Red Hat OpenShift Service on AWS 4

开始使用

设置集群和帐户

Last Updated: 2024-06-28

Red Hat OpenShift Service on AWS 4 开始使用

设置集群和帐户

法律通告

摘要

本文档提供有关如何在 AWS (ROSA) 集群上开始使用 Red Hat OpenShift Service 的信息。

目录

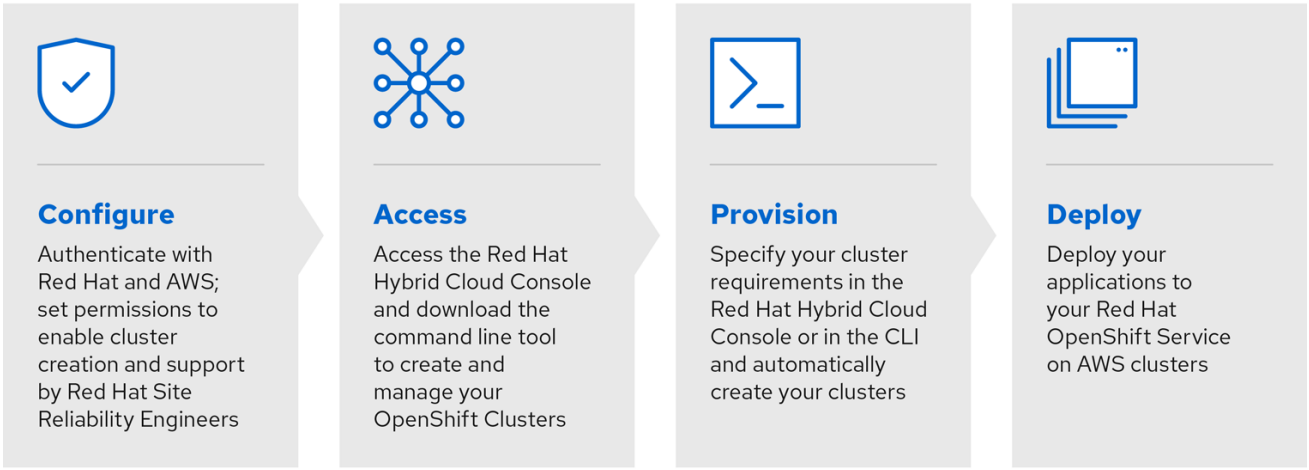
第 1 章 RED HAT OPENSHIFT SERVICE ON AWS 快速启动指南

注意

如果您要寻找 Red Hat OpenShift Service on AWS (ROSA) 的全面入门指南，请参阅 Red Hat OpenShift Service on AWS 的完整指南。如需有关 ROSA 安装的更多信息，请参阅在 AWS (ROSA)上安装 Red Hat OpenShift Service 。

按照本指南，使用 Red Hat Hybrid Cloud Console 上的 Red Hat OpenShift Cluster Manager 快速创建 Red Hat OpenShift Service on AWS (ROSA)集群，授予用户访问权限、部署第一个应用程序，并了解如何撤销用户访问和删除您的集群。

本文档中的步骤可让您创建使用 AWS 安全令牌服务(STS)的集群。有关在 ROSA 集群中使用 AWS STS 的更多信息，请参阅使用 AWS 安全令牌服务。



1.1. 前提条件

- 您已参阅了对 Red Hat OpenShift Service on AWS (ROSA)的介绍，以及 ROSA 架构模型和 架构概念 的文档。
- 您已阅读有关限制和可扩展性的文档，以及规划环境的指导信息。
- 您已查看了使用 STS 的 ROSA 的 AWS 先决条件 。
- 您的系统满足运行 ROSA 集群的 AWS 服务配额要求 。

1.2. 设置环境

在 AWS (ROSA) 集群上创建 Red Hat OpenShift Service 前，您必须完成以下任务来设置您的环境：

- 根据您的 AWS 和 Red Hat 帐户验证 ROSA 的先决条件。
- 安装和配置所需的命令行界面(CLI)工具。
- 验证 CLI 工具的配置。

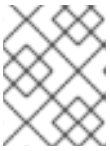
您可以按照本节中的步骤完成这些设置要求。

验证 ROSA 先决条件

使用此流程中的步骤在您的 AWS 帐户中启用 Red Hat OpenShift Service on AWS (ROSA)。

前提条件

- 您有红帽帐户。
- 您有一个 AWS 帐户。



注意

考虑使用专用的 AWS 帐户来运行生产环境集群。如果使用 AWS Organizations，您可以使用您所在机构的 AWS 帐户或创建一个新账户。

流程

1. 登录到 AWS 管理控制台。
2. 进入 ROSA 服务。
3. 单击 **Get started**。
   验证 ROSA 先决条件 页面将打开。
4. 在 **ROSA 启用** 下，确保显示绿色勾号，**并启用了之前启用的 ROSA**。
   如果没有，请按照以下步骤执行：
   a. 选中 **I agree to share my contact information to Red Hat** 旁边的复选框。
   b. 点 **Enable ROSA**。
      在短暂等待后，会显示应绿色勾号并显示**启用了 ROSA** 的信息。
5. 在 **Service Quotas** 下，确保显示一个绿色检查，**并且您的配额满足 ROSA 的要求**。
   如果您看到 **您的配额不符合最低要求**，请记下配额类型和错误消息中列出的最小值。有关 请求配额增加的信息， 请参阅 Amazon 文档。Amazon 可能需要几小时才能批准配额请求。
6. 在 **ELB 服务链接的角色** 下，确保显示绿色勾号和 **AWSServiceRoleForElasticLoadBalancing 已存在**。
7. 点 **Continue to Red Hat**。
   Get started with Red Hat OpenShift Service on AWS (ROSA)页面会在一个新标签页中打开。
   在此页面中已完成第 1 步，现在可以继续执行第 2 步。

其他资源

- ROSA 启用错误故障排除

安装和配置所需的 CLI 工具

使用以下步骤在您的工作站上安装和配置。

流程

1. 安装和配置最新的 AWS CLI (**aws**)。
   a. 按照 AWS 命令行界面文档为您的操作系统安装和配置 AWS CLI。

在 **.aws/credentials** 文件中指定 **aws_access_key_id**、**aws_secret_access_key** 和 **region**。请参阅 AWS 文档中的 AWS 配置基础知识。

