Red Hat OpenShift Service on AWS 4

スタートガイド

クラスターおよびアカウントの設定

Last Updated: 2022-11-20

Red Hat OpenShift Service on AWS 4 スタートガイド

クラスターおよびアカウントの設定

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.

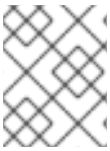
法律上の通知

概要

本書では、Red Hat OpenShift Service on AWS (ROSA) クラスターを開始する方法を説明します。

目次

第1章 RED HAT OPENSHIFT SERVICE ON AWS クイックスタートガイド



注記

ROSA の包括的な入門ガイドをお探しの場合は、Red Hat OpenShift Service on AWS の使用を開始するための包括的なガイド を参照してください。

このガイドに従って、Red Hat OpenShift Cluster Manager Hybrid Cloud Console を使用してすぐに Red Hat OpenShift Service on AWS (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を行い、ユーザーアクセスを取り消してクラスターの削除する方法を学びます。

このドキュメントの手順では、AWS Security Token Service (STS) を使用するクラスターを作成できます。ROSA クラスターで AWS STS を使用する方法は、AWS Security Token Service の使用 を参照してください。

1.1. 前提条件

- Red Hat OpenShift Service on AWS(ROSA) の概要 、および ROSA アーキテクチャーモデルおよびアーキテクチャー の 概念 を確認している。
- 制限およびスケーラビリティーに関するドキュメント と、環境の計画に関するガイドライン を確認している。
- STS を使用した ROSA の詳細な AWS の前提条件 を確認している。
- ROSA クラスターの実行に必要な AWS サービスクォータ がある。

1.2. 環境の設定

Red Hat OpenShift Service on AWS(ROSA) クラスターを作成する前に、以下のタスクを実行して環境を設定する必要があります。

- AWS アカウントで ROSA を有効化する
- 必要なコマンドラインインターフェイス (CLI) ツールをインストールして設定する
- CLI ツールの設定を確認する
- AWS Elastic Load Balancing (ELB) サービ出力ルが存在することを確認する
- 必要な AWS リソースクォータが利用可能であることを確認する

本セクションの手順に従って、これらの設定要件を完了できます。

AWS アカウントでの ROSA の有効化

以下の手順に従って、AWS アカウントで Red Hat OpenShift Service on AWS (ROSA) を有効にします。

前提条件

- AWS アカウントを作成している。

注記

専用の AWS アカウントを使用して実稼働クラスターを実行することを検討してください。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。

手順

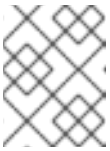
1. AWS 管理コンソール にログインします。
2. ROSA サービス に移動して、**Enable OpenShift** を選択して、AWS アカウントで ROSA を有効にします。

必要な CLI ツールのインストールと設定

次の手順を使用して、ワークステーションにインストールして設定します。

手順

1. 最新の AWS CLI (**aws**) をインストールして設定します。
   a. AWS コマンドラインインターフェイス ドキュメントに従って、お使いのオペレーティングシステム用の AWS CLI をインストールし、設定します。
   .aws/credentials ファイルに **aws_access_key_id**、**aws_secret_access_key**、および **region** 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。



注記

AWS_DEFAULT_REGION 環境変数を使用して、デフォルトの AWS リージョンを設定することもできます。

   b. AWS API をクエリーし、AWS CLI が適切にインストールおよび設定されているかどうかを確認します。

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

出力例

```
<aws_account_id>  arn:aws:iam::<aws_account_id>:user/<username>  <aws_user_id>
```

2. 最新の ROSA CLI (**rosa**) をインストールし、設定します。
   a. Red Hat OpenShift Cluster Manager Hybrid Cloud Console の **ダウンロード** ページから、オペレーティングシステム用の **rosa** CLI の最新バージョンをダウンロードします。
   b. ダウンロードしたアーカイブから **rosa** バイナリーファイルを展開します。以下の例は、Linux tar アーカイブからバイナリーを展開します。

```
$ tar xvf rosa-linux.tar.gz
```

   c. パスに **rosa** を加えてください。以下の例では、**/usr/local/bin** ディレクトリーがユーザーのパスに含まれます。

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

d. **rosa** バージョンをクエリーして、**rosa** CLI ツールが適切にインストールされていることを確認します。

```
$ rosa version
```

出力例

```
1.2.8
```

e. **rosa** CLI を使用して Red Hat アカウントにログインしました。

```
$ rosa login
```

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:
```

コマンド出力に一覧表示されている URL に移動し、オフラインアクセストークンを取得します。ログインする CLI プロンプトでトークンを指定します。

注記

その後に **rosa login** コマンドの実行時に **--token="<offline_access_token>"** 引数を使用してオフラインアクセストークンを指定できます。

f. 正常にログインできるかどうかを確認し、認証情報を確認します。

```
$ rosa whoami
```

出力例

```
AWS Account ID:               <aws_account_number>
AWS Default Region:           us-east-1
AWS ARN:                      arn:aws:iam::<aws_account_number>:user/<aws_user_name>
OCM API:                      https://api.openshift.com
OCM Account ID:               <red_hat_account_id>
OCM Account Name:             Your Name
OCM Account Username:         you@domain.com
OCM Account Email:            you@domain.com
OCM Organization ID:          <org_id>
OCM Organization Name:        Your organization
OCM Organization External ID: <external_org_id>
```

次に進む前に、出力の情報が正しいことを確認します。

ELB サービス出力の作成

AWSServiceRoleForElasticLoadBalancing AWS Elastic Load Balancing (ELB) サービス出力が存在するかどうかを確認し、存在しない場合には作成します。

注記

Error creating network Load Balancer: AccessDenied: AWS ELB サービス出力ルなしで Red Hat OpenShift Service on AWS (ROSA) クラスターを作成しようとすると生成されます。

手順

1. AWS アカウントに **AWSServiceRoleForElasticLoadBalancing** ロールが存在するかどうかを確認します。

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

出力例

以下の出力例では、ロールが存在することを確認します。

```
ROLE    arn:aws:iam::<aws_account_number>:role/aws-service-
role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing  2018-
09-27T19:49:23+00:00        Allows ELB to call AWS services on your behalf. 3600       /aws-
service-role/elasticloadbalancing.amazonaws.com/   <role_id>
AWSServiceRoleForElasticLoadBalancing
ASSUMEROLEPOLICYDOCUMENT        2012-10-17
STATEMENT       sts:AssumeRole  Allow
PRINCIPAL       elasticloadbalancing.amazonaws.com
ROLELASTUSED    2022-01-06T09:27:57+00:00       us-east-1
```

2. AWS ELB サービス出力ルが存在しない場合は、作成します。

```
$ aws iam create-service-linked-role --aws-service-name
"elasticloadbalancing.amazonaws.com"
```

AWS クォータの空きの確認

必要なリソースクォータがデフォルトの AWS リージョンのアカウントで利用可能であることを確認します。

手順

1. 必要なリソースクォータがデフォルトのリージョンで利用可能かどうかを確認します。

