Red Hat OpenShift Service on AWS 4

安装 ROSA Classic 集群

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

Last Updated: 2024-06-28

Red Hat OpenShift Service on AWS 4 安装 ROSA Classic 集群

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 AWS (ROSA) 集群上安装 Red Hat OpenShift Service 的信息。本文档还详细介绍了如何访问集群、配置身份提供程序、撤销集群访问和删除集群。

目录

第 1 章 使用默认选项创建带有 STS 的 ROSA 集群

注意

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

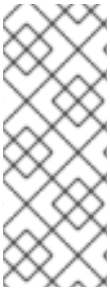
使用默认选项和自动 AWS Identity and Access Management (IAM)资源创建，快速创建 Red Hat OpenShift Service on AWS (ROSA) 集群。您可以使用 Red Hat OpenShift Cluster Manager 或 ROSA CLI (**rosa**)部署集群。

本文档中的步骤通过 ROSA CLI (**rosa**) 和 OpenShift Cluster Manager 中的 **auto** 模式，使用当前的 AWS 帐户创建所需的 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。有关 **使用手动模式** 或自定义自定义部署 ROSA 集群的步骤， 请参阅使用自定义创建集群。

后续步骤

- 确保您已完成 AWS 的先决条件。



注意

ROSA CLI 1.2.7 引入了对新集群的 OIDC 供应商端点 URL 格式的更改。Red Hat OpenShift Service on AWS 集群 OIDC 供应商 URL 不再是区域。AWS CloudFront 实现改进了访问速度和弹性，并缩短延迟。

因为这个更改仅适用于使用 ROSA CLI 1.2.7 或更高版本创建的新集群，所以现有的 OIDC-provider 配置没有任何支持的迁移路径。

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 Red Hat OpenShift Service on AWS (ROSA)集群。以下概述描述了默认集群规格。

表 1.1. 使用 STS 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

组件	默认规格
集群设置	• 默认集群版本： Latest • 使用 Red Hat OpenShift Cluster Manager Hybrid Cloud Console 的安装的默认 AWS 区域：us-east-1 (US East, North Virginia) • 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
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 • 没有额外的节点标签
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 • 节点排空 1 小时宽限期

1.2. 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。您可以通过创建和链接以下 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。

您可以使用 OpenShift Cluster Manager 角色的管理权限来快速部署集群。

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。

其他资源

- 有关创建并链接 OpenShift Cluster Manager 和用户 IAM 角色的详细信息，请参阅将 AWS 帐户与红帽机构 关联。

1.3. 非PRIVATELINK ROSA 集群的 AMAZON VPC 要求

要创建 Amazon VPC，您必须有以下内容：

- 互联网网关，

- NAT 网关，
- 提供互联网连接的私有和公共子网来安装所需组件。

对于 Single-AZ 集群，必须至少有一个私有和公共子网，并且需要至少三个私有和公共子网用于 Multi-AZ 集群。

其他资源

- 有关 AWS 集群所需的默认组件的更多信息，请参阅 AWS 文档中的 Default VPCs。
- 有关在 AWS 控制台中创建 VPC 的说明，请参阅 AWS 文档中的 创建 VPC。

1.4. 使用 OPENSHIFT CLUSTER MANAGER 快速创建集群

当使用 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。

在使用 OpenShift Cluster Manager 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。

1.4.1. 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。

前提条件

- 您为使用 STS 的 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**)。

注意

要成功安装 ROSA 集群，请使用 ROSA CLI 的最新版本。

- 已使用 ROSA CLI 登录到您的红帽帐户。
- 在 Red Hat 机构中具有机构管理员特权。

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 Hybrid Cloud Console 启用特定于集群 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 **Accounts and roles** 步骤中选择 *Admin OCM role* 命令将管理特权应用到角色。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 Hybrid Cloud Console 中创建 ROSA 集群的 **Accounts and roles** 步骤中选择了 *Basic OCM role* 命令，则必须使用手动模式部署 ROSA 集群。系统将提示您在后续步骤中配置特定于集群的 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。

1.4.2. 创建集群范围的 STS 角色和策略

在使用 Red Hat OpenShift Cluster Manager Hybrid Cloud Console 创建使用 AWS 安全令牌服务(STS)的 Red Hat OpenShift Service on AWS (ROSA)集群前，创建所需的帐户范围的 STS 角色和策略，包括 Operator 策略。

先决条件

- 您为使用 STS 的 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。

流程

1. 检查 AWS 帐户是否有现有的角色和策略：

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

2. 如果您的 AWS 帐户中不存在它们，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。

1.4.3. 创建 OpenID 连接配置

当在 AWS 集群上使用 Red Hat OpenShift Service 时，您可以在创建集群时创建 OpenID Connect (OIDC)配置。此配置已注册到 OpenShift Cluster Manager。

前提条件

- 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. 要将 OIDC 配置与 AWS 资源一同创建，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
```

1.4.4. 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 角色启用自动部署特定于集群的 Operator 角色和 OpenID Connect (OIDC)供应商。

前提条件

- 您为使用 STS 的 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。
- 已确认 AWS 帐户中存在 AWS Elastic Load Balancing (ELB)服务角色。
- 您已将 AWS 帐户与红帽机构相关联。在帐户关联时，您可以将管理权限应用到 OpenShift Cluster Manager 角色。有关详细步骤，*请参阅将 AWS 帐户与您的红帽机构* 关联。
- 您已创建了所需的集群范围的 STS 角色和策略。具体步骤请参阅 *创建集群范围的 STS 角色和策略*。

流程

1. 导航到 OpenShift Cluster Manager 并选择 **Create cluster**。
2. 在 **Create a OpenShift cluster** 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集群范围的 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*。

1.5. 使用 CLI 快速创建集群

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

前提条件

- 您为使用 STS 的 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。
- 已确认 AWS 帐户中存在 AWS Elastic Load Balancing (ELB)服务角色。

流程

1. 创建所需的集群范围的角色和策略，包括 Operator 策略：

```
$ rosa create account-roles --mode auto
```

注意

使用 **auto** 模式时，您可以选择指定 **-y** 参数来绕过交互式提示并自动确认操作。

2. 使用默认值创建带有 STS 的集群。使用默认值时，会安装最新的稳定 OpenShift 版本：

```
$ rosa create cluster --cluster-name <cluster_name> \ 1
--sts --mode auto 2
```

1 将 **<cluster_name>** 替换为集群的名称。

2 当您指定 **--mode auto** 时，**rosa create cluster** 命令会自动创建特定于集群的 Operator IAM 角色和 OIDC 供应商。Operator 使用 OIDC 供应商进行身份验证。

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**。

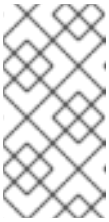
要自定义子域，请使用 **--domain-prefix** 标志。域前缀不能超过 15 个字符，它必须是唯一的，且在集群创建后无法更改。

3. 检查集群的状态：

```
$ rosa describe cluster --cluster <cluster_name|cluster_id>
```

在集群安装过程中，输出中会列出以下 **State** 字段更改：

- **等待（等待 OIDC 配置）**
- **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** 字段在大约 40 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*。

4. 通过观察 OpenShift 安装程序日志来跟踪集群创建的进度：

```
$ rosa logs install --cluster <cluster_name|cluster_id> --watch 1
```

1 指定在安装过程中监视新日志消息的 **--watch** 标志。这个参数是可选的。

1.6. 后续步骤

- 访问 ROSA 集群
- 添加通知联系人

1.7. 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 在 AWS 上部署 Red Hat OpenShift Service 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 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 Red Hat OpenShift Service on AWS 的支持。

第 2 章 使用自定义创建带有 STS 的 ROSA 集群

使用自定义，使用 AWS 安全令牌服务(STS)创建 Red Hat OpenShift Service on AWS (ROSA)集群。您可以使用 Red Hat OpenShift Cluster Manager 或 ROSA CLI (**rosa**)部署集群。

使用本文档中的步骤，在创建所需的 AWS Identity and Access Management (IAM)资源时，您还可以选择 **auto** 和 **manual** 模式。

2.1. 了解自动和手动部署模式

当使用 AWS 安全令牌服务 (STS) 在 AWS (ROSA) 集群中安装 Red Hat OpenShift Service 时，您可以选择 **auto** 和 **manual** 模式来创建所需的 AWS Identity and Access Management (IAM)资源。

自动 模式

使用这个模式，ROSA CLI (**rosa**)会立即创建所需的 IAM 角色和策略，以及 AWS 帐户中的 OpenID Connect (OIDC)供应商。

manual 模式

在这个版本中，**rosa** 输出创建 IAM 资源所需的 **aws** 命令。对应的策略 JSON 文件也保存到当前目录中。通过 **使用手动模式**，您可以在手动运行前查看生成的 **aws** 命令。**手动模式** 还允许您将命令传递给机构中的另一个管理员或组，以便他们可以创建资源。

重要

如果选择 **使用手动模式**，集群安装会等待，直到手动创建特定于集群的 Operator 角色和 OIDC 供应商。创建资源后，安装将继续。如需更多信息，*请参阅使用 OpenShift Cluster Manager 创建 Operator 角色和 OIDC 供应商*。

有关使用 STS 安装 ROSA 所需的 AWS IAM 资源的更多信息，*请参阅关于使用 STS 的集群的 IAM 资源*。

2.1.1. 使用 OpenShift Cluster Manager 创建 Operator 角色和 OIDC 供应商

如果使用 Red Hat OpenShift Cluster Manager 安装集群并选择使用手动模式创建所需的 AWS IAM Operator 角色和 OIDC 供应商，则会提示您输入以下安装方法之一来安装资源。允许您选择适合您的机构需求的资源创建方法：

AWS CLI (aws)

使用此方法，您可以下载并提取包含创建 IAM 资源所需的 **aws** 命令和策略文件的存档文件。从包含策略文件的目录运行提供的 CLI 命令，以创建 Operator 角色和 OIDC 供应商。

Red Hat OpenShift Service on AWS (ROSA) CLI,rosa

您可以运行此方法提供的命令，以使用 **rosa** 为集群创建 Operator 角色和 OIDC 供应商。

如果使用 **auto** 模式，OpenShift Cluster Manager 会自动创建 Operator 角色和 OIDC 供应商，使用 OpenShift Cluster Manager IAM 角色提供的权限。要使用此功能，您必须将 admin 权限应用到该角色。

2.2. 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。您可以通过创建和链接以下 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。

您可以使用 OpenShift Cluster Manager 角色的管理权限来快速部署集群。

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。

其他资源

- 有关创建并链接 OpenShift Cluster Manager 和用户 IAM 角色的详细步骤，请参阅使用 OpenShift Cluster Manager 使用自定义创建集群。

2.3. IAM 角色和策略的 ARN 路径自定义

当您创建使用 AWS 安全令牌服务(STS)的 Red Hat OpenShift Service on AWS (ROSA)集群上所需的 AWS IAM 角色和策略时，您可以指定自定义 Amazon Resource Name (ARN)路径。这可让您使用满足机构安全要求的角色和策略 ARN 路径。

在创建 OCM 角色、用户角色以及帐户范围内的角色和策略时，您可以指定自定义 ARN 路径。

如果您在创建一组集群范围的角色和策略时定义了自定义 ARN 路径，则相同的路径将应用到集合中的所有角色和策略。以下示例显示了一组集群范围的角色和策略的 ARN。在示例中，ARN 使用自定义路径 **/test/path/dev/** 和自定义角色前缀 **test-env** ：

- **arn:aws:iam::<account_id>:role/test/path/dev/test-env-Worker-Role**
- **arn:aws:iam::<account_id>:role/test/path/dev/test-env-Support-Role**
- **arn:aws:iam::<account_id>:role/test/path/dev/test-env-Installer-Role**
- **arn:aws:iam::<account_id>:role/test/path/dev/test-env-ControlPlane-Role**
- **arn:aws:iam::<account_id>:policy/test/path/dev/test-env-Worker-Role-Policy**
- **arn:aws:iam::<account_id>:policy/test/path/dev/test-env-Support-Role-Policy**
- **arn:aws:iam::<account_id>:policy/test/path/dev/test-env-Installer-Role-Policy**
- **arn:aws:iam::<account_id>:policy/test/path/dev/test-env-ControlPlane-Role-Policy**

在创建特定于集群的 Operator 角色时，相关集群范围的安装程序角色的 ARN 路径会自动检测到并应用 Operator 角色。

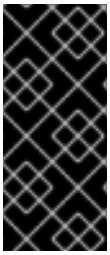
有关 ARN 路径的更多信息，请参阅 AWS 文档中的 Amazon 资源名称(ARN)。

其他资源

- 有关在 AWS 集群上创建 Red Hat OpenShift Service 时为 IAM 资源指定自定义 ARN 路径的步骤，请参阅使用自定义创建集群。

2.4. 支持使用 STS 的 ROSA 集群的注意事项

创建使用 AWS 安全令牌服务(STS)的 Red Hat OpenShift Service on AWS (ROSA)集群的支持方法是使用本文档中介绍的步骤。



重要

您可以将 **手动模式** 与 ROSA CLI (**rosa**)搭配使用来生成 AWS Identity and Access Management (IAM)策略文件和 **aws** 命令，用于安装 STS 资源所需的 aws 命令。

生成的文件和 **aws** 命令仅用于查看目的，不要对它们进行任何修改。红帽无法为使用策略文件或 **aws** 命令的修改版本部署的 ROSA 集群提供支持。

2.5. 非PRIVATELINK ROSA 集群的 AMAZON VPC 要求

要创建 Amazon VPC，您必须有以下内容：

- 互联网网关，
- NAT 网关，
- 提供互联网连接的私有和公共子网来安装所需组件。

对于 Single-AZ 集群，必须至少有一个私有和公共子网，并且需要至少三个私有和公共子网用于 Multi-AZ 集群。

其他资源

- 有关 AWS 集群所需的默认组件的更多信息，请参阅 AWS 文档中的 Default VPCs。
- 有关在 AWS 控制台中创建 VPC 的说明，请参阅 AWS 文档中的 创建 VPC。

2.6. 创建 OPENID 连接配置

当在 AWS 集群上使用 Red Hat OpenShift Service 时，您可以在创建集群时创建 OpenID Connect (OIDC)配置。此配置已注册到 OpenShift Cluster Manager。

前提条件

- 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. 要将 OIDC 配置与 AWS 资源一同创建，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
```

2.7. 使用自定义创建集群

使用符合您的环境需求的配置，在 AWS (ROSA) 上部署带有 AWS 安全令牌服务 (STS) 集群的 Red Hat OpenShift Service。您可以使用 Red Hat OpenShift Cluster Manager 或 ROSA CLI (**rosa**)使用自定义部署集群。

2.7.1. 使用 OpenShift Cluster Manager 使用自定义创建集群

当您创建使用 AWS 安全令牌服务 (STS) 的 Red Hat OpenShift Service on AWS (ROSA) 集群时，您可以使用 Red Hat OpenShift Cluster Manager 以交互自定义安装。

重要

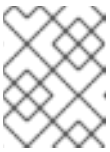
STS 仅支持公共和 AWS PrivateLink 集群。常规私有集群（非PrivateLink）无法用于 STS。

前提条件

- 您为使用 STS 的 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。
- 已确认 AWS 帐户中存在 AWS Elastic Load Balancing (ELB)服务角色。
- 如果要配置集群范围代理，请验证可以从安装集群的 VPC 访问代理。该代理还必须从 VPC 的专用子网访问。

流程

1. 导航到 OpenShift Cluster Manager 并选择 **Create cluster**。
2. 在 **Create a OpenShift cluster** 页面中，在 **Red Hat OpenShift Service on AWS (ROSA)**行中选择 **Create cluster**。
3. 如果自动检测到 AWS 帐户，帐户 ID 会在 **关联的 AWS 帐户** 下拉菜单中列出。如果没有自动检测到 AWS 帐户，点 **Select a account → associated AWS account** 并按照以下步骤操作：
   a. 在 **Authenticate** 页面上，单击 **rosa login** 命令旁边的复制按钮。命令包括您的 OpenShift Cluster Manager API 登录令牌。



注意

您还可以在 OpenShift Cluster Manager 上的 OpenShift Cluster Manager API Token 页面中加载 API 令牌。

   b. 在 CLI 中运行复制的命令以登录到您的 ROSA 帐户。

```
$ rosa login --token=<api_login_token> (1)
```

(1) 将 **<api_login_token** > 替换为复制命令中提供的令牌。

输出示例

```
I: Logged in as '<username>' on 'https://api.openshift.com'
```

   c. 在 OpenShift Cluster Manager 中的 **Authenticate** 页面上，单击 **Next**。

d. 在 **OCM 角色**页面中，点 **Basic OCM role** 或 **Admin OCM role** 命令旁边的复制按钮。基本角色可让 OpenShift Cluster Manager 检测 ROSA 所需的 AWS IAM 角色和策略。admin 角色还启用角色和策略的检测。另外，admin 角色允许使用 OpenShift Cluster Manager 自动部署特定于集群 Operator 角色和 OpenID Connect (OIDC) 供应商。

e. 在 CLI 中运行复制的命令，并按照提示创建 OpenShift Cluster Manager IAM 角色。以下示例使用默认选项创建基本 OpenShift Cluster Manager IAM 角色：

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

输出示例

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

1. 指定要在 OCM IAM 角色名称中包含的前缀。默认值为 **ManagedOpenShift**。您只能为每个 AWS 帐户为 Red Hat 机构创建一个 OCM 角色。

2. 启用 admin OpenShift Cluster Manager IAM 角色，该角色等同于指定 **--admin** 参数。如果要使用 **Auto** 模式使用 OpenShift Cluster Manager 自动置备特定于集群的 Operator 角色和 OIDC 供应商，则需要 admin 角色。

3. 可选：为角色指定一个权限边界 Amazon Resource Name (ARN)。如需更多信息，请参阅 AWS 文档中的 IAM 实体的权限边界。

4. 为您的 OCM 角色指定自定义 ARN 路径。该路径必须仅包含字母数字字符，并以 / 开头和结尾，例如 **/test/path/dev/**。如需更多信息，请参阅 *IAM 角色和策略的 ARN 路径自定义*。

5. 选择角色创建模式。您可以使用 **auto** 模式自动创建 OpenShift Cluster Manager IAM 角色，并将其链接到您的红帽机构帐户。**在手动模式中**，ROSA CLI 生成创建和链接角色所需的 **aws** 命令。**在手动模式中**，对应的策略 JSON 文件也保存到当前目录中。**manual** 模式允许您在手动运行 **aws** 命令前查看详情。

6. 将 OpenShift Cluster Manager IAM 角色链接到您的红帽机构帐户。

f. 如果您不选择将 OpenShift Cluster Manager IAM 角色链接到上一命令中的红帽机构帐户，请从 OpenShift Cluster Manager **OCM 角色** 页面中复制 **rosa link** 命令并运行它：

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

1 将 **<arn>** 替换为上一命令输出中包含的 OpenShift Cluster Manager IAM 角色的 ARN。

g. 在 OpenShift Cluster Manager **OCM 角色** 页面中选择 **Next**。

h. 在 **User role** 页面上，点 **User role** 命令的复制按钮，并在 CLI 中运行命令。在使用 OpenShift Cluster Manager 安装集群和所需资源时，红帽使用用户角色来验证 AWS 身份。按照提示创建用户角色：

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

输出示例

```
I: Creating User role
? Role prefix: ManagedOpenShift 1
? Permissions boundary ARN (optional): 2
? Role Path (optional): [? for help] 3
? Role creation mode: auto 4
I: Creating ocm user role using 'arn:aws:iam::<aws_account_id>:user/<aws_username>'
? Create the 'ManagedOpenShift-User-<red_hat_username>-Role' role? Yes
I: Created role 'ManagedOpenShift-User-<red_hat_username>-Role' with ARN
'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-<red_hat_username>-
Role'
I: Linking User role
? User Role ARN: arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-
<red_hat_username>-Role
? Link the 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-User-
<red_hat_username>-Role' role with account '<red_hat_user_account_id>'? Yes 5
I: Successfully linked role ARN 'arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-
User-<red_hat_username>-Role' with account '<red_hat_user_account_id>'
```

1 指定要在用户角色名称中包含的前缀。默认值为 **ManagedOpenShift**。

2 可选：为角色指定一个权限边界 Amazon Resource Name (ARN)。如需更多信息，请参阅 AWS 文档中的 IAM 实体的权限边界。

3 为您的用户角色指定自定义 ARN 路径。该路径必须仅包含字母数字字符，并以 / 开头和结尾，例如 **/test/path/dev/**。如需更多信息，请参阅 *IAM 角色和策略的 ARN 路径自定义*。

4 选择角色创建模式。您可以使用 **auto** 模式自动创建用户角色并将其链接到 OpenShift Cluster Manager 用户帐户。**在手动模式中**，ROSA CLI 生成创建和链接角色所需的 **aws** 命令。**在手动模式中**，对应的策略 JSON 文件也保存到当前目录中。**manual** 模式允许您在手动运行 **aws** 命令前查看详情。

5 将用户角色链接到 OpenShift Cluster Manager 用户帐户。

i. 如果您没有将用户角色链接到上一命令中的 OpenShift Cluster Manager 用户帐户，请从 OpenShift Cluster Manager **User role** 页面中复制 **rosa link** 命令并运行它：

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

1 将 < **arn** > 替换为上一命令输出中包含的用户角色的 ARN。

j. 在 OpenShift Cluster Manager **User role** 页面上，单击 **Ok**。

k. 验证 AWS 帐户 ID 是否列在 **Accounts and roles** 页面的关联 **AWS** 帐户下拉菜单中。

l. 如果所需的帐户角色不存在，则会提供一个通知，表示**有些帐户角色 ARN 没有被检测到**。您可以通过点击 **rosa create account-roles** 命令旁边的复制缓冲区并在 CLI 中运行命令，创建 AWS 帐户范围的角色和策略，包括 Operator 策略：

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

输出示例

```
I: Logged in as '<red_hat_username>' on 'https://api.openshift.com'
I: Validating AWS credentials...
I: AWS credentials are valid!
I: Validating AWS quota...
I: AWS quota ok. If cluster installation fails, validate actual AWS resource usage against
https://docs.openshift.com/rosa/rosa_getting_started/rosa-required-aws-service-
quotas.html
I: Verifying whether OpenShift command-line tool is available...
I: Current OpenShift Client Version: 4.0
I: Creating account roles
? Role prefix: ManagedOpenShift 1
? Permissions boundary ARN (optional): 2
? Path (optional): [? for help] 3
? Role creation mode: auto 4
I: Creating roles using 'arn:aws:iam::<aws_account_number>:user/<aws_username>'
? Create the 'ManagedOpenShift-Installer-Role' role? Yes 5
I: Created role 'ManagedOpenShift-Installer-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Installer-Role'
? Create the 'ManagedOpenShift-ControlPlane-Role' role? Yes 6
I: Created role 'ManagedOpenShift-ControlPlane-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-ControlPlane-Role'
? Create the 'ManagedOpenShift-Worker-Role' role? Yes 7
I: Created role 'ManagedOpenShift-Worker-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Worker-Role'
? Create the 'ManagedOpenShift-Support-Role' role? Yes 8
I: Created role 'ManagedOpenShift-Support-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Support-Role'
I: To create a cluster with these roles, run the following command:
rosa create cluster --sts
```

1 指定要在 OpenShift Cluster Manager IAM 角色名称中包含的前缀。默认值为 **ManagedOpenShift**。

重要

您必须指定一个在 AWS 帐户之间是唯一的集群范围的角色前缀，即使您为帐户角色使用自定义 ARN 路径。

2 可选：为角色指定一个权限边界 Amazon Resource Name (ARN)。如需更多信息，请参阅 AWS 文档中的 IAM 实体的权限边界。

3 为您的集群范围的角色指定自定义 ARN 路径。该路径必须仅包含字母数字字符，并以 / 开头和结尾，例如 **/test/path/dev/**。如需更多信息，请参阅 *IAM 角色和策略的 ARN 路径自定义*。

4 选择角色创建模式。您可以使用 **auto** 模式自动创建帐户范围内的角色和策略。**在手动模式中**，ROSA CLI 生成创建角色和策略所需的 **aws** 命令。**在手动模式中**，对应的策略 JSON 文件也保存到当前目录中。**manual** 模式允许您在手动运行 **aws** 命令前查看详情。

5 6 7 8 创建集群范围的安装程序、control plane、worker 和支持角色以及对应的 IAM 策略。如需更多信息，请参阅 *帐户范围的 IAM 角色和策略参考*。

