443 で暗号化された HTTP 接続を使用して、特定のネットワークロードバランサー (NLB) 経由で送信されます。

    - 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、リージョンごとに Red Hat VPC に接続されます。リクエストを受信する VPC は、ターゲットのプライベートクラスターのリージョンに依存します。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。

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

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

図2.1 SRE による ROSA クラスターへのアクセス



2.10.2.1. ROSA の特権アクセスの制御

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

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

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

コンポーネント	通常の SRE 管理者アクセス (Red Hat ポータル)	通常の SRE 管理者アクセス (Red Hat SSO)	OpenShift の昇格	クラウドプロバイダーのアクセスまたは昇格
OpenShift Cluster Manager	R/W	アクセスなし	アクセスなし	アクセスなし
OpenShift コンソール	アクセスなし	R/W	R/W	アクセスなし

コンポーネント	通常の SRE 管理者アクセス (Red Hat ポータル)	通常の SRE 管理者アクセス (Red Hat SSO)	OpenShift の昇格	クラウドプロバイダーのアクセスまたは昇格
ノードのオペレーティングシステム	アクセスなし	昇格した OS およびネットワークのパーミッションのリスト。	昇格した OS およびネットワークのパーミッションのリスト。	アクセスなし
AWS コンソール	アクセスなし	アクセスはありませんが、これはクラウドプロバイダーのアクセスを要求するために使用されるアカウントです。	アクセスなし	SRE アイデンティティーを使用したすべてのクラウドプロバイダーのパーミッション。

2.10.2.2. SRE による AWS アカウントへのアクセス

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

分離されたバックプレーンフローでは、SRE が顧客のサポートロールへのアクセスを要求します。このリクエストは、バックプレーン API によってジャストインタイム (JIT) 処理され、特定の SRE 担当者のアカウントに対する組織ロールの権限が動的に更新されます。この SRE のアカウントには、特定の Red Hat 顧客の環境へのアクセス権が付与されます。Red Hat のお客様の環境への SRE アクセスは、アクセス要求時にのみ確立される一時的かつ短期間のアクセスです。

STS トークンへのアクセスは監査ログに記録され、個別のユーザーまでトレースできます。STS および非 STS クラスターはいずれも、SRE によるアクセスに AWS STS サービスを使用します。**ManagedOpenShift-Technical-Support-Role** に **ManagedOpenShift-Support-Access** ポリシーが割り当てられており、このロールが管理に使用されると、アクセス制御では統合バックプレーンフローが使用されます。**ManagedOpenShift-Support-Role** に **ManagedOpenShift-Technical-Support-<org_id>** ポリシーが割り当てられていると、アクセス制御で分離されたバックプレーンフローが使用されます。詳細は、KCS の記事 Updating Trust Policies for ROSA clusters を参照してください。

2.10.2.3. AWS アカウントの SRE STS ビュー

SRE が 2 要素認証を使用する VPN を使用している場合、SRE と Red Hat サポートは AWS アカウントで **ManagedOpenShift-Support-Role** を引き受けることができます。**ManagedOpenShift-Support-Role** には、SRE が AWS リソースを直接トラブルシューティングして管理するために必要なすべての権限が含まれています。**ManagedOpenShift-Support-Role** を引き受けると、SRE は AWS Security Token Service (STS) を使用して、顧客のアカウントの AWS Web UI への有効期限付きの一意の URL を生成します。その後、SRE は次のような複数のトラブルシューティングアクションを実行できます。

- CloudTrail ログの表示
- 障害のある EC2 インスタンスのシャットダウン

SRE によって実行されるすべてのアクティビティーは Red Hat IP アドレスから受信され、CloudTrail に記録されるため、すべてのアクティビティーを監査およびレビューできます。このロールは、AWS サービスへのアクセスが必要な場合にのみ使用されます。権限の大部分は読み取り専用です。ただし、一部の権限にはわずかに、インスタンスの再起動や新しいインスタンスのスピンアップなど、より多くのアクセス権があります。SRE によるアクセスは、**ManagedOpenShift-Support-Role** に割り当てられているポリシー権限に制限されます。

権限の完全なリストについては、STS を使用する ROSA クラスターの IAM リソース ユーザーガイドの sts_support_permission_policy.json を参照してください。

2.10.2.4. PrivateLink VPC エンドポイントサービスを介した SRE によるアクセス

PrivateLink VPC エンドポイントサービスは、ROSA クラスター作成の一部として作成されます。

PrivateLink ROSA クラスターがある場合、その Kubernetes API サーバーは、デフォルトでは VPC 内からのみアクセスできるロードバランサーを通じて公開されます。Red Hat Site Reliability Engineering (SRE) は、Red Hat が所有する AWS アカウントに VPC エンドポイントが関連付けられている VPC エンドポイントサービスを介して、このロードバランサーに接続できます。このエンドポイントサービスには、ARN にも含まれるクラスターの名前が含まれています。

