Red Hat OpenShift Service on AWS 4

准备您的环境

Red Hat OpenShift Service on AWS 的规划、限制和可扩展性

Last Updated: 2024-07-03

Red Hat OpenShift Service on AWS 4 准备您的环境

Red Hat OpenShift Service on AWS 的规划、限制和可扩展性

法律通告

摘要

本文档为 Red Hat OpenShift Service on AWS (ROSA)集群部署提供了规划注意事项，包括集群限值和可扩展性的信息。

目录

第 1 章 使用 STS 部署 ROSA 的先决条件清单

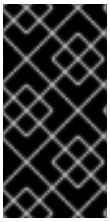
这是使用 STS 创建 Red Hat OpenShift Service on AWS (ROSA)经典集群所需的前提条件清单。

注意

这是高级别清单，您的实施可能会有所不同。

在运行安装过程前，请验证您从可访问的机器中部署它：

- 您置备的云的 API 服务。
- 访问 **api.openshift.com**、**oidc.op1.openshiftapps.com** 和 **sso.redhat.com**。
- 您调配的网络上的主机。
- 用于获取安装介质的互联网。



重要

从 ROSA CLI 版本 1.2.7 开始，新集群中的所有 OIDC 供应商端点 URL 使用 Amazon CloudFront 和 oidc.op1.openshiftapps.com 域。这个变化提高了访问速度，降低延迟，并改进了使用 ROSA CLI 1.2.7 或更高版本创建的新集群的弹性。不支持现有 OIDC 供应商配置的迁移路径。

1.1. 帐户和 CLI 先决条件

您必须安装帐户和 CLI 以部署集群。

1.1.1. AWS 帐户

- 收集以下详情：
  - AWS IAM 用户
  - AWS 访问密钥 ID
  - AWS Secret 访问密钥
- 确保您具有正确的权限，作为 ROSA 的 ROSA 和 About IAM 资源用于使用 STS 的 ROSA 集群的详细权限。
- 如需了解更多详细信息，请参阅 帐户。

1.1.2. AWS CLI (aws)

- 如果还没有从 AWS 命令行界面 安装。
- 配置 CLI：
  1. 在终端中输入 **aws 配置** ：

```
$ aws configure
```

2. 输入 AWS 访问密钥 ID 并按 **输入**。
3. 输入 AWS Secret Access Key 并按 **输入**。
4. 输入您要部署到的默认区域。
5. 输入您想要的输出格式，"table" 或 "json"。
6. 运行以下命令验证输出：

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

7. 运行以下命令，确保 ELB 的服务角色已存在：

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

a. 如果不存在，请运行：

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

1.1.3. 红帽帐户

- 如果还没有创建 Red Hat Hybrid Cloud Console 帐户。

1.1.4. ROSA CLI (rosa)

1. 如果还没有，从 AWS 控制台的 AWS 帐户启用 ROSA。
2. 通过安装 Red Hat OpenShift Service on AWS (ROSA) CLI、rosa 或 OpenShift 控制台 AWS 控制台安装 CLI。
3. 在终端中输入 **rosa 登录**，这将提示您通过控制台进入 令牌页面 ：

```
$ rosa login
```

4. 使用您的红帽帐户凭证登录。
5. 点 **Load token** 按钮。
6. 复制令牌并将其粘贴到 CLI 提示符，然后按 Enter 键。
   - 或者，您可以复制完整的 **$ rosa login --token=abc...** 命令，并在终端中粘贴：

```
$ rosa login --token=<abc..>
```

7. 运行以下命令验证您的凭证：

```
$ rosa whoami
```

8. 运行以下命令确保您有足够的配额：

```
$ rosa verify quota
```

- 有关为 ROSA 集群置备的 AWS 服务的详情，请参阅置备 AWS 基础架构。
- 有关 AWS 服务配额的详情，请参阅所需的 AWS 服务配额。

1.1.5. OpenShift CLI (oc)

1. 通过 OpenShift CLI 或 OpenShift 控制台 命令行界面(CLI) 工具安装。
2. 运行以下命令验证 OpenShift CLI 是否已正确安装：