注意

在此步骤中，ROSA CLI 还会自动创建特定于集群 Operator 策略的帐户范围的 Operator IAM 策略，以允许 ROSA 集群 Operator 执行核心 OpenShift 功能。如需更多信息，请参阅 *帐户范围的 IAM 角色和策略参考*。

m. 在 **Accounts and roles** 页面中，点 **Refresh ARNs** 并验证是否列出了安装程序、支持、worker 和 control plane 帐户角色 ARN。
如果您的集群版本的 AWS 帐户中有多个帐户角色，则会提供一个 **安装程序角色** ARN 的下拉列表。选择您要用于集群的安装程序角色的 ARN。集群使用与所选安装程序角色相关的集群范围的角色和策略。

4. 点击 **Next**。

注意

如果更改了 **Accounts and roles** 页面，您可能需要再次选择复选框，以确认您已读取并完成所有先决条件。

5. 在 **Cluster details** 页面中，为集群提供一个名称并指定集群详情：

a. 添加**集群名称**。

b. 可选：集群创建会生成域前缀，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给 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。域前缀不能超过 15 个字符，在您的机构内必须是唯一的，且在集群创建后无法更改。

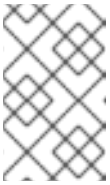
c. 从 **Version** 下拉菜单中选择集群版本。

d. 从 **Region** 下拉菜单中选择云供应商区域。

e. 选择 **Single zone** 或 **Multi-zone** 配置。

f. 选择 **Enable user workload monitoring** 以监控您自己的项目，使其与 Red Hat Site Reliability 工程师(SRE)平台指标隔离。默认启用这个选项。

g. 可选：如果您需要 etcd 键值加密，请选择 **Enable additional etcd encryption**。使用此选项时，etcd 键的值被加密，而不是键本身。这个选项除了 control plane 存储加密外，它默认加密 Red Hat OpenShift Service on AWS 集群中的 etcd 卷。



注意

通过在 etcd 中为密钥值启用 etcd 加密，则会出现大约 20% 的性能开销。除了加密 etcd 卷的默认 control plane 存储加密外，还会引入第二层加密的开销。只有在特别需要时才考虑启用 etcd 加密。

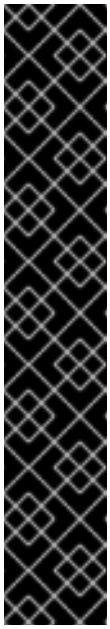
h. 可选：如果要提供自己的 AWS 密钥管理服务(KMS) 密钥 Amazon 资源名称(ARN)，请选择 **Encrypt persistent volumes with customer key**。用于加密集群中的持久性卷的密钥。

重要

默认情况下，仅加密从默认存储类创建的持久性卷 (PV)。

只有在将存储类配置为加密时，使用其他存储类创建的 PV 才会被加密。

i. 可选。要创建客户管理的 KMS 密钥，请按照创建对称加密 KMS 密钥的步骤进行操作。



重要

除了成功创建集群的帐户角色外，还需要 EBS Operator 角色。

此角色必须附加到 **ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials** 策略，这是 ROSA 所需的 IAM 策略，以通过 Container Storage Interface (CSI)管理后端存储。

有关集群 Operator 所需的策略和权限的更多信息，请参阅 *集群范围的角色创建方法*。

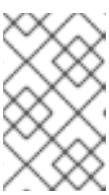
EBS Operator 角色示例

"ARN:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-ebs-cloud-credent"

创建 Operator 角色后，您必须在 AWS 控制台的**Key Management Service (KMS)** 页面中 编辑 *Key Policy* 以添加角色。

j. 点击 **Next**。

6. 在 **Default machine pool** 页面中，选择一个 **Compute 节点实例类型**。



注意

创建集群后，您可以更改集群中的计算节点数量，但您无法更改默认机器池中的计算节点实例类型。您可用的节点数量和类型取决于您是否使用单一或者多个可用区。它们还取决于您 AWS 帐户和所选区域中的启用和可用的内容。

7. 可选：为默认机器池配置自动扩展：

   a. 选择 **Enable autoscaling** 以自动扩展默认机器池中的机器数量，以满足部署需求。

   b. 设置自动扩展的最小和最大节点数限值。集群自动扩展不会减少或增加默认的机器池节点数超过您指定的限制。

      - 如果您使用一个可用区部署集群，请设置**最小节点数**和**最大节点数**。这会在可用区中定义最小和最大计算节点限值。
      - 如果您使用多个可用区部署集群，请为每个区设置 **Minimum nodes per zone** 和 **Maximum nodes per zone**。它定义每个区的最小和最大计算节点限值。

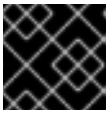
注意

另外，您可以在创建机器池后为默认机器池设置自动扩展首选项。

8. 如果没有启用自动扩展，请为默认机器池选择计算节点计数：

   - 如果您使用一个可用区部署集群，请从下拉菜单中选择 **Compute 节点数**。这定义了置备到区域的机器池的计算节点数量。
   - 如果您使用多个可用区部署集群，请从下拉菜单中选择 **Compute 节点数（每个区）**。这定义了每个区要置备到机器池的计算节点数量。

9. 可选： 选择 EC2 实例元数据服务(IMDS)配置 - **可选** （默认）或 **必需** - 来强制使用 IMDSv2。有关 IMDS 的更多信息，请参阅 AWS 文档中的实例元数据和用户数据。



重要

在集群创建后无法更改实例元数据服务设置。

10. 可选：展开 **标记节点标签**，为节点添加标签。点 **Add label** 来添加更多节点标签并选择 **Next**。

11. 在网络 **配置**页面 的集群 **隐私** 部分中，选择 **Public** 或 **Private** 来使用集群的公共或私有 API 端点和应用程序路由。

重要

在集群创建后，无法在公共和私有之间更改 API 端点。

公共 API 端点

如果您不想限制对集群的访问，请选择 **Public**。您可以从互联网访问 Kubernetes API 端点和应用程序路由。

私有 API 端点

如果要限制集群的网络访问，请选择 **Private**。Kubernetes API 端点和应用程序路由只能从直接连接访问。

重要

如果使用私有 API 端点，则在更新云供应商帐户中的网络设置之前，您无法访问集群。

12. 可选：如果您选择使用公共 API 端点，则默认为集群创建新的 VPC。如果要在现有 VPC 中安装集群，请选择 **Install into an existing VPC**。

警告

您无法将 ROSA 集群安装到 OpenShift 安装程序创建的现有 VPC 中。这些 VPC 在集群部署期间创建，且必须只与单个集群关联，以确保集群置备和删除操作正常工作。

要验证 OpenShift 安装程序是否已创建 VPC，请检查 **kubernetes.io/cluster/<infra-id>** 标签上的 **owned** 值。例如，当查看名为 **mycluster-12abc-34def** 的 VPC 标签时，**kubernetes.io/cluster/mycluster-12abc-34def** 标签的值为 **owned**。因此，VPC 由安装程序创建的，不得由管理员修改。

注意

如果选择使用私有 API 端点，则必须使用现有的 VPC 和 PrivateLink，**Install into an existing VPC** 和 **Use a PrivateLink** 选项会被自动选择。使用这些选项，Red Hat Site Reliability Engineering (SRE)团队可以连接到集群，以帮助只使用 AWS PrivateLink 端点。

13. 可选： 如果要将集群安装到现有的 VPC 中，请选择**配置集群范围代理** 来启用 HTTP 或 HTTPS 代理来拒绝从集群直接访问互联网。

14. 点击 **Next**。

15. 如果您选择在现有 AWS VPC 中安装集群，请提供 **Virtual Private Cloud (VPC)子网设置**。

注意

您必须确保您的 VPC 配置了一个公有和私有子网，以及您要安装到的每个可用区的专用子网。如果您选择使用 PrivateLink，则只需要专用子网。

a. 可选：扩展 **Additional security groups** 并选择额外的自定义安全组，以应用到默认创建的机器池中的节点。您必须已创建了安全组，并将其与您为这个集群选择的 VPC 关联。您无法在创建集群时将安全组添加到默认机器池中。
默认情况下，您指定的安全组将为所有节点类型添加。取消选择 **Apply the same security groups to all node type (control plane, infrastructure and worker)复选框，以为每个节点类型** 选择不同的安全组。

如需更多信息，*请参阅附加资源* 下 *安全组* 的要求。

16. 如果您选择配置集群范围代理，在 **Cluster-wide proxy** 页面中提供代理配置详情：

a. 至少在以下字段之一中输入值：

- 指定有效的 **HTTP 代理 URL**。
- 指定有效的 **HTTPS 代理 URL**。

- 在 **Additional trust bundle** 字段中，提供 PEM 编码 X.509 证书捆绑包。捆绑包添加到集群节点的可信证书存储中。如果您使用 TLS-inspecting 代理，则需要额外的信任捆绑包文件，除非代理的身份证书由 Red Hat Enterprise Linux CoreOS (RHCOS)信任捆绑包的颁发机构签名。无论代理是透明还是需要使用 **http-proxy** 和 **https-proxy** 参数显式配置，这个要求都适用。

b. 点击 **Next**。
有关使用 Red Hat OpenShift Service on AWS 配置代理的更多信息，*请参阅配置集群范围代理*。

17. 在 **CIDR 范围** 对话框中，配置自定义无类别间路由 (CIDR) 范围，或使用提供默认值并点 **Next**。

注意

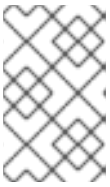
如果您要安装到 VPC 中，**Machine CIDR** 范围必须与 VPC 子网匹配。

重要

稍后无法更改 CIDR 配置。在继续操作前，请联系您的网络管理员选择。

18. 在 **Cluster roles and policies** 页面中，选择您首选的特定于集群的 Operator IAM 角色和 OIDC 供应商创建模式。
使用 **Manual** 模式，您可以使用 **rosa** CLI 命令或 **aws** CLI 命令为集群生成所需的 Operator 角色和 OIDC 供应商。通过**手动**模式，您可以在使用首选选项手动创建 IAM 资源并完成集群安装前查看详情。

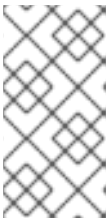
另外，您可以使用 **Auto** 模式自动创建 Operator 角色和 OIDC 供应商。要启用 **Auto** 模式，OpenShift Cluster Manager IAM 角色必须具有管理员权限。



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，则会自动检测自定义路径并将其应用到 Operator 角色。当使用 **Manual** 或 **Auto** 模式创建 Operator 角色时，会应用自定义 ARN 路径。

19. 可选：为特定于集群 Operator IAM 角色指定**自定义 operator 角色前缀**。



注意

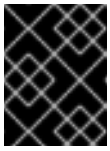
默认情况下，特定于集群的 Operator 角色名称使用集群名称和随机 4 位哈希值作为前缀。您可以选择指定自定义前缀来替换角色名称中的 < **cluster_name>-<hash** >。创建特定于集群的 Operator IAM 角色时会应用前缀。有关前缀的详情，*请参阅关于自定义 Operator IAM 角色前缀*。

20. 选择 **Next**。

21. 在 **Cluster update 策略** 页面中，配置您的更新首选项：

a. 选择集群更新方法：

- 如果要 **单独调度每个更新，请选择单个更新**。这是默认选项。
- 选择 **Recurring updates** 以在更新可用是在您的首先日期、开始时间上更新集群。



重要

即使选择了周期性更新，在次版本间升级集群前，您必须更新帐户和特定于集群的 IAM 资源。

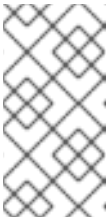
注意

您可以在 Red Hat OpenShift Service on AWS 更新生命周期文档中查看生命周期结束日期。如需更多信息，请参阅 *Red Hat OpenShift Service on AWS 更新生命周期*。

b. 如果您选择重复更新，请从下拉菜单中选择 UTC 中的星期天和升级开始时间。

c. 可选：您可以在集群安装过程中为**节点排空**设置宽限期。默认设置 **1 小时** 宽限期。

d. 点击 **Next**。



注意

如果出现严重影响集群安全性或稳定性的关键安全问题，Red Hat Site Reliability Engineering (SRE)可能会调度自动更新到不受影响的最新 z-stream 版本。在通知客户后，更新会在 48 小时内应用。有关严重影响安全评级的信息，请参阅 了解红帽安全评级。

22. 查看您选择的概述并点 **Create cluster** 启动集群安装。

23. 如果选择使用 **Manual** 模式，请手动创建特定于集群的 Operator 角色和 OIDC 供应商以继续安装：

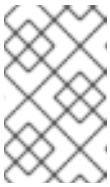
    a. 在 **Action required to continue installation** 对话框中，选择 **AWS CLI** 或 **ROSA CLI** 选项卡并手动创建资源：

    - 如果您选择使用 **AWS CLI** 方法，点 **Download .zip**，保存文件，然后提取 AWS CLI 命令和策略文件。然后，在 CLI 中运行提供的 **aws** 命令。

注意

您必须在包含策略文件的目录中运行 **aws** 命令。

    - 如果您选择使用 **ROSA CLI** 方法，点 **rosa create** 命令旁边的复制按钮，并在 CLI 中运行它们。



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，并在使用这些手动方法创建时应用到 Operator 角色。

    b. 在 **Action required to continue installation** 对话框中，点 **x** 返回到集群的 **Overview** 页。

    c. 验证集群的 **Overview** 页面的 **Details** 部分中的 Cluster **Status** 是否已从 **Waiting** 改为 **Installing**。在状态更改前，可能需要大约两分钟的延迟时间。

注意

如果选择使用 **Auto** 模式，OpenShift Cluster Manager 会自动创建 Operator 角色和 OIDC 供应商。

重要

除了成功创建集群的帐户角色外，还需要 EBS Operator 角色。

此角色必须附加到 **ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials** 策略，这是 ROSA 所需的 IAM 策略，以通过 Container Storage Interface (CSI)管理后端存储。

有关集群 Operator 所需的策略和权限的更多信息，请参阅 *集群范围的角色创建方法*。

EBS Operator 角色示例

"ARN:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-ebs-cloud-credent"

创建 Operator 角色后，您必须在 AWS 控制台的Key Management Service (KMS) 页面中 编辑 *Key Policy* 以添加角色。

验证

- 您可以在集群的 **Overview** 页面中监控安装的进度。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*。

其他资源

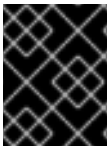
- *使用 ROSA CLI 管理对象中的* 创建集群
- 集群范围的角色创建方法

2.7.2. 使用 CLI 使用自定义创建集群

当您创建使用 AWS 安全令牌服务 (STS) 的 Red Hat OpenShift Service on AWS (ROSA) 集群时，您可以使用交互模式自定义安装。

当在集群创建时运行 **rosa create cluster --interactive** 命令时，您会看到一系列互动提示，供您自定义部署。如需更多信息，请参阅 *交换式集群创建模式参考*。

使用互动模式安装集群后，输出中会提供一个单个命令，供您使用相同的自定义配置部署更多集群。



重要

STS 仅支持公共和 AWS PrivateLink 集群。常规私有集群（非PrivateLink）无法用于 STS。

前提条件

- 您为使用 STS 的 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。
- 如果要使用客户管理的 AWS 密钥管理服务(KMS)密钥进行加密，您必须创建一个对称 KMS 密钥。创建集群时您必须提供 Amazon 资源名称(ARN)。要创建客户管理的 KMS 密钥，请按照创建对称加密 KMS 密钥的步骤进行操作。

重要

除了成功创建集群的帐户角色外，还需要 EBS Operator 角色。

此角色必须附加到 **ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials** 策略，这是 ROSA 所需的 IAM 策略，以通过 Container Storage Interface (CSI)管理后端存储。

有关集群 Operator 所需的策略和权限的更多信息，请参阅 *集群范围的角色创建方法*。

EBS Operator 角色示例

"ARN:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-ebs-cloud-credent"

创建 Operator 角色后，您必须在 AWS 控制台的Key Management Service (KMS) 页面中 编辑 *Key Policy* 以添加角色。

流程

1. 创建所需的集群范围的角色和策略，包括 Operator 策略：
   a. 在当前工作目录中生成 IAM 策略 JSON 文件，并输出 **aws** CLI 命令进行审核：

```
$ rosa create account-roles --interactive \ 1
                            --mode manual 2
```

1 **交互模式** 允许您在互动提示中指定配置选项。如需更多信息，请参阅 *交换式集群创建模式参考*。

2 **手动模式** 生成创建集群范围的角色和策略所需的 **aws** CLI 命令和 JSON 文件。检查后，您必须手动运行命令以创建资源。

输出示例

```
I: Logged in as '<red_hat_username>' on 'https://api.openshift.com'
I: Validating AWS credentials...
I: AWS credentials are valid!
I: Validating AWS quota...
I: AWS quota ok. If cluster installation fails, validate actual AWS resource usage against
https://docs.openshift.com/rosa/rosa_getting_started/rosa-required-aws-service-
quotas.html
I: Verifying whether OpenShift command-line tool is available...
I: Current OpenShift Client Version: 4.0
I: Creating account roles
? Role prefix: ManagedOpenShift 1
? Permissions boundary ARN (optional): 2
? Path (optional): [? for help] 3
? Role creation mode: auto 4
I: Creating roles using 'arn:aws:iam::<aws_account_number>:user/<aws_username>'
? Create the 'ManagedOpenShift-Installer-Role' role? Yes 5
I: Created role 'ManagedOpenShift-Installer-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Installer-Role'
? Create the 'ManagedOpenShift-ControlPlane-Role' role? Yes 6
I: Created role 'ManagedOpenShift-ControlPlane-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-ControlPlane-Role'
? Create the 'ManagedOpenShift-Worker-Role' role? Yes 7
I: Created role 'ManagedOpenShift-Worker-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Worker-Role'
? Create the 'ManagedOpenShift-Support-Role' role? Yes 8
I: Created role 'ManagedOpenShift-Support-Role' with ARN 'arn:aws:iam::
<aws_account_number>:role/ManagedOpenShift-Support-Role'
I: To create a cluster with these roles, run the following command:
rosa create cluster --sts
```

1. 指定要在 OpenShift Cluster Manager IAM 角色名称中包含的前缀。默认值为 **ManagedOpenShift**。

重要

您必须指定一个在 AWS 帐户之间是唯一的集群范围的角色前缀，即使您为帐户角色使用自定义 ARN 路径。

2. 可选：为角色指定权限边界 Amazon Resource Name (ARN)。如需更多信息，请参阅 AWS 文档中的 IAM 实体的权限边界。

3. 为您的集群范围的角色指定自定义 ARN 路径。该路径必须仅包含字母数字字符，并以 / 开头和结尾，例如 **/test/path/dev/**。如需更多信息，请参阅 *IAM 角色和策略的 ARN 路径自定义*。

4. 选择角色创建模式。您可以使用 **auto** 模式自动创建帐户范围内的角色和策略。**在手动模式中**，**rosa** CLI 生成创建角色和策略所需的 **aws** 命令。**在手动模式中**，对应的策略 JSON 文件也保存到当前目录中。**manual** 模式允许您在手动运行 **aws** 命令前查看详情。

5 6 7 8 创建集群范围的安装程序、control plane、worker 和支持角色以及对应的 IAM 策略。如需更多信息，请参阅 *帐户范围的 IAM 角色和策略参考*。

注意

在此步骤中，ROSA CLI 还会自动创建特定于集群 Operator 策略的帐户范围的 Operator IAM 策略，以允许 ROSA 集群 Operator 执行核心 OpenShift 功能。如需更多信息，请参阅 *帐户范围的 IAM 角色和策略参考*。

b. 查看后，手动运行 **aws** 命令来创建角色和策略。另外，您可以使用 **--mode auto** 运行上述命令来立即运行 **aws** 命令。

2. 可选：如果您使用自己的 AWS KMS 密钥加密 control plane、基础架构、worker 节点根卷和持久性卷(PV)，请将帐户范围内安装程序角色的 ARN 添加到 KMS 密钥策略中。

重要

只有从默认存储类创建的持久性卷(PV)才会使用此特定密钥加密。

使用任何其他存储类创建的 PV 仍然会被加密，但 PV 不会使用此密钥加密，除非存储类被特别配置为使用这个密钥。

a. 将 KMS 密钥的密钥策略保存到本地机器的文件中。以下示例将输出保存到当前工作目录中的 **kms-key-policy.json** ：

```
$ aws kms get-key-policy --key-id <key_id_or_arn> --policy-name default --output text > kms-key-policy.json (1)
```

(1) 将 **<key_id_or_arn** > 替换为 KMS 密钥的 ID 或 ARN。

b. 将您在上一步中创建的集群范围的安装程序角色的 ARN 添加到文件的 claim **.Principal.AWS** 部分。在以下示例中，添加了默认 **ManagedOpenShift-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": "Allow ROSA use of the key",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Support-Role", (1)
          "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Installer-Role",
          "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role",
          "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-ControlPlane-
```

```
Role",
                "arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-
cluster-csi-drivers-ebs-cloud-credent" (2)
            ]
        },
        "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*",
            "kms:DescribeKey"
        ],
        "Resource": "*"
    },
    {
        "Sid": "Allow attachment of persistent resources",
        "Effect": "Allow",
        "Principal": {
            "AWS": [
                "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Support-Role", (3)
                "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Installer-Role",
                "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role",
                "arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-ControlPlane-
Role",
                "arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-
cluster-csi-drivers-ebs-cloud-credent" (4)
            ]
        },
        "Action": [
            "kms:CreateGrant",
            "kms:ListGrants",
            "kms:RevokeGrant"
        ],
        "Resource": "*",
        "Condition": {
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
    }
]
}
```

(1)(3) 您必须为创建 ROSA 集群时要使用的集群范围的角色指定 ARN。部分中列出的 ARN 必须用逗号分开。

(2)(4) 您必须为创建 ROSA 集群时使用的 operator 角色指定 ARN。部分中列出的 ARN 必须用逗号分开。

c. 将更改应用到您的 KMS 密钥策略：

```
$ aws kms put-key-policy --key-id <key_id_or_arn> \ (1)
    --policy file://kms-key-policy.json \ (2)
    --policy-name default
```

1. 将 **<key_id_or_arn>** 替换为 KMS 密钥的 ID 或 ARN。
2. 在本地文件引用密钥策略时，您必须包含 **file://** 前缀。

在下一步中创建集群时，您可以引用 KMS 密钥的 ARN。

3. 使用自定义安装选项创建带有 STS 的集群。您可以使用 **--interactive** 模式以交互方式指定自定义设置：

警告

您无法将 ROSA 集群安装到 OpenShift 安装程序创建的现有 VPC 中。这些 VPC 在集群部署期间创建，且必须只与单个集群关联，以确保集群置备和删除操作正常工作。

要验证 OpenShift 安装程序是否已创建 VPC，请检查 **kubernetes.io/cluster/<infra-id>** 标签上的 **owned** 值。例如，当查看名为 **mycluster-12abc-34def** 的 VPC 标签时，**kubernetes.io/cluster/mycluster-12abc-34def** 标签的值为 **owned**。因此，VPC 由安装程序创建的，不得由管理员修改。

