aws

ユーザーガイド

Red Hat OpenShift Service on AWS

Red Hat OpenShift Service on AWS: ユーザーガイド

Table of Contents

とは Red Hat OpenShift Service on AWS

Red Hat OpenShift Service on AWS (ROSA) は、オンプレミスの Red Hat OpenShift OpenShift ワークロードを に移行する Red Hat OpenShift エンタープライズ Kubernetes プラットフォーム on AWS. ROSA streamlines を使用してコンテナ化されたアプリケーションを構築、スケーリング、デプロイするために使用できるマネージドサービスであり AWS、他の と緊密に統合されています AWS のサービス。

機能

ROSA は、 と Red Hat によって共同でサポート AWS および運用されています。各 ROSA クラスターには、Red Hat の 99.95% の稼働時間サービスレベルアグリーメント (SLA) に基づくクラスター管理の 24 時間 Red Hat サイト信頼性エンジニア (SRE) サポートが付属しています。サービスのサポートモデルの詳細については、「」を参照してくださいthe section called “サポート情報”。

ROSA には、次の機能も用意されています。

- Red Hat SRE 対応クラスターインストール、クラスターメンテナンス、クラスターアップグレード。
- AWS のサービス 統合には、 AWS コンピューティング、データベース、分析、機械学習、ネットワーク、モバイルが含まれます。
- Kubernetes コントロールプレーンを複数の AWS アベイラビリティーゾーンで実行してスケーリングし、高可用性を確保します。
- OpenShift API と、サービスメッシュ、CodeReady ワークスペース、サーバーレスなどの開発者生産性向上ツールを使用してクラスターを運用します。

アクセス ROSA

次のインターフェイスを使用して、 ROSA サービスデプロイを定義および設定できます。

AWS

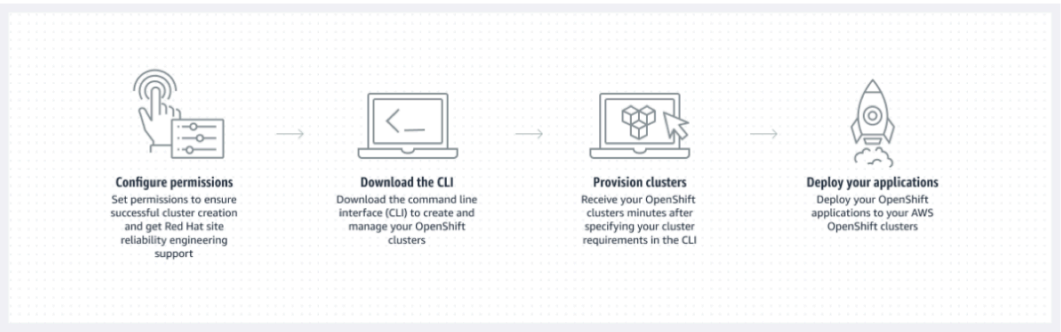
- ROSA コンソール — ROSA サブスクリプションを有効にして ROSA ソフトウェア契約を購入するためのウェブインターフェイスを提供します。

- AWS Command Line Interface (AWS CLI) — Windows、macOS、および Linux で AWS のサービス サポートされている の幅広いセットのコマンドを提供します。詳細については、「AWS Command Line Interface」を参照してください。

Red Hat OpenShift

- Red Hat Hybrid Cloud Console — ROSA クラスターの作成、更新、管理、クラスターアドオンのインストール、 ROSA クラスターへのアプリケーションの作成とデプロイを行うためのウェブインターフェイスを提供します。
- ROSA CLI (rosa) — ROSA クラスターを作成、更新、管理するコマンドを提供します。
- OpenShift CLI (oc) — アプリケーションを作成し、OpenShift コンテナプラットフォームプロジェクトを管理するコマンドを提供します。
- Knative CLI (kn) - Knative Serving や Eventing などの OpenShift Serverless コンポーネントとやり取りするために使用できるコマンドを提供します。
- Pipelines CLI (tkn) - ターミナルを使用して OpenShift Pipelines を操作するコマンドを提供します。
- opm CLI - オペレータ開発者とクラスター管理者がターミナルから OpenShift Operator カタログを作成および維持するのに役立つコマンドを提供します。
- オペレータ SDK CLI - オペレータ開発者が OpenShift オペレータの構築、テスト、デプロイに使用できるコマンドを提供します。

の使用を開始する方法 ROSA



以下は、 の開始プロセスの概要です ROSA。開始方法の詳細については、「」を参照してくださいの使用を開始する ROSA 。

AWS Management Console/AWS CLI

1. サービス機能を提供するために ROSA が依存 AWS のサービス する のアクセス許可を設定します。詳細については、「the section called “前提条件”」を参照してください。
2. 最新の AWS CLI ツールをインストールして設定します。詳細については、「 ユーザーガイド」の「 の最新バージョンの更新 AWS CLIのインストール」を参照してください。 AWS CLI
3. ROSA コンソール ROSA で を有効にします。

Red Hat Hybrid Cloud コンソール/ROSA CLI

1. Red Hat Hybrid Cloud Console ROSA から CLI と OpenShift CLI の最新バージョンをダウンロードします。詳細については、Red Hat ドキュメントの「 CLI ROSA の開始方法」を参照してください。
2. Red Hat Hybrid Cloud Console または CLI ROSA で ROSA クラスターを作成します。
3. クラスターの準備ができたら、クラスターへのユーザーアクセスを許可するように ID プロバイダーを設定します。
4. 他の OpenShift 環境と同じ方法で ROSA 、クラスターにワークロードをデプロイして管理します。

料金

の合計コスト ROSA は、 ROSA サービス料金と AWS インフラストラクチャ料金の 2 つのコンポーネントで構成されます。料金の詳細については、「Red Hat OpenShift Service on AWS 料金」を参照してください。

ROSA サービス料金

デフォルトでは、 ROSA サービス料金はワーカーノードで使用される 4 vCPU ごとに時間単位でオンデマンドで発生します。サービス料金は、サポートされているすべての AWS 標準リージョンで統一されています。ワーカーノードサービス料金に加えて、ホストされたコントロールプレーン (HCP) クラスターを持つ ROSA には、時間単位のクラスター料金が発生します。

ROSA では、ワーカーノードのオンデマンドサービス料金を節約するために購入できる 1 年および 3 年サービス料金契約を提供しています。詳細については、「the section called “ROSA 契約の購入”」を参照してください。

AWS インフラストラクチャ料金

AWS インフラストラクチャ料金は、 AWS 基盤となるワーカーノード、インフラストラクチャノード、コントロールプレーンノード、ストレージ、グローバルインフラストラクチャでホストされているネットワークリソースに適用されます。 AWS インフラストラクチャ料金は によって異なります AWS リージョン。

の責任の概要 ROSA

このドキュメントでは、 Amazon Web Services (AWS)、Red Hat、および Red Hat OpenShift Service on AWS (ROSA) マネージドサービスのお客様の責任の概要を説明します。 ROSA とそのコンポーネントの詳細については、Red Hat ドキュメントの「ポリシーとサービス定義」を参照してください。

責任AWS 共有モデルは、 で提供されるすべてのサービスを実行するインフラストラクチャを保護する AWS 責任を定義します AWS クラウド ROSA。 AWS インフラストラクチャには、 AWS クラウド サービスを実行するハードウェア、ソフトウェア、ネットワーク、施設が含まれます。この AWS 責任は一般的に「クラウドのセキュリティ」と呼ばれます。フルマネージドサービス ROSA として運用するために、Red Hat とお客様は、 AWS 責任モデルが「クラウド内のセキュリティ」として定義するサービスの要素に責任を負います。

Red Hat は、 ROSA クラスターインフラストラクチャ、基盤となるアプリケーションプラットフォーム、オペレーティングシステムの継続的な管理とセキュリティを担当します。 ROSA クラスターはお客様の AWS リソースでホストされますが AWS アカウント、お客様が作成した IAM ロールを通じて、 ROSA サービスコンポーネントと Red Hat サイト信頼性エンジニア (SREs) によってリモートでアクセスされます。Red Hat はこのアクセスを使用して、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ノードのデプロイとキャパシティを管理し、コントロールプレーンノード、インフラストラクチャノード、ワーカーノードのバージョンを管理します。

Red Hat とお客様は、 ROSA ネットワーク管理、クラスターのログ記録、クラスターのバージョニング、キャパシティ管理の責任を共有します。Red Hat が ROSA サービスを管理する間、お客様はデプロイ先のアプリケーション、ワークロード、データの管理と保護に全責任を負います ROSA。

概要:

次の表に AWS、Red Hat とお客様の責任の概要を示します Red Hat OpenShift Service on AWS。

> **Note**
>
> `cluster-admin` ロールがユーザーに追加されている場合は、「Red Hat Enterprise 免責事項の付録 4 (オンラインサブスクリプションサービス)」の責任と免責事項を参照してください。

[リソース]	インシデント管理と運用管理	変更管理	アクセスと ID 認可	セキュリティと規制の遵守	ディザスタリカバリ
顧客データ	カスタマー	カスタマー	カスタマー	カスタマー	お客様
カスタマーアプリケーション	カスタマー	カスタマー	カスタマー	カスタマー	お客様
デベロッパー用サービス	カスタマー	カスタマー	カスタマー	カスタマー	お客様
プラットフォーム監視	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
ログ記録	Red Hat	Red Hat とお客様	Red Hat とお客様	Red Hat とお客様	Red Hat
アプリケーションネットワーク	Red Hat とお客様	Red Hat とお客様	Red Hat とお客様	Red Hat	Red Hat
クラスターネットワーク	Red Hat	Red Hat とお客様	Red Hat とお客様	Red Hat	Red Hat
仮想ネットワーク管理	Red Hat とお客様	Red Hat とお客様	Red Hat とお客様	Red Hat とお客様	Red Hat とお客様
仮想コンピューティング管理 (コ	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat

[リソース]	インシデント管理と運用管理	変更管理	アクセスと ID 認可	セキュリティと規制の遵守	ディザスタリカバリ
ントロールプレーン、インフラストラクチャ、ワーカーノード)					
クラスターバージョン	Red Hat	Red Hat とお客様	Red Hat	Red Hat	Red Hat
キャパシティ管理	Red Hat	Red Hat とお客様	Red Hat	Red Hat	Red Hat
仮想ストレージ管理	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS ソフトウェア (パブリック AWS のサービス)	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	AWS	AWS	AWS	AWS	AWS

地域別の責任分担に関するタスク

AWS、Red Hat、および のお客様は、 ROSA コンポーネントのモニタリングとメンテナンスの責任を共有します。このドキュメントでは、エリアとタスクごとに ROSA サービスの責任を定義します。

インシデント管理と運用管理

AWS は、 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を保護する責任があります AWS クラウド。Red Hat は、デフォルトプラットフォームネットワークに必要なサービスコンポーネントの管理を担当します。お客様は、お客様のアプリケーションデータ、およびお客様が設定したカスタムネットワークのインシデント管理と運用管理に責任を負います。

[リソース]	サービス責任	お客様の責任
アプリケーションネットワーク	Red Hat • ネイティブ OpenShift ルーターサービスを監視し、アラートに対応します。	お客様 • アプリケーションルートとその背後にあるエンドポイントの正常性を監視します。 • AWS および Red Hat に停止を報告します。
仮想ネットワーク管理	Red Hat • 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 ロードバランサー、 Amazon VPC サブネット、 AWS のサービスコンポーネントをモニタリングします。アラートに対応します。	お客様 • AWS ロードバランサーエンドポイントのヘルスをモニタリングします。 • オプションで VPC Amazon VPCへの接続、接続 Site-to-Site VPN 、または潜在的な問題やセキュリティの脅威を介して設定されるネットワークトラフィック Direct Connect をモニタリングします。
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イメージ	お客様 • アプリケーションデータの正常性を監視します。 • カスタマーマネージド AWS KMS keys を使用する場合

[リソース]	サービス責任	お客様の責任
	レジストリに使用される Amazon S3 バケットをモニタリングします。アラートに対応します。	は、 Amazon EBS 暗号化用のキーライフサイクルとキーポリシーを作成して制御します。
AWS ソフトウェア (パブリック AWS のサービス)	AWS • AWS インシデントと運用管理の詳細については、 AWS ホワイトペーパーの「 が運用レジリエンスとサービスの継続性 AWS を維持する方法」を参照してください。	お客様 • カスタマーアカウントの AWS リソースの正常性をモニタリングします。 • IAM ツールを使用して、お客様のアカウントの 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	AWS • AWS インシデントと運用管理の詳細については、 AWS ホワイトペーパーの「 が運用レジリエンスとサービスの継続性 AWS を維持する方法」を参照してください。	お客様 • お客様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制御が適切に実施されていることを確認します。

変更管理

AWS は、 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を保護する責任があります AWS クラウド。Red Hat は、コントロールプレーンノード、インフラストラクチャノード、ワーカーノードのバージョン管理だけでなく、お客様が管理するクラスターインフラストラクチャとサービスへの変更を可能にすることにも責任を負います。インフラストラクチャの変更を開始する責任はお客様にあります。また、オプションサービスのインストールと保守、クラスター上のネットワーク構成、顧客データやアプリケーションの変更もお客様の責任となります。

[リソース]	サービス責任	お客様の責任
ログ記録	Red Hat • プラットフォーム監査ログを一元的に集約して監視します。 • お客様がデフォルトのアプリケーションログ記録用のログ記録スタックをデプロイできるように、ログ記録オペレーターを提供および管理します。 • お客様の要求に応じて監査ログを提供します。	お客様 • オプションとして、デフォルトのアプリケーションログ記録オペレーターをクラスターにインストールします。 • ログ記録サイドカーコンテナやサードパーティのログ記録アプリケーションなど、オプションのアプリケーションログ記録用ソリューションをインストール、設定、保守します。 • 顧客アプリケーションが生成するアプリケーションログがログ記録スタックやクラスターの安定性に影響する場合は、サイズと頻度を調整してください。 • 特定のインシデントを調査するために、サポートケースを通じてプラットフォーム監査ログをリクエストしてください。
アプリケーションネットワーク	Red Hat • パブリックロードバランサーをセットアップします。必要に応じて、プライベートロードバランサーと最大 1 つの追加ロードバランサーをセットアップできるようにします。	お客様 • `NetworkPolicy` オブジェクトを使用して、プロジェクトとポッドネットワーク、ポッドの入口、およびポッドの出口に対して、デフォルト以外のポッドネッ

[リソース]	サービス責任	お客様の責任
	• ネイティブ OpenShift ルーターサービスをセットアップします。ルーターをプライベートに設定し、ルーターシャードを 1 つまで追加できるようにします。 • デフォルトの内部ポッドトラフィック用に OpenShift SDN コンポーネントをインストール、設定、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ようにします。	トワーク権限を設定します。 • 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用のプライベートロードバランサーをリクエストします。 • OpenShift Cluster Manager を使用して、パブリックまたはプライベートのルーターシャードとそれに対応するロードバランサーを最大 1 つ追加設定します。 • 特定のサービス用に、追加のサービスロードバランサーをリクエストして設定します。 • 必要な DNS 転送ルールを設定します。

[リソース]	サービス責任	お客様の責任
クラスターネットワーク	Red Hat • パブリックまたはプライベートサービスエンドポイントや必要なコンポーネントとの統合などのクラスター管理 Amazon VPC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、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。	お客様 • クラスターのプロビジョニング時に OpenShift Cluster Manager を使用して、必要に応じてマシン CIDR、サービス CIDR、ポッド CIDR のデフォルト以外の IP アドレス範囲をオプションで提供します。 • クラスターの作成時、または OpenShift Cluster Manager によるクラスター作成後に 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リクエストします。

[リソース]	サービス責任	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 コンポーネントを設定および設定します。 • OpenShift Cluster Manager を使用して、オンプレミスリソースと Site-to-Site VPN の接続、VPC Amazon VPC への接続、および Direct Connect 必要に応じて を管理できるようにします。 • お客様がサービス AWS ロードバランサーで使用する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。	お客様 • VPC Amazon VPCへの接続、接続、 Site-to-Site VPN などのオプション Amazon VPC コンポーネントを設定および維持します Direct Connect。 • 特定のサービス用に、追加のロードバランサーをリクエストして設定します。

[リソース]	サービス責任	お客様の責任
仮想コンピュート管理	Red Hat • クラスター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設定および設定します。 • クラスター上の Amazon EC2 コントロールプレーンノードとインフラストラクチャノードのデプロイを監視および管理します。	お客様 • OpenShift クラスターマネージャーまたは CLI を使用してマシンプールを作成して、 Amazon EC2 ワーカーノードをモニタリングおよび管理 ROSA します。 • お客様がデプロイ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。
クラスターバージョン	Red Hat • アップグレードのスケジュール設定プロセスを有効にします。 • アップグレードの進行状況を監視し、発生した問題を解決します。 • マイナーアップグレードやメンテナンスアップグレードに関する変更ログとリリースノートを公開します。	お客様 • メンテナンスバージョンのアップグレードは、即時または将来にスケジュールするか、自動アップグレードを設定できます。 • マイナーバージョンアップグレードを確認してスケジュールを設定します。 • クラスターバージョンが、サポートされているマイナーバージョンのままであることを確認してください。 • お客様のアプリケーションをマイナーバージョンとメンテナンスバージョンでテストして、互換性を確認します。

[リソース]	サービス責任	お客様の責任
キャパシティ管理	Red Hat • コントロールプレーンの使用状況を監視します。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ノードが含まれます。 • サービス品質を維持するために、コントロールプレーンノードをスケーリングおよびサイズ変更します。	お客様 • ワーカーノードの使用状況を監視し、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戦略を決定します。 • 提供されている OpenShift Cluster Manager コントロールを使用して、必要に応じて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。

[リソース]	サービス責任	お客様の責任
仮想ストレージ管理	Red Hat • 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 Amazon EBS するように を設定および設定します。 • 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を設定および設定します。 • でイメージレジストリリソースを定期的にプルーニング Amazon S3 して、Amazon S3 使用状況とクラスターのパフォーマンスを最適化します。	お客様 • 必要に応じて Amazon EBS 、クラスターに永続的ボリュームをプロビジョニングするように CSI Amazon EFS ドライバーまたは CSI ドライバーを設定します。

[リソース]	サービス責任	お客様の責任

AWS ソフトウェア (パブリック AWS サービス)	AWS
	
	コンピューティング
	
	• ROSA コントロールプレーン、インフラストラクチャ、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 (ストレージ)]
	
	• ROSA サービスが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できるように Amazon EBS を指定します。
	
	ネットワーク
	
	• ROSA 仮想ネットワークインフラストラクチャのニーズを満たすために、次の AWS クラウド サービスを提供します。
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• 次のオプション AWS のサービス の統合を指定します ROSA。
	  • Site-to-Site VPN
	  • Direct Connect
		お客様
		
		• プリンシ IAM パルまたは AWS STS 一時的なセキュリティ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。
		• 必要に応じて、 ROSA クラスターで使用するカスタマーマネージド VPC を設定します。

[リソース]	サービス責任	お客様の責任
	• AWS PrivateLink • AWS Transit Gateway	
ハードウェア/AWS グローバルインフラストラクチャ	AWS • AWS データセンターの管理コントロールの詳細については、 AWS クラウド 「 セキュリティ」ページの「コントロール」を参照してください。 • 変更管理のベストプラクティスについては、 AWS 「 ソリューションライブラリ」の「 での変更管理のガイダンス AWS」を参照してください。	お客様 • AWS クラウドでホストされている顧客アプリケーションとデータに変更管理のベストプラクティスを実装します。

アクセスと ID 認可

アクセスと ID の認可には、クラスタ、アプリケーション、インフラストラクチャリソースへの許可されたアクセスを管理する責任が含まれます。これには、アクセス制御メカニズムの提供、認証、認可、リソースへのアクセスの管理などのタスクが含まれます。

[リソース]	サービス責任	お客様の責任
ログ記録	Red Hat • プラットフォーム監査ログには、業界標準に基づく段階的な内部アクセスプロセスを遵守してください。 • ネイティブの OpenShift RBAC 機能を提供します。	お客様 • OpenShift RBAC を設定して、プロジェクト、ひいては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します。 • サードパーティ製またはカスタムのアプリケーション

[リソース]	サービス責任	お客様の責任
		ログ記録ソリューションの場合、アクセス管理はお客様の責任となります。
アプリケーションネットワーク	Red Hat • ネイティブの OpenShift RBAC と `dedicated-admin` 機能を提供します。	お客様 • 必要に応じて、ルート設定へのアクセスを制御するために OpenShift `dedicated-admin` と RBAC を設定します。 • Red Hat の Red Hat 組織管理者を管理して OpenShift Cluster Manager へのアクセス権を付与します。クラスターマネージャーはルーターオプションの設定とサービスロードバランサーのクォータの提供に使用されます。
クラスターネットワーク	Red Hat • OpenShift クラスターマネージャーを通じて顧客がアクセス制御を行えるようにします。ネイティブの OpenShift RBAC と `dedicated-admin` 機能を提供します。	お客様 • 必要に応じて、ルート設定へのアクセスを制御するために OpenShift `dedicated-admin` と RBAC を設定します。 • Red Hat アカウントの Red Hat 組織メンバーシップを管理します。 • Red Hat の組織管理者を管理して OpenShift Cluster Manager へのアクセス権を付与します。

[リソース]	サービス責任	お客様の責任
仮想ネットワーク管理	Red Hat • OpenShift クラスターマネージャーを通じて顧客がアクセス制御を行えるようにします。	お客様 • OpenShift Cluster Manager を使用して、 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。
仮想コンピュート管理	Red Hat • OpenShift クラスターマネージャーを通じて顧客がアクセス制御を行えるようにします。	お客様 • OpenShift Cluster Manager を使用して、 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 サービスアクセスを有効にするために必要な IAM ロールとアタッチされたポリシーを作成します。
仮想ストレージ管理	Red Hat • OpenShift クラスターマネージャーを通じて顧客がアクセス制御を行えるようにします。	お客様 • OpenShift Cluster Manager を使用して、 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 サービスアクセスを有効にするために必要な 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 コンピューティング • ROSA コントロールプレーン、インフラストラクチャ、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 (ストレージ)] • クラスター ROSA 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のプロビジョニングを に許可する Amazon EBSために使用される を指定します。 • サービスの組み込みイメージレジストリ Amazon S3に使用される を指定します。 ネットワーク • Provide AWS Identity and Access Management (IAM)。お客様のアカウントで実行されている ROSA リソースへのアクセスを制御するために、お客様が使用します。	お客様 • ROSA サービスアクセスを有効にするために必要な 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、お客様のアカウントの 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 ROSA で 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 ROSA で を有効にするには、 を使用して ROSA 使用権限付与を配布する責任があります AWS License Manager。

[リソース]	サービス責任	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	AWS • AWS データセンターの物理アクセスコントロールの詳細については、 AWS クラウド 「 セキュリティ」ページの「コントロール」を参照してください。	お客様 • お客様は、 AWS グローバルインフラストラクチャについて責任を負いません。

セキュリティと規制の遵守

次に、コンプライアンスに関連する責任と統制を示します。

[リソース]	サービス責任	お客様の責任
ログ記録	Red Hat • クラスター監査ログを Red Hat SIEM に送信して、セキュリティイベントを分析します。フォレンジック分析に役立つよう、監査ログを一定期間保持します。	お客様 • セキュリティイベントのアプリケーションログを分析します。 • デフォルトのログ記録スタックで提供されているよりも長い保存期間が必要な場合は、ログ記録サイドカーコンテナまたはサードパーティのログ記録アプリケーションを使用して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上の脅威について、仮	お客様 • 潜在的な問題やセキュリティ上の脅威について、

[リソース]	サービス責任	お客様の責任
	想ネットワークコンポーネントを監視します。 • 追加のモニタリングと保護には、パブリック AWS ツールを使用します。	任意に設定した仮想ネットワーク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や顧客データセンターの保護を設定します。
仮想コンピュート管理	Red Hat • 潜在的な問題やセキュリティ上の脅威について、仮想コンピュートコンポーネントを監視します。 • 追加のモニタリングと保護には、パブリック AWS ツールを使用します。	お客様 • 潜在的な問題やセキュリティ上の脅威について、任意に設定した仮想ネットワーク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や顧客データセンターの保護を設定します。

[リソース]	サービス責任	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上の脅威について、仮想ストレージコンポーネントを監視します。 • 追加のモニタリングと保護には、パブリック AWS ツールを使用します。 • Amazon EBS が提供する AWS マネージド KMS キーを使用して、コントロールプレーン、インフラストラクチャ、ワーカーノードボリュームデータをデフォルトで暗号化するように ROSA サービスを設定します。 • Amazon EBS が提供する AWS マネージド 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カスタマー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。 • お客様がカスタマー管理のを使用して永続ボリューム KMS key を暗号化する機能を提供します。 • Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-3) を使用して、保管中のイメージレジストリ	お客様 • 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、ボリュームとしてマウントするのに十分なストレージを確保します ROSA。 • OpenShift Cluster Manager を使用して永続ボリュームクレームを作成し、永続ボリュームを生成します。

[リソース]	サービス責任	お客様の責任
	データを暗号化するようにコンテナイメージレジストリを設定します。 • 顧客がパブリックイメージレジストリまたはプライベート Amazon S3 イメージレジストリを作成して、コンテナイメージを不正なユーザーアクセスから保護できるようにします。	