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

安装并启用了上述先决条件后，继续执行后续步骤。

1.2. SCP 先决条件

ROSA 集群托管在 AWS 机构单元中的 AWS 帐户中。创建 服务控制策略(SCP) 并应用到 AWS 机构单元，以管理 AWS 子帐户可以访问的服务。

- 确保机构的 SCP 不比集群所需的角色和策略更严格。
- 从控制台选择 **启用 ROSA** 时，请确保您的 SCP 配置为允许所需的 **aws-marketplace:Subscribe** 权限，并参阅 AWS Organizations service control policy (SCP)拒绝所需的 AWS Marketplace 权限 以了解更多详细信息。
- 当您创建 ROSA 经典集群时，会创建一个关联的 AWS OpenID Connect (OIDC)身份提供程序。
  - 此 OIDC 供应商配置依赖于位于 **us-east-1** AWS 区域的公钥。
  - 具有 AWS SCP 的客户必须允许使用 **us-east-1** AWS 区域，即使这些集群部署在不同的区域中。

1.3. 网络先决条件

网络的角度来看，需要预备条件。

1.3.1. 防火墙

- 配置防火墙以允许访问 AWS 防火墙先决条件 中列出的域和端口。

1.3.2. 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。在创建集群前完成这些先决条件：

- 在创建集群时，在 AWS 中创建自定义安全组。
- 将自定义安全组与用于创建集群的 VPC 关联。不要将自定义安全组与任何其他 VPC 关联。
- 您可能需要为每个网络接口 为 **安全组** 请求额外的 AWS 配额。

如需了解更多详细信息，请参阅 安全组 的详细要求。

1.3.3. 自定义 DNS

- 如果要使用自定义 DNS，则 ROSA 安装程序必须能够使用带有默认 DHCP 选项的 VPC DNS，以便它可以在本地解析主机。
  - 要做到这一点，运行 **aws ec2 describe-dhcp-options** 并查看 VPC 是否使用 VPC Resolver：

```
$ aws ec2 describe-dhcp-options
```

- 否则，上游 DNS 需要将集群范围转发到这个 VPC，以便集群可以解析内部 IP 和服务。

1.4. PRIVATELINK 先决条件

如果您选择部署 PrivateLink 集群，请确保在预先存在的 BYO VPC 中部署集群：

- 为集群使用的每个 AZ 创建一个公共和私有子网。
  - 或者，使用适当的路由为互联网和出口实施传输网关。
- VPC 的 CIDR 块必须包含 **Networking.MachineCIDR** 范围，这是集群机器的 IP 地址。
  - 子网 CIDR 块必须属于您指定的机器 CIDR。
- 将 **enableDnsHostnames** 和 **enableDnsSupport** 设置为 **true**。
  - 这样，集群可以使用附加到 VPC 的 Route 53 区域来解析集群内部 DNS 记录。
- 运行以下命令验证路由表：

```
----
$ aws ec2 describe-route-tables --filters "Name=vpc-id,Values=<vpc-id>"
----
```

  - 确保集群可以通过公共子网中的 NAT 网关或通过传输网关出站。
  - 确保设置了您要跟随的任何 UDR。
- 您还可以在安装过程中或安装后配置集群范围代理。配置集群范围代理以 了解更多详细信息。

注意

您可以在预先存在的 BYO VPC 中安装非PrivateLink ROSA 集群。

第 2 章 使用 STS 部署 ROSA 的详细要求

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。

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。

在使用 STS 安装 ROSA 前，请确保满足以下 AWS 先决条件。

重要

当使用 AWS STS 创建 ROSA 集群时，也会创建一个关联的 AWS OpenID Connect (OIDC)身份提供程序。此 OIDC 供应商配置依赖于位于 **us-east-1** AWS 区域的公钥。具有 AWS SCP 的客户必须允许使用 **us-east-1** AWS 区域，即使这些集群部署在不同的区域。

2.1. 使用 STS 进行部署时的客户要求

在部署使用 AWS 安全令牌服务(STS)的 Red Hat OpenShift Service on AWS (ROSA)集群前，需要完成以下先决条件。

2.1.1. 帐户

- 您必须确保 AWS 限制足以支持 AWS 帐户中置备的 Red Hat OpenShift Service on AWS。在 CLI 中运行 **rosa verify quota** 命令会验证您是否具有运行集群所需的配额。