注意

您可以选择使用 **AWS_DEFAULT_REGION** 环境变量设置默认 AWS 区域。

b. 查询 AWS API 以验证是否已安装并配置了 AWS CLI：

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

输出示例

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

2. 安装和配置最新的 ROSA CLI (**rosa**)。

a. 从 Red Hat OpenShift Cluster Manager Hybrid Cloud Console 上的 **Downloads** 页面下载您的操作系统的 ROSA CLI 的最新版本。

b. 从下载的存档中提取 **rosa** 二进制文件。以下示例从 Linux tar 归档中提取二进制文件：

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

c. 在您的路径中添加 **rosa**。在以下示例中，**/usr/local/bin** 目录包含在用户的路径中：

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

d. 通过查询 **rosa** 版本来验证 ROSA CLI 是否已正确安装：

```
$ rosa version
```

输出示例

```
1.2.15
Your ROSA CLI is up to date.
```

e. 使用 ROSA CLI 登录您的红帽帐户：

```
$ rosa login
```

输出示例

```
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:
```

进入命令输出中列出的 URL，以获取离线访问令牌。在 CLI 提示符后指定令牌以进行登录。

注意

之后，您可以在运行 **rosa login** 命令时使用 **--token="<offline_access_token>"** 参数指定离线访问令牌。

f. 验证您是否已成功登录，并检查您的凭证：

```
$ rosa whoami
```

输出示例

```
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>
```

在继续进行前，检查输出中的信息是否正确。

1.3. 使用默认自动模式创建带有 AWS STS 的 ROSA 集群

Red Hat OpenShift Cluster Manager 是 Red Hat Hybrid Cloud Console 上的受管服务，您可以安装、修改、操作和升级 Red Hat OpenShift 集群。此服务允许您通过单一仪表板处理机构的所有集群。本文档中的步骤使用 OpenShift Cluster Manager 中的 **自动** 模式，使用当前的 AWS 帐户立即创建所需的 Identity and Access Management (IAM)资源。所需资源包括帐户范围内的 IAM 角色和策略、特定于集群的 Operator 角色和策略，以及 OpenID Connect (OIDC)身份提供程序。

当使用 OpenShift Cluster Manager Hybrid Cloud Console 在 AWS (ROSA)集群中创建使用 STS 的 Red Hat OpenShift Service 时，您可以选择默认选项来快速创建集群。

在使用 OpenShift Cluster Manager Hybrid Cloud Console 部署带有 STS 的 ROSA 集群之前，您必须将 AWS 帐户与红帽机构相关联，并创建所需的账户范围的 STS 角色和策略。

默认集群规格概述
您可以使用默认安装选项快速创建带有安全令牌服务(STS)的 Red Hat OpenShift Service on AWS (ROSA)集群。以下摘要描述了默认集群规格。

组件	默认规格
帐户和角色	• 默认 IAM 角色前缀： **ManagedOpenShift** • 没有创建集群管理员角色

组件	默认规格
集群设置	• 默认集群版本：Latest • 使用 Red Hat OpenShift Cluster Manager 混合云控制台安装的默认 AWS 区域：us-east-1 （美国东部，北弗吉尼亚） • 可用性： data plane 的单一区 • 启用默认的 EC2 IMDS 端点(v1 和 v2) • 监控用户定义的项目：启用
Encryption	• 云存储以静态方式加密 • 未启用额外的 etcd 加密 • 默认 AWS Key Management Service (KMS)密钥用作持久数据的加密密钥
Control plane 节点配置	• control plane 节点实例类型： m5.2xlarge (8 vCPU, 32 GiB RAM) • control plane 节点数： 3
基础架构节点配置	• 基础架构节点实例类型：r5.xlarge (4 vCPU，32 GiB RAM) • 基础架构节点数： 2
Compute 节点机器池	• Compute 节点实例类型： m5.xlarge (4 vCPU 16, GiB RAM) • Compute 节点数： 2 • 自动扩展：未启用 • 没有额外节点标签
网络配置	• 集群隐私：公共 • 没有配置集群范围的代理
无类别域间路由 (CIDR) 范围	• Machine CIDR: 10.0.0.0/16 • Service CIDR: 172.30.0.0/16 • Pod CIDR: 10.128.0.0/16 • 主机前缀：/23

组件	默认规格
集群角色和策略	• 用于创建 Operator 角色和 OpenID Connect(OIDC)供应商的模式： **auto** **注意** 对于在混合云控制台上使用 OpenShift Cluster Manager 的安装，**自动** 模式需要管理员特权的 OpenShift Cluster Manager 角色。 • 默认 Operator 角色前缀： <**cluster_name>-<4_digit_random_string>**
集群更新策略	• 独立更新 • 1 小时用于节点排空的宽限期

了解 AWS 帐户关联

在 Red Hat Hybrid Cloud Console 上使用 Red Hat OpenShift Cluster Manager 创建使用 AWS 安全令牌服务(STS)的 Red Hat OpenShift Service on AWS (ROSA)集群之前，您必须将 AWS 帐户与您的红帽机构相关联。您可以通过创建并链接以下 IAM 角色来关联您的帐户。

OpenShift Cluster Manager 角色

创建 OpenShift Cluster Manager IAM 角色并将其链接到您的红帽机构。
您可以将基本或管理权限应用到 OpenShift Cluster Manager 角色。基本权限使用 OpenShift Cluster Manager 启用集群维护。管理权限允许使用 OpenShift Cluster Manager 自动部署特定于集群的 Operator 角色和 OpenID Connect(OIDC)供应商。

用户角色

创建用户 IAM 角色并将其链接到您的红帽用户帐户。红帽用户帐户必须存在于链接到 OpenShift Cluster Manager 角色的红帽机构中。
当使用 OpenShift Cluster Manager Hybrid Cloud Console 安装集群和所需的 STS 资源时，红帽使用用户角色来验证 AWS 身份。

将您的 AWS 帐户与红帽机构相关联

在 Red Hat Hybrid Cloud Console 上使用 Red Hat OpenShift Cluster Manager 创建使用 AWS 安全令牌服务(STS)的 Red Hat OpenShift Service on AWS (ROSA)集群之前，创建一个 OpenShift Cluster Manager IAM 角色并将其链接到您的红帽机构。然后，创建一个用户 IAM 角色，并将其链接到同一红帽机构中的红帽用户帐户。

流程

1. 创建 OpenShift Cluster Manager 角色并将其链接到您的红帽机构：

注意

要使用 OpenShift Cluster Manager 混合云控制台启用集群特定 Operator 角色和 OpenID Connect (OIDC)供应商的自动部署，您必须在创建 ROSA 集群的 *帐户和角色步骤中选择 Admin OCM* **角色** 命令。如需有关 OpenShift Cluster Manager 角色的基本和管理特权的更多信息，*请参阅了解 AWS 帐户关联*。

注意

如果您在 OpenShift Cluster Manager 混合云控制台中创建 ROSA 集群的 **帐户和角色** 步骤中选择了 *Basic OCM* 角色命令，则必须使用手动模式部署 ROSA 集群。在后续步骤中，系统将提示您配置特定于集群的 Operator 角色和 OpenID Connect (OIDC)供应商。

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

选择提示符处的默认值，以快速创建和连接角色。

2. 创建用户角色并将其链接到您的红帽用户帐户：

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

选择提示符处的默认值，以快速创建和连接角色。

注意

红帽用户帐户必须存在于链接到 OpenShift Cluster Manager 角色的红帽机构中。

创建集群范围的 STS 角色和策略

在使用 Red Hat OpenShift Cluster Manager Hybrid Cloud Console 之前，请先在 AWS (ROSA)集群上创建使用 AWS 安全令牌服务(STS)的 Red Hat OpenShift Service，创建所需的 account-wide STS 角色和策略，包括 Operator 策略。

