Red Hat OpenShift Service on AWS 4

安装带有 HCP 的 ROSA

在 AWS (ROSA) 集群上安装、访问和删除 Red Hat OpenShift Service。

Last Updated: 2024-07-03

Red Hat OpenShift Service on AWS 4 安装带有 HCP 的 ROSA

在 AWS (ROSA) 集群上安装、访问和删除 Red Hat OpenShift Service。

法律通告

摘要

本文档提供有关如何在使用托管 control plane 的 AWS (ROSA) 集群上安装 Red Hat OpenShift Service 的信息。

目录

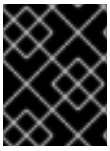
第 1 章 使用默认选项创建带有 HCP 集群的 ROSA

注意

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

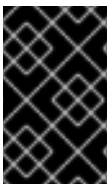
带有托管 control plane (HCP) 的 Red Hat OpenShift Service on AWS (ROSA) 提供了更高效且可靠的架构，以便在 AWS (ROSA) 集群上创建 Red Hat OpenShift Service。使用带有 HCP 的 ROSA 时，每个集群都有一个专用的 control plane，它在 ROSA 服务帐户中被隔离。

使用默认选项和自动 AWS Identity and Access Management (IAM) 资源快速创建带有 HCP 集群的 ROSA。您可以使用 ROSA CLI (**rosa**)部署集群。



重要

由于无法将现有的 ROSA 集群升级或转换为托管的 control plane 架构，您必须创建一个新集群以使用带有 HCP 功能的 ROSA。



重要

目前，使用 HCP 的 ROSA 不支持在 多个 AWS 帐户间共享 VPC。不要将带有 HCP 集群的 ROSA 安装到与另一个 AWS 帐户共享的子网。如需更多信息，请参阅 "支持单个 VPC 中的多个 ROSA 集群？"。

注意

带有 HCP 集群的 ROSA 仅支持 AWS 安全令牌服务(STS)身份验证。

进一步阅读

- 有关 ROSA 与 HCP 和 ROSA Classic 之间的比较，请参阅 比较架构模型 文档。
- 有关在 自动模式中使用 ROSA CLI 开始使用 HCP 的信息， 请参阅 AWS 文档。

其他资源

有关支持的证书的完整列表，请参阅 "Understanding process and security for Red Hat OpenShift Service on AWS" 的 Compliance 部分。

关于自动创建模式的注意事项

本文档中的步骤使用 ROSA CLI 中的 **auto** 模式，使用当前的 AWS 帐户立即创建所需的 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。

另外，您可以使用 **手动模式**，它输出创建 IAM 资源所需的 **aws** 命令，而不是自动部署它们。

后续步骤

- 确保您已完成 AWS 先决条件。

1.1. 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 HCP 集群的 ROSA。以下概述描述了默认集群规格。

表 1.1. 带有 HCP 集群规格的默认 ROSA

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
集群设置	• 默认集群版本： Latest • 使用 ROSA CLI (**rosa**)安装的默认 AWS 区域：由 **aws** CLI 配置定义 • 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	• 云存储会加密 • 没有启用额外的 etcd 加密 • 默认 AWS 密钥管理服务(KMS)密钥用作持久数据的加密密钥
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 • 没有额外的节点标签
网络配置	• 集群隐私：公共 • 您必须已经配置了自己的虚拟私有云(VPC) • 没有配置集群范围的代理

组件	默认规格
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  **注意** 在使用带有 HCP 的 ROSA 时，静态 IP 地址 **172.20.0.1** 会为内部 Kubernetes API 地址保留。机器、pod 和服务 CIDR 范围不得与此 IP 地址冲突。
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 • 节点排空 1 小时宽限期

1.2. 带有 HCP 先决条件的 ROSA

要使用 HCP 集群创建 ROSA，您必须有以下项目：

- 配置的虚拟私有云(VPC)
- 帐户范围内的角色
- OIDC 配置
- Operator 角色

1.2.1. 使用 HCP 集群为您的 ROSA 创建虚拟私有云

您必须有一个 Virtual Private Cloud (VPC)才能使用 HCP 集群创建 ROSA。您可以使用以下方法创建 VPC：

- 使用 Terraform 模板创建 VPC
- 在 AWS 控制台中手动创建 VPC 资源

注意

Terraform 指令用于测试和演示目的。您自己的安装需要对 VPC 进行一些修改，以便您自己的使用。您还应确保在使用这个 Terraform 脚本时，它位于您要安装集群的同一区域。在这些示例中，使用 **us-east-2**。

使用 Terraform 创建虚拟私有云

Terraform 是一个工具，允许您使用已建立的模板创建各种资源。以下过程使用默认选项来创建带有 HCP 集群的 ROSA。有关使用 Terraform 的更多信息，请参阅其他资源。

先决条件

- 您已在机器上安装 Terraform 版本 1.4.0 或更新版本。
- 您已在机器上安装了 Git。

流程

1. 运行以下命令，打开 shell 提示符并克隆 Terraform VPC 存储库：

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

2. 运行以下命令进入创建的目录：

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

3. 运行以下命令来启动 Terraform 文件：

```
$ terraform init
```

此进程完成后会出现确认初始化的消息。

4. 要基于现有的 Terraform 模板构建 VPC Terraform 计划，请运行 **plan** 命令。您必须包含 AWS 区域。您可以选择指定集群名称。在 **terraform plan** 完成后，一个 **rosa.tfplan** 文件会被添加到 **hypershift-tf** 目录。有关更详细的选项，请参阅 Terraform VPC 存储库的 README 文件。

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

5. 运行以下命令应用此计划文件来构建 VPC：

```
$ terraform apply rosa.tfplan
```

   a. 可选：您可以运行以下命令来捕获 Terraform-provisioned private、public 和 machinepool 子网 ID 的值作为环境变量，以便在使用 HCP 集群创建 ROSA 时使用：

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

   b. 使用以下命令验证变量是否已正确设置：

```
$ echo $SUBNET_IDS
```

输出示例

```
$ subnet-0a6a57e0f784171aa,subnet-078e84e5b10ecf5b0
```

其他资源

- 有关自定义 VPC 时可用选项的详细列表，请参阅 Terraform VPC 存储库。

手动创建虚拟私有云

如果您选择手动创建 Virtual Private Cloud (VPC)而不是使用 Terraform，请访问 AWS 控制台中的 VPC 页面。您的 VPC 必须满足下表中显示的要求。

表 1.2. VPC 的要求

要求	详情
VPC 名称	创建集群时需要具有特定的 VPC 名称和 ID。
CIDR 范围	您的 VPC CIDR 范围应该与您的机器 CIDR 匹配。
可用区	单个区需要一个可用区，对于多区的可用区需要三个可用区。
公共子网	对于公共集群，您必须有一个带有 NAT 网关的公共子网。私有集群不需要公共子网。
DNS 主机名和解析	您必须确保启用 DNS 主机名和解析。

标记您的子网

在使用 VPC 创建使用 HCP 集群的 ROSA 之前，您必须标记 VPC 子网。在使用这些资源前，自动化服务 preflight 检查会验证这些资源是否已正确标记。下表显示了您的资源应如何标记为以下内容：

资源	键	值
公共子网	**kubernetes.io/role/elb**	**1** 或没有值
专用子网	**kubernetes.io/role/internal-elb**	**1** 或没有值

注意

您必须至少标记一个专用子网，如果适用，以及一个公共子网。

先决条件

- 您已创建了 VPC。
- 已安装 **aws** CLI。

流程

1. 运行以下命令在终端中标记您的资源：

   a. 对于公共子网，请运行：

   ```
   $ aws ec2 create-tags --resources <public-subnet-id> --tags
   Key=kubernetes.io/role/elb,Value=1
   ```

   b. 对于专用子网，请运行：

   ```
   $ aws ec2 create-tags --resources <private-subnet-id> --tags
   Key=kubernetes.io/role/internal-elb,Value=1
   ```

验证

- 运行以下命令验证标签是否已正确应用：

  ```
  $ aws ec2 describe-tags --filters "Name=resource-id,Values=<subnet_id>"
  ```

  输出示例

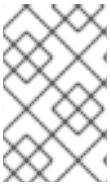
  ```
  TAGS    Name                        <subnet-id>       subnet  <prefix>-subnet-public1-us-east-1a
  TAGS    kubernetes.io/role/elb  <subnet-id>       subnet  1
  ```

其他资源

- Amazon VPC 入门
- HashiCorp Terraform 文档
- 子网自动发现

1.2.2. 创建集群范围的 STS 角色和策略

在使用 Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**)创建带有托管 control plane (HCP)集群的 Red Hat OpenShift Service on AWS (ROSA)前，请创建所需的帐户范围角色和策略，包括 Operator 策略。



注意

使用 HCP 集群的 ROSA 需要附加 AWS 受管策略的帐户和 Operator 角色。不支持客户管理的策略。有关使用 HCP 集群的 ROSA 的 AWS 管理策略的更多信息，请参阅 ROSA 帐户角色的 AWS 管理策略。

先决条件

- 您已使用 HCP 为 ROSA 完成 AWS 的先决条件。
- 您有可用的 AWS 服务配额。
- 您已在 AWS 控制台中启用了 ROSA 服务。

- 您已在安装主机上安装并配置了最新的 ROSA CLI (**rosa**)。
- 已使用 ROSA CLI 登录到您的红帽帐户。

流程

1. 如果 AWS 帐户中不存在它们，请创建所需的账户范围的 STS 角色，并通过运行以下命令附加策略：

```
$ rosa create account-roles --hosted-cp
```

2. 可选：运行以下命令将前缀设置为环境变量：

```
$ export ACCOUNT_ROLES_PREFIX=<account_role_prefix>
```

   - 运行以下命令，查看变量的值：

```
$ echo $ACCOUNT_ROLES_PREFIX
```

   输出**示例**

```
ManagedOpenShift
```

如需有关 ROSA 的 AWS 管理 IAM 策略的更多信息，请参阅 ROSA 的 AWS 管理的 IAM 策略。

1.2.3. 创建 OpenID Connect 配置

当将 ROSA 与 HCP 集群搭配使用时，您必须先创建 OpenID Connect (OIDC)配置。此配置已注册到 OpenShift Cluster Manager。

先决条件

- 您已使用 HCP 为 ROSA 完成 AWS 的先决条件。
- 您已完成了 Red Hat OpenShift Service on AWS 的 AWS 的先决条件。
- 您已在安装主机上安装并配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa**。

流程

1. 要创建 OIDC 配置和 AWS 资源，请运行以下命令：

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

   此命令返回以下信息：

   输出**示例**

```
? Would you like to create a Managed (Red Hat hosted) OIDC Configuration Yes
I: Setting up managed OIDC configuration
I: To create Operator Roles for this OIDC Configuration, run the following command and remember to replace <user-defined> with a prefix of your choice:
 rosa create operator-roles --prefix <user-defined> --oidc-config-id 13cdr6b
```

```
If you are going to create a Hosted Control Plane cluster please include '--hosted-cp'
I: Creating OIDC provider using 'arn:aws:iam::4540112244:user/userName'
? Create the OIDC provider? Yes
I: Created OIDC provider with ARN 'arn:aws:iam::4540112244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/13cdr6b'
```

在创建集群时，您必须提供 OIDC 配置 ID。CLI 输出为 **--mode auto** 提供这个值，否则您必须根据 **--mode manual** 的 **aws** CLI 输出来确定这些值。

2. 可选：您可以将 OIDC 配置 ID 保存为变量，以便稍后使用。运行以下命令来保存变量：

```
$ export OIDC_ID=<oidc_config_id> 1
```

1 在上面的示例输出中，OIDC 配置 ID 是 13cdr6b。

- 运行以下命令，查看变量的值：

```
$ echo $OIDC_ID
```

输**出示例**

```
13cdr6b
```

验证

- 您可以列出与用户机构关联的集群可用的 OIDC 配置。运行以下命令：

```
$ rosa list oidc-config
```

输**出示例**

```
ID                               MANAGED  ISSUER URL
SECRET ARN
2330dbs0n8m3chkkr25gkkcd8pnj3lk2  true
https://dvbwgdztaeq9o.cloudfront.net/2330dbs0n8m3chkkr25gkkcd8pnj3lk2
233hvnrjoqu14jltk6lhbhf2tj11f8un  false    https://oidc-r7u1.s3.us-east-1.amazonaws.com
aws:secretsmanager:us-east-1:242819244:secret:rosa-private-key-oidc-r7u1-tM3MDN
```

1.2.4. 创建 Operator 角色和策略

当将 ROSA 与 HCP 集群搭配使用时，您必须创建带有托管 control plane (HCP)部署的 Red Hat OpenShift Service on AWS (ROSA)所需的 Operator IAM 角色。集群 Operator 使用 Operator 角色获取执行集群操作所需的临时权限，如管理后端存储、云供应商凭证和对集群的外部访问权限。

先决条件

- 您已使用 HCP 为 ROSA 完成 AWS 的先决条件。
- 您已在安装主机上安装并配置了最新的 Red Hat OpenShift Service on AWS ROSA CLI (**rosa**)。
- 您创建了集群范围的 AWS 角色。

流程

1. 使用以下命令将前缀名称设置为环境变量：

```
$ export OPERATOR_ROLES_PREFIX=<prefix_name>
```

2. 要创建 Operator 角色，请运行以下命令：

```
$ rosa create operator-roles --hosted-cp --prefix=$OPERATOR_ROLES_PREFIX --oidc-config-id=$OIDC_ID --installer-role-arn arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role
```

以下分类提供了 Operator 角色创建的选项。

```
$ rosa create operator-roles --hosted-cp
 --prefix=$OPERATOR_ROLES_PREFIX (1)
 --oidc-config-id=$OIDC_ID (2)
 --installer-role-arn
arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role (3)
```

(1) 在创建这些 Operator 角色时，您必须提供一个前缀。如果不这样做会产生错误。如需有关 Operator 前缀的信息，请参阅本节的附加资源。

(2) 这个值是您为使用 HCP 集群的 ROSA 创建的 OIDC 配置 ID。

(3) 这个值是您在创建 ROSA 帐户角色时创建的安装程序角色 ARN。

您必须包含 **--hosted-cp** 参数，以使用 HCP 集群为 ROSA 创建正确的角色。此命令返回以下信息：

输出示例

```
? Role creation mode: auto
? Operator roles prefix: <pre-filled_prefix> (1)
? OIDC Configuration ID: 23soa2bgvpek9kmes9s7os0a39i13qm4 |
https://dvbwgdztaeq9o.cloudfront.net/23soa2bgvpek9kmes9s7os0a39i13qm4 (2)
? Create hosted control plane operator roles: Yes
W: More than one Installer role found
? Installer role ARN: arn:aws:iam::4540112244:role/<prefix>-HCP-ROSA-Installer-Role
? Permissions boundary ARN (optional):
I: Reusable OIDC Configuration detected. Validating trusted relationships to operator roles:
I: Creating roles using 'arn:aws:iam::4540112244:user/<userName>'
I: Created role '<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials'
I: Created role '<prefix>-openshift-cloud-network-config-controller-cloud-credenti' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-controller-cloud-credenti'
I: Created role '<prefix>-kube-system-kube-controller-manager' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager'
I: Created role '<prefix>-kube-system-capa-controller-manager' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager'
I: Created role '<prefix>-kube-system-control-plane-operator' with ARN
```

```
'arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator'
I: Created role '<prefix>-kube-system-kms-provider' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider'
I: Created role '<prefix>-openshift-image-registry-installer-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-credentials'
I: Created role '<prefix>-openshift-ingress-operator-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials'
I: To create a cluster with these roles, run the following command:
 rosa create cluster --sts --oidc-config-id 23soa2bgvpek9kmes9s7os0a39i13qm4 --operator-
roles-prefix <prefix> --hosted-cp
```