Allow principals タブに、Red Hat 所有の AWS アカウントがリストされます。この特定のユーザーにより、他のエンティティーが PrivateLink クラスターの Kubernetes API サーバーへの VPC エンドポイント接続を作成できないようになります。

Red Hat SRE が API にアクセスすると、このフリート管理プレーンは VPC エンドポイントサービスを通じて内部 API に接続できます。

2.10.3. 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	読み取り: All 書き込み: Very 限定的[1]	読み取り: All 書き込み: None	読み取り: None[2] 書き込み: None	読み取り: All [3] 書き込み: All [3]
CEE	読み取り: All 書き込み: None	読み取り: All 書き込み: None	読み取り: None[2] 書き込み: None	読み取り: None 書き込み: None
お客様管理者	読み取り: None 書き込み: None	読み取り: None 書き込み: None	読み取り: All 書き込み: All	読み取り: All 書き込み: All
お客様ユーザー	読み取り: None 書き込み: None	読み取り: None 書き込み: None	読み取り: Limited[4] 書き込み: Limited[4]	読み取り: None 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*
上記以外	読み取り: None 書き込み: None	読み取り: None 書き込み: None	読み取り: None 書き込み: None	読み取り: None 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. Red Hat は、デフォルトではお客様のデータにアクセスできません。
3. SRE は AWS アカウントに、文書化されたインシデントの発生時の例外的なトラブルシューティングのための緊急手順としてアクセスします。
4. 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。

2.10.4. 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。

2.10.5. アクセスの承認およびレビュー

新規の SRE ユーザーアクセスには、管理者の承認が必要です。分離された SRE アカウントまたは転送された SRE アカウントは、自動化されたプロセスで認可されたユーザーとして削除されます。さらに、SRE は、認可されたユーザー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
ロギング	**Red Hat** ● 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。 ● 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。 ● 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。

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** ● 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。 ● 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。
Cluster networking	**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。 ● 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。 ● 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。 ● 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** ● 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。
仮想ストレージ管理	**Red Hat** ● 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。 ● 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。

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** ● 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。 ● 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** **Compute:** ROSA コントロールプレーン、インフラストラクチャー、ワーカーノードに使用される Amazon EC2 サービスを提供します。 **Storage:** ROSA がクラスターに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できるようにするために使用される Amazon EBS を提供します。 **Storage:** サービスの組み込みイメージレジストリーに使用される Amazon S3 を提供します。 **Networking:** 顧客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顧客が使用する AWS Identity and Access Management (IAM) を提供します。	● 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。 ● 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。 ● 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。 ● 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** ● 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。

2.10.6. 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

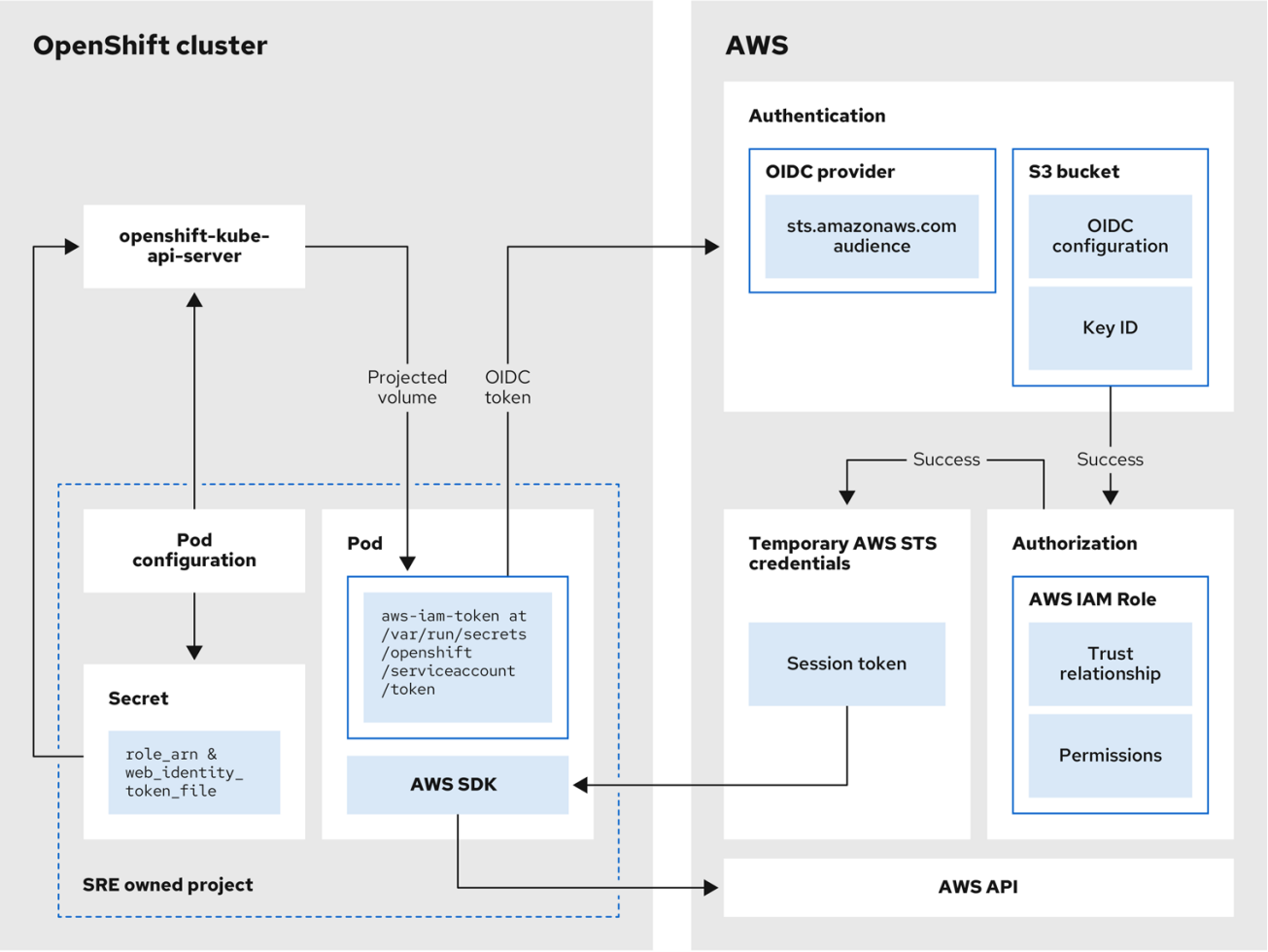
AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS クラスターをインストールすると、クラスター固有の Operator AWS Identity and Access Management (IAM) ロールが作成されます。これらの IAM ロールにより、Red Hat OpenShift Service on AWS クラスター Operator がコア OpenShift 機能を実行できるようになります。