注意

配额验证检查 AWS 配额，但不会将您的消耗与 AWS 配额进行比较。如需更多信息，请参阅附加资源中的 "Limits and scalability" 链接。

- 如果应用并强制实施 SCP 策略，则这些策略必须比集群所需的角色和策略更严格。
- 您的 AWS 帐户不能转移到红帽。
- 您应该不会在红帽活动中除定义的角色和策略外增加额外的 AWS 使用量限制。受损限制将严重阻碍红帽响应事件的能力。
- 您可以在同一 AWS 帐户内部署原生 AWS 服务。
- 您的帐户必须设置有 service-linked 角色，因为它需要配置 Elastic Load Balancing (ELB)。有关之前没有在 AWS 帐户中创建负载均衡器的信息，请参阅附加资源中的"创建弹性负载均衡(ELB)服务链接角色"链接角色"。

注意

建议您在 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。

其他资源

- 限制和可扩展性
- 创建 Elastic Load Balancing (ELB) 服务链接的角色

2.1.2. 访问要求

- 红帽必须具有 AWS 控制台访问客户提供的 AWS 帐户。红帽保护和管理此访问。
- 您不能使用 AWS 帐户在 Red Hat OpenShift Service on AWS (ROSA)集群中提升权限。
- ROSA CLI (**rosa**)或 OpenShift Cluster Manager 控制台中可用的操作不能直接在 AWS 帐户中执行。
- 您不需要有一个预配置的域来部署 ROSA 集群。如果要使用自定义域，请参阅附加资源以了解更多信息。

其他资源

- 请参阅 为应用程序配置自定义域

2.1.3. 支持要求

- 红帽建议客户从 AWS 至少有 业务支持。
- 红帽可能有权代表他们请求 AWS 支持。
- 红帽可能拥有客户权限来请求 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。

2.1.4. 安全要求

- 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。
- 红帽必须对记录的域有出口。有关指定域的"AWS 防火墙先决条件"部分。

其他资源

- AWS 防火墙先决条件

2.1.5. 使用 OpenShift Cluster Manager 的要求

以下小节描述了 OpenShift Cluster Manager 的要求。如果您只使用 CLI 工具，您可以忽略要求。

要使用 OpenShift Cluster Manager，您必须链接 AWS 帐户。此链接概念也称为帐户关联。

2.1.5.1. AWS 帐户关联

Red Hat OpenShift Service on AWS (ROSA)集群置备任务需要使用 Amazon Resource Name (ARN)将 **ocm-role** 和 **user-role** IAM 角色链接到 AWS 帐户。

ocm-role ARN 存储为红帽机构中的标签，而 **user-role** ARN 则作为标签存储在红帽用户帐户中。红帽使用这些 ARN 标签来确认用户是有效的帐户拥有者，并可使用正确的权限来执行 AWS 帐户中的必要任务。

2.1.5.2. 链接 AWS 帐户

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa** 将 AWS 帐户链接到现有的 IAM 角色。

前提条件

- 您有一个 AWS 帐户。
- 您可以使用 OpenShift Cluster Manager 创建集群。
- 您有安装 AWS 范围的角色所需的权限。如需更多信息，请参阅本节的"附加资源"。
- 您已在安装主机上安装和配置了最新的 AWS (**aws**) 和 ROSA (**rosa**) CLI。
- 您已创建了 **ocm-role** 和 **user-role** IAM 角色，但还没有将它们链接到 AWS 帐户。您可以运行以下命令来检查您的 IAM 角色是否已链接：

```
$ rosa list ocm-role
```

```
$ rosa list user-role
```