1. 此字段预先填充您在初始创建命令中设置的前缀。
2. 此字段要求您选择为使用 HCP 集群的 ROSA 创建的 OIDC 配置。

Operator 角色现已创建，并可用于使用 HCP 集群创建 ROSA。

验证

- 您可以列出与 ROSA 帐户关联的 Operator 角色。运行以下命令：

```
$ rosa list operator-roles
```

输**出示例**

```
I: Fetching operator roles
ROLE PREFIX  AMOUNT IN BUNDLE
<prefix>      8
? Would you like to detail a specific prefix Yes 1
? Operator Role Prefix: <prefix>
ROLE NAME                                          ROLE ARN
VERSION  MANAGED
<prefix>-kube-system-capa-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager
4.13     No
<prefix>-kube-system-control-plane-operator
arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator
4.13     No
<prefix>-kube-system-kms-provider
arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider                    4.13
No
<prefix>-kube-system-kube-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager
4.13     No
<prefix>-openshift-cloud-network-config-controller-cloud-credenti
arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-controller-cloud-
credenti  4.13     No
<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
4.13     No
<prefix>-openshift-image-registry-installer-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-credentials
4.13     No
```

```
<prefix>-openshift-ingress-operator-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials
4.13     No
```

1 命令运行后，它会显示与 AWS 帐户关联的所有前缀，并记下与这个前缀关联的角色数量。如果您需要查看所有这些角色及其详情，请在详细信息提示符处输入"是"，使这些角色按特定情况列出。

其他资源

- 如需有关 Operator 前缀的信息，请参阅关于自定义 Operator IAM 角色 前缀。

1.3. 使用 CLI 创建带有 HCP 集群的 ROSA

当使用 Red Hat OpenShift Service on AWS (ROSA) CLI (**rosa**)创建集群时，您可以选择默认选项来快速创建集群。

先决条件

- 您已使用 HCP 为 ROSA 完成 AWS 的先决条件。
- 您有可用的 AWS 服务配额。
- 您已在 AWS 控制台中启用了 ROSA 服务。
- 您已在安装主机上安装并配置了最新的 ROSA CLI (**rosa**)。运行 **rosa version** 以查看您当前安装的 ROSA CLI 版本。如果有更新的版本，CLI 会提供下载此升级的链接。
- 已使用 ROSA CLI 登录到您的红帽帐户。
- 您已创建了 OIDC 配置。
- 已确认 AWS 帐户中存在 AWS Elastic Load Balancing (ELB)服务角色。

流程

1. 使用以下命令之一使用 HCP 集群创建 ROSA：

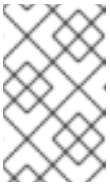
注意

当使用 HCP 集群创建 ROSA 时，默认的机器无类别间路由(CIDR)为 **10.0.0.0/16**。如果这与 VPC 子网的 CIDR 范围不匹配，请在以下命令中添加 **--machine-cidr <address_block >**。要了解更多有关 Red Hat OpenShift Service on AWS 的默认 CIDR 范围的信息，请参阅 CIDR 范围定义。

- 如果您没有设置环境变量，请运行以下命令：

```
$ rosa create cluster --cluster-name=<cluster_name> \ <.>
    --mode=auto --hosted-cp [--private] \ <.>
    --operator-roles-prefix <operator-role-prefix> \ <.>
    --oidc-config-id <id-of-oidc-configuration> \
    --subnet-ids=<public-subnet-id>,<private-subnet-id>
```

<.> 指定集群的名称。如果您的集群名称超过 15 个字符，它将包含自动生成的域前缀，作为 openshiftapps.com 上置备的集群的子域。要自定义子域，请使用 **--domain-prefix** 标志。域前缀不能超过 15 个字符，它必须是唯一的，且在集群创建后无法更改。<.> 可选： **--private** 参数用于创建带有 HCP 集群的私有 ROSA。如果使用此参数，请确保仅将专用子网 ID 用于 **--subnet-ids**。<.> 默认情况下，特定于集群的 Operator 角色名称使用集群名称和随机 4 位哈希值作为前缀。您可以选择指定一个自定义前缀来替换角色名称中的 < **cluster_name>-<hash** >。在创建特定于集群的 Operator IAM 角色时，会应用前缀。有关前缀的详情，*请参阅关于自定义 Operator IAM 角色前缀*。



注意

如果您在创建关联的集群范围的角色时指定了自定义 ARN 路径，则会自动检测到自定义路径。在稍后的步骤中创建时，自定义路径会应用到特定于集群的 Operator 角色。

- 如果设置环境变量，使用以下命令创建带有单个初始机器池的集群，使用公开或私有可用的 API，以及公开或私有可用的 Ingress：

```
$ rosa create cluster --private --cluster-name=<cluster_name> \
    --mode=auto --hosted-cp --operator-roles-prefix=$OPERATOR_ROLES_PREFIX \
    --oidc-config-id=$OIDC_ID --subnet-ids=$SUBNET_IDS
```

- 如果设置环境变量，请运行以下命令创建带有单个初始机器池、公开可用的 API 和公开可用的 Ingress 的集群：

```
$ rosa create cluster --cluster-name=<cluster_name> --mode=auto \
    --hosted-cp --operator-roles-prefix=$OPERATOR_ROLES_PREFIX \
    --oidc-config-id=$OIDC_ID --subnet-ids=$SUBNET_IDS
```

2. 运行以下命令检查集群的状态：

```
$ rosa describe cluster --cluster=<cluster_name>
```

在集群安装过程中，输出中会列出以下 **State** 字段更改：

- **待定（准备帐户）**
- **安装（正在进行中的DNS 设置）**
- **安装**
- **ready**

注意

如果安装失败，或者 **State** 字段在超过 10 分钟后没有变为 **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*。

3. 通过观察 Red Hat OpenShift Service on AWS 安装程序日志来跟踪集群创建的进度。要检查日志，请运行以下命令：

```
$ rosa logs install --cluster=<cluster_name> --watch \ <.>
```

-

<.> 可选：要在安装过程中监视新日志消息，请使用 **--watch** 参数。

1.4. 后续步骤

- 访问 ROSA 集群
- 添加通知联系人

1.5. 其他资源

- 有关使用手动模式部署 ROSA 集群的步骤，请参阅使用自定义创建集群。
- 有关使用 STS 部署 Red Hat OpenShift Service on AWS 所需的 AWS Identity Access Management (IAM)资源的更多信息，请参阅关于使用 STS 的集群的 IAM 资源。
- 有关 安全组 要求的信息，请参阅其他自定义安全组。
- 有关可选设置 Operator 角色名称前缀的详情，请参阅关于自定义 Operator IAM 角色前缀。
- 有关使用 STS 安装 ROSA 的先决条件的详情，请参考使用 STS 的 ROSA 的 AWS 先决条件。
- 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。
- 有关在 AWS IAM 中使用 OpenID Connect (OIDC)身份提供程序的更多信息，请参阅 AWS 文档中的 创建 OpenID Connect (OIDC)身份供应商。
- 有关 ROSA 集群安装故障排除的更多信息，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 获取对 Red Hat OpenShift Service on AWS 的支持。

第 2 章 使用 TERRAFORM 创建 ROSA 集群

2.1. 使用 TERRAFORM 创建默认 ROSA 集群

使用使用默认集群选项配置的 Terraform 集群模板，快速创建 Red Hat OpenShift Service on AWS (ROSA)集群。

以下描述的集群创建过程使用 Terraform 配置来准备带有以下资源的带有 HCP 集群的 ROSA：

- 带有受管 **oidc-config** 配置的 OIDC 供应商
- 带有关联的 AWS Managed ROSA 策略的先决条件 IAM Operator 角色
- 带有关联的 AWS Managed ROSA 策略的 IAM 帐户角色
- 创建使用 STS 集群的 ROSA 所需的所有其他 AWS 资源

2.1.1. Terraform 概述

Terraform 是一个基础架构即代码工具，提供一次配置资源并根据需要复制这些资源的方法。Terraform 使用声明性语言完成创建任务。您可以声明基础架构资源的最终状态，Terraform 会根据您的规格创建这些资源。

先决条件

要在 Terraform 配置中使用 Red Hat Cloud Services 供应商，您必须满足以下条件：

- 您已在 AWS (ROSA)命令行界面(CLI)工具上安装了 Red Hat OpenShift Service。
- 您有离线的 Red Hat OpenShift Cluster Manager 令牌 。
- 已安装 Terraform 版本 1.4.6 或更新版本。
- 您已创建了 AWS 帐户范围的 IAM 角色。
  特定的帐户范围的 IAM 角色和策略提供 ROSA 支持、安装、control plane 和计算功能所需的 STS 权限。这包括集群范围的 Operator 策略。如需有关 AWS 帐户角色的更多信息，请参阅附加资源。
- 您有一个 AWS 帐户 和相关凭证，供您创建资源。为 AWS 供应商配置了凭证。请参阅 AWS Terraform 供应商文档中的 身份验证和 配置部分。
- 您至少在 AWS IAM 角色策略中具有以下权限，其运行 Terraform。在 AWS 控制台中检查这些权限。

例 2.1. Terraform 的最低 AWS 权限

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:CreatePolicyVersion",
```

```
        "iam:UpdateAssumeRolePolicy",
        "secretsmanager:DescribeSecret",
        "iam:ListRoleTags",
        "secretsmanager:PutSecretValue",
        "secretsmanager:CreateSecret",
        "iam:TagRole",
        "secretsmanager:DeleteSecret",
        "iam:UpdateOpenIDConnectProviderThumbprint",
        "iam:DeletePolicy",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "secretsmanager:GetSecretValue",
        "iam:DetachRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicyTags",
        "iam:ListRolePolicies",
        "iam:DeleteOpenIDConnectProvider",
        "iam:DeleteInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:DeleteRole",
        "iam:TagPolicy",
        "iam:CreateOpenIDConnectProvider",
        "iam:CreatePolicy",
        "secretsmanager:GetResourcePolicy",
        "iam:ListPolicyVersions",
        "iam:UpdateRole",
        "iam:GetOpenIDConnectProvider",
        "iam:TagOpenIDConnectProvider",
        "secretsmanager:TagResource",
        "sts:AssumeRoleWithWebIdentity",
        "iam:ListRoles"
      ],
      "Resource": [
        "arn:aws:secretsmanager:*:<ACCOUNT_ID>:secret:*",
        "arn:aws:iam::<ACCOUNT_ID>:instance-profile/*",
        "arn:aws:iam::<ACCOUNT_ID>:role/*",
        "arn:aws:iam::<ACCOUNT_ID>:oidc-provider/*",
        "arn:aws:iam::<ACCOUNT_ID>:policy/*"
      ]
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:*"
        ],
      "Resource": "*"
    }
  ]
}
```

使用 Terraform 时的注意事项

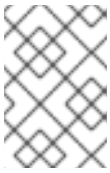
通常，使用 Terraform 管理云资源应按照预期完成任何更改，以便使用 Terraform 方法进行任何更改。在使用 Terraform 之外的工具（如 AWS 控制台或红帽控制台）时，请小心修改 Terraform 创建的云资源。使用 Terraform 以外的工具来管理已经由 Terraform 管理的云资源，从您声明的 Terraform 配置中引入配置偏移。

例如，如果您使用 Red Hat Hybrid Cloud Console 升级 Terraform 创建的集群，则需要在应用任何受影响的配置更改前协调 Terraform 状态。如需更多信息，请参阅 HashiCorp Developer 文档中的管理 Terraform 状态的资源。

2.1.2. 默认集群规格概述

表 2.1. 带有 HCP 集群规格的默认 ROSA

组件	默认规格
帐户和角色	• 默认 IAM 角色前缀： **rosa-<6-digit-alphanumeric-string>** • 没有创建集群管理员角色
集群设置	• 默认集群版本： **4.14** • Cluster name: **rosa-<6-digit-alphanumeric-string>** • 使用 Red Hat OpenShift Cluster Manager 混合云控制台安装的默认 AWS 区域：us-east-2 (US East, Ohio) • 可用性：数据平面的多个区域 • 启用默认的 EC2 IMDS 端点(v1 和 v2) • 监控用户定义的项目：启用
Encryption	• 云存储会加密 • 没有启用额外的 etcd 加密 • 默认 AWS 密钥管理服务(KMS)密钥用作持久数据的加密密钥
Compute 节点机器池	• Compute 节点实例类型： m5.xlarge (4 vCPU 16, GiB RAM) • Compute 节点数： 3 个 • 自动扩展：未启用 • 没有额外的节点标签

组件	默认规格
网络配置	• 集群隐私：公共或私有 • 您可以选择在 Terraform 集群创建过程中创建新 VPC。 • 您必须已经配置了自己的虚拟私有云(VPC) • 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: 10.128.0.0/14 • 主机前缀：/23  **注意** 在使用带有 HCP 的 ROSA 时，静态 IP 地址 **172.20.0.1** 会为内部 Kubernetes API 地址保留。机器、pod 和服务 CIDR 范围不得与此 IP 地址冲突。
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： **rosa-<6-digit-alphanumeric-string>**
集群更新策略	• 独立更新 • 节点排空 1 小时宽限期

2.1.3. 使用 Terraform 创建默认 ROSA 集群

以下概述的集群创建过程演示了如何使用 Terraform 创建您的帐户范围的 IAM 角色和带有受管 OIDC 配置的 ROSA 集群。

2.1.3.1. 为 Terraform 准备您的环境

在使用 Terraform 在 AWS 集群上创建 Red Hat OpenShift Service 前，您需要导出 离线 Red Hat OpenShift Cluster Manager 令牌。

流程

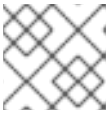
1. **可选** ：因为在此过程中，Terraform 文件会在当前目录中创建，因此您可以创建一个新目录来存储这些文件并运行以下命令来进入其中：

```
$ mkdir terraform-cluster && cd terraform-cluster
```

2. 使用 离线 Red Hat OpenShift Cluster Manager 令牌 向您的帐户授予权限。

3. 复制离线令牌，并通过运行以下命令来将令牌设置为环境变量：

```
$ export RHCS_TOKEN=<your_offline_token>
```



注意

此环境变量会在每个会话的末尾重置，如重启计算机或关闭终端。

验证

- 导出令牌后，运行以下命令来验证值：