流程

1. 如果 AWS 帐户中没有它们，请创建所需的集群范围的 STS 角色和策略：

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

选择提示中的默认值，以快速创建角色和策略。

使用 OpenShift Cluster Manager 默认选项创建集群

当在 Red Hat Hybrid Cloud Console 上使用 Red Hat OpenShift Cluster Manager 创建使用 AWS 安全令牌服务(STS)的 Red Hat OpenShift Service on AWS (ROSA)集群时，您可以选择默认选项来快速创建集群。您还可以使用 admin OpenShift Cluster Manager IAM 角色启用集群特定 Operator 角色和 OpenID Connect (OIDC)供应商的自动部署。

流程

1. 导航到 OpenShift Cluster Manager 并选择 **Create cluster**。

2. 在 **Create an OpenShift 集群** 页面中，在 **Red Hat OpenShift Service on AWS (ROSA)** 行中选择 **Create cluster**。

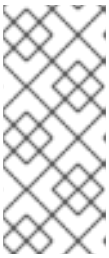
3. 验证您的 AWS 帐户 ID 是否在**关联的 AWS 帐户** 下拉菜单中列出，且安装程序、支持、worker 和 control plane 帐户角色 Amazon Resource Names (ARN) 是否在 **Accounts 和 roles** 页面中列出。

注意

如果您的 AWS 帐户 ID 没有列出，请检查您已成功将 AWS 帐户与红帽机构相关联。如果没有列出您的帐户角色 ARN，请检查 AWS 帐户中是否存在所需的 account-wide STS 角色。

4. 点击 **Next**。

5. 在 **Cluster details** 页面中，输入 **Cluster name**。将默认值留在剩余的字段中，然后点 **Next**。



注意

集群创建生成域前缀，作为您在 **openshiftapps.com** 上置备的集群的子域。如果集群名称小于或等于 15 个字符，该名称用于域前缀。如果集群名称超过 15 个字符，则域前缀会随机生成为 15 个字符的字符串。要自定义子域，请选择 **Create custom domain prefix** 复选框，然后在 **Domain prefix** 字段中输入您的域前缀名称。

6. 要快速部署集群，保留 **Cluster settings**, **Networking**, **Cluster roles and policies**, 和 **Cluster updates** 页中的默认选项，点每个页中的 **Next**。

7. 在 **Review your ROSA cluster** 页中，查看您选择的概述并点 **Create cluster** 开始安装。

8. 可选：在 **Overview** 选项卡中，您可以通过选择 **Enable** 来启用删除保护功能，该功能直接位于 **Delete Protection: Disabled** 下。这将阻止集群被删除。要禁用删除保护，请选择 **Disable**。默认情况下，集群禁用了删除保护功能来创建。

验证

- 您可以在集群的 **Overview** 页面中检查安装的进度。您可以在同一页面中查看安装日志。当页面的 **Details** 部分中的 **Status** 列为 **Ready** 时，您的集群已就绪。

注意

如果安装失败，或者集群的**状**态在大约 40 分钟后仍没有变为 **Ready**，请检查安装故障排除文档以了解详细信息。如需更多信息，*请参阅故障排除安装*。有关联系红帽支持以获取帮助的步骤，请参阅 *获取 Red Hat OpenShift Service on AWS 的支持*。

1.4. 创建集群管理员用户以快速集群访问

在配置身份提供程序前，您可以创建具有 **cluster-admin** 特权的用户，以便立即在 AWS (ROSA) 集群上访问 Red Hat OpenShift Service。

注意

当您需要快速访问新部署的集群时，集群管理员用户很有用。但是，请考虑配置身份提供程序，并根据需要为身份提供程序用户授予集群管理员特权。有关为您的 ROSA 集群设置身份提供程序的更多信息，请参阅*配置身份提供程序并授予集群访问权限*。

流程

1. 创建集群管理员用户：

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

1 将 **<cluster_name>** 替换为集群的名称。

输**出示例**

```
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.
```

注意

激活 **cluster-admin** 用户的过程可能需要大约一分钟才能完成。

其他资源

- 有关登录到 ROSA web 控制台的步骤，请参阅通过 Web 控制台访问集群。

1.5. 配置身份提供程序并授予集群访问权限

Red Hat OpenShift Service on AWS (ROSA)包括内置 OAuth 服务器。创建 ROSA 集群后，您必须将 OAuth 配置为使用身份提供程序。然后，您可以在配置的身份提供程序中添加成员以授予它们对集群的访问权限。

您还可以根据需要为身份提供程序用户授予具有 **cluster-admin** 或 **dedicated-admin** 特权的身份提供程序用户。

配置身份提供程序

您可以在 AWS (ROSA) 集群上为 Red Hat OpenShift Service 配置不同的身份提供程序类型。支持的类型包括 GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect 和 htpasswd 身份提供程序。

重要

htpasswd 身份提供程序选项仅包含创建单个静态管理用户。htpasswd 不支持作为 AWS 上的 Red Hat OpenShift Service 的通用身份提供程序。

以下流程将 GitHub 身份提供程序配置为示例。

流程

1. 进入 github.com 并登录到您的 GitHub 帐户。
2. 如果您没有用于置备 ROSA 集群的现有 GitHub 组织，请创建一个。按照 GitHub 文档中的步骤操作。
3. 为集群配置 GitHub 身份提供程序，仅限于 GitHub 组织的成员。

   a. 使用互动模式配置身份提供程序：

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

   (1) 将 **<cluster_name>** 替换为集群的名称。

   输出示例

```
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) 使用您的 GitHub 机构的名称替换 **<github_org_name>**。

   b. 使用输出中的 URL 并选择 **Register application**，在 GitHub 组织中注册新的 OAuth 应用程序。通过注册应用程序，您可以启用 ROSA 中构建的 OAuth 服务器，以便验证您的 GitHub 组织的成员到集群中。

注意

Register a new OAuth application GitHub 表单中的字段通过 ROSA CLI 定义的 URL 自动填充所需的值。

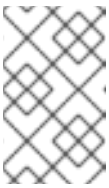
   c. 使用 GitHub OAuth 应用页面中的信息填充剩余的 **rosa create idp** 交互式提示。

   持续的输出示例

```
...
? 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. 使用 GitHub OAuth 应用程序的客户端 ID 替换 **<github_client_id>**。
2. 使用 GitHub OAuth 应用程序的客户端 secret 替换 **<github_client_secret>**。
3. 指定 **claim** 作为映射方法。



注意

激活身份提供商配置的过程可能需要大约两分钟。如果您配置了 **cluster-admin** 用户，可以通过运行 **oc get pods -n openshift-authentication --watch** 来监控使用更新的配置重新部署 OAuth pod。

d. 输入以下命令验证身份提供程序是否已正确配置：

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

输**出示例**

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

其他资源

- 有关配置每个 支持的身份提供程序类型的详细步骤，请参阅为 STS 配置身份提供程序。

授予用户对集群的访问权限

您可以通过将 Red Hat OpenShift Service 添加到您配置的身份供应商，授予用户对 Red Hat OpenShift Service on AWS (ROSA) 集群的访问权限。

