aws

ユーザーガイド

Red Hat OpenShift Service on AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。

Table of Contents

とは Red Hat OpenShift Service on AWS 1
機能 1
アクセス ROSA 1
の使用を開始する方法 ROSA 2
料金 3
ROSA サービス料金 3
AWS インフラストラクチャ料金 4
責任 4
概要: 4
地域別の責任分担に関するタスク 6
データとアプリケーションに対するお客様の責任 30
アーキテクチャ 33
ROSA と HCP および ROSA Classic の比較 34
の使用を開始する ROSA 36
セットアップする 36
前提条件 36
AWS 前提条件の有効化 ROSA と設定 37
ROSA HCP クラスターの作成 - CLI 38
前提条件 39
Amazon VPC アーキテクチャの作成 39
必要な IAM ロールと OpenID Connect 設定を作成する 46
CLI と を使用して ROSA with HCP ROSA クラスターを作成する AWS STS 47
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 48
へのアクセスをユーザーに許可する クラスター 50
cluster-admin のアクセス許可を設定します。 51
dedicated-admin のアクセス許可を設定します。 51
Red Hat Hybrid Cloud コンソール クラスター から にアクセスする 51
Developer Catalog からアプリケーションをデプロイする 52
ユーザーから cluster-admin 権限を取り消す 53
ユーザーから dedicated-admin 権限を取り消す 53
へのユーザーアクセスを取り消す クラスター 54
クラスターと AWS STS リソースを削除する 54
ROSA クラシッククラスターの作成 - CLI 55
前提条件 56

CLI と を使用して ROSA Classic ROSA クラスターを作成する AWS STS 56
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 58
へのアクセスをユーザーに許可する クラスター 60
cluster-admin のアクセス許可を設定します。 61
dedicated-admin のアクセス許可を設定します。 61
Red Hat Hybrid Cloud コンソール クラスター から にアクセスする 61
Developer Catalog からアプリケーションをデプロイする 62
ユーザーから cluster-admin 権限を取り消す 63
ユーザーから dedicated-admin 権限を取り消す 63
へのユーザーアクセスを取り消す クラスター 64
クラスターと AWS STS リソースを削除する 64
ROSA Classic クラスターを作成する - AWS PrivateLink 65
前提条件 66
Amazon VPC アーキテクチャを作成する 66
CLI と を使用して ROSA Classic ROSA クラスターを作成する AWS PrivateLink 71
DNS AWS PrivateLink 転送を設定する 73
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 75
へのアクセスをユーザーに許可する クラスター 77
cluster-admin のアクセス許可を設定します。 77
dedicated-admin のアクセス許可を設定します。 77
Red Hat Hybrid Cloud コンソール クラスター から にアクセスする 78
Developer Catalog からアプリケーションをデプロイする 78
ユーザーから cluster-admin 権限を取り消す 79
ユーザーから dedicated-admin 権限を取り消す 80
へのユーザーアクセスを取り消す クラスター 80
クラスターと AWS STS リソースを削除する 80
セキュリティ 82
データ保護 82
データ暗号化 83
ID とアクセス管理 84
オーディエンス 85
アイデンティティを使用した認証 85
ポリシーを使用したアクセスの管理 86
..... 88
..... 104
トラブルシューティング 114

耐障害性 115
..... 115
..... 116
お客様がデプロイしたアプリケーションの耐障害性 116
インフラストラクチャセキュリティ 116
クラスターネットワークの分離 117
ポッドネットワークの隔離 117
サービスクォータ 118
他のサービスでの使用 119
ROSA および AWS Marketplace 119
用語 119
ROSA 支払いと請求 120
コンソールから ROSA Marketplace 出品にサブスクライブする 121
ROSA 契約の購入 121
Private Marketplace 127
トラブルシューティング 128
ROSA クラスターのデバッグログにアクセスする 128
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 128
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 129
osdCcsAdmin エラー クラスター で を作成できませんでした 129
次の手順 130
サポート情報 130
サポート ケースを開く 130
Red Hat サポートケースを開く 131
ドキュメント履歴 132
..... cxlii

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

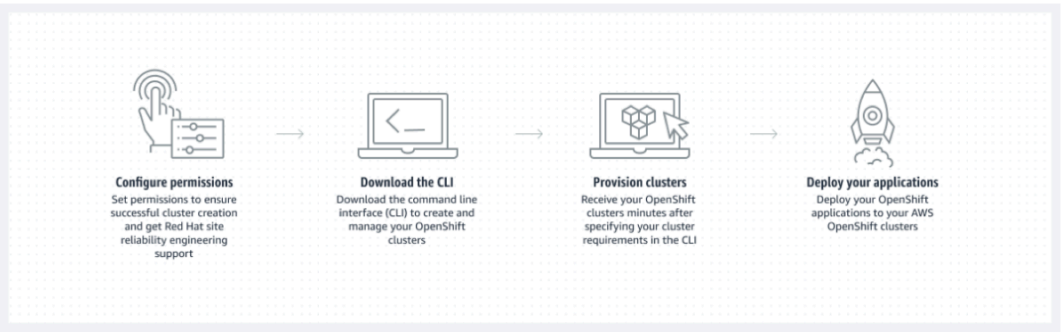
- ROSA コンソール — ROSA サブスクリプションを有効にして ROSA ソフトウェア契約を購入するためのウェブインターフェイスを提供します。