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 で使用するサービスアカウントに一時的な 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。

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
次の図は、SRE 所有プロジェクトで 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2.2 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。Red Hat OpenShift Service on AWS 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 Red Hat OpenShift Service on AWS 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 Operator によって使用される AWS IAM ロールの詳細は、クラスター固有の Operator IAM ロールのリファレンス を参照してください。
- クラスター Operator に必要なポリシーと権限の詳細は、アカウント全体のロールの作成方法 を参照してください。

第3章 STS を使用する ROSA クラスターの IAM リソースについて

AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターをデプロイするには、以下の AWS Identity Access Management (IAM) リソースを作成する必要があります。

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

このドキュメントでは、STS を使用する ROSA クラスターの作成時にデプロイする必要のある IAM リソースに関する参考情報を提供します。また、**rosa create** コマンドで **manual** モードを使用する場合に生成される **aws** CLI コマンドも含まれます。

関連情報

- AWS IAM リソースを含む STS を使用して ROSA クラスターをすばやく作成するための詳細な手順は、デフォルトオプションを使用した STS を使用した ROSA クラスターの作成 を参照してください。
- AWS IAM リソースを含むカスタマイズを使用して STS で ROSA クラスターを作成する手順は、カスタマイズを使用して STS を使用する ROSA クラスターの作成 を参照してください。

3.1. 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。IAM ロールを AWS アカウントにリンクする方法は、AWS アカウントの関連付け を参照してください。

ヒント

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

これらの AWS IAM ロールは以下のとおりです。

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

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

注記

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

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

3.1.1. 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。

3.1.1.1. 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3.1 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。

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

表3.2 admin **ocm-role リソースの追加パーミッション**

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

リソース	説明

関連情報

- アカウント全体のロールを作成する方法

ocm-role IAM ロールの作成

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

前提条件

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

手順

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

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

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

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

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

出力例

```
I: Creating ocm role
? Role prefix: ManagedOpenShift 1
? Enable admin capabilities for the OCM role (optional): No 2
? Permissions boundary ARN (optional): 3
? Role Path (optional): 4
? Role creation mode: auto 5
I: Creating role using 'arn:aws:iam::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes 6
I: Created role 'ManagedOpenShift-OCM-Role-182' with ARN  'arn:aws:iam::
<ARN>:role/ManagedOpenShift-OCM-Role-182'
I: Linking OCM role
? OCM Role ARN: arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182 7
```

```
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with organization
'<AWS ARN>'? Yes 8
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' with
organization account '<AWS ARN>'
```

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

注記

--admin オプションを使用した場合、このプロンプトは表示されません。

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

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

関連情報

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

3.2. アカウント全体の IAM ロールおよびポリシー参照

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

アカウント全体のロールおよびポリシーは、OpenShift マイナーリリースバージョン (OpenShift 4.16 など) に固有のものであり、後方互換性があります。パッチバージョンに関係なく、同じマイナーバージョンの複数のクラスターにアカウント全体のロールおよびポリシーを再利用することで、必要な STS リソースを最小限に抑えることができます。

3.2.1. 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。手動で、またはこれらのロールおよびポリシーに事前定義された名前を使用する自動プロセスを使用して、ロールを作成できます。