您可以为 ROSA 集群配置不同类型的身份提供程序。以下示例流程将用户添加到配置为集群身份的 GitHub 机构中。

流程

1. 进入 github.com 并登录到您的 GitHub 帐户。
2. 邀请需要访问您的 GitHub 机构 ROSA 集群的用户。按照 GitHub 文档中的邀请用户加入到您的机构 。

为用户授予管理员权限

将用户添加到配置的身份提供程序后，您可以在 AWS (ROSA) 集群中为 Red Hat OpenShift Service 授予用户 **cluster-admin** 或 **dedicated-admin** 权限。

流程

- 为身份提供程序用户配置 **cluster-admin** 权限：

  a. 授予用户 **cluster-admin** 权限：

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

  (1) 使用身份提供程序用户和集群名称替换 **<idp_user_name>** 和 **<cluster_name>**。

  输**出示例**

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

  b. 验证该用户是否被列为 **cluster-admins** 组的成员：

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

  输**出示例**

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

- 为身份提供程序用户配置 **dedicated-admin** 权限：

  a. 授予用户 **dedicated-admin** 权限：

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

  输**出示例**

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

  b. 验证该用户是否被列为 **dedicated-admins** 组的成员：

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

  输**出示例**

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

其他资源

- 集群管理角色
- 客户管理员用户

1.6. 通过 WEB 控制台访问集群

创建集群管理员用户或将用户添加到配置的身份提供程序后，您可以通过 Web 控制台登录到 Red Hat OpenShift Service on AWS (ROSA) 集群。

流程

1. 获取集群的控制台 URL：

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

(1) 将 **<cluster_name>** 替换为集群的名称。

输**出示例**

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

2. 进入上一步输出中的控制台 URL 并登录。

- 如果创建了 **cluster-admin** 用户，请使用提供的凭证登录。
- 如果您为集群配置了身份提供程序，请在 **Log in with...** 对话框中选择身份提供程序名称，并完成您的供应商出示的任何授权请求。

1.7. 从 DEVELOPER CATALOG 部署应用程序

在 AWS Web 控制台中，从 Developer Catalog 部署测试应用程序，并使用路由公开测试应用程序。

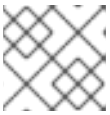
前提条件

- 已登陆到 Red Hat Hybrid Cloud Console 。
- 您在 AWS 集群上创建了 Red Hat OpenShift Service。
- 已为集群配置身份提供程序。
- 将您的用户帐户添加到配置的身份提供程序中。

流程

1. 进入 OpenShift Cluster Manager 中的 **Clusters** 页面。
2. 点击您要查看的集群旁的选项图标(HBAC)。
3. 单击 **Open console**。
4. 集群控制台将在新的浏览器窗口中打开。使用您配置的身份提供程序凭证登录到您的红帽帐户。
5. 在 **Administrator** 视角中，选择 **Home → Projects → Create Project**。
6. 输入项目的名称，并选择性地添加 **Display Name** 和 **Description**。
7. 点 **Create** 以创建该项目。
8. 切换到 **Developer** 视角并选择 **+Add**。验证 **所选项目** 是您刚刚创建的项目。
9. 在 **Developer Catalog** 对话框中，选择 **All services**。
10. 在 **Developer Catalog** 页面中，从菜单中选择 **Languages → JavaScript**。

11. 单击 **Node.js**，然后单击 **Create** 以打开 **Create Source-to-Image 应用** 页面。



注意

您可能需要点 **Clear All Filters** 以显示 **Node.js** 选项。

12. 在 **Git** 部分中，单击 **Try 示例**。
13. 在 **Name** 字段中添加一个唯一名称。该值将用于命名关联的资源。
14. 确认选择了 **Deployment** 和 **Create a route**。
15. 点 **Create** 以部署应用。部署 pod 需要几分钟时间。
16. 可选：选择 **Node.js** 应用程序并查看其边栏来检查 **Topology** 窗格中的 pod 状态。您必须等待 **nodejs** 构建完成，并且 **nodejs** Pod 处于 **Running** 状态，然后继续。
17. 部署完成后，点应用程序的路由 URL，其格式与以下内容类似：

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

浏览器中打开一个新标签页，其中包含类似如下的信息：

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

18. 可选：删除应用程序并清理您创建的资源：
    a. 在 **Administrator** 视角中，进入 **Home → Projects**。
    b. 点项目的操作菜单，再选择 **Delete Project**。

1.8. 撤销管理员特权和用户访问权限

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa** 为用户撤销 **cluster-admin** 或 **dedicated-admin** 权限。

要从用户撤销集群访问，您必须从配置的身份提供程序中删除该用户。

按照本节中的步骤从用户撤销管理员权限或集群访问。

从用户撤销管理员权限

按照本节中的步骤从用户撤销 **cluster-admin** 或 **dedicated-admin** 权限。

流程

- 从身份提供程序用户撤销 **cluster-admin** 权限：
  a. 撤销 **cluster-admin** 权限：

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

(1) 使用身份提供程序用户和集群名称替换 **<idp_user_name>** 和 **<cluster_name>**。

输出示例

```
? 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. 验证该用户没有列为 **cluster-admins** 组的成员：

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

输出示例

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

- 从身份提供程序用户撤销 **dedicated-admin** 权限：

a. 撤销 **dedicated-admin** 权限：

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

输出示例

```
? 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. 验证该用户没有列为 **dedicated-admins** 组的成员：

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

输出示例

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

撤销对集群的用户访问权限
您可以将身份提供程序用户从配置的身份提供程序中删除来撤销集群访问权限。

您可以为 ROSA 集群配置不同类型的身份提供程序。以下示例流程为为集群配置身份的 GitHub 组织的成员撤销集群访问权限。

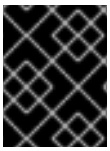
流程

1. 进入 github.com 并登录到您的 GitHub 帐户。
2. 从 GitHub 组织中删除该用户。按照 GitHub 文档中的从您的机构中删除成员的步骤进行操作。

1.9. 删除 ROSA 集群和 AWS STS 资源

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa** 删除使用 AWS 安全令牌服务 (STS) 的 ROSA 集群。您还可以使用 ROSA CLI 删除 AWS Identity and Access Management (IAM) 帐户范围内的角色、特定于集群的 Operator 角色，以及 OpenID Connect (OIDC)供应商。要删除集群范围的内联和

Operator 策略，您可以使用 AWS IAM 控制台。



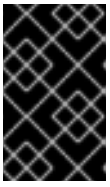
重要

帐户范围的 IAM 角色和策略可能被同一 AWS 帐户中的其他 ROSA 集群使用。只有其他集群不需要的资源，才必须删除这些资源。

流程

1. 删除集群并观察日志，将 **<cluster_name>** 替换为集群的名称或 ID:

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



重要

在删除 IAM 角色、策略和 OIDC 供应商前，您必须等待集群删除完成。需要集群范围的角色来删除安装程序创建的资源。需要特定于集群的 Operator 角色来清理 OpenShift Operator 创建的资源。Operator 使用 OIDC 供应商进行身份验证。

