Red Hat OpenShift Service on AWS 4

環境の準備

Red Hat OpenShift Service on AWS の計画、制限、およびスケーラビリティ

Last Updated: 2022-11-21

Red Hat OpenShift Service on AWS 4 環境の準備

Red Hat OpenShift Service on AWS の計画、制限、およびスケーラビリティ

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

法律上の通知

概要

このドキュメントでは、クラスターの制限やスケーラビリティーに関する情報など、Red Hat OpenShift Service on AWS (ROSA) クラスターのデプロイに関する計画上の考慮事項を説明します。

目次

第1章 STS を使用した ROSA の AWS 前提条件

Red Hat OpenShift Service on AWS (ROSA) は、Red Hat によるクラスターのお客様の既存 Amazon Web Service (AWS) アカウントへのデプロイを可能にするモデルを提供します。

ヒント

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

STS で ROSA をインストールする前に、以下の AWS 前提条件を満たしていることを確認してください。

1.1. デプロイメントの前提条件

Red Hat OpenShift Service on AWS (ROSA) を既存の Amazon Web Services (AWS) アカウントにデプロイするには、Red Hat が求める複数の前提条件を満たす必要があります。

Red Hat では、複数の AWS アカウントを管理するために AWS Organizations を使用することを推奨します。お客様が管理する AWS Organizations は、複数の AWS アカウントをホストします。すべてのアカウントがアカウント階層で参照する組織には root アカウントがあります。

ROSA クラスターが AWS Organizational Unit 内の AWS アカウントでホストされるようにすることがベストプラクティスです。Service Control Policy (SCP) が作成され、AWS サブアカウントのアクセスが許可されるサービスを管理する AWS Organizational Unit に適用されます。SCP は、Organizational Unit 内のすべての AWS サブアカウントの単一の AWS アカウント内で利用可能なパーミッションにのみ適用されます。SCP を単一の AWS アカウントに適用することもできます。お客様の AWS Organizations 内の他のすべてのアカウントは、お客様が必要とされる方法に応じて管理されます。Red Hat のサイト信頼性エンジニアリング (SRE) には、AWS Organizations 内の SCP に対する制御がありません。

重要

AWS STS を使用して ROSA クラスターを作成すると、関連付けられた AWS OpenID Connect(OIDC) アイデンティティープロバイダーも作成されます。この OIDC プロバイダー設定は、**us-east-1** AWS リージョンにある公開鍵に依存します。AWS SCP をお持ちのお客様は、これらのクラスターが別のリージョンにデプロイされている場合でも **us-east-1** AWS リージョンを使用できるようにする必要があります。

1.2. デプロイメントに STS を使用する場合のカスタマー要件

AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターをデプロイする前に、以下の前提条件を満たす必要があります。

1.2.1. アカウント

- AWS アカウント内にプロビジョニングされる Red Hat OpenShift Service on AWS をサポートするのに十分な AWS 制限が設定されていることを確認する必要があります。CLI で **rosa verify quota** を実行すると、クラスターの実行に必要なクォータがあることを検証します。

注記

クォータの検証は AWS クォータを確認しますが、消費を AWS クォータと比較しません。詳細については、追加リソースの制限とスケーラビリティリンクを参照してください。

- SCP ポリシーを適用し、強制される場合、これらのポリシーは、クラスターが必要とするロールおよびポリシーよりも制限的であってはなりません。
- AWS アカウントを Red Hat に譲渡できないようにする必要があります。
- Red Hat のアクティビティーに対する定義されたロールおよびポリシー以外に、追加の AWS 使用制限を課すことはできません。制限を課すことにより、Red Hat のインシデントへの対応が大幅に妨げられます。
- ネイティブ AWS サービスを同じ AWS アカウントにデプロイできます。
- エラスティックロードバランサー (ELB) を設定するために必要なため、アカウントにはサービスにリンクされたロールを設定する必要があります。以前に AWS アカウントでロードバランサーを作成したことがない場合の ELB のサービスリンクロールの作成については、追加リソースの Elastic Load Balancer (ELB) のサービ出力ルの作成リンクを参照してください。

注記

Red Hat OpenShift Service on AWS およびその他の Red Hat がサポートするサービスをホストする VPC とは別に、仮想プライベートクラウド (VPC) にリソースを展開することをお勧めしますが、必須ではありません。

関連情報

- 制限およびスケーラビリティー
- Elastic Load Balancer (ELB) のサービ出力ルの作成

1.2.2. アクセス要件

- Red Hat には、お客様が指定する AWS アカウントへの AWS コンソールへのアクセスが必要です。Red Hat は、このアクセスを保護および管理します。
- Red Hat OpenShift Service on AWS 内でパーミッションを昇格させるために AWS アカウントを使用しないでください。
- **rosa** CLI ユーティリティーまたは OpenShift Cluster Manager Hybrid Cloud Console コンソールで使用可能なアクションは、AWS アカウントで直接実行しないでください。
- ROSA クラスターをデプロイするために、事前に設定されたドメインは必要ありません。カスタムドメインを使用する場合は、追加のリソースを参照してください。

関連情報

- Configuring custom domains for applications を参照してください。

1.2.3. サポート要件

- Red Hat では、お客様が少なくとも AWS の ビジネスサポート を用意することを推奨します。

- Red Hat は、お客様の代わりに AWS サポートをリクエストする許可をお客様から受けている場合があります。
- Red Hat は、お客様のアカウントで AWS リソース制限の引き上げをリクエストする許可をお客様から受けている場合があります。
- Red Hat は、この要件に関するセクションで指定されていない場合に、すべての Red Hat OpenShift Service on AWS クラスターについての制約、制限、予想される内容およびデフォルトの内容を管理します。

1.2.4. セキュリティー要件

- Red Hat には、許可リストにある IP アドレスから EC2 ホストおよび API サーバーへの ingress アクセスが必要です。
- Red Hat では、文書化されたドメインで egress を許可する必要があります。指定されたドメインについては、AWS ファイアウォールの前提条件セクションを参照してください。

関連情報

- AWS ファイアウォールの前提条件

1.2.5. OpenShift Cluster Manager を使用するための要件

以下のセクションでは、OpenShift Cluster Manager Hybrid Cloud Console の要件について説明します。CLI ツールのみを使用する場合は、この要件を無視できます。

OpenShift Cluster Manager を使用するには、AWS アカウントをリンクする必要があります。このリンクの概念は、アカウントの関連付けとしても知られています。

1.2.5.1. AWS アカウントの関連付け

Red Hat OpenShift Service on AWS (ROSA) クラスタープロビジョニングタスクでは、Amazon リソースネーム (ARN) を使用して、**ocm-role** および **user-role** OpenShift Cluster Manager IAM リソースを AWS アカウントにリンクする必要があります。

ocm-role ARN は Red Hat 組織にラベルとして保存され、 **user-role** ARN は Red Hat ユーザーアカウント内にラベルとして保存されます。Red Hat は、これらの ARN ラベルを使用して、ユーザーが有効なアカウント所有者であり、AWS アカウントで必要なタスクを実行するための正しいアクセス許可が利用可能であることを確認します。

1.2.5.2. AWS アカウントのリンク

rosa CLI を使用して AWS アカウントをリンクします。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager Hybrid Cloud Console を使用してクラスターを作成している。
- AWS アカウント全体のロールをインストールするために必要な権限がある。詳細については、このセクションのその他のリソースを参照してください。

- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成している。

手順

1. CLI から、Amazon Resource Name (ARN) を使用して、**ocm-role** リソースを Red Hat 組織にリンクします。

注記

rosa link コマンドを実行するには、Red Hat Organization Administrator (組織管理者権限) が必要です。**ocm-role** リソースを AWS アカウントにリンクすると、組織内のすべてのユーザーに表示されます。

```
$ rosa link ocm-role --role-arn <arn>
```

出力例

```
I: Linking OCM role
? Link the '<AWS ACCOUNT ID>` role with organization '<ORG ID>'? Yes
I: Successfully linked role-arn '<AWS ACCOUNT ID>' with organization account '<ORG ID>'
```

2. CLI から、Amazon Resource Name (ARN) を使用して、**user-role** リソースを Red Hat ユーザーアカウントにリンクします。

```
$ rosa link user-role --role-arn <arn>
```

出力例

```
I: Linking User role
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125' role with
organization '<AWS ID>'? Yes
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125'
with organization account '<AWS ID>'
```