手動 ocm-role リソースの作成
システムでこれらのロールを作成するのに必要な CLI アクセスがある場合は、手動作成方法を使用できます。このオプションは、目的の CLI ツールまたは OpenShift Cluster Manager から実行できます。手動作成プロセスを開始すると、CLI は、ロールを作成して必要なポリシーにリンクする一連のコマンドを実行するために表示します。

自動 ocm-role リソースの作成
管理者権限で **ocm-role** リソースを作成した場合は、OpenShift Cluster Manager からの自動作成方法を使用できます。ROSA CLI では、これらのロールとポリシーを自動的に作成するために、この管理 **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。

注記

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

表3.3 ROSA インストーラーロール、ポリシー、およびポリシーファイル

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

例3.1 sts_installer_trust_policy.json

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

```
        }
    ]
}
```

例3.2 sts_installer_permission_policy.json

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

```
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:DetachInternetGateway",
                "ec2:DisassociateRouteTable",
                "ec2:GetConsoleOutput",
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVpcAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
```

```
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:ModifyLoadBalancerAttributes",
"elasticloadbalancing:ModifyTargetGroup",
"elasticloadbalancing:ModifyTargetGroupAttributes",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
"iam:AddRoleToInstanceProfile",
"iam:CreateInstanceProfile",
"iam:DeleteInstanceProfile",
"iam:GetInstanceProfile",
"iam:TagInstanceProfile",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:ListAttachedRolePolicies",
"iam:ListInstanceProfiles",
"iam:ListInstanceProfilesForRole",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:PassRole",
"iam:RemoveRoleFromInstanceProfile",
"iam:SimulatePrincipalPolicy",
"iam:TagRole",
"iam:UntagRole",
"route53:ChangeResourceRecordSets",
"route53:ChangeTagsForResource",
"route53:CreateHostedZone",
"route53:DeleteHostedZone",
"route53:GetAccountLimit",
"route53:GetChange",
"route53:GetHostedZone",
"route53:ListHostedZones",
"route53:ListHostedZonesByName",
"route53:ListResourceRecordSets",
"route53:ListTagsForResource",
"route53:UpdateHostedZoneComment",
"s3:CreateBucket",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:GetAccelerateConfiguration",
"s3:GetBucketAcl",
"s3:GetBucketCORS",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketPolicy",
"s3:GetBucketRequestPayment",
"s3:GetBucketTagging",
```

```
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListAWSDefaultServiceQuotas",
                "sts:AssumeRole",
                "sts:AssumeRoleWithWebIdentity",
                "sts:GetCallerIdentity",
                "tag:GetResources",
                "tag:UntagResources",
                "ec2:CreateVpcEndpointServiceConfiguration",
                "ec2:DeleteVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:ModifyVpcEndpointServicePermissions",
                "kms:DescribeKey",
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

表3.4 ROSA コントロールプレーンのロール、ポリシー、およびポリシーファイル

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

例3.3 sts_instance_controlplane_trust_policy.json

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

例3.4 sts_instance_controlplane_permission_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteVolume",
                "ec2:Describe*",
                "ec2:DetachVolume",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyVolume",
                "ec2:RevokeSecurityGroupIngress",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:CreateListener",
```

```
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerPolicy",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteLoadBalancerListeners",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:Describe*",
                "elasticloadbalancing:DetachLoadBalancerFromSubnets",
                "elasticloadbalancing:ModifyListener",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

表3.5 ROSA コンピュートノードロール、ポリシー、およびポリシーファイル

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

例3.5 sts_instance_worker_trust_policy.json

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