```
$ rosa verify quota
```

出力例

```
I: Validating AWS quota...
I: AWS quota ok. If cluster installation fails, validate actual AWS resource usage against
https://docs.openshift.com/rosa/rosa_getting_started/rosa-required-aws-service-quotas.html
```

1.3. デフォルトの自動モードを使用した AWS STS での ROSA クラスターの作成

このドキュメントの手順では、OpenShift Cluster Manager Hybrid Cloud Console の **自動** モードを使用して、現在の AWS アカウントで、必要な Identity and Access Management (IAM) リソースをすぐに作

成します。必要なリソースには、アカウント全体の IAM ロールおよびポリシー、クラスター固有の Operator ロール、ならびに OpenID Connect (OIDC) ID プロバイダーが含まれます。

OpenShift Cluster Manager Hybrid Cloud Console で、STS を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する場合に、デフォルトのオプションを選択するとクラスターをすばやく作成できます。

OpenShift Cluster Manager Hybrid Cloud Console を使用して STS クラスターで ROSA をデプロイする前に、AWS アカウントを Red Hat 組織に関連付け、必要なアカウント全体の STS ロールおよびポリシーを作成する必要があります。

デフォルトのクラスター仕様の概要

デフォルトのインストールオプションを使用して、AWS Security Token Service (STS) で Red Hat OpenShift Service on AWS (ROSA) クラスターをすばやく作成できます。次の要約では、デフォルトのクラスター仕様について説明します。

表1.1 STS クラスター仕様のデフォルト ROSA

コンポーネント	デフォルトの仕様
アカウントおよびロール	• デフォルトの IAM ロールの接頭辞: **ManagedOpenShift**
クラスター設定	• デフォルトのクラスターバージョン: 最新 • Red Hat OpenShift Cluster Manager Hybrid Cloud Console を使用したインストール用のデフォルトの AWS リージョン: us-east-1 (US East, North Virginia) • **rosa** CLI を使用したインストールのデフォルトの AWS リージョン:**aws** CLI 設定によって定義される • 可用性: 単一ゾーン • ユーザー定義プロジェクトの監視: 有効
暗号化	• クラウドストレージは保存時に暗号化される • 追加の etcd 暗号化が有効になっていない • デフォルトの AWS Key Management Service (KMS) キーは、永続データの暗号化キーとして使用される
コントロールプレーンノードの設定	• コントロールプレーンノードのインスタンスタイプ: m5.x2large (8 vCPU, 32 GiB RAM) • コントロールプレーンノード数: 3

コンポーネント	デフォルトの仕様
インフラストラクチャーノードの設定	• インフラストラクチャーノードインスタンスタイプ: r5.xlarge (4 vCPU, 32 GiB RAM) • インフラストラクチャーノード数: 2
コンピュートノードマシンプール	• コンピュートノードインスタンスタイプ: m5.xlarge (4 vCPU 16, GiB RAM) • コンピュートノード数: 2 • 自動スケーリング: 無効 • 追加のノードラベルなし
ネットワーク設定	• クラスターのプライバシー: パブリック • クラスター用の新しい VPC が作成される • クラスター全体のプロキシーは設定されていない
Classless Inter-Domain Routing (CIDR) の範囲	• Machine CIDR: 10.0.0.0/16 • Service CIDR: 172.30.0.0/16 • Pod CIDR: 10.128.0.0/16 • Host prefix: /23
クラスターのロールおよびポリシー	• Operator ロールおよび OpenID Connect (OIDC) プロバイダーの作成に使用されるモード: **auto**  **注記** OpenShift Cluster Manager Hybrid Cloud Console Hybrid Cloud Console を使用したインストールの場合、**自動** モードには管理者特権の OpenShift Cluster Manager ロールが必要です。 • デフォルトの Operator ロールの接頭辞: **<cluster_name>-<4_digit_random_string>**
クラスター更新戦略	• 個別の更新 • ノードドレインの 1 時間の猶予期間

AWS アカウントの関連付けについて

Red Hat OpenShift Cluster Manager Hybrid Cloud Console を使用して、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、AWS アカウントを Red Hat 組織に関連付ける必要があります。次の IAM ロールを作成してリンクすることで、アカウントを関連付けることができます。

OpenShift Cluster Manager ロール

OpenShift Cluster Manager IAM ロールを作成し、Red Hat 組織にリンクします。
基本権限または管理権限を OpenShift Cluster Manager ロールに適用できます。基本的なアクセス許可により、OpenShift Cluster Manager Hybrid Cloud Console を使用したクラスターのメンテナンスが可能になります。管理パーミッションにより、OpenShift Cluster Manager Hybrid Cloud Console を使用して、クラスター固有の Operator ロールおよび OpenID Connect (OIDC) プロバイダーの自動デプロイが可能になります。

User role

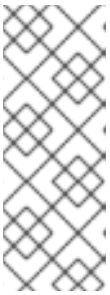
ユーザー IAM ロールを作成し、Red Hat ユーザーアカウントにリンクします。Red Hat ユーザーアカウントは、OpenShift Cluster Manager ロールにリンクされている Red Hat 組織に存在する必要があります。
ユーザーロールは、OpenShift Cluster Manager Hybrid Cloud Console を使用してクラスターと必要な STS リソースをインストールするときに、AWS Identity を確認するために Red Hat によって使用されます。

AWS アカウントを Red Hat 組織に関連付ける

Red Hat OpenShift Cluster Manager Hybrid Cloud Console を使用して、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、OpenShift Cluster Manager IAM ロールを作成し、Red Hat 組織にリンクします。次に、ユーザー IAM ロールを作成し、同じ Red Hat 組織内の Red Hat ユーザーアカウントにリンクします。

手順

1. OpenShift Cluster Manager ロールを作成し、Red Hat 組織にリンクします。



注記

OpenShift Cluster Manager Hybrid Cloud Console を使用してクラスター固有の Operator ロールと OpenID Connect (OIDC) プロバイダーの自動デプロイを有効にするには、ROSA クラスターの作成の **アカウントとロール** の手順で、**Admin OCM role** コマンドを選択して、ロールに管理権限を適用する必要があります。OpenShift Cluster Manager ロールの基本権限および管理権限の詳細については、**AWS アカウントの関連付けについて** を参照してください。

注記

OpenShift Cluster Manager Hybrid Cloud Console で ROSA クラスターを作成する **アカウントとロール** の手順で **Basic OCM role** コマンドを選択した場合は、手動モードを使用して ROSA クラスターをデプロイする必要があります。後のステップで、クラスター固有の Operator ロールと OpenID Connect (OIDC) プロバイダーを設定するように求められます。

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

ロールをすばやく作成してリンクするには、プロンプトでデフォルト値を選択します。

2. ユーザーロールを作成し、それを OpenShift Cluster Manager ユーザーアカウントにリンクします。

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

プロンプトでデフォルト値を選択して、ロールをすばやく作成してリンクします

注記

Red Hat ユーザーアカウントは、OpenShift Cluster Manager ロールにリンクされている Red Hat 組織に存在する必要があります。

アカウント全体の STS ロールおよびポリシーの作成

Red Hat OpenShift Cluster Manager Hybrid Cloud Console を使用して 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、Operator ポリシーを含む、必要なアカウント全体の STS ロールおよびポリシーを作成します。

手順

1. それらが AWS アカウントに存在しない場合は、アカウント全体の STS ロールとポリシーで必要なものを作成します。

```
$ rosa create account-roles
```

プロンプトでデフォルト値を選択して、ロールとポリシーをすばやく作成します。

OpenShift Cluster Manager Hybrid Cloud Console を使用したデフォルトオプションでのクラスターの作成

Red Hat OpenShift Cluster Manager Hybrid Cloud Console で 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場合、デフォルトのオプションを選択するとクラスターをすばやく作成できます。管理 OpenShift Cluster Manager IAM ロールを使用して、クラスター固有の Operator ロールおよび OpenID Connect (OIDC) プロバイダーの自動デプロイメントを有効にすることもできます。

手順

1. OpenShift Cluster Manager Hybrid Cloud Console に移動し、**Create cluster** を選択します。
2. **Create an OpenShift cluster** ページの **Red Hat OpenShift Service on AWS (ROSA)** 行で **Create cluster** を選択します。
3. AWS アカウント ID が **Associated AWS accounts** ドロップダウンメニューに表示されていること、およびインストーラー、サポート、ワーカー、およびコントロールプレーンのアカウントロールの Amazon Resource Names (ARN) が **Accounts and roles** ページに表示されていることを確認します。

注記

AWS アカウント ID が表示されていない場合は、AWS アカウントが Red Hat 組織に正常に関連付けられていることを確認してください。アカウントロール ARN が表示されていない場合は、必要なアカウント全体の STS ロールが AWS アカウントに存在することを確認してください。

4. **Next** をクリックします。

5. **Cluster details** ページで、**Cluster name** を指定します。残りのフィールドはデフォルト値のままにして、**Next** をクリックします。

6. クラスターをすばやくデプロイするには、**Cluster settings**、**Networking**、**Cluster roles and policies**、および **Cluster updates** ページのデフォルトのオプションをそのままにして、各ページで **Next** をクリックします。

7. **Review your ROSA cluster**確認ページで、選択内容の概要を確認し、**Create cluster** をクリックしてインストールを開始します。

検証

- クラスターの **Overview** ページで、インストールの進捗をモニターできます。同じページでインストールのログを表示できます。そのページの **Details** セクションの **Status** が **Ready** として表示されると、クラスターは準備が完了した状態になります。

注記

インストールが失敗するか、約 40 分経ってもクラスターの **状態** が **Ready** に変わらない場合は、インストールのトラブルシューティングのドキュメントで詳細を確認してください。詳細は、**インストールのトラブルシューティング**を参照してください。Red Hat サポートにサポートを依頼する手順は、**Red Hat OpenShift Service on AWS のサポートを受ける**を参照してください。

1.4. クラスターにすぐアクセスできるようにクラスター管理者ユーザーの作成

アイデンティティープロバイダーを設定する前に、**cluster-admin** 権限のあるユーザーを作成して、Red Hat OpenShift Service on AWS (ROSA) クラスターへすぐにアクセスできるようにします。

注記

クラスター管理者ユーザーは、新たにデプロイされたクラスターにすぐアクセスが必要な場合に役立ちます。ただし、アイデンティティープロバイダーを設定し、必要に応じてクラスター管理者権限をアイデンティティープロバイダーユーザーに付与することを検討してください。ROSA クラスターのアイデンティティープロバイダーの設定の詳細は、**アイデンティティープロバイダーの設定およびクラスターのアクセスの付与** を参照してください。

手順

1. クラスター管理者ユーザーを作成します。