如果这两个角色的 **Linked** 列中显示了 **Yes**，您已将角色链接到 AWS 帐户。

流程

1. 在 CLI 中，使用 Amazon 资源名称(ARN)将 **ocm-role** 资源链接到您的红帽机构：

注意

您必须具有红帽机构管理员权限才能运行 **rosa link** 命令。将 **ocm-role** 资源与 AWS 帐户链接后，对机构的所有用户可见。

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

输出示例

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

2. 在 CLI 中，使用 Amazon 资源名称(ARN)将您的 **user-role** 资源链接到您的红帽用户帐户：

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

输出示例

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

其他资源

- 如需创建 集群所需的 IAM 角色列表，请参阅帐户范围的 IAM 角色和策略引用。

2.1.5.3. 将多个 AWS 帐户与红帽机构相关联

您可以将多个 AWS 帐户与红帽机构相关联。通过关联多个帐户，您可以从红帽机构在 AWS (ROSA)集群上创建 Red Hat OpenShift Service。

使用此功能，您可以使用多个 AWS 配置集作为区域密集型环境在不同的 AWS 区域中创建集群。

前提条件

- 您有一个 AWS 帐户。
- 您可以使用 OpenShift Cluster Manager 创建集群。
- 您有安装 AWS 范围的角色所需的权限。
- 您已在安装主机上安装和配置了最新的 AWS (**aws**) 和 ROSA (**rosa**) CLI。
- 您已创建了 **ocm-role** 和 **user-role** IAM 角色。

流程

要关联一个额外的 AWS 帐户，首先在本地 AWS 配置中创建配置集。然后，通过在其他 AWS 帐户中创建 **ocm-role**、用户帐户角色，将帐户与您的红帽机构相关联。

要在附加区域中创建角色，在运行 **rosa create** 命令时指定 **--profile <aws-profile>** 参数，将 **<aws_profile>** 替换为附加帐户配置集名称：

- 在创建 OpenShift Cluster Manager 角色时指定 AWS 帐户配置集：

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

- 在创建用户角色时指定 AWS 帐户配置集：

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

- 在创建帐户角色时指定 AWS 帐户配置集：

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

注意

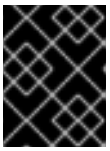
如果没有指定配置集，则使用默认 AWS 配置集。

2.2. 在 OPT-IN 区域部署集群的要求

AWS opt-in 区域是一个默认情况下不启用的区域。如果您需要在一个 opt-in 区域中部署带有 AWS Security Token Service (STS) 的 Red Hat OpenShift Service on AWS (ROSA)，必须满足以下要求：

- 区域必须在 AWS 帐户中启用。有关启用 opt-in 区域的更多信息，请参阅 AWS 文档中的管理 AWS 区域。

- AWS 帐户中的安全令牌版本必须设置为版本 2。对于选择的（opt-in）区域，您将不能使用版本 1 安全令牌。



重要

由于令牌长度增加，到安全令牌版本 2 可能会影响存储令牌的系统。如需更多信息，请参阅有关设置 STS 首选项的 AWS 文档。

2.2.1. 设置 AWS 安全令牌版本

如果要在 AWS opt-in 区域中创建使用 AWS 安全令牌服务(STS) 的 Red Hat OpenShift Service (ROSA) 集群，您必须将安全令牌版本设置为 AWS 帐户中的 2 版本。

前提条件

- 您已在安装主机上安装并配置了最新的 AWS CLI。

流程

1. 列出 AWS CLI 配置中定义的 AWS 帐户 ID：

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

确保输出与相关 AWS 帐户的 ID 匹配。

2. 列出 AWS 帐户中设置的安全令牌版本：

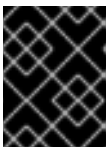
```
$ aws iam get-account-summary --query SummaryMap.GlobalEndpointTokenVersion --output json
```

输出示例

```
1
```

3. 要将 AWS 帐户中的所有区域的安全令牌版本更新为版本 2，请运行以下命令：

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



重要

由于令牌长度增加，到安全令牌版本 2 可能会影响存储令牌的系统。如需更多信息，请参阅有关设置 STS 首选项的 AWS 文档。

2.3. RED HAT MANAGED IAM REFERENCE FOR AWS

使用 STS 部署模型时，红帽不再负责管理 Amazon Web Services (AWS) IAM 策略、IAM 用户或 IAM 角色。有关创建这些角色和策略的详情，请参考 IAM 角色的以下部分。

- 要使用 **ocm** CLI，您必须有一个 **ocm-role** 和 **user-role** 资源。请参阅 OpenShift Cluster Manager IAM 角色资源。
- 如果您有单个集群，请参阅 帐户范围的 IAM 角色和策略参考。