[リソース]	サービス責任	お客様の責任
AWS ソフトウェア (パブリック AWS サービス)	AWS コンピューティング • ROSA コントロールプレーン Amazon EC2、インフラストラクチャ、ワーカーノードに使用します。詳細については、「 Amazon EC2 ユーザーガイド」の「 のインフラストラクチャセキュリティ Amazon EC2」を参照してください。 [Storage (ストレージ)] • ROSA コントロールプレーン Amazon EBS、インフラストラクチャ、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します。詳細については、「 Amazon EC2 ユーザーガイド」の「 でのデータ保護 Amazon EC2」を参照してください。 • は、 ROSA を使用してコントロールプレーン AWS KMS、インフラストラクチャ、ワーカーノードボリューム、永続ボリュームを暗号化します。詳細については、「 Amazon EC2 ユーザーガイド」のAmazon	お客様 • Amazon EC2 インスタンス上のデータを保護するために、セキュリティのベストプラクティスと最小特権の原則に従っていることを確認します。詳細については、「Amazon EC2におけるインフラストラクチャセキュリティ」および「Amazon EC2におけるデータ保護」を参照してください。 • 潜在的な問題やセキュリティ上の脅威について、任意に設定した仮想ネットワーク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や顧客データセンターの保護を設定します。 • オプションのカスタマーマネージド KMS キーを作成し、KMS キーを使用して永 Amazon EBS 続ボリュームを暗号化します。 • 潜在的な問題やセキュリティ上の脅威について、仮想ストレージコンポーネントを監視します。詳細については、AWS 責任共有モデルを参照してください。

[リソース]	サービス責任	お客様の責任
	EBS 「暗号化」を参照してください。 • ROSA サービスの組み込みコンテナイメージレジストリ Amazon S3に使用されます。詳細については、「 Amazon S3 ユーザーガイド」のAmazon S3 「セキュリティ」を参照してください。 ネットワーク • 組み込みのネットワークファイアウォール、プライベートネットワーク接続または専用ネットワーク接続 Amazon VPC、 AWS 保護された施設間の AWS グローバルネットワークおよびリージョン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、 AWS グローバルインフラストラクチャのプライバシーを強化し、ネットワークアクセスを制御するセキュリティ機能およびサービスを提供します。詳細については、「セキュリティ入門ホワイトペーパー」のAWS 「責任共有モデルとインフラストラクチャ AWS のセキュ	

[リソース]	サービス責任	お客様の責任
	リティ」を参照してください。	
ハードウェア/AWS グローバルインフラストラクチャ	AWS • がサービス機能を提供するために ROSA 使用する AWS グローバルインフラストラクチャを提供します。AWS セキュリティコントロールの詳細については、AWS ホワイトペーパーの AWS 「インフラストラクチャのセキュリティ」を参照してください。 • コンプライアンスのニーズを管理し、 AWS Artifact や Security Hub AWS などの AWS ツールを使用して のセキュリティ状態をチェックするためのドキュメントを顧客に提供します。	お客様 • お客様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、お客様のアカウントの AWS リソースに適切なアクセス許可を適用します。

ディザスタリカバリ

ディザスタリカバリには、データと設定のバックアップ、ディザスタリカバリ環境のデータ複製と設定、および障害発生時のフェイルオーバーが含まれます。

[リソース]	サービス責任	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、影響を受ける仮想ネットワークコン	お客様 • 障害から保護するため、可能な場合は複数のトンネル

[リソース]	サービス責任	お客様の責任
	ポーネントを復元または再作成します。	を使用して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 と負荷分散を維持してください。
仮想コンピュート管理	Red Hat • クラスターをモニタリングし、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ノードを置き換えます。 • 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ようにします。	お客様 • OpenShift クラスターマネージャーまたは ROSA CLI を使用し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。
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 AWS 作成された ROSA クラスターの場合、クラスター上のすべての Kubernetes オブジェクトを時間単位、日単位、週単位のボリュームスナップショットでバックアップします。	お客様 • 顧客アプリケーションとアプリケーションデータをバックアップします。

[リソース]	サービス責任	お客様の責任
AWS ソフトウェア (パブリック AWS サービス)	AWS コンピューティング • Amazon EBS スナップショットや などのデータの耐障害性をサポートする Amazon EC2 機能を提供します Amazon EC2 Auto Scaling。詳細については、「 Amazon EC2 ユーザーガイド」の「 の耐障害性 Amazon EC2」を参照してください。 [Storage (ストレージ)] • ROSA サービスおよびお客様が Amazon EBS ボリュームスナップショットを使用してクラスター上の Amazon EBS ボリュームをバックアップできるようにします。 • データの耐障害性をサポートする Amazon S3 機能の詳細については、「 の耐障害性 Amazon S3」を参照してください。 ネットワーク • データの耐障害性をサポートする Amazon VPC 機能の詳細については、	お客様 • ROSA マルチ AZ クラスターを設定して、耐障害性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。 • 永 Amazon EBS 続ボリュームの CSI ボリュームスナップショットを作成します。

[リソース]	サービス責任	お客様の責任
	「 Amazon VPC ユーザーガイド」の「 の耐障害性 Amazon Virtual Private Cloud」を参照してください。	
ハードウェア/AWS グローバルインフラストラクチャ	AWS • がアベイラビリティーゾーン間でコントロールプレーン、インフラストラクチャ、ワーカーノード ROSA をスケールできるようにする AWS グローバルインフラストラクチャを提供します。この機能を使用すると ROSA 、 はゾーン間で自動フェイルオーバーを中断することなくオーケストレーションできます。 • ディザスタリカバリのベストプラクティスの詳細については、 AWS Well-Architected フレームワークの「クラウドのディザスタリカバリオプション」を参照してください。	お客様 • ROSA マルチ AZ クラスターを設定して、耐障害性とクラスターの可用性を向上させます。

データとアプリケーションに対するお客様の責任

お客様は、デプロイ先のアプリケーション、ワークロード、データに対して責任を負います Red Hat OpenShift Service on AWS。ただし、 AWS Red Hat には、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するのに役立つさまざまなツールが用意されています。

[リソース]	AWS と Red Hat がどのように役立つか	お客様の責任
顧客データ	Red Hat • 業界のセキュリティおよびコンプライアンス基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基準を維持してください。 • 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。 • クラスターの外部や などのデータサービスとの統合を有効に Amazon RDS して、データを保存および管理します AWS。 AWS • を Amazon RDS に提供して、お客様がクラスターの外部でデータを保存および管理できるようにします。	お客様 • プラットフォームに保存されているすべての顧客データ、および顧客アプリケーションがこのデータをどのように消費および公開するかについて、責任を維持します。
カスタマーアプリケーション	Red Hat • OpenShift コンポーネントがインストールされたクラスターをプロビジョニングして、お客様が OpenShift および Kubernetes APIs にアクセスしてコンテナ化されたアプリケーションをデ	お客様 • 顧客とサードパーティのアプリケーション、データ、およびアプリケーションライフサイクル全体に対する責任を維持します。 • お客様が Operator または外部イメージを使用して Red

[リソース]	AWS と Red Hat がどのように役立つか	お客様の責任
	プロイおよび管理できるようにします。 • お客様のデプロイが Red Hat Container Catalog レジストリからイメージを取得できるように、イメージプルシークレットを使用してクラスターを作成します。 • お客様がコミュニティ、サードパーティー、 AWS Red Hat サービスをクラスターに追加するためのオペレーターの設定に使用できる OpenShift APIs へのアクセスを提供します。 • お客様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ためのストレージクラスおよびプラグインを提供します。 • コンテナイメージレジストリを提供して、お客様がアプリケーションのコンテナイメージをクラスターに安全に保管し、アプリケーションをデプロイおよび管理できるようにします。 AWS • カスタマー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ために	Hat、コミュニティ、サードパーティ、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した場合、お客様はそれらのサービスについて責任を負うとともに、適切なプロバイダー (Red Hat を含む) と協力して問題のトラブルシューティングを行う責任を負うものとします。 • 提供されているツールと機能を使用して、設定とデプロイ、最新の状態の維持、リソース要求と制限の設定、アプリケーションを実行するのに十分なリソースを確保するためのクラスターのサイズ設定、権限の設定、他のサービスとの統合、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の管理、外部への配信、データの保存、バックアップ、復元、および可用性が高く回復力のあるワークロードの管理を行います。 • で実行されるアプリケーションをモニタリングする責任を維持します。これには Red Hat OpenShift Service on AWS、メトリ

[リソース]	AWS と Red Hat がどのように役立つか	お客様の責任
	Amazon EBS を提供します。 • コンテナイメージレジストリの Red Hat プロビジョニングをサポートするために Amazon S3 を指定します。	クスの収集、アラートの作成、アプリケーション内のシークレットの保護のためのソフトウェアのインストールと運用が含まれます。

ROSA アーキテクチャ

Red Hat OpenShift Service on AWS (ROSA) には次のクラスタートポロジがあります。

- ホスト型コントロールプレーン (HCP) - コントロールプレーンは Red Hat の 内でホスト AWS アカウント され、Red Hat によって管理されます。ワーカーノードはお客様の にデプロイされます AWS アカウント。
- Classic – コントロールプレーンとワーカーノードは、お客様の にデプロイされます AWS アカウント。

ROSA with HCP は、実行時に発生する AWS インフラストラクチャ料金を削減 ROSA し、クラスター作成時間を短縮するのに役立つ、より効率的なコントロールプレーンアーキテクチャを提供します。HCP を含む ROSA と ROSA Classic の両方を ROSA コンソール AWS で有効にできます。ROSA CLI を使用して ROSA クラスターをプロビジョニングするときに使用するアーキテクチャを選択できます。

> **Note**
>
> - ROSA は、クラシックコントロールプレーンアーキテクチャとホスト型コントロールプレーンアーキテクチャの両方で AWS GovCloud で FedRAMP High および HIPAA 認定コンプライアンス証明書を提供します。詳細については、Red Hat ドキュメントの「コンプライアンス」を参照してください。
> - ROSA は、クラシックコントロールプレーンアーキテクチャとホスト型コントロールプレーンアーキテクチャの両方で AWS GovCloud で連邦情報処理規格 (FIPS) エンドポイントを提供します。

ROSA と HCP および ROSA Classic の比較

次の表は、ROSA と HCP および ROSA クラシックアーキテクチャモデルを比較したものです。

	HCP を備えた ROSA	ROSA Classic
クラスターインフラストラクチャのホスティング	etcd、API サーバー、oauth などのコントロールプレーンコンポーネントは、Red Hat 所有の でホストされます AWS アカウント。	etcd、API サーバー、oauth などのコントロールプレーンコンポーネントは、お客様所有の でホストされます AWS アカウント。
Amazon VPC	ワーカーノードは、 を介してコントロールプレーンと通信しますAWS PrivateLink。	ワーカーノードとコントロールプレーンノードは、お客様の VPC にデプロイされます。
AWS Identity and Access Management	AWS 管理ポリシーを使用します。	サービスによって定義されたカスタマー管理ポリシーを使用します。
マルチゾーンデプロイ	コントロールプレーンは複数のアベイラビリティーゾーン (AZs。	コントロールプレーンは、単一の AZ 内にデプロイすることも、複数の AZs にデプロイすることもできます。
インフラストラクチャノード	専用インフラストラクチャノードを使用しません。プラットフォームコンポーネントはワーカーノードにデプロイされます。	プラットフォームコンポーネントをホストするには、2 つのシングル AZ または 3 つのマルチ AZ 専用ノードを使用します。
OpenShift 機能	プラットフォームモニタリング、イメージレジストリ、イングレスコントローラーは、ワーカーノードにデプロイされます。	プラットフォームモニタリング、イメージレジストリ、イングレスコントローラーは、専用のインフラストラクチャノードにデプロイされます。

	HCP を備えた ROSA	ROSA Classic
クラスターのアップグレード	コントロールプレーンと各マシンプールは個別にアップグレードできます。	クラスター全体を同時にアップグレードする必要があります。
最小 Amazon EC2 フットプリント	クラスターを作成するには 2 つの Amazon EC2 インスタンスが必要です。	クラスターを作成するには、7 つのシングル AZ または 9 つのマルチ AZ Amazon EC2 インスタンスが必要です。
AWS リージョン	AWS リージョン 可用性については、「 AWS 全般のリファレンスガイド」のRed Hat OpenShift Service on AWS「エンドポイントとクォータ」を参照してください。	AWS リージョン 可用性については、「 AWS 全般のリファレンスガイド」のRed Hat OpenShift Service on AWS「エンドポイントとクォータ」を参照してください。

の使用を開始する ROSA

Red Hat OpenShift Service on AWS (ROSA) は、Red Hat OpenShift エンタープライズ Kubernetes プラットフォームを使用してコンテナ化されたアプリケーションを構築、スケーリング、デプロイするために使用できるマネージドサービスです AWS。

次のガイドを使用して、最初の ROSA クラスターの作成、ユーザーアクセスの許可、最初のアプリケーションのデプロイ、ユーザーアクセスの取り消し方法とクラスターの削除方法を学ぶことができます。

- the section called “ ROSA HCP クラスターの作成 - CLI” - AWS STS と CLI を使用して、最初の ROSA with HCP ROSA クラスターを作成します。
- the section called “ROSA Classic クラスターを作成する - AWS PrivateLink ” - を使用して最初の ROSA クラシッククラスターを作成します AWS PrivateLink。
- the section called “ROSA クラシッククラスターの作成 - CLI” - AWS STS と CLI を使用して最初の ROSA ROSA クラシッククラスターを作成します。

を使用するように をセットアップする ROSA

ROSA クラスターを作成する環境を準備するには、次のアクションを実行する必要があります。

前提条件

ROSA クラスターの作成を有効にするには、次の前提条件を満たす必要があります。

- 最新の をインストールして設定します AWS CLI。詳細については、「Installing or updating the latest version of the AWS CLI」を参照してください。
- 最新の CLI ROSA と OpenShift コンテナプラットフォーム CLI をインストールして設定します。詳細については、「 ROSA CLI の開始方法」を参照してください。
- 、 Amazon EC2、および に必要なサービスクォータを設定する必要があります Elastic Load Balancing。 AWS または Amazon VPC Amazon EBS、Red Hat が問題解決の必要に応じてユーザーに代わってサービスクォータの引き上げをリクエストする場合があります。に必要なサービスクォータを確認するには ROSA、 AWS 全般のリファレンスのRed Hat OpenShift Service on AWS 「エンドポイントとクォータ」を参照してください。
- サポートを受けるには AWS ROSA、 AWS ビジネス、エンタープライズオンランプ、またはエンタープライズサポートプランを有効にする必要があります。Red Hat は、問題解決の必要に応

じて、ユーザーに代わって AWS サポートをリクエストすることがあります。詳細については、「the section called “サポート情報”」を参照してください。を有効にするには サポート、サポート「」ページを参照してください。

- AWS Organizations を使用して ROSA サービスをホスト AWS アカウント する を管理する場合は、組織のサービスコントロールポリシー (SCP) を設定して、Red Hat が制限なしで SCP にリストされているポリシーアクションを実行できるようにする必要があります。詳細については、「the section called “AWS Organizations サービスコントロールポリシーが必要な AWS Marketplace アクセス許可を拒否する”」を参照してください。SCP の詳細については、「サービスコントロールポリシー」をご参照ください。
- デフォルトでは無効 AWS リージョン になっている有効な AWS STS に クラスター を ROSA デプロイする場合は、次のコマンド AWS アカウント を使用して、 内のすべてのリージョンのセキュリティトークンをバージョン 2 に更新する必要があります。

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

リージョンの有効化の詳細については、「link:accounts/latest/reference/manage」を参照してください。

AWS 前提条件の有効化 ROSA と設定

を作成するには ROSA クラスター、 ROSA コンソールで ROSA AWS サービスを有効にする必要があります。 ROSA コンソールは AWS 、 に必要な AWS Marketplace アクセス許可、サービスクォータ、および という名前の Elastic Load Balancing (ELB) サービスにリンクされたロール AWS アカウント があるかどうかを検証しますAWSServiceRoleForElasticLoadBalancing。これらの前提条件のいずれかが満たされていない場合、コンソールは前提条件を満たすようにアカウントを設定する方法についてのガイダンスを表示します。

1. ROSA コンソールに移動します。
2. [開始する] を選択します。
3. ROSA 「前提条件の確認」ページで、連絡先情報を Red Hat と共有することに合意します。
4. [ROSA を有効にする] を選択します。
5. ページがサービスクォータが ROSA 前提条件を満たしていることを検証し、ELB サービスにリンクされたロールが作成されたら、新しいターミナルセッションを開いて CLI ROSA クラスター を使用して最初の ROSA を作成します。

CLI を使用して ROSA with HCP ROSA クラスターを作成する

以下のセクションでは、 AWS STS および CLI を使用して、ホスト型コントロールプレーン (ROSA with HCP) で ROSA ROSA の使用を開始する方法について説明します。Terraform を使用して ROSA with HCP クラスターを作成する手順については、Red Hat のドキュメントを参照してください。 ROSA クラスターを作成するための Terraform プロバイダーの詳細については、Terraform ドキュメントを参照してください。

ROSA CLI は `auto` モードまたは `manual` モードを使用して、 の作成に必要な IAM ROSA リソースと OpenID Connect (OIDC) 設定を作成します クラスター。 `auto` モードは、必要な IAM ロールとポリシーと OIDC プロバイダーを自動的に作成します。 `manual` モードは、 IAM リソースを手動で作成するために必要な AWS CLI コマンドを出力します。`manual` モードを使用すると、生成された AWS CLI コマンドを手動で実行する前に確認できます。`manual` モードを使用すると、コマンドを組織内の別の管理者またはグループに渡して、リソースを作成してもらうこともできます。

このドキュメントの手順では、 CLI ROSA の `auto` モードを使用して、HCP を使用する ROSA に必要な IAM リソースと OIDC 設定を作成します。開始するためのその他のオプションについては、「」を参照してくださいの使用を開始する ROSA 。

トピック

- 前提条件
- Amazon VPC アーキテクチャの作成
- 必要な IAM ロールと OpenID Connect 設定を作成する
- CLI と を使用して ROSA with HCP ROSA クラスターを作成する AWS STS
- ID プロバイダーを設定し、 クラスター アクセス権を付与する
- へのアクセスをユーザーに許可する クラスター
- cluster-admin のアクセス許可を設定します。
- dedicated-admin のアクセス許可を設定します。
- Red Hat Hybrid Cloud コンソール クラスター から にアクセスする
- Developer Catalog からアプリケーションをデプロイする
- ユーザーから cluster-admin 権限を取り消す
- ユーザーから dedicated-admin 権限を取り消す
- へのユーザーアクセスを取り消す クラスター
- クラスターと AWS STS リソースを削除する

前提条件

に記載されている前提条件となるアクションを完了しますthe section called “セットアップする”。

Amazon VPC アーキテクチャの作成

次の手順では、クラスターをホストするために使用できる Amazon VPC アーキテクチャを作成します。すべての クラスター リソースはプライベートサブネットでホストされます。パブリックサブネットは、プライベートサブネットからのアウトバウンドトラフィックを NAT ゲートウェイ経由でパブリックインターネットにルーティングします。この例では、 Amazon VPCに CIDR ブロック `10.0.0.0/16` を使用しています。別の CIDR ブロックを選択することもできます。詳細については、「VPC のサイズ設定」を参照してください。

> **Important**
>
> Amazon VPC 要件を満たさない場合、クラスターの作成は失敗します。

Example

Terraform

1. Terraform CLI をインストールします。詳細については、Terraform ドキュメントのインストール手順を参照してください。
2. ターミナルセッションを開き、Terraform VPC リポジトリのクローンを作成します。

   ```
   git clone https://github.com/openshift-cs/terraform-vpc-example
   ```

3. 作成したディレクトリに移動します。

   ```
   cd terraform-vpc-example
   ```

4. Terraform ファイルを開始します。

   ```
   terraform init
   ```

   完了すると、CLI は Terraform が正常に初期化されたことを示すメッセージを返します。

5. 既存のテンプレートに基づいて Terraform プランを構築するには、次のコマンドを実行します。を指定 AWS リージョン する必要があります。必要に応じて、クラスター名を指定できます。

```
terraform plan -out rosa.tfplan -var region=<region>
```

コマンドが実行されると、rosa.tfplanファイルが hypershift-tf ディレクトリに追加されます。詳細については、Terraform VPC リポジトリの README ファイルを参照してください。

6. プランファイルを適用して VPC を構築します。

```
terraform apply rosa.tfplan
```

完了すると、CLI は、追加されたリソースを検証する成功メッセージを返しました。

a. (オプション) HCP クラスターで ROSA を作成するときに使用する Terraform でプロビジョニングされたプライベートサブネット、パブリックサブネット、およびマシンプールサブネット IDs の環境変数を作成します。

```
export SUBNET_IDS=$(terraform output -raw cluster-subnets-string)
```

b. (オプション) 環境変数が正しく設定されていることを確認します。

```
echo $SUBNET_IDS
```

Amazon VPC console

1. Amazon VPC コンソール を開きます。
2. VPC ダッシュボードで、[Create VPC (VPC を作成する)] を選択します。
3. [Resources to create] (作成するリソース) で、[VPC and more] (VPC など) を選択します。
4. [名前タグの自動生成] を選択したままにすると VPC リソース用の名前タグが作成され、オフにすると VPC リソース用の独自の名前タグが作成されます。
5. [IPv4 CIDR ブロック] に VPC の IPv4 アドレス範囲を入力します。VPC には IPv4 アドレス範囲が必要です。
6. (オプション) IPv6 トラフィックをサポートするには、IPv6 CIDR ブロック、Amazon 提供の IPv6 CIDR ブロックを選択します。

7. テナンシーは のままにしますDefault。
8. アベイラビリティーゾーンの数 (AZs) で、必要な数を選択します。マルチ AZ 配置の場合、ROSA には 3 つのアベイラビリティーゾーンが必要です。サブネットの AZ を選択するには、[AZ のカスタマイズ] を展開します。

> **Note**
>
> 一部の ROSA インスタンスタイプは、一部のアベイラビリティーゾーンでのみ使用できます。 ROSA CLI `rosa list instance-types` コマンドを使用して、使用可能なすべての ROSA インスタンスタイプを一覧表示できます。特定のアベイラビリティーゾーンでインスタンスタイプが使用可能かどうかを確認するには、 AWS CLI コマンド を使用しますaws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"。

9. サブネットを設定するには、[パブリックサブネットの数] と [プライベートサブネットの数] の値を選択します。サブネットの IP アドレス範囲を選択するには、[サブネット CIDR ブロックをカスタマイズ] を展開します。

> **Note**
>
> HCP を備えた ROSA では、お客様がクラスターの作成に使用するアベイラビリティーゾーンごとに少なくとも 1 つのパブリックサブネットとプライベートサブネットを設定する必要があります。

10. プライベートサブネット内のリソースに IPv4 経由でパブリックインターネットへのアクセスを許可するには、NAT ゲートウェイの場合は、NAT ゲートウェイを作成する AZs の数を選択します。本番環境では、パブリックインターネットへのアクセスを必要とするリソースがある各 AZ に NAT ゲートウェイをデプロイすることをお勧めします。
11. (オプション) VPC Amazon S3 から直接 にアクセスする必要がある場合は、VPC エンドポイント、S3 Gateway を選択します。
12. デフォルトの DNS オプションを選択したままにします。VPC での DNS ホスト名のサポート ROSA が必要です。
13. 追加タグを展開し、新しいタグを追加を選択し、次のタグキーを追加します。 は、これらのタグが使用されていることを確認する自動プリフライトチェック ROSA を使用します。

- [Key] (キー): kubernetes.io/role/elb
- [Key] (キー): kubernetes.io/role/internal-elb

14[Create VPC (VPC の作成)] を選択します。

AWS CLI

1. 10.0.0.0/16 CIDR ブロックを持つ VPC を作成します。

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

前述のコマンドは VPC ID を返します。以下に出力例を示します。

```
vpc-1234567890abcdef0
```

2. VPC ID を 環境変数に保存します。

```
export VPC_ID=vpc-1234567890abcdef0
```

3. VPC_ID 環境変数を使用して、VPC のNameタグを作成します。

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. VPC で DNS ホスト名サポートを有効にします。

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. VPC にパブリックサブネットとプライベートサブネットを作成し、リソースを作成するアベイラビリティーゾーンを指定します。

> **Important**
>
> HCP を備えた ROSA では、お客様がクラスターの作成に使用するアベイラビリティーゾーンごとに少なくとも 1 つのパブリックサブネットとプライベートサブネットを設

定する必要があります。マルチ AZ 配置の場合、3 つのアベイラビリティーゾーンが必要です。これらの要件を満たさないと、クラスターの作成は失敗します。

> **Note**
>
> 一部の ROSA インスタンスタイプは、一部のアベイラビリティーゾーンでのみ使用できます。 ROSA CLI `rosa list instance-types` コマンドを使用して、使用可能なすべての ROSA インスタンスタイプを一覧表示できます。特定のアベイラビリティーゾーンでインスタンスタイプが使用可能かどうかを確認するには、 AWS CLI コマンド を使用しますaws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"。

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. パブリックサブネット ID とプライベートサブネット IDsを環境変数に保存します。

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. VPC subnets に次のタグを作成します。これらのタグが使用されていることを確認する ROSA 自動プリフライトチェックを使用します。

> **Note**
>
> 少なくとも 1 つのプライベートサブネット、および該当する場合は 1 つのパブリックサブネットにタグを付ける必要があります。

```
aws ec2 create-tags --resources $PUBLIC_SUB --tags Key=kubernetes.io/role/
elb,Value=1
aws ec2 create-tags --resources $PRIVATE_SUB --tags Key=kubernetes.io/role/
internal-elb,Value=1
```

8. アウトバウンドトラフィック用のインターネットゲートウェイとルートテーブルを作成します。プライベートトラフィックのルートテーブルと Elastic IP アドレスを作成します。

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

9. IDsを環境変数に保存します。

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

10. インターネットゲートウェイを VPC にアタッチします。

```
aws ec2 attach-internet-gateway \
```

```
    --vpc-id $VPC_ID \
    --internet-gateway-id $IGW
```