```
$ rosa create admin --cluster=<cluster_name> 1
```

1 **<cluster_name>** は、クラスター名に置き換えます。

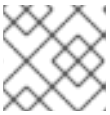
出力例

```
W: It is recommended to add an identity provider to login to this cluster. See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster '<cluster_name>'.
I: Please securely store this generated password. If you lose this password you can delete
```

```
and recreate the cluster admin user.
I: To login, run the following command:

   oc login https://api.example-cluster.wxyz.p1.openshiftapps.com:6443 --username cluster-admin --password d7Rca-Ba4jy-YeXhs-WU42J

I: It may take up to a minute for the account to become active.
```



注記

cluster-admin ユーザーがアクティブになるまで約1分かかる場合があります。

関連情報

- ROSA Web コンソールにログインする手順は、Web コンソールを使用したクラスターへのアクセス を参照してください。

1.5. アイデンティティープロバイダーの設定およびクラスターアクセスの付与

Red Hat OpenShift Service on AWS (ROSA) には、ビルトイン OAuth サーバーが含まれます。ROSA クラスターの作成後に、OAuth をアイデンティティープロバイダーを使用するように設定する必要があります。その後、メンバーを設定済みのアイデンティティープロバイダーに追加して、クラスターへのアクセス権限を付与できます。

また、必要に応じて、アイデンティティープロバイダーユーザーに **cluster-admin** 権限または **dedicated-admin** 権限を付与することもできます。

アイデンティティープロバイダーの設定

Red Hat OpenShift Service on AWS (ROSA) クラスターにさまざまなアイデンティティープロバイダータイプを設定できます。サポート対象のタイプには、GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect、HTPasswd アイデンティティープロバイダーが含まれます。

重要

HTPasswd アイデンティティープロバイダーのオプションは、静的な管理者ユーザーを1つ作成するのを可能にするために含まれています。Htpasswd は、Red Hat OpenShift Service on AWS の一般使用向けのアイデンティティー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 アイデンティティープロバイダーを設定します。

手順

1. github.com に移動し、GitHub アカウントにログインします。
2. ROSA クラスターのアイデンティティープロビジョニングに使用する既存の GitHub 組織がない場合は、これを作成します。GitHub ドキュメント の手順に従います。
3. GitHub 組織のメンバーに限定するように、クラスターの GitHub アイデンティティープロバイダーを設定します。
   a. インタラクティブモードを使用してアイデンティティープロバイダーを設定します。

```
$ rosa create idp --cluster=<cluster_name> --interactive (1)
```

(1) **<cluster_name>** は、クラスター名に置き換えます。

出力例

```
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> (1)
? 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'
...
```

(1) **<github_org_name>** は、GitHub 組織の名前に置き換えます。

b. 出力された URL に従い、**Register application** を選択すると、Git Hub の組織に新しい OAuth アプリケーションが登録されます。アプリケーションを登録することで、ROSA に内蔵されている OAuth サーバーが GitHub 組織のメンバーをクラスターに認証することができるようになります。

注記

Register a new OAuth application GitHub フォームのフィールドには、**rosa** CLI ツールで定義された URL を介して、必要な値が自動的に入力されます。

c. GitHub OAuth アプリケーションページの情報を使用して、残りの **rosa create idp** の対話式プロンプトを設定します。

出力例 (続き)

```
...
? Client ID: <github_client_id> (1)
? Client Secret: [? for help] <github_client_secret> (2)
? GitHub Enterprise Hostname (optional):
? Mapping method: claim (3)
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.
```

■

1. **<github_client_id>** は、GitHub OAuth アプリケーションのクライアント ID に置き換えます。
2. **<github_client_secret>** は、GitHub OAuth アプリケーションのクライアントシークレットに置き換えます。
3. **claim** をマッピング方法として指定します。

注記

アイデンティティープロバイダー設定がアクティブになるまでに、約 2 分かかる場合があります。**cluster-admin** ユーザーを設定している場合は、**oc get pods -n openshift-authentication --watch** を実行して、更新された設定で OAuth Pod の再デプロイを確認できます。

d. 以下のコマンドを実行して、アイデンティティー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>
```

出力例

```
NAME      TYPE     AUTH URL
github-1  GitHub   https://oauth-openshift.apps.<cluster_name>.
<random_string>.p1.openshiftapps.com/oauth2callback/github-1
```

関連情報

- サポート対象の各アイデンティティープロバイダータイプを設定する詳細な手順は、STS のアイデンティティープロバイダーの設定 を参照してください。

クラスターへのユーザーアクセスの付与

ユーザーアクセスを設定済みのアイデンティティープロバイダーに追加して、Red Hat OpenShift Service on AWS (ROSA) クラスターに付与できます。

ROSA クラスターに異なるタイプのアイデンティティープロバイダーを設定できます。以下の手順例では、クラスターへのアイデンティティープロビジョニング用に設定された GitHub 組織に、ユーザーを追加します。

手順

1. github.com に移動し、GitHub アカウントにログインします。
2. GitHub 組織への ROSA 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。GitHub ドキュメントの 組織に参加するようにユーザーを招待する の手順を実行してください。

ユーザーへの管理者権限の付与

ユーザーを設定済みのアイデンティティープロバイダーに追加した後に、Red Hat OpenShift Service on AWS (ROSA) クラスターの **cluster-admin** 権限または **dedicated-admin** 権限を付与できます。

手順

- アイデンティティープロバイダーユーザーの **cluster-admin** 権限を設定するには、以下を実行します。

  a. ユーザーに **cluster-admin** 権限を付与します。

  ```
  $ rosa grant user cluster-admin --user=<idp_user_name> --cluster=<cluster_name>
  ```
  (1)

  (1) **<idp_user_name>** および **<cluster_name>** は、アイデンティティープロバイダーのユーザーおよびクラスター名に置き換えます。

  出力例

  ```
  I: Granted role 'cluster-admins' to user '<idp_user_name>' on cluster '<cluster_name>'
  ```

  b. ユーザーが **cluster-admins** グループのメンバーとして一覧表示されているかどうかを確認します。

  ```
  $ rosa list users --cluster=<cluster_name>
  ```

  出力例

  ```
  ID                GROUPS
  <idp_user_name>   cluster-admins
  ```

- アイデンティティープロバイダーユーザーに **dedicated-admin** 権限を設定するには、以下を実行します。

  a. ユーザーに **dedicated-admin** 権限を付与します。

  ```
  $ rosa grant user dedicated-admin --user=<idp_user_name> --cluster=<cluster_name>
  ```

  出力例

  ```
  I: Granted role 'dedicated-admins' to user '<idp_user_name>' on cluster '<cluster_name>'
  ```

  b. ユーザーが **dedicated-admins** グループのメンバーとして一覧表示されているかどうかを確認します。

  ```
  $ rosa list users --cluster=<cluster_name>
  ```

  出力例

  ```
  ID                GROUPS
  <idp_user_name>   dedicated-admins
  ```

1.6. WEB コンソールを使用したクラスターへのアクセス

クラスター管理者ユーザーの作成後や、設定済みのアイデンティティープロバイダーへのユーザーの追加後に、Web コンソールを使用して Red Hat OpenShift Service on AWS (ROSA) クラスターにログインできます。

手順

1. クラスターのコンソール URL を取得します。

```
$ rosa describe cluster -c <cluster_name> | grep Console
```
(1)

(1) **<cluster_name>** は、クラスター名に置き換えます。

出力例

```
Console URL:                https://console-openshift-console.apps.example-
cluster.wxyz.p1.openshiftapps.com
```

2. 前述の手順の出力にあるコンソール 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、指定した認証情報を使用してログインします。
   - クラスターにアイデンティティープロバイダーを設定している場合は、**Log in with...** ダイアログでアイデンティティープロバイダー名を選択し、プロバイダーによって提示される承認要求を完了します。

1.7. DEVELOPER CATALOG からのアプリケーションのデプロイ

Red Hat OpenShift Service on AWS Web コンソールの Developer Catalog からテストアプリケーションをデプロイし、ルートで公開できます。

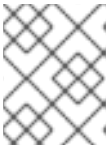
前提条件

- OpenShift Cluster Manager Hybrid Cloud Console にログインしている。
- Red Hat OpenShift Service on AWS クラスターを作成している。
- クラスターにアイデンティティープロバイダーを設定している。
- 設定したアイデンティティープロバイダーにユーザーアカウントを追加している。