```
$ rosa create cluster --interactive --sts
```

输出示例

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Cluster name: <cluster_name>
? Domain prefix: <domain_prefix> 1
? Deploy cluster with Hosted Control Plane (optional): No
? Create cluster admin user: Yes 2
? Username: user-admin 3
? Password: [? for help] ********** 4
? OpenShift version: 4.16.0 5
? Configure the use of IMDSv2 for ec2 instances optional/required (optional): 6
I: Using arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Installer-Role for the
Installer role 7
I: Using arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-ControlPlane-Role for the
ControlPlane role
I: Using arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role for the Worker
role
I: Using arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Support-Role for the
Support role
? External ID (optional): 8
? Operator roles prefix: <cluster_name>-<random_string> 9
? Deploy cluster using pre registered OIDC Configuration ID:
? Tags (optional) 10
? Multiple availability zones (optional): No 11
```

```
? AWS region: us-east-1
? PrivateLink cluster (optional): No
? Install into an existing VPC (optional): Yes (12)
? Select availability zones (optional): No
? Enable Customer Managed key (optional): No (13)
? Compute nodes instance type (optional):
? Enable autoscaling (optional): No
? Compute nodes: 2
? Additional Security Group IDs (optional): (14)
? > [*]  sg-0e375ff0ec4a6cfa2 ('sg-1')
? > [ ]  sg-0e525ef0ec4b2ada7 ('sg-2')
? Machine CIDR: 10.0.0.0/16
? Service CIDR: 172.30.0.0/16
? Pod CIDR: 10.128.0.0/14
? Host prefix: 23
? Encrypt etcd data (optional): No (15)
? Disable Workload monitoring (optional): No
I: Creating cluster '<cluster_name>'
I: To create this cluster again in the future, you can run:
   rosa create cluster --cluster-name <cluster_name> --role-arn arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Installer-Role --support-role-arn arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Support-Role --master-iam-role arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-ControlPlane-Role --worker-iam-role
arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role --operator-roles-prefix
<cluster_name>-<random_string> --region us-east-1 --version 4.16.0 --additional-compute-
security-group-ids sg-0e375ff0ec4a6cfa2 --additional-infra-security-group-ids sg-
0e375ff0ec4a6cfa2 --additional-control-plane-security-group-ids sg-0e375ff0ec4a6cfa2 --
replicas 2 --machine-cidr 10.0.0.0/16 --service-cidr 172.30.0.0/16 --pod-cidr 10.128.0.0/14 --
host-prefix 23 (16)
I: To view a list of clusters and their status, run 'rosa list clusters'
I: Cluster '<cluster_name>' has been created.
I: Once the cluster is installed you will need to add an Identity Provider before you can login
into the cluster. See 'rosa create idp --help' for more information.
...
```

(1) 可选。在创建集群时，您可以使用 **--domain-prefix** 标志在 **Stopopenshiftapps.com** 上自定义集群的子域。此标志的值在您的机构中必须是唯一的，它不能超过 15 个字符，且在集群创建后无法更改。如果没有提供标志，则会创建一个自动生成的值，它依赖于集群名称的长度。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给 15 个字符的字符串。

(2) (3) (4) 在创建集群时，您可以为集群创建本地管理员用户。选择 **Yes**，然后提示您为集群 admin 创建用户名和密码。用户名不得包含 /、**:** 或 **%**。密码必须至少为 14 个字符 (ASCII-standard)，且无空格。此过程自动配置 htpasswd 身份提供程序。

(5) 在创建集群时，列出的 **OpenShift 版本** 选项包括主版本、次版本和补丁版本，如 **4.16.0**。

(6) 可选：指定 'optional' 以将所有 EC2 实例配置为使用 EC2 实例和 EC2 实例(IMDS)的 v1 和 v2 端点。这是默认值。指定 'required' 将所有 EC2 实例配置为只使用 IMDSv2。

重要

在集群创建后无法更改实例元数据服务设置。

7 如果您在 AWS 帐户中有多个集群版本的帐户角色，则会提供交互式选项列表。

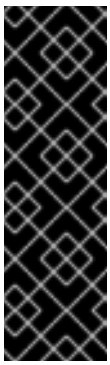
8 可选：指定在假定帐户角色时由 Red Hat OpenShift Service on AWS 和 OpenShift 安装程序传递的唯一标识符。这个选项只适用于希望外部 ID 的自定义帐户角色。

9 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。您可以选择指定自定义前缀来替换角色名称中的 <**cluster_name>-<hash** >。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，请参考 *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自定义路径时，自定义路径会应用到特定于集群的 Operator 角色。

10 可选：指定一个标签，用于 AWS 中由 Red Hat OpenShift Service on AWS 创建的所有资源。标签可帮助您管理、识别、组织、搜索和过滤 AWS 中的资源。标签用逗号分开，例如："密钥值、数据输入"。



重要

Red Hat OpenShift Service on AWS 仅在集群创建过程中支持到 Red Hat OpenShift 资源的自定义标签。添加后，无法删除或编辑标签。集群需要添加的标签才能遵守红帽产品服务等级协议(SLA)。这些标签不能被删除。

Red Hat OpenShift Service on AWS 不支持在 ROSA 集群管理的资源外添加额外的标签。当 AWS 资源由 ROSA 集群管理时，这些标签可能会丢失。在这些情况下，您可能需要自定义解决方案或工具来协调标签，并保持它们保持不变。

11 可选： 在生产环境中，建议使用多个可用区。默认为单个可用区。

12 可选：您可以在现有 VPC 中创建集群，或者 ROSA 可以创建一个新的 VPC 来使用。

警告

您无法将 ROSA 集群安装到 OpenShift 安装程序创建的现有 VPC 中。这些 VPC 在集群部署期间创建，且必须只与单个集群关联，以确保集群置备和删除操作正常工作。

要验证 OpenShift 安装程序是否已创建 VPC，请检查 **kubernetes.io/cluster/<infra-id>** 标签上的 **owned** 值。例如，当查看名为 **mycluster-12abc-34def** 的 VPC 标签时，**kubernetes.io/cluster/mycluster-12abc-34def** 标签的值为 **owned**。因此，VPC 由安装程序创建的，不得由管理员修改。

13 可选：如果您使用自己的 AWS KMS 密钥加密 control plane、基础架构、worker 节点根卷和 PV，则启用这个选项。指定在上一步中添加到集群范围的角色的 ARN 中的 KMS 密钥的 ARN。

重要

只有从默认存储类创建的持久性卷(PV)才会使用此特定密钥加密。

使用任何其他存储类创建的 PV 仍然会被加密，但 PV 不会使用此密钥加密，除非存储类被特别配置为使用这个密钥。

14 可选：您可以选择在集群中使用的额外自定义安全组。您必须已创建了安全组，并将其与您为这个集群选择的 VPC 关联。创建机器池后，您无法为默认机器池添加或编辑安全组。如需更多信息，*请参阅附加资源* 下 *安全组* 的要求。

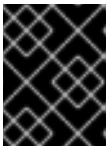
15 可选：除默认加密 etcd 卷的 control plane 存储加密外，才启用这个选项。使用此选项时，etcd 键的值会被加密，而不是键。

重要

通过在 etcd 中为密钥值启用 etcd 加密，则会出现大约 20% 的性能开销。除了加密 etcd 卷的默认 control plane 存储加密外，还会引入第二层加密的开销。红帽建议仅在特别需要时才启用 etcd 加密。

16 输出中包括了一个可以运行的自定义命令来创建使用相同配置的集群。

作为使用 **--interactive** 模式的替代选择，您可以在运行 **rosa create cluster** 命令时直接指定自定义选项。运行 **rosa create cluster --help** 命令来查看可用 CLI 选项列表，或参阅 *使用 ROSA CLI 管理对象*中的*创建集群*。



重要

您必须完成以下步骤来创建 Operator IAM 角色和 OpenID Connect (OIDC)供应商，将集群的状态移到 **ready**。

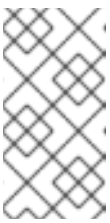
4. 创建特定于集群的 Operator IAM 角色：

   a. 在当前工作目录中生成 Operator IAM 策略 JSON 文件，并输出 **aws** CLI 命令进行审核：

   ```
   $ rosa create operator-roles --mode manual --cluster <cluster_name|cluster_id> 1
   ```

   1 **手动模式** 生成创建 Operator 角色所需的 **aws** CLI 命令和 JSON 文件。检查后，您必须手动运行命令以创建资源。

   b. 检查后，运行 **aws** 命令，以创建 Operator IAM 角色并将受管 Operator 策略附加到它们。另外，您可以使用 **--mode auto** 再次运行上述命令来立即运行 **aws** 命令。



注意

如果您在上一步中指定了前缀，则会对 Operator 角色名称应用自定义前缀。

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，则会自动检测自定义路径并将其应用到 Operator 角色。

重要

除了成功创建集群的帐户角色外，还需要 EBS Operator 角色。

此角色必须附加到 **ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials** 策略，这是 ROSA 所需的 IAM 策略，以通过 Container Storage Interface (CSI)管理后端存储。

有关集群 Operator 所需的策略和权限的更多信息，请参阅 *集群范围的角色创建方法。示例 EBS Operator role* **"arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-ebs-cloud-credent"**

创建 Operator 角色后，您必须在 AWS 控制台的Key Management Service (KMS) 页面中 编辑 *Key Policy* 以添加角色。

5. 创建集群 Operator 用于身份验证的 OpenID Connect (OIDC)供应商：

```
$ rosa create oidc-provider --mode auto --cluster <cluster_name|cluster_id> 1
```

1 **auto** 模式会立即运行创建 OIDC 供应商的 **aws** CLI 命令。

6. 检查集群的状态：

```
$ rosa describe cluster --cluster <cluster_name|cluster_id>
```

输出示例

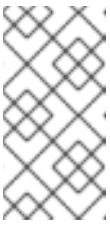
```
Name:                  <cluster_name>
ID:                    <cluster_id>
External ID:           <external_id>
OpenShift Version:     <version>
Channel Group:         stable
DNS:                   <cluster_name>.xxxx.p1.openshiftapps.com
AWS Account:           <aws_account_id>
API URL:               https://api.<cluster_name>.xxxx.p1.openshiftapps.com:6443
Console URL:           https://console-openshift-console.apps.
<cluster_name>.xxxx.p1.openshiftapps.com
Region:                <aws_region>
Multi-AZ:              false
Nodes:
 - Master:             3
 - Infra:              2
 - Compute:            2
Network:
 - Service CIDR:       172.30.0.0/16
 - Machine CIDR:       10.0.0.0/16
 - Pod CIDR:           10.128.0.0/14
 - Host Prefix:        /23
STS Role ARN:          arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Installer-
Role
Support Role ARN:      arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Support-
Role
Instance IAM Roles:
```

```
 - Master:                arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-ControlPlane-
Role
 - Worker:                arn:aws:iam::<aws_account_id>:role/ManagedOpenShift-Worker-Role
Operator IAM Roles:
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-ingress-operator-
cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cluster-csi-drivers-
ebs-cloud-credent
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-machine-api-aws-
cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-cloud-credential-
operator-cloud-crede
 - arn:aws:iam::<aws_account_id>:role/<cluster_name>-xxxx-openshift-image-registry-
installer-cloud-creden
Ec2 Metadata Http Tokens:   optional
State:                      ready
Private:                    No
Created:                    Oct  1 2021 08:12:25 UTC
Details Page:               https://console.redhat.com/openshift/details/s/<subscription_id>
OIDC Endpoint URL:          https://oidc.op1.openshiftapps.com/<cluster_id>|<oidc_config_id>
\ 1
```

1. 端点 URL 取决于 BYO OIDC 配置。如果您要预先填充 OIDC 配置，URL 会以 < **oidc_config_id** > 值结束；否则，URL 以 < **cluster-ID** > 值结尾。

在集群安装过程中，输出中会列出以下 **State** 字段更改：

- **等待（等待 OIDC 配置）**
- **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** 字段在大约 40 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*。

7. 通过观察 OpenShift 安装程序日志来跟踪集群创建的进度：

```
$ rosa logs install --cluster <cluster_name|cluster_id> --watch 1
```

1 1 指定在安装过程中监视新日志消息的 **--watch** 标志。这个参数是可选的。

其他资源

- 安全组

- 集群范围的角色创建方法

2.8. 后续步骤

- 访问 ROSA 集群
- 添加通知联系人

2.9. 其他资源

- 有关在共享虚拟私有云(VPC)中配置 ROSA 集群的更多信息，请参阅为 ROSA 集群配置共享 VPC。
- 有关使用 STS 在 AWS 上部署 Red Hat OpenShift Service 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。
- 有关使用互动模式创建 AWS IAM 资源和 集群时显示的选项概述，请参阅 交互式集群创建模式。
- 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 etcd 加密的更多信息，请参阅 etcd 加密服务定义。
- 有关使用 ROSA 配置代理的详情，请参考配置集群范围代理。
- 有关 ROSA 集群安装故障排除的更多信息，请参阅 对集群部署进行故障排除。
- 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。

第 3 章 使用 TERRAFORM 创建 ROSA （经典架构）集群

3.1. 使用 TERRAFORM 创建默认 ROSA （经典架构）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)（经典架构）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 ROSA （经典架构）AWS 安全令牌服务(STS)集群：

- 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

3.1.1. 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。

前提条件

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 3.1. 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。

3.1.2. 默认集群规格概述

表 3.1. 使用 STS 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
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

组件	默认规格
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
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。 • 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
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

3.1.3. 使用 Terraform 创建默认 ROSA （经典架构）集群

以下概述的集群创建过程演示了如何使用 Terraform 创建帐户范围的 IAM 角色和带有受管 OIDC 配置的 ROSA （经典架构）集群。

3.1.3.1. 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**: 因为在安装过程中在当前目录中创建 Terraform 文件，所以您可以创建一个新的目录来存储这些文件并导航到其中：

```
$ 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. 运行以下命令复制离线令牌，并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
```

3.1.3.2. 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 {
  # The default setting creates 3 availability zones. Set to "false" to create a single availability
zones.
  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 {
  path                 = coalesce(var.path, "/")
  worker_node_replicas = try(var.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-classic" {
  source               = "terraform-redhat/rosa-classic/rhcs"
  version              = "1.5.0"
  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_private_link       = 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
  multi_az               = var.multi_az
  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 "path" {
  description = "(Optional) The arn path for the account/operator roles as well as their
policies."
  type        = string
  default     = null
}

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.private_subnet_cidrs
  public_subnets  = var.public_subnet_cidrs

  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。

3.1.3.3. 使用 Terraform 创建 ROSA 集群

创建 Terraform 文件后，您必须启动 Terraform 以提供所有所需的依赖项。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: 74 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.

  Enter a value: yes
```

如果输入 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-ControlPlane-Role              Control plane  arn:aws:iam::<ID>:role/ROSA-
demo-ControlPlane-Role             4.14             No
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      6
```

3.1.3.4. 使用 Terraform 删除 ROSA 集群

使用 terraform destroy 命令删除通过 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, 74 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.

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 创建的帐户角色的输出示例：

```
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
```

显示没有由 Terraform 创建的 Operator 角色的输出示例：

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

第 4 章 交互式集群创建模式参考

本节概述了通过 ROSA CLI (rosa)，使用互动模式创建 OCM 角色、用户角色和 Red Hat OpenShift Service on AWS (ROSA) 集群时的选项。

4.1. 交互式 OCM 和用户角色创建模式选项

在使用 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)集群前，您必须通过创建和链接 OCM 和用户角色将 AWS 帐户与红帽机构相关联。在运行 **rosa create ocm-role** 命令或 **rosa create user-role** 命令时，您可以通过指定 **--interactive** 选项来启用交互模式。

下表描述了交互式 OCM 角色创建模式选项：

表 4.1. --interactive OCM 角色创建模式选项

字段	描述
角色前缀	指定要在 OCM IAM 角色名称中包含的前缀。默认值为 **ManagedOpenShift**。您只能为每个 AWS 帐户为 Red Hat 机构创建一个 OCM 角色。
为 **OCM 角色启用管理功能（可选）**	启用 admin OCM IAM 角色，该角色等同于指定 **--admin** 参数。如果要使用 **自动** 模式使用 OpenShift Cluster Manager 自动置备特定于集群的 Operator 角色和 OIDC 供应商，则需要 admin 角色。
权限边界 ARN （可选）	为 OCM 角色指定权限边界 Amazon Resource Name (ARN)。如需更多信息，请参阅 AWS 文档中的 IAM 实体的权限边界。
角色路径（可选）	为您的 OCM 角色指定自定义 ARN 路径。该路径必须仅包含字母数字字符，并以 / 开头和结尾，例如 **/test/path/dev/**。如需更多信息，请参阅 *IAM 角色和策略的 ARN 路径自定义*。
角色创建模式	选择角色创建模式。您可以使用 **auto** 模式自动创建 OCM 角色，并将其链接到您的红帽机构帐户。**在手动模式中**，ROSA CLI (**rosa**)生成创建和链接角色所需的 **aws** 命令。**在手动模式中**，对应的策略 JSON 文件也保存到当前目录中。**manual** 模式允许您在手动运行 **aws** 命令前查看详情。
创建 '<ocm_role_name>' 角色？	确认您要创建 OCM 角色。
将 '<ocm_role_arn>' 角色链接到机构 '<red_hat_organization_id>'?	确认您要将 OCM 角色与您的红帽机构相关联。

下表描述了交互式用户角色创建模式选项：

表 4.2. --interactive 用户角色创建模式选项

字段	描述
角色前缀	指定要在用户角色名称中包含的前缀。默认值为 **ManagedOpenShift**。
权限边界 ARN （可选）	为用户角色指定权限边界 Amazon Resource Name (ARN)。如需更多信息，请参阅 AWS 文档中的 IAM 实体的权限边界。
角色路径（可选）	为您的用户角色指定自定义 ARN 路径。该路径必须仅包含字母数字字符，并以 / 开头和结尾，例如 **/test/path/dev/**。如需更多信息，请参阅 *IAM 角色和策略的 ARN 路径自定义*。
角色创建模式	选择角色创建模式。您可以使用 **auto** 模式自动创建用户角色并将其链接到 OpenShift Cluster Manager 用户帐户。**在手动模式中**，ROSA CLI 生成创建和链接角色所需的 **aws** 命令。**在手动模式中**，对应的策略 JSON 文件也保存到当前目录中。**manual** 模式允许您在手动运行 **aws** 命令前查看详情。
创建 '<user_role_name>' 角色？	确认您要创建用户角色。
将 '<user_role_arn>' 角色链接到帐户 '<red_hat_user_account_id>'?	确认您要使用您的红帽用户帐户链接用户角色。

4.2. 交互式集群创建模式选项

您可以使用互动模式使用 AWS 安全令牌服务(STS)创建 Red Hat OpenShift Service on AWS 集群。您可以在运行 rosa create cluster 命令时指定 --interactive 选项来启用模式。

下表描述了交互式集群创建模式选项：

表 4.3. --interactive 集群创建模式选项

字段	描述
集群名称	为集群输入一个名称，如 **my-rosa-cluster**。
域前缀	为集群的子域输入域前缀的名称，如 **my-rosa-cluster**。
使用 Hosted Control Plane 部署集群（可选）	启用 Hosted Control Planes 的使用。

字段	描述
创建集群管理员用户	在使用 htpasswd 身份提供程序创建集群时，创建集群管理员用户。用户名不得包含 /、**:** 或 **%**。密码必须至少为 14 个字符 (ASCII-standard)，且无空格。
使用 AWS STS 部署集群	创建一个 OpenShift 集群，它使用 AWS 安全令牌服务 (STS) 为组件特定的 AWS Identity and Access Management (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。默认值为 **Yes**。
OpenShift version	选择要安装的 OpenShift 版本，如 4。默认为最新版本。
为 **ec2 实例配置 IMDSv2 的 optional/required （可选）**	指定所有 EC2 实例是否同时使用 EC2 实例元数据服务(IMDS)的 v1 和 v2 端点（可选）还是仅 IMDSv2 （必需）。
安装程序角色 ARN	如果您在 AWS 帐户中有多个帐户角色用于集群版本，则会提供一个安装程序角色 ARN 列表。选择您要用于集群的安装程序角色的 ARN。集群使用与所选安装程序角色相关的集群范围的角色和策略。
外部 ID （可选）	指定在假定帐户角色时由 OpenShift Cluster Manager 和 OpenShift 安装程序传递的唯一标识符。这个选项只适用于希望外部 ID 的自定义帐户角色。
Operator 角色前缀	输入要分配给特定于集群的 Operator IAM 角色的前缀。默认值是集群名称和 4 位随机字符串，如 **my-rosa-cluster-a0b1**。
使用预注册的 OIDC 配置 ID 部署集群	指定您是否要使用预配置的 OIDC 配置，还是要创建新的 OIDC 配置作为集群创建过程的一部分。
tags （可选）	指定标签，用于 AWS 中由 Red Hat OpenShift Service on AWS 创建的所有资源。标签可帮助您管理、识别、组织、搜索和过滤 AWS 中的资源。标签用逗号分开，例如：“key value, foo bar”。 **重要** Red Hat OpenShift Service on AWS 仅在集群创建过程中支持到 Red Hat OpenShift 资源的自定义标签。添加后，无法删除或编辑标签。集群需要添加的标签才能遵守红帽产品服务等级协议 (SLA)。这些标签不能被删除。 Red Hat OpenShift Service on AWS 不支持在 ROSA 集群管理的资源外添加额外的标签。当 AWS 资源由 ROSA 集群管理时，这些标签可能会丢失。在这些情况下，您可能需要自定义解决方案或工具来协调标签，并保持它们保持不变。

字段	描述
多个可用区（可选）	将集群部署到 AWS 区域中的多个可用区。默认值为 **No**，这会导致集群部署到单个可用区。如果您将集群部署到多个可用区，AWS 区域必须至少有 3 个可用区。对于生产环境工作负载，建议使用多个可用区。
AWS 区域	指定要将集群部署到的 AWS 区域。这会覆盖 **AWS_REGION** 环境变量。
PrivateLink 集群（可选）	使用 AWS PrivateLink 创建集群。这个选项提供虚拟私有云 (VPC)、AWS 服务和内部网络之间的私有连接，而无需向公共互联网公开流量。为了提供支持，Red Hat Site Reliability Engineering (SRE)可以使用 AWS PrivateLink Virtual Private Cloud (VPC)端点连接到集群。在集群创建后无法更改这个选项。默认值为 **No**。
Machine CIDR	指定机器（集群节点）的 IP 地址范围，它您的 VPC 子网的所有 CIDR 地址范围。子网必须是连续的。单个可用区部署支持最少有 128 个地址的 IP 地址范围（使用子网前缀 **/25**）。多可用区部署支持最少 256 个地址的 IP 地址范围（使用子网前缀 **/24**）。默认值为 **10.0.0.0/16**。这个范围不得与任何连接的网络冲突。
Service CIDR	指定服务的 IP 地址范围。建议不要要求地址块在集群之间是相同的。这将不会创建 IP 地址冲突。范围必须足够大，以适应您的工作负载。该地址块不得与从集群内部访问的任何外部服务重叠。默认为 **172.30.0.0/16**。
Pod CIDR	指定 pod 的 IP 地址范围。建议不要要求地址块在集群之间是相同的。这将不会创建 IP 地址冲突。范围必须足够大，以适应您的工作负载。该地址块不得与从集群内部访问的任何外部服务重叠。默认为 **10.128.0.0/14**。
安装到现有的 VPC 中（可选）	将集群安装到现有的 AWS VPC 中。要使用这个选项，您的 VPC 必须为每个要将集群安装到的可用区有 2 个子网。默认值为 **No**。
选择可用区（可选）	指定安装到现有 AWS VPC 时使用的可用区。使用以逗号分隔的列表来提供可用区。如果您指定 **No**，安装程序将自动选择可用区。
启用客户管理的密钥（可选）	启用这个选项，使用特定的 AWS 密钥管理服务(KMS)密钥作为持久数据的加密密钥。此密钥功能作为 control plane、基础架构和 worker 节点根卷的加密密钥。密钥也在默认存储类上配置，以确保使用默认存储类创建的持久性卷将使用特定的 KMS 密钥加密。禁用后，默认使用指定区域的帐户 KMS 密钥来确保始终加密持久数据。默认值为 **No**。
Compute 节点实例类型	选择计算节点实例类型。默认值为 **m5.xlarge**。
启用自动扩展（可选）	启用计算节点自动扩展。自动缩放器会调整集群的大小，以满足您的部署需求。默认值为 **No**。