2. 删除集群 Operator 用于身份验证的 OIDC 供应商：

```
$ rosa delete oidc-provider -c <cluster_id> --mode auto 1
```

1 将 **<cluster_id>** 替换为集群的 ID。

注意

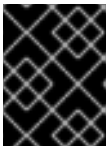
您可以使用 **-y** 选项，在提示符处自动回答 yes。

3. 删除特定于集群的 Operator IAM 角色：

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

1 将 **<cluster_id>** 替换为集群的 ID。

4. 删除集群范围的角色：



重要

帐户范围的 IAM 角色和策略可能被同一 AWS 帐户中的其他 ROSA 集群使用。只有其他集群不需要的资源，才必须删除这些资源。

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

1 您必须包含 **--<prefix>** 参数。将 **<prefix>** 替换为要删除的集群范围角色前缀。如果您在创建集群范围的角色时没有指定自定义前缀，请指定默认前缀 **ManagedOpenShift**。

5. 删除您为使用 STS 的 ROSA 部署创建的账户范围的内联（inline）和 Operator IAM 策略：

a. 登录到 AWS IAM 控制台。

b. 进入到 **Access management → Policies**，再选中其中一个帐户范围策略的复选框。

c. 选择策略后，点 **Actions → Delete** 以打开删除策略对话框。

d. 输入策略名称以确认删除，然后选择 **Delete** 以删除策略。

e. 重复此步骤，从集群中删除每个集群范围的内联和 Operator 策略。

1.10. 后续步骤

- 使用 OpenShift Cluster Manager 控制台在集群中添加服务
- 管理计算节点
- 配置监控堆栈

1.11. 其他资源

- 有关使用 AWS STS 设置帐户和 ROSA 集群的更多信息，请参阅使用 STS 部署工作流了解 ROSA。
- 有关在不使用 AWS STS 的情况下设置帐户和 ROSA 集群的更多信息，请参阅了解 ROSA 部署工作流。
- 有关升级集群的更多信息，请参阅升级 ROSA Classic 集群。

第 2 章 在 AWS 上开始使用 RED HAT OPENSHIFT SERVICE 的完整指南

注意

如果您要寻找 ROSA 的快速入门指南，请参阅 Red Hat OpenShift Service on AWS 快速入门指南。

按照本入门文档，在 AWS (ROSA)集群上创建 Red Hat OpenShift Service，授予用户访问权限、部署第一个应用程序，并了解如何撤销用户访问和删除您的集群。

您可以创建使用 AWS Security Token Service (STS) 的集群，也可以创建不使用它的集群。本文档中的步骤可让您创建使用 AWS STS 的集群。有关在 ROSA 集群中使用 AWS STS 的更多信息，请参阅使用 AWS 安全令牌服务。

2.1. 前提条件

- 您已参阅了对 Red Hat OpenShift Service on AWS (ROSA)的介绍，以及 ROSA 架构模型和 架构概念 的文档。
- 您已阅读有关限制和可扩展性的文档，以及规划环境的指导信息。
- 您已查看了使用 STS 的 ROSA 的 AWS 先决条件 。
- 您的系统满足运行 ROSA 集群的 AWS 服务配额要求 。

2.2. 设置环境

在 AWS (ROSA) 集群上创建 Red Hat OpenShift Service 前，您必须完成以下任务来设置您的环境：

- 根据您的 AWS 和 Red Hat 帐户验证 ROSA 的先决条件。
- 安装和配置所需的命令行界面(CLI)工具。
- 验证 CLI 工具的配置。

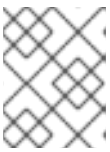
您可以按照本节中的步骤完成这些设置要求。

2.2.1. 验证 ROSA 先决条件

使用此流程中的步骤在您的 AWS 帐户中启用 Red Hat OpenShift Service on AWS (ROSA)。

前提条件

- 您有红帽帐户。
- 您有一个 AWS 帐户。



注意

考虑使用专用的 AWS 帐户来运行生产环境集群。如果使用 AWS Organizations，您可以使用您所在机构的 AWS 帐户或创建一个新账户。

流程

1. 登录到 AWS 管理控制台。
2. 进入 ROSA 服务。
3. 单击 **Get started**。
   验证 ROSA 先决条件 页面将打开。
4. 在 **ROSA 启用** 下，确保显示绿色勾号，**并启用了之前启用的 ROSA**。
   如果没有，请按照以下步骤执行：
   a. 选中 **I agree to share my contact information to Red Hat** 旁边的复选框。
   b. 点 **Enable ROSA**。
      在短暂等待后，会显示应绿色勾号并显示**启用了 ROSA** 的信息。
5. 在 **Service Quotas** 下，确保显示一个绿色检查，**并且您的配额满足 ROSA 的要求**。
   如果您看到 **您的配额不符合最低要求**，请记下配额类型和错误消息中列出的最小值。有关 请求配额增加的信息，请参阅 Amazon 文档。Amazon 可能需要几小时才能批准配额请求。
6. 在 **ELB 服务链接的角色** 下，确保显示绿色勾号和 **AWSServiceRoleForElasticLoadBalancing 已存在**。
7. 点 **Continue to Red Hat**。
   Get started with Red Hat OpenShift Service on AWS (ROSA)页面会在一个新标签页中打开。
   在此页面中已完成第 1 步，现在可以继续执行第 2 步。

其他资源

- ROSA 启用错误故障排除

2.2.2. 安装和配置所需的 CLI 工具

使用以下步骤在您的工作站上安装和配置 AWS、Red Hat OpenShift Service on AWS (ROSA)和 OpenShift CLI 工具。

前提条件

- 您有一个 AWS 帐户。
- 您创建了红帽帐户。

注意

您可以通过进入到 console.redhat.com 并选择 **Register for a Red Hat account** 来创建红帽帐户。

流程

1. 安装和配置最新的 AWS CLI (**aws**)。
   a. 按照 AWS 命令行界面文档为您的操作系统安装和配置 AWS CLI。
      在 **.aws/credentials** 文件中指定 **aws_access_key_id**、**aws_secret_access_key** 和 **region**。请参阅 AWS 文档中的 AWS 配置基础知识。

注意

您可以选择使用 **AWS_DEFAULT_REGION** 环境变量设置默认 AWS 区域。

b. 查询 AWS API 以验证是否已安装并配置了 AWS CLI：

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

输**出示例**

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

2. 安装和配置最新的 ROSA CLI (**rosa**)。

a. 从 Red Hat OpenShift Cluster Manager Hybrid Cloud Console 上的 Downloads 页面下载您的操作系统的 ROSA CLI 的最新版本。

b. 从下载的存档中提取 **rosa** 二进制文件。以下示例从 Linux tar 归档中提取二进制文件：

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

c. 在您的路径中添加 **rosa**。在以下示例中，**/usr/local/bin** 目录包含在用户的路径中：

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

d. 通过查询 **rosa** 版本来验证 ROSA CLI 是否已正确安装：

```
$ rosa version
```

输**出示例**

```
1.2.15
Your ROSA CLI is up to date.
```

e. 可选：为 ROSA CLI 启用 tab 自动完成功能。启用 tab 自动完成功能后，您可以按 **Tab** 键两次来自动完成子命令并接收命令建议。
ROSA Tab 补全可用于不同的 shell 类型。以下示例在 Linux 主机上为 Bash 启用永久性 tab 自动完成功能。该命令为 Bash 生成 **rosa** 选项卡的完成配置文件，并将其保存到 **/etc/bash_completion.d/** 目录中：