手順

1. OpenShift Cluster Manager Hybrid Cloud Console から、**Open console** をクリックします。
2. **Administrator** パースペクティブで、**Home → Projects → Create Project** の順に選択します。
3. プロジェクトの名前を入力し、必要に応じて **Display Name** および **Description** を追加します。
4. **Create** をクリックしてプロジェクトを作成します。
5. **Developer** パースペクティブに切り替え、**+Add** を選択します。選択した **Project** が、作成したプロジェクトであることを確認します。
6. **Developer Catalog** ダイアログで、**All services** を選択します。
7. **Developer Catalog** ページで、メニューから **Languages → JavaScript** を選択します。

8. **Node.js** をクリックしてから **Create Application** をクリックし、**Create Source-to-Image Application** ページを開きます。



注記

Clear All Filtersをクリックして **Node.js** オプションを表示する必要がある場合があります。

9. **Git** セクションで **Try Sample** をクリックします。
10. **Name** フィールドに一意の名前を追加します。この値を使用して、関連付けられたリソースに名前を付けます。
11. **Deployment** および **Create a route to the application**が選択されていることを確認します。
12. **Create** をクリックしてアプリケーションをデプロイします。Pod のデプロイには数分かかります。
13. オプション: **nodejs** アプリケーションを選択し、そのサイドバーを確認して、**Topology** ペインで Pod のステータスを確認します。**nodejs** ビルドが完了し、**nodejs** Pod が **Running** 状態になるまで待機してから続行します。
14. デプロイメントが完了したら、以下のような形式のアプリケーションのルート URL をクリックします。

```
http://nodejs-<project>.<cluster_name>.<hash>.<region>.openshiftapps.com/
```

ブラウザーの新しいタブが開き、以下のようなメッセージが表示されます。

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

15. オプション: アプリケーションを削除し、作成したリソースをクリーンアップします。
    a. **Administrator** パースペクティブで、**Home → Projects** に移動します。
    b. プロジェクトのアクションメニューをクリックし、**Delete Project** を選択します。

1.8. 管理者権限とユーザーアクセスの取り消し

ROSA CLI (**rosa**) を使用して、ユーザーから **cluster-admin** 権限または **dedicated-admin** 権限を取り消すことができます。

ユーザーからのクラスターアクセスを取り消すには、設定したアイデンティティープロバイダーからユーザーを削除する必要があります。

このセクションの手順に従って、ユーザーからの管理者権限またはクラスターアクセスを取り消すことができます。

ユーザーからの管理者権限の削除

このセクションの手順に従って、ユーザーから **cluster-admin** 権限または **dedicated-admin** 権限を取り消すことができます。

手順

- アイデンティティープロバイダーユーザーから **cluster-admin** 権限を取り消すには、以下を実行します。

  a. **cluster-admin** 権限を取り消します。

  ```
  $ rosa revoke user cluster-admin --user=<idp_user_name> --cluster=<cluster_name> 1
  ```

  1 **<idp_user_name>** および **<cluster_name>** は、アイデンティティープロバイダーのユーザーおよびクラスター名に置き換えます。

  出力例

  ```
  ? Are you sure you want to revoke role cluster-admins from user <idp_user_name> in cluster <cluster_name>? Yes
  I: Revoked role 'cluster-admins' from user '<idp_user_name>' on cluster '<cluster_name>'
  ```

  b. ユーザーが **cluster-admins** グループのメンバーとして一覧表示されていないことを確認します。

  ```
  $ rosa list users --cluster=<cluster_name>
  ```

  出力例

  ```
  W: There are no users configured for cluster '<cluster_name>'
  ```

- アイデンティティープロバイダーユーザーから **dedicated-admin** 権限を取り消すには、以下を実行します。

  a. **dedicated-admin** 特権を取り消します。

  ```
  $ rosa revoke user dedicated-admin --user=<idp_user_name> --cluster=<cluster_name>
  ```

  出力例

  ```
  ? Are you sure you want to revoke role dedicated-admins from user <idp_user_name> in cluster <cluster_name>? Yes
  I: Revoked role 'dedicated-admins' from user '<idp_user_name>' on cluster '<cluster_name>'
  ```

  b. ユーザーが **dedicated-admins** グループのメンバーとして一覧表示されていないことを確認します。

  ```
  $ rosa list users --cluster=<cluster_name>
  ```

  出力例

  ```
  W: There are no users configured for cluster '<cluster_name>'
  ```

クラスターへのユーザーアクセスの取り消し

アイデンティティープロバイダーを設定済みのアイデンティティープロバイダーから削除して、アイデンティティープロバイダーからクラスターへのアクセス権限を取り除くことができます。

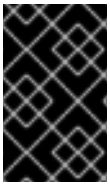
ROSA クラスターに異なるタイプのアイデンティティープロバイダーを設定できます。以下の手順例では、クラスターへのアイデンティティープロビジョニング用に設定された GitHub 組織のメンバーのクラスターへのアクセス権を取り消すことができます。

手順

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。GitHub ドキュメントの 組織からのメンバーの削除 の手順に従います。

1.9. ROSA クラスターおよび AWS STS リソースの削除

ROSA CLI (**rosa**) を使用して、AWS Security Token Service (STS) を使用する ROSA クラスターを削除できます。また、ROSA CLI を使用して、AWS Identity and Access Management (IAM) アカウントワイドロール、クラスター固有の Operator ロール、および OpenID Connect (OIDC) プロバイダーを削除することもできます。アカウント全体のインラインポリシーと Operator ポリシーを削除するには、AWS IAM Console を使用できます。



重要

アカウント全体の IAM ロールおよびポリシーは、同じ AWS アカウントの他の ROSA クラスターによって使用される可能性があります。他のクラスターで必要とされていない場合に限り、リソースを削除する必要があります。

手順

1. クラスターを削除し、ログを監視します。**<cluster_name>** はクラスターの名前または ID に置き換えます。

```
$ rosa delete cluster --cluster=<cluster_name> --watch
```

重要

IAM ロール、ポリシー、および OIDC プロバイダーを削除する前に、クラスターの削除が完了するのを待つ必要があります。インストーラーで作成されたリソースを削除するために、アカウント全体のロールが必要です。クラスター固有の Operator ロールは、OpenShift Operator によって作成されるリソースをクリーンアップするために必要です。Operator は、OIDC プロバイダーを利用して認証を行います。

2. クラスター Operator 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 1
```

1 **<cluster_id>** をクラスターの ID に置き換えてください。

注記

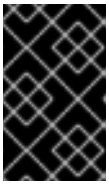
-y オプションを使用すると、プロンプトに対して自動的にはいと答えることができます。

3. クラスター固有の Operator IAM ロールを削除します。

```
$ rosa delete operator-roles -c <cluster_id> --mode auto 1
```

1 **<cluster_id>** をクラスターの ID に置き換えてください。

4. アカウント全体のロールを削除します。



重要

アカウント全体の IAM ロールおよびポリシーは、同じ AWS アカウントの他の ROSA クラスターによって使用される可能性があります。他のクラスターで必要とされていない場合に限り、リソースを削除する必要があります。