字段	描述
其他计算安全组 ID （可选）	选择与集群端创建的标准机器池一起使用的额外自定义安全组 ID。默认为 none 选择。仅显示与所选 VPC 关联的安全组。您可以选择最多 5 个额外的安全组。
额外的 Infra Security Group ID （可选）	选择与集群端创建的 infra 节点一起使用的额外自定义安全组 ID。默认为 none 选择。仅显示与所选 VPC 关联的安全组。您可以选择最多 5 个额外的安全组。
其他 Control Plane 安全组 ID （可选）	选择与集群侧创建的 control plane 节点一起使用的额外自定义安全组 ID。默认为 none 选择。仅显示与所选 VPC 关联的安全组。您可以选择最多 5 个额外的安全组。
Compute 节点	指定要置备到每个可用区的计算节点数量。在单个可用区中部署的集群至少需要 2 个节点。在多个区中部署的集群必须至少有 3 个节点。worker 节点的最大数量是 180 个节点。默认值为 **2**。
默认机器池标签（可选）	指定默认机器池的标签。标签格式应该是以逗号分隔的键值对列表。此列表会持续覆盖对节点标签所做的任何修改。
主机前缀	指定分配给调度到各个机器的 pod 的子网前缀长度。主机前缀决定了每台机器的 pod IP 地址池。例如，如果主机前缀设置为 **/23**，则每台机器从 pod CIDR 地址范围中分配一个 **/23** 子网。默认值为 **/23**，允许 512 个集群节点和每个节点 512 个 pod，它们超过我们支持的最大值。有关支持的最大值的详情，请参考下面的附加资源部分。
机器池根磁盘大小(GiB 或 TiB)	指定机器池根磁盘的大小。这个值必须包含单位后缀，如 GiB 或 TiB，例如默认值 **300GiB**。
启用 FIPS 支持（可选）	启用或禁用 FIPS 模式。默认值为 **false** （禁用）。如果启用了 FIPS 模式，运行 Red Hat OpenShift Service on AWS 的 Red Hat Enterprise Linux CoreOS (RHCOS)机器会绕过默认的 Kubernetes 加密套件，并使用由 RHCOS 提供的加密模块。  **重要** 要为集群启用 FIPS 模式，您必须从配置为以 FIPS 模式操作的 {op-system-base-full} 计算机运行安装程序。有关在 RHEL 中配置 FIPS 模式的更多信息，请参阅在 FIPS 模式中安装该系统。 当以 FIPS 模式运行 {op-system-base-full} 或 Red Hat Enterprise Linux CoreOS (RHCOS)引导时，Red Hat OpenShift Service on AWS 核心组件使用 {op-system-base} 加密库，该库在 x86_64、ppc64le 和 s390x 构架上提交给 NIST FIPS 140-2/140-3 Validation。

字段	描述
加密 etcd 数据（可选）	Red Hat OpenShift Service on AWS 中，control plane 存储会默认加密，这包括 etcd 卷的加密。您还可以启用 **Encrypt etcd data** 选项加密 etcd 中某些资源的键值，而不是键本身。  **重要** 通过在 etcd 中为密钥值启用 etcd 加密，则会出现大约 20% 的性能开销。除了加密 etcd 卷的默认 control plane 存储加密外，还会引入第二层加密的开销。红帽建议仅在特别需要时才启用 etcd 加密。
禁用工作负载监控（可选）	禁用监控用户定义的项目。默认启用对用户定义的项目的监控。
ingress 的 route Selector （可选）	指定入口的路由选择器。格式应该是以逗号分隔的键值对列表。如果没有指定标签，则所有路由将在两个路由器上公开。对于旧的入口支持，这些标签会包含标签；否则，它们被视为排除标签。
ingress 排除的命名空间（可选）	指定入口的排除命名空间。格式应该是用逗号分开的列表 **值 1，value2...**。如果没有指定任何值，则会公开所有命名空间。
通配符策略（可选，选择 'Skip' 来跳过选择。将提供默认值。	为您的入口选择通配符策略。选项为 **WildcardsDisallowed** 和 **WildcardsAllowed**。默认为 **WildcardsDisallowed**。
命名空间所有权策略（可选，选择 'Skip' 来跳过选择。将提供默认值。	选择 ingress 的命名空间所有权策略。选项为 **Strict** 和 **InterNamespaceAllowed**。默认为 **Strict**。

4.3. 其他资源

- 有关为 OCM 角色、用户角色和帐户范围角色使用自定义 ARN 路径的更多信息，请参阅 IAM 角色和策略的 ARN 路径自定义。
- 有关支持的最大值列表，请参阅 ROSA 测试的集群最大值。
- 有关快速创建带有 STS 的 ROSA 集群（包括 AWS IAM 资源）的详细步骤，请参阅 使用默认选项创建带有 STS 的 ROSA 集群。
- 有关使用自定义（包括 AWS IAM 资源）创建带有 STS 的 ROSA 集群的详细步骤，请参阅使用自定义创建带有 STS 的 ROSA 集群。

- 有关 etcd 加密的更多信息，请参阅 etcd 加密服务定义。

- 有关 VPC 架构示例，请参阅 VPC 架构示例。

第 5 章 在 ROSA 上创建 AWS PRIVATELINK 集群

本文档论述了如何使用 AWS PrivateLink 创建 ROSA 集群。

5.1. 了解 AWS PRIVATELINK

可以在 AWS 集群上创建 Red Hat OpenShift Service，无需公共子网、互联网网关或网络地址转换 (NAT) 网关。在这个配置中，红帽使用 AWS PrivateLink 管理和监控集群以避免所有公共入口网络流量。如果没有公共子网，就无法将应用程序路由器配置为公共路由器。配置私有应用路由器是唯一选项。

如需更多信息，请参阅 AWS 网站上的 AWS PrivateLink。

重要

您只能在安装时创建一个 PrivateLink 集群。您不能在安装后将集群改为 PrivateLink。

5.2. 使用 AWS PRIVATELINK 集群的要求

对于 AWS PrivateLink 集群，互联网网关、NAT 网关和公共子网不需要，但专用子网必须提供安装所需组件的互联网连接。Single-AZ 集群需要至少一个私有子网，而 Multi-AZ 集群需要至少 3 个私有子网。下表显示了成功安装所需的 AWS 资源：

表 5.1. 所需的 AWS 资源

组件	AWS 类型	描述
VPC	• AWS::EC2::VPC • AWS::EC2::VPCEndpoint	您必须提供 VPC 供集群使用。

<table>
<tr><th>组件</th><th>AWS 类型</th><th>描述</th></tr>
<tr><td>网络访问控制</td><td>AWS::EC2::NetworkAcl
AWS::EC2::NetworkAclEntry</td><td>您必须允许访问以下端口：<table><tr><th>端口</th><th>原因</th></tr><tr><td>80</td><td>入站 HTTP 流量</td></tr><tr><td>443</td><td>入站 HTTPS 流量</td></tr><tr><td>22</td><td>入站 SSH 流量</td></tr><tr><td>1024-65535</td><td>入站临时流量</td></tr><tr><td>0-65535</td><td>出站临时流量</td></tr></table></td></tr>
<tr><td>专用子网</td><td>AWS::EC2::Subnet
AWS::EC2::RouteTable
AWS::EC2::SubnetRouteTableAssociation</td><td>您的 VPC 在 1 个可用区中必须具有私有子网，用于 Single-AZ 部署，或 3 个可用区用于 Multi-AZ 部署。您必须提供适当的路由和路由表。</td></tr>
</table>

5.3. 创建 AWS PRIVATELINK 集群

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI rosa 创建 AWS PrivateLink 集群。

注意

仅在现有的 **VPC** 上支持 **AWS PrivateLink**。

先决条件

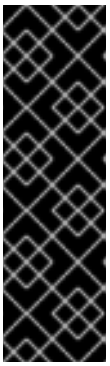
- **您有可用的 AWS 服务配额。**
- **您已在 AWS 控制台中启用了 ROSA 服务。**
-

您已在安装主机上安装并配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI rosa。

流程

创建集群最多可能需要 40 分钟。

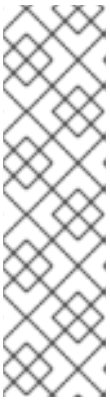
1. 使用 AWS PrivateLink，您可以创建一个单一可用区 (Single-AZ) 或多个可用区 (Multi-AZ) 的集群。在这两种情况下，您的机器的无类别间路由 (CIDR) 必须与虚拟私有云的 CIDR 匹配。如需更多信息，请参阅使用您自己的 VPC 和 VPC 验证 的要求。



重要

如果使用防火墙，您必须进行配置，以便 Red Hat OpenShift Service on AWS 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。



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。

- 创建 Single-AZ 集群：

```
$ rosa create cluster --private-link --cluster-name=<cluster-name> [--machine-cidr=<VPC CIDR>/16] --subnet-ids=<private-subnet-id>
```

- 创建 Multi-AZ 集群：

```
$ rosa create cluster --private-link --multi-az --cluster-name=<cluster-name> [--machine-cidr=<VPC CIDR>/16] --subnet-ids=<private-subnet-id1>,<private-subnet-id2>,<private-subnet-id3>
```

2.

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 40 分钟后没有变为 ready，请检查安装故障排除文档以了解更多详细信息。

3. 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
```

5.4. 配置 AWS PRIVATELINK DNS 转发

使用 AWS PrivateLink 集群时，在 Route 53 中创建公共托管区和一个私有托管区。使用私有托管区，区中的记录只能从 VPC 中将其分配给它。

Let 的 Encrypt DNS-01 验证需要一个公共区，以便为域发布有效的公开可信证书。验证记录会在 *Let's Encrypt* 验证完成后删除。但是，在发布和更新这些证书时仍需要该区域，这通常需要 60 天。虽然这些区域通常会出现为空，但在验证过程中提供关键角色。

如需有关私有托管区的更多信息，请参阅 AWS 私有托管区文档。有关公共托管区的更多信息，请参阅 AWS 公共托管区文档。

先决条件

- 您的公司网络或其他 VPC 有连接
- 在您的网络中启用 UDP 端口 53 和 TCP 端口 53 以允许 DNS 查询
- 已使用 Red Hat OpenShift Service on AWS 创建 AWS PrivateLink 集群

流程

1. 要允许记录（如 api.<cluster_domain> 和 *.apps.<cluster_domain>） 在 VPC 之外解析，配置一个 Route 53 Resolver Inbound Endpoint。

2. 配置入站端点时，选择创建集群时使用的 VPC 和专用子网。

3. 在端点运行并关联后，配置公司网络以将 DNS 查询转发到顶级集群域（如 drow-pl-01.htno.p1.openshiftapps.com ）的 IP 地址。

4. 如果您要将 DNS 查询从一个 VPC 转发到另一个 VPC，请配置转发规则。

5. 如果要配置远程网络 DNS 服务器，请参阅您的特定 DNS 服务器文档为已安装集群域配置选择性 DNS 转发。

5.5. 后续步骤

- 配置身份提供程序
- 添加通知联系人

5.6. 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

第 6 章 为 ROSA 集群配置共享 VPC

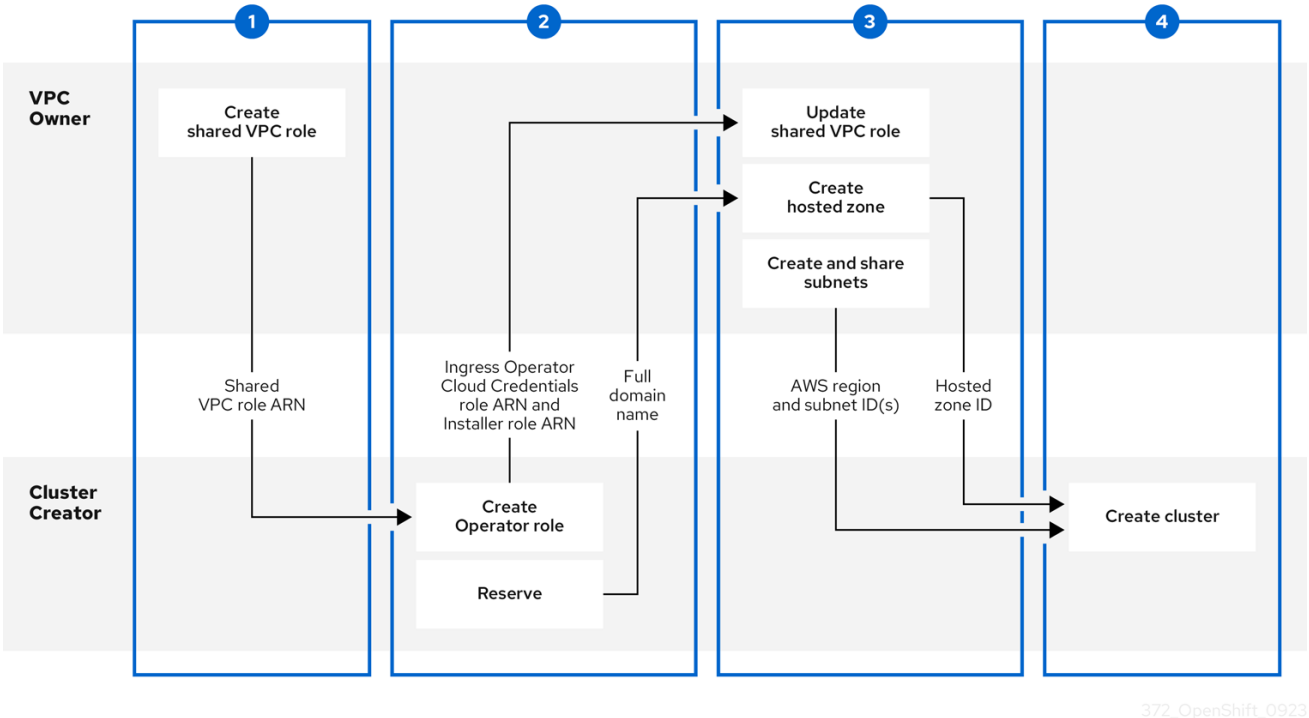
您可以在共享、集中管理的 AWS 虚拟私有云(VPC)上创建 Red Hat OpenShift Service on AWS (ROSA)集群。

重要

目前，只有使用 STS 进行身份验证的 ROSA Classic 集群才支持 在多个 AWS 帐户间共享 VPC。

注意

此过程需要 两个属于同一 AWS 机构的独立 AWS 帐户。一个帐户作为 VPC-owning AWS 帐户(VPC Owner)，另一个帐户在集群创建 AWS 帐户(Cluster Creator)中创建集群。



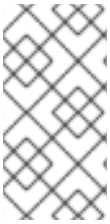
VPC Owner的先决条件

- 您有一个具有适当权限的 AWS 帐户，以创建角色和共享资源。
- Cluster Creator 的 AWS 帐户与 VPC 所有者的 AWS 帐户分开。

- 两个 AWS 帐户都属于同一 AWS 机构。
- 您从机构的管理帐户启用了资源共享。
- 您可以访问 AWS 控制台。

集群创建器的先决条件

- 已安装 ROSA CLI (rosa) 1.2.26 或更高版本。
- 创建了用于创建集群的所有必需的 ROSA 帐户角色。
- Cluster Creator 的 AWS 帐户与 VPC 所有者的 AWS 帐户分开。
- 两个 AWS 帐户都属于同一 AWS 机构。

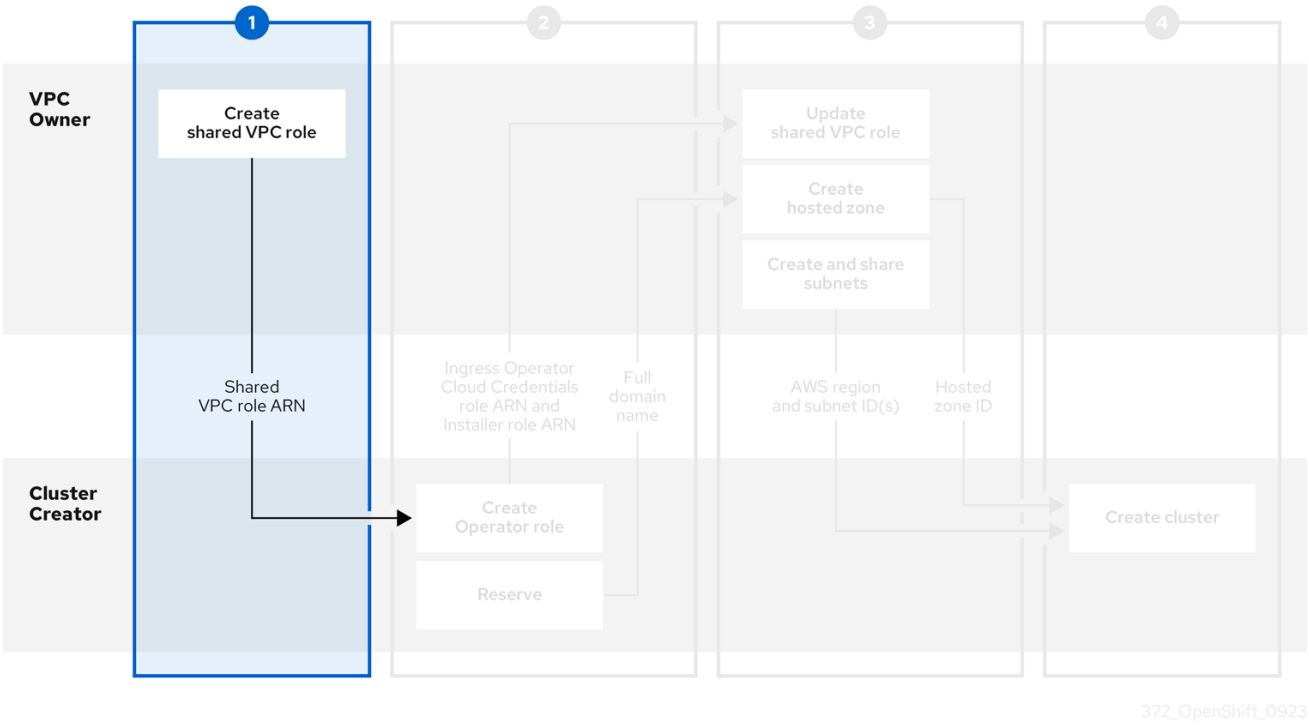


注意

在共享 VPC 上安装集群只支持 OpenShift 4.12.34 及更新的版本、4.13.10 及更新的版本，以及将来的 4.y-streams。

6.1. 第 1 步 - VPC 所有者：配置 VPC 以在 AWS 机构中共享

如果该帐户位于当前 AWS 机构中，您可以将配置的 VPC 中的子网与另一个 AWS 用户帐户共享。



流程

1. 在 AWS 控制台的 VPC 部分中，创建或修改 VPC 部分的 VPC。

2. 创建一个自定义策略文件，以允许使用名称 SharedVPCPolicy 的必要共享 VPC 权限：

```
$ cat <<EOF > /tmp/shared-vpc-policy.json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "route53:ChangeResourceRecordSets",
            "route53:ListHostedZones",
            "route53:ListHostedZonesByName",
            "route53:ListResourceRecordSets",
            "route53:ChangeTagsForResource",
            "route53:GetAccountLimit",
            "route53:GetChange",
            "route53:GetHostedZone",
            "route53:ListTagsForResource",
            "route53:UpdateHostedZoneComment",
            "tag:GetResources",
            "tag:UntagResources"
         ],
         "Resource": "*"
      }
```

```
    ]
}
EOF
```

3. 在 AWS 中创建策略：

```
$ aws iam create-policy \
  --policy-name SharedVPCPolicy \
  --policy-document file:///tmp/shared-vpc-policy.json
```

您可以将此策略附加到共享 VPC 权限所需的角色。

4. 创建自定义信任策略文件，授予授予角色的权限：

```
$ cat <<EOF > /tmp/shared-vpc-role.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<Account-ID>:root" (1)
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
```

(1) 主体将在 Cluster Creator 创建必要的集群角色后被限定。在创建时，您必须使用 Cluster Creator 的 AWS 帐户 ID 作为 arn:aws:iam::{Account}:root 来创建 root 用户占位符。

5. 创建 IAM 角色：

```
$ aws iam create-role --role-name <role_name> \ (1)
  --assume-role-policy-document file:///tmp/shared-vpc-role.json
```

(1) 将 < *role_name* > 替换为您要创建的角色的名称。

6. 附加自定义 SharedVPCPolicy 权限策略：

```
$ aws iam attach-role-policy --role-name <role_name> --policy-arn \ 1
  arn:aws:iam::<AWS_account_ID>:policy/SharedVPCPolicy 2
```

1. 将 *<role_name>* 替换为您创建的角色的名称。

2. 将 *<AWS_account_ID>* 替换为 VPC 所有者的 AWS 帐户 ID。

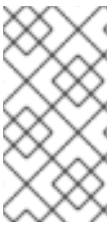
7. 为 Cluster Creator 提供 SharedVPCRole ARN 以继续配置。

其他资源

- 有关 共享 AWS 资源的信息，请参阅 AWS 文档。

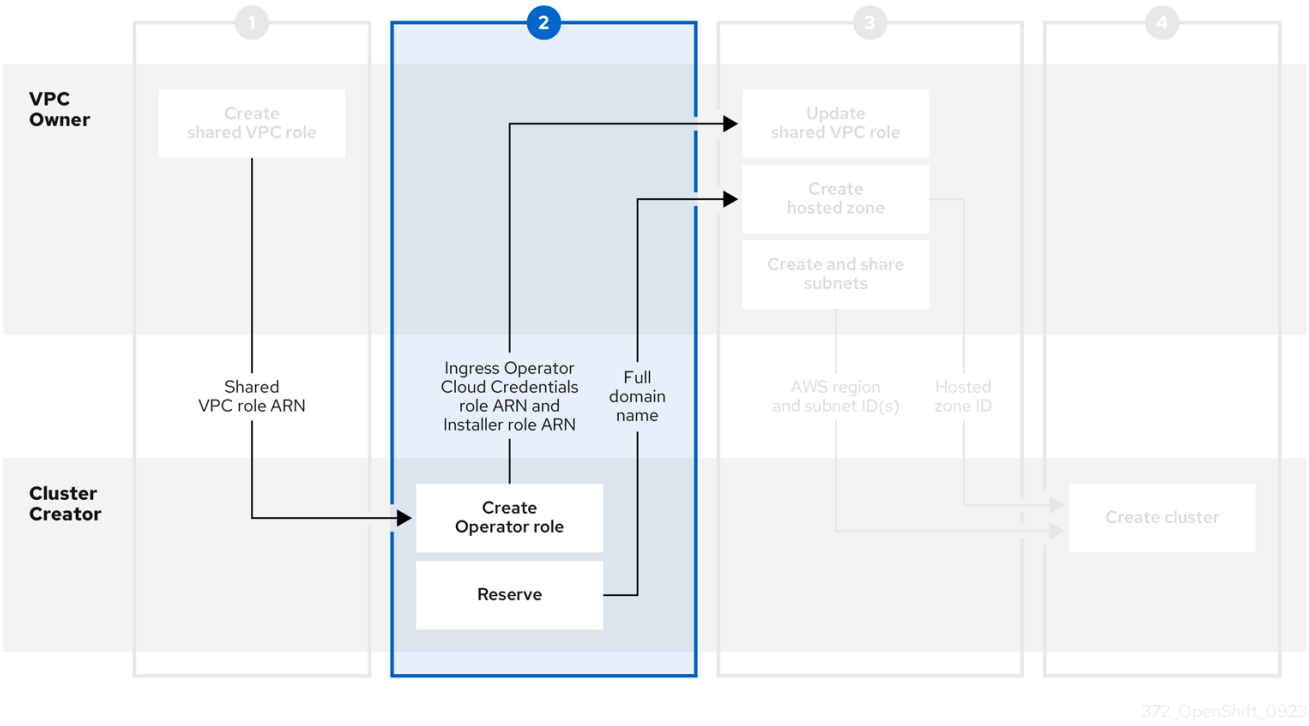
6.2. 第 2 步- 集群创建：保留您的 DNS 并创建集群操作器角色

在 VPC Owner 创建虚拟私有云、子网和 IAM 角色后，共享 VPC 资源，保留 openshiftapps.com DNS 域，并创建 Operator 角色来回与 VPC Owner 进行通信。



注意

对于共享 VPC 集群，您可以选择在集群创建步骤后创建 Operator 角色。集群将处于等待状态，直到 Ingress Operator 角色 ARN 添加到共享 VPC 角色可信关系中。



前提条件

- **您有来自 VPC Owner 的 IAM 角色的 SharedVPCRole ARN。**

流程

1. **使用以下命令保留 openshiftapps.com DNS 域：**

```
$ rosa create dns-domain
```

该命令创建一个保留的 openshiftapps.com DNS 域。

```
I: DNS domain '14eo.p1.openshiftapps.com' has been created.
I: To view all DNS domains, run 'rosa list dns-domains'
```

2. **创建 OIDC 配置。**

有关 OIDC 配置过程的更多信息，请参阅此文档。以下命令生成您需要的 OIDC 配置 ID：

```
$ rosa create oidc-config
```

您会收到确认命令创建了 OIDC 配置：

```
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
25tu67hq45rto1am3slpf5lq6jargg
```

3. 运行以下命令来创建 Operator 角色：