```
$ echo $RHCS_TOKEN
```

2.1.3.2. 在本地创建 Terraform 文件

设置 离线 Red Hat OpenShift Cluster Manager 令牌 后，您需要在本地创建 Terraform 文件以构建集群。您可以使用以下代码模板创建这些文件。

流程

1. 运行以下命令来创建 **main.tf** 文件：

```
$ cat<<-EOF>main.tf
#
# Copyright (c) 2023 Red Hat, Inc.
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#   http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#
terraform {
  required_providers {
    aws = {
      source  = "hashicorp/aws"
      version = ">= 4.20.0"
    }
```

```
    rhcs = {
      version = ">= 1.6.2"
      source  = "terraform-redhat/rhcs"
    }
  }
}

# Export token using the RHCS_TOKEN environment variable
provider "rhcs" {}

provider "aws" {
  region = var.aws_region
  ignore_tags {
    key_prefixes = ["kubernetes.io/"]
  }
  default_tags {
    tags = var.default_aws_tags
  }
}

data "aws_availability_zones" "available" {}

locals {
  # Extract availability zone names for the specified region, limit it to 3 if multi az or 1 if single
  region_azs = var.multi_az ? slice([for zone in data.aws_availability_zones.available.names :
format("%s", zone)], 0, 3) : slice([for zone in data.aws_availability_zones.available.names :
format("%s", zone)], 0, 1)
}

resource "random_string" "random_name" {
  length  = 6
  special = false
  upper   = false
}

locals {
  worker_node_replicas = var.multi_az ? 3 : 2
  # If cluster_name is not null, use that, otherwise generate a random cluster name
  cluster_name = coalesce(var.cluster_name, "rosa-\${random_string.random_name.result}")
}

# The network validator requires an additional 60 seconds to validate Terraform clusters.
resource "time_sleep" "wait_60_seconds" {
  count = var.create_vpc ? 1 : 0
  depends_on = [module.vpc]
  create_duration = "60s"
}

module "rosa-hcp" {
  source               = "terraform-redhat/rosa-hcp/rhcs"
  version              = "1.6.2"
  cluster_name         = local.cluster_name
  openshift_version    = var.openshift_version
  account_role_prefix  = local.cluster_name
  operator_role_prefix = local.cluster_name
  replicas             = local.worker_node_replicas
```

```
  aws_availability_zones = local.region_azs
  create_oidc            = true
  private                = var.private_cluster
  aws_subnet_ids         = var.create_vpc ? var.private_cluster ?
module.vpc[0].private_subnets : concat(module.vpc[0].public_subnets,
module.vpc[0].private_subnets) : var.aws_subnet_ids
  create_account_roles   = true
  create_operator_roles  = true

  depends_on = [time_sleep.wait_60_seconds]
}
EOF
```

2. 运行以下命令来创建 **variables.tf** 文件：

注意

在运行该命令 *以构建* 集群前复制并编辑此文件。

```
$ cat<<-EOF>variables.tf
#
# Copyright (c) 2023 Red Hat, Inc.
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#   http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#
variable "openshift_version" {
  type        = string
  default     = "4.14.20"
  description = "Desired version of OpenShift for the cluster, for example '4.14.20'. If version is
greater than the currently running version, an upgrade will be scheduled."
}

variable "create_vpc" {
  type        = bool
  description = "If you would like to create a new VPC, set this value to 'true'. If you do not
want to create a new VPC, set this value to 'false'."
}

# ROSA Cluster info
variable "cluster_name" {
  default     = null
  type        = string
  description = "The name of the ROSA cluster to create"
}
```

```
variable "additional_tags" {
  default = {
    Terraform   = "true"
    Environment = "dev"
  }
  description = "Additional AWS resource tags"
  type        = map(string)
}

variable "multi_az" {
  type        = bool
  description = "Multi AZ Cluster for High Availability"
  default     = true
}

variable "worker_node_replicas" {
  default     = 3
  description = "Number of worker nodes to provision. Single zone clusters need at least 2
nodes, multizone clusters need at least 3 nodes"
  type        = number
}

variable "aws_subnet_ids" {
  type        = list(any)
  description = "A list of either the public or public + private subnet IDs to use for the cluster
blocks to use for the cluster"
  default     = ["subnet-01234567890abcdef", "subnet-01234567890abcdef", "subnet-
01234567890abcdef"]
}

variable "private_cluster" {
  type        = bool
  description = "If you want to create a private cluster, set this value to 'true'. If you want a
publicly available cluster, set this value to 'false'."
}

#VPC Info
variable "vpc_name" {
  type        = string
  description = "VPC Name"
  default     = "tf-qs-vpc"
}

variable "vpc_cidr_block" {
  type        = string
  description = "value of the CIDR block to use for the VPC"
  default     = "10.0.0.0/16"
}

variable "private_subnet_cidrs" {
  type        = list(any)
  description = "The CIDR blocks to use for the private subnets"
  default     = ["10.0.1.0/24", "10.0.2.0/24", "10.0.3.0/24"]
}

variable "public_subnet_cidrs" {
```

```
  type        = list(any)
  description = "The CIDR blocks to use for the public subnets"
  default     = ["10.0.101.0/24", "10.0.102.0/24", "10.0.103.0/24"]
}

variable "single_nat_gateway" {
  type        = bool
  description = "Single NAT or per NAT for subnet"
  default     = false
}

#AWS Info
variable "aws_region" {
  type    = string
  default = "us-east-2"
}

variable "default_aws_tags" {
  type        = map(string)
  description = "Default tags for AWS"
  default     = {}
}
EOF
```

3. 运行以下命令来创建 **vpc.tf** 文件：

```
$ cat<<-EOF>vpc.tf
#
# Copyright (c) 2023 Red Hat, Inc.
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#   http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#
module "vpc" {
  source  = "terraform-aws-modules/vpc/aws"
  version = "5.1.2"

  count = var.create_vpc ? 1 : 0
  name  = var.vpc_name
  cidr  = var.vpc_cidr_block

  azs             = local.region_azs
  private_subnets = var.multi_az ? var.private_subnet_cidrs : [var.private_subnet_cidrs[0]]
  public_subnets  = var.multi_az ? var.public_subnet_cidrs : [var.public_subnet_cidrs[0]]

  enable_nat_gateway   = true
  single_nat_gateway   = var.single_nat_gateway
```

```
  enable_dns_hostnames = true
  enable_dns_support   = true

  tags = var.additional_tags
}
EOF
```

您已准备好启动 Terraform。

2.1.3.3. 使用 Terraform 创建 ROSA 集群

创建 Terraform 文件后，您必须启动 Terraform 以提供所有需要的依赖软件包。然后应用 Terraform 计划。

重要

不要修改 Terraform 状态文件。如需更多信息，请参阅使用 Terraform 时的注意事项

流程

1. 将 Terraform 设置为根据您的 Terraform 文件创建资源，运行以下命令：

```
$ terraform init
```

2. **可选** ：运行以下命令来验证您复制的 Terraform 是否正确：

```
$ terraform validate
```

输出示例

```
Success! The configuration is valid.
```

3. 运行以下命令，使用 Terraform 创建集群：

```
$ terraform apply
```

Terraform 界面需要两个问题来创建集群，并熟悉以下内容：

输出示例

```
var.create_vpc
  If you would like to create a new VPC, set this value to 'true'. If you do not want to create a
new VPC, set this value to 'false'.

  Enter a value:

var.private_cluster
  If you want to create a private cluster, set this value to 'true'. If you want a publicly available
cluster, set this value to 'false'.

  Enter a value:
```

4. 当 Terraform 界面列出要创建或修改的资源并提示确认时，输入 **yes** 才能继续或取消：

输出示例

```
Plan: 63 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.
```

如果您输入 yes，您的 Terraform 计划将启动，创建 AWS 帐户角色、Operator 角色和 ROSA Classic 集群。

验证

1. 运行以下命令验证集群是否已创建：

```
$ rosa list clusters
```

显示集群的 ID、名称和状态的输出示例：

```
ID                            NAME         STATE  TOPOLOGY
27c3snjsupa9obua74ba8se5kcj11269  rosa-tf-demo  ready  Classic (STS)
```

2. 运行以下命令验证您的帐户角色是否已创建：

```
$ rosa list account-roles
```

输出示例

```
I: Fetching account roles
```

```
ROLE NAME                          ROLE TYPE      ROLE ARN
OPENSHIFT VERSION  AWS Managed
ROSA-demo-Installer-Role           Installer      arn:aws:iam::<ID>:role/ROSA-demo-
Installer-Role              4.14          No
ROSA-demo-Support-Role             Support        arn:aws:iam::<ID>:role/ROSA-
demo-Support-Role           4.14          No
ROSA-demo-Worker-Role              Worker         arn:aws:iam::<ID>:role/ROSA-
demo-Worker-Role            4.14          No
```

3. 运行以下命令验证您的 Operator 角色是否已创建：

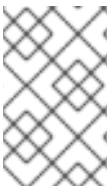
```
$ rosa list operator-roles
```

显示 Terraform 创建的 Operator 角色的输出示例：

```
I: Fetching operator roles
ROLE PREFIX    AMOUNT IN BUNDLE
rosa-demo      8
```

2.1.3.4. 使用 Terraform 删除 ROSA 集群

使用 terraform destroy 命令删除使用 terraform apply 命令创建的所有资源。



注意

在销毁资源前不要修改 Terraform .tf 文件。这些变量与要删除的资源匹配。

流程

1. 在运行 terraform apply 命令来创建集群的目录中，运行以下命令删除集群：

```
$ terraform destroy
```

Terraform 接口提示您输入两个变量。它们应与创建集群时提供的答案匹配：

```
var.create_vpc
  If you would like to create a new VPC, set this value to 'true.' If you do not want to
create a new VPC, set this value to 'false.'

  Enter a value:

var.private_cluster
  If you want to create a private cluster, set this value to 'true.' If you want a publicly
available cluster, set this value to 'false.'

  Enter a value:
```

2. 输入 yes 以启动角色和集群删除：

输出示例

```
Plan: 0 to add, 0 to change, 63 to destroy.

Do you really want to destroy all resources?
  Terraform will destroy all your managed infrastructure, as shown above.
  There is no undo. Only 'yes' will be accepted to confirm.

  Enter a value: yes
```

验证

1. 运行以下命令验证集群是否已销毁：

```
$ rosa list clusters
```

没有显示集群的输出示例

```
I: No clusters available
```

2. 运行以下命令验证帐户角色是否已销毁：

```
$ rosa list account-roles
```

显示没有 Terraform 创建的帐户角色的示例：

```
I: Fetching account roles
I: No account roles available
```

3. 运行以下命令验证 Operator 角色是否已销毁：

```
$ rosa list operator-roles
```

输出显示没有 Terraform 创建的 Operator 角色示例：

```
I: Fetching operator roles
I: No operator roles available
```

第 3 章 使用自定义 AWS KMS 加密密钥创建带有 HCP 集群的 ROSA

使用自定义 AWS 密钥管理服务(KMS)密钥，使用托管的 control plane (HCP)集群创建一个 Red Hat OpenShift Service on AWS (ROSA)集群。

3.1. 带有 HCP 先决条件的 ROSA

要使用 HCP 集群创建 ROSA，您必须有以下项目：

- 配置的虚拟私有云(VPC)
- 帐户范围内的角色
- OIDC 配置
- Operator 角色

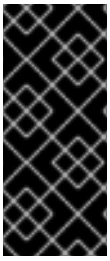
3.1.1. 使用 HCP 集群为您的 ROSA 创建虚拟私有云

您必须有一个 Virtual Private Cloud (VPC)才能使用 HCP 集群创建 ROSA。您可以使用以下方法创建 VPC：

- 使用 Terraform 模板创建 VPC
- 在 AWS 控制台中手动创建 VPC 资源

注意

Terraform 指令用于测试和演示目的。您自己的安装需要对 VPC 进行一些修改，以便您自己的使用。您还应确保在使用这个 Terraform 脚本时，它位于您要安装集群的同一区域。在这些示例中，使用 us-east-2。



重要

目前，使用 HCP 的 ROSA 不支持在 多个 AWS 帐户间共享 VPC。不要将带有 HCP 集群的 ROSA 安装到与另一个 AWS 帐户共享的子网。如需更多信息，请参阅 "支持单个 VPC 中的多个 ROSA 集群？"。

使用 Terraform 创建虚拟私有云

Terraform 是一个工具，允许您使用已建立的模板创建各种资源。以下过程使用默认选项来创建带有 HCP 集群的 ROSA。有关使用 Terraform 的更多信息，请参阅其他资源。

先决条件

- 您已在机器上安装 Terraform 版本 1.4.0 或更新版本。
- 您已在机器上安装了 Git。

流程

1. 运行以下命令，打开 shell 提示符并克隆 Terraform VPC 存储库：

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

2. 运行以下命令进入创建的目录：

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

3. 运行以下命令来启动 Terraform 文件：

```
$ terraform init
```

此进程完成后会出现确认初始化的消息。

4. 要基于现有的 Terraform 模板构建 VPC Terraform 计划，请运行 plan 命令。您必须包含 AWS 区域。您可以选择指定集群名称。在 terraform plan 完成后，一个 rosa.tfplan 文件会被添加到 hypershift-tf 目录。有关更详细的选项，请参阅 Terraform VPC 存储库的 README 文件。

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

5. 运行以下命令应用此计划文件来构建 VPC：

```
$ terraform apply rosa.tfplan
```

a. 可选：您可以运行以下命令来捕获 Terraform-provisioned private、public 和 machinepool 子网 ID 的值作为环境变量，以便在使用 HCP 集群创建 ROSA 时使用：

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

b. 使用以下命令验证变量是否已正确设置：

```
$ echo $SUBNET_IDS
```

输出示例

```
$ subnet-0a6a57e0f784171aa,subnet-078e84e5b10ecf5b0
```

其他资源

- 有关自定义 VPC 时可用选项的详细列表，请参阅 Terraform VPC 存储库。

手动创建虚拟私有云

如果您选择手动创建 Virtual Private Cloud (VPC)而不是使用 Terraform，请访问 AWS 控制台中的 VPC 页面。您的 VPC 必须满足下表中显示的要求。

表 3.1. VPC 的要求

要求	详情
VPC 名称	创建集群时需要具有特定的 VPC 名称和 ID。
CIDR 范围	您的 VPC CIDR 范围应该与您的机器 CIDR 匹配。

要求	详情
可用区	单个区需要一个可用区，对于多区的可用区需要三个可用区。
公共子网	对于公共集群，您必须有一个带有 NAT 网关的公共子网。私有集群不需要公共子网。
DNS 主机名和解析	您必须确保启用 DNS 主机名和解析。

其他资源

- Amazon VPC 入门
- HashiCorp Terraform 文档

3.1.2. 创建集群范围的 STS 角色和策略

在使用 Red Hat OpenShift Service on AWS (ROSA) CLI (rosa)创建带有托管 control plane (HCP) 集群的 Red Hat OpenShift Service on AWS (ROSA)前，请创建所需的帐户范围角色和策略，包括 Operator 策略。

注意

使用 HCP 集群的 ROSA 需要附加 AWS 受管策略的帐户和 Operator 角色。不支持客户管理的策略。有关使用 HCP 集群的 ROSA 的 AWS 管理策略的更多信息，请参阅 ROSA 帐户角色的 AWS 管理策略。

先决条件

- 您已使用 HCP 为 ROSA 完成 AWS 的先决条件。
- 您有可用的 AWS 服务配额。
- 您已在 AWS 控制台中启用了 ROSA 服务。

- 您已在安装主机上安装并配置了最新的 ROSA CLI (rosa)。
- 已使用 ROSA CLI 登录到您的红帽帐户。

流程

1. 如果 AWS 帐户中不存在它们，请创建所需的账户范围的 STS 角色，并通过运行以下命令附加策略：