```
$ rosa delete account-roles --prefix <prefix> --mode auto 1
```

1 その際、**--<prefix>** 引数を含める必要があります。**<prefix>** を削除するアカウント全体のロールの接頭辞に置き換えてください。アカウント全体のロールを作成したときにカスタム接頭辞を指定しなかった場合は、デフォルトの接頭辞である **ManagedOpenShift** を指定します。

5. STS を使用する ROSA デプロイメント用に作成したアカウント全体のインラインおよび Operator IAM ポリシーを削除します。

   a. AWS IAM コンソール にログインします。

   b. **Access management → Policies** に移動し、アカウント全体のポリシーのいずれかを選択します。

   c. ポリシーを選択した状態で、**Actions → Delete** をクリックし、削除ポリシーダイアログを開きます。

   d. ポリシー名を入力して削除の確認を行い、**Delete** を選択してポリシーを削除します。

   e. この手順を繰り返して、クラスターのアカウント全体のインラインおよび Operator ポリシーを削除します。

1.10. 次のステップ

- OpenShift Cluster Manager コンソールを使用したサービスのクラスターへの追加
- コンピュートノードの管理
- モニタリングスタックの設定
- ロギングアドオンサービスのインストール

1.11. 関連情報

- AWS STS を使用してアカウントおよび ROSA クラスターを設定する方法の詳細は、STS デプロイメントワークフローでの ROSA について を参照してください。
- AWS STS を使用せずにアカウントおよび ROSA クラスターを設定する方法の詳細は、ROSA デプロイメントワークフローについて を参照してください。
- クラスターのアップグレードに関する詳細は、ROSA クラスターのアップグレード を参照してください。

第2章 RED HAT OPENSHIFT SERVICE ON AWS の使用を開始するための包括的なガイド

注記

ROSA のクイックスタートガイドをお探しの場合は、Red Hat OpenShift Service on AWS クイックスタートガイド を参照してください。

以下の手順に従って、Red Hat OpenShift Service on AWS (ROSA) クラスターを作成し、ユーザーアクセスを付与し、最初のアプリケーションをデプロイすると共に、ユーザーアクセスを取り消して、クラスターを削除する方法を確認します。

ROSA クラスターは、AWS Security Token Service (STS) の有無にかかわらず作成できます。本書の手順では、AWS STS を使用するクラスターを作成できます。ROSA クラスターで AWS STS を使用する方法は、AWS Security Token Service の使用 を参照してください。

2.1. 前提条件

- Red Hat OpenShift Service on AWS(ROSA) の概要 、および ROSA アーキテクチャーモデルおよびアーキテクチャー の 概念 を確認している。
- 制限およびスケーラビリティーに関するドキュメント と、環境の計画に関するガイドライン を確認している。
- STS を使用した ROSA の詳細な AWS の前提条件 を確認している。
- ROSA クラスターの実行に必要な AWS サービスクォータ がある。

2.2. 環境の設定

Red Hat OpenShift Service on AWS(ROSA) クラスターを作成する前に、以下のタスクを実行して環境を設定する必要があります。

- AWS アカウントで ROSA を有効化する
- 必要なコマンドラインインターフェイス (CLI) ツールをインストールして設定する
- CLI ツールの設定を確認する
- AWS Elastic Load Balancing (ELB) サービ出力ルが存在することを確認する
- 必要な AWS リソースクォータが利用可能であることを確認する

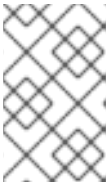
本セクションの手順に従って、これらの設定要件を完了できます。

2.2.1. AWS アカウントでの ROSA の有効化

以下の手順に従って、AWS アカウントで Red Hat OpenShift Service on AWS (ROSA) を有効にします。

前提条件

- AWS アカウントを作成している。



注記

専用の AWS アカウントを使用して実稼働クラスターを実行することを検討してください。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。

手順

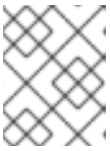
1. AWS 管理コンソール にログインします。
2. ROSA サービス に移動して、**Enable OpenShift** を選択して、AWS アカウントで ROSA を有効にします。

2.2.2. 必要な CLI ツールのインストールと設定

以下の手順を使用して、AWS、Red Hat OpenShift Service on AWS (ROSA) および OpenShift CLI ツールをワークステーションにインストールし、設定します。

前提条件

- AWS アカウントがある。
- Red Hat アカウントを作成している。

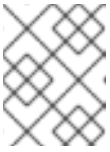


注記

console.redhat.com に移動し、**Red Hat アカウントの登録** を選択して、Red Hat アカウントを作成できます。

手順

1. 最新の AWS CLI (**aws**) をインストールして設定します。
   a. AWS コマンドラインインターフェイス ドキュメントに従って、お使いのオペレーティングシステム用の AWS CLI をインストールし、設定します。
   .aws/credentials ファイルに **aws_access_key_id**、**aws_secret_access_key**、および **region** 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。

   注記

   AWS_DEFAULT_REGION 環境変数を使用して、デフォルトの AWS リージョンを設定することもできます。

   b. AWS API をクエリーし、AWS CLI が適切にインストールおよび設定されているかどうかを確認します。

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

   出力例

   ```
   <aws_account_id>    arn:aws:iam::<aws_account_id>:user/<username>  <aws_user_id>
   ```

2. 最新の ROSA CLI (**rosa**) をインストールし、設定します。

a. Red Hat OpenShift Cluster Manager Hybrid Cloud Console の **ダウンロード** ページから、オペレーティングシステム用の **rosa** CLI の最新バージョンをダウンロードします。

b. ダウンロードしたアーカイブから **rosa** バイナリーファイルを展開します。以下の例は、Linux tar アーカイブからバイナリーを展開します。

```
$ tar xvf rosa-linux.tar.gz
```

c. パスに **rosa** を加えてください。以下の例では、**/usr/local/bin** ディレクトリーがユーザーのパスに含まれます。

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

d. **rosa** バージョンをクエリーして、**rosa** CLI ツールが適切にインストールされていることを確認します。

```
$ rosa version
```

出力例

```
1.2.8
```

e. オプション: **rosa** CLI のタブ補完を有効にします。タブ補完を有効にすると、**Tab** キーを 2 回押すことでサブコマンドが自動的に補完され、コマンドの提案が表示されます。
さまざまなシェルタイプで **rosa** のタブ補完が使用できます。以下の例では、Linux ホストで Bash の永続タブ補完を有効にします。このコマンドは、Bash の **rosa** タブ補完設定ファイルを生成して **/etc/bash_completion.d/** ディレクトリーに保存します。

```
# rosa completion bash > /etc/bash_completion.d/rosa
```

設定を有効にするには、新しいターミナルを開いている必要があります。

注記

さまざまなシェルタイプの **rosa** タブ補完を設定する手順は、**rosa completion --help** を実行してヘルプメニューを参照してください。

f. **rosa** CLI を使用して Red Hat アカウントにログインしました。

```
$ rosa login
```

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:
```

コマンド出力に一覧表示されている URL に移動し、オフラインアクセストークンを取得します。ログインする CLI プロンプトでトークンを指定します。

注記

その後に **rosa login** コマンドの実行時に **--token="<offline_access_token>"** 引数を使用してオフラインアクセストークンを指定できます。

g. 正常にログインできるかどうかを確認し、認証情報を確認します。

```
$ rosa whoami
```

出力例

```
AWS Account ID:               <aws_account_number>
AWS Default Region:           us-east-1
AWS ARN:                      arn:aws:iam::<aws_account_number>:user/<aws_user_name>
OCM API:                      https://api.openshift.com
OCM Account ID:               <red_hat_account_id>
OCM Account Name:             Your Name
OCM Account Username:         you@domain.com
OCM Account Email:            you@domain.com
OCM Organization ID:          <org_id>
OCM Organization Name:        Your organization
OCM Organization External ID: <external_org_id>
```

次に進む前に、出力の情報が正しいことを確認します。

3. 最新の OpenShift CLI (**oc**) をインストールして設定します。

a. **rosa** CLI を使用して、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. ダウンロードしたアーカイブから **oc** バイナリーファイルを展開します。以下の例は、Linux tar アーカイブからファイルを展開します。

```
$ tar xvf openshift-client-linux.tar.gz
```

c. **oc** バイナリーをパスに追加します。以下の例では、**/usr/local/bin** ディレクトリーがユーザーのパスに含まれます。

```
$ sudo mv oc /usr/local/bin/oc
```

d. **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
```

出力例

```
I: Verifying whether OpenShift command-line tool is available...
I: Current OpenShift Client Version: 4.9.12
```

2.2.3. ELB サービス出力の作成

AWSServiceRoleForElasticLoadBalancing AWS Elastic Load Balancing (ELB) サービス出力ルが存在するかどうかを確認し、存在しない場合には作成します。

注記

Error creating network Load Balancer: AccessDenied: AWS ELB サービス出力ルなしで Red Hat OpenShift Service on AWS (ROSA) クラスターを作成しようとすると生成されます。

前提条件

- AWS アカウントがある。
- 最新の AWS CLI (**aws**) をワークステーションにインストールし、設定している。

手順

1. AWS アカウントに **AWSServiceRoleForElasticLoadBalancing** ロールが存在するかどうかを確認します。

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

出力例

以下の出力例では、ロールが存在することを確認します。

```
ROLE    arn:aws:iam::<aws_account_number>:role/aws-service-role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing  2018-09-27T19:49:23+00:00       Allows ELB to call AWS services on your behalf. 3600       /aws-service-role/elasticloadbalancing.amazonaws.com/   <role_id>  AWSServiceRoleForElasticLoadBalancing
ASSUMEROLEPOLICYDOCUMENT        2012-10-17
STATEMENT       sts:AssumeRole  Allow
PRINCIPAL       elasticloadbalancing.amazonaws.com
ROLELASTUSED    2022-01-06T09:27:57+00:00       us-east-1
```

2. AWS ELB サービス出力ルが存在しない場合は、作成します。

```
$ aws iam create-service-linked-role --aws-service-name "elasticloadbalancing.amazonaws.com"
```

2.2.4. AWS クォータの空きの確認

必要なリソースクォータがデフォルトの AWS リージョンのアカウントで利用可能であることを確認します。

前提条件

- AWS アカウントがある。
- ワークステーションに最新の AWS (**aws**)、ROSA (**rosa**)、OpenShift (**oc**) の CLI をインストールして設定している。
- **rosa** CLI を使用して Red Hat アカウントにログインしている。

手順

1. 必要なリソースクォータがデフォルトのリージョンで利用可能かどうかを確認します。