関連情報

- クラスターの作成に必要な IAM ロールのリストについては、アカウント全体の IAM ロールとポリシー参照 を参照してください。

1.2.5.3. 複数の AWS アカウントを Red Hat 組織に関連付ける

複数の AWS アカウントを Red Hat 組織に関連付けることができます。複数のアカウントを関連付けると、Red Hat 組織の関連付けられた AWS アカウントのいずれかに Red Hat OpenShift Service on AWS (ROSA) クラスターを作成できます。

この機能を使用すると、リージョンにバインドされた環境として複数の AWS プロファイルを使用することにより、さまざまな AWS リージョンにクラスターを作成できます。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager Hybrid Cloud Console を使用してクラスターを作成している。
- AWS アカウント全体のロールをインストールするために必要な権限がある。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成している。

手順

追加の AWS アカウントを関連付けるには、最初にローカル AWS 設定でプロファイルを作成します。次に、追加の AWS アカウントに **ocm-role**、user、および account のロールを作成して、アカウントを Red Hat 組織に関連付けます。

追加のリージョンでロールを作成するには、**rosa create** コマンドの実行時に **--profile <aws-profile>** パラメーターを指定し、**<aws_profile>** を追加のアカウントプロファイル名に置き換えます。

- OpenShift Cluster Manager ロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

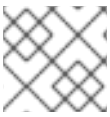
```
$ rosa create --profile <aws_profile> ocm-role
```

- ユーザーロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> user-role
```

- アカウントロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> account-roles
```



注記

プロファイルを指定しない場合は、デフォルトの AWS プロファイルが使用されます。

1.3. オプトインリージョンでのクラスターデプロイの要件

AWS のオプトインリージョンは、デフォルトで有効になっていないリージョンです。オプトインリージョンで AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターをデプロイする場合には、以下の要件を満たす必要があります。

- リージョンは AWS アカウントで有効にする必要があります。オプトインリージョンの有効化の詳細は、AWS ドキュメント AWS リージョンの管理 を参照してください。
- AWS アカウントのセキュリティートークンバージョンは、バージョン 2 に設定する必要があります。オプトインリージョンにバージョン 1 セキュリティートークンを使用することはできません。

重要

セキュリティートークンのバージョン 2 に更新すると、トークンが長くなるため、トークンを保管するシステムに影響が出ることがあります。詳細は、the AWS documentation on setting STS preferences を参照してください。

1.3.1. AWS セキュリティートークンのバージョン設定

AWS のオプトインリージョンで AWS Security Token Service (STS) を使用して Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する場合は、AWS アカウントでセキュリティートークンのバージョンをバージョン 2 に設定する必要があります。

前提条件

- インストールホストに、最新の AWS CLI をインストールして設定している。

手順

1. AWS CLI の設定で定義されている AWS アカウントの ID を一覧表示します。

```
$ aws sts get-caller-identity --query Account --output json
```

   出力が該当する AWS アカウントの ID と一致していることを確認します。

2. AWS アカウントに設定されているセキュリティートークンのバージョンを記載します。

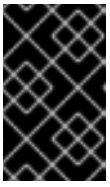
```
$ aws iam get-account-summary --query SummaryMap.GlobalEndpointTokenVersion --
output json
```

   出力例

```
1
```

3. AWS アカウントの全リージョンのセキュリティートークンのバージョンをバージョン 2 に更新するには、以下のコマンドを実行します。

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



重要

セキュリティートークンのバージョン 2 に更新すると、トークンが長くなるため、トークンを保管するシステムに影響が出ることがあります。詳細は、the AWS documentation on setting STS preferences を参照してください。

1.4. AWS の RED HAT 管理 IAM リファレンス

STS デプロイメントモデルでは、Red Hat は Amazon Web Services (AWS) IAM ポリシー、IAM ユーザー、または IAM ロールを作成し、管理しなくなります。これらのロールとポリシーの作成については、IAM ロールに関する以下のセクションを参照してください。

- **ocm** CLI を使用するには、**ocm-role** および **user-role** リソースが必要です。OpenShift Cluster Manager IAM ロールリソース を参照してください。

- クラスターが 1 つの場合は、アカウント全体の IAM ロールとポリシー参照 を参照してください。
- すべてのクラスターについて、必要な Operator ロールが必要です。クラスター固有の Operator IAM ロール参照 を参照してください。

1.5. プロビジョニングされる AWS インフラストラクチャー

以下は、デプロイされた Red Hat OpenShift Service on AWS (ROSA) クラスターでプロビジョニングされる Amazon Web Services (AWS) コンポーネントの概要です。プロビジョニングされたすべての AWS コンポーネントの詳細な一覧は、OpenShift Container Platform ドキュメント を参照してください。

1.5.1. EC2 インスタンス

AWS EC2 インスタンスは、AWS パブリッククラウドに ROSA のコントロールプレーンおよびデータプレーン機能をデプロイするために必要です。

インスタンスタイプは、ワーカーノードの数に応じてコントロールプレーンおよびインフラストラクチャーノードによって異なる場合があります。少なくとも、以下の EC2 インスタンスがデプロイされます。

- 3 つの **m5.2xlarge** コントロールプレーンノード
- 2 つの **r5.xlarge** インフラストラクチャーノード
- 2 つの **m5.xlarge** カスタマイズ可能なワーカーノード

ワーカーノード数の詳細なガイダンスは、このページの関連情報セクションに一覧表示されている「インスタンスタイプ」トピックの初期計画に関する考慮事項に関する情報を参照してください。

1.5.2. AWS Elastic Block Store (EBS) ストレージ

Amazon EBS ブロックストレージは、ローカルノードストレージおよび永続ボリュームストレージの両方に使用されます。

各 EC2 インスタンスのボリューム要件:

- コントロールプレーンボリューム
  - サイズ: 350GB
  - タイプ: io1
  - 1 秒あたりの I/O 処理数: 1000
- インフラストラクチャーボリューム
  - サイズ: 300GB
  - タイプ: gp2
  - 1 秒あたりの入出力操作: 900
- ワーカーボリューム
  - サイズ: 300GB

- タイプ: gp2
- 1 秒あたりの入出力操作: 900

1.5.3. Elastic Load Balancer

API 用に最大 2 つの Network Elastic Load Balancers (ELB) と、アプリケーションルーター用に最大 2 つの Classic ELB。詳細は、AWS についての ELB ドキュメント を参照してください。

1.5.4. S3 ストレージ

イメージレジストリーは、AWS S3 ストレージによって支えられています。S3 の使用およびクラスターのパフォーマンスを最適化するために、リソースのプルーニングを定期的に実行します。