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

您必须打开一个新终端，才能激活配置。

注意

有关为不同 shell 类型配置 **rosa** 选项卡完成的步骤，请参阅运行 **rosa completion --help** 的帮助菜单。

f. 使用 ROSA CLI 登录您的红帽帐户：

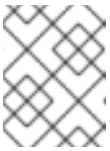
```
$ rosa login
```

-

输出示例

```
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:
```

进入命令输出中列出的 URL，以获取离线访问令牌。在 CLI 提示符后指定令牌以进行登录。



注意

之后，您可以在运行 **rosa login** 命令时使用 **--token="<offline_access_token>"** 参数指定离线访问令牌。

g. 验证您是否已成功登录，并检查您的凭证：

```
$ rosa whoami
```

输出示例

```
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>
```

在继续进行前，检查输出中的信息是否正确。

3. 安装和配置最新的 OpenShift CLI (**oc**)。

a. 使用 ROSA CLI 下载 **oc** CLI 的最新版本：

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

b. 从下载的存档中提取 **oc** 二进制文件。以下示例从 Linux tar 归档中提取文件：

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

c. 在您的路径中添加 **oc** 二进制文件。在以下示例中，**/usr/local/bin** 目录包含在用户的路径中：

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

d. 验证 **oc** CLI 是否已正确安装：

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

输出示例

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

2.3. 创建带有 STS 的 ROSA 集群

使用以下方法之一，部署使用 AWS 安全令牌服务 (STS)的 Red Hat OpenShift Service on AWS (ROSA)集群。在每个场景中，您可以使用 Red Hat OpenShift Cluster Manager 或 ROSA CLI (**rosa**)来部署集群：

- **使用默认选项创建带有 STS 的 ROSA 集群：您可以使用默认选项**和自动 STS 资源创建快速创建带有 STS 的 ROSA 集群。
- **使用自定义创建带有 STS 的 ROSA 集群：您可以使用自定义**创建带有 STS 的 ROSA 集群。您还可以在创建所需的 STS 资源时选择**自动**和**手动**模式。

其他资源

- 有关部署没有 STS 的 ROSA 集群的详细步骤，请参阅 创建没有 AWS STS 的 ROSA 集群 和 在 ROSA 上创建 AWS PrivateLink 集群。
- 有关使用 STS 的 ROSA 部署所需的集群范围的 IAM 角色和策略的信息，请参阅帐户范围内的 IAM 角色和策略引用。
- 有关使用**自动**和**手动**模式创建所需的 STS 资源的详情，请参阅了解自动和手动部署模式。
- 有关 ROSA 更新生命周期的信息，请参阅 Red Hat OpenShift Service on AWS 更新生命周期 。

2.4. 创建集群管理员用户以快速集群访问

在配置身份提供程序前，您可以创建具有 **cluster-admin** 特权的用户，以便立即在 AWS (ROSA) 集群上访问 Red Hat OpenShift Service。

注意

当您需要快速访问新部署的集群时，集群管理员用户很有用。但是，请考虑配置身份提供程序，并根据需要为身份提供程序用户授予集群管理员特权。有关为您的 ROSA 集群设置身份提供程序的更多信息，请参阅*配置身份提供程序并授予集群访问权限*。

前提条件

- 您有一个 AWS 帐户。
- 在您的工作站上安装和配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa**。
- 您可以使用 ROSA CLI (**rosa**)登录到您的红帽帐户。
- 您创建了 ROSA 集群。

流程

1. 创建集群管理员用户：

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

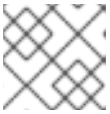
1 将 **<cluster_name>** 替换为集群的名称。

输**出示例**

```
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.
```



注意

激活 **cluster-admin** 用户的过程可能需要大约一分钟才能完成。

2. 通过 CLI 登录到集群：

   a. 运行上一步输出中提供的命令以登录：

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

   1 使用您的环境的 API URL 和集群管理员替换 **<api_url>** 和 **<cluster_admin_password>**。

   b. 验证您是否以 **cluster-admin** 用户身份登录到 ROSA 集群：

   ```
   $ oc whoami
   ```

   输**出示例**

   ```
   cluster-admin
   ```

其他资源

- 有关登录到 ROSA web 控制台的步骤，请参阅通过 Web 控制台访问集群

2.5. 配置身份提供程序并授予集群访问权限

Red Hat OpenShift Service on AWS (ROSA)包括内置 OAuth 服务器。创建 ROSA 集群后，您必须将 OAuth 配置为使用身份提供程序。然后，您可以在配置的身份提供程序中添加成员以授予它们对集群的访问权限。

您还可以根据需要为身份提供程序用户授予具有 **cluster-admin** 或 **dedicated-admin** 特权的身份提供程序用户。

2.5.1. 配置身份提供程序

您可以在 AWS (ROSA) 集群上为 Red Hat OpenShift Service 配置不同的身份提供程序类型。支持的类型包括 GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect 和 htpasswd 身份提供程序。

重要

htpasswd 身份提供程序选项仅包含创建单个静态管理用户。htpasswd 不支持作为 AWS 上的 Red Hat OpenShift Service 的通用身份提供程序。

以下流程将 GitHub 身份提供程序配置为示例。

前提条件

- 您有一个 AWS 帐户。
- 在您的工作站上安装和配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa**。
- 您可以使用 ROSA CLI (**rosa**)登录到您的红帽帐户。
- 您创建了 ROSA 集群。
- 您有一个 GitHub 用户帐户。

流程

1. 进入 github.com 并登录到您的 GitHub 帐户。
2. 如果您没有用于置备 ROSA 集群的现有 GitHub 组织，请创建一个。按照 GitHub 文档中的步骤操作。
3. 为集群配置 GitHub 身份提供程序，仅限于 GitHub 组织的成员。
   a. 使用互动模式配置身份提供程序：

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

1 将 **<cluster_name>** 替换为集群的名称。

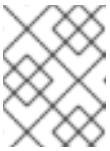
输**出示例**

```
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 使用您的 GitHub 机构的名称替换 **<github_org_name>**。

b. 使用输出中的 URL 并选择 **Register application**，在 GitHub 组织中注册新的 OAuth 应用程序。通过注册应用程序，您可以启用 ROSA 中构建的 OAuth 服务器，以便验证您的 GitHub 组织的成员到集群中。



注意

Register a new OAuth application GitHub 表单中的字段通过 ROSA CLI 定义的 URL 自动填充所需的值。

c. 使用 GitHub OAuth 应用页面中的信息填充剩余的 **rosa create idp** 交互式提示。

持续的输出示例

```
...
? 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 使用 GitHub OAuth 应用程序的客户端 ID 替换 **<github_client_id>**。