```
$ rosa verify quota
```

出力例

```
I: Validating AWS quota...
I: AWS quota ok. If cluster installation fails, validate actual AWS resource usage against
https://docs.openshift.com/rosa/rosa_getting_started/rosa-required-aws-service-quotas.html
```

2.3. STS を使用した ROSA クラスターの作成

以下のいずれかの方法を選択して、AWS Security Token Service (STS) を使用する Red Hat OpenShift Service on AWS (ROSA) クラスターをデプロイします。どちらのシナリオでも、Red Hat OpenShift Cluster Manager または ROSA CLI (**rosa**) を使用してクラスターをデプロイできます。

- **デフォルトオプションを使用した STS での ROSA クラスターの作成** デフォルトのオプションと STS リソースの自動作成を使用して、STS で ROSA クラスターをすばやく作成できます。
- **カスタマイズを使用して STS を使用する ROSA クラスターの作成** カスタマイズを使用して、STS で ROSA クラスターを作成できます。必要な STS リソースを作成するときに、**auto** モードと **manual** モードのいずれかを選択することもできます。

関連情報

- STS を使用せずに ROSA クラスターをデプロイする詳細な手順については、AWS STS を使用せずに ROSA クラスターの作成 および ROSA での AWS PrivateLink クラスターの作成 を参照してください。
- STS を使用する ROSA デプロイメントに必要なアカウント全体の IAM ロールおよびポリシーについては、アカウント全体の IAM ロールおよびポリシー参照 を参照してください。
- **auto** モードと **manual** モードを使用して必要な STS リソースを作成する方法の詳細は、自動デプロイメントモードと手動デプロイメントモードについて を参照してください。
- ROSA の更新ライフサイクルについては、Red Hat OpenShift Service on AWS 更新ライフサイクル を参照してください。

2.4. クラスターにすぐアクセスできるようにクラスター管理者ユーザーの作成

アイデンティティープロバイダーを設定する前に、**cluster-admin** 権限のあるユーザーを作成して、Red Hat OpenShift Service on AWS (ROSA) クラスターへすぐにアクセスできるようにします。

注記

クラスター管理者ユーザーは、新たにデプロイされたクラスターにすぐアクセスが必要な場合に役立ちます。ただし、アイデンティティープロバイダーを設定し、必要に応じてクラスター管理者権限をアイデンティティープロバイダーユーザーに付与することを検討してください。ROSA クラスターのアイデンティティープロバイダーの設定の詳細は、**アイデンティティープロバイダーの設定およびクラスターのアクセスの付与** を参照してください。

前提条件

- AWS アカウントがある。
- ワークステーションに最新の AWS (**aws**)、ROSA (**rosa**)、OpenShift (**oc**) の CLI をインストールして設定している。
- **rosa** CLI を使用して Red Hat アカウントにログインしている。
- ROSA クラスターを作成している。

手順

1. クラスター管理者ユーザーを作成します。

```
$ rosa create admin --cluster=<cluster_name> 1
```

1 **<cluster_name>** は、クラスター名に置き換えます。

出力例

```
W: It is recommended to add an identity provider to login to this cluster. See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster '<cluster_name>'.
I: Please securely store this generated password. If you lose this password you can delete and recreate the cluster admin user.
I: To login, run the following command:

   oc login https://api.example-cluster.wxyz.p1.openshiftapps.com:6443 --username cluster-admin --password d7Rca-Ba4jy-YeXhs-WU42J

I: It may take up to a minute for the account to become active.
```

注記

cluster-admin ユーザーがアクティブになるまで約 1 分かかる場合があります。

2. CLI でクラスターにログインします。
   a. 上記の手順の出力で提供されたコマンドを実行して、ログインします。

```
$ oc login <api_url> --username cluster-admin --password <cluster_admin_password> 1
```

1 **<api_url>** および **<cluster_admin_password>** は、環境の API URL およびクラスター管理者のパスワードに置き換えます。

b. ROSA クラスターに **cluster-admin** ユーザーとしてログインしているかどうかを確認します。

```
$ oc whoami
```

出力例

```
cluster-admin
```

関連情報

- ROSA Web コンソールにログインする手順は、Web コンソールを使用したクラスターへのアクセス を参照してください。

2.5. アイデンティティープロバイダーの設定およびクラスターアクセスの付与

Red Hat OpenShift Service on AWS (ROSA) には、ビルトイン OAuth サーバーが含まれます。ROSA クラスターの作成後に、OAuth をアイデンティティープロバイダーを使用するように設定する必要があります。その後、メンバーを設定済みのアイデンティティープロバイダーに追加して、クラスターへのアクセス権限を付与できます。

また、必要に応じて、アイデンティティープロバイダーユーザーに **cluster-admin** 権限または **dedicated-admin** 権限を付与することもできます。

2.5.1. アイデンティティープロバイダーの設定

Red Hat OpenShift Service on AWS (ROSA) クラスターにさまざまなアイデンティティープロバイダータイプを設定できます。サポート対象のタイプには、GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect、HTPasswd アイデンティティープロバイダーが含まれます。

重要

HTPasswd アイデンティティープロバイダーのオプションは、静的な管理者ユーザーを 1 つ作成するのを可能にするために含まれています。Htpasswd は、Red Hat OpenShift Service on AWS の一般使用向けのアイデンティティー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 アイデンティティープロバイダーを設定します。

前提条件

- AWS アカウントがある。
- ワークステーションに最新の AWS (**aws**)、ROSA (**rosa**)、OpenShift (**oc**) の CLI をインストールして設定している。
- **rosa** CLI を使用して Red Hat アカウントにログインしている。

- ROSA クラスターを作成している。
- GitHub ユーザーアカウントがある。

手順

1. github.com に移動し、GitHub アカウントにログインします。
2. ROSA クラスターのアイデンティティープロビジョニングに使用する既存の GitHub 組織がない場合は、これを作成します。GitHub ドキュメント の手順に従います。
3. GitHub 組織のメンバーに限定するように、クラスターの GitHub アイデンティティープロバイダーを設定します。

   a. インタラクティブモードを使用してアイデンティティープロバイダーを設定します。

   ```
   $ rosa create idp --cluster=<cluster_name> --interactive (1)
   ```

   (1) **<cluster_name>** は、クラスター名に置き換えます。

   出力例

   ```
   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> (1)
   ? 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'
   ...
   ```

   (1) **<github_org_name>** は、GitHub 組織の名前に置き換えます。

   b. 出力された URL に従い、**Register application** を選択すると、Git Hub の組織に新しい OAuth アプリケーションが登録されます。アプリケーションを登録することで、ROSA に内蔵されている OAuth サーバーが GitHub 組織のメンバーをクラスターに認証することができるようになります。

   注記

   Register a new OAuth application GitHub フォームのフィールドには、**rosa** CLI ツールで定義された URL を介して、必要な値が自動的に入力されます。

c. GitHub OAuth アプリケーションページの情報を使用して、残りの **rosa create idp** の対話式プロンプトを設定します。

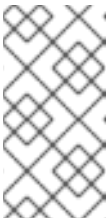
出力例 (続き)

```
...
? Client ID: <github_client_id> 1
? Client Secret: [? for help] <github_client_secret> 2
? GitHub Enterprise Hostname (optional):
? Mapping method: claim 3
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.
```

1 **<github_client_id>** は、GitHub OAuth アプリケーションのクライアント ID に置き換えます。

2 **<github_client_secret>** は、GitHub OAuth アプリケーションのクライアントシークレットに置き換えます。

3 **claim** をマッピング方法として指定します。



注記

アイデンティティープロバイダー設定がアクティブになるまでに、約 2 分かかる場合があります。**cluster-admin** ユーザーを設定している場合は、**oc get pods -n openshift-authentication --watch** を実行して、更新された設定で OAuth Pod の再デプロイを確認できます。

d. 以下のコマンドを実行して、アイデンティティー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>
```

出力例

```
NAME       TYPE      AUTH URL
github-1   GitHub    https://oauth-openshift.apps.<cluster_name>.
<random_string>.p1.openshiftapps.com/oauth2callback/github-1
```

関連情報

- サポート対象の各アイデンティティープロバイダータイプを設定する詳細な手順は、STS のアイデンティティープロバイダーの設定 を参照してください。

2.5.2. クラスターへのユーザーアクセスの付与

ユーザーアクセスを設定済みのアイデンティティープロバイダーに追加して、Red Hat OpenShift Service on AWS (ROSA) クラスターに付与できます。