11パブリックルートテーブルをパブリックサブネットに関連付け、インターネットゲートウェイにルーティングするようにトラフィックを設定します。

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

12NAT ゲートウェイを作成し、Elastic IP アドレスに関連付けて、プライベートサブネットへのトラフィックを有効にします。

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

13.プライベートルートテーブルをプライベートサブネットに関連付け、NAT ゲートウェイにルーティングするようにトラフィックを設定します。

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

14(オプション) マルチ AZ 配置の場合は、上記のステップを繰り返して、パブリックサブネットとプライベートサブネットでさらに 2 つのアベイラビリティーゾーンを設定します。

必要な IAM ロールと OpenID Connect 設定を作成する

HCP クラスターで ROSA を作成する前に、必要な IAM ロールとポリシー、および OpenID Connect (OIDC) 設定を作成する必要があります。HCP を使用した ROSA の IAM ロールとポリシーの詳細については、「」を参照してくださいthe section called “ AWS マネージドポリシー”。

この手順では、 CLI ROSA の `auto` モードを使用して、HCP クラスターで ROSA を作成するために必要な OIDC 設定を自動的に作成します。

1. 必要な IAM アカウントロールとポリシーを作成します。`--force-policy-creation` パラメータは、存在する既存のロールとポリシーを更新します。ロールとポリシーが存在しない場合、コマンドは代わりにこれらのリソースを作成します。

```
rosa create account-roles --force-policy-creation
```

> **Note**
>
> オフラインアクセストークンの有効期限が切れている場合、 ROSA CLI は認可トークンを更新する必要があることを示すエラーメッセージを出力します。トラブルシューティングの手順については、「」を参照してくださいthe section called “CLI ROSA の有効期限が切れたオフラインアクセストークンのトラブルシューティング”。

2. クラスターへのユーザー認証を有効にする OpenID Connect (OIDC) 設定を作成します。この設定は OpenShift クラスターマネージャー (OCM) で使用できるように登録されます。

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

3. CLI 出力で指定された OIDC 設定 ID ROSA をコピーします。HCP を備えた ROSA クラスターを作成するには、後で OIDC 構成 ID を指定する必要があります。
4. ユーザー組織に関連するクラスターで使用可能な OIDC 設定を確認するには、以下のコマンドを実行します。

```
rosa list oidc-config
```

5. 必要な IAM オペレータロールを作成し、 を前にコピーした OIDC 設定 ID `<OIDC_CONFIG_ID>`に置き換えます。

Example

> **Important**
>
> オペレータロールを作成するときは、<PREFIX_NAME> でプレフィックスを指定する必要があります。そうしないと、エラーが発生します。

```
rosa create operator-roles --prefix <PREFIX_NAME> --oidc-config-id <OIDC_CONFIG_ID>
 --hosted-cp
```

6. IAM オペレータロールが作成されたことを確認するには、次のコマンドを実行します。

```
rosa list operator-roles
```

CLI と を使用して ROSA with HCP ROSA クラスターを作成する AWS STS

AWS Security Token Service (AWS STS) と CLI で提供されているautoモード クラスター を使用して、HCP で ROSA ROSA を作成できます。クラスターを作成するには、パブリック API と Ingress を使用するか、プライベート API と Ingress を使用するかを選択できます。

は、単一のアベイラビリティーゾーン (シングル AZ) または複数のアベイラビリティーゾーン (マルチ AZ) クラスター で作成できます。いずれの場合も、マシンの CIDR 値は VPC の CIDR 値と一致する必要があります。

次の手順では、 `rosa create cluster --hosted-cp` コマンドを使用して、HCP でシングル AZ ROSA を作成します クラスター。マルチ AZ を作成するには クラスター、 コマンドmulti-azで を指定し、デプロイする各プライベートサブネットのプライベートサブネット IDs を指定します。

1. 次のいずれかのコマンドを使用して、HCP クラスターを持つ ROSA を作成します。

   - パブリック API と Ingress を使用して HCP を備えた ROSA クラスターを作成し、クラスター名、オペレーターロールプレフィックス、OIDC 構成 ID、パブリックサブネット ID とプライベートサブネット ID を指定します。

```
rosa create cluster --cluster-name=<CLUSTER_NAME> --sts --mode=auto --hosted-cp --
operator-roles-prefix <OPERATOR_ROLE_PREFIX> --oidc-config-id <OIDC_CONFIG_ID> --
subnet-ids=<PUBLIC_SUBNET_ID>,<PRIVATE_SUBNET_ID>
```

- プライベート API と Ingress を使用して HCP を備えた ROSA クラスターを作成し、クラスター名、オペレーターロールプレフィックス、OIDC 構成 ID、プライベートサブネット ID を指定します。

```
rosa create cluster --private --cluster-name=<CLUSTER_NAME> --sts --mode=auto --
hosted-cp --subnet-ids=<PRIVATE_SUBNET_ID>
```

2. のステータスを確認します クラスター。

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> 作成プロセスが失敗した場合、または State フィールドが 10 分後に準備完了ステータスに変わらない場合は、「」を参照してくださいトラブルシューティング。
> サポートが必要な場合は、 サポート 「」または「Red Hat サポート」を参照してくださいthe section called “サポート情報”。

3. OpenShift インストーラログを監視して、 クラスター 作成の進行状況を追跡します。

```
rosa logs install -c <CLUSTER_NAME> --watch
```

ID プロバイダーを設定し、 クラスター アクセス権を付与する

ROSA には組み込みの OAuth サーバーが含まれています。 クラスター を作成したら、ID プロバイダーを使用するように OAuth を設定する必要があります。次に、設定した ID プロバイダーにユーザーを追加すると、そのユーザーに クラスターへのアクセス権を付与できます。必要に応じて、これらのユーザーに `cluster-admin` または `dedicated-admin` 権限を付与できます。

ROSA クラスターにはさまざまな ID プロバイダータイプを設定できます。サポートされているタイプには、GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect、および HTPasswd ID プロバイダーが含まれます。

> **Important**
>
> HTPasswd ID プロバイダーは、単一の静的な管理者ユーザーを作成できるようにするためだけに組み込まれています。HTPasswd は ROSAにおける汎用の ID プロバイダーとしてはサポートされていません。

以下の手順では、例として GitHub ID プロバイダーを設定します。サポートされている各 ID プロバイダータイプを設定する方法については、「AWS STS用 ID プロバイダーの設定」を参照してください。

1. github.com に移動し、GitHub アカウントにログインします。
2. の ID プロビジョニングに使用する GitHub 組織がない場合は クラスター、作成します。詳細については、GitHub ドキュメントの手順を参照してください。
3. CLI ROSA のインタラクティブモードを使用して、クラスターの ID プロバイダーを設定します。

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 出力の設定プロンプトに従って、GitHub 組織のメンバー クラスター へのアクセスを制限します。

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 出力内の URL を開き、<GITHUB_ORG_NAME> を GitHub 組織の名前に置き換えます。

6. GitHub ウェブページで、[アプリケーションを登録] を選択して、新しい OAuth アプリケーションを GitHub 組織に登録します。
7. 次のコマンドを実行して、GitHub OAuth ページの情報を使用して残りの `rosa create idp` インタラクティブプロンプトを入力します。<GITHUB_CLIENT_ID> と <GITHUB_CLIENT_SECRET> を GitHub OAuth アプリケーションの認証情報に置き換えます。

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> ID プロバイダーの設定が有効になるまでに約 2 分かかる場合があります。`cluster-admin` ユーザーを設定した場合は、`oc get pods -n openshift-authentication --watch` を実行して OAuth ポッドが更新された設定で再デプロイされることを確認できます。

8. ID プロバイダーが正しく設定されていることを確認します。

```
rosa list idps --cluster=<CLUSTER_NAME>
```

へのアクセスをユーザーに許可する クラスター

設定済みの ID プロバイダーに追加 クラスター することで、 へのアクセス権をユーザーに付与できます。

以下の手順では、クラスターに ID をプロビジョニングするように設定されている GitHub 組織にユーザーを追加します。

1. github.com に移動し、GitHub アカウントにログインします。

2. GitHub 組織 クラスター へのアクセスを必要とするユーザーを招待します。詳細については、GitHub ドキュメントの「ユーザーを組織に招待する」を参照してください。

cluster-admin のアクセス許可を設定します。

1. 次のコマンドを実行して cluster-admin 権限を付与します。<IDP_USER_NAME> と <CLUSTER_NAME> をお使いのユーザー名とクラスター名に置き換えます。

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが cluster-admins グループのメンバーとしてリストされていることを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

dedicated-admin のアクセス許可を設定します。

1. 次のコマンドを入力して dedicated-admin 権限を付与します。次のコマンド クラスター を実行して、 <IDP_USER_NAME> と をユーザー名とパスワード<CLUSTER_NAME>に置き換えます。

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが cluster-admins グループのメンバーとしてリストされていることを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

Red Hat Hybrid Cloud コンソール クラスター から にアクセスする

Red Hat Hybrid Cloud Console クラスター を使用して にログインします。

1. 次のコマンド クラスター を使用して、 のコンソール URL を取得します。を の名前<CLUSTER_NAME>に置き換えます クラスター。

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 出力内のコンソール URL に移動し、ログインします。

Log in with... ダイアログで、ID プロバイダー名を選択し、プロバイダーから提示された認可リクエストを完了します。

Developer Catalog からアプリケーションをデプロイする

Red Hat Hybrid Cloud Console から、開発者カタログのテストアプリケーションをデプロイし、ルートを使用して公開できます。

1. Red Hat Hybrid Cloud Console に移動し、アプリケーションをデプロイするクラスターを選択します。
2. クラスターのページで、[コンソールを開く] を選択します。
3. 管理者パースペクティブで、[ホーム] > [プロジェクト] > [プロジェクトを作成] を選択します。
4. プロジェクトの名前を入力し、オプションで [表示名] と [説明] を追加します。
5. [作成] を選択してプロジェクトを作成します。
6. 開発者パースペクティブに切り替えて [+追加] を選択します。選択したプロジェクトが、今作成したプロジェクトであることを確認してください。
7. [開発者カタログ] ダイアログで、[すべてのサービス] を選択します。
8. [開発者カタログ] ページで、メニューから[言語] > [JavaScript] を選択します。
9. [Node.js] を選択し、[アプリケーションの作成] を選択して [Source-to-Image アプリケーションの作成] ページを開きます。

> **Note**
>
> Node.js オプションを表示するには、[すべてのフィルターをクリア] を選択する必要がある場合があります。

10[Git] セクションで、[サンプルを試す] を選択します。

11[名前] フィールドに、一意の名前を追加します。

12[作成] を選択します。

> **Note**
>
> 新しいアプリケーションのデプロイには数分かかります。

13.デプロイが完了したら、アプリケーションのルート URL を選択します。

ブラウザの新しいタブが開き、次のようなメッセージが表示されます。

```
Welcome to your Node.js application on OpenShift
```

14(オプション) アプリケーションを削除し、リソースをクリーンアップします。

a. 管理者パースペクティブで、[ホーム] > [プロジェクト] を選択します。

b. プロジェクトのアクションメニューを開き、[プロジェクトを削除] を選択します。

ユーザーから **cluster-admin** 権限を取り消す

1. 次のコマンドを使用して cluster-admin 権限を無効にします。<IDP_USER_NAME> と を自分のユーザー名とパスワード<CLUSTER_NAME>に置き換えます クラスター 。

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが cluster-admins グループのメンバーとしてリストされていないことを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

ユーザーから **dedicated-admin** 権限を取り消す

1. 次のコマンドを使用して dedicated-admin 権限を無効にします。<IDP_USER_NAME> と を自分のユーザー名とパスワード<CLUSTER_NAME>に置き換えます クラスター 。

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが dedicated-admins グループのメンバーとしてリストされていないことを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

へのユーザーアクセスを取り消す クラスター

ID プロバイダーユーザーの クラスター アクセスを取り消すには、設定した ID プロバイダーから削除します。

クラスターにはさまざまな ID プロバイダータイプを設定できます。次の手順では、GitHub 組織のメンバーの クラスター アクセスを取り消します。

1. github.com に移動し、GitHub アカウントにログインします。
2. GitHub 組織からユーザーを削除します。詳細については、GitHub ドキュメントの「組織からのメンバーアカウントの削除」を参照してください。

クラスターと AWS STS リソースを削除する

CLI を使用して、 AWS Security Token Service () ROSA クラスター を使用する を削除できます AWS STS。 ROSA CLI を使用して、 によって作成された IAM ロールと OIDC プロバイダーを削除することもできます ROSA。によって作成された IAM ポリシーを削除するには ROSA、 IAM コンソールを使用できます。

> **Note**
>
> IAM によって作成された ロールとポリシーは、同じアカウントの他の ROSA クラスターで使用される ROSA 場合があります。

1. を削除 クラスター し、ログを確認します。<CLUSTER_NAME> を クラスターの名前または ID で置き換えます。

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> が完全に削除 クラスター されるまで待ってから、 IAM ロール、ポリシー、および OIDC プロバイダーを削除する必要があります。インストーラーが作成したリソースを削除するには、アカウント IAM ロールが必要です。OpenShift オペレーターが作成したリソースをクリーンアップするには、オペレーター IAM ロールが必要です。オペレーターは OIDC プロバイダーを使用して認証します。

2. 次のコマンドを実行して、 クラスター オペレーターが認証に使用する OIDC プロバイダーを削除します。

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. クラスター固有のオペレーター IAM ロールを削除します。

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 以下のコマンドを使用してアカウントの IAM ロールを削除します。<PREFIX> を、削除するアカウントの IAM ロールのプレフィックスに置き換えます。アカウントの IAM ロールの作成時にカスタムプレフィックスを指定した場合は、デフォルトの ManagedOpenShift プレフィックスを指定します。

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. によって作成された IAM ポリシーを削除します ROSA。

   a. IAM コンソールにログインします。

   b. [アクセス管理] の左側のパネルで、[ポリシー] をクリックします。

   c. 削除するポリシーを選択し、[アクション] > [削除] を選択します。

   d. ポリシー名を入力し、[削除] を選択します。

   e. このステップを繰り返して、 クラスターの各 IAM ポリシーを削除します。

CLI を使用して ROSA Classic ROSA クラスターを作成する

以下のセクションでは、 AWS STS と CLI を使用して ROSA Classic ROSA の使用を開始する方法について説明します。Terraform を使用して ROSA Classic クラスターを作成する手順については、Red Hat のドキュメントを参照してください。 ROSA クラスターを作成するための Terraform プロバイダーの詳細については、Terraform ドキュメントを参照してください。

ROSA CLI は auto モードまたは manual モードを使用して、 のプロビジョニング ROSA に必要な IAM リソースを作成します クラスター。 auto モードは、必要な IAM ロールとポリシー、および OpenID Connect (OIDC) プロバイダーを直ちに作成します。 manual モードは、 IAM リソースの作成に必要な AWS CLI コマンドを出力します。manual モードを使用すると、生成された AWS CLI コマンドを手動で実行する前に確認できます。manual モードを使用すると、コマンドを組織内の別の管理者またはグループに渡して、リソースを作成してもらうこともできます。

開始するためのその他のオプションについては、「」を参照してくださいの使用を開始する ROSA
。

トピック

- 前提条件
- CLI と を使用して ROSA Classic ROSA クラスターを作成する AWS STS
- ID プロバイダーを設定し、 クラスター アクセス権を付与する
- へのアクセスをユーザーに許可する クラスター
- cluster-admin のアクセス許可を設定します。
- dedicated-admin のアクセス許可を設定します。
- Red Hat Hybrid Cloud コンソール クラスター から にアクセスする
- Developer Catalog からアプリケーションをデプロイする
- ユーザーから cluster-admin 権限を取り消す
- ユーザーから dedicated-admin 権限を取り消す
- へのユーザーアクセスを取り消す クラスター
- クラスターと AWS STS リソースを削除する

前提条件

に記載されている前提条件となるアクションを完了しますthe section called “セットアップする”。

CLI と を使用して ROSA Classic ROSA クラスターを作成する AWS STS

CLI と クラスター を使用して ROSA Classic ROSA を作成できます AWS STS。

1. `--mode auto` または を使用して、必要な IAM アカウントロールとポリシーを作成します`--mode manual`。

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

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

> **Note**
>
> オフラインアクセストークンの有効期限が切れている場合、 ROSA CLI は認可トークンを更新する必要があることを示すエラーメッセージを出力します。トラブルシューティングの手順については、「」を参照してくださいthe section called “CLI ROSA の有効期限が切れたオフラインアクセストークンのトラブルシューティング”。

2. `--mode auto` または クラスター を使用して を作成します`--mode manual`。 `auto` モードを使用すると、クラスターをより迅速に作成できます。 `manual` モードを使用すると、クラスターのカスタム設定を指定するように求められます。

- ```
  rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode auto
  ```

  > **Note**
  >
  > を指定すると`--mode auto`、 `rosa create cluster` コマンドはクラスター固有のオペレーター IAM ロールと OIDC プロバイダーを自動的に作成します。オペレーターは OIDC プロバイダーを使用して認証します。

  > **Note**
  >
  > `--mode auto` デフォルトを使用する場合、最新の安定した OpenShift バージョンがインストールされます。

- ```
  rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode manual
  ```

  > **Important**
  >
  > `manual` モードで etcd 暗号化を有効にすると、約 20% のパフォーマンスオーバーヘッドが発生します。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 Amazon EBS 暗号化に加えて、この 2 番目の暗号化レイヤーを導入した結果です。

> **Note**
>
> `manual` モードを実行してクラスターを作成したら、クラスター固有のオペレーター IAM ロールと、クラスターオペレーターが認証に使用する OpenID Connect プロバイダーを手動で作成する必要があります。

3. のステータスを確認します クラスター。

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> プロビジョニングプロセスが失敗した場合、または `State`フィールドが 40 分後に準備完了ステータスに変わらない場合は、「」を参照してくださいトラブルシューティング。サポートが必要な場合は、 サポート 「」または「Red Hat サポート」を参照してくださいthe section called “サポート情報”。

4. OpenShift インストーラログを監視して、 クラスター 作成の進行状況を追跡します。

```
rosa logs install -c <CLUSTER_NAME> --watch
```

ID プロバイダーを設定し、 クラスター アクセス権を付与する

ROSA には組み込みの OAuth サーバーが含まれています。 クラスター を作成したら、ID プロバイダーを使用するように OAuth を設定する必要があります。次に、設定した ID プロバイダーにユーザーを追加すると、そのユーザーに クラスターへのアクセス権を付与できます。必要に応じて、これらのユーザーに `cluster-admin` または `dedicated-admin` 権限を付与できます。

ROSA クラスターにはさまざまな ID プロバイダータイプを設定できます。サポートされているタイプには、GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect、および HTPasswd ID プロバイダーが含まれます。

> **Important**
>
> HTPasswd ID プロバイダーは、単一の静的な管理者ユーザーを作成できるようにするためだけに組み込まれています。HTPasswd は ROSAにおける汎用の ID プロバイダーとしてはサポートされていません。

以下の手順では、例として GitHub ID プロバイダーを設定します。サポートされている各 ID プロバイダータイプを設定する方法については、「AWS STS用 ID プロバイダーの設定」を参照してください。

1. github.com に移動し、GitHub アカウントにログインします。
2. の ID プロビジョニングに使用する GitHub 組織がない場合は クラスター、組織を作成します。詳細については、GitHub ドキュメントの手順を参照してください。
3. CLI ROSA のインタラクティブモードを使用して、クラスターの ID プロバイダーを設定します。

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 出力の設定プロンプトに従って、GitHub 組織のメンバー クラスター へのアクセスを制限します。

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 出力内の URL を開き、<GITHUB_ORG_NAME> を GitHub 組織の名前に置き換えます。

6. GitHub ウェブページで、[アプリケーションを登録] を選択して、新しい OAuth アプリケーションを GitHub 組織に登録します。
7. 次のコマンドを実行して、GitHub OAuth ページの情報を使用して残りの `rosa create idp` インタラクティブプロンプトを入力します。<GITHUB_CLIENT_ID> と <GITHUB_CLIENT_SECRET> を GitHub OAuth アプリケーションの認証情報に置き換えます。

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> ID プロバイダーの設定が有効になるまでに約 2 分かかる場合があります。`cluster-admin` ユーザーを設定した場合は、`oc get pods -n openshift-authentication --watch` を実行して OAuth ポッドが更新された設定で再デプロイされることを確認できます。

8. ID プロバイダーが正しく設定されていることを確認します。

```
rosa list idps --cluster=<CLUSTER_NAME>
```

へのアクセスをユーザーに許可する クラスター

設定済みの ID プロバイダーに追加 クラスター することで、 へのアクセス権をユーザーに付与できます。

以下の手順では、クラスターに ID をプロビジョニングするように設定されている GitHub 組織にユーザーを追加します。

1. github.com に移動し、GitHub アカウントにログインします。

2. GitHub 組織 クラスター へのアクセスを必要とするユーザーを招待します。詳細については、GitHub ドキュメントの「ユーザーを組織に招待する」を参照してください。

cluster-admin のアクセス許可を設定します。

1. 次のコマンドを実行して cluster-admin 権限を付与します。<IDP_USER_NAME> と <CLUSTER_NAME> をお使いのユーザー名とクラスター名に置き換えます。

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが cluster-admins グループのメンバーとしてリストされていることを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

dedicated-admin のアクセス許可を設定します。

1. 次のコマンドを入力して dedicated-admin 権限を付与します。次のコマンド クラスター を実行して、 <IDP_USER_NAME> と をユーザー名とパスワード<CLUSTER_NAME>に置き換えます。

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが cluster-admins グループのメンバーとしてリストされていることを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

Red Hat Hybrid Cloud コンソール クラスター から にアクセスする

クラスター 管理者ユーザーを作成するか、設定された ID プロバイダーにユーザーを追加したら、Red Hat Hybrid Cloud Console クラスター を使用して にログインできます。

1. 次のコマンド クラスター を使用して、 のコンソール URL を取得します。を の名前<CLUSTER_NAME>に置き換えます クラスター。

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 出力内のコンソール URL に移動し、ログインします。

- `cluster-admin` ユーザーを作成した場合は、提供された認証情報を使用してログインします。
- の ID プロバイダーを設定した場合は クラスター、Log in with... ダイアログで ID プロバイダー名を選択し、プロバイダーから提示された認可リクエストを完了します。

Developer Catalog からアプリケーションをデプロイする

Red Hat Hybrid Cloud Console から、開発者カタログのテストアプリケーションをデプロイし、ルートを使用して公開できます。

1. Red Hat Hybrid Cloud Console に移動し、アプリケーションをデプロイするクラスターを選択します。
2. クラスターのページで、[コンソールを開く] を選択します。
3. 管理者パースペクティブで、[ホーム] > [プロジェクト] > [プロジェクトを作成] を選択します。
4. プロジェクトの名前を入力し、オプションで [表示名] と [説明] を追加します。
5. [作成] を選択してプロジェクトを作成します。
6. 開発者パースペクティブに切り替えて [+追加] を選択します。選択したプロジェクトが、今作成したプロジェクトであることを確認してください。
7. [開発者カタログ] ダイアログで、[すべてのサービス] を選択します。
8. [開発者カタログ] ページで、メニューから[言語] > [JavaScript] を選択します。
9. [Node.js] を選択し、[アプリケーションの作成] を選択して [Source-to-Image アプリケーションの作成] ページを開きます。

> **Note**
>
> Node.js オプションを表示するには、[すべてのフィルターをクリア] を選択する必要がある場合があります。

10[Git] セクションで、[サンプルを試す] を選択します。

11[名前] フィールドに、一意の名前を追加します。

12[作成] を選択します。

> **Note**
> 新しいアプリケーションのデプロイには数分かかります。

13.デプロイが完了したら、アプリケーションのルート URL を選択します。

ブラウザの新しいタブが開き、次のようなメッセージが表示されます。

```
Welcome to your Node.js application on OpenShift
```

14.(オプション) アプリケーションを削除し、リソースをクリーンアップします。

a. 管理者パースペクティブで、[ホーム] > [プロジェクト] を選択します。

b. プロジェクトのアクションメニューを開き、[プロジェクトを削除] を選択します。

ユーザーから cluster-admin 権限を取り消す

1. 次のコマンドを使用して cluster-admin 権限を無効にします。<IDP_USER_NAME> と を自分のユーザー名とパスワード<CLUSTER_NAME>に置き換えます クラスター 。

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが cluster-admins グループのメンバーとしてリストされていないことを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

ユーザーから dedicated-admin 権限を取り消す

1. 次のコマンドを使用して dedicated-admin 権限を無効にします。<IDP_USER_NAME> と を自分のユーザー名とパスワード<CLUSTER_NAME>に置き換えます クラスター 。

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが dedicated-admins グループのメンバーとしてリストされていないことを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

へのユーザーアクセスを取り消す クラスター

ID プロバイダーユーザーの クラスター アクセスを取り消すには、設定された ID プロバイダーから削除します。

クラスターにはさまざまな ID プロバイダータイプを設定できます。次の手順では、GitHub 組織のメンバーの クラスター アクセスを取り消します。

1. github.com に移動し、GitHub アカウントにログインします。
2. GitHub 組織からユーザーを削除します。詳細については、GitHub ドキュメントの「組織からのメンバーアカウントの削除」を参照してください。

クラスターと AWS STS リソースを削除する

CLI を使用して、 AWS Security Token Service () ROSA クラスター を使用する を削除できます AWS STS。 ROSA CLI を使用して、 によって作成された IAM ロールと OIDC プロバイダーを削除することもできます ROSA。によって作成された IAM ポリシーを削除するには ROSA、 IAM コンソールを使用できます。

> **Important**
>
> IAM によって作成された ロールとポリシーは、同じアカウントの他の ROSA クラスターで使用される ROSA 場合があります。

1. を削除 クラスター し、ログを監視します。<CLUSTER_NAME> を クラスターの名前または ID で置き換えます。

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> IAM ロール クラスター 、ポリシー、および OIDC プロバイダーを削除する前に、 が完全に削除されるのを待つ必要があります。インストーラーが作成したリソースを削除するに