- 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 マネジメントコンソール/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 “”」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 “ ”。

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。

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。

- 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。
- 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。

内容

-
-
-
-

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。 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。

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。
- TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
-
-
-
- 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。 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

> **Important**
>
> そうすると、顧客データが失われる可能性があります。

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**

etcd 暗号化

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。

キー管理

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

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。

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。 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、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

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

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。

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。

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。

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。

-
- 詳細については、AWS Key Management Service 料金表を参照してください。

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
-
-

•

オーディエンス

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。

アイデンティティを使用した認証

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。

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。

フェデレーテッドアイデンティティ

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。

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。

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。

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。

- 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。

-
- 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。
- 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。
  - 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。 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。
  - 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。
-

ポリシーを使用したアクセスの管理

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。 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。

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。

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。

アイデンティティベースのポリシー

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。 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。

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。

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。

その他のポリシータイプ

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。

- 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。
- 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。
- 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。

ROSAManageSubscription の詳細については、「the section called “”」を参照してください。

詳細については、「the section called “ ”」を参照してください。

> **Note**
>
> 詳細については、「the section called “ ”」を参照してください。

詳細については、「the section called “”」および「the section called “”」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

```
{
    "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": "*"
        }
    ]
}
```

IAM エンティティに [Prefix]-Installer-Role-Policy をアタッチできます。

アクセス許可ポリシー

```
{
    "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"
                }
            }
        }
    ]
}
```

IAM エンティティに [Prefix]-ControlPlane-Role-Policy をアタッチできます。

アクセス許可ポリシー

```
{
    "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": "*"
        }
    ]
}
```

IAM エンティティに [Prefix]-Worker-Role-Policy をアタッチできます。

アクセス許可ポリシー

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

IAM エンティティに [Prefix]-Support-Role-Policy をアタッチできます。

アクセス許可ポリシー

```
{
    "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*"
            ]
        }
    ]
```

```
}
```

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。

IAM エンティティに `[Prefix]-openshift-ingress-operator-cloud-credentials` をアタッチできます。 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

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

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。

アクセス許可ポリシー

```
{
    "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": "*"
        }
    ]
}
```

IAM エンティティに [Prefix]-openshift-machine-api-aws-cloud-credentials をアタッチできます。

アクセス許可ポリシー

```
{
    "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
                }
            }
        }
    ]
}
```

IAM エンティティに [Prefix]-openshift-cloud-credential-operator-cloud-credentials をアタッチできます。

アクセス許可ポリシー

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

IAM エンティティに `[Prefix]-openshift-image-registry-installer-cloud-credentials` をアタッチできます。 オペレーターの詳細については、OpenShift GitHub ドキュメントの「Image Registry Operator」を参照してください。

アクセス許可ポリシー

```
{
    "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": "*"
        }
    ]
}
```

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。 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

```
{
    "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": "*"
        }
    ]
}
```

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。

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。

•
•
•

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

アクセス許可の詳細

•
•

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

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。

-
-
-
-
-
- route53 — クラスターの正常性に関連する DNS 設定を確認します。
-

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口ールをインスタンスプロファイルに追加できます。

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。

-
- 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。
- 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。 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。
-
- 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。
- 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。

アクセス許可の詳細

-
-

アクセス許可の詳細

-

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

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。

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

-
-

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、タグ値への読み取りアクセスを許可します。 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。
-
- `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。

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。

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。

-

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。

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。

-

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。

- 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。
-
- 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。

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。

-
-
- 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。
-

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。

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。

-
-
-
-

アクセス許可の詳細

-
-
-
-

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
	詳細についてはthe section called “”を参照してください。	2026 年 8 月 18 日
	詳細についてはthe section called “”を参照してください。	2026 年 7 月 28 日
	詳細についてはthe section called “”を参照してください。	2026 年 7 月 28 日
	詳細についてはthe section called “”を参照してください。	
	詳細についてはthe section called “”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	詳細についてはthe section called “”を参照してください。	2026 年 3 月 5 日
	詳細についてはthe section called “”を参照してください。	2025 年 9 月 3 日
	詳細についてはthe section called “”を参照してください。	2025 年 8 月 7 日
	詳細についてはthe section called “”を参照してください。	2025 年 8 月 7 日
	詳細についてはthe section called “”を参照してください。	2025 年 8 月 7 日
ROSAImageRegistryOperatorPolicy — ポリシーが更新されました	詳細についてはthe section called “”を参照してください。	2025 年 5 月 19 日