```
        ]
      }
    ]
}
```

例3.6 sts_instance_worker_permission_policy.json

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

表3.6 ROSA サポートロール、ポリシー、およびポリシーファイル

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

例3.7 sts_support_trust_policy.json

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

例3.8 sts_support_permission_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:LookupEvents",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:CopySnapshot",
                "ec2:CreateNetworkInsightsPath",
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:DeleteTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAddressesAttribute",
                "ec2:DescribeAggregateIdFormat",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeCarrierGateways",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeCoipPools",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeIdFormat",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLocalGatewayRouteTables",
                "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
```

```
"ec2:DescribeLocalGatewayRouteTableVpcAssociations",
"ec2:DescribeLocalGateways",
"ec2:DescribeLocalGatewayVirtualInterfaceGroups",
"ec2:DescribeLocalGatewayVirtualInterfaces",
"ec2:DescribeManagedPrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInsightsAnalyses",
"ec2:DescribeNetworkInsightsPaths",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePlacementGroups",
"ec2:DescribePrefixLists",
"ec2:DescribePrincipalIdFormat",
"ec2:DescribePublicIpv4Pools",
"ec2:DescribeRegions",
"ec2:DescribeReservedInstances",
"ec2:DescribeRouteTables",
"ec2:DescribeScheduledInstances",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshotAttribute",
"ec2:DescribeSnapshots",
"ec2:DescribeSpotFleetInstances",
"ec2:DescribeStaleSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayConnectPeers",
"ec2:DescribeTransitGatewayConnects",
"ec2:DescribeTransitGatewayMulticastDomains",
"ec2:DescribeTransitGatewayPeeringAttachments",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGateways",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeVolumeAttribute",
"ec2:DescribeVolumeStatus",
"ec2:DescribeVolumes",
"ec2:DescribeVolumesModifications",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcClassicLink",
"ec2:DescribeVpcClassicLinkDnsSupport",
"ec2:DescribeVpcEndpointConnectionNotifications",
"ec2:DescribeVpcEndpointConnections",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcEndpointServicePermissions",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetAssociatedIpv6PoolCidrs",
"ec2:GetConsoleOutput",
"ec2:GetManagedPrefixListEntries",
"ec2:GetSerialConsoleAccessStatus",
```

```
            "ec2:GetTransitGatewayAttachmentPropagations",
            "ec2:GetTransitGatewayMulticastDomainAssociations",
            "ec2:GetTransitGatewayPrefixListReferences",
            "ec2:GetTransitGatewayRouteTableAssociations",
            "ec2:GetTransitGatewayRouteTablePropagations",
            "ec2:ModifyInstanceAttribute",
            "ec2:RebootInstances",
            "ec2:RunInstances",
            "ec2:SearchLocalGatewayRoutes",
            "ec2:SearchTransitGatewayMulticastGroups",
            "ec2:SearchTransitGatewayRoutes",
            "ec2:StartInstances",
            "ec2:StartNetworkInsightsAnalysis",
            "ec2:StopInstances",
            "ec2:TerminateInstances",
            "elasticloadbalancing:ConfigureHealthCheck",
            "elasticloadbalancing:DescribeAccountLimits",
            "elasticloadbalancing:DescribeInstanceHealth",
            "elasticloadbalancing:DescribeListenerCertificates",
            "elasticloadbalancing:DescribeListeners",
            "elasticloadbalancing:DescribeLoadBalancerAttributes",
            "elasticloadbalancing:DescribeLoadBalancerPolicies",
            "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeRules",
            "elasticloadbalancing:DescribeSSLPolicies",
            "elasticloadbalancing:DescribeTags",
            "elasticloadbalancing:DescribeTargetGroupAttributes",
            "elasticloadbalancing:DescribeTargetGroups",
            "elasticloadbalancing:DescribeTargetHealth",
            "iam:GetRole",
            "iam:ListRoles",
            "kms:CreateGrant",
            "route53:GetHostedZone",
            "route53:GetHostedZoneCount",
            "route53:ListHostedZones",
            "route53:ListHostedZonesByName",
            "route53:ListResourceRecordSets",
            "s3:GetBucketTagging",
            "s3:GetObjectAcl",
            "s3:GetObjectTagging",
            "s3:ListAllMyBuckets"
            "sts:DecodeAuthorizationMessage",
            "tiros:CreateQuery",
            "tiros:GetQueryAnswer",
            "tiros:GetQueryExplanation"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::managed-velero*",
            "arn:aws:s3:::*image-registry*"
        ]
```

```
        }
    ]
}
```

表3.7 ROSA OCM ロールおよびポリシーファイル

リソース	説明
ManagedOpenShift-OCM-Role	この IAM ロールを使用して、OpenShift Cluster Manager で ROSA クラスターを作成および管理します。

例3.9 **sts_ocm_role_trust_policy.json**

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

表3.8 ROSA ユーザーロールとポリシーファイル

リソース	説明
ManagedOpenShift-User-<OCM_user>-Role	お客様の AWS アイデンティティーを検証するために Red Hat が使用する IAM ロール。

例3.10 **sts_user_role_trust_policy.json**

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

```
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "<OCM_account_ID>"
                }
            }
        }
    ]
}
```

表3.9 ROSA Ingress Operator IAM ポリシーおよびポリシーファイル

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

例3.11 **openshift_ingress_operator_cloud_credentials_policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "route53:ChangeResourceRecordSets",
        "tag:GetResources"
      ],
      "Resource": "*"
    }
  ]
}
```

表3.10 ROSA バックエンドストレージ IAM ポリシーおよびポリシーファイル

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

例3.12 **openshift_cluster_csi_drivers_ebs_cloud_credentials_policy.json**

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

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

表3.11 ROSA Machine Config Operator ポリシーおよびポリシーファイル

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

例3.13 openshift_machine_api_aws_cloud_credentials_policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
```

```
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "iam:PassRole",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlainText",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:RevokeGrant",
        "kms:CreateGrant",
        "kms:ListGrants"
      ],
      "Resource": "*",
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}
```

表3.12 ROSA Cloud Credential Operator ポリシーおよびポリシーファイル

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

例3.14
openshift_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json

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

```
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

表3.13 ROSA Image Registry Operator ポリシーおよびポリシーファイル

リソース	説明
ManagedOpenShift-openshift-image-registry-installer-cloud-credentials	クラスターの AWS S3 で 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パーミッションを持つ ROSA イメージレジストリー Operator を提供する IAM ポリシー。

例3.15 openshift_image_registry_installer_cloud_credentials_policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketTagging",
        "s3:GetBucketTagging",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetBucketPublicAccessBlock",
        "s3:PutEncryptionConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": "*"
    }
  ]
}
```