```
$ rosa create account-roles --hosted-cp
```

2. 可选：运行以下命令将前缀设置为环境变量：

```
$ export ACCOUNT_ROLES_PREFIX=<account_role_prefix>
```

- 运行以下命令，查看变量的值：

```
$ echo $ACCOUNT_ROLES_PREFIX
```

输出示例

```
ManagedOpenShift
```

如需有关 ROSA 的 AWS 管理 IAM 策略的更多信息，请参阅 ROSA 的 AWS 管理的 IAM 策略。

3.1.3. 创建 OpenID Connect 配置

当将 ROSA 与 HCP 集群搭配使用时，您必须先创建 OpenID Connect (OIDC)配置。此配置已注册到 OpenShift Cluster Manager。

先决条件

- 您已使用 HCP 为 ROSA 完成 AWS 的先决条件。
- 您已完成了 Red Hat OpenShift Service on AWS 的 AWS 的先决条件。
- 您已在安装主机上安装并配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI rosa。

流程

1. 要创建 OIDC 配置和 AWS 资源，请运行以下命令：

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

此命令返回以下信息：

输出示例

```
? Would you like to create a Managed (Red Hat hosted) OIDC Configuration Yes
I: Setting up managed OIDC configuration
I: To create Operator Roles for this OIDC Configuration, run the following command
and remember to replace <user-defined> with a prefix of your choice:
 rosa create operator-roles --prefix <user-defined> --oidc-config-id 13cdr6b
If you are going to create a Hosted Control Plane cluster please include '--hosted-cp'
I: Creating OIDC provider using 'arn:aws:iam::4540112244:user/userName'
? Create the OIDC provider? Yes
I: Created OIDC provider with ARN 'arn:aws:iam::4540112244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/13cdr6b'
```

在创建集群时，您必须提供 OIDC 配置 ID。CLI 输出为 --mode auto 提供这个值，否则您必须根据 --mode manual 的 aws CLI 输出来确定这些值。

2. 可选： 您可以将 OIDC 配置 ID 保存为变量，以便稍后使用。运行以下命令来保存变量：

```
$ export OIDC_ID=<oidc_config_id> 1
```

1

在上面的示例输出中，OIDC 配置 ID 是 13cdr6b。

- 运行以下命令，查看变量的值：

```
$ echo $OIDC_ID
```

输出示例

```
13cdr6b
```

验证

- 您可以列出与用户机构关联的集群可用的 OIDC 配置。运行以下命令：

```
$ rosa list oidc-config
```

输出示例

```
ID                               MANAGED  ISSUER URL
SECRET ARN
2330dbs0n8m3chkkr25gkkcd8pnj3lk2  true
https://dvbwgdztaeq9o.cloudfront.net/2330dbs0n8m3chkkr25gkkcd8pnj3lk2
233hvnrjoqu14jltk6lhbhf2tj11f8un  false    https://oidc-r7u1.s3.us-east-
1.amazonaws.com                  aws:secretsmanager:us-east-
1:242819244:secret:rosa-private-key-oidc-r7u1-tM3MDN
```

3.1.4. 创建 Operator 角色和策略

当将 ROSA 与 HCP 集群搭配使用时，您必须创建带有托管 control plane (HCP)部署的 Red Hat OpenShift Service on AWS (ROSA)所需的 Operator IAM 角色。集群 Operator 使用 Operator 角色获取执行集群操作所需的临时权限，如管理后端存储、云供应商凭证和对集群的外部访问权限。

先决条件

- 您已使用 HCP 为 ROSA 完成 AWS 的先决条件。
- 您已在安装主机上安装并配置了最新的 Red Hat OpenShift Service on AWS ROSA CLI (rosa)。
- 您创建了集群范围的 AWS 角色。

流程

1. 使用以下命令将前缀名称设置为环境变量：

```
$ export OPERATOR_ROLES_PREFIX=<prefix_name>
```

2. 要创建 Operator 角色，请运行以下命令：

```
$ rosa create operator-roles --hosted-cp --prefix=$OPERATOR_ROLES_PREFIX --oidc-config-id=$OIDC_ID --installer-role-arn arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role
```

以下分类提供了 Operator 角色创建的选项。

```
$ rosa create operator-roles --hosted-cp
 --prefix=$OPERATOR_ROLES_PREFIX 1
 --oidc-config-id=$OIDC_ID 2
 --installer-role-arn
arn:aws:iam::${AWS_ACCOUNT_ID}:role/${ACCOUNT_ROLES_PREFIX}-HCP-ROSA-Installer-Role 3
```

1. 在创建这些 Operator 角色时，您必须提供一个前缀。如果不这样做会产生错误。如需有关 Operator 前缀的信息，请参阅本节的附加资源。
2. 这个值是您为使用 HCP 集群的 ROSA 创建的 OIDC 配置 ID。
3.

您必须包含 --hosted-cp 参数，以使用 HCP 集群为 ROSA 创建正确的角色。此命令返回以下信息：

输出示例

```
? Role creation mode: auto
? Operator roles prefix: <pre-filled_prefix> 1
? OIDC Configuration ID: 23soa2bgvpek9kmes9s7os0a39i13qm4 |
https://dvbwgdztaeq9o.cloudfront.net/23soa2bgvpek9kmes9s7os0a39i13qm4 2
? Create hosted control plane operator roles: Yes
W: More than one Installer role found
? Installer role ARN: arn:aws:iam::4540112244:role/<prefix>-HCP-ROSA-Installer-Role
? Permissions boundary ARN (optional):
I: Reusable OIDC Configuration detected. Validating trusted relationships to operator
roles:
I: Creating roles using 'arn:aws:iam::4540112244:user/<userName>'
I: Created role '<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-
credentials'
I: Created role '<prefix>-openshift-cloud-network-config-controller-cloud-credenti' with
ARN 'arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-
controller-cloud-credenti'
I: Created role '<prefix>-kube-system-kube-controller-manager' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager'
I: Created role '<prefix>-kube-system-capa-controller-manager' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager'
I: Created role '<prefix>-kube-system-control-plane-operator' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator'
I: Created role '<prefix>-kube-system-kms-provider' with ARN
'arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider'
I: Created role '<prefix>-openshift-image-registry-installer-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-
credentials'
I: Created role '<prefix>-openshift-ingress-operator-cloud-credentials' with ARN
'arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials'
I: To create a cluster with these roles, run the following command:
 rosa create cluster --sts --oidc-config-id 23soa2bgvpek9kmes9s7os0a39i13qm4 --
operator-roles-prefix <prefix> --hosted-cp
```

1

此字段预先填充您在初始创建命令中设置的前缀。

2

此字段要求您选择为使用 HCP 集群的 ROSA 创建的 OIDC 配置。

Operator 角色现已创建，并可用于使用 HCP 集群创建 ROSA。

验证

- 您可以列出与 ROSA 帐户关联的 Operator 角色。运行以下命令：

```
$ rosa list operator-roles
```

输出示例

```
I: Fetching operator roles
ROLE PREFIX  AMOUNT IN BUNDLE
<prefix>     8
? Would you like to detail a specific prefix Yes 1
? Operator Role Prefix: <prefix>
ROLE NAME                                          ROLE ARN
VERSION  MANAGED
<prefix>-kube-system-capa-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-capa-controller-manager
4.13     No
<prefix>-kube-system-control-plane-operator
arn:aws:iam::4540112244:role/<prefix>-kube-system-control-plane-operator
4.13     No
<prefix>-kube-system-kms-provider
arn:aws:iam::4540112244:role/<prefix>-kube-system-kms-provider
4.13     No
<prefix>-kube-system-kube-controller-manager
arn:aws:iam::4540112244:role/<prefix>-kube-system-kube-controller-manager
4.13     No
<prefix>-openshift-cloud-network-config-controller-cloud-credenti
arn:aws:iam::4540112244:role/<prefix>-openshift-cloud-network-config-controller-
cloud-credenti  4.13     No
<prefix>-openshift-cluster-csi-drivers-ebs-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-cluster-csi-drivers-ebs-cloud-
credentials       4.13     No
<prefix>-openshift-image-registry-installer-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-image-registry-installer-cloud-
credentials      4.13     No
<prefix>-openshift-ingress-operator-cloud-credentials
arn:aws:iam::4540112244:role/<prefix>-openshift-ingress-operator-cloud-credentials
4.13     No
```

1

命令运行后，它会显示与 AWS 帐户关联的所有前缀，并记下与这个前缀关联的角色数量。如果您需要查看所有这些角色及其详情，请在详细信息提示符处输入"是"，使这些角色按特定情况列出。

3.1.5. 使用自定义 AWS KMS 密钥创建 ROSA 集群

您可以使用客户提供的 KMS 密钥来加密节点根卷、etcd 数据库或两者，创建 Red Hat OpenShift Service on AWS (ROSA)集群。可以为每个选项提供不同的 KMS 密钥 ARN。

注意

使用 HCP 的 ROSA 不会自动配置 默认存储类，以使用客户提供的 KMS 密钥加密持久性卷。这是安装后可以在集群中配置的对象。

流程

1. 运行以下命令，创建自定义 AWS 客户管理的 KMS 密钥：

```
$ KMS_ARN=$(aws kms create-key --region $AWS_REGION --description 'Custom ROSA Encryption Key' --tags TagKey=red-hat,TagValue=true --query KeyMetadata.Arn --output text)
```

此命令保存此自定义密钥的 Amazon 资源名称(ARN)输出以获取进一步步骤。

注意

客户必须提供客户 KMS 密钥所需的 --tags TagKey=red-hat,TagValue=true 参数。

2. 运行以下命令验证 KMS 密钥是否已创建：

```
$ echo $KMS_ARN
```

3. 将 AWS 帐户 ID 设置为环境变量。

```
$ AWS_ACCOUNT_ID=<aws_account_id>
```

4. 将您在上一步中创建的集群范围的安装程序角色和 operator 角色的 ARN 添加到 文件中的 Statement.Principal.AWS 部分。在以下示例中，添加了默认 ManagedOpenShift-HCP-ROSA-Installer-Role 角色的 ARN：

```
{
 "Version": "2012-10-17",
 "Id": "key-rosa-policy-1",
 "Statement": [
 {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
       {
            "Sid": "Installer Permissions",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:role/ManagedOpenShift-HCP-
ROSA-Installer-Role"
            },
            "Action": [
               "kms:CreateGrant",
               "kms:DescribeKey",
               "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ROSA KubeControllerManager Permissions",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:role/<operator_role_prefix>-
kube-system-kube-controller-manager"

            },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "ROSA KMS Provider Permissions",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:role/<operator_role_prefix>-
kube-system-kms-provider"
```

```
            },
            "Action": [
               "kms:Encrypt",
               "kms:Decrypt",
               "kms:DescribeKey"
            ],
            "Resource": "*"
         },
         {
            "Sid": "ROSA NodeManager Permissions",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::${AWS_ACCOUNT_ID}:role/<operator_role_prefix>-
kube-system-capa-controller-manager"
            },
            "Action": [
               "kms:DescribeKey",
               "kms:GenerateDataKeyWithoutPlaintext",
               "kms:CreateGrant"
            ],
            "Resource": "*"
         }
      ]
   }
```

5. 运行以下命令确认创建的策略文件详情：

```
$ cat rosa-key-policy.json
```

6. 运行以下命令，将新生成的密钥策略应用到自定义 KMS 密钥：

```
$ aws kms put-key-policy --key-id $KMS_ARN \
--policy file://rosa-key-policy.json \
--policy-name default
```

7. 运行以下命令来创建集群：

注意

如果您的集群名称超过 15 个字符，它将包含自动生成的域前缀作为您 provisioned 集群 的子域。

要自定义子域，请使用 --domain-prefix 标志。域前缀不能超过 15 个字符，它必须是唯一的，且在集群创建后无法更改。

```
$ rosa create cluster --cluster-name <cluster_name> \
--subnet-ids <private_subnet_id>,<public_subnet_id> \
--sts \
--mode auto \
--machine-cidr 10.0.0.0/16 \
--compute-machine-type m5.xlarge \
--hosted-cp \
--region <aws_region> \
--oidc-config-id $OIDC_ID \
--kms-key-arn $KMS_ARN \ 1
--etcd-encryption-kms-arn $KMS_ARN \ 2
--operator-roles-prefix $OPERATOR_ROLES_PREFIX
```

1 这个 KMS 密钥 ARN 用于加密所有 worker 节点根卷。如果只需要 etcd 数据库加密，则不需要它。

2 这个 KMS 密钥 ARN 用于加密 etcd 数据库。默认情况下，etcd 数据库总是使用 AES 密码块加密，但可以使用 KMS 密钥加密。如果只需要节点根卷加密，则不需要它。

验证

您可以使用 OpenShift Cluster Manager 验证 KMS 密钥是否正常工作。

1. 导航到 OpenShift Cluster Manager 并选择 Instances。
2. 选择您的实例。
3. 点 Storage 选项卡。
4. 复制 KMS 密钥 ID。
5. 搜索并选择 Key Management Service。
6. 在 Filter 字段中输入您复制的 *KMS 密钥 ID*。

3.2. 后续步骤

- 访问 ROSA 集群

3.3. 其他资源

- 有关使用 CLI 创建集群的详情，请参考使用 CLI 使用 HCP 集群创建 ROSA。
- 有关使用手动模式部署 ROSA 集群的步骤，请参阅使用自定义创建集群。
- 有关使用 STS 部署 Red Hat OpenShift Service on AWS 所需的 AWS Identity Access Management (IAM)资源的更多信息，请参阅关于使用 STS 的集群的 IAM 资源。
- 有关可选设置 Operator 角色名称前缀的详情，请参阅关于自定义 Operator IAM 角色前缀。
- 有关使用 STS 安装 ROSA 的先决条件的详情，请参考使用 STS 的 ROSA 的 AWS 先决条件。
- 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。
- 有关在 AWS IAM 中使用 OpenID Connect (OIDC)身份提供程序的更多信息，请参阅创建 OpenID Connect (OIDC)身份提供程序。
- 有关 ROSA 集群安装故障排除的更多信息，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 获取对 Red Hat OpenShift Service on AWS 的支持。

第 4 章 使用 HCP 在 ROSA 上创建私有集群

本文档论述了如何使用托管的 control plane (HCP)私有集群在 AWS (ROSA)上创建 Red Hat OpenShift Service。

4.1. 创建 AWS 私有集群

您可以使用 ROSA 命令行界面(CLI)在带有 HCP 的 ROSA 上创建带有多个可用区(Multi-AZ)的私有集群。

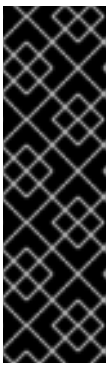
先决条件

- 您有可用的 AWS 服务配额。
- 您已在 AWS 控制台中启用了 ROSA 服务。
- 您已在安装主机上安装并配置了 ROSA CLI 的最新版本。

流程

使用托管 control plane 创建集群可能需要大约 10 分钟。

1. 创建至少具有一个专用子网的 VPC。确保机器的无类别域间路由(CIDR)与您的虚拟私有云的 CIDR 匹配。如需更多信息，请参阅 使用您自己的 VPC 和 VPC 验证 的要求。



重要

如果使用防火墙，您必须进行配置，以便 ROSA 可以访问正常工作所需的站点。

如需更多信息，请参阅"AWS PrivateLink 防火墙先决条件"部分。

2. 运行以下命令来创建集群范围的 IAM 角色：