- 对于每个集群，您必须具有必要的 operator 角色。请参阅 特定于 Cluster 的 Operator IAM 角色参考。

2.4. 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。

2.4.1. 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。

2.4.2. 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。

2.4.3. 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。

2.4.4. 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。

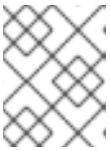
注意

需要两个存储桶，每个 bucket 典型的大小为 2TB。

2.4.5. 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。

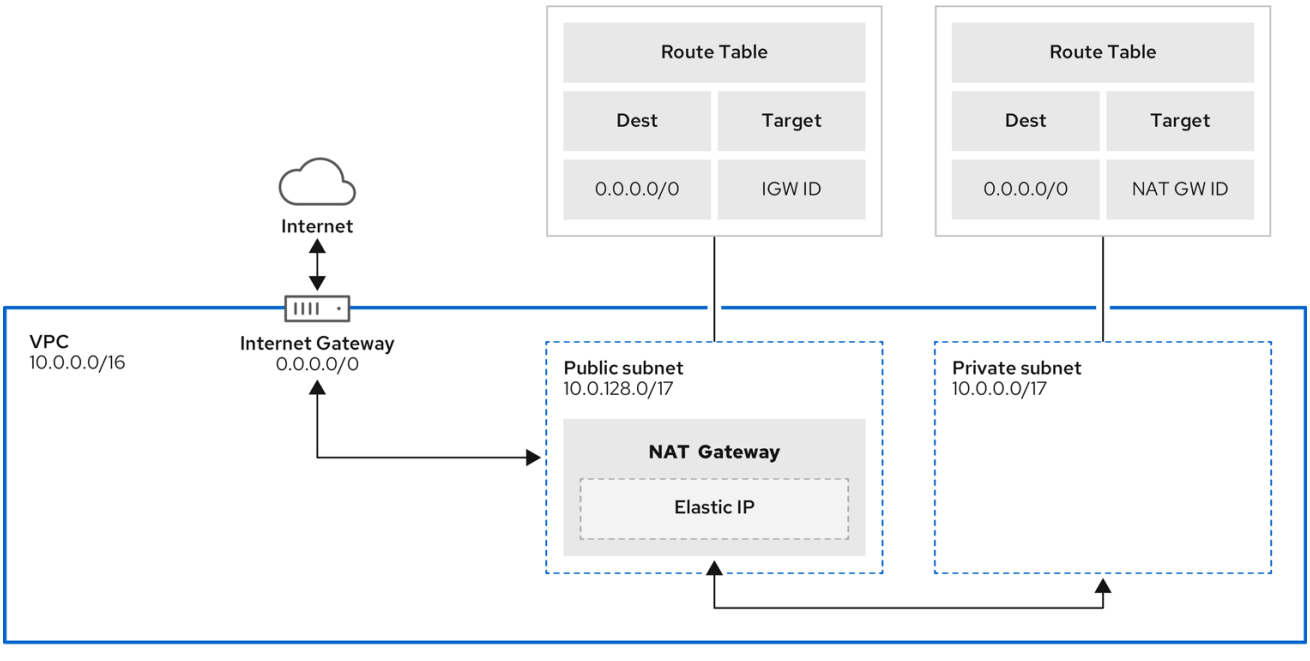


注意

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 2.1. VPC 架构示例



2.4.6. 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 2.1. 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**
		tcp	**22623**
WorkerSecurityGroup	**AWS::EC2::SecurityGroup**	**icmp**	**0**
		tcp	**22**
BootstrapSecurityGroup	**AWS::EC2::SecurityGroup**	**tcp**	**22**
		tcp	**19531**

2.4.6.1. 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。

2.5. 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某些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。

2.5.1. ROSA Classic

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。
time-a-g.nist.gov	123 [2]	允许 FedRAMP 的 NTP 流量。
time-a-wwv.nist.gov	123 [2]	允许 FedRAMP 的 NTP 流量。
time-a-b.nist.gov	123 [2]	允许 FedRAMP 的 NTP 流量。

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. TCP 和 UDP 端口。

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。
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 URls：