関連情報

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

3.2.2. 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。

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 (**4.16** 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

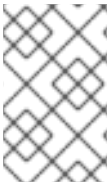
```
aws iam create-role \
 --role-name ManagedOpenShift-Installer-Role \
 --assume-role-policy-document file://sts_installer_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=rosa_role_type,Value=installer

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
```

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

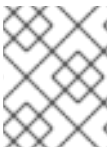
提供されているコマンドの例には、**ManagedOpenShift** 接頭辞が含まれています。**--prefix** オプションを使用してカスタム接頭辞を指定しない場合は、**ManagedOpenShift** 接頭辞がデフォルト値です。

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
```

3.3. インストーラーロールのパーミッション境界

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



注記

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

パーミッション境界ポリシーファイルは以下のとおりです。

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

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

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

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

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

- **Core** は、インストーラーロールに対して最も限定的な権限だけを設定します。VPC および PL 権限は **Core only** の境界ポリシーに含まれません。
  - インストーラーは VPC または PL を作成または管理できません。
  - 顧客が提供する VPC が必要であり、PrivateLink (PL) は利用できません。

- **Core + VPC** は、インストーラーロールのコアおよび VPC パーミッションを設定します。
  - インストーラーは PL を作成または管理できません。
  - カスタム/BYO-VPC を使用していないことを前提としています。
  - インストーラーが VPC を作成して管理することを前提としています。

- **Core + PrivateLink (PL)** は、インストーラーが PL インフラストラクチャーをプロビジョニングできることを意味します。
  - お客様が提供する VPC が必要です。
  - これは、PL のプライベートクラスター用です。

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

例3.16 sts_installer_core_permission_boundary_policy.json

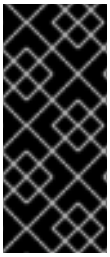
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
      "autoscaling:DescribeAutoScalingGroups",
      "ec2:AllocateAddress",
```

```
        "ec2:AssociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetConsoleOutput",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
```

```
"elasticloadbalancing:AddTags",
"elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
"elasticloadbalancing:AttachLoadBalancerToSubnets",
"elasticloadbalancing:ConfigureHealthCheck",
"elasticloadbalancing:CreateListener",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing:CreateLoadBalancerListeners",
"elasticloadbalancing:CreateTargetGroup",
"elasticloadbalancing:DeleteLoadBalancer",
"elasticloadbalancing:DeleteTargetGroup",
"elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
"elasticloadbalancing:DeregisterTargets",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:ModifyLoadBalancerAttributes",
"elasticloadbalancing:ModifyTargetGroup",
"elasticloadbalancing:ModifyTargetGroupAttributes",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
"iam:AddRoleToInstanceProfile",
"iam:CreateInstanceProfile",
"iam:DeleteInstanceProfile",
"iam:GetInstanceProfile",
"iam:TagInstanceProfile",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:ListAttachedRolePolicies",
"iam:ListInstanceProfiles",
"iam:ListInstanceProfilesForRole",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:PassRole",
"iam:RemoveRoleFromInstanceProfile",
"iam:SimulatePrincipalPolicy",
"iam:TagRole",
"iam:UntagRole",
"route53:ChangeResourceRecordSets",
"route53:ChangeTagsForResource",
"route53:CreateHostedZone",
"route53:DeleteHostedZone",
"route53:GetAccountLimit",
"route53:GetChange",
"route53:GetHostedZone",
"route53:ListHostedZones",
"route53:ListHostedZonesByName",
"route53:ListResourceRecordSets",
```

```
            "route53:ListTagsForResource",
            "route53:UpdateHostedZoneComment",
            "s3:CreateBucket",
            "s3:DeleteBucket",
            "s3:DeleteObject",
            "s3:GetAccelerateConfiguration",
            "s3:GetBucketAcl",
            "s3:GetBucketCORS",
            "s3:GetBucketLocation",
            "s3:GetBucketLogging",
            "s3:GetBucketObjectLockConfiguration",
            "s3:GetBucketPolicy",
            "s3:GetBucketRequestPayment",
            "s3:GetBucketTagging",
            "s3:GetBucketVersioning",
            "s3:GetBucketWebsite",
            "s3:GetEncryptionConfiguration",
            "s3:GetLifecycleConfiguration",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:GetObjectTagging",
            "s3:GetObjectVersion",
            "s3:GetReplicationConfiguration",
            "s3:ListBucket",
            "s3:ListBucketVersions",
            "s3:PutBucketAcl",
            "s3:PutBucketTagging",
            "s3:PutEncryptionConfiguration",
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:PutObjectTagging",
            "servicequotas:GetServiceQuota",
            "servicequotas:ListAWSDefaultServiceQuotas",
            "sts:AssumeRole",
            "sts:AssumeRoleWithWebIdentity",
            "sts:GetCallerIdentity",
            "tag:GetResources",
            "tag:UntagResources",
            "kms:DescribeKey",
            "cloudwatch:GetMetricData",
            "ec2:CreateRoute",
            "ec2:DeleteRoute",
            "ec2:CreateVpcEndpoint",
            "ec2:DeleteVpcEndpoints",
            "ec2:CreateVpcEndpointServiceConfiguration",
            "ec2:DeleteVpcEndpointServiceConfigurations",
            "ec2:DescribeVpcEndpointServiceConfigurations",
            "ec2:DescribeVpcEndpointServicePermissions",
            "ec2:DescribeVpcEndpointServices",
            "ec2:ModifyVpcEndpointServicePermissions"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
```

```
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```



重要

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

前提条件

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

手順

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

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

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

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

出力例