```
$ rosa create account-roles --hosted-cp
```

3. 运行以下命令来创建 OIDC 配置：

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

保存 OIDC 配置 ID，因为您需要创建 Operator 角色。

输出示例

```
I: Setting up managed OIDC configuration
I: To create Operator Roles for this OIDC Configuration, run the following command
and remember to replace <user-defined> with a prefix of your choice:
 rosa create operator-roles --prefix <user-defined> --oidc-config-id
28s4avcdt2l318r1jbk3ifmimkurk384
If you are going to create a Hosted Control Plane cluster please include '--hosted-cp'
I: Creating OIDC provider using 'arn:aws:iam::46545644412:user/user'
I: Created OIDC provider with ARN 'arn:aws:iam::46545644412:oidc-
provider/oidc.op1.openshiftapps.com/28s4avcdt2l318r1jbk3ifmimkurk384'
```

4. 运行以下命令来创建 Operator 角色：

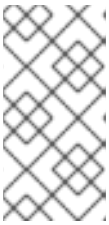
```
$ rosa create operator-roles --hosted-cp --prefix <operator_roles_prefix> --oidc-config-
id <oidc_config_id> --installer-role-arn
arn:aws:iam::$<account_roles_prefix>:role/$<account_roles_prefix>-HCP-ROSA-
Installer-Role
```

5. 运行以下命令，使用 HCP 集群创建私有 ROSA：

```
$ rosa create cluster --private --cluster-name=<cluster-name> --sts --mode=auto --
hosted-cp --operator-roles-prefix <operator_role_prefix> --oidc-config-id
<oidc_config_id> [--machine-cidr=<VPC CIDR>/16] --subnet-ids=<private-subnet-id1>[,
<private-subnet-id2>,<private-subnet-id3>]
```

6. 输入以下命令检查集群的状态。在集群创建过程中，输出中的 State 字段将从 pending 过渡到 Installing，最后变为 ready。

```
$ rosa describe cluster --cluster=<cluster_name>
```



注意

如果安装失败，或者 State 字段在 10 分钟后没有变为 ready，请参阅附加资源部分中的 "Troubleshooting Red Hat OpenShift Service on AWS"。

7. 输入以下命令跟踪 OpenShift 安装程序日志以跟踪集群进度：

```
$ rosa logs install --cluster=<cluster_name> --watch
```

4.2. 配置 AWS 安全组以访问 API

使用带有 HCP 私有集群的 ROSA，客户 VPC 中公开的 AWS PrivateLink 端点具有默认安全组。这个安全组可以访问 PrivateLink 端点，仅限于 VPC 或存在与 VPC CIDR 范围关联的 IP 地址的资源。要通过 VPC 对等和传输网关授予对 VPC 之外的任何实体的访问权限，您必须创建另一个安全组并将其附加到 PrivateLink 端点，以授予必要的访问权限。

先决条件

- 您的企业网络或其他 VPC 已连接。
- 您有在 VPC 中创建和附加安全组的权限。

流程

1. 运行以下命令，将集群名称设置为环境变量：

```
$ export CLUSTER_NAME=<cluster_name>
```

您可以运行以下命令来验证变量是否已设置：

```
$ echo $CLUSTER_NAME
```

输出示例

-

```
hcp-private
```

2. 运行以下命令，查找 VPC 端点(VPCE) ID 和 VPC ID：

```
$ read -r VPCE_ID VPC_ID <<< $(aws ec2 describe-vpc-endpoints --filters
"Name=tag:api.openshift.com/id,Values=$(rosa describe cluster -c
${CLUSTER_NAME} -o yaml | grep '^id: ' | cut -d' ' -f2)" --query 'VpcEndpoints[].
[VpcEndpointId,VpcId]' --output text)
```

3. 运行以下命令来创建您的安全组：

```
$ export SG_ID=$(aws ec2 create-security-group --description "Granting API access to
${CLUSTER_NAME} from outside of VPC" --group-name "${CLUSTER_NAME}-api-sg"
--vpc-id $VPC_ID --output text)
```

4. 运行以下命令，在安全组中添加入站规则：

```
$ aws ec2 authorize-security-group-ingress --group-id $SG_ID --ip-permissions
FromPort=443,ToPort=443,IpProtocol=tcp,IpRanges=[{CidrIp=0.0.0.0/0}]
```

5. 运行以下命令，在 VPCE 中添加新安全组：

```
$ aws ec2 modify-vpc-endpoint --vpc-endpoint-id $VPCE_ID --add-security-group-ids
$SG_ID
```

现在，您可以使用 HCP 私有集群通过 ROSA 访问 API。

4.3. 后续步骤

配置身份提供程序

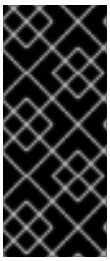
4.4. 其他资源

- AWS PrivateLink 防火墙先决条件

- 使用 STS 部署工作流的 ROSA 概述
- 删除 ROSA 集群
- ROSA 架构模型
- Red Hat OpenShift Service on AWS 安装故障排除

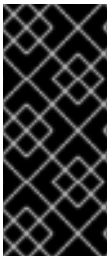
第 5 章 使用外部身份验证创建带有 HCP 集群的 ROSA

您可以使用外部身份验证的托管 control plane (HCP)集群创建 Red Hat OpenShift Service on AWS (ROSA)来发布您的访问令牌。



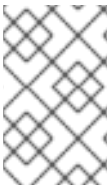
重要

由于无法将现有的 ROSA 集群升级或转换为托管的 control plane 架构，您必须创建一个新集群以使用带有 HCP 功能的 ROSA。您还无法转换创建的集群，以使用外部身份验证供应商使用内部 OAuth2 服务器。您还必须创建新集群。



重要

目前，使用 HCP 的 ROSA 不支持在 多个 AWS 帐户间共享 VPC。不要将带有 HCP 集群的 ROSA 安装到与另一个 AWS 帐户共享的子网。如需更多信息，请参阅 "支持单个 VPC 中的多个 ROSA 集群？"。



注意

使用 HCP 集群的 ROSA 仅支持安全令牌服务(STS)身份验证。

进一步阅读

- 有关 ROSA 与 HCP 和 ROSA Classic 之间的比较，请参阅 比较架构模型 文档。
- 有关在 自动模式中使用 ROSA CLI 开始使用 HCP 的信息， 请参阅 AWS 文档。

其他资源

有关支持的证书的完整列表，请参阅 "Understanding process and security for Red Hat OpenShift Service on AWS" 的 Compliance 部分。

5.1. 带有 HCP 先决条件的 ROSA

要使用 HCP 集群创建 ROSA，您必须完成以下步骤：

- 完成 AWS 的先决条件
- 配置的虚拟私有云(VPC)
- 创建集群范围的角色
- 创建 OIDC 配置
- 创建的 Operator 角色

5.2. 使用外部身份验证供应商创建带有 HCP 集群的 ROSA

在 ROSA CLI 中使用 --external-auth-providers-enabled 标志来创建使用外部身份验证服务的集群。

注意

当使用 HCP 集群创建 ROSA 时，默认的机器无类别间路由(CIDR)为 10.0.0.0/16。如果这与 VPC 子网的 CIDR 范围不匹配，请在以下命令中添加 --machine-cidr <address_block >。

流程

- 如果您使用 OIDC_ID、SUBNET_IDS 和 OPERATOR_ROLES_PREFIX 变量来准备您的环境，您可以在创建集群时继续使用这些变量。例如，运行以下命令：

```
$ rosa create cluster --hosted-cp --subnet-ids=$SUBNET_IDS \
  --oidc-config-id=$OIDC_ID --cluster-name=<cluster_name> \
  --operator-roles-prefix=$OPERATOR_ROLES_PREFIX \
  --external-auth-providers-enabled
```

- 如果您没有设置环境变量，请运行以下命令：

```
$ rosa create cluster --cluster-name=<cluster_name> --sts --mode=auto \
   --hosted-cp --operator-roles-prefix <operator-role-prefix> \
   --oidc-config-id <ID-of-OIDC-configuration> \
   --external-auth-providers-enabled \
   --subnet-ids=<public-subnet-id>,<private-subnet-id>
```

-

验证

- 运行以下命令，验证您的外部身份验证是否在集群详情中启用：

```
$ rosa describe cluster --cluster=<cluster_name>
```

```
Name:                  rosa-ext-test
Display Name:          rosa-ext-test
ID:                    <cluster_id>
External ID:           <cluster_ext_id>
Control Plane:         ROSA Service Hosted
OpenShift Version:     4.16.3
Channel Group:         stable
DNS:                   <dns>
AWS Account:           <AWS_id>
AWS Billing Account:   <AWS_id>
API URL:               <ocm_api>
Console URL:
Region:                us-east-1
Availability:
 - Control Plane:      MultiAZ
 - Data Plane:         SingleAZ

Nodes:
 - Compute (desired):  2
 - Compute (current):  0
Network:
 - Type:               OVNKubernetes
 - Service CIDR:       <service_cidr>
 - Machine CIDR:       <machine_cidr>
 - Pod CIDR:           <pod_cidr>
 - Host Prefix:        /23
 - Subnets:            <subnet_ids>
EC2 Metadata Http Tokens:   optional
Role (STS) ARN:        arn:aws:iam::<AWS_id>:role/<account_roles_prefix>-HCP-ROSA-Installer-Role
Support Role ARN:      arn:aws:iam::<AWS_id>:role/<account_roles_prefix>-HCP-ROSA-Support-Role
Instance IAM Roles:
 - Worker:             arn:aws:iam::<AWS_id>:role/<account_roles_prefix>-HCP-ROSA-Worker-Role
Operator IAM Roles:
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-openshift-cloud-network-config-controller-clo
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-kube-system-capa-controller-manager
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-kube-system-control-plane-operator
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-kube-system-kms-provider
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-kube-system-kube-controller-manager
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-openshift-image-registry-
```

```
installer-cloud-cred
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-openshift-ingress-operator-cloud-credentials
 - arn:aws:iam::<AWS_id>:role/<operator_roles_prefix>-openshift-cluster-csi-drivers-ebs-cloud-crede
Managed Policies:          Yes
State:                     ready
Private:                   No
Created:                   Mar 29 2024 14:25:52 UTC
User Workload Monitoring:  Enabled
Details Page:              https://<url>
OIDC Endpoint URL:         https://<endpoint> (Managed)
Audit Log Forwarding:      Disabled
External Authentication:   Enabled 1
```

1

External Authentication 标志已启用，您现在可以创建外部身份验证供应商。

5.3. 创建外部身份验证供应商

在使用为外部身份验证供应商启用的选项创建带有 HCP 集群的 ROSA 后，您必须使用 ROSA CLI 创建供应商。

注意

与 ROSA CLI 中的 rosa create|delete|list idp[s] 命令类似，您无法编辑使用 rosa create external-auth-provider 创建的现有身份提供程序。相反，您必须删除外部身份验证供应商并创建一个新供应商。

下表显示了创建外部身份验证供应商时可以使用的 CLI 标志：

CLI 标记	描述
--cluster	集群的名称或 ID。
--name	用于引用外部身份验证提供程序的名称。
--console-client-secret	此字符串是客户端 secret，用于将您的帐户与应用程序关联。如果没有包括客户端 secret，这个命令会使用公共 OIDC OAuthClient。
--issuer-audiences	这是以逗号分隔的令牌受众列表。

CLI 标记	描述
--issuer-url	令牌签发者的 URL。
--claim-mapping-username-claim	用于构建集群身份的用户名的声明名称。
--claim-mapping-groups-claim	应该用来构造集群身份组名称的声明名称。

流程

- **要使用交互式命令界面，请运行以下命令：**

```
$ rosa create external-auth-provider -c <cluster_name>
```

```
I: Enabling interactive mode
? Name: 1
? Issuer audiences: 2
? The serving url of the token issuer: 3
? CA file path (optional): 4
? Claim mapping username: 5
? Claim mapping groups: 6
? Claim validation rule (optional): 7
? Console client id (optional): 8
```

1. **外部身份验证供应商的名称。此名称应为带有数字和短划线的小写。**
2. **此身份验证提供程序发布令牌的受众 ID。**
3. **提供令牌的签发者 URL。**
4. **可选：发出请求时使用的证书文件。**
5. **用于构造集群身份的用户名的声明名称，如使用 电子邮件。**

6

将 ID 令牌转换为集群身份的方法，例如使用 组。

7

可选：帮助验证用户验证令牌声明的规则。此字段应格式化为 :< required_value>。

8

可选：应用程序注册用于控制台的应用程序或客户端 ID。

- 您可以使用以下命令包括创建外部身份验证供应商所需的 ID：

```
rosa create external-auth-provider --cluster=<cluster_id> \
  --name=<provider_name> --issuer-url=<issuing_url> \
  --issuer-audiences=<audience_id> \
  --claim-mapping-username-claim=email \
  --claim-mapping-groups-claim=groups \
  --console-client-id=<client_id_for_app_registration> \
  --console-client-secret=<client_secret>
```

输出示例

```
I: Successfully created an external authentication provider for cluster '<cluster_id>'
```

验证

- 要验证外部身份验证供应商，请运行以下选项之一：
  - 使用以下命令列出指定集群中的外部身份验证配置：

```
$ rosa list external-auth-provider -c <cluster_name>
```

输出示例

以下示例显示了配置的 Microsoft Entra ID 外部身份验证供应商：

```
NAME       ISSUER URL
m-entra-id  https://login.microsoftonline.com/<group_id>/v2.0
```

- 使用以下命令在指定集群中显示外部身份验证配置：

```
$ rosa describe external-auth-provider \
  -c <cluster_name> --name <name_of_external_authentication>
```

输出示例