注記

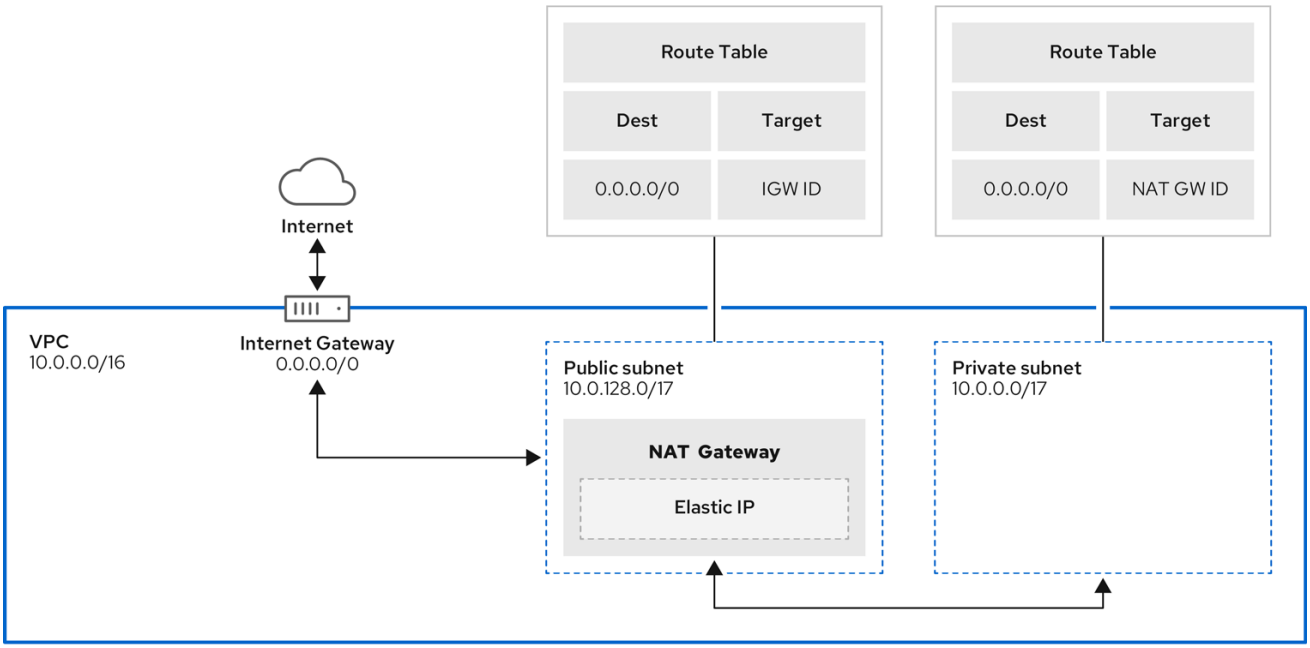
通常のサイズがそれぞれ 2TB の 2 つのバケットが必要です。

1.5.5. VPC

お客様はクラスターごとに 1 つの VPC を確認できるはずです。さらに、VPC には以下の設定が必要です。

- **サブネット**: 単一アベイラビリティーゾーンがあるクラスターの 2 つのサブネット、または複数のアベイラビリティーゾーンがあるクラスターの 6 つのサブネット。
- **ルートテーブル**: プライベートサブネットごとに 1 つのルートテーブルと、クラスターごとに 1 つの追加テーブル。
- **インターネットゲートウェイ**: クラスターごとに 1 つのインターネットゲートウェイ。
- **NAT ゲートウェイ**: パブリックサブネットごとに 1 つの NAT ゲートウェイ。

1.5.5.1. サンプル VPC アーキテクチャー

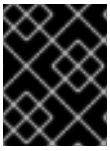


1.5.6. セキュリティーグループ

AWS セキュリティーグループは、プロトコルおよびポートアクセスレベルでセキュリティーを提供します。これらは EC2 インスタンスおよび Elastic Load Balancer に関連付けられます。各セキュリティーグループには、EC2 インスタンスに出入りするトラフィックをフィルターする一連のルールが含まれます。OpenShift インストールに必要なポートがネットワーク上で開いており、ホスト間のアクセスを許可するよう設定されていることを確認する必要があります。

グループ	タイプ	IP プロトコル	ポート範囲
MasterSecurityGroup	**AWS::EC2::SecurityGroup**	**icmp**	**0**
		tcp	**22**
		tcp	**6443**
		tcp	**22623**
WorkerSecurityGroup	**AWS::EC2::SecurityGroup**	**icmp**	**0**
		tcp	**22**
BootstrapSecurityGroup	**AWS::EC2::SecurityGroup**	**tcp**	**22**
		tcp	**19531**

1.6. AWS ファイアウォールの前提条件



重要

PrivateLink で展開された ROSA クラスターのみが、ファイアウォールを使用して出力トラフィックを制御できます。

このセクションでは、Red Hat OpenShift Service on AWS クラスターからの出力トラフィックを制御できるようにするために必要な詳細を提供します。ファイアウォールを使用して出力トラフィックを制御している場合は、以下のドメインとポートの組み合わせへのアクセスを許可するようにファイアウォールを設定する必要があります。Red Hat OpenShift Service on AWS は、フルマネージド Open Shift サービスを提供するためにこのアクセスを必要とします。

手順

1. パッケージとツールのインストールおよびダウンロードに使用される以下の URL を許可リストに指定します。

Domain	ポート	機能
registry.redhat.io	443	コアコンテナーイメージを指定します。
quay.io	443	コアコンテナーイメージを指定します。
***.quay.io**	443	コアコンテナーイメージを指定します。
sso.redhat.com	443、80	必須。**https://console.redhat.com/openshift** サイトでは、**sso.redhat.com** からの認証を使用してプルシークレットをダウンロードし、Red Hat SaaS ソリューションを使用してサブスクリプション、クラスターインベントリー、チャージバックレポートなどのモニターリングを行います。
quay-registry.s3.amazonaws.com	443	コアコンテナーイメージを指定します。
cm-quay-production-s3.s3.amazonaws.com	443	コアコンテナーイメージを指定します。
cart-rhcos-ci.s3.amazonaws.com	443	Red Hat Enterprise Linux CoreOS (RHCOS) イメージを提供します。
openshift.org	443	Red Hat Enterprise Linux CoreOS (RHCOS) イメージを提供します。

Domain	ポート	機能
registry.access.redhat.com	443	開発者が OpenShift および Kubernetes でビルドするのに役立つ **odo** CLI ツールへのアクセス。
console.redhat.com	443、80	必須。クラスターと OpenShift Console Manager との間の対話が、スケジューリングアップグレードなどの機能を有効にすることを許可します。
sso.redhat.com	443	**https://console.redhat.com/openshift** サイトは、**sso.redhat.com** からの認証を使用します。
pull.q1w2.quay.rhcloud.com	443	quay.io が利用できない場合のフォールバックとして、コアコンテナーイメージを提供します。
.q1w2.quay.rhcloud.com	443	quay.io が利用できない場合のフォールバックとして、コアコンテナーイメージを提供します。

quay.io などのサイトを許可リストに追加する場合は、***.quay.io** などのワイルドカードエントリーを拒否リストに加えないでください。ほとんどの場合、イメージレジストリーはコンテンツ配信ネットワーク (CDN) を使用してイメージを提供します。ファイアウォールがアクセスをブロックすると、初回のダウンロード要求が **cdn01.quay.io** などのホスト名にリダイレクトされると、イメージのダウンロードが拒否されます。

cdn01.quay.io などの CDN ホスト名は、許可リストに **.quay.io** などのワイルドカードエントリーを追加する場合に説明されます。

2. 次のテレメトリー URL を許可リストします。

Domain	ポート	機能
cert-api.access.redhat.com	443	テレメトリーで必要です。
api.access.redhat.com	443	テレメトリーで必要です。
infogw.api.openshift.com	443	テレメトリーで必要です。
console.redhat.com	443	テレメトリーと Red Hat Insights で必要です。

Domain	ポート	機能
observatorium.api.openshift.comm	443	Managed OpenShift 固有のテレメトリーに使用されます。

マネージドクラスターでは、テレメトリーを有効にして、Red Hat が問題に迅速に対応し、顧客をより適切にサポートし、製品のアップグレードがクラスターに与える影響をよりよく理解できるようにする必要があります。Red Hat によるリモートヘルスモニターリングデータの使用方法の詳細は、リモートヘルスモニターリングについて を参照してください。

3. 次の Amazon Web Services (AWS) API URI を許可リストします。

Domain	ポート	機能
.amazonaws.com	443	AWS サービスおよびリソースへのアクセスに必要です。

または、Amazon Web Services (AWS) API にワイルドカードを使用しない場合は、次の URL を許可リストに追加する必要があります。

Domain	ポート	機能
ec2.amazonaws.com	443	AWS 環境でクラスターをインストールし、管理するのに使用されます。
events.amazonaws.com	443	AWS 環境でクラスターをインストールし、管理するのに使用されます。
iam.amazonaws.com	443	AWS 環境でクラスターをインストールし、管理するのに使用されます。
route53.amazonaws.com	443	AWS 環境でクラスターをインストールし、管理するのに使用されます。
sts.amazonaws.com	443	AWS 環境でクラスターをインストールし、管理するのに使用されます。
tagging.us-east-1.amazonaws.com	443	AWS 環境でクラスターをインストールし、管理するのに使用されます。このエンドポイントは、クラスターが展開されているリージョンに関係なく、常に us-east-1 です。

Domain	ポート	機能
ec2.<aws_region>.amazonaws.com	443	AWS 環境でクラスターをインストールし、管理するのに使用されます。
elasticloadbalancing.<aws_region>.amazonaws.com	443	AWS 環境でクラスターをインストールし、管理するのに使用されます。
servicequotas.<aws region>.amazonaws.com	443、80	必須。サービスをデプロイするためのクォータを確認するのに使用されます。
tagging.<region>.amazonaws.com	443、80	タグの形式で AWS リソースに関するメタデータを割り当てることができます。

4. 以下の OpenShift URL を許可リストします。

Domain	ポート	機能
mirror.openshift.com	443	ミラーリングされたインストールのコンテンツおよびイメージへのアクセスに使用されます。Cluster Version Operator (CVO) には単一の機能ソースのみが必要ですが、このサイトはリリースイメージ署名のソースでもあります。
storage.googleapis.com/openshift-release (推奨)	443	mirror.openshift.com/ の代替サイト。quay.io からプルするイメージを把握するのにクラスターが使用するプラットフォームリリース署名をダウンロードするのに使用されます。
api.openshift.com	443	クラスターに更新が利用可能かどうかを確認するのに使用されます。