は、アカウント IAM ロールが必要です。OpenShift オペレーターが作成したリソースをクリーンアップするには、オペレーター IAM ロールが必要です。オペレーターは OIDC プロバイダーを使用して認証します。

2. 次のコマンドを実行して、 クラスター オペレーターが認証に使用する OIDC プロバイダーを削除します。

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. クラスター固有のオペレーター IAM ロールを削除します。

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 以下のコマンドを使用してアカウントの IAM ロールを削除します。<PREFIX> を、削除するアカウントの IAM ロールのプレフィックスに置き換えます。アカウントの IAM ロールの作成時にカスタムプレフィックスを指定した場合は、デフォルトの ManagedOpenShift プレフィックスを指定します。

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. によって作成された IAM ポリシーを削除します ROSA。
   a. IAM コンソールにログインします。
   b. [アクセス管理] の左側のパネルで、[ポリシー] をクリックします。
   c. 削除するポリシーを選択し、[アクション] > [削除] を選択します。
   d. ポリシー名を入力し、[削除] を選択します。
   e. このステップを繰り返して、 クラスターの各 IAM ポリシーを削除します。

を使用する ROSA Classic クラスターを作成する AWS PrivateLink

ROSA クラシッククラスターは、パブリック、プライベート、プライベートのいくつかの方法でデプロイできます AWS PrivateLink。ROSA Classic の詳細については、「」を参照してくださいthe section called “アーキテクチャ”。パブリック設定とプライベート クラスター 設定の両方で、OpenShift クラスター はインターネットにアクセスでき、プライバシーはアプリケーションレイヤーのアプリケーションワークロードに設定されます。

クラスター とアプリケーションワークロードの両方をプライベートにする必要がある場合は、ROSA Classic AWS PrivateLink を使用して を設定できます。 AWS PrivateLink は、 ROSA

を使用して、 AWS カスタマーアカウントの ROSA サービスとクラスターリソース間にプライベート接続を作成する、可用性が高くスケーラブルなテクノロジーです。を使用すると AWS PrivateLink、Red Hat サイト信頼性エンジニアリング (SRE) チームは、クラスターの AWS PrivateLink エンドポイントに接続されたプライベートサブネットを使用して、サポートと修復の目的でクラスターにアクセスできます。

詳細については AWS PrivateLink、「 とは」を参照してください AWS PrivateLink。

トピック

- 前提条件
- Amazon VPC アーキテクチャを作成する
- CLI と を使用して ROSA Classic ROSA クラスターを作成する AWS PrivateLink
- DNS AWS PrivateLink 転送を設定する
- ID プロバイダーを設定し、 クラスター アクセス権を付与する
- へのアクセスをユーザーに許可する クラスター
- cluster-admin のアクセス許可を設定します。
- dedicated-admin のアクセス許可を設定します。
- Red Hat Hybrid Cloud コンソール クラスター から にアクセスする
- Developer Catalog からアプリケーションをデプロイする
- ユーザーから cluster-admin 権限を取り消す
- ユーザーから dedicated-admin 権限を取り消す
- へのユーザーアクセスを取り消す クラスター
- クラスターと AWS STS リソースを削除する

前提条件

に記載されている前提条件となるアクションを完了しますthe section called “セットアップする”。

Amazon VPC アーキテクチャを作成する

次の手順では、クラスターをホストするために使用できる Amazon VPC アーキテクチャを作成します。すべての クラスター リソースはプライベートサブネットでホストされます。パブリックサブネットは、プライベートサブネットからのアウトバウンドトラフィックを NAT ゲートウェイ経由でパブリックインターネットにルーティングします。この例では、 Amazon VPCに CIDR ブロック

10.0.0.0/16 を使用しています。別の CIDR ブロックを選択することもできます。詳細については、「VPC のサイズ設定」を参照してください。

> **Important**
>
> Amazon VPC 要件を満たさない場合、クラスターの作成は失敗します。

Example

Amazon VPC console

1. Amazon VPC コンソール を開きます。
2. VPC ダッシュボードで、[Create VPC (VPC を作成する)] を選択します。
3. [Resources to create] (作成するリソース) で、[VPC and more] (VPC など) を選択します。
4. [名前タグの自動生成] を選択したままにすると VPC リソース用の名前タグが作成され、オフにすると VPC リソース用の独自の名前タグが作成されます。
5. [IPv4 CIDR ブロック] に VPC の IPv4 アドレス範囲を入力します。VPC には IPv4 アドレス範囲が必要です。
6. (オプション) IPv6 トラフィックをサポートするには、IPv6 CIDR ブロック、Amazon 提供の IPv6 CIDR ブロックを選択します。
7. テナンシーは のままにしますDefault。
8. アベイラビリティーゾーンの数 (AZs) で、必要な数を選択します。マルチ AZ 配置の場合、には 3 つのアベイラビリティーゾーン ROSA が必要です。サブネットの AZ を選択するには、[AZ のカスタマイズ] を展開します。

   > **Note**
   >
   > 一部の ROSA インスタンスタイプは、一部のアベイラビリティーゾーンでのみ使用できます。 ROSA CLI `rosa list instance-types` コマンドを使用して、使用可能なすべての ROSA インスタンスタイプを一覧表示できます。特定のアベイラビリティーゾーンでインスタンスタイプが使用可能かどうかを確認するには、 AWS CLI コマンド を使用しますaws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"。

9. サブネットを設定するには、[パブリックサブネットの数] と [プライベートサブネットの数] の値を選択します。サブネットの IP アドレス範囲を選択するには、[サブネット CIDR ブロックをカスタマイズ] を展開します。

> **Note**
>
> ROSA では、クラスターの作成に使用するアベイラビリティーゾーンごとに少なくとも 1 つのプライベートサブネットを設定する必要があります。

10. プライベートサブネット内のリソースに IPv4 経由でパブリックインターネットへのアクセスを許可するには、NAT ゲートウェイの場合は、NAT ゲートウェイを作成する AZs の数を選択します。本番環境では、パブリックインターネットへのアクセスを必要とするリソースがある各 AZ に NAT ゲートウェイをデプロイすることをお勧めします。
11. (オプション) VPC Amazon S3 から直接 にアクセスする必要がある場合は、VPC エンドポイント、S3 Gateway を選択します。
12. デフォルトの DNS オプションを選択したままにします。VPC での DNS ホスト名のサポート ROSA が必要です。
13. [Create VPC (VPC の作成)] を選択します。

AWS CLI

1. `10.0.0.0/16` CIDR ブロックを持つ VPC を作成します。

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

前述のコマンドは VPC ID を返します。以下に出力例を示します。

```
vpc-1234567890abcdef0
```

2. VPC ID を 環境変数に保存します。

```
export VPC_ID=vpc-1234567890abcdef0
```

3. `VPC_ID` 環境変数を使用して、VPC の`Name`タグを作成します。

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. VPC で DNS ホスト名サポートを有効にします。

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. VPC にパブリックサブネットとプライベートサブネットを作成し、リソースを作成するアベイラビリティーゾーンを指定します。

> **Important**
>
> ROSA では、クラスターの作成に使用するアベイラビリティーゾーンごとに少なくとも 1 つのプライベートサブネットを設定する必要があります。マルチ AZ 配置の場合、3 つのアベイラビリティーゾーンが必要です。これらの要件を満たさないと、クラスターの作成は失敗します。

> **Note**
>
> 一部の ROSA インスタンスタイプは、一部のアベイラビリティーゾーンでのみ使用できます。 ROSA CLI `rosa list instance-types` コマンドを使用して、使用可能なすべての ROSA インスタンスタイプを一覧表示できます。特定のアベイラビリティーゾーンでインスタンスタイプが使用可能かどうかを確認するには、 AWS CLI コマンド を使用しますaws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"。

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
```

```
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. パブリックサブネット ID とプライベートサブネット IDsを環境変数に保存します。

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. アウトバウンドトラフィックのインターネットゲートウェイとルートテーブルを作成します。プライベートトラフィックのルートテーブルと Elastic IP アドレスを作成します。

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

8. IDsを環境変数に保存します。

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

9. インターネットゲートウェイを VPC にアタッチします。

```
aws ec2 attach-internet-gateway \
    --vpc-id $VPC_ID \
    --internet-gateway-id $IGW
```

10パブリックルートテーブルをパブリックサブネットに関連付け、インターネットゲートウェイにルーティングするようにトラフィックを設定します。

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

11NAT ゲートウェイを作成し、Elastic IP アドレスに関連付けて、プライベートサブネットへのトラフィックを有効にします。

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

12プライベートルートテーブルをプライベートサブネットに関連付け、NAT ゲートウェイにルーティングするようにトラフィックを設定します。

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

13(オプション) マルチ AZ 配置の場合は、上記のステップを繰り返して、パブリックサブネットとプライベートサブネットでさらに 2 つのアベイラビリティーゾーンを設定します。

CLI と を使用して ROSA Classic ROSA クラスターを作成する AWS PrivateLink

ROSA CLI と を使用して AWS PrivateLink 、単一のアベイラビリティーゾーン (シングル AZ) または複数のアベイラビリティーゾーン (マルチ AZ) クラスター を持つ を作成できます。いずれの場合も、マシンの CIDR 値は VPC の CIDR 値と一致する必要があります。

次の手順では、 `rosa create cluster` コマンドを使用して ROSA Classic を作成します クラスター。マルチ AZ を作成するには クラスター、 コマンド`--multi-az`で を指定し、プロンプトが表示されたら使用するプライベートサブネット IDsを選択します。

> **Note**
>
> ファイアウォールを使用する場合は、 が機能するために必要なサイト ROSA にアクセスできるように設定する必要があります。
> 詳細については、Red Hat ドキュメントのAWS PrivateLink クラスターを使用するための要件」を参照してください。

1. `--mode auto` または を使用して、必要な IAM アカウントロールとポリシーを作成します`--mode manual`。

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

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

     > **Note**
     >
     > オフラインアクセストークンの有効期限が切れている場合、 ROSA CLI は認可トークンを更新する必要があることを示すエラーメッセージを出力します。トラブルシューティングの手順については、「」を参照してくださいthe section called “CLI ROSA の有効期限が切れたオフラインアクセストークンのトラブルシューティング”。

2. 次のいずれかのコマンド クラスター を実行して、 を作成します。

   - シングル AZ

     ```
     rosa create cluster --private-link --cluster-name=<CLUSTER_NAME> --machine-cidr=10.0.0.0/16 --subnet-ids=<PRIVATE_SUBNET_ID>
     ```

   - マルチ AZ

     ```
     rosa create cluster --private-link --multi-az --cluster-name=<CLUSTER_NAME> --machine-cidr=10.0.0.0/16
     ```

> **Note**
>
> AWS Security Token Service (AWS STS) の存続期間の短い認証情報 AWS PrivateLink を使用するクラスターを作成するには、 `rosa create cluster` コマンドの最後に `--sts --mode manual` `--sts --mode auto`または を追加します。

3. インタラクティブプロンプトに従って クラスター オペレーター IAM ロールを作成します。

```
rosa create operator-roles --interactive -c <CLUSTER_NAME>
```

4. クラスター オペレーターが認証に使用する OpenID Connect (OIDC) プロバイダーを作成します。

```
rosa create oidc-provider --interactive -c <CLUSTER_NAME>
```

5. のステータスを確認します クラスター。

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> `State` フィールドのステータス クラスター が表示されるまでに最大 40 分かかる場合があります`ready`。プロビジョニングが失敗した場合、または 40 分`ready`後に と表示されない場合は、「」を参照してくださいトラブルシューティング。サポートが必要な場合は、 サポート 「」または「Red Hat サポート」を参照してくださいthe section called “サポート情報”。

6. OpenShift インストーラログを監視して、 クラスター 作成の進行状況を追跡します。

```
rosa logs install -c <CLUSTER_NAME> --watch
```

DNS AWS PrivateLink 転送を設定する

を使用するクラスターは、パブリックホストゾーンとプライベートホストゾーン AWS PrivateLink を作成します Route 53。 Route 53 プライベートホストゾーン内のレコードは、割り当てられた VPC 内からのみ解決できます。

Let's Encrypt DNS-01 の検証では、有効で公的に信頼されている証明書をドメイン用に発行できるようにパブリックゾーンが必要です。Let's Encrypt の検証が完了すると、検証レコードは削除されます。そのゾーンはこれらの証明書の発行と更新にも必要で、通常は 60 日ごとに求められます。通常、これらのゾーンは空のように見えますが、検証プロセスではパブリックゾーンが重要な役割を果たします。

AWS プライベートホストゾーンの詳細については、「プライベートゾーンの使用」を参照してください。パブリックホストゾーンの設定の詳細については、「パブリックホストゾーンの使用」を参照してください。

Route 53 Resolver インバウンドエンドポイントを設定する

1. `api.<cluster_domain>` や などのレコードを VPC の外部`*.apps.<cluster_domain>`で解決できるようにするには、 Route 53 Resolver インバウンドエンドポイントを設定します。

   > **Note**
   >
   > インバウンドエンドポイントを設定する場合、冗長性を確保するために最低 2 つの IP アドレスを指定する必要があります。少なくとも 2 つのアベイラビリティーゾーンで IP アドレスを指定することをお勧めします。必要に応じて、それらのアベイラビリティーゾーンまたは他のアベイラビリティーゾーンに追加の IP アドレスを指定できます。

2. インバウンドエンドポイントを設定するときは、クラスターの作成時に使用された VPC とプライベートサブネットを選択します。

クラスターの DNS 転送を設定する

Route 53 Resolver 内部エンドポイントが関連付けられて動作したら、ネットワーク上の指定されたサーバーが DNS クエリを処理できるように DNS 転送を設定します。

1. DNS クエリをトップレベルドメイン (`drow-pl-01.htno.p1.openshiftapps.com` など) の IP アドレスに転送するように企業ネットワークを設定します。
2. DNS クエリをある VPC から別の VPC に転送する場合は、「転送ルールの管理」の手順に従ってください。
3. リモートネットワークの DNS サーバーを設定する場合は、使用している DNS サーバーのドキュメントを参照して、インストールしたクラスタードメインの選択的 DNS 転送を設定してください。

ID プロバイダーを設定し、 クラスター アクセス権を付与する

ROSA には組み込みの OAuth サーバーが含まれています。 ROSA クラスター を作成したら、ID プロバイダを使用するように OAuth を設定する必要があります。次に、設定した ID プロバイダーにユーザーを追加すると、そのユーザーに クラスターへのアクセス権を付与できます。必要に応じて、これらのユーザーに `cluster-admin` または `dedicated-admin` 権限を付与できます。

クラスターにはさまざまな ID プロバイダータイプを設定できます。サポートされているタイプには、GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect、および HTPasswd ID プロバイダーが含まれます。

> **Important**
>
> HTPasswd ID プロバイダーは、単一の静的な管理者ユーザーを作成できるようにするためだけに組み込まれています。HTPasswd は ROSAにおける汎用の ID プロバイダーとしてはサポートされていません。

以下の手順では、例として GitHub ID プロバイダーを設定します。サポートされている各 ID プロバイダータイプを設定する方法については、「AWS STS用 ID プロバイダーの設定」を参照してください。

1. github.com に移動し、GitHub アカウントにログインします。
2. ROSA クラスターの ID プロビジョニングに使用する GitHub 組織がない場合は、新規に作成します。詳細については、GitHub ドキュメントの手順を参照してください。
3. CLI ROSA のインタラクティブモードを使用して、次のコマンドを実行してクラスターの ID プロバイダーを設定します。

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 出力の設定プロンプトに従って、GitHub 組織のメンバー クラスター へのアクセスを制限します。

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
```

```
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 出力内の URL を開き、<GITHUB_ORG_NAME> を GitHub 組織の名前に置き換えます。
6. GitHub ウェブページで、[アプリケーションを登録] を選択して、新しい OAuth アプリケーションを GitHub 組織に登録します。
7. GitHub OAuth ページの情報を使用して残りの `rosa create idp` インタラクティブプロンプトを入力します。<GITHUB_CLIENT_ID> と <GITHUB_CLIENT_SECRET> は、GitHub OAuth アプリケーションの認証情報に置き換えます。

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> ID プロバイダーの設定が有効になるまでに約 2 分かかる場合があります。`cluster-admin` ユーザーを設定した場合は、`oc get pods -n openshift-authentication --watch` コマンドを実行して OAuth ポッドが更新された設定で再デプロイされることを確認できます。

8. ID プロバイダーが正しく設定されていることを確認します。

```
rosa list idps --cluster=<CLUSTER_NAME>
```

へのアクセスをユーザーに許可する クラスター

設定済みの ID プロバイダーに追加 クラスター することで、 へのアクセス権をユーザーに付与できます。

以下の手順では、クラスターに ID をプロビジョニングするように設定されている GitHub 組織にユーザーを追加します。

1. github.com に移動し、GitHub アカウントにログインします。
2. GitHub 組織 クラスター へのアクセスを必要とするユーザーを招待します。詳細については、GitHub ドキュメントの「ユーザーを組織に招待する」を参照してください。

cluster-admin のアクセス許可を設定します。

1. 次のコマンドを入力して cluster-admin 権限を付与します。<IDP_USER_NAME> と <CLUSTER_NAME> をお使いのユーザー名とクラスター名に置き換えます。

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが cluster-admins グループのメンバーとしてリストされていることを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

dedicated-admin のアクセス許可を設定します。

1. 次のコマンドを入力して dedicated-admin 権限を付与します。<IDP_USER_NAME> と を自分のユーザー名とパスワード<CLUSTER_NAME>に置き換えます クラスター 。

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが cluster-admins グループのメンバーとしてリストされていることを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

Red Hat Hybrid Cloud コンソール クラスター から にアクセスする

クラスター 管理者ユーザーを作成した後、または設定された ID プロバイダーにユーザーを追加したら、Red Hat Hybrid Cloud Console クラスター を使用して にログインできます。

1. 次のコマンド クラスター を使用して、 のコンソール URL を取得します。を の名前<CLUSTER_NAME>に置き換えます クラスター。

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 出力内のコンソール URL に移動し、ログインします。
   - cluster-admin ユーザーを作成した場合は、提供された認証情報を使用してログインします。
   - の ID プロバイダーを設定した場合は クラスター、Log in with... ダイアログで ID プロバイダー名を選択し、プロバイダーから提示された認可リクエストを完了します。

Developer Catalog からアプリケーションをデプロイする

Red Hat Hybrid Cloud Console から、開発者カタログのテストアプリケーションをデプロイし、ルートを使用して公開できます。

1. Red Hat Hybrid Cloud Console に移動し、アプリケーションをデプロイするクラスターを選択します。
2. クラスターのページで、[コンソールを開く] を選択します。
3. 管理者パースペクティブで、[ホーム] > [プロジェクト] > [プロジェクトを作成] を選択します。
4. プロジェクトの名前を入力し、オプションで [表示名] と [説明] を追加します。
5. [作成] を選択してプロジェクトを作成します。
6. 開発者パースペクティブに切り替えて [+追加] を選択します。選択したプロジェクトが、今作成したプロジェクトであることを確認してください。
7. [開発者カタログ] ダイアログで、[すべてのサービス] を選択します。
8. [開発者カタログ] ページで、メニューから[言語] > [JavaScript] を選択します。
9. [Node.js] を選択し、[アプリケーションの作成] を選択して [Source-to-Image アプリケーションの作成] ページを開きます。

> **Note**
>
> Node.js オプションを表示するには、[すべてのフィルターをクリア] を選択する必要がある場合があります。

10[Git] セクションで、[サンプルを試す] を選択します。

11[名前] フィールドに、一意の名前を追加します。

12[作成] を選択します。

> **Note**
>
> 新しいアプリケーションのデプロイには数分かかります。

13.デプロイが完了したら、アプリケーションのルート URL を選択します。

ブラウザの新しいタブが開き、次のようなメッセージが表示されます。

```
Welcome to your Node.js application on OpenShift
```

14.(オプション) アプリケーションを削除し、リソースをクリーンアップします。

a. 管理者パースペクティブで、[ホーム] > [プロジェクト] を選択します。

b. プロジェクトのアクションメニューを開き、[プロジェクトを削除] を選択します。

ユーザーから cluster-admin 権限を取り消す

1. 次のコマンドを使用して cluster-admin 権限を無効にします。<IDP_USER_NAME> と を自分のユーザー名とパスワード<CLUSTER_NAME>に置き換えます クラスター 。

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが cluster-admins グループのメンバーとしてリストされていないことを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

ユーザーから dedicated-admin 権限を取り消す

1. 次のコマンドを使用して dedicated-admin 権限を無効にします。<IDP_USER_NAME> と を自分のユーザー名とパスワード<CLUSTER_NAME>に置き換えます クラスター 。

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. ユーザーが dedicated-admins グループのメンバーとしてリストされていないことを確認します。

```
rosa list users --cluster=<CLUSTER_NAME>
```

へのユーザーアクセスを取り消す クラスター

ID プロバイダーユーザーの クラスター アクセスを取り消すには、設定された ID プロバイダーから削除します。

クラスターにはさまざまな ID プロバイダータイプを設定できます。次の手順では、GitHub 組織のメンバーの クラスター アクセスを取り消します。

1. github.com に移動し、GitHub アカウントにログインします。
2. GitHub 組織からユーザーを削除します。詳細については、GitHub ドキュメントの「組織からのメンバーアカウントの削除」を参照してください。

クラスターと AWS STS リソースを削除する

CLI を使用して、 AWS Security Token Service () ROSA クラスター を使用する を削除できます AWS STS。 ROSA CLI を使用して、 によって作成された IAM ロールと OIDC プロバイダーを削除することもできます ROSA。によって作成された IAM ポリシーを削除するには ROSA、 IAM コンソールを使用できます。

> **Important**
>
> IAM によって作成された ロールとポリシーは、同じアカウントの他の ROSA クラスターで使用される ROSA 場合があります。

1. を削除 クラスター し、ログを監視します。<CLUSTER_NAME> を クラスターの名前または ID で置き換えます。

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> IAM ロール クラスター 、ポリシー、および OIDC プロバイダーを削除する前に、 が完全に削除されるのを待つ必要があります。インストーラーが作成したリソースを削除するには、アカウント IAM ロールが必要です。OpenShift オペレーターが作成したリソースをクリーンアップするには、オペレーター IAM ロールが必要です。オペレーターは OIDC プロバイダーを使用して認証します。

2. 次のコマンドを実行して、 クラスター オペレーターが認証に使用する OIDC プロバイダーを削除します。

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. クラスター固有のオペレーター IAM ロールを削除します。

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 以下のコマンドを使用してアカウントの IAM ロールを削除します。<PREFIX> を、削除するアカウントの IAM ロールのプレフィックスに置き換えます。アカウントの IAM ロールの作成時にカスタムプレフィックスを指定した場合は、デフォルトの ManagedOpenShift プレフィックスを指定します。

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. によって作成された IAM ポリシーを削除します ROSA。
   a. IAM コンソールにログインします。
   b. [アクセス管理] の左側のパネルで、[ポリシー] をクリックします。
   c. 削除するポリシーを選択し、[アクション] > [削除] を選択します。
   d. ポリシー名を入力し、[削除] を選択します。
   e. このステップを繰り返して、 クラスターの各 IAM ポリシーを削除します。

のセキュリティ ROSA

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。サードパーティーの監査人は、AWS コンプライアンスプログラム の一環として、セキュリティの有効性を定期的にテストおよび検証します。が適用されるコンプライアンスプログラムの詳細については ROSA、AWS のサービス「コンプライアンスプログラムによる対象範囲内」を参照してください。
- クラウドのセキュリティ – お客様の責任は、使用する によって決まり AWS のサービス ます。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます ROSA。セキュリティとコンプライアンスの目的を達成する ROSA ように を設定する方法を示します。また、 ROSA リソースのモニタリングと保護 AWS のサービス に役立つ他の の使用方法についても説明します。

内容

- でのデータ保護 ROSA
- の ID とアクセスの管理 ROSA
- の耐障害性 ROSA
- のインフラストラクチャセキュリティ ROSA

でのデータ保護 ROSA

the section called “責任” ドキュメントとAWS 責任共有モデルは、 でのデータ保護を定義します ROSA。 AWS は、 のすべてを実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。Red Hat は、クラスターインフラストラクチャと基盤となるサービスプラットフォームを保護する責任を負います。お客様は、このインフラストラクチャでホストされているコン

テンツに対する管理を維持する責任を負います。このコンテンツには、 AWS のサービス 使用するのセキュリティ設定および管理タスクが含まれます。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログの AWS 責任共有モデルと GDPR ブログ記事を参照してください。

データ保護の目的で、 AWS アカウント 認証情報を保護し、 AWS Identity and Access Management () を使用して個々のユーザーを設定することをお勧めしますIAM。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- などの高度なマネージドセキュリティサービスを使用して Amazon Macie、 に保存されている機密データの検出と保護を支援します Amazon S3。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」 を参照してください。

顧客のアカウント番号などの機密の識別情報は、[Name] (名前)フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これは、コンソール ROSA 、API、または SDK AWS のサービス を使用して AWS CLIまたは他の を操作する場合も同様です。 AWS SDKs ROSA または他の サービスに入力したデータは、診断ログに取り込まれる可能性があります。外部サーバーへの URL を指定するときは、そのサーバーへのリクエストを検証するための認証情報を URL に含めないでください。

トピック

- 暗号化を使用したデータの保護

暗号化を使用したデータの保護

データ保護とは、転送中 (送受信中 ROSA) および保管中 (AWS データセンターのディスクに保存中) のデータを保護することです。

Red Hat OpenShift Service on AWS は、 ROSA コントロールプレーン、インフラストラクチャ、ワーカーノードの Amazon EC2 インスタンスにアタッチされた Amazon Elastic Block Store (Amazon EBS) ストレージボリューム、および永続ストレージの Kubernetes 永続ボリュームへの安全なアクセスを提供します。 は、保管中および転送中のボリュームデータを ROSA 暗号化し、暗号化されたデータを保護するために AWS Key Management Service (AWS KMS) を使用します。サービスは、デフォルトで保管時に暗号化されるコンテナイメージレジストリストレージ Amazon S3 にを使用します。