```
ID:                         ms-entra-id
Cluster ID:                 <cluster_id>
Issuer audiences:
                          - <audience_id>
Issuer Url:                 https://login.microsoftonline.com/<group_id>/v2.0
Claim mappings group:       groups
Claim mappings username:    email
```

其他资源

- 有关为您的 IDP 配置 Entra ID 的更多信息，请参阅 Azure 文档中的 Microsoft Entra ID? 或配置 Microsoft Entra ID （以前称为 Azure Active Directory）部分作为文档的身份提供程序 指南 部分。
- 有关 ROSA CLI 中类似的 idps 工具的详情，请参考 创建 idp。
- 有关 ROSA CLI 中的选项的更多信息，请参阅创建 external-auth-provider、列出 external-auth-provider，并删除 external-auth-provider。

5.4. 为使用 HCP 集群的 ROSA 创建中断特征凭证

作为带有 HCP 集群所有者的 ROSA，您可以使用 breakcommands 凭证创建临时管理客户端凭证来访问配置了自定义 OpenID Connect (OIDC)令牌签发者的集群。创建 breakfish 凭证会生成新的 cluster-admin kubeconfig 文件。kubeconfig 文件包含关于 CLI 用来将客户端连接到正确的集群和 API 服务器的集群的信息。您可以使用新生成的 kubeconfig 文件来允许使用 HCP 集群访问 ROSA。

先决条件

- 您已创建了启用了外部身份验证的 HCP 集群的 ROSA。如需更多信息，*请参阅使用外部身份验证供应商 的 HCP 集群创建 ROSA*。

- 您已创建了外部身份验证供应商。如需更多信息，*请参阅创建外部身份验证供应商*。

- 有 具有集群管理员权限的帐户。

流程

1. 使用以下命令之一创建中断特征凭证：

   - 要使用互动命令界面以交互方式指定自定义设置来创建中断特征凭证，请运行以下命令：

     ```
     $ rosa create break-glass-credential -c <cluster_name> -i (1)
     ```

     (1) 将 <cluster_name> 替换为集群的名称。

     这个命令启动交互式 CLI 进程：

     输出示例

     ```
     I: Enabling interactive mode
     ? Username (optional): (1)
     ? Expiration duration (optional): (2)
     I: Successfully created a break glass credential for cluster 'ac-hcp-test'.
     ```

     (1) 如果留空，则 用户名中的值 将具有随机生成的用户名值。

     (2)

- 使用指定的值，为名为 mycluster 的集群创建一个 break trait 凭证：

```
$ rosa create break-glass-credential -c mycluster --username test-username --
expiration 1h
```

2. 运行以下命令，列出适用于名为 mycluster 的集群可用的 break space 凭证 ID、状态和关联的用户：

```
$ rosa list break-glass-credential -c mycluster
```

输出示例

```
ID                           USERNAME    STATUS
2a7jli9n4phe6c02ul7ti91djtv2o51d  test-user   issued
```

注意

您还可以通过在命令中添加 -o json 参数来查看 JSON 输出中的凭证。

3. 要查看 breakuildDefaults 凭证的状态，请运行以下命令，将 <break_glass_credential_id> 替换为 breakerior 凭证 ID：

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c <cluster_name>
```

输出示例

```
ID:                          2a7jli9n4phe6c02ul7ti91djtv2o51d
Username:                         test-user
Expire at:                     Dec 28 2026 10:23:05 EDT
Status:                        issued
```

以下是可能的 Status 字段值列表：

- 签发 了 breakinitial 凭证，并可供使用。
- 已过期的 breakinitial 凭证已过期，无法再使用。
- 失败，导致凭证创建失败。在这种情况下，您会收到一个服务日志，详细描述了故障。如需有关服务日志的更多信息，*请参阅访问 Red Hat OpenShift Service on AWS 集群的服务日志*。有关联系红帽支持以获取帮助的步骤，请参阅 *获取支持*。
- awaiting_revocation The breakuildDefaults credential 当前正在撤销，这意味着无法使用它。
- 已撤销 的 break zones 凭证已被撤销，无法再使用。

4. 要检索 kubeconfig，请运行以下命令：

- 创建 kubeconfigs 目录：

```
$ mkdir ~/kubeconfigs
```

- 导出新生成的 kubeconfig 文件，将 <cluster_name> 替换为集群的名称：

```
$ export CLUSTER_NAME=<cluster_name> && export
KUBECONFIG=~/kubeconfigs/break-glass-${CLUSTER_NAME}.kubeconfig
```

- 查看 kubeconfig ：

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c mycluster --
kubeconfig
```

输出示例

```
apiVersion: v1
clusters:
- cluster:
    server: <server_url>
  name: cluster
contexts:
- context:
    cluster: cluster
    namespace: default
    user: test-username
  name: admin
current-context: admin
kind: Config
preferences: {}
users:
- name: test-user
  user:
    client-certificate-data: <client-certificate-data> (1)
    client-key-data: <client-key-data> (2)
```

(1) client-certificate 包含由 Kubernetes 证书颁发机构(CA)签名的用户的证书。

(2) client-key 包含签署客户端证书的密钥。

5. 可选： 要保存 kubeconfig，请运行以下命令：

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c mycluster --
kubeconfig > $KUBECONFIG
```

其他资源

- 有关创建启用了外部身份验证的 HCP 集群的 ROSA 的更多信息，请参阅创建带有外部身份验证供应商的 HCP 集群的 ROSA。
- 如需有关 CLI 配置的更多信息，请参阅管理 CLI 配置集。

5.5. 使用 BREAKLET CREDENTIAL 访问带有 HCP 集群的 ROSA

使用 breakuildDefaults 凭证中的新的 kubeconfig 来获取对带有 HCP 集群的 ROSA 的临时管理员访问权限。

先决条件

- 您可以访问启用了外部身份验证的 HCP 集群的 ROSA。如需更多信息，*请参阅使用外部身份验证供应商的 HCP 集群创建 ROSA*。
- 已安装 oc 和 kubectl CLI。
- 您已配置了新的 kubeconfig。如需更多信息，请参阅 *使用 HCP 集群为 ROSA 创建中断凭证*。

流程

1. 访问集群的详情：

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c <cluster_name>
--kubeconfig > $KUBECONFIG
```

2. 列出集群中的节点：

```
$ oc get nodes
```

输出示例

```
NAME                          STATUS   ROLES   AGE   VERSION
ip-10-0-0-27.ec2.internal   Ready    worker  8m    v1.28.7+f1b5f6c
ip-10-0-0-67.ec2.internal   Ready    worker  9m    v1.28.7+f1b5f6c
```

3. 验证您是否有正确的凭证：

```
$ kubectl auth whoami
```

输出示例

```
ATTRIBUTE    VALUE
Username     system:customer-break-glass:test-user
Groups       [system:masters system:authenticated]
```

4. 为外部 OIDC 供应商中定义的组应用 ClusterRoleBinding。ClusterRoleBinding 将在 Microsoft Entra ID 中创建的 rosa-hcp-admins 组映射到带有 HCP 集群的 ROSA 中的组。

```
$ oc apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: rosa-hcp-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: f715c264-ab90-45d5-8a29-2e91a609a895
EOF
```

输出示例

```
clusterrolebinding.rbac.authorization.k8s.io/rosa-hcp-admins created
```

注意

应用 ClusterRoleBinding 后，配置了 HCP 集群的 ROSA，并且 rosa CLI 和 Red Hat Hybrid Cloud Console 通过外部 OpenID Connect (OIDC)供应商进行身份验证。现在，您可以开始分配角色并在集群中部署应用程序。

其他资源

- 有关集群角色绑定的更多信息，请参阅使用 RBAC 定义和应用权限。

5.6. 为带有 HCP 集群的 ROSA 撤销一个断外凭证

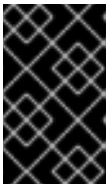
您可以使用 revoke break-glass-credentials 命令撤销对您随时置备的任何断查看凭证的访问。

先决条件

- 您已创建了一个断动凭证。
- 您是集群所有者。

流程

- 运行以下命令，为带有 HCP 集群的 ROSA 撤销 breakinitial 凭证。



重要

运行此命令将撤销对集群相关的所有 breakerior 凭据的访问权限。

```
$ rosa revoke break-glass-credentials -c <cluster_name> 1
```

1

将 <cluster_name> 替换为集群的名称。

输出示例

```
? Are you sure you want to revoke all the break glass credentials on cluster 'my-cluster'?: Yes
I: Successfully requested revocation for all break glass credentials from cluster 'my-cluster'
```

验证

- 吊销过程可能需要几分钟。您可以运行以下命令来验证集群的 breaklet 凭证是否已撤销：
  - 列出所有 breakinitial 凭证，并检查每个凭证的状态：

```
$ rosa list break-glass-credential -c <cluster_name>
```

输出示例

```
ID                            USERNAME    STATUS
2330dbs0n8m3chkkr25gkkcd8pnj3lk2  test-user   awaiting_revocation
```

  - 您还可以通过检查单个凭证来验证状态：

```
$ rosa describe break-glass-credential <break_glass_credential_id> -c
<cluster_name>
```

输出示例

```
ID:                       2330dbs0n8m3chkkr25gkkcd8pnj3lk2
Username:                       test-user
Expire at:                 Dec 28 2026 10:23:05 EDT
Status:                   issued
Revoked at:                     Dec 27 2026 15:30:33 EDT
```

5.7. 删除外部身份验证供应商

使用 ROSA CLI 删除外部身份验证供应商。

流程

1. 运行以下命令，在集群中显示外部身份验证供应商：

```
$ rosa list external-auth-provider -c <cluster_name>
```

输出示例

```
NAME        ISSUER URL
entra-test  https://login.microsoftonline.com/<group_id>/v2.0
```

2. 运行以下命令来删除外部身份验证供应商：

```
$ rosa delete external-auth-provider <name_of_provider> -c <cluster_name>
```

输出示例

```
? Are you sure you want to delete external authentication provider entra-test on
cluster rosa-ext-test? Yes
I: Successfully deleted external authentication provider 'entra-test' from cluster 'rosa-
ext-test'
```

验证

1. 运行以下命令，查询集群中的任何外部身份验证供应商：

```
$ rosa list external-auth-provider -c <cluster_name>
```

输出示例

> E: there are no external authentication providers for this cluster

5.8. 其他资源

- 有关使用手动模式部署 ROSA 集群的步骤，请参阅使用自定义创建集群。
- 有关使用 STS 部署 Red Hat OpenShift Service on AWS 所需的 AWS Identity Access Management (IAM)资源的更多信息，请参阅关于使用 STS 的集群的 IAM 资源。
- 要了解更多有关 Red Hat OpenShift Service on AWS 的默认 CIDR 范围的信息，请参阅 CIDR 范围定义。
- 有关可选设置 Operator 角色名称前缀的详情，请参阅关于自定义 Operator IAM 角色前缀。
- 有关使用 STS 安装 ROSA 的先决条件的详情，请参考使用 STS 的 ROSA 的 AWS 先决条件。
- 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。
- 有关在 AWS IAM 中使用 OpenID Connect (OIDC)身份提供程序的更多信息，请参阅 AWS 文档中的 创建 OpenID Connect (OIDC)身份供应商。
- 有关 ROSA 集群安装故障排除的更多信息，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 获取对 Red Hat OpenShift Service on AWS 的支持。

第 6 章 在带有 HCP 集群的 ROSA 上使用 NODE TUNING OPERATOR

带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)支持 Node Tuning Operator，以提高使用 HCP 集群中的 ROSA 上的节点性能。在创建节点调优配置前，必须创建自定义性能优化规格。

用途

Node Tuning Operator 可以帮助您通过编排 TuneD 守护进程来管理节点级别的性能优化，并使用 Performance Profile 控制器获得低延迟性能。大多数高性能应用程序都需要一定程度的内核级性能优化。Node Tuning Operator 为用户提供了一个统一的、节点一级的 sysctl 管理接口，并可以根据具体用户的需要灵活地添加自定义性能优化设置。

Operator 将 Red Hat OpenShift Service 的容器化 TuneD 守护进程作为 Kubernetes 守护进程集进行管理。它保证了自定义性能优化设置以可被守护进程支持的格式传递到在集群中运行的所有容器化的 TuneD 守护进程中。相应的守护进程会在集群的所有节点上运行，每个节点上运行一个。

在发生触发配置集更改的事件时，或通过接收和处理终止信号安全终止容器化 TuneD 守护进程时，容器化 TuneD 守护进程所应用的节点级设置将被回滚。

Node Tuning Operator 使用 Performance Profile 控制器来实现自动性能优化，以实现 Red Hat OpenShift Service on AWS 应用程序的低延迟性能。

集群管理员配置了性能配置集以定义节点级别的设置，例如：

- 将内核更新至 kernel-rt。
- 为内务选择 CPU。
- 为运行工作负载选择 CPU。

注意

目前，cgroup v2 不支持禁用 CPU 负载均衡。因此，如果您启用了 cgroup v2，则可能无法从性能配置集中获取所需的行为。如果您使用性能配置集，则不建议启用 cgroup v2。

Node Tuning Operator 是版本 4.1 及更高版本中的标准 Red Hat OpenShift Service on AWS 安装的一部分。

注意

在早期版本的 Red Hat OpenShift Service on AWS 中，Performance Addon Operator 用来实现自动性能优化，以便为 OpenShift 应用程序实现低延迟性能。在 Red Hat OpenShift Service on AWS 4.11 及更新的版本中，这个功能是 Node Tuning Operator 的一部分。

6.1. 自定义调整规格

Operator 的自定义资源 (CR) 包含两个主要部分。第一部分是 profile:，这是 TuneD 配置集及其名称的列表。第二部分是 recommend:，用来定义配置集选择逻辑。

多个自定义调优规格可以共存，作为 Operator 命名空间中的多个 CR。Operator 会检测到是否存在新 CR 或删除了旧 CR。所有现有的自定义性能优化设置都会合并，同时更新容器化 TuneD 守护进程的适当对象。

管理状态

通过调整默认的 Tuned CR 来设置 Operator Management 状态。默认情况下，Operator 处于 Managed 状态，默认的 Tuned CR 中没有 spec.managementState 字段。Operator Management 状态的有效值如下：

- Managed: Operator 会在配置资源更新时更新其操作对象
- Unmanaged: Operator 将忽略配置资源的更改
- Removed: Operator 将移除 Operator 置备的操作对象和资源

配置集数据

profile: 部分列出了 TuneD 配置集及其名称。

```
{
  "profile": [
    {
      "name": "tuned_profile_1",
      "data": "# TuneD profile specification\n[main]\nsummary=Description of tuned_profile_1
profile\n\n[sysctl]\nnet.ipv4.ip_forward=1\n# ... other sysctl's or other TuneD daemon plugins
supported by the containerized TuneD\n"
    },
    {
      "name": "tuned_profile_n",
      "data": "# TuneD profile specification\n[main]\nsummary=Description of tuned_profile_n
profile\n\n# tuned_profile_n profile settings\n"
    }
  ]
}
```

建议的配置集

profile: 选择逻辑通过 CR 的 recommend: 部分来定义。recommend: 部分是根据选择标准推荐配置集的项目列表。