5. 次のサイト信頼性エンジニアリング (SRE) および管理 URL を許可リストします。

Domain	ポート	機能
api.pagerduty.com	443	このアラートサービスは、クラスター内の alertmanager が使用します。これにより、Red Hat SRE に対してイベントの SRE 通知についてのアラートが送信されます。

Domain	ポート	機能
events.pagerduty.com	443	このアラートサービスは、クラスター内の alertmanager が使用します。これにより、Red Hat SRE に対してイベントの SRE 通知についてのアラートが送信されます。
api.deadmanssnitch.com	443	Red Hat OpenShift Service on AWS がクラスターが使用可能で実行中であるかどうかを示す定期的な ping を送信するために使用するアラートサービス。
nosnch.in	443	Red Hat OpenShift Service on AWS がクラスターが使用可能で実行中であるかどうかを示す定期的な ping を送信するために使用するアラートサービス。
***.osdsecuritylogs.splunkcloud.com** OR **inputs1.osdsecuritylogs.splunkcloud.com** **inputs2.osdsecuritylogs.splunkcloud.com** **inputs4.osdsecuritylogs.splunkcloud.com** **inputs5.osdsecuritylogs.splunkcloud.com** **inputs6.osdsecuritylogs.splunkcloud.com** **inputs7.osdsecuritylogs.splunkcloud.com** **inputs8.osdsecuritylogs.splunkcloud.com** **inputs9.osdsecuritylogs.splunkcloud.com** **inputs10.osdsecuritylogs.splunkcloud.com** **inputs11.osdsecuritylogs.splunkcloud.com** **inputs12.osdsecuritylogs.splunkcloud.com** **inputs13.osdsecuritylogs.splunkcloud.com** **inputs14.osdsecuritylogs.splunkcloud.com** **inputs15.osdsecuritylogs.splunkcloud.com**	9997	**splunk-forwarder-operator** によって使用され、ログベースのアラートについて Red Hat SRE が使用するロギング転送エンドポイントとして使用されます。

Domain	ポート	機能
http-inputs-osdsecuritylogs.splunkcloud.com	443	必須。**splunk-forwarder-operator** によって使用され、ログベースのアラートについて Red Hat SRE が使用するロギング転送エンドポイントとして使用されます。
sftp.access.redhat.com (推奨)	22	**must-gather-operator** が、クラスターに関する問題のトラブルシューティングに役立つ診断ログをアップロードするのに使用される SFTP サーバー。

6. Amazon Web Services (AWS) API のワイルドカードを許可しなかった場合は、内部 OpenShift レジストリーに使用される S3 バケットも許可する必要があります。そのエンドポイントを取得するには、クラスターが正常にプロビジョニングされた後に次のコマンドを実行します。

```
$ oc -n openshift-image-registry get pod -l docker-registry=default -o json | jq
'.items[].spec.containers[].env[] | select(.name=="REGISTRY_STORAGE_S3_BUCKET")'
```

   S3 エンドポイントは '<cluster-name>-<random-string>-image-registry-<cluster-region>-<random-string>.s3.dualstack.<cluster-region>.amazonaws.com' の形式である必要があります。

7. ビルドに必要な言語またはフレームワークのリソースを提供するサイトを許可リストに指定します。

8. OpenShift で使用される言語およびフレームワークに依存するアウトバウンド URL を許可リストに指定します。ファイアウォールまたはプロキシーで許可できる推奨 URL の一覧は、OpenShift Outbound URLs to Allow を参照してください。

1.7. 次のステップ

- 必要な AWS サービスクォータの確認

1.8. 関連情報

- SRE のすべての Red Hat OpenShift Service on AWS 4 クラスターへのアクセス
- アプリケーションのカスタムドメインの設定
- インスタンスタイプ

第2章 OPENSHIFT CLUSTER MANAGER IAM ロールリソース

Red Hat OpenShift Service on AWS (ROSA) Web UI では、OpenShift Cluster Manager Hybrid Cloud Console および **rosa** コマンドラインインターフェイス (CLI) でエンドユーザーエクスペリエンスを提供するための信頼関係を作成する、AWS アカウントに対する特定のパーミッションが必要です。.

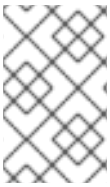
この信頼関係は **ocm-role** AWS IAM ロールの作成と関連付けによって実現されます。このロールには、Red Hat アカウントを AWS アカウントにリンクする AWS インストーラーとの信頼ポリシーがあります。さらに、Web UI ユーザーごとに**user-role** AWS IAM ロールも必要です。これは、これらのユーザーを特定する役割を果たします。この **user-role** の AWS IAM ロールにはパーミッションがありません。

OpenShift Cluster Manager を使用するために必要な AWS IAM ロールは次のとおりです。

- **ocm ロール**
- ユーザーロール。

rosa CLI または OpenShift Cluster Manager Web UI のどちらを使用してクラスターを管理する場合でも、**rosa** CLI を使用して、**rosa** CLI で **account-roles** と呼ばれるアカウント全体のロールを作成する必要があります。これらのアカウントのロールは最初のクラスターに必要であり、これらのロールは複数のクラスターで使用できます。これらの必要なアカウントロールは次のとおりです。

- **Worker-Role**
- **Support-Role**
- **Installer-Role**
- **ControlPlane-Role**



注記

ロールの作成では、AWS アクセスまたはシークレットキーは要求されません。このワークフローのベースとして、AWS Secure Token Service (STS) が使用されます。AWS STS は、一時的な制限付きの認証情報を使用して認証を行います。

これらのロールの作成の詳細は、アカウント全体の IAM ロールとポリシー参照 を参照してください。

rosa CLI では **operator-roles** と呼ばれるクラスター固有の Operator ロールは、バックエンドストレージ、Ingress、レジストリーの管理など、クラスター操作を実行するために必要な一時的なパーミッションを取得します。これらのロールは、作成するクラスターに必要です。これらの必要な Operator ロールは次のとおりです。

- **<cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credentials**
- **<cluster_name>-<hash>-openshift-cloud-network-config-controller-credentials**
- **<cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials**
- **<cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-credentials**
- **<cluster_name>-<hash>-openshift-image-registry-installer-cloud-credentials**
- **<cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials**

これらのロールの作成の詳細は、クラスター固有の Operator IAM ロール参照 を参照してください。

2.1. OCM-ROLE IAM リソースについて

ユーザーの Red Hat 組織が ROSA クラスターを作成できるようにするには、**ocm-role** IAM リソースを作成する必要があります。AWS へのリンクのコンテキストでは、Red Hat 組織は OpenShift Cluster Manager 内の単一のユーザーです。

以下は、**ocm-role** IAM リソースに関するいくつかの考慮事項です。

- Red Hat 組織ごとに 1 つの **ocm-role** IAM ロールのみをリンクできますが、AWS アカウントごとに任意の数の **ocm-role** IAM ロールを指定できます。Web UI では、一度にリンクできるのはこれらのロールの内 1 つだけです。
- Red Hat 組織のすべてのユーザーは、**ocm-roleIAM** リソースを作成してリンクできます。
- Red Hat Organization Administrator (組織管理者) のみが **ocm-roleIAM** IAM リソースのリンクを解除できます。この制限は、他の Red Hat 組織のメンバーが他のユーザーのインターフェイス機能を妨害しないように保護するためのものです。

注記

既存組織の一部ではない Red Hat アカウントを作成したばかりの場合、このアカウントは Red Hat Organization Administrator でもあります。

- 基本および管理 **ocm-role** IAM リソースの AWS アクセス許可ポリシーのリストについては、このセクションの追加リソースの OpenShift Cluster Manager ロールについてを参照してください。

rosa CLI を使用すると、IAM リソースを作成するときにリンクできます。

注記

IAM リソースを AWS アカウントにリンクするまたは関連付けることは、**ocm-role** IAM ロールと Red Hat OpenShift Cluster Manager ロールを使用して信頼ポリシーを作成することを意味します。IAM リソースを作成してリンクすると、AWS の **ocm-role** IAM リソース と **arn:aws:iam::7333:role/RH-Managed-OpenShift-Installer** リソースとの信頼関係が表示されます。

Red Hat Organization Administrator (組織管理者) **ocm-role** IAM リソースを作成してリンクした後、すべての組織メンバーが独自の **user-role** IAM ロールを作成してリンクする場合もあります。この IAM リソースは、ユーザーごとに 1 回だけ作成およびリンクする必要があります。Red Hat 組織内の別のユーザーがすでに **ocm-role** IAM リソースを作成してリンクしている場合は、独自の **user-role** IAM ロールを作成してリンクしていることを確認する必要があります。