> **Important**
>
> ROSA はマネージドサービスであり、 AWS Red Hat は が ROSA 使用するインフラストラクチャを管理します。お客様は、 AWS コンソールまたは CLI から が ROSA 使用する Amazon EC2 インスタンスを手動でシャットダウンしようとしないでください。そうすると、顧客データが失われる可能性があります。

Amazon EBSバックアップストレージボリュームのデータ暗号化

Red Hat OpenShift Service on AWS は Kubernetes 永続ボリューム (PV) フレームワークを使用して、クラスター管理者が永続ストレージでクラスターをプロビジョニングできるようにします。永続的ボリューム、コントロールプレーン、インフラストラクチャ、ワーカーノードは、 Amazon EC2 インスタンスにアタッチされた Amazon Elastic Block Store (Amazon EBS) ストレージボリュームによってバックアップされます。

によってバックアップされる ROSA 永続的ボリュームとノードの場合 Amazon EBS、EC2 インスタンスをホストするサーバーで暗号化オペレーションが実行され、インスタンスとそのアタッチされたストレージ間で保管中のデータと転送中のデータの両方のセキュリティが確保されます。詳細については、「 Amazon EC2 ユーザーガイド」のAmazon EBS 「暗号化」を参照してください。

CSI Amazon EBS ドライバーと CSI Amazon EFS ドライバーのデータ暗号化

ROSA は、デフォルトで CSI Amazon EBS ドライバーを使用して Amazon EBS ストレージをプロビジョニングします。 Amazon EBS CSI ドライバーと CSI Amazon EBS ドライバーオペレーターは、デフォルトで `openshift-cluster-csi-drivers`名前空間のクラスターにインストールされます。 Amazon EBS CSI ドライバーとオペレーターを使用すると、永続的ボリュームを動的にプロビジョニングし、ボリュームスナップショットを作成できます。

ROSA は、CSI ドライバーと Amazon EFS CSI Amazon EFS ドライバーオペレーターを使用して永続ボリュームをプロビジョニングすることもできます。 Amazon EFS ドライバーとオペレーター

は、ポッド間、または Kubernetes 内外の他のアプリケーションとファイルシステムデータを共有することもできます。

ボリュームデータは、CSI ドライバーと Amazon EBS CSI Amazon EFS ドライバーの両方で転送中に保護されます。詳細については Red Hat ドキュメントの「コンテナストレージインターフェース (CSI) の使用」を参照してください。

> **Important**
>
> Amazon EFS CSI ドライバーを使用して ROSA 永続的ボリュームを動的にプロビジョニングする場合、 はファイルシステムのアクセス許可を評価するときに、アクセスポイントのユーザー ID、グループ ID (GID)、セカンダリグループ IDs Amazon EFS を考慮します。 は、ファイルのユーザー ID とグループ IDs をアクセスポイントのユーザー ID とグループ IDs Amazon EFS に置き換え、NFS クライアント IDs。その結果、 は`fsGroup`設定を Amazon EFS サイレントに無視します。 ROSA は を使用してファイルの GIDs を置き換えることができません`fsGroup`。マウントされた Amazon EFS アクセスポイントにアクセスできるポッドは、ボリューム上の任意のファイルにアクセスできます。詳細については、「 ユーザーガイド」の Amazon EFS 「アクセスポイントの使用」を参照してください。 Amazon EFS

etcd 暗号化

ROSA には、クラスターの作成中に`etcd`ボリューム内の`etcd`キー値の暗号化を有効にし、暗号化レイヤーを追加するオプションが用意されています。`etcd` が暗号化されると、パフォーマンスオーバーヘッドが約 20% 増加します。ユースケースで特に必要とされる場合にのみ、`etcd` 暗号化を有効にすることをお勧めします。詳細については、 ROSA サービス定義の「 etcd 暗号化」を参照してください。

キー管理

ROSA は KMS keys を使用して、お客様のアプリケーションのコントロールプレーン、インフラストラクチャ、ワーカーデータボリュームと永続ボリュームを安全に管理します。クラスターの作成時に、 KMS key が提供するデフォルトの AWS マネージドを使用するか Amazon EBS、独自のカスタマーマネージドキーを指定することができます。詳細については、「the section called “キー管理”」を参照してください。

ビルトインイメージレジストリのデータ暗号化

ROSA には、 Amazon S3 バケットストレージを介してコンテナイメージを保存、取得、共有するための組み込みコンテナイメージレジストリが用意されています。レジストリは OpenShift Image Registry Operator によって設定および管理されます。これは、ユーザーがワークロードを実行するイメージを管理するためのすぐに利用できるソリューションとなり、既存のクラスターインフラストラクチャ上で実行されます。詳細については、Red Hat ドキュメントの「レジストリ」を参照してください。

ROSA は、パブリックイメージレジストリとプライベートイメージレジストリを提供します。エンタープライズアプリケーションでは、権限のないユーザーによるイメージの使用を防ぐため、プライベートレジストリの使用をお勧めします。レジストリの保管中のデータを保護するために、 はデフォルトで Amazon S3 マネージドキー (SSE-S3) によるサーバー側の暗号化 ROSA を使用します。これは、お客様によるアクションを必要とせず、追加料金なしで提供されます。詳細については、「 Amazon S3 ユーザーガイド」の Amazon S3 「マネージド暗号化キーによるサーバー側の暗号化 (SSE-S3) を使用したデータの保護」を参照してください。

ROSA は Transport Layer Security (TLS) プロトコルを使用して、イメージレジストリとの間で転送中のデータを保護します。詳細については、Red Hat ドキュメントの「レジストリ」を参照してください。

ネットワーク間のトラフィックのプライバシー

Red Hat OpenShift Service on AWS は Amazon Virtual Private Cloud (Amazon VPC) を使用して、ROSA クラスター内のリソース間の境界を作成し、クラスター、オンプレミスネットワーク、インターネット間のトラフィックを制御します。 Amazon VPC セキュリティの詳細については、「 Amazon VPC ユーザーガイド」の「 でのインターネットトラフィックのプライバシー Amazon VPC」を参照してください。

VPC 内で、HTTP または HTTPS プロキシサーバーを使用して直接インターネットアクセスを拒否するように ROSA クラスターを設定できます。クラスター管理者の場合は、インターネットネットワークトラフィックを ROSA クラスター内のポッドに制限するネットワークポリシーをポッドレベルで定義することもできます。詳細については、「the section called “インフラストラクチャセキュリティ”」を参照してください。

KMS を使用したデータ暗号化

ROSA は AWS 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。コントロールプレーン、インフラストラクチャ、ワーカーノードボリュームは、 KMS key が提供する AWS マネージドを使用してデフォルトで暗号化されます Amazon EBS。これにはエイリアス KMS key がありま

すaws/ebs。デフォルトの gp3 ストレージクラスを使用する永続ボリュームも、デフォルトでこの KMS keyを使用して暗号化されます。

新しく作成された ROSA クラスターは、デフォルトの gp3 ストレージクラスを使用して永続ボリュームを暗号化するように設定されています。他のストレージクラスを使用して作成された永続ボリュームは、ストレージクラスが暗号化されるように設定されている場合にのみ暗号化されます。ROSA 構築済みのストレージクラスの詳細については、Red Hat ドキュメントの「永続的ストレージの設定」を参照してください。

クラスターの作成時に、デフォルト Amazon EBSが提供するキーを使用してクラスター内の永続ボリュームを暗号化するか、独自のカスタマーマネージド対称を指定することができます KMS key。キーの作成の詳細については、「 AWS KMS デベロッパーガイド」の「対称暗号化 KMS キーの作成」を参照してください。

KMS keyを定義することで、クラスター内の個々のコンテナの永続ボリュームを暗号化することもできます。これは、デプロイ時に明示的なコンプライアンスとセキュリティのガイドラインがある場合に便利です AWS。詳細については、Red Hat ドキュメントの AWS 「 でのコンテナ永続ボリュームの暗号化 KMS key」を参照してください。

独自の KMS keysを使用して永続ボリュームを暗号化する場合は、次の点を考慮する必要があります。

- 独自の KMS 暗号化を使用する場合 KMS key、キーはクラスター AWS リージョン と同じ に存在する必要があります。
- 独自の の作成と使用にはコストがかかります KMS keys。詳細については、AWS Key Management Service 料金表を参照してください。

の ID とアクセスの管理 ROSA

AWS Identity and Access Management (IAM) は、管理者が AWS resources へのアクセスを安全に制御 AWS のサービス するのに役立つ です。 IAM 管理者は、誰を認証 (サインイン) し、誰に ROSA resources の使用を許可する (アクセス許可を付与 AWS のサービス する) かを制御します。 IAM は、追加料金なしで使用できる です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理

- ROSA アイデンティティベースのポリシーの例
- AWS の 管理ポリシー ROSA
- ROSA ID とアクセスのトラブルシューティング

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、作業内容によって異なります ROSA。

サービスユーザー - ROSA サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が提供されます。さらに多くの ROSA 機能を使用して作業を行う場合は、追加のアクセス許可が必要になる場合があります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。の機能にアクセスできない場合は ROSA、「」を参照してくださいthe section called “トラブルシューティング”。

サービス管理者 - 社内の ROSA リソースを担当している場合は、通常、 へのフルアクセスがあります ROSA。サービスユーザーがどの ROSA 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、 IAM 管理者にリクエストを送信して、サービスユーザーのアクセス許可を変更する必要があります。このページの情報を確認して、 の基本概念を理解します IAM。

IAM 管理者 - IAM 管理者は、アクセスの管理に使用されるポリシーの詳細について確認する場合があります ROSA。で使用できる ROSA アイデンティティベースのポリシーの例を表示するには IAM、「」を参照してくださいthe section called “ ROSA アイデンティティベースのポリシーの例”。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。 AWS アカウント ルートユーザー、、または IAM ロールを引き受けることで IAM ユーザー、認証 (にサインイン AWS) される必要があります。

ID ソースを通じて提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM アイデンティティセンター (IAM アイデンティティセンター) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインすると、管理者は以前に IAM ロールを使用して ID フェデレーションをセットアップしていました。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 サインインユーザーガイド」の「 へのサインイン方法 AWS アカウント」を参照してください。 AWS

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。 AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。推奨される方法を使用してリクエストに署名する方法の詳細については、「 IAM ユーザーガイド」の AWS 「API リクエストの署名」を参照してください。

使用する認証方法を問わず、追加のセキュリティ情報の提供を要求される場合もあります。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「IAM アイデンティティセンター (シングルサインオンの後継) ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「 での多要素認証 (MFA) の使用 AWS」を参照してください。 AWS AWS

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての AWS のサービス およびリソースへの完全なアクセス権を持つ単一のサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報を保護し、ルートユーザーのみが実行できるタスク実行に使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザーの認証情報を必要とするタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを介して提供された認証情報 AWS のサービス を使用して にアクセスするすべてのユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、独自の ID ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、「IAM Identity Center とは」を参照してください。 AWS 「IAM アイデンティティセンター (AWS シングルサインオンの後継) ユーザーガイド」の「」。

IAM ユーザー および グループ

IAM ユーザー は、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を持つ IAM ユーザー ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、 で長期的な認証情報を必要とする特定のユースケースがある場合は IAM ユーザー、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、 のコレクションを指定する ID です IAM ユーザー。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が簡単になります。たとえば、IAMAdmins という名前のグループがあり、そのグループに IAM リソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、IAM ユーザーガイドの IAM ユーザー 「 (ロールではなく) を作成するタイミング」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは に似ていますが IAM ユーザー、特定のユーザーに関連付けられていません。 IAM ロールを切り替える AWS Management Console ことで、 で ロールを一時的に引き受けることができます。ロールを引き受けるには、 AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用します。ロールの使用方法の詳細については、IAM ユーザーガイドの IAM「ロールの使用」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーティッドユーザーアクセス - フェデレーティッドアイデンティティにアクセス許可を割り当てるには、ロールを作成し、そのロールのアクセス許可を定義します。フェデレーテッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。ID が認証後にアクセスできるものをコントロールするため

に、IAM アイデンティティセンター は権限セットを IAMのロールに関連付けます。アクセス許可セットの詳細については、 AWS 「IAM アイデンティティセンター (AWS シングルサインオンの後継) ユーザーガイド」の「アクセス許可セット」を参照してください。

- 一時的な IAM ユーザー アクセス許可 - は、特定のタスクに対して異なるアクセス許可を一時的に引き受けるための IAM ロールを引き受け IAM ユーザー ることができます。
- クロスアカウントアクセス - IAM ロールを使用して、別のアカウントのユーザー (信頼されたプリンシパル) が自分のアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、IAM ユーザーガイドの IAM 「ロールとリソースベースのポリシーの違い」を参照してください。
- クロスサービスアクセス - 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。たとえば、サービスで呼び出しを行うと、そのサービスが でアプリケーションを実行 Amazon EC2 したり、オブジェクトを保存したりするのが一般的です Amazon S3。サービスは、呼び出し元のプリンシパルの許可、サービスロール、サービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) - IAM ユーザー または ロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAM ロールです。 IAM 管理者は、 内からサービスロールを作成、変更、削除できます IAM。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール - サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは IAM アカウントに表示され、サービスによって所有されます。 IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- で Amazon EC2 実行されているアプリケーション - IAM ロールを使用して、 Amazon EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、 Amazon EC2 インスタンス内にアクセスキーを保存するよりも推奨されます。 AWS ロールを Amazon EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれ、 Amazon EC2 インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、IAM ユーザーガイドの「 IAM ロールを使用して Amazon EC2 インスタンスで実行されているアプリケーションにアクセス許可を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、IAM ユーザーガイドの (ユーザーではなく) IAM ロールを作成するタイミングを参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、 IAM 管理者は IAM ポリシーを作成できます。その後、管理者は IAM ポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用するメソッドに関係なく、アクションのアクセス許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

ID ベースのポリシーは、、 IAM ユーザーロール、グループなどの ID にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM 「ポリシーの作成」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれます。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、IAM ユーザーガイドのマネージドポリシーとインラインポリシーの比較を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、 IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシー IAM で の AWS 管理ポリシーを使用することはできません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、 Amazon VPC は ACLs。ACLs「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーが IAM エンティティ (IAM ユーザー またはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として許可される範囲は、エンティティのアイデンティティベースのポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM ユーザーガイドのIAM 「エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) - SCPs は、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 AWS アカウント ルートユーザーを含むメンバーアカウントのエンティティのアクセス許可を制限します。Organizations と SCPs「サービスコントロールポリシー (SCPs」を参照してください。 AWS Organizations
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーティッドユーザーの一時セッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果として得られるセッションの許可は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分です。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

ROSA アイデンティティベースのポリシーの例

デフォルトでは、 IAM ユーザー および ロールには AWS リソースを作成または変更するアクセス許可はありません。また、 AWS Management Console、 AWS CLI、または AWS API を使用してタスクを実行することはできません。 IAM 管理者は、必要な指定されたリソースに対して特定の API オペレーションを実行するアクセス許可をユーザーとロールに付与する IAM ポリシーを作成する必要があります。管理者は、これらのアクセス許可を必要とする IAM ユーザー または グループにこれらのポリシーをアタッチする必要があります。

これらのサンプル JSON ポリシードキュメントを使用して IAM アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドの「JSON タブでのポリシーの作成」を参照してください。

ROSA コンソールの使用

コンソール ROSA から にサブスクライブするには、IAM プリンシパルに必要な AWS Marketplace アクセス許可が必要です。アクセス許可により、プリンシパルは で ROSA 製品リストをサブスクライブおよびサブスクライブ解除 AWS Marketplace し、 AWS Marketplace サブスクリプションを表示できます。必要なアクセス許可を追加するには、 ROSA コンソールに移動し、 AWS 管理ポリシーを IAM プリンシパル`ROSAManageSubscription`にアタッチします。`ROSAManageSubscription` の詳細については、「the section called “AWS マネージドポリシー: ROSAManageSubscription”」を参照してください。

HCP で ROSA に AWS リソースの管理を許可する

ホスト型コントロールプレーン (HCP) を備えた ROSA は、サービスのオペレーションとサポートに必要なアクセス許可を持つ AWS マネージドポリシーを使用します。CLI または IAM コンソールを使用して、これらのポリシーを ROSA のサービスロールにアタッチします AWS アカウント。

詳細については、「the section called “ AWS マネージドポリシー”」を参照してください。

AWS リソースの管理を ROSA Classic に許可する

ROSA Classic は、 サービスによって事前定義されたアクセス許可を持つカスタマー管理 IAM ポリシーを使用します。 ROSA CLI を使用してこれらのポリシーを作成し、 のサービスロールにアタッチします AWS アカウント。 では、継続的なオペレーションとサービスサポートを確保するために、これらのポリシーがサービスで定義されているように設定されている ROSA 必要があります。

> **Note**
>
> Red Hat に相談せずに ROSA クラシックポリシーを変更しないでください。これにより、Red Hat の 99.95% クラスターのアップタイムサービスレベル契約が無効になる可能性があります。ホストされたコントロールプレーンを持つ ROSA は、アクセス許可のセットがより限定された AWS 管理ポリシーを使用します。詳細については、「the section called “AWS マネージドポリシー”」を参照してください。

のカスタマー管理ポリシーには、アカウントポリシーとオペレーターポリシーの 2 ROSA種類があります。アカウントポリシーは、サービスがサイト信頼性エンジニア (SRE) サポート、クラスター作成、コンピューティング機能のために Red Hat との信頼関係を確立するために使用する IAM ロールにアタッチされます。オペレーターポリシーは、OpenShift オペレーターが進入、ストレージ、イメージレジストリ、ノード管理に関連するクラスターオペレーションに使用する IAM ロールにアタッチされます。アカウントポリシーは ごとに 1 回作成されますが AWS アカウント、オペレーターポリシーはクラスターごとに 1 回作成されます。

詳細については、「the section called “ROSA Classic アカウントポリシー”」および「the section called “ROSA Classic オペレーターポリシー”」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、 がユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示 IAM ユーザー できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または を使用してプログラムでこのアクションを実行するアクセス許可が含まれています AWS CLI。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Effect": "Allow",
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
```

```
        },
        {
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

ROSA Classic アカウントポリシー

このセクションでは、ROSA Classic に必要なアカウントポリシーについて詳しく説明します。これらのアクセス許可は、ROSA Classic がクラスターが で実行される AWS リソースを管理し、Red Hat サイト信頼性エンジニアがクラスターをサポートできるようにするために必要です。ポリシー名にカスタムプレフィックスを割り当てることはできますが、それ以外の場合は、このページで定義されているように名前を付ける必要があります (例: `ManagedOpenShift-Installer-Role-Policy`)。

アカウントポリシーは OpenShift マイナーリリースバージョンに固有であり、下位互換性があります。クラスターを作成またはアップグレードする前に、 を実行してポリシーバージョンとクラスターバージョンが同じであることを確認しますrosa list account-roles。ポリシーバージョンがクラスターバージョンより小さい場合は、 rosa upgrade account-roles を実行してロールとアタッチされたポリシーをアップグレードします。同じマイナーリリースバージョンの複数のクラスターに同じアカウントポリシーとロールを使用できます。

[プレフィックス]-Installer-Role-Policy

IAM エンティティに [Prefix]-Installer-Role-Policy をアタッチできます。ROSA クラシッククラスターを作成する前に、このポリシーを という名前の IAM ロールにアタッチする必要があります[Prefix]-Installer-Role。このポリシーは、 ROSA インストーラがクラスターの作成に必要な AWS リソースを管理できるようにする必要なアクセス許可を付与します。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "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: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:GetReplicationConfiguration",
                "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"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

[プレフィックス]-ControlPlane-Role-Policy

IAM エンティティに [Prefix]-ControlPlane-Role-Policy をアタッチできます。ROSA クラシッククラスターを作成する前に、このポリシーを という名前の IAM ロールにアタッチする必要があります[Prefix]-ControlPlane-Role。このポリシーは、 ROSA コントロールプレーンをホストする Amazon EC2 および Elastic Load Balancing リソースの管理と読み取りに必要なアクセス許可を ROSA Classic に付与します KMS keys。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

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

[プレフィックス]-Worker-Role-Policy

IAM エンティティに [Prefix]-Worker-Role-Policy をアタッチできます。ROSA クラシック クラスターを作成する前に、このポリシーを という名前の IAM ロールにアタッチする必要があります[Prefix]-Worker-Role。このポリシーは、ワーカーノードとして実行されている EC2 インスタンスを記述するために必要なアクセス許可を ROSA Classic に付与します。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

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

```
    ]
}
```

[プレフィックス]-Support-Role-Policy

IAM エンティティに [Prefix]-Support-Role-Policy をアタッチできます。ROSA クラシッククラスターを作成する前に、このポリシーを という名前の IAM ロールにアタッチする必要があります[Prefix]-Support-Role。このポリシーは、クラスターノードの状態を変更する機能など、ROSA Classic クラスターが使用する AWS リソースを監視、診断、サポートするために必要なアクセス許可を Red Hat サイト信頼性エンジニアリングに付与します。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "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:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "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"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
```

```
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::managed-velero*",
                "arn:aws:s3:::*image-registry*"
            ]
        }
    ]
}
```

ROSA Classic オペレーターポリシー

このセクションでは、ROSA Classic に必要なオペレータポリシーについて詳しく説明します。ROSA クラシッククラスターを作成する前に、まずこれらのポリシーを関連するオペレーターロールにアタッチする必要があります。クラスターごとに固有のオペレーターロールのセットが必要です。

これらのアクセス許可は、OpenShift オペレーターが ROSA Classic クラスターノードを管理できるようにするために必要です。ポリシー名にカスタムプレフィックスを割り当てることで、ポリシー管理を簡素化できます (例: `ManagedOpenShift-openshift-ingress-operator-cloud-credentials`)。

[プレフィックス]-openshift-ingress-operator-cloud-credentials

IAM エンティティに `[Prefix]-openshift-ingress-operator-cloud-credentials` をアタッチできます。このポリシーは、外部クラスターアクセスのロードバランサーと DNS 設定をプロビジョニングおよび管理するために必要なアクセス許可を Ingress Operator に付与します。このポリシーでは、Ingress Operator が Route 53 リソースタグ値を読み取ってフィルタリングし、ホストゾーンを検出することもできます。オペレーターの詳細については、OpenShift GitHub ドキュメントの「OpenShift Ingress Operator」を参照してください。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

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

```
        {
            "Action": [
                "elasticloadbalancing:DescribeLoadBalancers",
                "route53:ListHostedZones",
                "route53:ListTagsForResources",
                "route53:ChangeResourceRecordSets",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[プレフィックス]-openshift-cluster-csi-drivers-ebs-cloud-credentials

IAM エンティティに `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` をアタッチできます。このポリシーは、ROSA クラシッククラスターに Amazon EBS CSI Amazon EBS ドライバーをインストールして維持するために必要なアクセス許可を CSI ドライバーオペレーターに付与します。演算子の詳細については、OpenShift GitHub ドキュメントの[aws-ebs-csi-driver-operator]」を参照してください。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateSnapshot",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
                "ec2:DescribeTags",
```

```
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DetachVolume",
                "ec2:EnableFastSnapshotRestores",
                "ec2:ModifyVolume"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[プレフィックス]-openshift-machine-api-aws-cloud-credentials

IAM エンティティに [Prefix]-openshift-machine-api-aws-cloud-credentials をアタッチできます。このポリシーは、ワーカーノードとして管理される Amazon EC2 インスタンスを記述、実行、終了するために必要なアクセス許可を Machine Config Operator に付与します。このポリシーは、 を使用したワーカーノードのルートボリュームのディスク暗号化を許可するアクセス許可も付与します AWS KMS keys。演算子の詳細については、OpenShift GitHub ドキュメントの machine-config-operator を参照してください。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
```

```
                "ec2:TerminateInstances",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

[プレフィックス]-openshift-cloud-credential-operator-cloud-credentials

IAM エンティティに `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` をアタッチできます。このポリシーは、アクセスキー IDs IAM ユーザー 、アタッチされたインラインポリシードキュメント、ユーザー作成日、パス、ユーザー ID、Amazon リソースネーム (ARN) などの詳細を取得するために必要なアクセス許可をクラウド認証情報オペレーターに付与します。演算子の詳細については、OpenShift GitHub ドキュメントのcloud-credential-operator」を参照してください。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

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

[プレフィックス]-openshift-image-registry-installer-cloud-credentials

IAM エンティティに `[Prefix]-openshift-image-registry-installer-cloud-credentials` をアタッチできます。このポリシーは、ROSA Classic のクラスター内イメージレジストリと依存サービスのリソースをプロビジョニングおよび管理するために必要なアクセス許可を Image Registry Operator に付与します Amazon S3。これは、オペレーターが ROSA Classic クラスターの内部レジストリをインストールして維持できるようにするために必要です。オペレーターの詳細については、OpenShift GitHub ドキュメントの「Image Registry Operator」を参照してください。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

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

[プレフィックス]-openshift-cloud-network-config-controller-cloud-cr

IAM エンティティに `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` をアタッチできます。このポリシーは、ROSA Classic クラスターネットワーキングオーバーレイで使用するネットワークリソースをプロビジョニングおよび管理するために必要なアクセス許可を Cloud Network Config Controller Operator に付与します。オペレーターは、これらのアクセス許可を使用して、ROSA Classic クラスターの一部として Amazon EC2 インスタンスのプライベート IP ア

ドレスを管理します。オペレーターの詳細については、OpenShift GitHub ドキュメントの「Cloud-network-config-controller」を参照してください。

アクセス許可ポリシー

このポリシードキュメントで定義されているアクセス許可は、どのアクションを許可または拒否するかを指定します。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignIpv6Addresses",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS の 管理ポリシー ROSA