```
"recommend": [
    {
      "recommend-item-1": details_of_recommendation,
      # ...
      "recommend-item-n": details_of_recommendation,
    }
  ]
```

列表中的独立项：

```
{
  "profile": [
    {
    # ...
    }
  ],
  "recommend": [
    {
      "profile": <tuned_profile_name>, (1)
      "priority":{ <priority>, (2)
      },
      "match": [ (3)
        {
          "label": <label_information> (4)
        },
      ]
```

```
    },
  ]
}
```

1 在匹配项中应用的 TuneD 配置集。例如 tuned_profile_1。

2 配置集排序优先级。较低数字表示优先级更高（0 是最高优先级）。

3 如果省略，则会假定配置集匹配，除非优先级较高的配置集首先匹配。

4 配置集匹配项目的标签。

<match> 是一个递归定义的可选数组，如下所示：

```
"match": [
      {
        "label": 1
      },
]
```

1 节点或 pod 标签名称。

如果不省略 <match>，则所有嵌套的 <match> 部分也必须评估为 true。否则会假定 false，并且不会应用或建议具有对应 <match> 部分的配置集。因此，嵌套（子级 <match> 部分）会以逻辑 AND 运算来运作。反之，如果匹配 <match> 列表中任何一项，整个 <match> 列表评估为 true。因此，该列表以逻辑 OR 运算来运作。

示例：基于节点或 pod 标签的匹配

```
[
  {
    "match": [
```

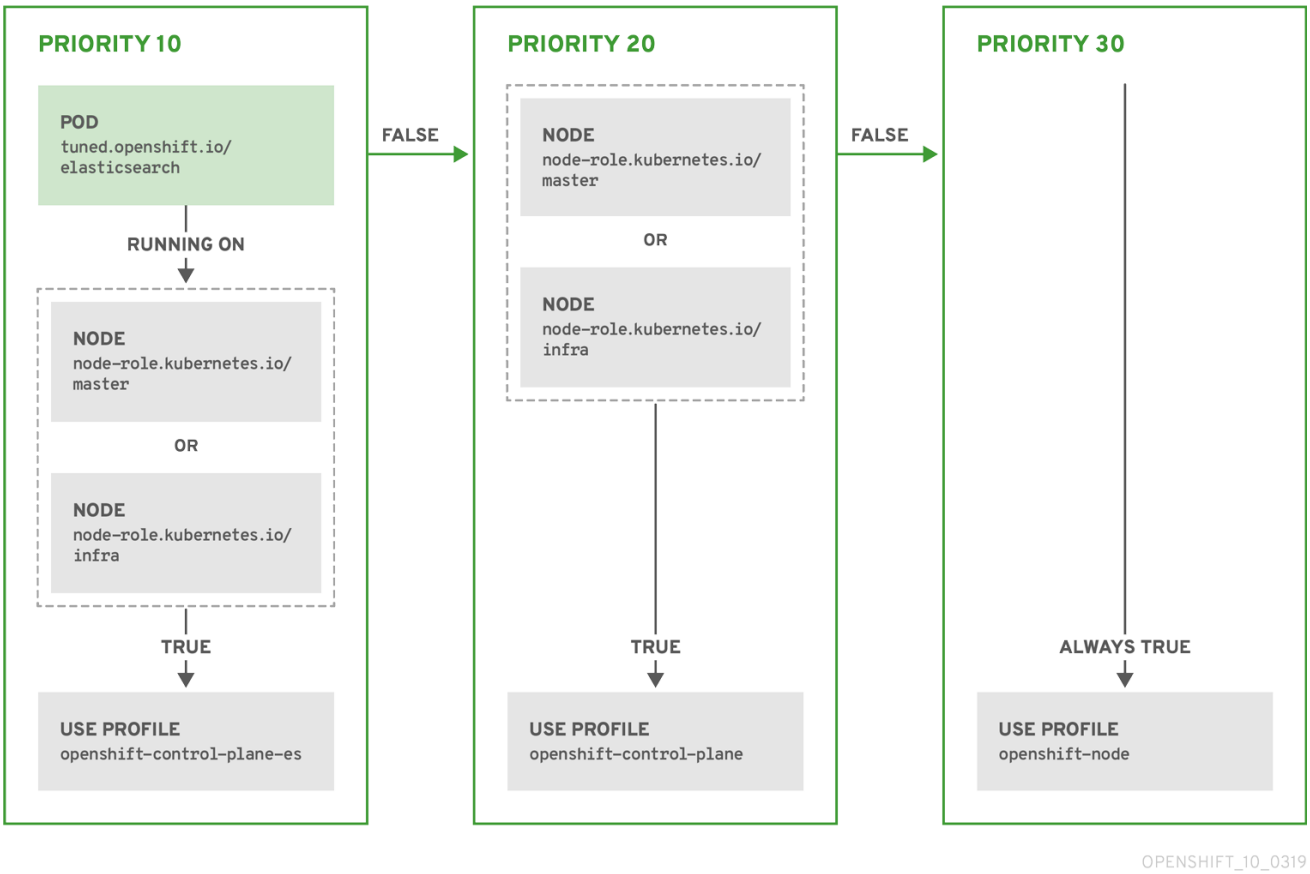
```
      {
        "label": "tuned.openshift.io/elasticsearch",
        "match": [
          {
            "label": "node-role.kubernetes.io/master"
          },
          {
            "label": "node-role.kubernetes.io/infra"
          }
        ],
        "type": "pod"
      }
    ],
    "priority": 10,
    "profile": "openshift-control-plane-es"
  },
  {
    "match": [
      {
        "label": "node-role.kubernetes.io/master"
      },
      {
        "label": "node-role.kubernetes.io/infra"
      }
    ],
    "priority": 20,
    "profile": "openshift-control-plane"
  },
  {
    "priority": 30,
    "profile": "openshift-node"
  }
]
```

根据配置集优先级，以上 CR 针对容器化 TuneD 守护进程转换为 recommend.conf 文件。优先级最高 (10) 的配置集是 openshift-control-plane-es，因此会首先考虑它。在给定节点上运行的容器化 TuneD 守护进程会查看同一节点上是否在运行设有 tuned.openshift.io/elasticsearch 标签的 pod。如果没有，则整个 <match> 部分评估为 false。如果存在具有该标签的 pod，为了让 <match> 部分评估为 true，节点标签也需要是 node-role.kubernetes.io/master 或 node-role.kubernetes.io/infra。

如果这些标签对优先级为 10 的配置集而言匹配，则应用 openshift-control-plane-es 配置集，并且不考虑其他配置集。如果节点/pod 标签组合不匹配，则考虑优先级第二高的配置集 (openshift-control-plane)。如果容器化 TuneD Pod 在具有标签 node-role.kubernetes.io/master 或 node-role.kubernetes.io/infra 的节点上运行，则应用此配置集。

最后，配置集 openshift-node 的优先级最低 (30)。它没有 <match> 部分，因此始终匹配。如果给定节点上不匹配任何优先级更高的配置集，它会作为一个适用于所有节点的配置集来设置 openshift-node

配置集。



示例：基于机器池的匹配

```
{
  "apiVersion": "tuned.openshift.io/v1",
  "kind": "Tuned",
  "metadata": {
    "name": "openshift-node-custom",
    "namespace": "openshift-cluster-node-tuning-operator"
  },
  "spec": {
    "profile": [
      {
        "data": "[main]\nsummary=Custom OpenShift node profile with an additional kernel
parameter\ninclude=openshift-
node\n[bootloader]\ncmdline_openshift_node_custom=+skew_tick=1\n",
        "name": "openshift-node-custom"
      }
    ],
    "recommend": [
      {
        "priority": 20,
        "profile": "openshift-node-custom"
      }
```

```
    ]
  }
}
```

特定于云供应商的 TuneD 配置集

通过此功能，所有针对 Red Hat OpenShift Service on AWS 集群上的特定云供应商都可以方便地分配一个 TuneD 配置集。这可实现，而无需添加额外的节点标签或将节点分组到机器池中。

这个功能会利用 spec.providerID 节点对象值（格式为 <cloud-provider>://<cloud-provider-specific-id>），并在 NTO operand 容器中写带有 <cloud-provider> 值的文件 /var/lib/ocp-tuned/provider。然后，TuneD 会使用这个文件的内容来加载 provider-<cloud-provider> 配置集（如果这个配置集存在）。

openshift 配置集（openshift-control-plane 和 openshift-node 配置集都从其中继承设置）现在被更新来使用这个功能（通过使用条件配置集加载）。NTO 或 TuneD 目前不包含任何特定于云供应商的配置集。但是，您可以创建一个自定义配置集 provider-<cloud-provider>，它将适用于所有针对于所有云供应商的集群节点。

GCE 云供应商配置集示例

```
{
  "apiVersion": "tuned.openshift.io/v1",
  "kind": "Tuned",
  "metadata": {
    "name": "provider-gce",
    "namespace": "openshift-cluster-node-tuning-operator"
  },
  "spec": {
    "profile": [
      {
        "data": "[main]\nsummary=GCE Cloud provider-specific profile\n# Your tuning for GCE Cloud provider goes here.\n",
        "name": "provider-gce"
      }
    ]
  }
}
```

注意

由于配置集的继承，provider-<cloud-provider> 配置集中指定的任何设置都会被 openshift 配置集及其子配置集覆盖。

6.2. 在带有 HCP 的 ROSA 上创建节点调优配置

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI rosa 创建调优配置。

先决条件

- 您已下载了 ROSA CLI 的最新版本。
- 在最新版本中有一个集群。
- 您已为节点调整配置了规格文件。

流程

1. 运行以下命令来创建调整配置：

```
$ rosa create tuning-config -c <cluster_id> --name <name_of_tuning> --spec-path
<path_to_spec_file>
```

您必须提供 spec.json 文件的路径，或者命令会返回错误。

输出示例

```
$ I: Tuning config 'sample-tuning' has been created on cluster 'cluster-example'.
$ I: To view all tuning configs, run 'rosa list tuning-configs -c cluster-example'
```

验证

- 您可以使用以下命令验证您的帐户应用的现有性能优化配置：

```
$ rosa list tuning-configs -c <cluster_name> [-o json]
```

您可以为配置列表指定输出类型。

- 如果没有指定输出类型，您会看到调优配置的 ID 和名称：

不指定输出类型的输出示例

```
ID                                   NAME
20468b8e-edc7-11ed-b0e4-0a580a800298  sample-tuning
```

- 如果指定了输出类型，如 json，您将以 JSON 文本形式接收调优配置：

注意

以下 JSON 输出具有硬行处理，用于读清晰性。除非在 JSON 字符串中删除新行，否则此 JSON 输出无效。

指定 JSON 输出的输出示例

```
[
  {
    "kind": "TuningConfig",
    "id": "20468b8e-edc7-11ed-b0e4-0a580a800298",
    "href":
"/api/clusters_mgmt/v1/clusters/23jbsevqb22l0m58ps39ua4trff9179e/tuning_config
s/20468b8e-edc7-11ed-b0e4-0a580a800298",
```

```
    "name": "sample-tuning",
    "spec": {
      "profile": [
        {
          "data": "[main]\nsummary=Custom OpenShift profile\ninclude=openshift-
node\n\n[sysctl]\nvm.dirty_ratio=\"55\"\n",
          "name": "tuned-1-profile"
        }
      ],
      "recommend": [
        {
          "priority": 20,
          "profile": "tuned-1-profile"
        }
      ]
    }
  }
]
```

6.3. 为带有 HCP 的 ROSA 修改节点调优配置

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI (rosa)查看和更新节点调优配置。

先决条件

- 您已下载了 ROSA CLI 的最新版本。
- 在最新版本中有一个集群
- 您的集群已添加了节点调优配置

流程

1. 您可以使用 rosa describe 命令查看调优配置：

```
$ rosa describe tuning-config -c <cluster_id> 1
    --name <name_of_tuning> 2
    [-o json] 3
```

此 spec 文件中的以下项是：

1

为您拥有的集群提供集群 ID，以应用节点调优配置。

2

提供调优配置的名称。

3

另外，您还可以提供输出类型。如果没有指定任何输出，则只看到调优配置的 ID 和名称。

不指定输出类型的输出示例

```
Name:    sample-tuning
ID:      20468b8e-edc7-11ed-b0e4-0a580a800298
Spec:    {
          "profile": [
            {
              "data": "[main]\nsummary=Custom OpenShift profile\ninclude=openshift-
node\n\n[sysctl]\nvm.dirty_ratio=\"55\"\n",
              "name": "tuned-1-profile"
            }
          ],
          "recommend": [
            {
              "priority": 20,
              "profile": "tuned-1-profile"
            }
          ]
        }
```

指定 JSON 输出的输出示例

```
{
  "kind": "TuningConfig",
  "id": "20468b8e-edc7-11ed-b0e4-0a580a800298",
  "href":
```

```
"/api/clusters_mgmt/v1/clusters/23jbsevqb22l0m58ps39ua4trff9179e/tuning_configs/20
468b8e-edc7-11ed-b0e4-0a580a800298",
  "name": "sample-tuning",
  "spec": {
    "profile": [
      {
        "data": "[main]\nsummary=Custom OpenShift profile\ninclude=openshift-
node\n\n[sysctl]\nvm.dirty_ratio=\"55\"\n",
        "name": "tuned-1-profile"
      }
    ],
    "recommend": [
      {
        "priority": 20,
        "profile": "tuned-1-profile"
      }
    ]
  }
}
```

2. 验证调优配置后，您可以使用 rosa edit 命令编辑现有的配置：

```
$ rosa edit tuning-config -c <cluster_id> --name <name_of_tuning> --spec-path
<path_to_spec_file>
```

在这个命令中，您可以使用 spec.json 文件编辑您的配置。

验证

- 再次运行 rosa describe 命令，以查看您在调优配置中更新了对 spec.json 文件所做的更改：

```
$ rosa describe tuning-config -c <cluster_id> --name <name_of_tuning>
```

输出示例

```
Name:  sample-tuning
ID:    20468b8e-edc7-11ed-b0e4-0a580a800298
Spec:  {
         "profile": [
           {
            "data": "[main]\nsummary=Custom OpenShift profile\ninclude=openshift-
```

```
node\n\n[sysctl]\nvm.dirty_ratio=\"55\"\n",
            "name": "tuned-2-profile"
          }
        ],
        "recommend": [
          {
           "priority": 10,
           "profile": "tuned-2-profile"
          }
        ]
      }
```

6.4. 删除带有 HCP 的 ROSA 上的节点调优配置

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI rosa 删除调优配置。

注意

您无法删除机器池中引用的调优配置。您必须先从所有机器池中删除调优配置，然后才能删除它。

先决条件

- 您已下载了 ROSA CLI 的最新版本。
- 在最新版本上有一个集群。
- 集群具有您要删除的节点调优配置。

流程

- 要删除调整配置，请运行以下命令：

```
$ rosa delete tuning-config -c <cluster_id> <name_of_tuning>
```

集群的调优配置已删除

输出示例