```
$ rosa create operator-roles --oidc-config-id <oidc-config-ID> (1)
   --installer-role-arn <Installer_Role> (2)
   --shared-vpc-role-arn <Created_VPC_Role_Arn> (3)
   --prefix <operator-prefix> (4)
```

(1) 提供您在上一步中创建的 OIDC 配置 ID。

(2) 提供作为 rosa create account-roles 进程一部分创建的安装程序 ARN。

(3) 为 VPC 所有者 创建的角色提供 ARN。

(4) 为 Operator 角色提供前缀。

注意

安装程序帐户角色和共享 VPC 角色必须具有一对一的关系。如果要创建多个共享 VPC 角色，您应该为每个共享 VPC 角色创建一个帐户角色。

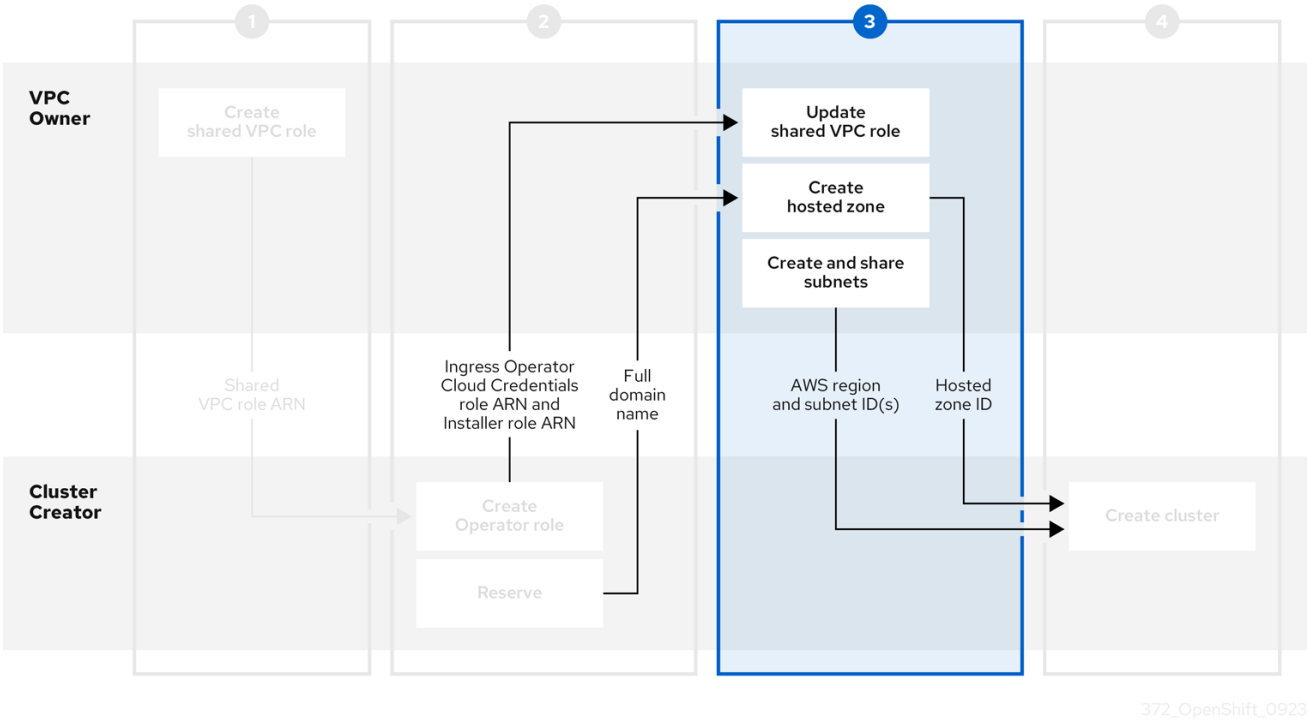
4. 创建 Operator 角色后，共享使用 <intended _cluster_name>.<reserved_dns_domain> 创建的完整域名、*Ingress Operator Cloud Credentials* 角色的 ARN 以及您的 *安装程序* 角色的 ARN 来继续配置。

共享信息类似这些示例：

- my-rosa-cluster.14eo.p1.openshiftapps.com
- arn:aws:iam::111122223333:role/ManagedOpenShift-Installer-Role
- arn:aws:iam::111122223333:role/my-rosa-cluster-openshift-ingress-operator-cloud-credentials

6.3. STEP THREE - VPC OWNER: 更新共享 VPC 角色并创建托管区

在 Cluster Creator 提供 DNS 域和 IAM 角色后，创建一个私有托管区并更新为共享 VPC 创建的 IAM 角色上的信任策略。



前提条件

- 您有 Cluster Creator 的完整域名。
- 您有来自 Cluster Creator 的 *Ingress Operator Cloud Credentials* 角色的 ARN。
- 您有来自 Cluster Creator 的 *Installer* 角色的 ARN。

流程

1. 在 AWS 控制台的 Resource Access Manager 中，创建一个与 Cluster Creator 的 AWS 帐户 ID 共享之前创建的公共和私有子网的资源共享。

2. 更新 VPC 共享 IAM 角色，并将安装程序和 *Ingress Operator Cloud Credentials* 角色添加到信任策略的 principal 部分。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
   "Sid": "Statement1",
   "Effect": "Allow",
   "Principal": {
    "AWS": [
        "arn:aws:iam::<Cluster-Creator's-AWS-Account-ID>:role/<prefix>-ingress-operator-cloud-credentials",
        "arn:aws:iam::<Cluster-Creator's-AWS-Account-ID>:role/<prefix>-Installer-Role"
      ]
   },
   "Action": "sts:AssumeRole"
  }
  ]
}
```

3. *在 AWS 控制台的 Route 53 部分中，创建一个私有托管区。在托管区配置中，域名是 <cluster_name>.<reserved_dns_domain >。私有托管区必须与创建的 VPC 关联。*

4. *创建托管区并与 VPC 关联后，向 Cluster Creator 提供以下内容以继续配置：*

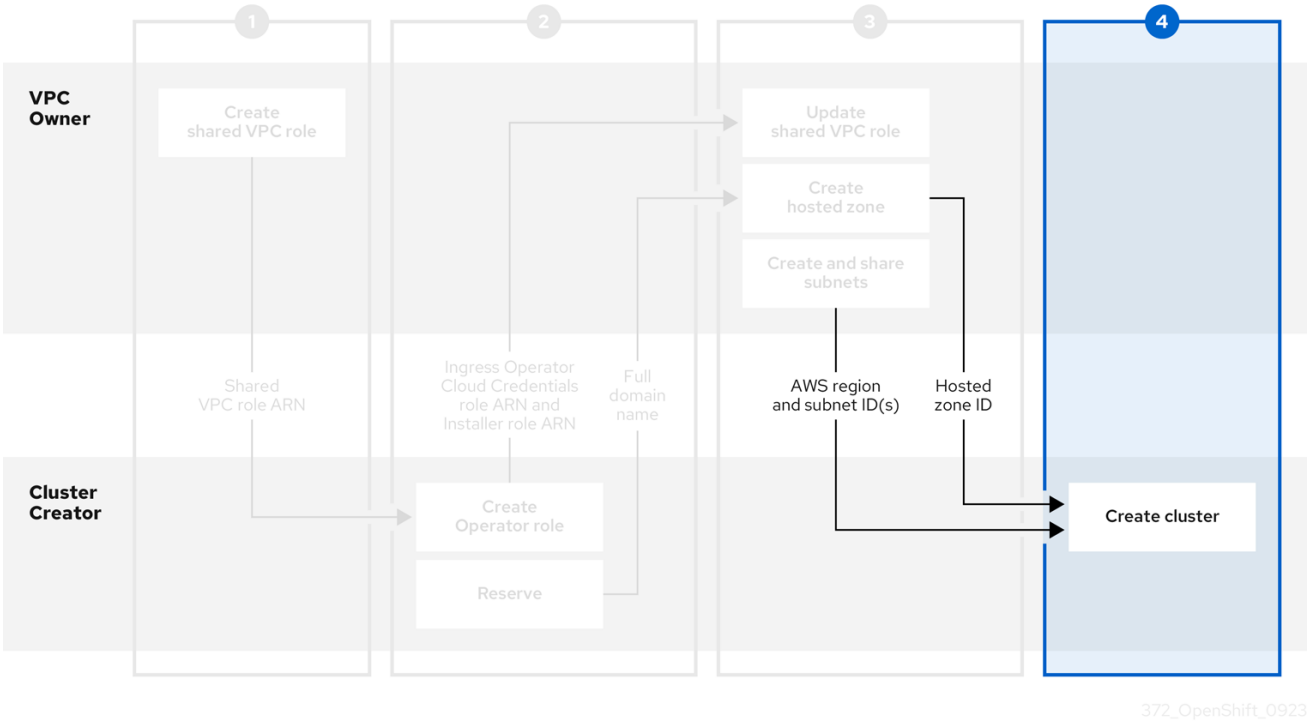
   - *托管区 ID*
   - *AWS 区域*
   - *子网 ID*

6.4. 步骤四 - 集群创建： 在共享 VPC 中创建集群

要在共享 VPC 中创建集群，请完成以下步骤。

注意

在共享 VPC 上安装集群只支持 OpenShift 4.12.34 及更新的版本、4.13.10 及更新的版本，以及将来的 4.y-streams。



前提条件

- *您有来自 VPC Owner 的托管区 ID。*
- *您有来自 VPC Owner 的 AWS 区域。*
- *您有来自 VPC Owner 的子网 ID。*
- *您有 VPC Owner 的 SharedVPCRole ARN。*

流程

- *在终端中，输入以下命令创建共享 VPC：*

```
rosa create cluster --cluster-name <cluster_name> --sts --operator-roles-prefix
<prefix> --oidc-config-id <oidc_config_id> --region us-east-1 --subnet-ids
```

```
<subnet_ids> --private-hosted-zone-id <hosted_zone_ID> --shared-vpc-role-arn <vpc-role-arn> --base-domain <dns-domain>
```

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。

第 7 章 访问 ROSA 集群

建议您使用身份提供程序(IDP)帐户访问 Red Hat OpenShift Service on AWS (ROSA)集群。但是，创建集群的集群管理员可以使用快速访问过程访问它。

本文档论述了如何使用 ROSA CLI (rosa) 访问集群并设置 IDP。另外，您可以使用 OpenShift Cluster Manager 控制台创建 IDP 帐户。

7.1. 快速访问集群

您可以使用此快速访问过程来登录到集群。

注意

作为最佳实践，请使用 IDP 帐户访问集群。

流程

1. 输入以下命令：

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

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'. It may take up to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.cluster-name.t6k4.i1.organization.org:6443 \ 1
--username cluster-admin \
--password FWGYL-2mkJI-3ZTTZ-rINns
```

1 对于带有托管 control plane (HCP)集群的 Red Hat OpenShift Service on AWS (ROSA)，端口号应为 443。

2. 在上一命令的输出中输入 oc login 命令、用户名和密码：

输出示例

```
$ oc login https://api.cluster_name.t6k4.i1.organization.org:6443 \ 1
>  --username cluster-admin \
>  --password FWGYL-2mkJI-3ZTTZ-rlNns
Login successful.

You have access to 77 projects, the list has been suppressed. You can list all projects with 'projects'
```

1 对于使用 HCP 集群的 ROSA，端口号应为 443。

3. 使用 default 项目，输入此 oc 命令来验证是否已创建集群管理员访问权限：

```
$ oc whoami
```

输出示例

```
cluster-admin
```

7.2. 使用 IDP 帐户访问集群

要登录到集群，您可以配置身份提供程序(IDP)。此流程使用 GitHub 作为示例 IDP。要查看其他支持的 IDP，请运行 rosa create idp --help 命令。

注意

或者，作为创建集群的用户，您可以使用快速访问过程。

流程

使用 IDP 帐户访问集群：

1. 添加 IDP。

   a. 以下命令创建一个由 GitHub 支持的 IDP。运行此命令后，按照输出中的交互式提示访问 GitHub 开发人员设置 并配置新的 OAuth 应用。

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

   b. 输入以下值：

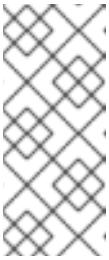
   - 身份提供程序类型： github
   - Restrict to members of: organizations（如果您没有 GitHub 机构，您可以立即创建一个）
   - GitHub organizations: rh-test-org （您的组织的名称）

   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
   ? Restrict to members of: organizations
   ? GitHub organizations: rh-test-org
   ? To use GitHub as an identity provider, you must first register the application:
    - Open the following URL:
      https://github.com/organizations/rh-rosa-test-cluster/settings/applications/new?
   oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
   openshift.apps.rh-rosa-test-
   cluster.z7v0.s1.devshift.org%2Foauth2callback%2Fgithub-
   ```

```
1&oauth_application%5Bname%5D=rh-rosa-test-cluster-
stage&oauth_application%5Burl%5D=https%3A%2F%2Fconsole-openshift-
console.apps.rh-rosa-test-cluster.z7v0.s1.devshift.org
 - Click on 'Register application'
...
```

c. 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 Red Hat OpenShift Service on AWS (ROSA) CLI rosa 定义的 URL 自动填充所需的值。

d. 使用您创建的 GitHub 应用程序的信息并继续提示。输入以下值：

- 客户端 ID: & lt;my_github_client_id>
- Client Secret: [? for help] &lt ;my_github_client_secret>
- hostname ：（可选，您可以立即将其留空）
- 映射方法： claim

持续的输出示例

```
...
? Client ID: <my_github_client_id>
? Client Secret: [? for help] <my_github_client_secret>
? Hostname:
? Mapping method: claim
I: Configuring IDP for cluster 'rh_rosa_test_cluster'
I: Identity Provider 'github-1' has been created. You need to ensure that there is a
```

```
list of cluster administrators defined. See 'rosa create user --help' for more
information. To login into the console, open https://console-openshift-
console.apps.rh-test-org.z7v0.s1.devshift.org and click on github-1
```

在集群中配置 IDP 可能需要 1-2 分钟。

e. 输入以下命令验证您的 IDP 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.rh-rosa-test-
cluster1.j9n4.s1.devshift.org/oauth2callback/github-1
```

2. 登录到您的集群。

a. 输入以下命令获取集群 的控制台 URL ：

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

输出示例

```
Name:       rh-rosa-test-cluster1
ID:         1de87g7c30g75qechgh7l5b2bha6r04e
External ID: 34322be7-b2a7-45c2-af39-2c684ce624e1
API URL:    https://api.rh-rosa-test-cluster1.j9n4.s1.devshift.org:6443 (1)
Console URL: https://console-openshift-console.apps.rh-rosa-test-
cluster1.j9n4.s1.devshift.org
Nodes:      Master: 3, Infra: 3, Compute: 4
```

```
Region:      us-east-2
State:       ready
Created:     May 27, 2020
```

1

对于带有托管 control plane (HCP)集群的 Red Hat OpenShift Service on AWS (ROSA)，端口号应为 443。

b. 导航到 Console URL，再使用 Github 凭据登录。

c. 在 OpenShift 控制台右上角，点您的名称并点击 Copy Login Command。

d. 选择您添加的 IDP 的名称（在这里是 github-1），然后点 Display Token。

e. 将 oc login 命令复制并粘贴到终端中。

```
$ oc login --token=z3sgOGVDk0k4vbqo_wFqBQQTnT-nA-nQLb8XEmWnw4X --
server=https://api.rh-rosa-test-cluster1.j9n4.s1.devshift.org:6443 1
```

1

对于使用 HCP 集群的 ROSA，使用端口号 443。

输出示例

```
Logged into "https://api.rh-rosa-cluster1.j9n4.s1.devshift.org:6443" as "rh-rosa-
test-user" using the token provided. 1

You have access to 67 projects, the list has been suppressed. You can list all
projects with 'oc projects'

Using project "default".
```

1

对于使用 HCP 集群的 ROSA，端口号应为 443。

f. 输入一个简单的 oc 命令，以验证一切设置是否正确且已登录。

```
$ oc version
```

输出示例

```
Client Version: 4.4.0-202005231254-4a4cd75
Server Version: 4.3.18
Kubernetes Version: v1.16.2
```

7.3. 授予 CLUSTER-ADMIN 访问权限

作为创建集群的用户，将 cluster-admin 用户角色添加到您的帐户中，使其具有最大管理员特权。创建集群时，这些权限不会自动分配给您的用户帐户。

另外，只有创建集群的用户才能向其他 cluster-admin 或 dedicated-admin 用户授予集群访问权限。具有 dedicated-admin 访问权限的用户具有较少的特权。作为最佳实践，将 cluster-admin 用户数量限制为尽量少。

前提条件

- 您已在集群中添加身份提供程序(IDP)。
- 您有要创建的用户的 IDP 用户名。
- 已登陆到集群。

流程

1. 授予用户 cluster-admin 权限：

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

2. 验证您的用户是否以集群管理员身份列出：

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

输出示例

```
GROUP          NAME
cluster-admins    rh-rosa-test-user
dedicated-admins  rh-rosa-test-user
```

3. 输入以下命令验证您的用户现在是否有 cluster-admin 访问权限。集群管理员可以在不出错的情况下运行此命令，但一个专用的管理员无法运行。

```
$ oc get all -n openshift-apiserver
```

输出示例

```
NAME              READY   STATUS    RESTARTS   AGE
pod/apiserver-6ndg2   1/1     Running   0          17h
pod/apiserver-lrmxs   1/1     Running   0          17h
pod/apiserver-tsqhz   1/1     Running   0          17h
NAME         TYPE        CLUSTER-IP     EXTERNAL-IP   PORT(S)   AGE
service/api   ClusterIP   172.30.23.241   <none>       443/TCP   18h
NAME                  DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE
SELECTOR                 AGE
daemonset.apps/apiserver   3         3         3       3            3           node-
role.kubernetes.io/master=   18h
```

其他资源

- *集群管理角色*

7.4. 授予 DEDICATED-ADMIN 访问权限

只有创建集群的用户才能向其他 cluster-admin 或 dedicated-admin 用户授予集群访问权限。具有 dedicated-admin 访问权限的用户具有较少的特权。作为最佳实践，为您的大多数管理员授予 dedicated-admin 访问权限。

前提条件

- *您已在集群中添加身份提供程序(IDP)。*
- *您有要创建的用户的 IDP 用户名。*
- *已登陆到集群。*

流程

1. *输入以下命令将用户提升到 dedicated-admin ：*

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

2. *输入以下命令验证您的用户现在是否有 dedicated-admin 访问权限：*

```
$ oc get groups dedicated-admins
```

输出示例

```
NAME              USERS
dedicated-admins   rh-rosa-test-user
```

注意

如果用户没有 **dedicated-admin** 权限，则会显示 **Forbidden** 错误。

其他资源

- 客户管理员用户

7.5. 其他资源

- 使用 Red Hat OpenShift Cluster Manager 控制台配置身份提供程序
- 了解使用 STS 部署工作流的 ROSA
- 添加通知联系人

第 8 章 为 STS 配置身份提供程序

创建 Red Hat OpenShift Service on AWS (ROSA)集群后，您必须配置身份提供程序，以确定用户如何登录以访问集群。

以下主题描述了如何使用 OpenShift Cluster Manager 控制台配置身份提供程序。另外，您可以使用 ROSA CLI (rosa)来配置身份提供程序并访问集群。

8.1. 了解身份提供程序

Red Hat OpenShift Service on AWS 包含内置的 OAuth 服务器。开发人员和管理员获取 OAuth 访问令牌，以完成自身的 API 身份验证。作为管理员，您可以在安装集群后通过配置 OAuth 来指定身份提供程序。配置身份提供程序可让用户登录和访问集群。

8.1.1. 支持的身份提供程序

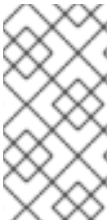
您可以配置以下类型的身份提供程序：

用户身份提供程序	描述
Github 或 GitHub Enterprise	配置 GitHub 身份提供程序，针对 GitHub 或 GitHub Enterprise 的 OAuth 身份验证服务器验证用户名和密码。
GitLab	配置 GitLab 身份提供程序，以使用 GitLab.com 或任何其他 GitLab 实例作为身份提供程序。
Google	使用 Google's OpenID Connect integration 配置 Google 身份提供程序。
LDAP	配置 LDAP 身份提供程序，使用简单绑定身份验证来针对 LDAPv3 服务器验证用户名和密码。
OpenID Connect	配置 OpenID Connect (OIDC) 身份提供程序，以使用授权代码流与 OIDC 身份提供程序集成。
htpasswd	为单个静态管理用户配置 htpasswd 身份提供程序。您可以以用户身份登录到集群来排除问题。 **重要** htpasswd 身份提供程序选项仅用于创建单一静态管理用户。htpasswd 不支持作为 Red Hat OpenShift Service on AWS 的通用身份提供程序。有关配置单个用户的步骤，请参阅*配置 htpasswd 身份提供程序*。

8.1.2. 身份提供程序参数

以下是所有身份提供程序通用的参数：

参数	描述
name	此提供程序名称作为前缀放在提供程序用户名前，以此组成身份名称。
mappingMethod	定义在用户登录时如何将新身份映射到用户。输入以下值之一： **claim** 默认值。使用身份的首选用户名置备用户。如果具有该用户名的用户已映射到另一身份，则失败。 **lookup** 查找现有的身份、用户身份映射和用户，但不自动置备用户或身份。这允许集群管理员手动或使用外部流程设置身份和用户。使用此方法需要手动置备用户。 **add** 使用身份的首选用户名置备用户。如果已存在具有该用户名的用户，此身份将映射到现有用户，添加到该用户的现有身份映射中。如果配置了多个身份提供程序并且它们标识同一组用户并映射到相同的用户名，则需要进行此操作。



注意

在添加或更改身份提供程序时，您可以通过把 **mappingMethod** 参数设置为 **add**，将新提供程序中的身份映射到现有的用户。

8.2. 配置 GITHUB 身份提供程序

配置 GitHub 身份提供程序，针对 GitHub 或 GitHub Enterprise 的 OAuth 身份验证服务器验证用户名和密码，并访问 Red Hat OpenShift Service on AWS 集群。OAuth 有助于 Red Hat OpenShift Service on AWS 和 GitHub Enterprise 之间的令牌交换流。

警告

配置 GitHub 身份验证后，用户可以使用 GitHub 凭证在 AWS 上登录 Red Hat OpenShift Service。要防止具有任何 GitHub 用户 ID 的任何人登录到 AWS 集群上的 Red Hat OpenShift Service，您必须将访问权限限制为只有特定 GitHub 机构或团队中的访问权限。

前提条件

- *OAuth 应用程序必须直接由 GitHub 机构管理员在 GitHub 机构设置中创建。*
- *GitHub 机构或团队 在您的 GitHub 帐户中设置。*

流程

1. *在 OpenShift Cluster Manager 中，进入到 Clusters 页面，再选择您需要为其配置身份提供程序的集群。*
2. *点 Access control 选项卡。*
3. *点 Add identity provider。*

注意

您还可以点在集群创建后显示的警告信息中的 Add Oauth 配置 链接来配置身份提供程序。

4. *从下拉菜单中选择 GitHub。*
5. *输入身份提供程序的唯一名称。之后无法更改此名称。*

- *在提供的字段中自动生成 OAuth 回调 URL。您将使用它来注册 GitHub 应用。*

```
https://oauth-openshift.apps.<cluster_name>.
<cluster_domain>/oauth2callback/<idp_provider_name>
```

例如：

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/github
```

6. 在 GitHub 上注册应用程序。

7. 返回到 Red Hat OpenShift Service on AWS，然后从下拉菜单中选择映射方法。在大多数情况下推荐使用 声明。

8. 输入 GitHub 提供的客户端 ID 和客户端 secret。

9. 输入一个主机名。在使用托管 GitHub Enterprise 实例时，必须输入一个主机名。

10. 可选： 您可以指定证书颁发机构 (CA) 文件来验证配置的 GitHub Enterprise URL 的服务器证书。点 Browse 找到并附加 CA 文件到身份提供程序。

11. 选择 Use organizations 或 Use teams 以限制对特定 GitHub 组织或 GitHub 团队的访问。

12. 输入您要限制访问权限的机构或团队的名称。点 Add more 指定用户可以成为用户所属的多个机构或团队。

13. 单击 Confirm。

验证

- 配置的身份提供程序可以在 Cluster details 页面的 Access control 选项卡中看到。

8.3. 配置 GITLAB 身份提供程序

配置 GitLab 身份提供程序，以使用 GitLab.com 或任何其他 GitLab 实例作为身份提供程序。

前提条件

- 如果使用 GitLab 版本 7.7.0 到 11.0，您可以使用 OAuth 集成进行连接。如果使用 GitLab 版本 11.1 或更高版本，您可以使用 OpenID Connect (OIDC) 进行连接，而不使用 OAuth。