関連情報

- OpenShift Cluster Manager ロールについて を参照してください。

2.1.1. OpenShift Cluster Manager ロールの作成

コマンドラインインターフェイス (CLI) を使用して、OpenShift Cluster Manager IAM ロールを作成します。

前提条件

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

手順

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

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

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

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

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

出力例

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

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

注記

--admin オプションを使用した場合、このプロンプトは表示されません。

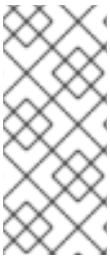
3. パーミッション境界を設定するためのポリシーの Amazon Resource Name (ARN)。
4. AWS ロールを作成する方法を選択します。**auto** を使用して、**rosa** CLI ツールはロールおよびポリシーを生成してリンクします。**auto** モードでは、AWS ロールを作成するためのいくつかの異なるプロンプトが表示されます。
5. auto メソッドは、接頭辞を使用して特定の **ocm-role** を作成するかどうかを尋ねます。
6. IAM ロールを OpenShift Cluster Manager に関連付けることを確認します。
7. 作成した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

2.2. USER-ROLE IAM ロールについて

Web UI ユーザーごとに **ユーザーロール** IAM ロールを作成して、これらのユーザーが ROSA クラスターを作成できるようにする必要があります。

user-role IAM ロールに関するいくつかの考慮事項は次のとおりです。

- Red Hat ユーザーアカウントごとに必要な **user-role** IAM ロールは 1 つだけですが、Red Hat 組織は IAM リソースの多くを持つことができます。
- Red Hat 組織のすべてのユーザーは、**user-role** IAM ロールを作成してリンクできます。
- Red Hat 組織の AWS アカウントごとに多数の **user-role** IAM ロールが存在する可能性があります。
- Red Hat は、**user-role** IAM ロールを使用してユーザーを識別します。この IAM リソースには AWS アカウントのパーミッションがありません。
- AWS アカウントは複数の **user-role** IAM ロールを指定できますが、各 IAM ロールを Red Hat 組織の各ユーザーにリンクする必要があります。ユーザーには、リンクされた **user-role** IAM ロールを複数指定できません。



注記

IAM リソースを AWS アカウントにリンクするまたは関連付けることは、**user-role** IAM ロールと Red Hat OpenShift Cluster Manager ロールを使用して信頼ポリシーを作成することを意味します。IAM リソースを作成してリンクすると、AWS の **user-role** IAM リソース と **arn:aws:iam::710019948333:role/RH-Managed-OpenShift-Installer** リソースとの信頼関係が表示されます。

2.2.1. user-role IAM ロールの作成

コマンドラインインターフェイス (CLI) を使用して、OpenShift Cluster Manager IAM ロールを作成できます。

前提条件

- AWS アカウントがある。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。

手順

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

```
$ rosa create user-role
```

このコマンドを使用すると、特定の属性を指定してロールを作成できます。次の出力例は、選択された自動モードを示しています。これにより、**rosa** CLI で Operator のロールとポリシーを作成できます。詳細は、関連情報の自動および手動のデプロイメントモードについてを参照してください。

出力例

```
I: Creating User role
? Role prefix: ManagedOpenShift 1
? Permissions boundary ARN (optional): 2
? Role creation mode: auto 3
I: Creating ocm user role using 'arn:aws:iam::2066:user'
? Create the 'ManagedOpenShift-User.osdocs-Role' role? Yes 4
I: Created role 'ManagedOpenShift-User.osdocs-Role' with ARN
'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role'
I: Linking User role
? User Role ARN: arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role
? Link the 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' role with account '1AGE'?
Yes 5
I: Successfully linked role ARN 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' with
account '1AGE'
```

1. 作成されたすべての AWS リソースの接頭辞値。この例では、**ManagedOpenShift** がすべての AWS リソースを付加します。
2. パーミッション境界を設定するためのポリシーの Amazon Resource Name (ARN)。
3. AWS ロールを作成する方法を選択します。**auto** を使用して、**rosa** CLI ツールは AQS アカウントを生成してリンクします。**auto** モードでは、AWS ロールを作成するためのいくつかの異なるプロンプトが表示されます。
4. auto メソッドは、接頭辞を使用して特定の **user-role** を作成するかどうかを尋ねます。
5. 作成したロールを AWS 組織にリンクします。

重要

クラスターを削除する前に **user-role** IAM ロールのリンクを解除または削除すると、エラーが発生してクラスターを削除できなくなります。削除プロセスを続行するには、このロールを作成または再リンクする必要があります。詳細は、削除できないクラスターの修復 を参照してください。

2.3. AWS アカウントの関連付け

Red Hat OpenShift Service on AWS (ROSA) クラスタープロビジョニングタスクでは、Amazon リソースネーム (ARN) を使用して、**ocm-role** および **user-role** OpenShift Cluster Manager IAM リソースを AWS アカウントにリンクする必要があります。

ocm-role ARN は Red Hat 組織にラベルとして保存され、 **user-role** ARN は Red Hat ユーザーアカウント内にラベルとして保存されます。Red Hat は、これらの ARN ラベルを使用して、ユーザーが有効なアカウント所有者であり、AWS アカウントで必要なタスクを実行するための正しいアクセス許可が利用可能であることを確認します。

2.3.1. AWS アカウントのリンク

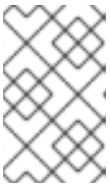
rosa CLI を使用して AWS アカウントをリンクします。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager Hybrid Cloud Console を使用してクラスターを作成している。
- AWS アカウント全体のロールをインストールするために必要な権限がある。詳細については、このセクションのその他のリソースを参照してください。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成している。

手順

1. CLI から、Amazon Resource Name (ARN) を使用して、**ocm-role** リソースを Red Hat 組織にリンクします。



注記

rosa link コマンドを実行するには、Red Hat Organization Administrator (組織管理者権限) が必要です。**ocm-role** リソースを AWS アカウントにリンクすると、組織内のすべてのユーザーに表示されます。

```
$ rosa link ocm-role --role-arn <arn>
```

出力例

```
I: Linking OCM role
? Link the '<AWS ACCOUNT ID>` role with organization '<ORG ID>'? Yes
I: Successfully linked role-arn '<AWS ACCOUNT ID>' with organization account '<ORG ID>'
```

2. CLI から、Amazon Resource Name (ARN) を使用して、**user-role** リソースを Red Hat ユーザーアカウントにリンクします。

```
$ rosa link user-role --role-arn <arn>
```

出力例

```
I: Linking User role
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125' role with
organization '<AWS ID>'? Yes
```

```
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-User-Role-125'
with organization account '<AWS ID>'
```

2.3.2. 複数の AWS アカウントを Red Hat 組織に関連付ける

複数の AWS アカウントを Red Hat 組織に関連付けることができます。複数のアカウントを関連付けると、Red Hat 組織の関連付けられた AWS アカウントのいずれかに Red Hat OpenShift Service on AWS (ROSA) クラスターを作成できます。

この機能を使用すると、リージョンにバインドされた環境として複数の AWS プロファイルを使用することにより、さまざまな AWS リージョンにクラスターを作成できます。

前提条件

- AWS アカウントがある。
- OpenShift Cluster Manager Hybrid Cloud Console を使用してクラスターを作成している。
- AWS アカウント全体のロールをインストールするために必要な権限がある。
- インストールホストに最新の AWS (**aws**) および ROSA (**rosa**) CLI をインストールして設定している。
- **ocm-role** および **user-role** IAM ロールを作成している。

手順

追加の AWS アカウントを関連付けるには、最初にローカル AWS 設定でプロファイルを作成します。次に、追加の AWS アカウントに **ocm-role**、user、および account のロールを作成して、アカウントを Red Hat 組織に関連付けます。

追加のリージョンでロールを作成するには、**rosa create** コマンドの実行時に **--profile <aws-profile>** パラメーターを指定し、**<aws_profile>** を追加のアカウントプロファイル名に置き換えます。

- OpenShift Cluster Manager ロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> ocm-role
```

- ユーザーロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> user-role
```

- アカウントロールを作成するときに AWS アカウントプロファイルを指定するには、以下を実行します。

```
$ rosa create --profile <aws_profile> account-roles
```

注記

プロファイルを指定しない場合は、デフォルトの AWS プロファイルが使用されます。

2.4. 関連情報

- Troubleshooting IAM roles を参照してください。
- クラスターの作成に必要な IAM ロールのリストについては、アカウント全体の IAM ロールとポリシー参照 を参照してください。