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。
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。

域	端口	功能
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.osdsecuritylogs.com inputs1.osdsecuritylogs.cominputs1.osdsecuritylogs.com inputs6.osdsecuritylogs.com**	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
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。

2.5.2. 使用 HCP 的 ROSA

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. 允许列出用于下载和安装软件包和工具的以下 URL：

域	端口	功能
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。
quayio-production-s3.s3.amazonaws.com	443	提供核心容器镜像。
registry.redhat.io	443	提供核心容器镜像。
registry.access.redhat.com	443	必需。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。
mirror.openshift.com	443	必需。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。

2. 将以下遥测 URL 列入允许列表：

域	端口	功能
infogw.api.openshift.com	443	遥测是必需的。
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	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。

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 URls：

域	端口	功能
sts.<aws_region>.amazonaws.com [1]	443	必需。用于访问 AWS Secure Token Service (STS)区域端点。确保将 &lt **;aws-region** > 替换为集群部署到的区域。
sts.amazonaws.com [2]	443	请参阅 footnote。用于访问 AWS Secure Token Service (STS)全局端点。

1. 这也可以通过将 AWS Virtual Private Cloud (VPC)中的私有接口端点配置为区域 AWS STS 端点来实现。

2. 只有在 4.14.18 或 4.15.4 之前运行 OpenShift 版本时，才需要 AWS STS 全局端点。ROSA HCP 版本 4.14.18+、4.15.4+ 和 4.16.0+ 使用 AWS STS 区域端点。

4. 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	可选。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	可选。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	可选。对于 Sonatype Nexus, F5 Big IP operator 是必需的。

5. 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。

6. 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

2.6. 后续步骤

- 查看所需的 AWS 服务配额

2.7. 其他资源

- SRE 访问 AWS 集群中的所有 Red Hat OpenShift Service

- 为应用程序配置自定义域
- 实例类型

第 3 章 ROSA IAM 角色资源

Red Hat OpenShift Service on AWS (ROSA) Web UI 要求您在 AWS 帐户上具有特定权限，以便在 OpenShift Cluster Manager 和 **rosa** 命令行界面(CLI)提供最终用户体验。

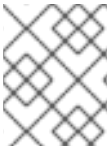
此信任关系通过 **ocm-role** AWS IAM 角色的创建和关联来实现。此角色有一个信任策略，AWS 安装程序将您的红帽帐户链接到 AWS 帐户。另外，您还需要为每个 Web UI 用户提供一个 **user-role** AWS IAM 角色，用于识别这些用户。这个 **user-role** AWS IAM 角色没有权限。

使用 OpenShift Cluster Manager 所需的 AWS IAM 角色有：

- **ocm-role**
- **user-role**

无论您是使用 ROSA CLI (**rosa**)或 OpenShift Cluster Manager Web UI 管理集群，您必须使用 ROSA CLI 创建集群范围的角色，在 ROSA CLI 中称为 **account-roles**。这些帐户角色是第一个集群所必需的，这些角色可以在多个集群中使用。这些所需的帐户角色有：

- **Worker-Role**
- **support-Role**
- **installer-Role**
- **controlPlane-Role**



注意

角色创建不会请求 AWS 访问或 secret 密钥。AWS 安全令牌服务(STS)用作此工作流的基础。AWS STS 使用临时的、有有限权限的凭证来提供身份验证。

有关创建这些角色的更多信息，请参阅 帐户范围的 IAM 角色和策略参考。

在 ROSA CLI 中，特定于集群的 Operator 角色（称为 **operator-roles** ）获取执行集群操作所需的临时权限，如管理后端存储、入口和 registry。您创建的集群需要这些角色。这些所需的 Operator 角色有：

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

有关创建这些角色的更多信息，请参阅 特定于集群的 Operator IAM 角色参考。

3.1. 关于 OCM-ROLE IAM 资源

您必须创建 **ocm-role** IAM 资源，以便红帽机构在 AWS (ROSA)集群上创建 Red Hat OpenShift Service。在链接到 AWS 的上下文中，红帽机构是 OpenShift Cluster Manager 中的单个用户。

ocm-role IAM 资源的一些注意事项：

- 每个红帽机构只能链接一个 **ocm-role** IAM 角色，但每个 AWS 帐户可以有任意数量的 **ocm-role** IAM 角色。Web UI 要求一次只能链接其中一个角色。
- 红帽机构中的任何用户都可以创建并链接 **ocm-role** IAM 资源。
- 只有红帽机构管理员可以取消链接 **ocm-role** IAM 资源。这个限制是防止其他红帽机构成员干扰其他用户的接口功能。