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパ

ル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が最も高くなります。詳細については、「 IAM ユーザーガイド」の「 AWS 管理ポリシー」を参照してください。

AWS マネージドポリシー: ROSAManageSubscription

`ROSAManageSubscription` ポリシーを IAM エンティティにアタッチできます。 ROSA コンソール ROSA で を有効にする前に、まずこのポリシーを AWS IAM ロールにアタッチする必要があります。

このポリシーは、 ROSA サブスクリプションを管理するために必要な AWS Marketplace アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `aws-marketplace:Subscribe` - AWS Marketplace 製品をサブスクライブするアクセス許可を付与します ROSA。
- `aws-marketplace:Unsubscribe` - プリンシパルが AWS Marketplace 製品のサブスクリプションを削除できるようにします。
- `aws-marketplace:ViewSubscriptions` - プリンシパルにサブスクリプションの表示を許可します AWS Marketplace。これは、 IAM プリンシパルが利用可能な AWS Marketplace サブスクリプションを表示できるようにするために必要です。

JSON ポリシードキュメントの詳細については、 AWS 「 マネージドポリシーリファレンスガイド」のROSAManageSubscription」を参照してください。

HCP アカウントポリシーを使用する ROSA

このセクションでは、ホスト型コントロールプレーン (HCP) を使用する ROSA に必要なアカウントポリシーについて詳しく説明します。これらの AWS 管理ポリシーは、HCP IAM ロールを持つ ROSA で使用されるアクセス許可を追加します。この権限は Red Hat サイト信頼性エンジニアリング (SRE) のテクニカルサポート、クラスターのインストール、コントロールプレーンとコンピュート機能に必要です。

> **Note**
>
> AWS マネージドポリシーは、ROSA がホスト型コントロールプレーン (HCP) で使用することを目的としています。ROSA クラシッククラスターは、カスタマー管理の IAM ポリシーを使用します。ROSA クラシックポリシーの詳細については、the section called “ROSA Classic アカウントポリシー”「」および「」を参照してくださいthe section called “ROSA Classic オペレーターポリシー”。

AWS マネージドポリシー: ROSAWorkerInstancePolicy

IAM エンティティROSAWorkerInstancePolicyに をアタッチできます。クラスターを作成する前に、このポリシーがアタッチされた IAM ロールが必要です。ROSA サービスは、ユーザーに代わって他の を呼び出し AWS のサービス ます。これは、各クラスターで使用するリソースを管理するために行います。

アクセス許可の詳細

このポリシーには、ROSA ワーカーノードが次のタスクを完了できるようにする以下のアクセス許可が含まれています。

- ec2 — ROSA クラスターワーカーノードのライフサイクル管理の一環として、 AWS リージョンと Amazon EC2 インスタンスの詳細を評価します。
- ecr - クラスターのインストールとワーカーノードのライフサイクル管理に必要な ROSA 管理の ECR リポジトリからイメージを評価して取得します。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAWorkerInstancePolicy」を参照してください。

AWS マネージドポリシー: ROSASRESupportPolicy

IAM エンティティに ROSASRESupportPolicy をアタッチできます。

ホストされたコントロールプレーンクラスターで ROSA を作成する前に、まずこのポリシーを IAM ロールにアタッチする必要があります。このポリシーは、クラスター ROSA ノードの状態を変更する機能など、 ROSA クラスターに関連付けられた AWS リソースを直接監視、診断、サポートするために必要なアクセス許可を Red Hat サイト信頼性エンジニア (SREs) に付与します。

アクセス許可の詳細

このポリシーには、Red Hat SRE に以下のタスクを完了させるための以下の権限が含まれています。

- `cloudtrail` — クラスターに関連する AWS CloudTrail イベントと証跡を読み取ります。
- `cloudwatch` — クラスターに関連する Amazon CloudWatch メトリクスを読み取ります。
- `ec2` — セキュリティグループ、VPC エンドポイント接続、ボリュームステータスなど、クラスターの状態に関連する Amazon EC2 コンポーネントの読み取り、説明、レビューを行います。Amazon EC2 インスタンスを起動、停止、再起動、および終了します。
- `elasticloadbalancing` — クラスターの状態に関連する Elastic Load Balancing パラメータを読み、記述し、確認します。
- `iam` — クラスターの状態に関連する IAM ロールを評価します。
- `route53` — クラスターの正常性に関連する DNS 設定を確認します。
- `sts` — `DecodeAuthorizationMessage` — デバッグ目的で IAM メッセージを読み取ります。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSASRESupportPolicy」を参照してください。

AWS マネージドポリシー: ROSAInstallerPolicy

IAM エンティティ`ROSAInstallerPolicy`に をアタッチできます。

ホストされたコントロールプレーンクラスターで ROSA を作成する前に、このポリシーを という名前の IAM ロールにアタッチする必要があります`[Prefix]-ROSA-Worker-Role`。このポリシーにより、エンティティは `[Prefix]-ROSA-Worker-Role` パターンに従う任意のロールをインスタンスプロファイルに追加できます。このポリシーは、 ROSA クラスターのインストールをサポートする AWS リソースを管理するために必要なアクセス許可をインストーラに付与します。

アクセス許可の詳細

このポリシーには、インストーラーに以下のタスクを完了させるための以下の権限が含まれています。

- `ec2` — Red Hat が AWS アカウント 所有および管理する でホストされている AMIs を使用して Amazon EC2 インスタンスを実行します。 Amazon EC2 ノードに関連付けられた Amazon EC2 インスタンス、ボリューム、ネットワークリソースについて説明します。このアクセス許可は、Kubernetes コントロールプレーンがインスタンスをクラスターに結合し、クラスターがその内部に存在するかどうかを評価できるようにするために必要です Amazon VPC。Amazon

EC2 キャパシティ予約を検査し、ROSA の新しいキャパシティ予約機能をサポートします。に一致するタグキーを使用して、サブネットのタグをタグ付けおよび削除します"kubernetes.io/cluster/*"。これは、クラスターの進入に使用されるロードバランサーが該当するサブネットでのみ作成され、Kubernetes クラスター識別タグを管理するために必要です。

- elasticloadbalancing — クラスター上のターゲットノードにロードバランサーを追加します。クラスター上のターゲットノードからロードバランサーを削除します。この権限は、Kubernetes コントロールプレーンが Kubernetes サービスおよび OpenShift アプリケーションサービスによってリクエストされるロードバランサーを動的にプロビジョニングできるようにするために必要です。
- kms — AWS KMS キーを読み取り、 への許可を作成および管理し Amazon EC2、外部で使用する一意の対称データキーを返します AWS KMS。これは、クラスターの作成時に etcd 暗号化が有効になっている場合に、暗号化された etcd データを使用するために必要です。
- iam — IAM ポリシーとロールを検証します。クラスターに関連する Amazon EC2 インスタンスプロファイルを動的にプロビジョニングおよび管理します。iam:TagInstanceProfile 権限を使用して IAM インスタンスプロファイルにタグを追加します。お客様が指定したクラスター OIDC プロバイダーが見つからないためにクラスターのインストールに失敗した場合のインストーラエラーメッセージを提供します。
- route53 — クラスターの作成に必要な Route 53 リソースを管理します。
- servicequotas — クラスターの作成に必要なサービスクォータを評価します。
- sts — ROSA コンポーネントの一時的な AWS STS 認証情報を作成します。クラスター作成用の認証情報を仮定します。
- secretsmanager — クラスタープロビジョニングの一環として、シークレット値を読み取り、カスタマーマネージド OIDC 設定を安全に許可します。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAInstallerPolicy」を参照してください。

AWS マネージドポリシー: ROSASharedVPCRoute53Policy

IAM エンティティROSASharedVPCRoute53Policyに をアタッチできます。このポリシーを IAM ロールにアタッチして、ROSA クラスターが AWS のサービス 共有 VPC 環境で他の を呼び出すことができるようにする必要があります。

このポリシーにより、ROSA インストーラは Route 53 レコードを設定できます。このポリシーは、共有 VPC での使用を目的としており、共有 VPC ユースケースに合わせた Route 53 アクセス許可のサブセットを提供します。

アクセス許可の詳細

このポリシーには、ROSA インストーラが次のタスクを完了できるようにする以下のアクセス許可が含まれています。

- route53 — DNS ゾーン情報と既存の DNS レコードを読み取り、現在の DNS 設定を理解します。DNS レコードを作成、変更.openshiftapps.com.devshift.org、削除します。ただし、、.hypershift.local、、.openshiftusgov.com、 などの特定の ROSA 関連のドメインパターンのみを対象とします.devshiftusgov.com。リソース管理と整理のために Route 53 リソースのタグを追加、変更、または削除します。
- tag — タグに基づいて AWS リソースを検出して一覧表示します。これは、ROSA によって管理されるリソースを識別するのに役立ちます。

JSON ポリシードキュメントの最新バージョンなど、ポリシーの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSASharedVPCRoute53Policy」を参照してください。

AWS マネージドポリシー: ROSASharedVPCEndpointPolicy

IAM エンティティROSASharedVPCEndpointPolicyに をアタッチできます。このポリシーを IAM ロールにアタッチして、ROSA クラスターが AWS のサービス 共有 VPC 環境で他の を呼び出すことができるようにする必要があります。

このポリシーにより、ROSA インストーラは共有 VPC 環境で VPC エンドポイントとセキュリティグループを設定できます。

アクセス許可の詳細

このポリシーには、ROSA インストーラが次のタスクを完了できるようにする以下のアクセス許可が含まれています。

- ec2 — VPC エンドポイント、VPCs、セキュリティグループなどの VPC 関連リソースを記述してネットワーク環境を理解するための読み取り専用アクセス許可。タグベースの制限を使用してセキュリティグループを作成、削除、変更します。これにより、ROSA は ROSA タグ付きリソースのみにオペレーションを制限しながら、クラスターネットワーキングのセキュリティグループを作成および管理できます。タグベースの制限がある VPC エンドポイントを作成、変更、削除し、ROSA が AWS のサービス 共有 VPC 環境で へのプライベート接続用の VPC エンドポイントを作成および管理できるようにします。リソースの適切な識別と管理のために、作成時に新しく作成された VPC エンドポイントとセキュリティグループにタグを適用します。

JSON ポリシードキュメントの最新バージョンなど、ポリシーの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSASharedVPCEndpointPolicy」を参照してください。

HCP 演算子ポリシーを使用する ROSA

このセクションでは、ホスト型コントロールプレーン (HCP) を使用する ROSA に必要なオペレータポリシーについて詳しく説明します。これらの AWS 管理ポリシーは、HCP で ROSA を使用するために必要なオペレーターロールにアタッチできます。OpenShift オペレーターが HCP を備えた ROSA のクラスターノードを管理できるようにするには、この権限が必要です。

> **Note**
>
> AWS マネージドポリシーは、ROSA がホスト型コントロールプレーン (HCP) で使用することを目的としています。ROSA クラシッククラスターは、カスタマー管理の IAM ポリシーを使用します。ROSA クラシックポリシーの詳細については、the section called “ROSA Classic アカウントポリシー”「」および「」を参照してくださいthe section called “ROSA Classic オペレーターポリシー”。

AWS マネージドポリシー: ROSAAmazonEBSCSIDriverOperatorPolicy

IAM エンティティROSAAmazonEBSCSIDriverOperatorPolicyに をアタッチできます。このポリシーをオペレーター IAM ロールにアタッチして、ホストされたコントロールプレーンクラスターを持つ ROSA が他の を呼び出すことができるようにする必要があります AWS のサービス。クラスターごとに固有のオペレーターロールのセットが必要です。

このポリシーは、CSI Amazon EBS ドライバーを ROSA クラスターにインストールして維持するために必要なアクセス許可を CSI Amazon EBS ドライバーオペレーターに付与します。オペレーターの詳細については、OpenShift GitHub ドキュメントの「aws-ebs-csi-driver オペレーター」を参照してください。

アクセス許可の詳細

このポリシーには、 Amazon EBS ドライバーオペレーターが次のタスクを完了できるようにする以下のアクセス許可が含まれています。

- ec2 — Amazon EC2 インスタンスにアタッチされている Amazon EBS ボリュームを作成、変更、アタッチ、デタッチ、削除します。 Amazon EBS ボリュームスナップショットを作成および削除し、 Amazon EC2 インスタンス、ボリューム、スナップショットを一覧表示します。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAAmazonEBSCSIDriverOperatorPolicy」を参照してください。

AWS マネージドポリシー: ROSAIngressOperatorPolicy

IAM エンティティROSAIngressOperatorPolicyに をアタッチできます。このポリシーをオペレーター IAM ロールにアタッチして、ホストされたコントロールプレーンクラスターを持つ ROSA が他の を呼び出すことができるようにする必要があります AWS のサービス。クラスターごとに固有のオペレーターロールのセットが必要です。

このポリシーは、 ROSA クラスターのロードバランサーと DNS 設定をプロビジョニングおよび管理するために必要なアクセス許可を Ingress Operator に付与します。このポリシーは、タグ値への読み取りアクセスを許可します。次に、オペレーターは、ホストゾーンを検出する Route 53 リソースのタグ値をフィルタリングします。オペレーターの詳細については、OpenShift GitHub ドキュメントの「OpenShift Ingress Operator」を参照してください。

アクセス許可の詳細

このポリシーには、Ingress Operator に以下のタスクを完了させるための以下の権限が含まれています。

- `elasticloadbalancing` — プロビジョニングされたロードバランサーの状態を記述します。
- `route53` — Route 53 ホストゾーンを一覧表示し、ROSA クラスターによって制御される DNS を管理するレコードを編集します。
- `tag` — `tag:GetResources` 権限を使用してタグ付けされたリソースを管理します。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAIngressOperatorPolicy」を参照してください。

AWS マネージドポリシー: ROSAImageRegistryOperatorPolicy

IAM エンティティROSAImageRegistryOperatorPolicyに をアタッチできます。このポリシーをオペレーター IAM ロールにアタッチして、ホストされたコントロールプレーンクラスターを持つ ROSA が他の を呼び出すことができるようにする必要があります AWS のサービス。クラスターごとに固有のオペレーターロールのセットが必要です。

このポリシーは、クラスター ROSA 内のイメージレジストリと S3 を含む依存サービスのリソースをプロビジョニングおよび管理するために必要なアクセス許可を Image Registry Operator に付与します。これは、オペレーターが ROSA クラスターの内部レジストリをインストールして維持でき

るようにするために必要です。オペレーターの詳細については、OpenShift GitHub ドキュメントの「Image Registry Operator」を参照してください。

アクセス許可の詳細

このポリシーには、Image Registry Operator に以下のタスクを完了させるための以下の権限が含まれています。

- s3 — Amazon S3 バケットをコンテナイメージコンテンツとクラスターメタデータの永続的ストレージとして管理および評価します。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAImageRegistryOperatorPolicy」を参照してください。

AWS マネージドポリシー: ROSACloudNetworkConfigOperatorPolicy

IAM エンティティROSACloudNetworkConfigOperatorPolicyに をアタッチできます。このポリシーをオペレーター IAM ロールにアタッチして、ホストされたコントロールプレーンクラスターを持つ ROSA が他の を呼び出すことができるようにする必要があります AWS のサービス。クラスターごとに固有のオペレーターロールのセットが必要です。

このポリシーは、 ROSA クラスターネットワークオーバーレイのネットワークリソースをプロビジョニングおよび管理するために必要なアクセス許可を Cloud Network Config Controller Operator に付与します。オペレーターは、これらのアクセス許可を使用して、 ROSA クラスターの一部として Amazon EC2 インスタンスのプライベート IP アドレスを管理します。オペレーターの詳細については、OpenShift GitHub ドキュメントの「Cloud-network-config-controller」を参照してください。

アクセス許可の詳細

このポリシーには、Cloud Network Config Controller Operator に以下のタスクを完了させるための以下の権限が含まれています。

- ec2 — ROSA クラスター内の Amazon EC2 インスタンス、 Amazon VPC サブネット、および Elastic Network Interface を接続するための設定を読み取り、割り当て、記述します。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSACloudNetworkConfigOperatorPolicy」を参照してください。

AWS マネージドポリシー: ROSAKubeControllerPolicy

IAM エンティティROSAKubeControllerPolicyに をアタッチできます。このポリシーをオペレーター IAM ロールにアタッチして、ホストされたコントロールプレーンクラスターを持つ ROSA が他の を呼び出すことができるようにする必要があります AWS のサービス。クラスターごとに固有のオペレーターロールのセットが必要です。

このポリシーは Amazon EC2、kube コントローラーに必要なアクセス許可と Elastic Load Balancing、ホストされたコントロールプレーンクラスターを持つ ROSA の AWS KMS リソースを付与します。このコントローラーに関する詳細は、OpenShift ドキュメントの「コントローラーアーキテクチャ」を参照してください。

アクセス許可の詳細

このポリシーには、kube コントローラーに以下のタスクを完了させるための以下の権限が含まれています。

- ec2 — Amazon EC2 インスタンスセキュリティグループを作成、削除、およびタグを追加します。インバウンドルールをセキュリティグループに追加します。アベイラビリティーゾーン、Amazon EC2 インスタンス、ルートテーブル、セキュリティグループ、VPC、サブネットについて記述します。
- elasticloadbalancing — ロードバランサーとそのポリシーを作成および管理します。ロードバランサーリスナーを作成および管理します。ターゲットグループでターゲットを登録および登録解除し、ターゲットグループを管理します。ロードバランサーで Amazon EC2 インスタンスを登録および登録解除し、ロードバランサーにタグを追加します。
- kms — AWS KMS キーに関する詳細情報を取得します。これは、クラスターの作成時に etcd 暗号化が有効になっている場合に、暗号化された etcd データを使用するために必要です。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAKubeControllerPolicy」を参照してください。

AWS マネージドポリシー: ROSANodePoolManagementPolicy

IAM エンティティROSANodePoolManagementPolicyに をアタッチできます。このポリシーをオペレーター IAM ロールにアタッチして、ホストされたコントロールプレーンクラスターを持つ ROSA が他の AWS サービスを呼び出すことができるようにする必要があります。クラスターごとに固有のオペレーターロールのセットが必要です。

このポリシーは、ワーカーノードとして管理される Amazon EC2 インスタンスを記述、実行、終了するために必要なアクセス許可を NodePool コントローラーに付与します。このポリシーは、 AWS KMS キーを使用したワーカーノードのルートボリュームのディスク暗号化、ワーカーノードにアタッチされた Elastic Network Interface へのタグ付け、Amazon EC2 キャパシティ予約へのアクセスを許可するアクセス許可も付与します。このコントローラーに関する詳細は、OpenShift ドキュメントの「コントローラーアーキテクチャ」を参照してください。

アクセス許可の詳細

このポリシーには、NodePool コントローラーに以下のタスクを完了させるための以下の権限が含まれています。

- ec2 — Red Hat が AWS アカウント 所有および管理する でホストされている AMIs を使用して Amazon EC2 インスタンスを実行します。 ROSA クラスター内の EC2 ライフサイクルを管理します。ワーカーノードを動的に作成し Elastic Load Balancing、、 Amazon VPC Route 53 Amazon EBS、および と統合します Amazon EC2。ROSA のキャパシティ予約機能をサポートするために、キャパシティ予約にアクセスして説明します。
- iam — という名前のサービスにリンクされたロール Elastic Load Balancing を介して を使用しますAWSServiceRoleForElasticLoadBalancing。 Amazon EC2 インスタンスプロファイルにロールを割り当てます。
- kms — AWS KMS キーを読み取り、 への許可を作成および管理し Amazon EC2、外部で使用する一意の対称データキーを返します AWS KMS。これは、ワーカーノードのルートボリュームのディスク暗号化を可能にするために必要です。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSANodePoolManagementPolicy」を参照してください。

AWS マネージドポリシー: ROSAKMSProviderPolicy

IAM エンティティROSAKMSProviderPolicyに をアタッチできます。このポリシーをオペレーター IAM ロールにアタッチして、ホストされたコントロールプレーンクラスターを持つ ROSA が他の を呼び出すことができるようにする必要があります AWS のサービス。クラスターごとに固有のオペレーターロールのセットが必要です。

このポリシーは、etcdデータ AWS 暗号化をサポートする AWS KMS キーを管理するために必要なアクセス許可を組み込みの暗号化プロバイダーに付与します。このポリシーにより Amazon EC2 、AWS は、暗号化プロバイダーが提供する KMS キーを使用してetcdデータを暗号化および復号でき

ます。このプロバイダーの詳細については、Kubernetes GitHub ドキュメントの「AWS 暗号化プロバイダー」を参照してください。

アクセス許可の詳細

このポリシーには、 AWS 暗号化プロバイダーが次のタスクを完了できるようにする以下のアクセス許可が含まれています。

- `kms` — AWS KMS キーを暗号化、復号、取得します。これは、クラスターの作成時に `etcd` 暗号化が有効になっている場合に、暗号化された `etcd` データを使用するために必要です。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAKMSProviderPolicy」を参照してください。

AWS マネージドポリシー: ROSAControlPlaneOperatorPolicy

IAM エンティティ`ROSAControlPlaneOperatorPolicy`に をアタッチできます。このポリシーをオペレーター IAM ロールにアタッチして、ホストされたコントロールプレーンクラスターを持つ ROSA が他の を呼び出すことができるようにする必要があります AWS のサービス。クラスターごとに固有のオペレーターロールのセットが必要です。

このポリシーは、ホストされたコントロールプレーンクラスターで ROSA の Amazon EC2 および Route 53 リソースを管理するために必要なアクセス許可をコントロールプレーンオペレーターに付与します。このオペレーターに関する詳細は、OpenShift ドキュメントの「コントローラーアーキテクチャ」を参照してください。

アクセス許可の詳細

このポリシーには、コントロールプレーンオペレーターに以下のタスクを完了させるための以下の権限が含まれています。

- `ec2` — Amazon VPC エンドポイントを作成および管理します。
- `route53` — Route 53 レコードセットを一覧表示および変更し、ホストゾーンを一覧表示します。
- RedHatManagedSecurityGroups にタグを追加: コントロールプレーンオペレーターが作成後に Red Hat が管理するセキュリティグループにタグを付けることを許可します。これは、HCP クラスターを持つ ROSA に関連付けられたセキュリティグループの適切なリソースライフサイクル管理とクリーンアップに必要です。

- ManageVPCEndpointWithCondition: クラスターのアップグレード中の VPCE 調整の失敗を修正しました。演算子には、セキュリティグループを参照する VPC エンドポイントを変更するアクセス許可が必要です。

JSON ポリシードキュメントの詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAControlPlaneOperatorPolicy」を参照してください。

ROSA AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始 ROSA してからの の AWS 管理ポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートについては、ドキュメント履歴 ページの RSS フィードを購読してください。

変更	説明	日付
ROSAControlPlaneOperatorPolicy — ポリシーが更新されました	ROSA は、適切なリソースライフサイクル管理のために Red Hat が管理するセキュリティグループのタグ付けを許可し、Security-group/* を ManageVPCEndpointWithCondition に追加して、クラスターのアップグレード中の VPCE 調整の失敗を修正するようにポリシーを更新しました。詳細についてはthe section called “AWS マネージドポリシー: ROSAControlPlaneOperatorPolicy”を参照してください。	2026 年 4 月 9 日
ROSAKubeControllerPolicy — ポリシーが更新されました	ROSA は、ターゲットグループでターゲットを登録および登録解除するための Elastic Load Balancing アクセス許可を明確にするためにポリシーを更新しました。詳細	2026 年 3 月 5 日

変更	説明	日付
	については the section called “AWS マネージドポリシー: ROSAKubeControllerPolicy”を参照してください。	
ROSANodePoolManagementPolicy — ポリシーが更新されました	ROSA は、Amazon EC2 キャパシティ予約のリソースアクセスを追加するようにポリシーを更新しました。この変更により、NodePool コントローラーはキャパシティ予約にアクセスして記述し、リソース管理を改善できます。詳細については the section called “AWS マネージドポリシー: ROSANodePoolManagementPolicy”を参照してください。	2025 年 9 月 3 日
ROSASharedVPCEndpointPolicy — 新しいポリシーを追加	ROSA は、 ROSA インストーラが共有 VPC 環境で VPC エンドポイントとセキュリティグループを設定できるようにする新しいポリシーを追加しました。このポリシーは、共有 VPC ユースケースに合わせた EC2 アクセス許可のサブセットを提供します。詳細については the section called “AWS マネージドポリシー: ROSASharedVPCEndpointPolicy”を参照してください。	2025 年 8 月 7 日

変更	説明	日付
ROSASharedVPCRoute 53Policy — 新しいポリシーを追加	ROSA は、 ROSA インストーラが共有 VPC 環境で Route 53 レコードを設定できるようにする新しいポリシーを追加しました。このポリシーは、共有 VPC ユースケースに合わせた Route 53 アクセス許可のサブセットを提供します。詳細については the section called “AWS マネージドポリシー: ROSASharedVPCRoute 53Policy”を参照してください。	2025 年 8 月 7 日
ROSAInstallerPolicy — ポリシーが更新されました	ROSA はポリシーを更新し、 ROSA インストーラが Amazon EC2 キャパシティ予約を検査して ROSA の新しいキャパシティ予約機能をサポートできるようにしました。この更新により、インストーラはタグキーマッチングを使用してサブネット上のタグを削除し `"kubernetes.io/cluster/*"` 、Kubernetes クラスターのタグ管理を改善することもできます。詳細については the section called “AWS マネージドポリシー: ROSAInstallerPolicy”を参照してください。	2025 年 8 月 7 日