流程

1. 在 OpenShift Cluster Manager 中，进入到 Clusters 页面，再选择您需要为其配置身份提供程序的集群。

2. 点 Access control 选项卡。

3. 点 Add identity provider。

注意

您还可以点在集群创建后显示的警告信息中的 Add Oauth 配置 链接来配置身份提供程序。

4. 从下拉菜单中选择 GitLab。

5. 输入身份提供程序的唯一名称。之后无法更改此名称。

- 在提供的字段中自动生成 OAuth 回调 URL。您将提供此 URL 到 GitLab。

```
https://oauth-openshift.apps.<cluster_name>.
<cluster_domain>/oauth2callback/<idp_provider_name>
```

例如：

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/gitlab
```

6. 在 GitLab 中添加新应用程序。

7. 返回到 Red Hat OpenShift Service on AWS，然后从下拉菜单中选择映射方法。在大多数情况下推荐使用 声明。

8. 输入 GitLab 提供的客户端 ID 和客户端 secret。

9.

9. 输入 GitLab 供应商的 URL。

10. 可选：您可以使用证书颁发机构 (CA) 文件来验证配置的 GitLab URL 的服务器证书。点 Browse 找到并附加 CA 文件到身份提供程序。

11. 单击 Confirm。

验证

- 配置的身份提供程序可以在 Cluster details 页面的 Access control 选项卡中看到。

8.4. 配置 GOOGLE 身份提供程序

配置 Google 身份提供程序，以便用户通过 Google 凭证进行身份验证。

警告

使用 Google 作为身份提供程序时，任何 Google 用户都能与您的服务器进行身份验证。您可以使用 hostedDomain 配置属性，将身份验证限制为特定托管域的成员。

流程

1. 在 OpenShift Cluster Manager 中，进入到 Clusters 页面，再选择您需要为其配置身份提供程序的集群。

2. 点 Access control 选项卡。

3. 点 Add identity provider。

注意

您还可以点在集群创建后显示的警告信息中的 **Add Oauth 配置** 链接来配置身份提供程序。

4. 从下拉菜单中选择 **Google**。

5. 输入身份提供程序的唯一名称。之后无法更改此名称。

- 在提供的字段中自动生成 **OAuth 回调 URL**。您将为 **Google** 提供此 **URL**。

```
https://oauth-openshift.apps.<cluster_name>.
<cluster_domain>/oauth2callback/<idp_provider_name>
```

例如：

```
https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/google
```

6. 使用 Google's OpenID Connect integration 配置 **Google** 身份提供程序。

7. 返回到 **Red Hat OpenShift Service on AWS**，然后从下拉菜单中选择映射方法。在大多数情况下推荐使用 **声明**。

8. 输入注册 **Google** 项目的客户端 **ID**，以及 **Google** 发布的客户端 **secret**。

9. 输入托管域，将用户限制到 **Google Apps** 域。

10. 单击 **Confirm**。

验证

- 配置的身份提供程序可以在 **Cluster details** 页面的 **Access control** 选项卡中看到。

8.5. 配置 LDAP 身份提供程序

配置 LDAP 身份提供程序，以使用简单绑定身份验证针对 LDAPv3 服务器验证用户名和密码。

前提条件

- *在配置 LDAP 身份提供程序时，您需要输入配置的 LDAP URL。配置的 URL 是 RFC 2255 URL，指定要使用的 LDAP 主机和搜索参数。URL 的语法是：*

```
ldap://host:port/basedn?attribute?scope?filter
```

URL 组件	描述
ldap	对于常规 LDAP，使用 **ldap** 字符串。对于安全 LDAP (LDAPS)，改为使用 **ldaps**。
host:port	LDAP 服务器的名称和端口。LDAP 默认为 **localhost:389**，LDAPS 则默认为 **localhost:636**。
basedn	所有搜索都应从中开始的目录分支的 DN。至少，这必须是目录树的顶端，但也可指定目录中的子树。
attribute	要搜索的属性。虽然 RFC 2255 允许使用逗号分隔属性列表，但无论提供多少个属性，都仅使用第一个属性。如果没有提供任何属性，则默认使用 **uid**。建议选择一个在您使用的子树中的所有条目间是唯一的属性。
scope	搜索的范围。可以是 **one** 或 **sub**。如果未提供范围，则默认使用 **sub** 范围。
filter	有效的 LDAP 搜索过滤器。如果未提供，则默认为 **(objectClass=*)**

在进行搜索时，属性、过滤器和提供的用户名会组合在一起，创建类似如下的搜索过滤器：

```
(&(<filter>)(<attribute>=<username>))
```

重要

如果 LDAP 目录需要身份验证才能搜索，请指定用于执行条目搜索的 bindDN 和 bindPassword。

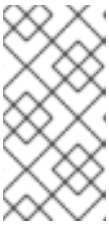
流程

1.

在 OpenShift Cluster Manager 中，进入到 Clusters 页面，再选择您需要为其配置身份提供程序的集群。

2. 点 Access control 选项卡。

3. 点 Add identity provider。



注意

您还可以点在集群创建后显示的警告信息中的 Add Oauth 配置 链接来配置身份提供程序。

4. 从下拉菜单中选择 LDAP。

5. 输入身份提供程序的唯一名称。之后无法更改此名称。

6. 从下拉菜单中选择映射方法。在大多数情况下推荐使用 声明。

7. 输入 LDAP URL 以指定要使用的 LDAP 搜索参数。

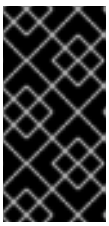
8. 可选：输入 绑定 DN 和 绑定密码。

9. 输入将 LDAP 属性映射到身份的属性。

   - 输入 ID 属性，其值应用作用户 ID。点 Add more 来添加多个 ID 属性。
   - 可选：输入一个 Preferred username 属性，其值应用作显示名称。点 Add more 来添加多个首选用户名属性。
   - 可选：输入 Email 属性，其值应用作电子邮件地址。点 Add more 来添加多个电子邮件属性。

10. 可选：点 Show advanced Options 将证书颁发机构 (CA) 文件添加到 LDAP 身份提供程序中，以验证所配置 URL 的服务器证书。点 Browse 找到并附加 CA 文件到身份提供程序。

11. 可选：在高级选项下，您可以选择使 LDAP 供应商不安全。如果您选择这个选项，则无法使用 CA 文件。



重要

如果您使用不安全的 LDAP 连接（ldap:// 或端口 389），则必须在配置向导中检查 Insecure 选项。

12. 单击 Confirm。

验证

- 配置的身份提供程序可以在 Cluster details 页面的 Access control 选项卡中看到。

8.6. 配置 OPENID 身份提供程序

配置 OpenID 身份提供程序，以使用授权代码流与 OpenID Connect 身份提供程序集成。

重要

Red Hat OpenShift Service on AWS 中的 Authentication Operator 要求配置的 OpenID Connect 身份提供程序实现 OpenID Connect Discovery 规格。

声明可读取自从 OpenID 身份提供程序返回的 JWT id_token；若有指定，也可读取自从 Issuer URL 返回的 JSON。

必须至少配置一个声明，以用作用户的身份。

您还可以指定将哪些声明用作用户的首选用户名、显示名称和电子邮件地址。如果指定了多个声明，则使用第一个带有非空值的声明。标准的声明是：

声明	描述
preferred_username	置备用户时的首选用户名。用户希望使用的简写名称，如 **janedoe**。通常，与身份验证系统中用户的登录或用户名对应的值，如用户名或电子邮件。
email	电子邮件地址。
name	显示名称。

如需更多信息，请参阅 OpenID 声明文档。

前提条件

- *在配置 OpenID Connect 前，请查看您要用于 Red Hat OpenShift Service on AWS 集群的任何红帽产品或服务的安装先决条件。*

流程

1. *在 OpenShift Cluster Manager 中，进入到 Clusters 页面，再选择您需要为其配置身份提供程序的集群。*
2. *点 Access control 选项卡。*
3. *点 Add identity provider。*

注意

您还可以点在集群创建后显示的警告信息中的 Add Oauth 配置 链接来配置身份提供程序。

4. *从下拉菜单中选择 OpenID。*
5. *输入身份提供程序的唯一名称。之后无法更改此名称。*

- *在提供的字段中自动生成 OAuth 回调 URL。*

> *https://oauth-openshift.apps.<cluster_name>.*
> *<cluster_domain>/oauth2callback/<idp_provider_name>*

例如：

> *https://oauth-openshift.apps.openshift-cluster.example.com/oauth2callback/openid*

6. ***按照 创建授权请求 的步骤在 OpenID 身份提供程序中注册新的 OpenID Connect 客户端。***

7. ***返回到 Red Hat OpenShift Service on AWS，然后从下拉菜单中选择映射方法。在大多数情况下推荐使用 声明。***

8. ***输入 OpenID 提供的客户端 ID 和客户端 secret。***

9. ***输入 Issuer URL。这是 OpenID 供应商断言为 Issuer 标识符的 URL。它必须使用没有 URL 查询参数或片段的 https 方案。***

10. ***输入 Email 属性，其值应用作电子邮件地址。点 Add more 来添加多个电子邮件属性。***

11. ***输入 Name 属性，其值应用作首选用户名。点 Add more 来添加多个首选用户名。***

12. ***输入 Preferred username 属性，其值应用作显示名称。点 Add more 来添加多个显示名称。***

13. ***可选：点 Show advanced Options 将证书颁发机构 (CA) 文件添加到 OpenID 身份提供程序中。***

14. ***可选：在高级选项下，您可以添加 其他范围。默认情况下，请求 OpenID 范围。***

15. ***单击 Confirm。***

验证

- 配置的身份提供程序可以在 Cluster details 页面的 Access control 选项卡中看到。

8.7. 配置 HTPASSWD 身份提供程序

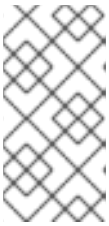
配置 htpasswd 身份提供程序，以创建具有集群管理特权的单个静态用户。您可以以用户身份登录集群来排除问题。

重要

htpasswd 身份提供程序选项仅用于创建单一静态管理用户。htpasswd 不支持作为 Red Hat OpenShift Service on AWS 的通用身份提供程序。

流程

1. 在 OpenShift Cluster Manager 中，进入到 Clusters 页面并选择您的集群。
2. 选择 Access control → Identity provider。
3. 点 Add identity provider。
4. 从 Identity Provider 下拉菜单中选择 HTPasswd。
5. 在身份提供程序的 Name 字段中添加唯一名称。
6. 为静态用户使用推荐的用户名和密码，或者自行创建。



注意

在以下步骤中选择 Add 后，此步骤中定义的凭证不可见。如果丢失了凭证，您必须重新创建身份提供程序并再次定义凭证。

7. 选择 Add 来创建 htpasswd 身份提供程序和单一静态用户。

8. 授予静态用户权限来管理集群：

   a. 在 Access control → Cluster Roles and Access 下，选择 Add user。

   b. 输入您在上一步中创建的静态用户的用户 ID。

   c. 选择一个 组。dedicated-admins 组中的用户具有 Red Hat OpenShift Service on AWS 的标准管理特权。cluster-admins 组中的用户对集群具有完全的管理访问权限。

   d. 选择 Add user 为用户授予管理权限。

验证

- 配置的 htpasswd 身份提供程序在 Access control → Identity provider 页面中可见。

注意

创建身份提供程序后，同步通常在两分钟内完成。您可以在 htpasswd 身份提供程序可用后以用户身份登录集群。

- 单、管理用户在 Access control → Cluster Roles 和 Access 页面中可见。也会显示用户的管理组成员资格。

8.8. 其他资源

- 访问集群
- 了解使用 STS 部署工作流的 ROSA

第 9 章 撤销对 ROSA 集群的访问

身份提供程序(IDP)控制对 AWS (ROSA)集群上的 Red Hat OpenShift Service 的访问。要撤销用户对集群的访问，您必须在为身份验证设置的 IDP 中配置。

9.1. 使用 ROSA CLI 撤销管理员访问权限

您可以撤销用户的管理员访问权限，以便在没有管理员特权的情况下访问集群。要删除用户的管理员访问权限，您必须撤销 dedicated-admin 或 cluster-admin 权限。您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI、rosa 或 OpenShift Cluster Manager 控制台撤销管理员特权。

9.1.1. 使用 ROSA CLI 撤销 dedicated-admin 访问

如果您是创建集群、机构管理员用户或超级用户用户的用户，您可以撤销 dedicated-admin 用户的访问权限。

前提条件

- 您已在集群中添加身份提供程序(IDP)。
- 您有 IDP 用户名，用于撤销其权限的用户。
- 已登陆到集群。

流程

1. 输入以下命令撤销用户的 dedicated-admin 访问权限：

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

2. 输入以下命令验证您的用户是否不再具有 dedicated-admin 访问权限。输出不会列出撤销的用户。

```
$ oc get groups dedicated-admins
```

9.1.2. 使用 ROSA CLI 撤销 cluster-admin 访问

只有创建集群的用户才能撤销 cluster-admin 用户的访问权限。

前提条件

- 您已在集群中添加身份提供程序(IDP)。
- 您有 IDP 用户名，用于撤销其权限的用户。
- 已登陆到集群。

流程

1. 输入以下命令撤销用户的 cluster-admin 访问权限：

```
$ rosa revoke user cluster-admins --user=myusername --cluster=mycluster
```

2. 输入以下命令验证用户是否不再具有 cluster-admin 访问权限。输出不会列出撤销的用户。

```
$ oc get groups cluster-admins
```

9.2. 使用 OPENSHIFT CLUSTER MANAGER 控制台撤销管理员访问权限

您可以通过 OpenShift Cluster Manager 控制台撤销用户的 dedicated-admin 或 cluster-admin 访问权限。用户可以在没有管理员特权的情况下访问集群。

前提条件

- 您已在集群中添加身份提供程序(IDP)。
- 您有 IDP 用户名，用于撤销其权限的用户。
- 您使用用于创建集群的 OpenShift Cluster Manager 帐户、机构管理员用户或超级用户登录到 OpenShift Cluster Manager 控制台。

流程

1. *在 OpenShift Cluster Manager 的 Clusters 选项卡中，选择集群名称来查看集群详情。*

2. *选择 Access control > Cluster Roles and Access。*

3. *对于您要删除的用户，点用户和组组合右侧的 Options 菜单*

，并点 Delete。

第 10 章 删除 ROSA 集群

本文档提供了删除使用 AWS 安全令牌服务 (STS) 的 Red Hat OpenShift Service on AWS (ROSA) 集群的步骤。删除集群后，您还可以删除集群使用的 AWS Identity and Access Management (IAM)资源。

10.1. 前提条件

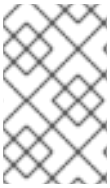
- 如果 Red Hat OpenShift Service on AWS 创建了一个 VPC，则必须从集群中删除以下项目，然后才能成功删除集群：
  - 网络配置，如 VPN 配置和 VPC 对等连接
  - 添加到 VPC 的任何其他服务

如果这些配置和服务仍然存在，集群不会正确删除。

10.2. 删除 ROSA 集群和特定于集群的 IAM 资源

您可以使用 ROSA CLI (rosa) 或 Red Hat OpenShift Cluster Manager 删除使用 AWS 安全令牌服务 (STS) 的 Red Hat OpenShift Service on AWS (ROSA) 集群。

删除集群后，您可以使用 ROSA CLI (rosa) 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。时间量取决于附加组件的数量和大小。

重要

如果在安装过程中创建 VPC 的集群被删除，相关的安装程序创建的 VPC 也会被删除，从而导致所有使用同一 VPC 的集群失败。另外，任何使用由安装程序创建的资源相同的 tagSet 键值对创建的，且带有值为 owned 的标签的资源也会被删除。

前提条件

- 已安装 ROSA 集群。
- 您已在安装主机上安装并配置了最新的 ROSA CLI (rosa)。

流程

1. 获取集群 ID、特定于集群 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> 1
```

1 将 <cluster_name> 替换为集群的名称。

输出示例

```
Name:                       mycluster
ID:                         1s3v4x39lhs8sm49m90mi0822o34544a 1
...
Operator IAM Roles: 2
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-machine-api-aws-cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cloud-credential-operator-cloud-crede
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-image-registry-installer-cloud-creden
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-ingress-operator-cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cluster-csi-drivers-ebs-cloud-credent
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cloud-network-config-controller-cloud
State:                      ready
```

```
Private:                No
Created:                May 13 2022 11:26:15 UTC
Details Page:
https://console.redhat.com/openshift/details/s/296kyEFwzoy1CREQicFRdZybrc0
OIDC Endpoint URL:      https://oidc.op1.openshiftapps.com/<oidc_config_id> 3
```

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

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

2. 删除集群：

- 使用 Red Hat OpenShift Cluster Manager 删除集群：

a. 导航到 OpenShift Cluster Manager。

b. 点集群

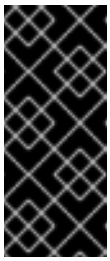
旁边的 Options 菜单并选择 Delete cluster。

c. 在提示符处键入集群名称并点 Delete。

- 使用 ROSA CLI (rosa)删除集群：

a. 输入以下命令删除集群并观察日志，将 < cluster_name& gt; 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。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。

3. 删除集群 Operator 用于身份验证的 OIDC 供应商：

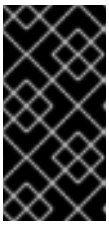
```
$ rosa delete oidc-provider -c <cluster_id> --mode auto 1
```

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。

4. 可选。删除特定于集群的 Operator IAM 角色：



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。

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

-

1

将 <cluster_id> 替换为集群的 ID。

故障排除

- 如果因为缺少 IAM 角色而无法删除 集群，请参阅 额外修复无法删除的集群。
- 如果因为其他原因无法删除集群：
  - 检查 混合云控制台中 是否有待处理的集群的附加组件。
  - 检查 Amazon Web 控制台中是否删除了所有 AWS 资源和依赖项。

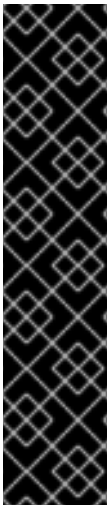
其他资源

- 有关删除帐户范围的 IAM 角色和策略的步骤，请参阅 删除帐户范围内的 IAM 角色和策略。
- 有关删除 OpenShift Cluster Manager 和用户 IAM 角色的步骤，请参阅 取消链接和删除 OpenShift Cluster Manager 和用户 IAM 角色。

10.3. 删除集群范围的 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。



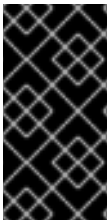
重要

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 "。

10.3.1. 删除集群范围的 IAM 角色和策略

本节提供了删除您为使用 STS ROSA 使用 HCP 部署的 ROSA 创建的账户范围的 IAM 角色和策略，以及帐户范围内的 Operator 策略的步骤。只有在删除所有带有 AWS Security Token Services (STS) ROSA 的 Red Hat OpenShift Service on AWS (ROSA)的 Red Hat OpenShift Service on AWS (ROSA) ROSA 后，才可以删除账户范围的 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 帐户的 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。

前提条件

- 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

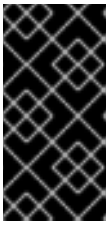
```
I: Fetching account roles
ROLE NAME                          ROLE TYPE      ROLE ARN
OPENSHIFT VERSION
ManagedOpenShift-ControlPlane-Role  Control plane  arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-ControlPlane-Role  4.10
ManagedOpenShift-Installer-Role     Installer      arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Installer-Role     4.10
ManagedOpenShift-Support-Role       Support        arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Support-Role       4.10
ManagedOpenShift-Worker-Role        Worker         arn:aws:iam::
<aws_account_id>:role/ManagedOpenShift-Worker-Role        4.10
```

```
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
```