第3章 制限およびスケーラビリティー

このドキュメントでは、Red Hat OpenShift Service on AWS (ROSA) クラスターでテストされたクラスターの最大値について、最大値のテストに使用されたテスト環境と設定に関する情報とともに詳しく説明します。コントロールプレーンとインフラストラクチャーノードのサイズ設定とスケーリングに関する情報も提供されます。

3.1. ROSA テスト済みのクラスターの最大値

Red Hat OpenShift Service on AWS (ROSA) クラスターのインストールを計画するときは、以下のテスト済みオブジェクトの最大値を考慮してください。この表は、ROSA クラスターでテストされた各タイプの最大制限を示しています。

これらのガイドラインは、複数のアベイラビリティーゾーン設定の 102 のコンピューティング (ワーカーとも呼ばれる) ノードのクラスターに基づいています。小規模なクラスターの場合、最大値はこれより低くなります。

注記

すべてのテストで使用される OpenShift Container Platform バージョンは OCP 4.8.0 です。

表3.1 テスト済みのクラスターの最大値

最大値のタイプ	4.8 テスト済みの最大値
ノード数	443、80
Pod 数 [1]	443、80
ノードあたりの Pod 数	250
コアあたりの Pod 数	デフォルト値はありません。
namespace 数 [2]	443、80
namespace あたりの Pod 数 [3]	443、80
サービス数 [4]	10,000
namespace あたりのサービス数	10,000
サービスあたりのバックエンド数	10,000
namespace あたりのデプロイメント数 [3]	1,000

1. ここで表示される Pod 数はテスト用の Pod 数です。実際の Pod 数は、アプリケーションのメモリー、CPU、およびストレージ要件により異なります。

2. 有効なプロジェクトが多数ある場合は、キースペースが過剰に拡大し、スペースのクォータを超過すると、etcd はパフォーマンスの低下による影響を受ける可能性があります。etcd ストレージを利用できるようにするには、デフラグを含む etcd の定期的なメンテナーンスを行うことが強く推奨されます。

3. システムには、状態の変更に対する対応として特定の namespace にある全オブジェクトに対して反復する多数のコントロールループがあります。単一の namespace にタイプのオブジェクトの数が多くなると、ループのコストが上昇し、状態変更を処理する速度が低下します。この制限については、アプリケーションの各種要件を満たすのに十分な CPU、メモリー、およびディスクがシステムにあることが前提となっています。

4. 各サービスポートと各サービスのバックエンドには、iptables の対応するエントリーがあります。特定のサービスのバックエンド数は、エンドポイントのオブジェクトサイズに影響があり、その結果、システム全体に送信されるデータサイズにも影響を与えます。

OpenShift Container Platform 4.8 では、CPU コア (500 ミリコア) の半分がシステムによって予約されます (OpenShift Container Platform の以前のバージョンと比較)。

3.2. OPENSHIFT CONTAINER PLATFORM テスト環境および設定

以下の表は、AWS クラウドプラットフォームについてクラスターの最大値をテストする OpenShift Container Platform 環境および設定を一覧表示しています。

ノード	タイプ	vCPU	RAM(GiB)	ディスクタイプ	ディスクサイズ (GiB)/IOS	カウント	Region
コントロールプレーン/etcd [1]	m5.4xlarge	16	64	io1	350 / 1,000	3	us-west-2
インフラストラクチャーノード [2]	r5.2xlarge	8	64	gp2	300 / 900	3	us-west-2
ワークロード [3]	m5.2xlarge	8	32	gp2	350 / 900	3	us-west-2
Compute nodes	m5.2xlarge	8	32	gp2	350 / 900	443、80	us-west-2

1. etcd は I/O 集約型であり、レイテンシーの影響を受けやすいため、io1 ディスクはコントロールプレーン/etcd ノードに使用されます。使用方法に応じて、より多くの IOPS が必要になる場合があります。

2. Prometheus は使用状況パターンに応じて大量のメモリーを要求できるため、インフラストラクチャーノードはモニターリングコンポーネントをホストするために使用されます。

3. ワークロードノードは、パフォーマンスとスケーラビリティーのワークロードジェネレーターを実行するための専用ノードです。

より大きなクラスターサイズとより多くのオブジェクト数に到達できる可能性があります。ただし、インフラストラクチャーノードのサイズによって、Prometheus で利用できるメモリー量が制限されます。オブジェクトの作成、変更、または削除時に、Prometheus はメトリクスをそのメモリーに保存してから、ディスクでメトリクスを永続化する前に 3 時間保存されます。オブジェクトの作成、変更、削除のレートが高すぎると、Prometheus はメモリーリソースがないために負荷がかかり、失敗する可能性があります。

3.3. コントロールプレーンとインフラストラクチャーノードのサイズ設定とスケーリング

Red Hat OpenShift Service on AWS (ROSA) クラスターをインストールすると、コントロールプレーンとインフラストラクチャーノードのサイズは、計算ノードの数によって自動的に決定されます。

インストール後にクラスター内の計算ノードの数を変更した場合、Red Hat サイト信頼性エンジニアリング (SRE) チームは、クラスターの安定性を維持するために、必要に応じてコントロールプレーンとインフラストラクチャーノードをスケーリングします。

3.3.1. インストール中のノードのサイズ設定

インストールプロセス中に、コントロールプレーンとインフラストラクチャーノードのサイズが動的に計算されます。サイズ計算は、クラスター内の計算ノードの数に基づいています。

次の表に、インストール中に適用されるコントロールプレーンとインフラストラクチャーノードのサイズを示します。

コンピュートノードの数	コントロールプレーンのサイズ	インフラストラクチャーノードのサイズ
1 から 25	m5.2xlarge	r5.xlarge
26 から 100	m5.4xlarge	r5.2xlarge
101 から 180 [1]	m5.8xlarge	r5.4xlarge

1. ROSA のコンピュートノードの最大数は 180 です。

3.3.2. インストール後のノードのスケーリング

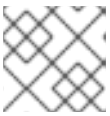
インストール後にコンピュートノードの数を変更した場合、コントロールプレーンとインフラストラクチャーノードは、必要に応じて Red Hat サイト信頼性エンジニアリング (SRE) チームによってスケーリングされます。ノードは、プラットフォームの安定性を維持するためにスケーリングされます。

コントロールプレーンおよびインフラストラクチャーノードのインストール後のスケーリング要件は、ケースごとに評価されます。ノードリソースの消費および受信アラートの考慮が行われます。

コントロールプレーンノードのサイズ変更のアラートのルール

以下のシナリオのいずれかが true の場合に、クラスターのコントロールプレーンノードについてアラートのサイズ変更がトリガーされます。

- 各コントロールプレーンノードは 16GiB RAM 未満で、25 未満のコンピュートノードは 101 未満です。
- 各コントロールプレーンノードの RAM は 32GiB 未満であり、100 を超える計算ノードがあります。



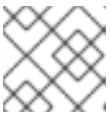
注記

ROSA のコンピュートノードの最大数は 180 です。

インフラストラクチャーノードのサイズ変更アラートのルール

以下のシナリオのいずれかが該当する場合、クラスターのインフラストラクチャーノードについてアラートのサイズ変更がトリガーされます。

- 各インフラストラクチャーノードは 16GiB 以下の RAM または 5 未満の CPU 未満で、101 台未満のコンピュートノードは 25 未満です。
- 各インフラストラクチャーノードの RAM は 32GiB 未満または CPU は 9 未満であり、計算ノードは 100 を超えています。



注記

ROSA のコンピュートノードの最大数は 180 です。

SRE チームは、ノードでのリソース消費の増加を管理するなど、追加の理由でコントロールプレーンとインフラストラクチャーノードをスケーリングする場合があります。

スケーリングが適用されると、サービスログエントリーを通じて顧客に通知されます。サービスログの詳細については、**ROSA クラスターのサービスログへのアクセス** を参照してください。

3.3.3. 大規模なクラスターのサイズに関する考慮事項

大規模なクラスターの場合、インフラストラクチャーノードのサイズ設定はスケーラビリティーに大きな影響を与える要因になる可能性があります。指定のしきい値に影響を与える要因には、etcd バージョンやストレージデータ形式などの多数の要因があります。

これらの制限を超えても、クラスターが障害が発生するとは限りません。ほとんど場合、これらの制限値を超えると、パフォーマンスが全体的に低下します。

3.4. 次のステップ

- 環境のプランニング

3.5. 関連情報

- ROSA クラスターのサービスログへのアクセス

第4章 環境のプランニング

4.1. テスト済みのクラスターの最大値に基づく環境計画

本書では、テスト済みのクラスターの最大値に基づいて、AWS での Red Hat OpenShift Service 環境をプランニングする方法を説明します。

ノード上で物理リソースを過剰にサブスクライブすると、Kubernetes スケジューラーが Pod の配置時に行うリソースの保証に影響が及びます。メモリースワップを防ぐために実行できる処置について確認してください。