変更	説明	日付
ROSAImageRegistryOperatorPolicy — ポリシーが更新されました	ROSA は、アクセス許可が S3 バケットリソースレベルにスコープダウンされるようにポリシーを更新しました。この変更は、 AWS 商用リージョンと GovCloud リージョンの両方の ROSA ストレージ要件を満たします。詳細については the section called “AWS マネージドポリシー: ROSAImageRegistryOperatorPolicy”を参照してください。	2025 年 5 月 19 日
ROSANodePoolManagementPolicy — ポリシーが更新されました	ROSA は、ワーカーノードにアタッチされている Elastic Network Interface のタグ付けを許可するようにポリシーを更新しました。詳細については the section called “AWS マネージドポリシー: ROSANodePoolManagementPolicy”を参照してください。	2025 年 5 月 5 日

変更	説明	日付
ROSAImageRegistryOperatorPolicy — ポリシーが更新されました	ROSA は、Red Hat OpenShift Image Registry Operator が ROSA クラスター内イメージレジストリで使用できるように、 AWS GovCloud リージョンの Amazon S3 バケットとオブジェクトをプロビジョニングおよび管理できるようにポリシーを更新しました。この変更は、 AWS GovCloud リージョンの ROSA ストレージ要件を満たしています。詳細については the section called “AWS マネージドポリシー: ROSAImageRegistryOperatorPolicy”を参照してください。	2025 年 4 月 16 日
ROSAWorkerInstancePolicy — ポリシーが更新されました	ROSA はポリシーを更新し、ワーカーノードがクラスターのインストールとワーカーノードのライフサイクル管理に必要な ROSA マネージド ECR リポジトリからイメージを評価および取得できるようにしました。詳細については the section called “AWS マネージドポリシー: ROSAWorkerInstancePolicy”を参照してください。	2025 年 3 月 3 日

変更	説明	日付
ROSANodePoolManagementPolicy — ポリシーが更新されました	ROSA は、リクエストにタグ が含まれている場合、ec2:RunInstances 呼び出し中にのみ、EC2 インスタンスと同様に Elastic Network Interface にタグを付けることができるようにポリシーを更新しました`red-hat-managed: true` 。これらのアクセス許可は、HCP 4.17 クラスターで ROSA をサポートするために必要です。詳細についてはthe section called “AWS マネージドポリシー: ROSANodePoolManagementPolicy”を参照してください。	2025 年 2 月 24 日
ROSAAmazonEBSCSIDriverOperatorPolicy — ポリシーが更新されました	ROSA は、新しい Amazon EBS スナップショット認可 API をサポートするようにポリシーを更新しました。詳細についてはthe section called “AWS マネージドポリシー: ROSAAmazonEBSCSIDriverOperatorPolicy”を参照してください。	2025 年 1 月 17 日

変更	説明	日付
ROSANodePoolManagementPolicy — ポリシーが更新されました	ROSA は、適切なプライベート DNS 名を設定するために、 ROSA ノードプールマネージャーが DHCP オプションセットを記述できるようにポリシーを更新しました。詳細については the section called “AWS マネージドポリシー: ROSANodePoolManagementPolicy”を参照してください。	2024 年 5 月 2 日
ROSAInstallerPolicy — ポリシーが更新されました	ROSA は、 ROSA インストーラが に一致するタグキーを使用してサブネットにタグを追加できるようにポリシーを更新しました`"kubernetes.io/cluster/*"` 。詳細については the section called “AWS マネージドポリシー: ROSAInstallerPolicy”を参照してください。	2024 年 4 月 24 日
ROSASRESupportPolicy — ポリシーが更新されました	ROSA は、SRE ロールが ROSA としてタグ付けされたインスタンスプロファイルに関する情報を取得できるようにポリシーを更新しました`red-hat-managed` 。詳細については the section called “AWS マネージドポリシー: ROSASRESupportPolicy”を参照してください。	2024 年 4 月 10 日

変更	説明	日付
ROSAInstallerPolicy — ポリシーが更新されました	ROSA は、 の AWS 管理ポリシーが で使用される IAM ロールにアタッチ ROSA されていることを ROSA インストーラが検証できるようにポリシーを更新しました ROSA。この更新により、インストーラはカスタマー管理ポリシーが ROSA ロールにアタッチされているかどうかを特定することもできます。詳細についてはthe section called “AWS マネージドポリシー: ROSAInstallerPolicy”を参照してください。	2024 年 4 月 10 日
ROSAInstallerPolicy — ポリシーが更新されました	ROSA は、お客様が指定したクラスター OIDC プロバイダーが見つからないためにクラスターのインストールが失敗した場合に、サービスがインストーラアラートメッセージを提供できるようにポリシーを更新しました。この更新により、サービスが既存の DNS ネームサーバーを取得して、クラスタープロビジョニングオペレーションがべき等になるようにすることもできます。詳細についてはthe section called “AWS マネージドポリシー: ROSAInstallerPolicy”を参照してください。	2024 年 1 月 26 日

変更	説明	日付
ROSASRESupportPolicy — ポリシーが更新されました	ROSA は、DescribeSecurity Groups API を使用してセキュリティグループで読み取りオペレーションを実行できるようにポリシーを更新しました。詳細については the section called “AWS マネージドポリシー: ROSASRESupportPolicy” を参照してください。	2024 年 1 月 22 日
ROSAImageRegistryOperatorPolicy — ポリシーが更新されました	ROSA は、Image Registry Operator が 14 文字の名前を持つリージョンの Amazon S3 バケットに対してアクションを実行できるようにポリシーを更新しました。詳細については the section called “AWS マネージドポリシー: ROSAImageRegistryOperatorPolicy” を参照してください。	2023 年 12 月 12 日
ROSAKubeControllerPolicy — ポリシーが更新されました	ROSA は、kube-controller-manager がアベイラビリティーゾーン、 Amazon EC2 インスタンス、ルートテーブル、セキュリティグループ、VPCs、サブネットを記述できるようにポリシーを更新しました。詳細については the section called “AWS マネージドポリシー: ROSAKubeControllerPolicy” を参照してください。	2023 年 10 月 16 日

変更	説明	日付
ROSAManageSubscription — ポリシーが更新されました	ROSA は、ホストされたコントロールプレーン ProductId を持つ ROSA を追加するようにポリシーを更新しました。詳細についてはthe section called “AWS マネージドポリシー: ROSAManageSubscription”を参照してください。	2023 年 8 月 1 日
ROSAKubeControllerPolicy — ポリシーが更新されました	ROSA は、kube-controller-manager が Network Load Balancer を Kubernetes サービスロードバランサーとして作成できるようにポリシーを更新しました。Network Load Balancer を使用すると、不安定なワークロードの処理能力が向上し、ロードバランサーの静的 IP アドレスのサポートが可能になります。詳細についてはthe section called “AWS マネージドポリシー: ROSAKubeControllerPolicy”を参照してください。	2023 年 7 月 13 日

変更	説明	日付
ROSANodePoolManagementPolicy — 新しいポリシーが追加されました	ROSA に、NodePool コントローラーがワーカーノードとして管理される Amazon EC2 インスタンスを記述、実行、終了できるようにする新しいポリシーが追加されました。このポリシーは、 AWS KMS キーを使用したワーカーノードのルートボリュームのディスク暗号化も有効にします。詳細については the section called “AWS マネージドポリシー: ROSANodePoolManagementPolicy” を参照してください。	2023 年 6 月 8 日
ROSAInstallerPolicy — 新しいポリシーが追加されました	ROSA は、インストーラがクラスターのインストールをサポートする AWS リソースを管理できるようにする新しいポリシーを追加しました。詳細については the section called “AWS マネージドポリシー: ROSAInstallerPolicy” を参照してください。	2023 年 6 月 6 日

変更	説明	日付
ROSASRESupportPolicy — 新しいポリシーが追加されました	ROSA は、Red Hat SREs が ROSA クラスターノードの状態を変更する機能など、ROSA クラスターに関連付けられた AWS リソースを直接監視、診断、サポートできるようにする新しいポリシーを追加しました。詳細については the section called “AWS マネージドポリシー: ROSASRESupportPolicy” を参照してください。	2023 年 6 月 1 日
ROSAKMSProviderPolicy — 新しいポリシーが追加されました	ROSA に、組み込みの AWS 暗号化プロバイダーが etcd データ暗号化をサポートする AWS KMS キーを管理できるようにする新しいポリシーが追加されました。詳細については the section called “AWS マネージドポリシー: ROSAKMSProviderPolicy” を参照してください。	2023 年 4 月 27 日

変更	説明	日付
ROSAKubeControllerPolicy — 新しいポリシーが追加されました	ROSA は、kube コントローラーがホストされたコントロールプレーンクラスター ROSA で Amazon EC2 Elastic Load Balancingと の AWS KMS リソースを管理できるようにする新しいポリシーを追加しました。詳細についてはthe section called “AWS マネージドポリシー: ROSAKubeControllerPolicy”を参照してください。	2023 年 4 月 27 日
ROSAImageRegistryOperatorPolicy — 新しいポリシーが追加されました	ROSA は、Image Registry Operator がクラスター ROSA 内のイメージレジストリと S3 を含む依存サービスのリソースをプロビジョニングおよび管理できるようにする新しいポリシーを追加しました。詳細についてはthe section called “AWS マネージドポリシー: ROSAImageRegistryOperatorPolicy”を参照してください。	2023 年 4 月 27 日

変更	説明	日付
ROSAControlPlaneOperatorPolicy — 新しいポリシーが追加されました	ROSA は、コントロールプレーンオペレーターがホストされたコントロールプレーンクラスター ROSA で の Amazon EC2 および Route 53 リソースを管理できるようにする新しいポリシーを追加しました。詳細についてはthe section called “AWS マネージドポリシー: ROSAControlPlaneOperatorPolicy”を参照してください。	2023 年 4 月 24 日
ROSACloudNetworkConfigOperatorPolicy — 新しいポリシーが追加されました	ROSA は、Cloud Network Config Controller Operator が ROSA クラスターネットワーキングオーバーレイのネットワークリソースをプロビジョニングおよび管理できるようにする新しいポリシーを追加しました。詳細についてはthe section called “AWS マネージドポリシー: ROSACloudNetworkConfigOperatorPolicy”を参照してください。	2023 年 4 月 20 日

変更	説明	日付
ROSAIngressOperatorPolicy — 新しいポリシーが追加されました	ROSA は、Ingress Operator が ROSA クラスターのロードバランサーと DNS 設定をプロビジョニングおよび管理できるようにする新しいポリシーを追加しました。詳細については the section called “AWS マネージドポリシー: ROSAIngressOperatorPolicy”を参照してください。	2023 年 4 月 20 日
ROSAAmazonEBSCSIDriverOperatorPolicy — 新しいポリシーが追加されました	ROSA は、CSI Amazon EBS ドライバーオペレーターが ROSA クラスターに CSI Amazon EBS ドライバーをインストールして維持できるようにする新しいポリシーを追加しました。詳細については the section called “AWS マネージドポリシー: ROSAAmazonEBSCSIDriverOperatorPolicy”を参照してください。	2023 年 4 月 20 日
ROSAWorkerInstancePolicy — 新しいポリシーが追加されました	ROSA は、サービスがクラスターリソースを管理できるようにする新しいポリシーを追加しました。詳細については the section called “AWS マネージドポリシー: ROSAWorkerInstancePolicy”を参照してください。	2023 年 4 月 20 日

変更	説明	日付
ROSAManageSubscription — 新しいポリシーが追加されました	ROSA は、 ROSA サブスクリプションの管理に必要な AWS Marketplace アクセス許可を付与する新しいポリシーを追加しました。詳細については the section called “AWS マネージドポリシー: ROSAManageSubscription” を参照してください。	2022 年 4 月 11 日
Red Hat OpenShift Service on AWS が変更の追跡を開始しました	Red Hat OpenShift Service on AWS は、 AWS 管理ポリシーの変更の追跡を開始しました。	2022 年 3 月 2 日

ROSA ID とアクセスのトラブルシューティング

以下の情報は、 ROSA および の使用時に発生する可能性がある一般的な問題の診断と修復に役立ちます IAM。

AWS Organizations サービスコントロールポリシーが必要な AWS Marketplace アクセス許可を拒否する

有効にしようとしたときに、 AWS Organizations サービスコントロールポリシー (SCP) で必要な AWS Marketplace サブスクリプションアクセス許可が許可されていない場合 ROSA、次のコンソールエラーが発生します。

```
An error occurred while enabling ROSA, because a service control policy (SCP) is
 denying required permissions. Contact your management account administrator, and
 consult the documentation for troubleshooting.
```

このエラーが表示された場合は、管理者に連絡してサポートを依頼する必要があります。管理者は、組織のアカウントを管理するユーザーです。そのユーザーに以下を行うよう依頼します。

1. aws-marketplace:Subscribe、、aws-marketplace:Unsubscribeおよび アクセスaws-marketplace:ViewSubscriptions許可を許可するように SCP を設定します。詳細については、「 AWS Organizations ユーザーガイド」の「SCP の更新」を参照してください。
2. 組織の管理アカウント ROSA で を有効にします。
3. 組織内のアクセスを必要とするメンバーアカウントに ROSA サブスクリプションを共有します。詳細については、「 AWS Marketplace 購入者ガイド」の「組織でのサブスクリプションの共有」を参照してください。

ユーザーまたはロールに必要な AWS Marketplace アクセス許可がない

有効にしようとしたときにプリン IAM シパルに必要な AWS Marketplace サブスクリプションアクセス許可がない場合 ROSA、次のコンソールエラーが発生します。

```
An error occurred while enabling ROSA, because your user or role does not have the
 required permissions.
```

この問題を解決するには、以下の手順を実行します。

1. IAM コンソールに移動し、 AWS 管理ポリシーを IAM ID ROSAManageSubscriptionにアタッチします。詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAManageSubscription」を参照してください。
2. 「the section called “AWS 前提条件の有効化 ROSA と設定”」の手順に従います。

でアクセス許可セットを表示または更新するアクセス許可がない場合 IAM 、または エラーが表示された場合は、管理者に連絡してサポートを依頼する必要があります。ID ROSAManageSubscription にアタッチ IAM し、「」の手順に従ってくださいthe section called “AWS 前提条件の有効化 ROSA と設定”。管理者がこのアクションを実行すると、 のすべての ID IAM のアクセス許可セットを更新 ROSA することで が有効になります AWS アカウント。

管理者によってブロックされた必要な AWS Marketplace アクセス許可

アカウント管理者が必要な AWS Marketplace サブスクリプションアクセス許可をブロックした場合、 を有効にしようとすると次のコンソールエラーが発生します ROSA。

```
An error occurred while enabling ROSA because required permissions have been blocked by
 an administrator. ROSAManageSubscription includes the permissions required to enable
 ROSA. Consult the documentation and try again.
```

このエラーが表示された場合は、管理者に連絡してサポートを依頼する必要があります。そのユーザーに以下を行うよう依頼します。

1. ROSA コンソールに移動し、 AWS 管理ポリシーを IAM ID ROSAManageSubscriptionにアタッチします。詳細については、「 AWS マネージドポリシーリファレンスガイド」のROSAManageSubscription」を参照してください。
2. の手順に従って the section called “AWS 前提条件の有効化 ROSA と設定”を有効にします ROSA。この手順では、 のすべての ID IAM のアクセス許可セットを更新 ROSA することで を有効にします AWS アカウント。

ロードバランサーの作成中にエラーが発生しました: AccessDenied

ロードバランサーを作成していない場合、AWSServiceRoleForElasticLoadBalacingサービスにリンクされたロールがアカウントに存在していない可能性があります。アカウントにAWSServiceRoleForElasticLoadBalacingロール クラスター なしで ROSA を作成しようとすると、次のエラーが発生します。

```
Error creating network Load Balancer: AccessDenied
```

この問題を解決するには、以下の手順を実行します。

1. アカウントに AWSServiceRoleForElasticLoadBalancing ロールがあるかどうかを確認してください。

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

2. このロールがない場合は、「 Elastic Load Balancing ユーザーガイド」の「サービスにリンクされたロールを作成する」にあるロールを作成する手順に従ってください。

の耐障害性 ROSA

AWS グローバルインフラストラクチャのレジリエンス

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。複数の物理的に分離および分離されたアベイラビリティーゾーン AWS リージョン は、低レイテンシー、高スループット、高度に冗長なネットワークを介して接続されます。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェールオーバーするアプリ

ケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、フォールトトレランス、および拡張性が優れています。

ROSA では、Kubernetes コントロールプレーンとデータプレーンを 1 つの AWS アベイラビリティーゾーンで実行するか、複数のアベイラビリティーゾーンで実行するかを選択できます。シングル AZ クラスターは実験には役立ちますが、複数のアベイラビリティーゾーンでワークロードを実行することをお勧めします。これにより、アベイラビリティーゾーン全体に障害が発生しても (ただし、それは非常に稀なことです)、アプリケーションは障害に耐えることができます。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「グローバルインフラストラクチャ」を参照してください。

ROSA クラスターの耐障害性

ROSA コントロールプレーンは、少なくとも 3 つの OpenShift コントロールプレーンノードで構成されます。各コントロールプレーンノードは API サーバーインスタンス、`etcd` インスタンス、コントローラーで構成されます。コントロールプレーンノードに障害が発生した場合、すべての API リクエストは利用可能な他のノードに自動的にルーティングされ、クラスターの可用性が確保されます。

ROSA データプレーンは、少なくとも 2 つの OpenShift インフラストラクチャノードと 2 つの OpenShift ワーカーノードで構成されます。インフラストラクチャノードは、デフォルトルーター、ビルトイン OpenShift レジストリ、クラスターメトリクスとモニタリング用のコンポーネントなどの OpenShift クラスターインフラストラクチャコンポーネントをサポートするポッドを実行します。OpenShift ワーカーノードはエンドユーザーアプリケーションポッドを実行します。

Red Hat サイト信頼性エンジニアリング (SRE) がコントロールプレーンとインフラストラクチャノードを完全に管理します。Red Hat SREsは ROSA クラスターをプロアクティブにモニタリングし、障害が発生したコントロールプレーンノードとインフラストラクチャノードを置き換えます。詳細については、「the section called “責任”」を参照してください。

> **Important**
>
> ROSA はマネージドサービスであるため、Red Hat は が ROSA 使用する基盤となる AWS インフラストラクチャの管理を担当します。お客様は、 AWS コンソールまたは から が ROSA 使用する Amazon EC2 インスタンスを手動でシャットダウンしようとしないでください AWS CLI。そうすると、顧客データが失われる可能性があります。

データプレーンでワーカーノードに障害が発生した場合、コントロールプレーンは、障害が発生したノードが復旧または交換されるまで、未スケジュールのポッドを機能しているワーカーノードに再配置します。障害が発生したワーカーノードは、手動で交換することも、クラスター内のマシンの自動スケーリングを有効にすることで自動的に交換することもできます。詳細については、Red Hat ドキュメントの「クラスターの自動スケーリング」を参照してください。

お客様がデプロイしたアプリケーションの耐障害性

ROSA は、サービスの高可用性を確保するために多くの保護を提供しますが、お客様は、ワークロードをダウンタイムから保護するために、高可用性のためにデプロイされたアプリケーションを構築する責任があります。詳細については、Red Hat ドキュメントの「ROSAの可用性」を参照してください。

のインフラストラクチャセキュリティ ROSA

マネージドサービスである Red Hat OpenShift Service on AWS は、 AWS グローバルネットワークセキュリティによって保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「Security Pillar — AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS が発行した API コールを使用して、 AWS ネットワーク ROSA 経由で にアクセスします。クライアントは次をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

クラスターネットワークの分離

Red Hat サイト信頼性エンジニアリング (SRE) は、クラスターと基盤となるアプリケーションプラットフォームの継続的な管理とネットワークセキュリティに責任を負います。Red Hat の責任の詳細については ROSA、「」を参照してくださいthe section called “責任”。

新しいクラスターを作成すると、 はパブリック Kubernetes API サーバーエンドポイントとアプリケーションルート、またはプライベート Kubernetes API エンドポイントとアプリケーションルートを作成するオプション ROSA を提供します。この接続は、(ROSA CLI や OpenShift CLI などの OpenShift 管理ツールを使用して) クラスターとの通信に使用されます。プライベート接続により、ノードと API サーバー間のすべての通信が VPC 内で行われるようにできます。API サーバーとアプリケーションルートへのプライベートアクセスを有効にする場合は、既存の VPC と AWS PrivateLink を使用して、VPC を OpenShift バックエンドサービスに接続する必要があります。

Kubernetes API サーバーへのアクセスは、 AWS Identity and Access Management (IAM) とネイティブ Kubernetes ロールベースのアクセスコントロール (RBAC) の組み合わせを使用して保護されます。Kubernetes RBAC の詳細については、Kubernetes ドキュメントの「RBAC 認可の使用」を参照してください。

ROSA では、複数のタイプの TLS 終了を使用して保護されたアプリケーションルートを作成し、クライアントに証明書を提供できます。詳細については、Red Hat ドキュメントの「保護されたルート」を参照してください。

既存の VPC に ROSA クラスターを作成する場合は、クラスターで使用する VPC サブネットとアベイラビリティーゾーンを指定します。また、使用するクラスターネットワークの CIDR 範囲を定義し、これらの CIDR 範囲を VPC サブネットと一致させます。詳細については、Red Hat ドキュメントの「CIDR 範囲の定義」を参照してください。

パブリック API エンドポイントを使用するクラスターの場合、 はクラスターをデプロイする各アベイラビリティーゾーンのパブリックサブネットとプライベートサブネットを VPC に設定 ROSA する必要があります。プライベート API エンドポイントを使用するクラスターでは、プライベートサブネットのみが必要です。

既存の VPC を使用している場合は、 ROSA クラスターの作成中または作成後に HTTP または HTTPS プロキシサーバーを使用してクラスターウェブトラフィックを暗号化するようにクラスターを設定し、データに別のセキュリティレイヤーを追加できます。プロキシを有効にすると、コアクラスターコンポーネントはインターネットへの直接アクセスが拒否されます。プロキシはユーザーワークロードのインターネットアクセスを拒否しません。詳しくは、Red Hat ドキュメントの「クラスター全体のプロキシーの設定」を参照してください。

ポッドネットワークの隔離

クラスター管理者の場合は、 ROSA クラスター内のポッドへのトラフィックを制限するネットワークポリシーをポッドレベルで定義できます。

ROSA サービスクォータ

Red Hat OpenShift Service on AWS (ROSA) は Amazon EC2、、 Amazon Virtual Private Cloud Amazon Elastic Block Store、 のサービスクォータ Elastic Load Balancing を使用してクラスターをプロビジョニングします。詳細については、「 AWS 全般のリファレンスガイド」のRed Hat OpenShift Service on AWS 「エンドポイントとクォータ」を参照してください。

AWS と統合された サービス ROSA

ROSA は他の と連携して AWS のサービス 、ビジネス上の課題に対する追加のソリューションを提供します。このトピックでは、 が機能の追加 ROSA に使用するサービス、または がタスクの実行 ROSA に使用するサービスを識別します。

トピック

- での ROSA の仕組み AWS Marketplace

での ROSA の仕組み AWS Marketplace

AWS Marketplace は、ソリューションを構築してビジネスを実行するために必要なサードパーティーのソフトウェア、データ、サービスを検索、購入、デプロイ、管理するために使用できる厳選されたデジタルカタログです。 AWS Marketplace は、柔軟な料金オプションと複数のデプロイ方法を使用して、ソフトウェアのライセンスと調達を簡素化します。

ROSA は、サービスの計測と請求 AWS Marketplace に を使用します。ROSA Classic は AWS Marketplace Amazon Machine Image (AMI) ベースの製品を通じて計測および請求されますが、ホストされたコントロールプレーン (HCP) を備えた ROSA は AWS Marketplace Software as a Service (SaaS) ベースの製品を通じて計測および請求されます。

このページでは、 での支払い、請求、サブスクリプション、契約購入 AWS Marketplace がどのように ROSA 機能するかについて説明します。

用語

このページでは、ROSA と の統合について説明するときに、次の用語を使用します AWS Marketplace。

[Amazon マシンイメージ (AMI)]

AWS上で動作するオペレーティングシステムや追加のソフトウェアを含むサーバーのイメージ。

AMI サブスクリプション

では AWS Marketplace、ROSA Classic などの AMI ベースのソフトウェア製品は、年間サブスクリプション料金モデルで 1 時間ごとに を使用します。時間単位の料金はデフォルトの料金モデルですが、1 つの Amazon EC2 インスタンスタイプに対して 1 年分の使用量を前払いで購入することもできます。

SaaS サブスクリプション

では AWS Marketplace、ROSA with HCP などの software-as-a-service (SaaS) 製品は、使用量ベースのサブスクリプションモデルを採用しています。SaaS サブスクリプションにおいて、ソフトウェア販売者が使用量を確認し、ユーザーは使用した分の料金だけを支払います。

パブリックオファー

パブリックオファーを使用すると、 から直接 AWS Marketplace ソフトウェアとサービスを購入できます AWS Management Console。

プライベートオファー

プライベートオファーは、販売者と購入者が での購入に関するカスタム価格とエンドユーザーライセンス契約 (EULA) の条件を交渉できるようにする購入プログラムです AWS Marketplace。

ROSA サービス料

Red Hat サイト信頼性エンジニア (SREs) による OpenShift ソフトウェアとクラスター管理に対して ROSA 課金される料金。 ROSA サービス料金は、 を通じて計測 AWS Marketplace され、AWS 請求書に表示されます。

AWS インフラ料金

および Amazon EC2を含む、 AWS のサービス 基盤となる ROSA クラスターに対して AWS 課金される標準料金 Amazon EBS Amazon S3 Elastic Load Balancing。料金は AWS のサービス 、使用されている を通じて計測され、 AWS 請求書に表示されます。