a. *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
```

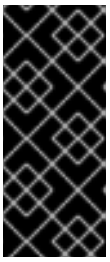
1. 删除集群范围的内行和 Operator 策略：

b. 在 AWS IAM 控制台中的 Policies 页面中，根据您在创建帐户范围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。

c. 使用 AWS IAM 控制台删除集群范围的内行策略和 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。

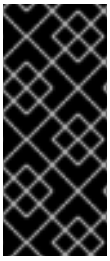


重要

帐户范围的 in-line 和 Operator IAM 策略可能被同一 AWS 帐户中的带有 HCP 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。

10.3.2. 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。

前提条件

- *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 OpenShift Cluster Manager IAM 角色的 Amazon Resource Name (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 Resource Name (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。

10.4. 其他资源

- 有关集群删除保护功能的详情，请参考 编辑对象。
- 有关使用 STS 的 ROSA 集群的 AWS IAM 资源的信息，请参阅关于使用 STS 的 ROSA 集群的 IAM 资源。
- 有关因为缺少 IAM 角色的集群错误的信息，请参阅 修复无法删除的集群。

第 11 章 在不使用 AWS STS 的情况下部署 ROSA

11.1. ROSA 的 AWS 先决条件

Red Hat OpenShift Service on AWS (ROSA)提供了一个模型，它允许红帽将集群部署到客户的现有 Amazon Web Service (AWS)帐户中。

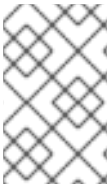
您必须确保在安装 ROSA 前满足先决条件。此要求文档不适用于 AWS 安全令牌服务(STS)。如果使用 STS，请参阅 STS 特定要求。

提示

AWS 安全令牌服务 (STS) 是推荐的凭证模式，用于安装 Red Hat OpenShift Service on AWS (ROSA) 集群并与之交互，因为它提供了增强的安全性。

11.1.1. 客户需求

在部署前，Red Hat OpenShift Service on AWS (ROSA)集群必须满足几个先决条件。

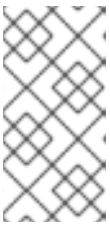


注意

要创建集群，用户必须以 IAM 用户身份登录，而不是假定的角色或 STS 用户。

11.1.1.1. 帐户

- 客户可确保 AWS limits 足以支持在客户 AWS 帐户中置备 Red Hat OpenShift Service on AWS。
- 客户的 AWS 帐户应该位于客户具有适用服务控制策略 (SCP) 的 AWS 机构中。



注意

不要求客户的帐户位于 AWS 机构内或要应用的 SCP，但红帽必须能够在不限制限制的情况下执行 SCP 中列出的所有操作。

- 客户的 AWS 帐户不能转移到红帽。
- 客户可能不会对红帽活动施加 AWS 使用限制。受损限制将严重阻碍红帽响应事件的能力。
- 客户可以在同一 AWS 帐户内部署原生 AWS 服务。

注意

我们鼓励用户（但不强制）在 Virtual Private Cloud (VPC)中部署与 Red Hat OpenShift Service on AWS 和其他红帽支持服务的 VPC 中的资源。

11.1.1.2. 访问要求

- 要在 AWS 服务上正确管理 Red Hat OpenShift Service，红帽始终必须将 AdministratorAccess 策略应用到管理员角色。如果您使用 AWS 安全令牌服务(STS)，则此要求 不适用。

注意

此策略只为红帽提供更改客户提供的 AWS 帐户中资源的权限和功能。

- 红帽必须具有 AWS 控制台访问客户提供的 AWS 帐户。此访问受红帽保护和管理。
- 客户不得使用 AWS 帐户在 Red Hat OpenShift Service on AWS 集群中提升其权限。
- Red Hat OpenShift Service on AWS (ROSA) CLI、rosa 或 OpenShift Cluster Manager 控制台中提供的操作不能直接在客户的 AWS 帐户中执行。

11.1.1.3. 支持要求

- 红帽建议客户从 AWS 至少有 业务支持。
- 红帽有权代表他们要求 AWS 支持。

- 红帽有客户授权来请求 AWS 资源限制来增加客户的帐户。

- 除非本要求部分中另有指定，否则红帽以相同的方式管理所有 Red Hat OpenShift Service on AWS 集群的限制、预期和默认值。

11.1.1.4. 安全要求

- 卷快照将保留在客户的 AWS 帐户和客户指定的区域。

- 红帽必须具有来自允许 IP 地址的对 EC2 主机和 API 服务器的入口访问权限。

- 红帽必须有出口状态，才能将系统和审计日志转发到红帽管理的中央日志记录堆栈。

11.1.2. 所需的客户流程

在部署 Red Hat OpenShift Service on AWS (ROSA)前完成这些步骤。

流程

1. 如果您作为客户使用 AWS 机构，那么您必须在您的机构中使用 AWS 帐户或 创建新帐户。

2. 为确保红帽可以执行必要的操作，您必须创建一个服务控制策略(SCP)，或者确保 none 应用到 AWS 帐户。

3. 将 SCP 附加到 AWS 帐户。

4. 按照设置环境的 ROSA 步骤进行操作。

11.1.2.1. 服务控制策略的最小有效权限集(SCP)

服务控制策略(SCP)是一种机构策略类型，可管理您的机构中的权限。SCP 可确保您机构中的帐户保留在您定义的访问控制指南中。这些策略在 AWS 机构中维护，并控制附加的 AWS 帐户中可用的服务。SCP 管理是客户的职责。

注意

使用 AWS 安全令牌服务(STS)时，最低 SCP 要求不适用。有关 STS 的更多信息，请参阅使用 STS 的 ROSA 的 AWS 先决条件。

验证您的服务控制策略(SCP)是否不限制任何这些所需的权限。

	Service	Actions	效果
必需	Amazon EC2	All	Allow
	Amazon EC2 自动扩展	All	Allow
	Amazon S3	All	Allow
	身份和访问管理	All	Allow
	Elastic Load Balancing	All	Allow
	Elastic Load Balancing V2	All	Allow
	Amazon CloudWatch	All	Allow
	Amazon CloudWatch Events	All	Allow
	Amazon CloudWatch Logs	All	Allow
	AWS EC2 实例连接	SendSerialConsoleSSH PublicKey	Allow
	AWS Support	All	Allow
	AWS 密钥管理服务	All	Allow
	AWS 安全令牌服务	All	Allow
	AWS Tiro	CreateQuery GetQueryAnswer GetQueryExplanation	Allow

	Service	Actions	效果
	AWS Marketplace	Subscription 取消订阅 查看订阅	Allow
	AWS Resource Tagging	All	Allow
	AWS Route53 DNS	All	Allow
	AWS Service Quotas	ListServices GetRequestedServiceQuotaChange GetServiceQuota RequestServiceQuotaIncrease ListServiceQuotas	Allow
选填	AWS Billing	ViewAccount Viewbilling ViewUsage	Allow
	AWS 成本和使用量报告	All	Allow
	AWS Cost Explorer Services	All	Allow

其他资源

- *服务控制策略*
- *SCP 对权限的影响*

11.1.3. Red Hat managed IAM reference for AWS

红帽负责创建和管理以下 Amazon Web Services (AWS)资源：IAM 策略、IAM 用户和 IAM 角色。

11.1.3.1. IAM 策略

注意

IAM 策略会随着 Red Hat OpenShift Service on AWS 的变化而进行修改。

- AdministratorAccess 策略由管理角色使用。此政策为红帽提供了在客户 AWS 帐户中管理 Red Hat OpenShift Service on AWS (ROSA)集群的访问权限。

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

11.1.3.2. IAM 用户

在将 ROSA 安装到客户的 AWS 帐户后，osdManagedAdmin 用户会立即创建。

11.1.4. 置备的 AWS 基础架构

这是在部署的 Red Hat OpenShift Service on AWS (ROSA) 中置备的 Amazon Web Services (AWS) 组件的概述。有关所有置备的 AWS 组件的详细列表，请参阅 OpenShift Container Platform 文档。

11.1.4.1. EC2 实例

在 AWS 公有云中部署 ROSA 的 control plane 和 data plane 功能需要 AWS EC2 实例。

根据 worker 节点数，实例类型可能会因 control plane 和基础架构节点而异。至少会部署以下 EC2 实例：

- 三个 m5.2xlarge control plane 节点
- 两个 r5.xlarge 基础架构节点

- 两个 m5.xlarge 自定义 worker 节点

有关 worker 节点计数的更多信息，请参阅此页面的"Limits and scalability"部分中有关初始规划注意事项的信息。

11.1.4.2. Amazon Elastic Block Store 存储

Amazon Elastic Block Store (Amazon EBS)块存储用于本地节点存储和持久性卷存储。

每个 EC2 实例的卷要求：

- Control Plane 卷
  - 大小：350GB
  - 类型： gp3
  - 每秒输入/输出操作： 1000
- 基础架构卷
  - 大小：300GB
  - 类型： gp3
  - 每秒输入/输出操作：900
- Worker 卷

- 大小：300GB
- 类型： gp3
- 每秒输入/输出操作：900

注意

在 OpenShift Container Platform 4.11 发布前部署的集群默认使用 gp2 类型存储。

11.1.4.3. Elastic Load Balancing

最多两个 Network Load Balancers for API，最多两个 Classic Load Balancers 用于应用程序路由器。如需更多信息，请参阅 AWS 的 ELB 文档。

11.1.4.4. S3 存储

镜像 registry 由 AWS S3 存储支持。定期修剪资源以优化 S3 使用量和集群性能。

注意

需要两个存储桶，每个 bucket 典型的大小为 2TB。

11.1.4.5. VPC

客户应该希望看到每个集群一个 VPC。另外，VPC 需要以下配置：

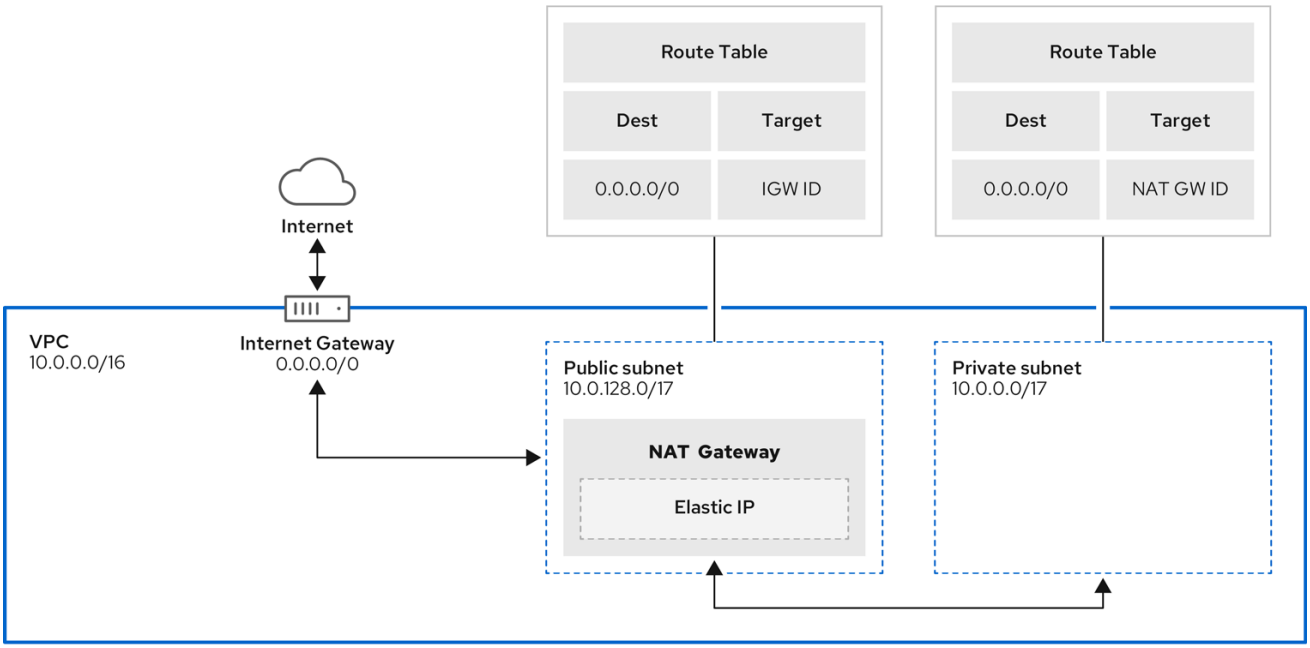
- 子网 ：一个具有单一可用区的集群的两个子网，或具有多个可用区的集群 6 个子网。

注意

公共子网 通过互联网网关直接连接到互联网。专用子网 通过网络地址转换(NAT)网关连接到互联网。

- *路由表 ：每个专用子网一个路由表，每个集群有一个额外的表。*
- *Internet 网关 ：每个集群一个互联网网关。*
- *NAT 网关 ：每个公共子网一个 NAT 网关。*

图 11.1. VPC 架构示例



11.1.4.6. 安全组

AWS 安全组在协议和端口访问级别提供安全性；它们与 EC2 实例和 Elastic Load Balancing (ELB) 负载均衡器关联。每个安全组包含一组规则，这些规则过滤进出一个或多个 EC2 实例的流量。您必须确保在网络上打开 OpenShift 安装所需的端口，并配置为允许主机间的访问。

表 11.1. 默认安全组所需的端口

组	类型	IP 协议	端口范围
MasterSecurityGroup	**AWS::EC2::SecurityGroup**	**icmp**	**0**
		tcp	**22**
		tcp	**6443**

组	类型	IP 协议	端口范围
		tcp	22623
WorkerSecurityGroup	AWS::EC2::Security Group	icmp	0
		tcp	22
BootstrapSecurityGroup	AWS::EC2::Security Group	tcp	22
		tcp	19531

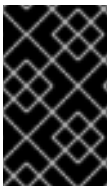
11.1.4.6.1. 其他自定义安全组

当使用现有非管理的 VPC 创建集群时，您可以在集群安装过程中添加额外的自定义安全组。自定义安全组受以下限制：

- 在创建集群时，您必须在 AWS 中创建自定义安全组。如需更多信息，请参阅 适用于 Linux 实例的 Amazon EC2 安全组。
- 您必须将自定义安全组与集群要安装的 VPC 关联。您的自定义安全组不能与另一个 VPC 关联。
- 如果要添加额外的自定义安全组，您可能需要为 VPC 请求额外的配额。有关 ROSA 的 AWS 配额要求的详情，请参考 准备您的环境 中的 必需 AWS 服务配额。有关请求 AWS 配额增加的详情，请参阅 请求配额增加。

11.1.5. AWS 防火墙先决条件

如果您使用防火墙来控制来自 Red Hat OpenShift Service on AWS 的出口流量，您必须配置防火墙以授予对以下特定域和端口组合的访问权限。Red Hat OpenShift Service on AWS 需要此访问权限来提供完全托管的 OpenShift 服务。



重要

只有使用 PrivateLink 部署的 ROSA 集群才能使用防火墙来控制出口流量。

前提条件

-

您已在 AWS Virtual Private Cloud (VPC)中配置了 Amazon S3 网关端点。需要此端点才能完成从集群到 Amazon S3 服务的请求。

流程

1. *允许列出用于安装和下载软件包和工具的以下 URL：*

域	端口	功能
registry.redhat.io	443	提供核心容器镜像。
quay.io	443	提供核心容器镜像。
cdn01.quay.io	443	提供核心容器镜像。
cdn02.quay.io	443	提供核心容器镜像。
cdn03.quay.io	443	提供核心容器镜像。
sso.redhat.com	443	必需。**https://console.redhat.com/openshift** 站点使用来自 **sso.redhat.com** 的身份验证下载 pull secret，并使用 Red Hat SaaS 解决方案来简化订阅、集群清单、计费报告等的监控。
quay-registry.s3.amazonaws.com	443	提供核心容器镜像。
ocm-quay-production-s3.s3.amazonaws.com	443	提供核心容器镜像。
quayio-production-s3.s3.amazonaws.com	443	提供核心容器镜像。
cart-rhcos-ci.s3.amazonaws.com	443	提供 Red Hat Enterprise Linux CoreOS (RHCOS)镜像。
openshift.org	443	提供 Red Hat Enterprise Linux CoreOS (RHCOS)镜像。
registry.access.redhat.com	443	托管存储在 Red Hat Ecosytem Catalog 中的所有容器镜像。另外，registry 提供了对 **odo** CLI 工具的访问，可帮助开发人员在 OpenShift 和 Kubernetes 上进行构建。
access.redhat.com	443	必需。托管容器客户端在从 **registry.access.redhat.com** 中拉取镜像时验证镜像所需的签名存储。

域	端口	功能
registry.connect.redhat.com	443	所有第三方镜像和认证 Operator 都需要。
console.redhat.com	443	必需。允许集群和 OpenShift Console Manager 之间的交互以启用功能，如调度升级。
sso.redhat.com	443	**https://console.redhat.com/openshift** 站点使用来自 **sso.redhat.com**的身份验证
pull.q1w2.quay.rhcloud.com	443	当 quay.io 不可用时，提供核心容器镜像作为回退。
.q1w2.quay.rhcloud.com	443	当 quay.io 不可用时，提供核心容器镜像作为回退。
www.okd.io	443	**openshift.org** 站点通过 **www.okd.io** 重定向。
www.redhat.com	443	**sso.redhat.com** 站点通过 **www.redhat.com** 重定向。
aws.amazon.com	443	**iam.amazonaws.com** 和 **sts.amazonaws.com** 站点通过 **aws.amazon.com** 重定向。
catalog.redhat.com	443	**registry.access.redhat.com** 和 **https://registry.redhat.io** 站点通过 **catalog.redhat.com** 重定向。
dvbwgdztaeq9o.cloudfront.net [1]	443	ROSA 用于带有管理的 OIDC 配置的 STS 实现。

1. ***如果 cloudfront.net 前面有一个主要云前端中断需要重定向资源，则字母数字字符的字符串可能会改变。***

2. ***将以下遥测 URL 列入允许列表：***

域	端口	功能
cert-api.access.redhat.com	443	遥测是必需的。
api.access.redhat.com	443	遥测是必需的。
infogw.api.openshift.com	443	遥测是必需的。

域	端口	功能
console.redhat.com	443	遥测和 Red Hat Insights 需要。
cloud.redhat.com/api/ingress	443	遥测和 Red Hat Insights 需要。
observatorium-mst.api.openshift.com	443	受管 OpenShift 遥测需要。
observatorium.api.openshift.com	443	受管 OpenShift 遥测需要。

受管集群需要启用遥测功能，以便红帽可以更快地对问题做出反应，更好地支持客户，并更好地了解产品升级对集群的影响。有关红帽如何使用远程健康监控数据的更多信息，请参阅附加资源部分 关于远程健康监控 的信息。

3. *允许以下 **Amazon Web Services (AWS) API URIs**：*

域	端口	功能
.amazonaws.com	443	需要此项以访问 AWS 服务和资源。

或者，如果您选择不为 Amazon Web Services (AWS) API 使用通配符，则必须允许列出以下 URL：

域	端口	功能
ec2.amazonaws.com	443	用于在 AWS 环境中安装和管理集群。
events. <aws_region>.amazonaws.com	443	用于在 AWS 环境中安装和管理集群。
iam.amazonaws.com	443	用于在 AWS 环境中安装和管理集群。
route53.amazonaws.com	443	用于在 AWS 环境中安装和管理集群。
sts.amazonaws.com	443	用于在 AWS 环境中安装和管理集群，用于配置为使用 AWS STS 的全局端点。
sts.<aws_region>.amazonaws.com	443	用于在 AWS 环境中安装和管理集群，用于配置为使用 AWS STS 的区域端点的集群。如需更多信息，请参阅 AWS STS 区域端点。

域	端口	功能
tagging.us-east-1.amazonaws.com	443	用于在 AWS 环境中安装和管理集群。此端点始终为 us-east-1，无论集群要部署到的区域。
ec2.<aws_region>.amazonaws.com	443	用于在 AWS 环境中安装和管理集群。
elasticloadbalancing.<aws_region>.amazonaws.com	443	用于在 AWS 环境中安装和管理集群。
servicequotas.<aws_region>.amazonaws.com	443	必需。用于确认用于部署该服务的配额。
tagging.<aws_region>.amazonaws.com	443	允许以标签的形式分配 AWS 资源的元数据。

4. ***将以下 OpenShift URL 列入允许列表：***

域	端口	功能
mirror.openshift.com	443	用于访问镜像安装内容和镜像。此站点也是发行版本镜像签名的来源，但 Cluster Version Operator (CVO)只需要一个可正常工作的源。
storage.googleapis.com/openshift-release (推荐)	443	mirror.openshift.com/ 的替代站点。用于下载集群用来从 quay.io 中拉取哪些镜像的平台发行版本签名。
api.openshift.com	443	用于检查集群是否有可用的更新。

5. ***将以下站点可靠性工程(SRE)和管理 URL 列入允许：***

域	端口	功能
api.pagerduty.com	443	此警报服务由 in-cluster alertmanager 用来发送通知 Red Hat SRE 的事件来执行操作的警报。
events.pagerduty.com	443	此警报服务由 in-cluster alertmanager 用来发送通知 Red Hat SRE 的事件来执行操作的警报。

域	端口	功能
api.deadmanssnitch.com	443	Red Hat OpenShift Service on AWS 用来发送定期 ping 的警报服务，以指示集群是否可用并在运行。
nosnch.in	443	Red Hat OpenShift Service on AWS 用来发送定期 ping 的警报服务，以指示集群是否可用并在运行。
.osdsecuritylogs.categoriescloud.com OR **inputs1.osdsecuritylogs.categoriescloud.com inputs2.osdsecuritylogs.mvapichcloud.com inputs4.osdsecuritylogs.categoriescloud.com inputs5.osdsecuritylogs.categoriescloud.com inputs6.osdsecuritylogs.categoriescloud.com inputs7 .osdsecuritylogs.splunkcloud.cominputs8.osdsecuritylogs.zFCPcloud.com inputs9.osdsecuritylogs.12 inputs10.osdsecuritylogs.osdsecuritylogs.osdsecuritylogs11 inputs10.osdsecuritylogs.osdsecuritycom inputs10.osdsecuritylogs.osdsecuritycominputs.osdsecuritylogs.osd.osdsecuritylogs.osdsecuritycominputs5.osdsecuritylogs.com inputs10.osdsecuritylogs.cominputs10.osdsecuritylogs.osdsecuritylogs.osdsecuritylogs.osdsecuritylogs.com inputs5.osdsecuritylogs.com inputs5.osdsecuritylogs.com inputs6.osdsecuritylogs.com inputs6.osdsecuritylogs.com inputs5.osdsecuritylogs.com inputs10.osdsecuritylogs.cominputs8.osdsecuritylogs.cominputs9.osdsecuritylogs.com inputs5.osdsecuritylogs.com inputs10.osdsecuritylogs.com inputs5.osdsecuritylogs.com inputs10.osdsecuritylogs.cominputs5.osdsecuritylogs.com inputs5.osdsecuritylogs.com inputs6.osdsecuritylogs.com inputs10.osdsecuritylogs.cominputs10.osdsecuritylogs.com inputs10.osdsecuritylogs.com inputs10.osdsecuritylogs.osd.osdsec**	9997	mvapich **-forwarder-operator** 使用为一个日志转发端点，供 Red Hat SRE 用于基于日志的警报。

域	端口	功能
uritylogs.com inputs1.osdsecuritylogs.cominputs1.osdsecuritylogs.com inputs6.osdsecuritylogs.com inputs1.osdsecuritylogs.com inputs1.osdsecuritylogs.cominputs.osdsecuritylogs.osd.osdsecuritylogs.com inputs4.osdsecuritylogs.com inputs5.osdsecuritylogs.cominputs5.osdsecuritylogs.cominputs10.osdsecuritylogs.com inputs10.osdsecuritylogs.com inputs4.osdsecuritylogs.cominputs8.osdsecuritylogs.cominputs8.osdsecuritylogs.com inputs5.osdsecuritylogs.com inputs5.osdsecuritylogs.com inputs6.osdsecuritylogs.cominputs6.osdsecuritylogs.com inputs6.osdsecuritylogs.com inputs6.osdsecuritylogs.com inputs6.osdsecuritylogs.cominputs		
http-inputs-osdsecuritylogs.splunkcloud.com	443	必需。mvapich **-forwarder-operator** 使用为一个日志转发端点，供 Red Hat SRE 用于基于日志的警报。
sftp.access.redhat.com (Recommended)	22	**must-gather-operator** 使用的 SFTP 服务器上传诊断日志，以帮助排除集群中的问题。

6. ***将以下 URL 列入允许的可选第三方内容：***

域	端口	功能
registry.connect.redhat.com	443	所有第三方镜像和认证操作器都需要。
rhc4tp-prod-z8cxf-image-registry-us-east-1-evenkyleffocxqvofrk.s3.dualstack.us-east-1.amazonaws.com	443	提供对托管在 **registry.connect.redhat.com** 上的容器镜像的访问
oso-rhc4tp-docker-registry.s3-us-west-2.amazonaws.com	443	对于 Sonatype Nexus, F5 Big IP operator 是必需的。

7. ***将提供构建所需语言或框架资源的任何站点列入允许列表。***

8. ***允许允许任何依赖于 OpenShift 中使用的语言和框架的出站 URL。如需防火墙或代理上允许的推荐 URL 列表，请参阅 OpenShift 出站 URL。***

其他资源

- *关于远程健康监控*
- *安全组*
- *所需的 AWS 服务配额*

11.1.6. 后续步骤

- *查看所需的 AWS 服务配额*

11.1.7. 其他资源

- *限制和可扩展性*
- *SRE 访问 AWS 集群中的所有 Red Hat OpenShift Service*
- *了解 ROSA 部署工作流*

11.2. 了解 ROSA 部署工作流

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 ROSA 工作流阶段，并引用每个阶段的详细资源。

提示

AWS 安全令牌服务 (STS) 是推荐的凭证模式，用于安装 Red Hat OpenShift Service on AWS (ROSA) 集群并与之交互，因为它提供了增强的安全性。

11.2.1. ROSA 部署工作流概述

您可以按照本节中介绍的工作流阶段设置和访问 Red Hat OpenShift Service on AWS (ROSA)集群。

1. 执行 AWS 的先决条件。要部署 ROSA 集群，您的 AWS 帐户必须满足先决条件要求。
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. 配置 AWS 帐户。在创建 ROSA 集群前，您必须在 AWS 帐户中启用 ROSA，安装和配置 AWS CLI (aws)工具，并验证 AWS CLI 工具配置。
4. 安装 ROSA 和 OpenShift CLI 工具并验证 AWS 服务配额。安装和配置 ROSA CLI (rosa) 和 OpenShift CLI (oc)。您可以使用 ROSA CLI 验证所需的 AWS 资源配额是否可用。
5. 创建 ROSA 集群 或使用 AWS PrivateLink 创建 ROSA 集群。使用 ROSA CLI (rosa)创建集群。您可以选择使用 AWS PrivateLink 创建 ROSA 集群。
6. 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。
7. 撤销对用户 的 ROSA 集群的访问权限。您可以使用 ROSA CLI 或 Web 控制台撤销用户对 ROSA 集群的访问。
8. 删除 ROSA 集群。您可以使用 ROSA CLI (rosa)删除 ROSA 集群。

11.2.2. 其他资源

- 有关使用 ROSA 部署工作流创建使用 AWS STS 的集群的信息，请参阅了解带有 STS 的 ROSA 部署工作流。
- 配置身份提供程序

- 删除集群
- 删除对集群的访问
- 创建集群和用户的命令快速参考

11.3. 所需的 AWS 服务配额

查看此列表，其中列出了在 AWS 集群上运行 Red Hat OpenShift Service on AWS 集群所需的服务配额。

提示

AWS 安全令牌服务 (STS) 是推荐的凭证模式，用于安装 Red Hat OpenShift Service on AWS (ROSA) 集群并与之交互，因为它提供了增强的安全性。

11.3.1. 所需的 AWS 服务配额

下表描述了在 AWS 集群中创建并运行一个 Red Hat OpenShift Service 所需的 AWS 服务配额和级别。虽然大多数默认值适合大多数工作负载，但您可能需要为以下情况请求额外的配额：

- ROSA （经典架构）集群至少需要 AWS EC2 服务配额 100 个 vCPU，以便为集群创建、可用性和升级提供。分配给运行按需标准 Amazon EC2 实例的 vCPU 的默认最大值是 5。因此，如果您之前没有使用同一 AWS 帐户创建 ROSA 集群，则必须请求额外的 EC2 配额来运行 按需标准(A、C、D、H、I、M、R、T、Z)实例。
- 某些可选集群配置功能（如自定义安全组）可能需要您请求额外的配额。例如，因为 ROSA 默认将 1 个安全组与 worker 机器池中的网络接口关联，并且 每个网络接口安全组的默认配额 为 5，如果要添加 5 自定义安全组，您需要请求额外的配额，因为这会将 worker 网络接口上的安全组总数设置为 6。

注意

AWS SDK 允许 ROSA 检查配额，但 AWS SDK 计算不会考虑您现有的用法。因此，配额检查可能会在 AWS SDK 中通过，但集群创建过程可能会失败。要解决这个问题，请提高配额。

如果您需要修改或增加特定配额，请参阅 Amazon 文档中有关请求配额增加的内容。大型配额请求被提交到 Amazon 支持以进行审核，需要一些时间被批准。如果您的配额请求是紧急的，请联系 AWS 支持。

表 11.2. ROSA 需要的服务配额

配额名称	服务代码	配额代码	AWS 默认	最低要求	描述
运行内部标准 (A、C、D、H、I、M、R、T、Z)实例	ec2	L-1216C47A	5	100	分配给 Running On-Demand Standard (A, C, D, H, I, M, R, T, Z)实例的最大 vCPU 数量。 默认值 5 个 vCPU 不足来创建 ROSA 集群。ROSA 的最低要求需要 100 个 vCPU 为集群创建。
通用目的 SSD (gp2)卷存储以 TiB 为单位	ebs	L-D18FCD1D	50	300	此区域中可以在跨 General Purpose SSD (gp2) 卷进行置备的最大聚合存储量（以 TiB 为单位）。
通用目的 SSD (gp3)卷存储以 TiB 为单位	ebs	L-7A658B76	50	300	此区域中可以在跨 General Purpose SSD (gp3) 卷进行置备的最大聚合存储量（以 TiB 为单位）。 300 TiB 存储是最佳性能所需的最低容量。

配额名称	服务代码	配额代码	AWS 默认	最低要求	描述
以 TiB 为单位的置备 IOPS SSD (io1)卷存储	ebs	L-FD252861	50	300	此区域中可以在跨 Provisioned IOPS SSD (io1) 卷进行置备的最大聚合存储量（以 TiB 为单位）。 300 TiB 存储是最佳性能所需的最低容量。

表 11.3. 常规 AWS 服务配额

配额名称	服务代码	配额代码	AWS 默认	最低要求	描述
EC2-VPC Elastic IP	ec2	L-0263D0A3	5	5	在此区域中可以为 EC2-VPC 分配的最大 Elastic IP 地址数量。
每个区域的 VPCs	vpc	L-F678F1CE	5	5	每个区域的 VPC 数量上限。这个配额直接与每个区域互联网网关的最大数量关联。
每个区域的互联网网关	vpc	L-A4707A72	5	5	每个区域的最大互联网网关数量。这个配额直接与每个区域 VPC 数量关联。要增加此配额，请增加每个区域的 VPC 数量。
每个区域的网络接口	vpc	L-DF5E4CA3	5,000	5,000	每个区域的最大网络接口数量。

配额名称	服务代码	配额代码	AWS 默认	最低要求	描述
每个网络接口的安全组	vpc	L-2AFB9258	5	5	每个网络接口的最大安全组数。此配额乘以每个安全组的规则配额，不能超过 1000。
每个区域的快照	ebs	L-309BACF6	10,000	10,000	每个区域的最大快照数
置备 IOPS SSD (Io1)卷的 IOPS	ebs	L-B3A130E6	300,000	300,000	此区域中可在置备 IOPS SDD (io1)卷之间置备的 IOPS 数量上限。
每个区域的应用程序负载均衡	elasticloadbalancing	L-53DA6B97	50	50	每个区域可存在的最大 Application Load Balancer 数量。
每个区域的 Classic Load Balancers	elasticloadbalancing	L-E9E9831D	20	20	每个区域可存在的最大 Classic Load Balancer 数量。

11.3.1.1. 其他资源

- *如何使用 AWS CLI 命令请求、查看和管理服务配额增加请求？*
- *ROSA 服务配额*
- *请求增加配额*

11.3.2. 后续步骤

- *配置 AWS 帐户*

11.3.3. 其他资源

- 了解 ROSA 部署工作流

11.4. 配置 AWS 帐户

完成 AWS 的先决条件后，配置 AWS 帐户并启用 Red Hat OpenShift Service on AWS (ROSA)服务。

提示

AWS 安全令牌服务 (STS) 是推荐的凭证模式，用于安装 Red Hat OpenShift Service on AWS (ROSA) 集群并与之交互，因为它提供了增强的安全性。

11.4.1. 配置 AWS 帐户

要将 AWS 帐户配置为使用 ROSA 服务，请完成以下步骤。

前提条件

- 检查并完成部署先决条件和策略。
- 如果还没有 红帽帐户，请创建一个红帽帐户。然后，检查您的电子邮件中的验证链接。您需要这些凭证来安装 ROSA。

流程

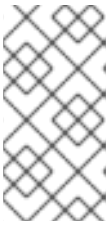
1. 登录到您要使用的 Amazon Web Services (AWS)帐户。

   建议专用 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。

   如果您使用 AWS 机构，且您需要有一个服务控制策略 (SCP) 应用于您计划使用的 AWS 帐户，请参阅 AWS 先决条件。

   作为集群创建过程的一部分，rosa 建立 osdCcsAdmin IAM 用户。此用户使用您在配置

AWS CLI 时提供的 IAM 凭证。



注意

此用户启用了 Programmatic 访问权限，并附加了 AdministratorAccess 策略。

2. *在 AWS 控制台中启用 ROSA 服务。*

   a. *登录您的 AWS 帐户。*

   b. *要启用 ROSA，请转至 ROSA 服务 并选择 Enable OpenShift。*

3. *安装和配置 AWS CLI。*

   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 文件中指定正确的 aws_access_key_id 和 aws_secret_access_key。请参阅 AWS 文档中的 AWS 配置基础知识。

   b. *设置默认 AWS 区域。*

注意

建议使用环境变量来设置默认的 AWS 区域。

ROSA 服务以以下优先级顺序评估区域：

i. *使用 --region 标志运行 rosa 命令时指定的区域。*

ii. *AWS_DEFAULT_REGION 环境变量中设置的区域。请参阅 AWS 文档中的配置 AWS CLI 的环境变量。*

iii. AWS 配置文件中设置的默认区域。请参阅 AWS 文档中的使用 aws 配置的快速配置。

c. 可选：使用名为 profile 的 AWS CLI 设置和凭证配置 AWS CLI 设置和凭证。ROSA 按照以下优先级顺序评估 AWS 命名配置集：

i. 使用 --profile 标志运行 rosa 命令时指定的配置集。

ii. 在 AWS_PROFILE 环境变量中设置的配置集。请参阅 AWS 文档中的 名称配置集。

d. 运行以下命令查询 AWS API 来验证 AWS CLI 是否已正确安装和配置：