```
{
    "Policy": {
```

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

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

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

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

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

出力例

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

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

例3.17 sts_installer_privatelink_permission_boundary_policy.json

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

```
    }
  ]
}
```

例3.18 sts_installer_vpc_permission_boundary_policy.json

```
{
    "Version": "2012-10-17",
   "Statement": [
      {
          "Effect": "Allow",
          "Action": [
    "ec2:AssociateDhcpOptions",
    "ec2:AssociateRouteTable",
    "ec2:AttachInternetGateway",
    "ec2:CreateDhcpOptions",
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet",
    "ec2:CreateVpc",
    "ec2:DeleteDhcpOptions",
    "ec2:DeleteInternetGateway",
    "ec2:DeleteNatGateway",
    "ec2:DeleteRouteTable",
    "ec2:DeleteSubnet",
    "ec2:DeleteVpc",
    "ec2:DetachInternetGateway",
    "ec2:DisassociateRouteTable",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:ReplaceRouteTableAssociation"
          ],
          "Resource": "*"
      }
   ]
}
```

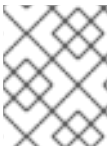
関連情報

- 詳細は、AWS ドキュメントの IAM エンティティーのアクセス許可の境界 を参照してください。
- 必要なアカウント全体の STS ロールとポリシーの作成の詳細は アカウント全体の STS ロールとポリシーの作成 を参照してください。

3.4. クラスター固有の OPERATOR IAM ロール参照

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

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



注記

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

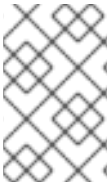
表3.14 ROSA クラスター固有の Operator ロール

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

3.4.1. 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。

3.4.2. カスタム Operator IAM ロールの接頭辞について

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

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

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

クラスターの Operator ロールを作成する場合は、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 Cloud Credential Operator のロール名は **mycluster-dev-openshift-cloud-credential-operator-cloud-credenti** です。

注記

ロール名は 64 文字に切り捨てられます。

関連情報

For steps to create the cluster-specific Operator IAM roles using a custom prefix, see link:https://docs.redhat.com/en/documentation/red_hat_openshift_service_on_aws/4/html-single/install_rosa_classic_clusters/#rosa-sts-creating-cluster-customizations-cli_rosa-sts-creating-a-cluster-with-customizations[Creating a cluster with customizations using the CLI] or

> link:https://docs.redhat.com/en/documentation/red_hat_openshift_service_on_aws/4/html-single/install_rosa_classic_clusters/#rosa-sts-creating-cluster-customizations-ocm_rosa-sts-creating-a-cluster-with-customizations[Creating a cluster with customizations by using {cluster-manager}].

3.5. 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。

3.5.1. 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。

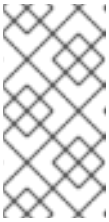
前提条件

- 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) ID 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 ID プロバイダーでサムプリントをしようする方法の詳細は、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'
```

3.5.2. 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。

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

前提条件

- インストールホストに、最新の Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールして設定している。

手順

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

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

このコマンドは次の情報を返します。

出力例

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

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

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

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

(1) 上記の出力例では、OIDC 設定 ID は 13cdr6b です。

- 次のコマンドを実行して、変数の値を表示します。

```
$ echo $OIDC_ID
```

出力例

```
13cdr6b
```

検証

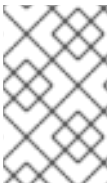
- ユーザー組織に関連付けられているクラスターで使用できる可能な OIDC 設定をリストできます。以下のコマンドを実行します。

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

出力例

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

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。

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
```

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、**自動** 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>
```