2 使用 GitHub OAuth 应用程序的客户端 secret 替换 **<github_client_secret>**。

3 指定 **claim** 作为映射方法。

注意

激活身份提供商配置的过程可能需要大约两分钟。如果您配置了 **cluster-admin** 用户，可以通过运行 **oc get pods -n openshift-authentication --watch** 来监控使用更新的配置重新部署 OAuth pod。

d. 输入以下命令验证身份提供程序是否已正确配置：

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

输出示例

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

其他资源

- 有关配置每个 支持的身份提供程序类型的详细步骤，请参阅为 STS配置身份提供程序

2.5.2. 授予用户对集群的访问权限

您可以通过将 Red Hat OpenShift Service 添加到您配置的身份供应商，授予用户对 Red Hat OpenShift Service on AWS (ROSA) 集群的访问权限。

您可以为 ROSA 集群配置不同类型的身份提供程序。以下示例流程将用户添加到配置为集群身份的 GitHub 机构中。

前提条件

- 您有一个 AWS 帐户。
- 在您的工作站上安装和配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa**。
- 您可以使用 ROSA CLI (**rosa**)登录到您的红帽帐户。
- 您创建了 ROSA 集群。
- 您有一个 GitHub 用户帐户。
- 您已为集群配置了 GitHub 身份提供程序。

流程

1. 进入 github.com 并登录到您的 GitHub 帐户。
2. 邀请需要访问您的 GitHub 机构 ROSA 集群的用户。按照 GitHub 文档中的邀请用户加入到您的机构 。

2.5.3. 为用户授予管理员权限

将用户添加到配置的身份提供程序后，您可以在 AWS (ROSA) 集群中为 Red Hat OpenShift Service 授予用户 **cluster-admin** 或 **dedicated-admin** 权限。

前提条件

- 您有一个 AWS 帐户。
- 在您的工作站上安装和配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa**。
- 您可以使用 ROSA CLI (**rosa**)登录到您的红帽帐户。
- 您创建了 ROSA 集群。
- 您已为集群配置了 GitHub 身份提供程序，并添加了身份提供程序用户。

流程

- 为身份提供程序用户配置 **cluster-admin** 权限：
  a. 授予用户 **cluster-admin** 权限：

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

(1) 使用身份提供程序用户和集群名称替换 **<idp_user_name>** 和 **<cluster_name>**。

输**出示例**

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

  b. 验证该用户是否被列为 **cluster-admins** 组的成员：

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

输**出示例**

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

- 为身份提供程序用户配置 **dedicated-admin** 权限：
  a. 授予用户 **dedicated-admin** 权限：

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

输**出示例**

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

  b. 验证该用户是否被列为 **dedicated-admins** 组的成员：

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

输**出示例**

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

其他资源

- 集群管理角色
- 客户管理员用户

2.6. 通过 WEB 控制台访问集群

创建集群管理员用户或将用户添加到配置的身份提供程序后，您可以通过 Web 控制台登录到 Red Hat OpenShift Service on AWS (ROSA) 集群。

前提条件

- 您有一个 AWS 帐户。
- 在您的工作站上安装和配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa**。
- 您可以使用 ROSA CLI (**rosa**)登录到您的红帽帐户。
- 您创建了 ROSA 集群。
- 您已创建了集群管理员用户，或将用户帐户添加到配置的身份提供程序。

流程

1. 获取集群的控制台 URL：

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

(1) 将 **<cluster_name>** 替换为集群的名称。

输**出示例**

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

2. 进入上一步输出中的控制台 URL 并登录。
   - 如果创建了 **cluster-admin** 用户，请使用提供的凭证登录。
   - 如果您为集群配置了身份提供程序，请在 **Log in with...** 对话框中选择身份提供程序名称，并完成您的供应商出示的任何授权请求。

2.7. 从 DEVELOPER CATALOG 部署应用程序

在 AWS Web 控制台中，从 Developer Catalog 部署测试应用程序，并使用路由公开测试应用程序。

前提条件

- 已登陆到 Red Hat Hybrid Cloud Console 。
- 您在 AWS 集群上创建了 Red Hat OpenShift Service。
- 已为集群配置身份提供程序。
- 将您的用户帐户添加到配置的身份提供程序中。

流程

1. 进入 OpenShift Cluster Manager 中的 **Clusters** 页面。
2. 点击您要查看的集群旁的选项图标(HBAC)。

3. 单击 **Open console**。
4. 集群控制台将在新的浏览器窗口中打开。使用您配置的身份提供程序凭证登录到您的红帽帐户。
5. 在 **Administrator** 视角中，选择 **Home → Projects → Create Project**。
6. 输入项目的名称，并选择性地添加 **Display Name** 和 **Description**。
7. 点 **Create** 以创建该项目。
8. 切换到 **Developer** 视角并选择 **+Add**。验证 **所选项目** 是您刚刚创建的项目。
9. 在 **Developer Catalog** 对话框中，选择 **All services**。
10. 在 **Developer Catalog** 页面中，从菜单中选择 **Languages → JavaScript**。
11. 单击 **Node.js**，然后单击 **Create** 以打开 **Create Source-to-Image 应用** 页面。

注意

您可能需要点 **Clear All Filters** 以显示 **Node.js** 选项。

12. 在 **Git** 部分中，单击 **Try 示例**。
13. 在 **Name** 字段中添加一个唯一名称。该值将用于命名关联的资源。
14. 确认选择了 **Deployment** 和 **Create a route**。
15. 点 **Create** 以部署应用。部署 pod 需要几分钟时间。
16. 可选：选择 **Node.js** 应用程序并查看其边栏来检查 **Topology** 窗格中的 pod 状态。您必须等待 **nodejs** 构建完成，并且 **nodejs** Pod 处于 **Running** 状态，然后继续。
17. 部署完成后，点应用程序的路由 URL，其格式与以下内容类似：

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

浏览器中打开一个新标签页，其中包含类似如下的信息：

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

18. 可选：删除应用程序并清理您创建的资源：
    a. 在 **Administrator** 视角中，进入 **Home → Projects**。
    b. 点项目的操作菜单，再选择 **Delete Project**。

2.8. 撤销管理员特权和用户访问权限

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa** 为用户撤销 **cluster-admin** 或 **dedicated-admin** 权限。

要从用户撤销集群访问，您必须从配置的身份提供程序中删除该用户。

按照本节中的步骤从用户撤销管理员权限或集群访问。

2.8.1. 从用户撤销管理员权限

按照本节中的步骤从用户撤销 **cluster-admin** 或 **dedicated-admin** 权限。

前提条件

- 在您的工作站上安装和配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa**。
- 您可以使用 ROSA CLI (**rosa**)登录到您的红帽帐户。
- 您创建了 ROSA 集群。
- 您已为集群配置了 GitHub 身份提供程序，并添加了身份提供程序用户。
- 为用户授予了 **cluster-admin** 或 **dedicated-admin** 权限。