ROSA クラスターに異なるタイプのアイデンティティープロバイダーを設定できます。以下の手順例では、クラスターへのアイデンティティープロビジョニング用に設定された GitHub 組織に、ユーザーを追加します。

前提条件

- AWS アカウントがある。
- ワークステーションに最新の AWS (**aws**)、ROSA (**rosa**)、OpenShift (**oc**) の CLI をインストールして設定している。
- **rosa** CLI を使用して Red Hat アカウントにログインしている。
- ROSA クラスターを作成している。
- GitHub ユーザーアカウントがある。
- クラスターに GitHub アイデンティティープロバイダーを設定している。

手順

1. github.com に移動し、GitHub アカウントにログインします。
2. GitHub 組織への ROSA 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。GitHub ドキュメントの 組織に参加するようにユーザーを招待する の手順を実行してください。

2.5.3. ユーザーへの管理者権限の付与

ユーザーを設定済みのアイデンティティープロバイダーに追加した後に、Red Hat OpenShift Service on AWS (ROSA) クラスターの **cluster-admin** 権限または **dedicated-admin** 権限を付与できます。

前提条件

- AWS アカウントがある。
- ワークステーションに最新の AWS (**aws**)、ROSA (**rosa**)、OpenShift (**oc**) の CLI をインストールして設定している。
- **rosa** CLI を使用して Red Hat アカウントにログインしている。
- ROSA クラスターを作成している。
- クラスターに GitHub アイデンティティープロバイダーを設定し、アイデンティティープロバイダーユーザーを追加している。

手順

- アイデンティティープロバイダーユーザーの **cluster-admin** 権限を設定するには、以下を実行します。
  a. ユーザーに **cluster-admin** 権限を付与します。

```
$ rosa grant user cluster-admin --user=<idp_user_name> --cluster=<cluster_name>
```
(1)

1. **<idp_user_name>** および **<cluster_name>** は、アイデンティティープロバイダーのユーザーおよびクラスター名に置き換えます。

出力例

```
I: Granted role 'cluster-admins' to user '<idp_user_name>' on cluster '<cluster_name>'
```

b. ユーザーが **cluster-admins** グループのメンバーとして一覧表示されているかどうかを確認します。

```
$ rosa list users --cluster=<cluster_name>
```

出力例

```
ID              GROUPS
<idp_user_name>    cluster-admins
```

- アイデンティティープロバイダーユーザーに **dedicated-admin** 権限を設定するには、以下を実行します。

a. ユーザーに **dedicated-admin** 権限を付与します。

```
$ rosa grant user dedicated-admin --user=<idp_user_name> --cluster=<cluster_name>
```

出力例

```
I: Granted role 'dedicated-admins' to user '<idp_user_name>' on cluster '<cluster_name>'
```

b. ユーザーが **dedicated-admins** グループのメンバーとして一覧表示されているかどうかを確認します。

```
$ rosa list users --cluster=<cluster_name>
```

出力例

```
ID              GROUPS
<idp_user_name>    dedicated-admins
```

2.6. WEB コンソールを使用したクラスターへのアクセス

クラスター管理者ユーザーの作成後や、設定済みのアイデンティティープロバイダーへのユーザーの追加後に、Web コンソールを使用して Red Hat OpenShift Service on AWS (ROSA) クラスターにログインできます。

前提条件

- AWS アカウントがある。
- ワークステーションに最新の AWS (**aws**)、ROSA (**rosa**)、OpenShift (**oc**) の CLI をインストールして設定している。

- **rosa** CLI を使用して Red Hat アカウントにログインしている。
- ROSA クラスターを作成している。
- クラスター管理者ユーザーを作成しているか、またはユーザーアカウントを設定済みのアイデンティティープロバイダーに追加している。

手順

1. クラスターのコンソール URL を取得します。

```
$ rosa describe cluster -c <cluster_name> | grep Console (1)
```

(1) **<cluster_name>** は、クラスター名に置き換えます。

出力例

```
Console URL:                https://console-openshift-console.apps.example-
cluster.wxyz.p1.openshiftapps.com
```

2. 前述の手順の出力にあるコンソール 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、指定した認証情報を使用してログインします。
   - クラスターにアイデンティティープロバイダーを設定している場合は、**Log in with...** ダイアログでアイデンティティープロバイダー名を選択し、プロバイダーによって提示される承認要求を完了します。

2.7. DEVELOPER CATALOG からのアプリケーションのデプロイ

Red Hat OpenShift Service on AWS Web コンソールの Developer Catalog からテストアプリケーションをデプロイし、ルートで公開できます。

前提条件

- OpenShift Cluster Manager Hybrid Cloud Console にログインしている。
- Red Hat OpenShift Service on AWS クラスターを作成している。
- クラスターにアイデンティティープロバイダーを設定している。
- 設定したアイデンティティープロバイダーにユーザーアカウントを追加している。

手順

1. OpenShift Cluster Manager Hybrid Cloud Console から、**Open console** をクリックします。
2. **Administrator** パースペクティブで、**Home → Projects → Create Project** の順に選択します。
3. プロジェクトの名前を入力し、必要に応じて **Display Name** および **Description** を追加します。
4. **Create** をクリックしてプロジェクトを作成します。

5. **Developer** パースペクティブに切り替え、**+Add** を選択します。選択した **Project** が、作成したプロジェクトであることを確認します。
6. **Developer Catalog** ダイアログで、**All services** を選択します。
7. **Developer Catalog** ページで、メニューから **Languages → JavaScript** を選択します。
8. **Node.js** をクリックしてから **Create Application** をクリックし、**Create Source-to-Image Application** ページを開きます。

注記

Clear All Filtersをクリックして **Node.js** オプションを表示する必要がある場合があります。

9. **Git** セクションで **Try Sample** をクリックします。
10. **Name** フィールドに一意の名前を追加します。この値を使用して、関連付けられたリソースに名前を付けます。
11. **Deployment** および **Create a route to the application**が選択されていることを確認します。
12. **Create** をクリックしてアプリケーションをデプロイします。Pod のデプロイには数分かかります。
13. オプション: **nodejs** アプリケーションを選択し、そのサイドバーを確認して、**Topology** ペインで Pod のステータスを確認します。**nodejs** ビルドが完了し、**nodejs** Pod が **Running** 状態になるまで待機してから続行します。
14. デプロイメントが完了したら、以下のような形式のアプリケーションのルート URL をクリックします。

```
http://nodejs-<project>.<cluster_name>.<hash>.<region>.openshiftapps.com/
```

ブラウザーの新しいタブが開き、以下のようなメッセージが表示されます。

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

15. オプション: アプリケーションを削除し、作成したリソースをクリーンアップします。
    a. **Administrator** パースペクティブで、**Home → Projects** に移動します。
    b. プロジェクトのアクションメニューをクリックし、**Delete Project** を選択します。

2.8. 管理者権限とユーザーアクセスの取り消し

ROSA CLI (**rosa**) を使用して、ユーザーから **cluster-admin** 権限または **dedicated-admin** 権限を取り消すことができます。

ユーザーからのクラスターアクセスを取り消すには、設定したアイデンティティープロバイダーからユーザーを削除する必要があります。

このセクションの手順に従って、ユーザーからの管理者権限またはクラスターアクセスを取り消すことができます。

2.8.1. ユーザーからの管理者権限の削除

このセクションの手順に従って、ユーザーから **cluster-admin** 権限または **dedicated-admin** 権限を取り消すことができます。

前提条件

- ワークステーションに最新の AWS (**aws**)、ROSA (**rosa**)、OpenShift (**oc**) の CLI をインストールして設定している。
- **rosa** CLI を使用して Red Hat アカウントにログインしている。
- ROSA クラスターを作成している。
- クラスターに GitHub アイデンティティープロバイダーを設定し、アイデンティティープロバイダーユーザーを追加している。
- ユーザーに **cluster-admin** または **dedicated-admin** 権限が付与されている。

手順

- アイデンティティープロバイダーユーザーから **cluster-admin** 権限を取り消すには、以下を実行します。
  a. **cluster-admin** 権限を取り消します。

```
$ rosa revoke user cluster-admin --user=<idp_user_name> --cluster=<cluster_name>
```
(1)

(1) **<idp_user_name>** および **<cluster_name>** は、アイデンティティープロバイダーのユーザーおよびクラスター名に置き換えます。

出力例

```
? Are you sure you want to revoke role cluster-admins from user <idp_user_name> in
cluster <cluster_name>? Yes
I: Revoked role 'cluster-admins' from user '<idp_user_name>' on cluster '<cluster_name>'
```

  b. ユーザーが **cluster-admins** グループのメンバーとして一覧表示されていないことを確認します。

```
$ rosa list users --cluster=<cluster_name>
```