変更	説明	日付
	詳細についてはthe section called “”を参照してください。	2025 年 5 月 5 日
ROSAImageRegistryOperatorPolicy — ポリシーが更新されました	詳細についてはthe section called “”を参照してください。	2025 年 4 月 16 日
	詳細についてはthe section called “”を参照してください。	2025 年 3 月 3 日
	詳細についてはthe section called “”を参照してください。	2025 年 2 月 24 日
	詳細についてはthe section called “”を参照してください。	2025 年 1 月 17 日
	詳細についてはthe section called “”を参照してください。	2024 年 5 月 2 日
	詳細についてはthe section called “”を参照してください。	2024 年 4 月 24 日
	詳細についてはthe section called “”を参照してください。	2024 年 4 月 10 日
	詳細についてはthe section called “”を参照してください。	2024 年 4 月 10 日
	詳細についてはthe section called “”を参照してください。	2024 年 1 月 26 日
	詳細についてはthe section called “”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	詳細についてはthe section called “”を参照してください。	2023 年 12 月 12 日

変更	説明	日付
ROSAKubeControllerPolicy — ポリシーが更新されました	詳細についてはthe section called “”を参照してください。	2023 年 10 月 16 日
ROSAManageSubscription — ポリシーが更新されました	詳細についてはthe section called “”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	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 “”を参照してください。	2023 年 7 月 13 日
ROSANodePoolManagementPolicy — 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 “”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	詳細についてはthe section called “”を参照してください。	2023 年 6 月 6 日
ROSASRESupportPolicy — 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 “”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	詳細についてはthe section called “”を参照してください。	2023 年 4 月 27 日
ROSAKubeControllerPolicy — 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 “”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	詳細についてはthe section called “”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	詳細についてはthe section called “”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	詳細についてはthe section called “”を参照してください。	2023 年 4 月 20 日
ROSAIngressOperatorPolicy — 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 “”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	詳細についてはthe section called “”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	詳細についてはthe section called “”を参照してください。	2023 年 4 月 20 日
	詳細についてはthe section called “”を参照してください。	2022 年 4 月 11 日
		2022 年 3 月 2 日

```
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.
```

1.
2.
3.

```
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.
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。

```
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.
```

1.
2.

```
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.

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。

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。

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。

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。 詳細については、「the section called “責任”」を参照してください。

> **Important**
>
> 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

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。

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。

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。

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。

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。

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。

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

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 マネジメントコンソール。

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
- 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
- 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
- osdCcsAdmin エラー クラスター で を作成できませんでした
- 次の手順
- ROSA サポートを受ける

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
ROSAAmazonEBSCSIDriverOperatorPolicy を更新	管理ポリシーを更新 `ROSAAmazonEBSCSIDriverOperatorPolicy` して、CSI Amazon EBS ドライバーを release-1.61 機能セットに拡張しました。この更新により、 Amazon EBS CSI ドライバーオペレーターは Amazon EBS スナップショットをコピーしてロックし、高速スナップショット復元を有効にできます。また、暗号化されたボリュームオペレーションにカスタマーマネージド AWS KMS キーを使用することもできます。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。	2026 年 8 月 18 日
ROSANodePoolManagementPolicy を更新	AWS マネージドポリシー ROSANodePoolManagementPolicy を更新し、Node Pool コントローラーが EC2 インスタンスタイプを記述できるようにしました。コントローラーは、`red-hat:"true"`リソースタグを持つカスタマー管理の Amazon	2026 年 7 月 28 日

	SQS キューからスポットインスタンス中断メッセージを受信および削除することもできます。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。	
ROSAControlPlaneOperatorPolicy を更新	AWS 管理ポリシー ROSAControlPlaneOperatorPolicy を更新しました。この更新により、コントロールプレーンオペレーターは Red Hat が管理するセキュリティグループ () でタグを追加および削除できますec2:DeleteTags 。保護により、オペレータはred-hat-managed タグ自体を削除できなくなります。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。	2026 年 7 月 28 日
新しい ROSAKarpenterControllerPolicy	AWS は、Karpenter 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を使用して ROSA の EC2 ワーカーノードを動的にプロビジョニング、スケーリング、管理ROSAKarpenterControllerPolicy 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。	2026 年 7 月 22 日

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ROSANodePoolManagementPolicy 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。	2025 年 9 月 3 日
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 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 (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 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 (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。