一部のテスト済みの最大値については、単一の namespace/ユーザーが作成するオブジェクトでのみ変更されます。これらの制限はクラスター上で数多くのオブジェクトが実行されている場合には異なります。

本書に記載されている数は、Red Hat のテスト方法、セットアップ、設定、およびチューニングに基づいています。これらの数は、独自のセットアップおよび環境に応じて異なります。

環境の計画時に、以下の式を使用して、ノードに配置できる Pod の数を判別します。

```
required pods per cluster / pods per node = total number of nodes needed
```

ノードあたりの現在の Pod の最大数は 250 です。ただし、ノードに適合する Pod 数はアプリケーション自体によって異なります。**アプリケーション要件を基にした環境計画** で説明されているように、アプリケーションのメモリー、CPU、およびストレージ要件を検討してください。

シナリオ例

クラスターごとに 2200 の Pod のあるクラスターのスコープを設定する場合、ノードごとに最大 250 の Pod があることを前提として、最低でも 9 つのノードが必要になります。

```
2200 / 250 = 8.8
```

ノード数を 20 に増やす場合は、Pod 配分がノードごとに 110 の Pod に変わります。

```
2200 / 20 = 110
```

詳細は以下のようになります。

```
required pods per cluster / total number of nodes = expected pods per node
```

4.2. アプリケーション要件に基づく環境計画

本書では、アプリケーション要件に応じて AWS 上の Red Hat OpenShift Service 環境をプランニングする方法を説明します。

アプリケーション環境の例を考えてみましょう。

Pod タイプ	Pod 数	最大メモリー	CPU コア数	永続ストレージ
apache	100	500 MB	0.5	1 GB

Pod タイプ	Pod 数	最大メモリー	CPU コア数	永続ストレージ
node.js	200	1 GB	1	1 GB
postgresql	100	1 GB	2	10 GB
JBoss EAP	100	1 GB	1	1 GB

推定要件: CPU コア 550 個、メモリー 450 GB、および 1.4 TB ストレージ

ノードのインスタンスサイズは、希望に応じて増減を調整できます。ノードのリソースはオーバーコミットされることが多く、デプロイメントシナリオでは、小さいノードで数を増やしたり、大きいノードで数を減らしたりして、同じリソース量を提供することもできます。このデプロイメントシナリオでは、小さいノードで数を増やしたり、大きいノードで数を減らしたりして、同じリソース量を提供することもできます。運用上の敏捷性やインスタンスあたりのコストなどの要因を考慮する必要があります。

ノードのタイプ	数量	CPU	RAM (GB)
ノード (オプション 1)	100	4	16
ノード (オプション 2)	50	8	32
ノード (オプション 3)	25	16	64

アプリケーションによってはオーバーコミットの環境に適しているものもあれば、そうでないものもあります。たとえば、Java アプリケーションや Huge Page を使用するアプリケーションの多くは、オーバーコミットに対応できません。対象のメモリーは、他のアプリケーションに使用できません。上記の例では、環境は一般的な比率として約 30 % オーバーコミットされています。

アプリケーション Pod は環境変数または DNS のいずれかを使用してサービスにアクセスできます。環境変数を使用する場合、それぞれのアクティブなサービスについて、変数が Pod がノードで実行される際に kubelet によって挿入されます。クラスター対応の DNS サーバーは、Kubernetes API で新規サービスの有無を監視し、それぞれに DNS レコードのセットを作成します。DNS がクラスター全体で有効にされている場合、すべての Pod は DNS 名でサービスを自動的に解決できるはずです。DNS を使用したサービス検出は、5000 サービスを超える使用できる場合があります。サービス検出に環境変数を使用し、namespace で 5000 サービスを超える場合に引数の一覧が許可される長さを超えると、Pod およびデプロイメントが失敗し始めます。

デプロイメントのサービス仕様ファイルのサービスリンクを無効にして、以下を解消します。

例

```
Kind: Template
apiVersion: template.openshift.io/v1
metadata:
  name: deploymentConfigTemplate
  creationTimestamp:
  annotations:
    description: This template will create a deploymentConfig with 1 replica, 4 env vars and a service.
    tags: ''
```

```
objects:
  - kind: DeploymentConfig
    apiVersion: apps.openshift.io/v1
    metadata:
      name: deploymentconfig${IDENTIFIER}
    spec:
      template:
        metadata:
          labels:
            name: replicationcontroller${IDENTIFIER}
        spec:
          enableServiceLinks: false
          containers:
          - name: pause${IDENTIFIER}
            image: "${IMAGE}"
            ports:
            - containerPort: 8080
              protocol: TCP
            env:
            - name: ENVVAR1_${IDENTIFIER}
              value: "${ENV_VALUE}"
            - name: ENVVAR2_${IDENTIFIER}
              value: "${ENV_VALUE}"
            - name: ENVVAR3_${IDENTIFIER}
              value: "${ENV_VALUE}"
            - name: ENVVAR4_${IDENTIFIER}
              value: "${ENV_VALUE}"
            resources: {}
            imagePullPolicy: IfNotPresent
            capabilities: {}
            securityContext:
              capabilities: {}
              privileged: false
          restartPolicy: Always
          serviceAccount: ''
      replicas: 1
      selector:
        name: replicationcontroller${IDENTIFIER}
      triggers:
      - type: ConfigChange
      strategy:
        type: Rolling
  - kind: Service
    apiVersion: v1
    metadata:
      name: service${IDENTIFIER}
    spec:
      selector:
        name: replicationcontroller${IDENTIFIER}
      ports:
      - name: serviceport${IDENTIFIER}
        protocol: TCP
        port: 80
        targetPort: 8080
      portalIP: ''
      type: ClusterIP
```

```
      sessionAffinity: None
    status:
      loadBalancer: {}
  parameters:
  - name: IDENTIFIER
    description: Number to append to the name of resources
    value: '1'
    required: true
  - name: IMAGE
    description: Image to use for deploymentConfig
    value: gcr.io/google-containers/pause-amd64:3.0
    required: false
  - name: ENV_VALUE
    description: Value to use for environment variables
    generate: expression
    from: "[A-Za-z0-9]{255}"
    required: false
  labels:
template: deploymentConfigTemplate
```

namespace で実行できるアプリケーション Pod の数は、環境変数がサービス検出に使用される場合にサービスの数およびサービス名の長さによって異なります。システムの **ARG_MAX** は、新規プロセスの引数の最大の長さを定義し、デフォルトで 2097152 KiB に設定されます。kubelet は、以下を含む namespace で実行するようにスケジュールされる各 Pod に環境変数を挿入します。

- **<SERVICE_NAME>_SERVICE_HOST=<IP>**
- **<SERVICE_NAME>_SERVICE_PORT=<PORT>**
- **<SERVICE_NAME>_PORT=tcp://<IP>:<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP=tcp://<IP>:<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_PROTO=tcp**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_PORT=<PORT>**
- **<SERVICE_NAME>_PORT_<PORT>_TCP_ADDR=<ADDR>**

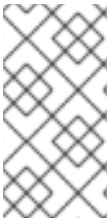
引数の長さが許可される値を超え、サービス名の文字数がこれに影響を及ぼす場合は、namespace の Pod が起動に失敗し始めます。

第5章 必要な AWS サービスクォータ

Red Hat OpenShift Service on AWS クラスターの実行に必要な Amazon Web Service (AWS) サービスクォータの一覧を確認します。

5.1. 必要な AWS サービスクォータ

以下の表は、Red Hat OpenShift Service on AWS クラスターを作成し、実行するために必要な AWS サービスクォータおよびレベルを説明します。



注記

AWS SDK は ROSA がクォータの確認を可能にしますが、AWS SDK 計算には既存の使用が含まれません。そのため、クォータチェックが AWS SDK で合格しても、クラスターの作成が失敗する可能性があります。この問題を修正するには、クォータを増やします。

特定のクォータを変更または増やす必要がある場合は、Amazon のドキュメントの requesting a quota inscrease を参照してください。

クォータ名	サービスコード	クォータコード	最小の必要な値	推奨される値
EIP 数 - VPC EIP	ec2	L-0263D0A3	5	5
オンデマンド標準 (A、C、D、H、I、M、R、T、Z) インスタンスの実行	ec2	L-1216C47A	100	100
リージョンあたりの VPC	vpc	L-F678F1CE	5	5
リージョンあたりのインターネットゲートウェイ	vpc	L-A4707A72	5	5
リージョンごとのネットワークインターフェイス	vpc	L-DF5E4CA3	5,000	5,000
汎用 SSD (gp2) ボリュームストレージ	ebs	L-D18FCD1D	50	300
EBS スナップショットの数	ebs	L-309BACF6	300	300
プロビジョニングされた IOPS	ebs	L-B3A130E6	300,000	300,000