```
$ 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>
```

完成这些步骤后，安装 ROSA。

11.4.2. 后续步骤

- 安装 ROSA CLI

11.4.3. 其他资源

- AWS 的先决条件

- 所需的 AWS 服务配额并请求增加
- 了解 ROSA 部署工作流

11.5. 在 AWS (ROSA) CLI 上安装 RED HAT OPENSHIFT SERVICE，ROSA

配置 AWS 帐户后，在 AWS (ROSA) CLI, rosa 处安装和配置 Red Hat OpenShift Service。

提示

AWS 安全令牌服务 (STS) 是推荐的凭证模式，用于安装 Red Hat OpenShift Service on AWS (ROSA) 集群并与之交互，因为它提供了增强的安全性。

11.5.1. 安装和配置 ROSA CLI

在 AWS (ROSA) CLI, rosa 上安装和配置 Red Hat OpenShift Service。您还可以安装 OpenShift CLI (oc)，并使用 ROSA CLI (rosa)验证所需的 AWS 资源配额是否可用。

前提条件

- 检查并完成 AWS 的先决条件和 ROSA 策略。
- 如果还没有 红帽帐户，请创建一个红帽帐户。然后，检查您的电子邮件中的验证链接。您需要这些凭证来安装 ROSA。
- 配置 AWS 帐户并在 AWS 帐户中启用 ROSA 服务。

流程

1. 安装 rosa，Red Hat OpenShift Service on AWS 的命令行接口 (CLI)。
   a. 为您的操作系统下载 ROSA CLI 的最新版本。

b.

可选：命名您下载到 rosa 的可执行文件。本文档使用 rosa 参考可执行文件。

c.

可选：在路径中添加 rosa。

示例

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

d.

输入以下命令验证您的安装：

```
$ rosa
```

输出示例

```
Command line tool for Red Hat OpenShift Service on AWS.
For further documentation visit https://access.redhat.com/documentation/zh-cn/red_hat_openshift_service_on_aws

Usage:
  rosa [command]

Available Commands:
  completion  Generates completion scripts
  create      Create a resource from stdin
  delete      Delete a specific resource
  describe    Show details of a specific resource
  download    Download necessary tools for using your cluster
  edit        Edit a specific resource
  grant       Grant role to a specific resource
  help        Help about any command
  init        Applies templates to support Red Hat OpenShift Service on AWS
  install     Installs a resource into a cluster
  link        Link a ocm/user role from stdin
  list        List all resources of a specific type
  login       Log in to your Red Hat account
  logout      Log out
  logs        Show installation or uninstallation logs for a cluster
  revoke      Revoke role from a specific resource
  uninstall   Uninstalls a resource from a cluster
  unlink      UnLink a ocm/user role from stdin
```

```
  upgrade     Upgrade a resource
  verify      Verify resources are configured correctly for cluster install
  version     Prints the version of the tool
  whoami      Displays user account information

Flags:
      --color string   Surround certain characters with escape sequences to display
them in color on the terminal. Allowed options are [auto never always] (default
"auto")
      --debug          Enable debug mode.
  -h, --help           help for rosa

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

e. 可选：为 ROSA CLI 生成命令完成脚本。以下示例为 Linux 机器生成 Bash 完成脚本：

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

f. 可选：从现有终端中为 ROSA CLI 启用命令完成。以下示例在 Linux 机器上的现有终端中启用 rosa 的 Bash 完成功能：

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

2. 使用 rosa 登录您的红帽帐户。

a. 输入以下命令。

```
$ rosa login
```

b. 将 <my_offline_access_token& gt; 替换为您的令牌。

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: <my-offline-access-token>
```

输出持续示例

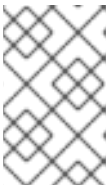
```
I: Logged in as 'rh-rosa-user' on 'https://api.openshift.com'
```

3. *输入以下命令验证您的 AWS 帐户是否有必要权限。*

```
$ rosa verify permissions
```

输出示例

```
I: Validating SCP policies...
I: AWS SCP policies ok
```



注意

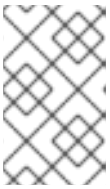
此命令只验证没有使用 AWS 安全令牌服务(STS)的 ROSA 集群的权限。

4. *验证您的 AWS 帐户是否具有在 AWS 集群上部署 Red Hat OpenShift Service 所需的配额。*

```
$ rosa verify quota --region=us-west-2
```

输出示例

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



注意

有时，AWS 配额因区域而异。如果您收到任何错误，请尝试不同的区域。

如果需要提高配额，进入 AWS 控制台，并为失败的服务请求配额增加。

权限和配额检查通过后，继续下一步。

5. 为集群部署准备 AWS 帐户：

a. 运行以下命令验证您的 Red Hat 和 AWS 凭证是否已正确设置。检查 AWS 帐户 ID、默认区域和 ARN 是否与您所期望的内容匹配。您可以安全地忽略以 OCM 开头的行。

```
$ rosa whoami
```

输出示例

```
AWS Account ID:               000000000000
AWS Default Region:           us-east-2
AWS ARN:                      arn:aws:iam::000000000000:user/hello
OCM API:                      https://api.openshift.com
OCM Account ID:               1DzGIdIhqEWyt8UUXQhSoWaaaaa
OCM Account Name:             Your Name
OCM Account Username:         you@domain.com
OCM Account Email:            you@domain.com
OCM Organization ID:          1HopHfA2hcmhup5gCr2uH5aaaaa
OCM Organization Name:        Red Hat
OCM Organization External ID: 0000000
```

b. 初始化 AWS 帐户。此步骤运行一个 CloudFormation 模板，用于准备 AWS 帐户以进行集群部署和管理。此步骤通常需要 1-2 分钟才能完成。

```
$ rosa init
```

输出示例

```
I: Logged in as 'rh-rosa-user' on 'https://api.openshift.com'
I: Validating AWS credentials...
I: AWS credentials are valid!
I: Validating SCP policies...
I: AWS SCP policies ok
I: Validating AWS quota...
I: AWS quota ok
I: Ensuring cluster administrator user 'osdCcsAdmin'...
I: Admin user 'osdCcsAdmin' created successfully!
I: Verifying whether OpenShift command-line tool is available...
E: OpenShift command-line tool is not installed.
Run 'rosa download oc' to download the latest version, then add it to your PATH.
```

6. 从 ROSA CLI 安装 OpenShift CLI (oc)。

   a. 输入这个命令下载 oc CLI 的最新版本：

   ```
   $ rosa download oc
   ```

   b. 下载 oc CLI 后，解压它并将其添加到您的路径中。

   c. 输入这个命令来验证 oc CLI 是否已正确安装：

   ```
   $ rosa verify oc
   ```

安装 ROSA 后，就可以创建集群。

11.5.2. 后续步骤

- 在 ROSA 上创建 ROSA 集群 或创建 AWS PrivateLink 集群。

11.5.3. 其他资源

- AWS 的先决条件
- 所需的 AWS 服务配额并请求增加
- 了解 ROSA 部署工作流

11.6. 创建没有 AWS STS 的 ROSA 集群

设置您的环境并在 AWS (ROSA)上安装 Red Hat OpenShift Service 后，创建一个集群。

本文档论述了如何设置 ROSA 集群。另外，您可以使用 AWS PrivateLink 创建 ROSA 集群。

提示

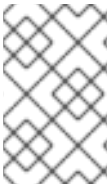
AWS 安全令牌服务 (STS) 是推荐的凭证模式，用于安装 Red Hat OpenShift Service on AWS (ROSA) 集群并与之交互，因为它提供了增强的安全性。

11.6.1. 创建集群

您可以使用 ROSA CLI (rosa)在 AWS (ROSA)集群上创建 Red Hat OpenShift Service。

前提条件

- 已安装 Red Hat OpenShift Service on AWS。



注意

目前，ROSA 安装不支持 AWS 共享 VPC。

流程

1. 您可以使用默认设置或使用互动模式指定自定义设置来创建集群。要在创建集群时查看其他选项，请输入 rosa create cluster --help 命令。

创建集群最多可能需要 40 分钟。

注意

对于生产环境工作负载，建议使用多个可用区(AZ)。默认为单个可用区。使用 --help 来手动设置这个选项，或使用互动模式进行此设置。

- *使用默认集群设置创建集群：*

```
$ rosa create cluster --cluster-name=<cluster_name>
```

输出示例

```
I: Creating cluster with identifier '1de87g7c30g75qechgh7l5b2bha6r04e' and name
'rh-rosa-test-cluster1'
I: To view list of clusters and their status, run `rosa list clusters`
I: Cluster 'rh-rosa-test-cluster1' has been created.
I: Once the cluster is 'Ready' you will need to add an Identity Provider and define
the list of cluster administrators. See `rosa create idp --help` and `rosa create user
--help` for more information.
I: To determine when your cluster is Ready, run `rosa describe cluster rh-rosa-test-
cluster1`.
```

- *使用交互式提示创建集群：*

```
$ rosa create cluster --interactive
```

- *要配置网络 IP 范围，您可以使用以下默认范围。有关使用手动模式时的更多信息，请使用 rosa create cluster --help | grep cidr 命令。在交互模式中，会提示您输入设置。*
  - *节点 CIDR: 10.0.0.0/16*
  - *Service CIDR: 172.30.0.0/16*

- *Pod CIDR: 10.128.0.0/14*

2. *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>
```

输出示例

```
Name: rh-rosa-test-cluster1
OpenShift Version: 4.6.8
DNS: *.example.com
ID: uniqueidnumber
External ID: uniqueexternalidnumber
AWS Account: 123456789101
API URL: https://api.rh-rosa-test-cluster1.example.org:6443
Console URL: https://console-openshift-console.apps.rh-rosa-test-cluster1.example.or
Nodes: Master: 3, Infra: 2, Compute: 2
Region: us-west-2
Multi-AZ: false
State: ready
Channel Group: stable
Private: No
Created: Jan 15 2021 16:30:55 UTC
Details Page: https://console.redhat.com/examplename/details/idnumber
```

注意

如果安装失败，或者 State 字段在 40 分钟后没有变为 ready，请检查安装故障排除文档以了解更多详细信息。

3. *通过观察 OpenShift 安装程序日志来跟踪集群创建的进度：*

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

11.6.2. 后续步骤

配置身份提供程序

11.6.3. 其他资源

- 了解 ROSA 部署工作流
- 删除 ROSA 集群
- ROSA 架构模型

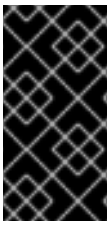
11.7. 配置私有集群

Red Hat OpenShift Service on AWS 集群可以被私有，以便内部应用程序可以托管在公司网络中。另外，私有集群只能配置为只具有内部 API 端点来提高安全性。

可在集群创建期间或建立集群后配置隐私设置。

11.7.1. 在新集群中启用私有集群

您可以在创建新 Red Hat OpenShift Service on AWS 集群时启用私有集群设置。



重要

私有集群不能与 AWS 安全令牌服务(STS)一起使用。但是 STS 支持 AWS PrivateLink 集群。

前提条件

- AWS VPC Peering、VPN、DirectConnect 或 TransitGateway 被配置为允许私有访问。

流程

输入以下命令来创建新私有集群。

```
$ rosa create cluster --cluster-name=<cluster_name> --private
```

注意

或者，使用 --interactive 来为每个集群选项提示。

11.7.2. 在现有集群中启用私有集群

创建集群后，您可以稍后启用集群为私有集群。

重要

私有集群不能与 AWS 安全令牌服务(STS)一起使用。但是 STS 支持 AWS PrivateLink 集群。

前提条件

AWS VPC Peering、VPN、DirectConnect 或 TransitGateway 被配置为允许私有访问。

流程

输入以下命令在现有集群中启用 --private 选项。

```
$ rosa edit cluster --cluster=<cluster_name> --private
```

注意

在私有和公共间迁移集群可能需要几分钟来完成。

11.7.3. 其他资源

- 在 ROSA 上创建 AWS PrivateLink 集群

11.8. 删除对 ROSA 集群的访问

使用 rosa 命令行删除对 AWS (ROSA)集群的 Red Hat OpenShift Service 的访问。

提示

AWS 安全令牌服务 (STS) 是推荐的凭证模式，用于安装 Red Hat OpenShift Service on AWS (ROSA) 集群并与之交互，因为它提供了增强的安全性。

11.8.1. 使用 ROSA CLI 撤销 dedicated-admin 访问

如果您是创建集群、机构管理员用户或超级用户用户的用户，您可以撤销 dedicated-admin 用户的访问权限。

前提条件

- 您已在集群中添加身份提供程序(IDP)。
- 您有 IDP 用户名，用于撤销其权限的用户。
- 已登陆到集群。

流程

1. 输入以下命令撤销用户的 dedicated-admin 访问权限：

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

2. 输入以下命令验证您的用户是否不再具有 dedicated-admin 访问权限。输出不会列出撤销的用户。

```
$ oc get groups dedicated-admins
```

11.8.2. 使用 ROSA CLI 撤销 cluster-admin 访问

只有创建集群的用户才能撤销 cluster-admin 用户的访问权限。

前提条件

- 您已在集群中添加身份提供程序(IDP)。
- 您有 IDP 用户名，用于撤销其权限的用户。
- 已登陆到集群。

流程

1. 输入以下命令撤销用户的 cluster-admin 访问权限：

```
$ rosa revoke user cluster-admins --user=myusername --cluster=mycluster
```

2. 输入以下命令验证用户是否不再具有 cluster-admin 访问权限。输出不会列出撤销的用户。

```
$ oc get groups cluster-admins
```

11.9. 删除 ROSA 集群

使用 rosa 命令行删除 Red Hat OpenShift Service on AWS (ROSA)集群。

提示

AWS 安全令牌服务 (STS) 是推荐的凭证模式，用于安装 Red Hat OpenShift Service on AWS (ROSA) 集群并与之交互，因为它提供了增强的安全性。

11.9.1. 前提条件

- 如果 Red Hat OpenShift Service on AWS 创建了一个 VPC，则必须从集群中删除以下项目，然后才能成功删除集群：
  - 网络配置，如 VPN 配置和 VPC 对等连接
  - 添加到 VPC 的任何其他服务

如果这些配置和服务仍然存在，集群不会正确删除。

11.9.2. 删除 ROSA 集群和特定于集群的 IAM 资源

您可以使用 ROSA CLI (rosa) 或 Red Hat OpenShift Cluster Manager 删除使用 AWS 安全令牌服务 (STS) 的 Red Hat OpenShift Service on AWS (ROSA) 集群。

删除集群后，您可以使用 ROSA CLI (rosa) 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。时间量取决于附加组件的数量和大小。

重要

如果在安装过程中创建 VPC 的集群被删除，相关的安装程序创建的 VPC 也会被删除，从而导致所有使用同一 VPC 的集群失败。另外，任何使用由安装程序创建的资源相同的 tagSet 键值对创建的，且带有值为 owned 的标签的资源也会被删除。

前提条件

- 已安装 ROSA 集群。
- 您已在安装主机上安装并配置了最新的 ROSA CLI (rosa)。

流程

1. 获取集群 ID、特定于集群 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> 1
```

1

将 <cluster_name> 替换为集群的名称。

输出示例

```
Name:                       mycluster
ID:                         1s3v4x39lhs8sm49m90mi0822o34544a 1
...
Operator IAM Roles: 2
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-machine-api-aws-cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cloud-credential-operator-cloud-crede
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-image-registry-installer-cloud-creden
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-ingress-operator-cloud-credentials
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cluster-csi-drivers-ebs-cloud-credent
 - arn:aws:iam::<aws_account_id>:role/mycluster-x4q9-openshift-cloud-network-config-controller-cloud
State:                      ready
Private:                    No
Created:                    May 13 2022 11:26:15 UTC
Details Page:
https://console.redhat.com/openshift/details/s/296kyEFwzoy1CREQicFRdZybrc0
OIDC Endpoint URL:          https://oidc.op1.openshiftapps.com/<oidc_config_id> 3
```

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

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

2. 删除集群：

- 使用 Red Hat OpenShift Cluster Manager 删除集群：

a. 导航到 OpenShift Cluster Manager。

b. 点集群

旁边的 Options 菜单并选择 Delete cluster。

c. 在提示符处键入集群名称并点 Delete。

- 使用 ROSA CLI (rosa)删除集群：

a. 输入以下命令删除集群并观察日志，将 < cluster_name& gt; 替换为集群的名称或 ID：

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

重要

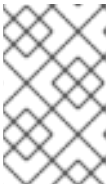
在删除 Operator 角色和 OIDC 供应商前，您必须等待集群删除完成。需要特定于集群的 Operator 角色来清理 OpenShift Operator 创建的资源。Operator 使用 OIDC 供应商进行身份验证。

3. 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

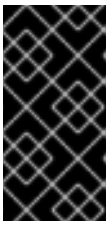
将 <cluster_id> 替换为集群的 ID。



注意

您可以使用 -y 选项，在提示符处自动回答 yes。

4. 可选。删除特定于集群的 Operator IAM 角色：



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。

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

1

将 <cluster_id> 替换为集群的 ID。

故障排除

- 如果因为缺少 IAM 角色而无法删除 集群，请参阅 额外修复无法删除的集群。
- 如果因为其他原因无法删除集群：
  - 检查 混合云控制台中 是否有待处理的集群的附加组件。
  - 检查 Amazon Web 控制台中是否删除了所有 AWS 资源和依赖项。

11.10. 创建集群和用户的命令快速参考

提示

AWS 安全令牌服务 (STS) 是推荐的凭证模式，用于安装 Red Hat OpenShift Service on AWS (ROSA) 集群并与之交互，因为它提供了增强的安全性。

11.10.1. 命令快速参考列表

如果您已经创建了第一个集群和用户，这个列表可在创建其他集群和用户时作为命令快速引用列表。

```
## Configures your AWS account and ensures everything is setup correctly
$ rosa init

## Starts the cluster creation process (~30-40minutes)
$ rosa create cluster --cluster-name=<cluster_name>

## Connect your IDP to your cluster
$ rosa create idp --cluster=<cluster_name> --interactive

## Promotes a user from your IDP to dedicated-admin level
$ rosa grant user dedicated-admin --user=<idp_user_name> --cluster=<cluster_name>

## Checks if your install is ready (look for State: Ready),
## and provides your Console URL to login to the web console.
$ rosa describe cluster --cluster=<cluster_name>
```

11.10.2. 其他资源

- *了解 ROSA 部署工作流*