ROSA 支払いと請求

ROSA は と統合 AWS Marketplace して、 ROSA サービス料金の計測と請求を有効にします。ROSA サービス料金は、Red Hat サイト信頼性エンジニア (SRE) による OpenShift ソフトウェアとクラスター管理へのアクセスを対象としています。 ROSA サービス料金は、サポートされているすべての AWS 標準リージョンで統一されています。 SREs ROSA with HCP サービス料金は、デフォルトでは、実行中のクラスターとそれらのクラスターで実行されているワーカーノード vCPU 数に基づき、1 時間当たりの定額料金でオンデマンドで発生します。ROSA Classic のサービス料金は、ワーカーノード vCPU 数に基づいてオンデマンドで発生します。ROSA Classic では、コントロールプレーンや必要なインフラストラクチャーノードのサービス料は請求されません。

ROSA のお客様は、 AWS のサービス 基盤となる ROSA クラスターの標準 AWS インフラストラクチャ料金も支払います Elastic Load Balancing。これには Amazon EC2 Amazon EBS Amazon S3、および AWS が含まれます。インフラストラクチャ料金は、従量制 ROSA のサービス料金とは別

の請求項目です AWS Marketplace。 AWS インフラストラクチャ料金は によって異なり AWS リージョン 、デフォルトで時間単位の使用に基づいています。 AWS インフラストラクチャのコストをさらに削減するために、 Amazon EC2 削減計画またはリザーブドインスタンスを購入できます。詳細については、Compute Savings Plans」および「リザーブドインスタンス」を参照してください。 Amazon EC2

ROSA は、 ROSA クラスターを作成するか、 ROSA 契約を購入するまで料金を請求しません。詳細については、Red Hat OpenShift Service on AWS 料金表を参照してください。

ROSA サービス料金と AWS インフラストラクチャ料金を表示し、 AWS Billing コンソールで支払いを管理できます。また、 AWS Cost Explorer Service インターフェイスを使用してコストを表示したり、使用量をモニタリングしたりすることもできます。詳細については、「 AWS Billing and Cost Management ユーザーガイド」の「請求の表示」および「 コスト管理ユーザーガイド」の「 を使用したコストの分析 AWS Cost Explorer Service」を参照してください。 AWS

コンソールから ROSA Marketplace 出品にサブスクライブする

ROSA コンソール ROSA で を有効にすると、 AWS アカウント は ROSA Classic と ROSA with HCP 出品にサブスクライブされます AWS Marketplace。 ROSA サブスクリプションの有効化には料金はかかりません。

AWS Organizations ユーザーの場合、 ROSA では ROSA Classic サブスクリプションを組織内の他のアカウントと共有できます。詳細については、「 AWS Marketplace 購入者ガイド」の「組織内のサブスクリプションの共有」を参照してください。

ROSA 契約の購入

ROSA は AWS Marketplace を使用して、HCP および ROSA Classic との ROSA のオプション契約を提供します。契約により、 ROSA ワーカーノードサービス料金を節約できます。 ROSA 契約は、AWS インフラストラクチャに対して請求される料金には影響しません。

12 か月契約

ROSA Classic および ROSA with HCP の 12 か月間の公開オファー契約は、 ROSA コンソールから購入できます。

> **Note**
>
> コンソールから 12 か月契約を購入する前に、ROSA Classic をアカウント内で有効にする必要があります。

> **Note**
>
> 12 か月契約は、プライベートオファーに移行することができません。

ROSA Classic の 12 か月契約を購入する

ROSA Classic の 12 か月契約をご購入いただいた場合、年間契約期間の前払いが発生し、その後12ヶ月間、対象となるインスタンスに対する時間単位のサービス料は無料となります。契約コストは、選択した Amazon EC2 インスタンスタイプとインスタンス数に基づきます。この契約は、使用されている基盤となる に対して ROSA 課金 AWS のサービス される AWS インフラストラクチャ料金には適用されません。詳細については、「Red Hat OpenShift Service on AWS 料金」を参照してください。

契約は、契約を作成する際に指定したインスタンスタイプ (m5.xlarge など) のみを対象としています。複数の Amazon EC2 インスタンスタイプでコスト削減のために、追加の 12 か月契約を購入できます。12 か月契約以外の使用には、オンデマンド料金で ROSA サービス料金が発生します。

> **Note**
>
> ROSA Classic の 12 か月契約は 自動で更新されません。

ROSA Classic の 12 か月契約を購入するには

> **Note**
>
> HCP で ROSA をまだサポートしていないリージョンで ROSA コンソールを使用している場合、このワークフローはまだ使用できません。HCP で ROSA をサポートするリージョンのリストについては、「」を参照してくださいthe section called “ROSA と HCP および ROSA Classic の比較”。
> ROSA を導入していない地域で HCP サポート付きの ROSA Classic 契約を購入するには、ROSA コンソールに移動して [ソフトウェア契約の購入と既存の契約の確認] を選択してください。

1. [ROSA コンソール] に移動します。
2. 左のナビゲーションペインで、[契約] を選択します。

3. [ROSA Classic の契約] を選択してください。
4. [契約の購入] を選択します。
5. EC2 インスタンスタイプを選択し、必要なインスタンスの数を入力します。
6. [契約書を確認] を選択します。
7. 契約の詳細を確認し、[契約の購入] を選択します。

> **Note**
>
> ROSA 12 か月契約は、 コンソールを使用して作成後にダウングレードまたはキャンセルすることはできません。契約期間がまだ有効な内に、契約をダウングレードまたはキャンセルする必要がある場合は、サポート センターにアクセスしてサポートケースをオープンしてください。

ROSA Classic with HCP の 12 か月契約を購入する

コンソールで ROSA with HCP を有効にすると、オンデマンド課金を容易にするため、最初に 12 か月間の無料の ROSA with HCP 契約がアカウントに作成されます。ワーカーノードのサービス料金を節約するために ROSA with HCP 契約を購入した場合、最初の契約は、指定したワーカーノード vCPU とコントロールプレーンの使用コストをカバーするように変更されます。

ROSA with HCP の 12 か月契約をご購入いただいた場合、年間契約期間の前払いが発生し、その後 12 か月間、対象となるワーカーノード vCPU とコントロールプレーンの時間単位の使用料は無料となります。契約コストは、選んだワーカーノード vCPU とコントロールプレーンの数に基づいています。契約は、契約作成時に指定したワーカーノード vCPU とコントロールプレーンのみを対象としています。契約は、使用されている基盤となる に対して ROSA 課金 AWS のサービス される AWS インフラストラクチャ料金には適用されません。詳細については、「Red Hat OpenShift Service on AWS 料金」を参照してください。

月額使用可能料

購入時に、プリペイド vCPU とコントロールプレーンは毎月使用可能量に変換されます。vCPU とコントロールプレーンの使用量が毎月の使用可能量を超えると、時間単位のオンデマンド利用料金が適用されます。ROSA with HCP では、以下の計算式を使用して契約に関連する毎月の使用可能量を掲載しています:

- ワーカーノード vCPU: vCPU の数 x 24 時間 x 365 日/ 12 か月

- コントロールプレーン: コントロールプレーンの数 x 24 時間 x 365 日/ 12 か月

例えば、4,000 個のワーカーノード vCPUs と 8 個のコントロールプレーンを購入すると、1 か月あたり 2,920,000 時間のワーカーノード vCPU 時間と 5,840 個のコントロールプレーン時間のクォータに変換されます。

ROSA Classic with HCP の 12 か月契約を購入するには

> **Note**
>
> ホストされたコントロールプレーンで ROSA をまだサポートしていないリージョンで Red Hat OpenShift Service on AWS コンソールを使用している場合、このワークフローはまだ使用できません。HCP で ROSA をサポートするリージョンのリストについては、「」を参照してくださいthe section called “ROSA と HCP および ROSA Classic の比較”。

1. [ROSA コンソール] に移動します。
2. 左のナビゲーションペインで、[契約] を選択します。
3. [ROSA with HCP の契約] を選択してください。
4. [契約の購入] を選択します。
5. 購入する vCPU の数を入力します。4 の倍数で指定してください。
6. 購入するコントロールプレーンの数を入力します。
7. [契約書を確認] を選択します。
8. 契約の詳細を確認し、[契約の購入] を選択します。

> **Note**
>
> ROSA 12 か月契約は、 コンソールを使用して作成後にダウングレードまたはキャンセルすることはできません。契約期間がまだ有効な内に、契約をダウングレードまたはキャンセルする必要がある場合は、サポート センターにアクセスしてサポートケースをオープンしてください。

ROSA with HCP 12 か月契約のアップグレード

有効な ROSA with HCP 12 か月契約は、ワーカーノードの vCPU とコントロールプレーンを追加して、いつでもアップグレードできます。ROSA with HCP の 12 か月契約をアップグレードする場合、追加リソースに対しては、日割り計算による前払いを行います。前払い料金は、残りの契約日数に基づいて計算されます。契約は、契約作成時に指定したワーカーノード vCPU とコントロールプレーンのみを対象としています。契約のアップグレードは、 AWS インフラストラクチャに対して請求される料金には影響しません。

アップグレード時に、追加された vCPU とコントロールプレーンは、元の契約購入時と同じ計算式を使用して月間使用可能量に変換されます。vCPU とコントロールプレーンの使用量が毎月の使用可能量を超えると、時間単位のオンデマンド利用料金が適用されます。詳細については、「the section called “月額使用可能料”」を参照してください。

ROSA with HCP 12 か月契約のアップグレードをするには

1. [ROSA コンソール] に移動します。
2. 左のナビゲーションペインで、[契約] を選択します。
3. [ROSA with HCP の契約] を選択してください。
4. [アップグレード] を選択します。
5. 購入する vCPU の数を入力します。4 の倍数で指定してください。
6. 契約に追加するコントロールプレーンの数を入力します。
7. [アップグレードを確認] を選択します。
8. 契約の詳細を確認し、[契約の購入] を選択します。

> **Note**
>
> ROSA Classicの 12 か月契約はアップグレードできません。追加の 12 か月間 ROSA クラシック契約は、 ROSA コンソールを使用していつでも購入できます。

プライベートオファーを受ける方法について

ROSA with HCP または ROSA Classic の AWS Marketplace プライベートオファーをリクエストして、Red Hat と交渉された製品料金とエンドユーザーライセンス契約 (EULA) 条件を受け取ることができます。詳細については、「 AWS Marketplace 購入者ガイド」の「プライベートオファー」を参照してください。

ROSA プライベートオファーを取得するには

> **Note**
>
> ユーザーで AWS Organizations 、支払者アカウントとメンバーアカウントに発行されたプライベートオファーを受け取った場合は、以下の手順に従って、組織内の各アカウントで ROSA に直接サブスクライブします。
> AWS Organizations 支払者アカウントに対してのみ発行された ROSA クラシックプライベートオファーを受け取った場合は、組織内のメンバーアカウントとサブスクリプションを共有する必要があります。詳細については、「 AWS Marketplace 購入者ガイド」の「組織でのサブスクリプションの共有」を参照してください。

1. プライベートオファーが発行されたら、AWS Marketplace コンソールにサインインします。
2. ROSA プライベートオファーリンクを使用して E メールを開きます。
3. リンクに従い、プライベートオファーに直接アクセスします。

> **Note**
>
> 正しいアカウントにログインする前にこのリンクをクリックすると、[ページが見つかりません] (404) というエラーが表示されます。

4. 利用規約を読みます。
5. 次に [規約の受諾] を選択します。

> **Note**
>
> AWS Marketplace プライベートオファーが受け入れられない場合、 のサービス ROSA 料金は引き続きパブリック時間料金で請求 AWS Marketplace されます。

6. オファーの詳細を確認するには、製品リストの [詳細を表示] を選択します。
7. の使用を開始するには ROSA、「設定に進む」を選択します。 ROSA コンソールにリダイレクトされます。

Private Marketplace

Private Marketplace を使用すると、管理者は承認済み製品のカスタマイズされたデジタルカタログを から構築できます AWS Marketplace。管理者は、 で AWS 組織単位 AWS Marketplace 用に利用できる、または組織 AWS アカウント 内で購入できる、検証済みのソフトウェアの一意のセットを作成できます。

組織がプライベートマーケットプレイスを使用している場合、管理者はユーザーがサービスを有効にする前に、 AWS Marketplace のリスト ROSA をプライベートマーケットプレイスに追加する必要があります。詳細については、「 購入者ガイド」の「プライベートマーケットプレイスの開始方法」を参照してください。 AWS Marketplace

トラブルシューティング

次のページでは、 ROSA クラスターの作成または管理中に発生する一般的な問題について詳しく説明します。

トピック

ROSA クラスターのデバッグログにアクセスする

アプリケーションに関する問題のトラブルシューティングを開始するには、まずデバッグログを確認してください。 ROSA CLI デバッグログは、 の作成に クラスター 失敗したときに生成されるエラーメッセージの詳細を提供します。

クラスター デバッグ情報を表示するには、次の ROSA CLI コマンドを実行します。コマンドで、 をの名前<cluster_name>に置き換えます クラスター。

```
rosa describe cluster -c <cluster_name> --debug
```

ROSA クラスター クラスター が作成中に AWS サービスクォータチェックに失敗する

を使用するには ROSA、アカウントのサービスクォータを増やす必要がある場合があります。詳細については、「Red Hat OpenShift Service on AWS エンドポイントとクォータ」を参照してください。

1. 次のコマンドを実行して、アカウントのクォータを確認します。

```
rosa verify quota
```

> **Note**
>
> クォータは AWS リージョンによって異なります。お使いのリージョンの各クォータを必ず確認してください。

2. クォータを増やす必要がある場合は、Service Quotas コンソールに移動します。
3. ナビゲーションペインで、 AWS サービスを選択します。
4. クォータを増やす必要があるサービスを選択してください。
5. 増やす必要があるクォータを選択し、[クォータの引き上げをリクエストする] を選択します。
6. [クォータの引き上げをリクエストする] に希望するクォータの合計を入力し、[リクエスト] を選択します。

CLI ROSA の有効期限が切れたオフラインアクセストークンのトラブルシューティング

ROSA CLI を使用していて、api.openshift.com オフラインアクセストークンの有効期限が切れると、エラーメッセージが表示されます。これは sso.redhat.com でトークンが無効になったときに発生します。

1. OpenShift Cluster Manager API トークンページに移動し、[トークンをロードする] を選択します。
2. ターミナルに次の認証コマンドをコピーして貼り付けます。

```
rosa login --token="<api_token>"
```

osdCcsAdmin エラー クラスター で を作成できませんでした

> **Note**
>
> このエラーは、非 STS メソッドを使用して ROSA クラスターをプロビジョニングする場合にのみ発生します。この問題を回避するには、 を使用して ROSA クラスターをプロビジョニングします AWS STS。詳細については、「the section called “ROSA クラシッククラスターの作成 - CLI”」を参照してください。

の作成に クラスター 失敗すると、次のエラーメッセージが表示されることがあります。

```
Failed to create cluster: Unable to create cluster spec: Failed to get access keys for
 user 'osdCcsAdmin': NoSuchEntity: The user with name osdCcsAdmin cannot be found.
```

1. スタックを削除します。

```
rosa init --delete-stack
```

2. アカウントを再初期化します。

```
rosa init
```

次の手順

- OpenShift のドキュメントを参照してください。
- サポート ケースまたは Red Hat サポートケースを開きます。
- に関するよくある質問への回答を見つけます Red Hat OpenShift Service on AWS。
- ROSA のサポートモデルの詳細については、「」を参照してくださいthe section called “サポート情報”。

ROSA サポートを受ける

を使用すると ROSA、 サポート および Red Hat サポートチームからサポートを受けることができます。サポートケースはどちらの組織でも開設できます。問題解決のため、適切なチームに転送されます。

サポート ケースを開く

ROSA 技術ケースを開くには AWS デベロッパーサポートプランが必要ですが、 ROSA 技術サポートとアーキテクチャガイダンスへの継続的なアクセスには、 AWS ビジネス、エンタープライズ、またはエンタープライズのオンランプサポートプランをお勧めします。Red Hat は サポート API を使用して、必要に応じてお客様のケースを開きます。 AWS ビジネス、エンタープライズ、エンタープライズのオンランプサポートプランにより、サポートエンジニアが電話、ウェブ、チャットに継続的にアクセスできるようになります。 サポート プランの詳細については、「」を参照してくださいサポート。

サポート プランを有効にする手順については、サポート「プランにサインアップするにはどうすればよいですか？」を参照してください。

サポート ケースの作成の詳細については、「サポートケースの作成」と「ケース管理」を参照してください。

Red Hat サポートケースを開く

ROSA には Red Hat プレミアムサポートが含まれています。Red Hat Premium サポートを受けるには、Red Hat カスタマーポータルに移動し、サポートケースツールを使用してサポートチケットを作成します。詳細は、「Red Hat サポートの利用方法」を参照してください。

ドキュメント履歴

以下の表は のドキュメントの重要な変更点をまとめたものです。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

変更	説明	日付
ROSAControlPlaneOperatorPolicy を更新	AWS マネージドポリシー ROSAControlPlaneOperatorPolicy を更新して、適切なリソースライフサイクル管理のために Red Hat が管理するセキュリティグループのタグ付けを許可し、Security-group/* を ManageVPCEndpointWithCondition に追加して、クラスターのアップグレード中の VPCE 調整の失敗を修正しました。詳細については、「ROSAAWS 管理ポリシーの更新」を参照してください。	2026 年 4 月 9 日
ROSAKubeControllerPolicy の更新	AWS マネージドポリシー ROSAKubeControllerPolicy を更新し、ターゲットグループでターゲットを登録および登録解除するための Elastic Load Balancing アクセス許可を明確にしました。詳細については、「ROSAAWS 管理ポリシーの更新」を参照してください。	2026 年 3 月 5 日
ROSANodePoolManagementPolicy を更新	ROSA は、 マネージドポリシーを更新ROSANodePoolManagementPolic	2025 年 9 月 3 日

	y して、キャパシティ予約機能をサポートするキャパシティ予約のリソースアクセスを追加しました。詳細については、「ROSAAWS 管理ポリシーの更新」を参照してください。	
ROSAInstallerPolicy の更新	AWS マネージドポリシー ROSAInstallerPolicy を更新して、ROSA の新しいキャパシティ予約機能をサポートし、Kubernetes クラスタータグ管理を改善しました。詳細については、「ROSAAWS 管理ポリシーの更新」を参照してください。	2025 年 8 月 7 日
新しい ROSASharedVPCRoute53Policy	ROSA は、ROSA インストーラが共有 VPC 環境で Route 53 レコードを設定`ROSASharedVPCRoute53Policy` できるようにする新しい マネージドポリシーをリリースしました。詳細については、「ROSAAWS 管理ポリシーの更新」を参照してください。	2025 年 8 月 7 日

新しい ROSASharedVPCEndpointPolicy	ROSA は、ROSA インストーラが共有 VPC 環境で VPC エンドポイントとセキュリティグループを設定できるようにする新しい マネージドポリシー`ROSASharedVPCEndpointPolicy` をリリースしました。このポリシーは、共有 VPC ユースケースに合わせた EC2 アクセス許可のサブセットを提供します。詳細については、「ROSAAWS 管理ポリシーの更新」を参照してください。	2025 年 8 月 7 日
ROSAImageRegistryOperatorPolicy を更新	AWS 管理ポリシー ROSAImageRegistryOperatorPolicy を更新しました。	2025 年 5 月 19 日
ROSANodePoolManagementPolicy を更新	AWS 管理ポリシー ROSANodePoolManagementPolicy を更新しました。	2025 年 5 月 5 日
ROSAImageRegistryOperatorPolicy を更新	AWS 管理ポリシー ROSAImageRegistryOperatorPolicy を更新しました。	2025 年 4 月 16 日
ROSAWorkerInstancePolicy を更新	AWS 管理ポリシー ROSAWorkerInstancePolicy を更新しました。	2025 年 3 月 3 日
ROSANodePoolManagementPolicy を更新	AWS 管理ポリシー ROSANodePoolManagementPolicy を更新しました。	2025 年 2 月 24 日

ROSAAmazonEBSCSIDriverOperatorPolicy を更新	AWS 管理ポリシー ROSAAmazonEBSCSIDriverOperatorPolicy を更新しました。	2025 年 1 月 17 日
HCP AWS リージョン 拡張による ROSA	ホスト型コントロールプレーン (HCP) を備えた ROSA が中東 (UAE) で利用可能になりました AWS リージョン。	2024 年 5 月 13 日
HCP AWS リージョン 拡張による ROSA	ホスト型コントロールプレーン (HCP) を備えた ROSA が欧州 (パリ) で利用可能になりました AWS リージョン。	2024 年 5 月 6 日
ROSANodePoolManagementPolicy を更新	AWS 管理ポリシー ROSANodePoolManagementPolicy を更新しました。	2024 年 5 月 2 日
HCP による ROSA AWS リージョン の拡張	ホスト型コントロールプレーン (HCP) を備えた ROSA が欧州 (スペイン) で利用可能になりました AWS リージョン。	2024 年 4 月 29 日
ROSAInstallerPolicy の更新	AWS 管理ポリシー ROSAInstallerPolicy を更新しました。	2024 年 4 月 24 日
HCP による ROSA AWS リージョン の拡張	ホスト型コントロールプレーン (HCP) を備えた ROSA が欧州 (チューリッヒ) で利用可能になりました AWS リージョン。	2024 年 4 月 19 日

HCP による ROSA AWS リージョン の拡張	ホスト型コントロールプレーン (HCP) を備えた ROSA が、アジアパシフィック (大阪) で利用可能になりました AWS リージョン。	2024 年 4 月 17 日
ROSAInstallerPolicy と ROSASRESupportPolicy を更新	AWS 管理ポリシー ROSAInstallerPolicy と ROSASRESupportPolicy を更新しました。	2024 年 4 月 10 日
HCP による ROSA AWS リージョン の拡張	ホスト型コントロールプレーン (HCP) を備えた ROSA が、アジアパシフィック (香港) で利用可能になりました AWS リージョン。	2024 年 4 月 8 日
HCP による ROSA AWS リージョン の拡張	ホスト型コントロールプレーン (HCP) を備えた ROSA が南米 (サンパウロ) で利用可能になりました AWS リージョン。	2024 年 4 月 1 日
HCP による ROSA AWS リージョン の拡張	ホスト型コントロールプレーン (HCP) を備えた ROSA が中東 (バーレーン) で利用可能になりました AWS リージョン。	2024 年 3 月 25 日
HCP による ROSA AWS リージョン の拡張	ホスト型コントロールプレーン (HCP) を備えた ROSA が、アジアパシフィック (ソウル) で利用可能になりました AWS リージョン。	2024 年 3 月 14 日

HCP による ROSA AWS リージョン の拡張	ホスト型コントロールプレーン (HCP) を備えた ROSA がアフリカ (ケープタウン) で利用可能になりました AWS リージョン。	2024 年 3 月 5 日
ROSAInstallerPolicy の更新	AWS 管理ポリシー ROSAInstallerPolicy を更新しました。	2024 年 1 月 26 日
ROSASRESupportPolicy の更新	AWS 管理ポリシー ROSASRESupportPolicy を更新しました。	2024 年 1 月 22 日
ROSAImageRegistryOperatorPolicy を更新	AWS 管理ポリシー ROSAImageRegistryOperatorPolicy を更新しました。	2023 年 12 月 12 日
ROSAKubeControllerPolicy の更新	AWS 管理ポリシー ROSAKubeControllerPolicy を更新しました。	2023 年 10 月 16 日
ROSAManageSubscription の更新	AWS 管理ポリシー ROSAManageSubscription を更新しました。	2023 年 8 月 1 日
ROSAKubeControllerPolicy の更新	AWS 管理ポリシー ROSAKubeControllerPolicy を更新しました。	2023 年 7 月 13 日
ROSA セキュリティページの追加	「ROSA のレジリエンス」、「ROSA のインフラストラクチャセキュリティ」、「ROSA のデータ保護」ページが追加されました。	2023 年 6 月 30 日

「デプロイオプション」ページの追加	「デプロイオプション」ページが追加されました。	2023 年 6 月 9 日
新しい AWS 管理ポリシー ROSANodePoolManagementPolicy を追加	新しい AWS 管理ポリシー ROSANodePoolManagementPolicy が追加されました。	2023 年 6 月 8 日
新しい AWS 管理ポリシー ROSAInstallerPolicy を追加	新しい AWS 管理ポリシー ROSAInstallerPolicy が追加されました。	2023 年 6 月 6 日
新しい AWS 管理ポリシー ROSASRESupportPolicy を追加	新しい AWS 管理ポリシー ROSASRESupportPolicy が追加されました。	2023 年 6 月 1 日
ROSA の責任の概要の追加	ROSA の責任の概要が追加されました。	2023 年 5 月 26 日
更新内容 Red Hat OpenShift Service on AWS	What is Red Hat OpenShift Service on AWS ページを更新しました。	2023 年 5 月 24 日
ROSA オペレーターロールの新しい AWS 管理ポリシーを追加	新しい AWS 管理ポリシー ROSAImageRegistryOperatorPolicy、ROSA KubeControllerPolicy、および ROSAKMSProviderPolicy が追加されました。	2023 年 4 月 27 日
新しい AWS 管理ポリシー ROSAControlPlaneOperatorPolicy を追加	新しい AWS 管理ポリシー ROSAControlPlaneOperatorPolicy が追加されました。	2023 年 4 月 24 日

ROSA アカウントロールの新しい AWS 管理ポリシーを追加	ROSA アカウントおよびオペレーターロールページの新しい AWS マネージドポリシーページが追加されました。	2023 年 4 月 20 日
ROSA サービスクォータページの追加	ROSA サービスクォータページが追加されました。	2022 年 12 月 22 日
トラブルシューティングページの追加	トラブルシューティングページが追加されました。	2022 年 11 月 1 日
開始方法ページの追加	開始方法ページが追加されました。	2022 年 8 月 12 日
新しい AWS 管理ポリシー ROSAManageSubscription を追加	新しい AWS 管理ポリシー ROSAManageSubscription が追加されました。	2022 年 4 月 11 日
初回リリース	Red Hat OpenShift Service on AWS ユーザーガイドの初回リリース。	2021 年 3 月 24 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。