クォータ名	サービスコード	クォータコード	最小の必要な値	推奨される値
プロビジョニングされた IOPS SSD (io1) ボリュームストレージ	ebs	L-FD252861	50	300
リージョンあたりのアプリケーションロードバランサー	elasticloadbalancing	L-53DA6B97	50	50
リージョンあたりの Classic Load Balancer	elasticloadbalancing	L-E9E9831D	20	20

5.2. 次のステップ

- 環境の設定および ROSA のインストール

第6章 STS を使用するための環境の設定

AWS の前提条件を満たしていることを確認した後に、環境を設定し、Red Hat OpenShift Service on AWS (ROSA) をインストールします。

ヒント

AWS Security Token Service (STS) は、セキュリティーが強化されているため、Red Hat OpenShift Service on AWS (ROSA) にクラスターをインストールして操作するのに推奨される認証情報モードです。

6.1. STS のための環境の設定

AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する前に、次の手順を実行して環境をセットアップします。

前提条件

- デプロイメントの前提条件およびポリシーを確認し、完了している。
- Red Hat アカウント がない場合は作成している。次に、確認リンクについてのメールを確認する。ROSA をインストールするには認証情報が必要です。

手順

1. 使用する Amazon Web Services (AWS) アカウントにログインします。
   実稼働クラスターを実行するには、専用の AWS アカウントを使用することが推奨されます。AWS Organizations を使用している場合は、組織内の AWS アカウントを使用するか、アカウントを新規作成 できます。

   AWS Organizations を使用しており、使用する予定の AWS アカウントにサービスコントロールポリシー (SCP) を適用する必要がある場合、これらのポリシーは、クラスターが必要とするロールおよびポリシーよりも制限的なものである必要はありません。

2. AWS マネジメントコンソールで ROSA サービスを有効にします。

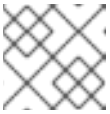
   a. AWS アカウント にサインインします。

   b. ROSA を有効にするには、ROSA service に移動し、**Enable OpenShift** を選択します。

3. AWS CLI をインストールし、設定します。

   a. AWS コマンドラインインターフェイスのドキュメントを参照し、オペレーティングシステムの AWS CLI を インストール し、設定 します。
   .aws/credentials ファイルで正しい **aws_access_key_id** および **aws_secret_access_key** を指定します。AWS ドキュメントの AWS 設定の基本 を参照してください。

   b. デフォルトの AWS リージョンを設定します。

   注記

   環境変数を使用してデフォルトの AWS リージョンを設定できます。

   ROSA は以下の優先順位でリージョンを評価します。

i. **--region** フラグを指定して **rosa** コマンドを実行する際に指定されるリージョン。

ii. **AWS_DEFAULT_REGION** 環境変数に設定されるリージョン。AWS ドキュメントの Environment variables to configure the AWS CLI を参照してください。

iii. AWS 設定ファイルで設定されるデフォルトのリージョン。AWS ドキュメントの Quick configuration with aws configure を参照してください。

c. オプション: AWS の名前付きプロファイルを使用して AWS CLI 設定および認証情報を設定します。**rosa** は以下の優先順位で AWS の名前付きプロファイルを評価します。

i. **rosa** コマンドを **--profile** フラグを指定して実行する場合に指定されるプロファイル。

ii. **AWS_PROFILE** 環境変数に設定されるプロファイル。AWS ドキュメントの Named profiles を参照してください。

d. 以下のコマンドを実行して AWS API をクエリーし、AWS CLI がインストールされ、正しく設定されていることを確認します。

```
$ aws sts get-caller-identity
```

4. ROSA CLI の最新バージョン (**rosa**) をインストールします。

a. お使いのオペレーティングシステム用の **rosa** CLI の 最新リリース をダウンロードします。

b. オプション: **rosa** にダウンロードしたファイルの名前を変更し、ファイルを実行可能にします。本書では、**rosa** を使用して実行可能ファイルを参照します。

```
$ chmod +x rosa
```

c. オプション: **rosa** をパスに追加します。

```
$ mv rosa /usr/local/bin/rosa
```

d. 以下のコマンドを実行して、インストールを確認します。

```
$ rosa
```

出力例

```
Command line tool for ROSA.

Usage:
  rosa [command]

Available Commands:
  completion  Generates bash completion scripts
  create      Create a resource from stdin
  delete      Delete a specific resource
  describe    Show details of a specific resource
  edit        Edit a specific resource
  help        Help about any command
  init        Applies templates to support Managed OpenShift on AWS clusters
  list        List all resources of a specific type
```

```
  login       Log in to your Red Hat account
  logout      Log out
  logs        Show logs of a specific resource
  verify      Verify resources are configured correctly for cluster install
  version     Prints the version of the tool

Flags:
      --debug     Enable debug mode.
  -h, --help      help for rosa
  -v, --v Level   log level for V logs

Use "rosa [command] --help" for more information about a command.
```

e. **rosa** CLI のコマンド補完スクリプトを生成します。以下の例では、Linux マシン用の Bash 補完スクリプトを生成します。

```
$ rosa completion bash | sudo tee /etc/bash_completion.d/rosa
```

f. 既存のターミナルから **rosa** コマンドの補完を可能にするためのスクリプトを作成します。以下の例では、Linux マシン上で **rosa** の Bash 補完スクリプトをソースとして使用しています。

```
$ source /etc/bash_completion.d/rosa
```

5. **rosa** CLI で Red Hat アカウントにログインします。

a. 以下のコマンドを入力します。

```
$ rosa login
```

b. **<my_offline_access_token>** をトークンに置き換えます。

出力例

```
To login to your Red Hat account, get an offline access token at
https://console.redhat.com/openshift/token/rosa
? Copy the token and paste it here: <my-offline-access-token>
```

出力例

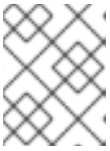
```
I: Logged in as '<rh-rosa-user>' on 'https://api.openshift.com'
```

6. AWS アカウントに ROSA クラスターをデプロイするために必要なクォータがあることを確認します。

```
$ rosa verify quota [--region=<region>]
```

出力例

```
I: Validating AWS quota...
I: AWS quota ok
```



注記

AWS クォータはリージョンによって異なる場合があります。エラーが発生した場合は、別のリージョンを試してください。

クォータを増やす必要がある場合は、AWS 管理コンソール に移動して、失敗したサービスのクォータの増加をリクエストします。

クォータの確認に成功したら、次のステップに進みます。

7. クラスターデプロイメント用に AWS アカウントを準備します。

   a. 以下のコマンドを実行して、Red Hat および AWS の認証情報が正しく設定されていることを確認します。AWS アカウント ID、デフォルトのリージョンおよび ARN が予想される内容と一致していることを確認します。現時点では、OpenShift Cluster Manager で始まる行は無視しても問題ありません。

   ```
   $ rosa whoami
   ```

   出力例

   ```
   AWS Account ID:               000000000000
   AWS Default Region:           us-east-1
   AWS ARN:                      arn:aws:iam::000000000000:user/hello
   OCM API:                      https://api.openshift.com
   OCM Account ID:               1DzGIdIhqEWyt8UUXQhSoWaaaaa
   OCM Account Name:             Your Name
   OCM Account Username:         you@domain.com
   OCM Account Email:            you@domain.com
   OCM Organization ID:          1HopHfA2hcmhup5gCr2uH5aaaaa
   OCM Organization Name:        Red Hat
   OCM Organization External ID: 0000000
   ```

8. ROSA (**rosa**) CLI から OpenShift CLI (**oc**) バージョン 4.7.9 以降をインストールします。

   a. 以下のコマンドを入力して、最新バージョンの **oc** CLI をダウンロードします。

   ```
   $ rosa download openshift-client
   ```

   b. **oc** CLI をダウンロードした後に、これを展開し、パスに追加します。

   c. 以下のコマンドを実行して、**oc** CLI が正常にインストールされていることを確認します。

   ```
   $ rosa verify openshift-client
   ```

ロールの作成

これらの手順を完了したら、IAM および OIDC アクセスベースのロールをセットアップできます。

6.2. 次のステップ

- STS をすばやく使用して ROSA クラスターを作成する か、カスタマイズを使用してクラスターを作成します。

6.3. 関連情報

- AWS 前提条件
- 必要な AWS サービスクォータおよび要求の増加