管理
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'
```

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

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

注記

AWS 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。

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

	サービス	アクション	効果
	AWS Tiro	CreateQuery GetQueryAnswer GetQueryExplanation	許可
	AWS Marketplace	サブスクライブ サブスクライブ解除 サブスクリプションの表示	許可
	AWS Resource Tagging	すべて	許可
	AWS Route53 DNS	すべて	許可
	AWS Service Quotas	ListServices GetRequestedServiceQuotaChange GetServiceQuota RequestServiceQuotaIncrease ListServiceQuotas	許可
オプション	AWS Billing	ViewAccount Viewbilling 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

3.7. 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 ロールにカスタマー管理ポリシーをアタッチできます。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

- インストーラーロールのパーミッション境界
- IAM エンティティーのパーミッション境界

第4章 OPENID CONNECT の概要

OpenID Connect (OIDC) は、セキュリティートークンサービス (STS) を使用して、クライアントが Web ID トークンを提供して複数のサービスにアクセスできるようにします。クライアントが STS を使用してサービスにサインインすると、トークンは OIDC ID プロバイダーに対して検証されます。

OIDC プロトコルは、クライアントの ID を認証するために必要な情報を含む設定 URL を使用します。プロトコルは、プロバイダーがクライアントを検証してサインインするために必要な認証情報をプロバイダーに応答します。

Red Hat OpenShift Service on AWS クラスターは、STS と OIDC を使用して、クラスター内のオペレーターに必要な AWS リソースへのアクセスを許可します。

4.1. OIDC 検証オプションについて

OIDC 検証には 3 つのオプションがあります。

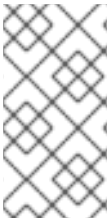
- 未登録のマネージド OIDC 設定
  未登録のマネージド OIDC 設定は、クラスターのインストールプロセス中に作成されます。設定は Red Hat の AWS アカウントでホストされます。このオプションでは、OIDC 設定にリンクする ID は提供されないため、このタイプの OIDC 設定は単一クラスターでのみ使用できます。

- 登録されたマネージド OIDC 設定
  クラスターの作成を開始する前に、登録済みのマネージド OIDC 設定を作成します。この設定は、未登録のマネージド OIDC 設定と同様に、Red Hat の AWS アカウントでホストされます。OIDC 設定にこのオプションを使用すると、OIDC 設定にリンクする ID を受け取ります。Red Hat は、この ID を使用して発行者の URL と秘密鍵を識別します。次に、この URL と秘密キーを使用して、認証プロバイダーと Operator ロールを作成できます。これらのリソースは、Identity and Access Management (IAM) AWS サービスを使用して、AWS アカウントの下に作成されます。クラスターの作成プロセス中に OIDC 設定 ID を使用することもできます。

- 登録済みのアンマネージドの OIDC 設定
  クラスターの作成を開始する前に、登録済みのアンマネージド OIDC 設定を作成できます。この設定は AWS アカウントでホストされます。このオプションを使用する場合は、秘密キーを管理する責任があります。Red Hat OpenShift Cluster Manager に設定を登録するには、AWS Secrets Manager (SM) サービスと設定をホストする発行者 URL を使用して AWS Secrets ファイルに秘密キーを保存します。Red Hat OpenShift Service on AWS (ROSA) CLI である **rosa** を使用して、**rosa create oidc-config --managed=false** コマンドを使用して、登録されたアンマネージドの OIDC 設定を作成できます。このコマンドは、アカウントの下に設定を作成してホストし、必要なファイルと秘密鍵を作成します。このコマンドは、OpenShift Cluster Manager に設定を登録します。

登録されたオプションを使用して、クラスターの作成を開始する前に必要な IAM リソースを作成できます。このオプションを選択すると、クラスターの作成中に待機時間があり、OIDC プロバイダーと Operator のロールを作成するまでインストールが一時停止するため、インストール時間が短縮されます。

ROSA Classic の場合は、任意の OIDC 設定オプションを使用できます。HCP で ROSA を使用している場合は、マネージドまたはアンマネージドとして登録済みの OIDC 設定を作成する必要があります。登録された OIDC 設定を他のクラスターと共有できます。この設定を共有する機能により、プロバイダーと Operator のロールを共有することもできます。



注記

実稼働クラスターでは認証検証がクラスター全体で使用されるため、クラスター間で OIDC 設定、OIDC プロバイダー、および Operator のロールを再利用することは推奨できません。Red Hat は、非実稼働テスト環境でのみリソースを再利用することを推奨します。

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。

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

前提条件

- インストールホストに、最新の Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**) をインストールして設定している。

手順

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

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

このコマンドは次の情報を返します。

出力例

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

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

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

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

1 上記の出力例では、OIDC 設定 ID は 13cdr6b です。

- 次のコマンドを実行して、変数の値を表示します。

```
$ echo $OIDC_ID
```

出力例

```
13cdr6b
```

検証

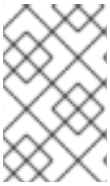
- ユーザー組織に関連付けられているクラスターで使用できる可能な OIDC 設定をリストできます。以下のコマンドを実行します。

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

出力例

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

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。

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
```

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、**自動** 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>
```

管理
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'
```

4.3. 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) ID 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 ID プロバイダーでサムプリントをしようする方法の詳細は、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'
```

4.4. 関連情報

- ROSA Classic の手順は、OpenID Connect 設定の作成 を参照してください。
- HCP を使用した ROSA の OpenID Connect 設定の作成 の手順を参照してください。