出力例

```
W: There are no users configured for cluster '<cluster_name>'
```

- アイデンティティープロバイダーユーザーから **dedicated-admin** 権限を取り消すには、以下を実行します。
  a. **dedicated-admin** 特権を取り消します。

```
$ rosa revoke user dedicated-admin --user=<idp_user_name> --cluster=<cluster_name>
```

出力例

```
? Are you sure you want to revoke role dedicated-admins from user <idp_user_name> in cluster <cluster_name>? Yes
I: Revoked role 'dedicated-admins' from user '<idp_user_name>' on cluster '<cluster_name>'
```

b. ユーザーが **dedicated-admins** グループのメンバーとして一覧表示されていないことを確認します。

```
$ rosa list users --cluster=<cluster_name>
```

出力例

```
W: There are no users configured for cluster '<cluster_name>'
```

2.8.2. クラスターへのユーザーアクセスの取り消し

アイデンティティープロバイダーを設定済みのアイデンティティープロバイダーから削除して、アイデンティティープロバイダーからクラスターへのアクセス権限を取り除くことができます。

ROSA クラスターに異なるタイプのアイデンティティープロバイダーを設定できます。以下の手順例では、クラスターへのアイデンティティープロビジョニング用に設定された GitHub 組織のメンバーのクラスターへのアクセス権を取り消すことができます。

前提条件

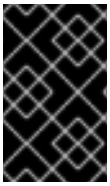
- ROSA クラスターがある。
- GitHub ユーザーアカウントがある。
- クラスターに GitHub アイデンティティープロバイダーを設定し、アイデンティティープロバイダーユーザーを追加している。

手順

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。GitHub ドキュメントの 組織からのメンバーの削除 の手順に従います。

2.9. ROSA クラスターおよび AWS STS リソースの削除

ROSA CLI (**rosa**) を使用して、AWS Security Token Service (STS) を使用する ROSA クラスターを削除できます。また、ROSA CLI を使用して、AWS Identity and Access Management (IAM) アカウントワイドロール、クラスター固有の Operator ロール、および OpenID Connect (OIDC) プロバイダーを削除することもできます。アカウント全体のインラインポリシーと Operator ポリシーを削除するには、AWS IAM Console を使用できます。



重要

アカウント全体の IAM ロールおよびポリシーは、同じ AWS アカウントの他の ROSA クラスターによって使用される可能性があります。他のクラスターで必要とされていない場合に限り、リソースを削除する必要があります。

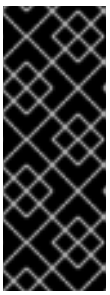
前提条件

- ワークステーションに最新の AWS (**aws**)、ROSA (**rosa**)、OpenShift (**oc**) の CLI をインストールして設定している。
- **rosa** CLI を使用して Red Hat アカウントにログインしている。
- ROSA クラスターを作成している。

手順

1. クラスターを削除し、ログを監視します。**<cluster_name>** はクラスターの名前または ID に置き換えます。

```
$ rosa delete cluster --cluster=<cluster_name> --watch
```



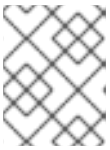
重要

IAM ロール、ポリシー、および OIDC プロバイダーを削除する前に、クラスターの削除が完了するのを待つ必要があります。インストーラーで作成されたリソースを削除するために、アカウント全体のロールが必要です。クラスター固有の Operator ロールは、OpenShift Operator によって作成されるリソースをクリーンアップするために必要です。Operator は、OIDC プロバイダーを利用して認証を行います。

2. クラスター Operator 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 (1)
```

(1) **<cluster_id>** をクラスターの ID に置き換えてください。



注記

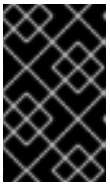
-y オプションを使用すると、プロンプトに対して自動的にはいと答えることができます。

3. クラスター固有の Operator IAM ロールを削除します。

```
$ rosa delete operator-roles -c <cluster_id> --mode auto (1)
```

(1) **<cluster_id>** をクラスターの ID に置き換えてください。

4. アカウント全体のロールを削除します。



重要

アカウント全体の IAM ロールおよびポリシーは、同じ AWS アカウントの他の ROSA クラスターによって使用される可能性があります。他のクラスターで必要とされていない場合に限り、リソースを削除する必要があります。

```
$ rosa delete account-roles --prefix <prefix> --mode auto 1
```

1 その際、**--<prefix>** 引数を含める必要があります。**<prefix>** を削除するアカウント全体のロールの接頭辞に置き換えてください。アカウント全体のロールを作成したときにカスタム接頭辞を指定しなかった場合は、デフォルトの接頭辞である **ManagedOpenShift** を指定します。

5. STS を使用する ROSA デプロイメント用に作成したアカウント全体のインラインおよび Operator IAM ポリシーを削除します。
   a. AWS IAM コンソール にログインします。
   b. **Access management → Policies** に移動し、アカウント全体のポリシーのいずれかを選択します。
   c. ポリシーを選択した状態で、**Actions → Delete** をクリックし、削除ポリシーダイアログを開きます。
   d. ポリシー名を入力して削除の確認を行い、**Delete** を選択してポリシーを削除します。
   e. この手順を繰り返して、クラスターのアカウント全体のインラインおよび Operator ポリシーを削除します。

2.10. 次のステップ

- OpenShift Cluster Manager コンソールを使用したサービスのクラスターへの追加
- コンピュートノードの管理
- モニタリングスタックの設定
- ロギングアドオンサービスのインストール

2.11. 関連情報

- AWS STS を使用してアカウントおよび ROSA クラスターを設定する方法の詳細は、STS デプロイメントワークフローでの ROSA について を参照してください。
- AWS STS を使用せずにアカウントおよび ROSA クラスターを設定する方法の詳細は、ROSA デプロイメントワークフローについて を参照してください。
- クラスターのアップグレードに関する詳細は、ROSA クラスターのアップグレード を参照してください。

第3章 STS デプロイメントワークフローでの ROSA について

Red Hat OpenShift Service on AWS (ROSA) クラスターを作成する前に、AWS の前提条件を満たし、必要な AWS サービスクォータが利用可能であることを確認し、環境をセットアップする必要があります。

本書では、STS デプロイメントワークフローステージを使用した ROSA の概要と、各ステージの詳細なリソースを説明します。

3.1. STS デプロイメントワークフローでの ROSA の概要

AWS Security Token Service (STS) は、IAM またはフェデレーションされたユーザーの短期認証情報を提供するグローバル Web サービスです。Red Hat OpenShift Service on AWS (ROSA) で AWS STS を使用し、コンポーネント固有の IAM ロールについて一時的な制限された権限付き認証情報を割り当てることができます。サービスを使用すると、クラスターコンポーネントはセキュアなクラウドリソース管理プラクティスを使用して AWS API 呼び出しを実行できます。

このセクションで説明されているワークフローステージに従い、STS を使用する ROSA クラスターを設定し、アクセスできます。

1. STS で ROSA の AWS の前提条件を完了します。STS で ROSA クラスターをデプロイするには、AWS アカウントが前提条件を満たしている必要があります。

2. 必要な AWS サービスクォータを確認します。クラスターのデプロイメントを準備するには、ROSA クラスターの実行に必要な AWS サービスクォータを確認します。

3. 環境を設定し、STS を使用して ROSA をインストールします。STS クラスターで ROSA を作成する前に、AWS アカウントで ROSA を有効にし、必要な CLI ツールをインストールして設定し、CLI ツールの設定を確認する必要があります。また、AWS Elastic Load Balancing (ELB) サービ出力ルが存在し、必要な AWS リソースクォータが利用可能であることを確認する必要があります。

4. 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。ROSA CLI (**rosa**) または Red Hat OpenShift Cluster Manager を使用して、STS でクラスターを作成します。デフォルトのオプションを使用してクラスターをすばやく作成するか、組織のニーズに合わせてカスタマイズを適用することができます。

5. クラスターにアクセスします。アイデンティティープロバイダーを設定し、必要に応じてクラスター管理者権限をアイデンティティープロバイダーユーザーに付与できます。**cluster-admin** ユーザーを設定して、新たにデプロイされたクラスターにすばやくアクセスすることもできます。

6. ユーザーの ROSA クラスターへのアクセスを取り消します。ROSA CLI または Web コンソールを使用して、STS クラスターが含まれる ROSA へのアクセス権をユーザーから取り消すことができます。

7. ROSA クラスターを削除します。ROSA CLI (**rosa**) を使用して、STS クラスターで ROSA を削除できます。クラスターの削除後に、AWS Identity and Access Management (IAM) コンソールを使用して STS リソースを削除できます。

3.2. 関連情報

- ROSA デプロイメントワークフローを使用して AWS STS を使用せずにクラスターを作成する方法は、ROSA デプロイメントワークフローについて を参照してください。