流程

- 从身份提供程序用户撤销 **cluster-admin** 权限：
  a. 撤销 **cluster-admin** 权限：

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

  1 使用身份提供程序用户和集群名称替换 **<idp_user_name>** 和 **<cluster_name>**。

  输**出示例**

```
? 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. 验证该用户没有列为 **cluster-admins** 组的成员：

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

  输**出示例**

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

- 从身份提供程序用户撤销 **dedicated-admin** 权限：
  a. 撤销 **dedicated-admin** 权限：

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

  输**出示例**

```
? 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. 验证该用户没有列为 **dedicated-admins** 组的成员：

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

输出示例

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

2.8.2. 撤销对集群的用户访问权限

您可以将身份提供程序用户从配置的身份提供程序中删除来撤销集群访问权限。

您可以为 ROSA 集群配置不同类型的身份提供程序。以下示例流程为为集群配置身份的 GitHub 组织的成员撤销集群访问权限。

前提条件

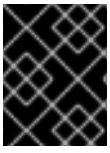
- 您有一个 ROSA 集群。
- 您有一个 GitHub 用户帐户。
- 您已为集群配置了 GitHub 身份提供程序，并添加了身份提供程序用户。

流程

1. 进入 github.com 并登录到您的 GitHub 帐户。
2. 从 GitHub 组织中删除该用户。按照 GitHub 文档中的从您的机构中删除成员的步骤进行操作。

2.9. 删除 ROSA 集群和 AWS STS 资源

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa** 删除使用 AWS 安全令牌服务 (STS) 的 ROSA 集群。您还可以使用 ROSA CLI 删除 AWS Identity and Access Management (IAM) 帐户范围内的角色、特定于集群的 Operator 角色，以及 OpenID Connect (OIDC)供应商。要删除集群范围的内联和 Operator 策略，您可以使用 AWS IAM 控制台。



重要

帐户范围的 IAM 角色和策略可能被同一 AWS 帐户中的其他 ROSA 集群使用。只有其他集群不需要的资源，才必须删除这些资源。

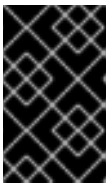
前提条件

- 在您的工作站上安装和配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa**。
- 您可以使用 ROSA CLI (**rosa**)登录到您的红帽帐户。
- 您创建了 ROSA 集群。

流程

1. 删除集群并观察日志，将 **<cluster_name>** 替换为集群的名称或 ID:

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



重要

在删除 IAM 角色、策略和 OIDC 供应商前，您必须等待集群删除完成。需要集群范围的角色来删除安装程序创建的资源。需要特定于集群的 Operator 角色来清理 OpenShift Operator 创建的资源。Operator 使用 OIDC 供应商进行身份验证。

2. 删除集群 Operator 用于身份验证的 OIDC 供应商：

```
$ rosa delete oidc-provider -c <cluster_id> --mode auto 1
```

1 将 **<cluster_id>** 替换为集群的 ID。

注意

您可以使用 **-y** 选项，在提示符处自动回答 yes。

3. 删除特定于集群的 Operator IAM 角色：

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

1 将 **<cluster_id>** 替换为集群的 ID。

4. 删除集群范围的角色：

重要

帐户范围的 IAM 角色和策略可能被同一 AWS 帐户中的其他 ROSA 集群使用。只有其他集群不需要的资源，才必须删除这些资源。

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

1 您必须包含 **--<prefix>** 参数。将 **<prefix>** 替换为要删除的集群范围角色前缀。如果您在创建集群范围的角色时没有指定自定义前缀，请指定默认前缀 **ManagedOpenShift**。

5. 删除您为使用 STS 的 ROSA 部署创建的账户范围的内联（inline）和 Operator IAM 策略：

   a. 登录到 AWS IAM 控制台。

   b. 进入到 **Access management → Policies**，再选中其中一个帐户范围策略的复选框。

   c. 选择策略后，点 **Actions → Delete** 以打开删除策略对话框。

   d. 输入策略名称以确认删除，然后选择 **Delete** 以删除策略。

   e. 重复此步骤，从集群中删除每个集群范围的内联和 Operator 策略。

2.10. 后续步骤

- 使用 OpenShift Cluster Manager 控制台在集群中添加服务
- 管理计算节点
- 配置监控堆栈

2.11. 其他资源

- 有关使用 AWS STS 设置帐户和 ROSA 集群的更多信息，请参阅使用 STS 的 ROSA 部署流程
- 有关在不使用 AWS STS 的情况下设置帐户和 ROSA 集群的更多信息，请参阅了解 ROSA 部署工作流
- 有关升级集群的更多信息，请参阅升级 ROSA Classic 集群

第 3 章 了解使用 STS 部署工作流的 ROSA

在 AWS (ROSA) 集群上创建 Red Hat OpenShift Service 前，您必须先满足 AWS 的先决条件，验证所需的 AWS 服务配额是否可用，并设置您的环境。

本文档概述了带有 STS 部署工作流阶段的 ROSA，并指代每个阶段的详细资源。

3.1. 使用 STS 部署工作流的 ROSA 概述

AWS 安全令牌服务 (STS) 是一个全局 Web 服务，它为 IAM 或联邦用户提供短期凭证。您可以在 AWS (ROSA) 上将 AWS STS 与 Red Hat OpenShift Service 搭配使用，为组件特定的 IAM 角色分配临时的、有有限权限的凭证。该服务可让集群组件使用安全云资源管理实践来发出 AWS API 调用。

您可以按照本节中介绍的工作流阶段设置和访问使用 STS 的 ROSA 集群。

1. 为使用 STS 的 ROSA 完成 AWS 的先决条件 。要部署使用 STS 的 ROSA 集群，您的 AWS 帐户必须满足先决条件。
2. 查看所需的 AWS 服务配额。要准备集群部署，请查看运行 ROSA 集群的 AWS 服务配额。
3. 设置环境并安装使用 STS 的 ROSA。在创建使用 STS 的 ROSA 集群前，您必须在 AWS 帐户中启用 ROSA，安装和配置所需的 CLI 工具，并验证 CLI 工具的配置。您还需要验证 AWS Elastic Load Balancing (ELB) 服务角色是否存在以及所需的 AWS 资源配额是否可用。
4. 快速创建使用 STS 的 ROSA 集群，或使用自定义来创建集群。使用 ROSA CLI (**rosa**) 或 Red Hat OpenShift Cluster Manager 创建使用 STS 的集群。您可以使用默认选项快速创建集群，也可以应用自定义以适应您的机构需求。
5. 访问集群。您可以配置身份提供程序，并根据需要为身份提供程序用户授予集群管理员特权。您还可以通过配置 **cluster-admin** 用户来快速访问新部署的集群。
6. 撤销用户对 ROSA 集群的访问权限。您可以使用 ROSA CLI 或 web 控制台撤销一个用户对使用 STS 的 ROSA 集群的访问。
7. 删除 ROSA 集群。您可以使用 ROSA CLI (**rosa**) 删除带有 STS 集群的 ROSA。删除集群后，您可以使用 AWS Identity and Access Management (IAM) 控制台删除 STS 资源。

3.2. 其他资源

- 有关使用 ROSA 部署工作流创建不使用 AWS STS 的集群的详情，请参阅了解 ROSA 部署工作流。