```
? Are you sure you want to delete tuning config sample-tuning on cluster sample-cluster? Yes
I: Successfully deleted tuning config 'sample-tuning' from cluster 'sample-cluster'
```

第 7 章 使用 HCP 集群删除 ROSA

如果要删除带有托管 control plane (HCP)集群的 Red Hat OpenShift Service on AWS (ROSA)，您可以使用 Red Hat OpenShift Cluster Manager 或 ROSA 命令行界面(CLI) (rosa)。删除集群后，您还可以删除集群使用的 AWS Identity and Access Management (IAM)资源。

7.1. 使用 HCP 集群和特定于集群的 IAM 资源删除 ROSA

您可以使用 ROSA 命令行界面(CLI)或 Red Hat OpenShift Cluster Manager 删除带有 HCP 集群的 ROSA。

删除集群后，您可以使用 ROSA CLI 清理 AWS 帐户中特定于集群的 Identity and Access Management (IAM)资源。特定于集群的资源包括 Operator 角色和 OpenID Connect (OIDC)供应商。

注意

集群删除必须在删除 IAM 资源前完成，因为集群删除和清理过程会用到这些资源。

如果安装了附加组件，集群删除需要更长的时间，因为在删除集群前卸载附加组件。所需时间取决于附加组件的数量和大小。

先决条件

- 已使用 HCP 集群安装了 ROSA。
- 您已在安装主机上安装并配置了最新的 ROSA CLI (rosa)。

流程

1. 运行以下命令，获取集群 ID、特定于集群的 Operator 角色的 Amazon 资源名称(ARN)和 OIDC 供应商的端点 URL：

```
$ rosa describe cluster --cluster=<cluster_name>
```

输出示例

```
Name:                  test_cluster
Domain Prefix:         test_cluster
Display Name:          test_cluster
ID:                    <cluster_id> (1)
External ID:           <external_id>
Control Plane:         ROSA Service Hosted
OpenShift Version:     4.16.0
Channel Group:         stable
DNS:                   test_cluster.l3cn.p3.openshiftapps.com
AWS Account:           <AWS_id>
AWS Billing Account:   <AWS_id>
API URL:               https://api.test_cluster.l3cn.p3.openshiftapps.com:443
Console URL:
Region:                us-east-1
Availability:
 - Control Plane:      MultiAZ
 - Data Plane:         SingleAZ

Nodes:
 - Compute (desired):  2
 - Compute (current):  0
Network:
 - Type:               OVNKubernetes
 - Service CIDR:       172.30.0.0/16
 - Machine CIDR:       10.0.0.0/16
 - Pod CIDR:           10.128.0.0/14
 - Host Prefix:        /23
 - Subnets:            <subnet_ids>
EC2 Metadata Http Tokens:   optional
Role (STS) ARN:        arn:aws:iam::<AWS_id>:role/test_cluster-HCP-ROSA-Installer-
Role
Support Role ARN:      arn:aws:iam::<AWS_id>:role/test_cluster-HCP-ROSA-
Support-Role
Instance IAM Roles:
 - Worker:             arn:aws:iam::<AWS_id>:role/test_cluster-HCP-ROSA-Worker-Role
Operator IAM Roles: (2)
 - arn:aws:iam::<AWS_id>:role/test_cluster-openshift-cloud-network-config-controller-
cloud-crede
 - arn:aws:iam::<AWS_id>:role/test_cluster-openshift-image-registry-installer-cloud-
credentials
 - arn:aws:iam::<AWS_id>:role/test_cluster-openshift-ingress-operator-cloud-
credentials
 - arn:aws:iam::<AWS_id>:role/test_cluster-kube-system-kube-controller-manager
 - arn:aws:iam::<AWS_id>:role/test_cluster-kube-system-capa-controller-manager
 - arn:aws:iam::<AWS_id>:role/test_cluster-kube-system-control-plane-operator
 - arn:aws:iam::<AWS_id>:role/hcpcluster-kube-system-kms-provider
 - arn:aws:iam::<AWS_id>:role/test_cluster-openshift-cluster-csi-drivers-ebs-cloud-
credentials
Managed Policies:      Yes
State:                 ready
Private:               No
Created:               Apr 16 2024 20:32:06 UTC
User Workload Monitoring:   Enabled
Details Page:          https://console.redhat.com/openshift/details/s/<cluster_id>
OIDC Endpoint URL:     https://oidc.op1.openshiftapps.com/<cluster_id> (Managed)
```

```
Audit Log Forwarding:      Disabled
External Authentication:   Disabled
```

1 列出集群 ID。

2 指定特定于集群 Operator 角色的 ARN。例如，在示例输出中，Machine Config Operator 所需的角色的 ARN 是 arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-machine-api-aws-cloud-credentials。

3 显示特定于集群的 OIDC 供应商的端点 URL。

重要

删除集群后，您需要集群 ID 来使用 ROSA CLI 删除特定于集群的 STS 资源。

2. 使用 OpenShift Cluster Manager 或 ROSA CLI (rosa)删除集群：

- 使用 OpenShift Cluster Manager 删除集群：

  a. 导航到 OpenShift Cluster Manager。

  b. 点击集群

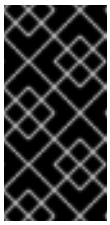
  旁边的 Options 菜单并选择 Delete cluster。

  c. 在提示符中输入集群名称并点 Delete。

- 使用 ROSA CLI 删除集群：

a. 运行以下命令，将 &lt ;cluster_name > 替换为集群的名称或 ID：

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



重要

在删除 Operator 角色和 OIDC 供应商前，您必须等待集群删除完成。

3. 运行以下命令来删除特定于集群的 Operator IAM 角色：

```
$ rosa delete operator-roles --prefix <operator_role_prefix>
```

4. 运行以下命令来删除 OIDC 供应商：

```
$ rosa delete oidc-provider --oidc-config-id <oidc_config_id>
```

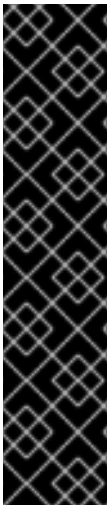
故障排除

- 如果因为缺少 IAM 角色而无法删除 集群，请参阅修复无法删除的集群。
- 如果因为其他原因无法删除集群：
  - 在 Hybrid Cloud Console 中，确保没有待处理的集群附加组件。
  - 确保 Amazon Web 控制台中删除了所有 AWS 资源和依赖项。

7.2. 删除帐户范围的 IAM 资源

删除所有依赖于账户范围的 AWS Identity and Access Management (IAM)资源的 Red Hat OpenShift Service on AWS (ROSA)集群后，您可以删除集群范围的资源。

如果您不再需要使用 Red Hat OpenShift Cluster Manager 安装带有 HCP 集群的 ROSA，您也可以删除 OpenShift Cluster Manager 和用户 IAM 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 HCP 集群使用。只有资源不再被其他集群需要时，才删除这些资源。

如果要使用 OpenShift Cluster Manager 在相同的 AWS 帐户中安装、管理和删除其他 Red Hat OpenShift Service on AWS 集群，则需要 OpenShift Cluster Manager 和用户 IAM 角色。只有在不再需要使用 OpenShift Cluster Manager 在账户的 AWS 集群上安装 Red Hat OpenShift Service 时，才删除角色。有关在删除前删除这些角色时修复集群的更多信息，请参阅"对集群 *部署的故障排除中的修复集群* "。

其他资源

- 修复无法删除的集群

7.2.1. 删除帐户范围的 IAM 角色和策略

本节提供了删除您为使用 HCP 部署的 ROSA 创建的帐户范围的 IAM 角色和策略，以及帐户范围内的 Operator 策略的步骤。只有在删除所有依赖它们的 HCP 集群的 ROSA 后，才能删除账户范围的 AWS Identity and Access Management (IAM)角色和策略。

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 Red Hat OpenShift Service on AWS 使用。只有角色不再被其他集群需要时，才删除这些资源。

先决条件

- 您有要删除的帐户范围的 IAM 角色。
- 您已在安装主机上安装并配置了最新的 ROSA CLI (rosa)。

流程

1. 删除集群范围的角色：

   a. 使用 ROSA CLI 列出 AWS 帐户中的系统范围角色 (rosa)：

```
$ rosa list account-roles
```

   输出示例

```
I: Fetching account roles
ROLE NAME                              ROLE TYPE      ROLE ARN
OPENSHIFT VERSION  AWS Managed
ManagedOpenShift-HCP-ROSA-Installer-Role  Installer      arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-HCP-ROSA-Installer-Role  4.16
Yes
ManagedOpenShift-HCP-ROSA-Support-Role    Support        arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-HCP-ROSA-Support-Role    4.16
Yes
ManagedOpenShift-HCP-ROSA-Worker-Role     Worker         arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-HCP-ROSA-Worker-Role     4.16
Yes
```

   b. 删除集群范围的角色：

```
$ 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。

   重要

   帐户范围的 IAM 角色可供同一 AWS 帐户中的其他 ROSA 集群使用。只有角色不再被其他集群需要时，才删除这些资源。

   输出示例

```
W: There are no classic account roles to be deleted
I: Deleting hosted CP account roles
? Delete the account role 'delete-rosa-HCP-ROSA-Installer-Role'? Yes
I: Deleting account role 'delete-rosa-HCP-ROSA-Installer-Role'
? Delete the account role 'delete-rosa-HCP-ROSA-Support-Role'? Yes
I: Deleting account role 'delete-rosa-HCP-ROSA-Support-Role'
? Delete the account role 'delete-rosa-HCP-ROSA-Worker-Role'? Yes
I: Deleting account role 'delete-rosa-HCP-ROSA-Worker-Role'
I: Successfully deleted the hosted CP account roles
```

2. 删除集群范围的 in-line 和 Operator 策略：

a. 在 AWS IAM Console 的 Policies 页面中，根据您在创建集群范围的角色和策略时指定的前缀过滤策略列表。

注意

如果您在创建集群范围的角色时没有指定自定义前缀，请搜索默认前缀 ManagedOpenShift。

b. 使用 AWS IAM 控制台删除集群范围的 in-line 策略和 Operator 策略。有关使用 AWS IAM 控制台删除 IAM 策略的更多信息，请参阅 AWS 文档中的删除 IAM 策略。

重要

帐户范围的 in-line 和 Operator IAM 策略可能被同一 AWS 帐户中的 HCP 使用其他 ROSA。只有角色不再被其他集群需要时，才删除这些资源。

其他资源

- 关于使用 STS 的 ROSA 集群的 IAM 资源

7.2.2. 取消链接和删除 OpenShift Cluster Manager 和用户 IAM 角色

当使用 Red Hat OpenShift Cluster Manager 安装带有 HCP 集群的 ROSA 时，您还可以创建 OpenShift Cluster Manager 和用户 Identity and Access Management (IAM)角色来链接到您的红帽机构。删除集群后，您可以使用 ROSA CLI (rosa) 取消链接和删除角色。

重要

如果要使用 OpenShift Cluster Manager 在同一个 AWS 帐户中使用 HCP 安装和管理其他 ROSA，则需要 OpenShift Cluster Manager 和用户 IAM 角色。只有在不再使用 OpenShift Cluster Manager 来安装使用 HCP 集群的 ROSA 时，才删除角色。

先决条件

- 您创建了 OpenShift Cluster Manager 和用户 IAM 角色，并将其链接到您的红帽机构。
- 您已在安装主机上安装并配置了最新的 ROSA CLI (rosa)。
- 在 Red Hat 机构中具有机构管理员特权。

流程

1. 从红帽机构取消链接 OpenShift Cluster Manager IAM 角色并删除角色：

   a. 列出 AWS 帐户中的 OpenShift Cluster Manager IAM 角色：

```
$ rosa list ocm-roles
```

输出示例

```
I: Fetching ocm roles
ROLE NAME                                          ROLE ARN
LINKED  ADMIN  AWS Managed
ManagedOpenShift-OCM-Role-<red_hat_organization_external_id>  arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-OCM-Role-
<red_hat_organization_external_id>  Yes      Yes     Yes
```

b.

如果您的 OpenShift Cluster Manager IAM 角色在上一命令的输出中被列为链接，请运行以下命令来取消链接红帽机构中的角色：

```
$ rosa unlink ocm-role --role-arn <arn> 1
```

1

将 <arn > 替换为您的 OpenShift Cluster Manager IAM 角色的 Amazon 资源名称(ARN)。ARN 在上一命令的输出中指定。在上例中，ARN 的格式为 arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-<red_hat_organization_external_id >。

输出示例

```
I: Unlinking OCM role
? Unlink the 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-<red_hat_organization_external_id>' role from organization '<red_hat_organization_id>'? Yes
I: Successfully unlinked role-arn 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-<red_hat_organization_external_id>' from organization account '<red_hat_organization_id>'
```

c.

删除 OpenShift Cluster Manager IAM 角色和策略：

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

输出示例

```
I: Deleting OCM role
? OCM Role ARN: arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-<red_hat_organization_external_id>
? Delete 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-OCM-Role-<red_hat_organization_external_id>' ocm role? Yes
? OCM role deletion mode: auto 1
I: Successfully deleted the OCM role
```

1

指定删除模式。您可以使用 auto 模式自动删除 OpenShift Cluster Manager IAM 角色和策略。在手动模式中，ROSA CLI 生成删除角色和策略所需的 aws 命令。manual 模式允许您在手动运行 aws 命令前查看详情。

2. 从您的红帽机构中取消链接用户 IAM 角色并删除角色：

a. 列出 AWS 帐户中的用户 IAM 角色：

```
$ rosa list user-roles
```

输出示例

```
I: Fetching user roles
ROLE NAME                          ROLE ARN
LINKED
ManagedOpenShift-User-<ocm_user_name>-Role  arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-User-<ocm_user_name>-Role  Yes
```

b. 如果您的用户 IAM 角色在上一命令的输出中被列为链接，请取消链接您的红帽机构中的角色：

```
$ rosa unlink user-role --role-arn <arn> 1
```

1

将 <arn > 替换为您的用户 IAM 角色的 Amazon 资源名称(ARN)。ARN 在上一命令的输出中指定。在上例中，ARN 格式为 arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-<ocm_user_name>-Role。

输出示例

-

```
I: Unlinking user role
? Unlink the 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-<ocm_user_name>-Role' role from the current account '<ocm_user_account_id>'? Yes
I: Successfully unlinked role ARN 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-<ocm_user_name>-Role' from account '<ocm_user_account_id>'
```

c. 删除用户 IAM 角色：

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

输出示例

```
I: Deleting user role
? User Role ARN: arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-<ocm_user_name>-Role
? Delete the 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-<ocm_user_name>-Role' role from the AWS account? Yes
? User role deletion mode: auto (1)
I: Successfully deleted the user role
```

(1) 指定删除模式。您可以使用 auto 模式自动删除用户 IAM 角色。在手动模式中，ROSA CLI 生成删除角色所需的 aws 命令。manual 模式允许您在手动运行 aws 命令前查看详情。