注意

如果您只创建了不属于现有机构的红帽帐户，则此帐户也是红帽机构管理员。

- 有关基本和 admin **ocm-role** IAM 资源的 AWS 权限策略列表，请参阅本节的附加资源中的"识别 OpenShift Cluster Manager 角色"。

使用 ROSA CLI (**rosa**)，您可以在创建时链接 IAM 资源。

注意

"链接"或"与 AWS 帐户关联您的 IAM 资源"意味着使用 **ocm-role** IAM 角色和 Red Hat OpenShift Cluster Manager AWS 角色创建信任策略。创建并链接您的 IAM 资源后，您会看到 AWS 中的 **ocm-role** IAM 资源与 **arn:aws:iam::7333:role/RH-Managed-OpenShift-Installer** 资源之间的信任关系。

在 Red Hat Organization Administrator 创建并链接 **ocm-role** IAM 资源后，所有机构成员都可能希望创建并链接自己的 **user-role** IAM 角色。此 IAM 资源只需要为每个用户创建并只连接一次。如果红帽机构中的其他用户已创建并链接了 **ocm-role** IAM 资源，则需要确保已创建并链接您自己的 **user-role** IAM 角色。

其他资源

- 请参阅了解 OpenShift Cluster Manager 角色

3.1.1. 创建 ocm-role IAM 角色

您可以使用命令行界面(CLI)创建 **ocm-role** IAM 角色。

前提条件

- 您有一个 AWS 帐户。
- 在 OpenShift Cluster Manager 机构中具有 Red Hat Organization Administrator 权限。
- 您有安装 AWS 范围的角色所需的权限。
- 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

- 要使用基本权限创建 ocm-role IAM 角色，请运行以下命令：

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

- 要使用 admin 权限创建 ocm-role IAM 角色，请运行以下命令：

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

此命令允许您通过指定特定属性来创建角色。以下示例输出显示选择了"自动模式"，它允许 ROSA CLI (**rosa**)创建 Operator 角色和策略。如需更多信息，请参阅附加资源中的"集群范围的角色创建"。

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::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes 6
I: Created role 'ManagedOpenShift-OCM-Role-182' with ARN  'arn:aws:iam::
<ARN>:role/ManagedOpenShift-OCM-Role-182'
I: Linking OCM role
? OCM Role ARN: arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182 7
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with organization
'<AWS ARN>'? Yes 8
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' with
organization account '<AWS ARN>'
```

1. 所有创建的 AWS 资源的前缀值。在本例中，**ManagedOpenShift** 会预先填充所有 AWS 资源。
2. 如果您希望此角色具有额外的 admin 权限，请选择。

注意

如果使用 **--admin** 选项，则不会显示此提示。

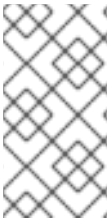
3. 用于设置权限边界的策略的 Amazon 资源名称 (ARN)。
4. 指定用户名的 IAM 路径。
5. 选择创建 AWS 角色的方法。使用 **auto** 时，ROSA CLI 生成并链接角色和策略。在 **auto** 模式中，您收到一些不同的提示来创建 AWS 角色。
6. **auto** 方法询问您是否要使用您的前缀创建特定的 **ocm-role**。
7. 确认您要将 IAM 角色与 OpenShift Cluster Manager 关联。
8. 将创建的角色与 AWS 组织相关联。

3.2. 关于 USER-ROLE IAM 角色

您需要为每个 Web UI **用户创建一个用户角色** IAM 角色，以便这些用户能够创建 ROSA 集群。

您的 **user-role** IAM 角色的一些注意事项：

- 每个红帽用户帐户您只需要一个 **user-role** IAM 角色，但您的红帽机构可以有许多这些 IAM 资源。
- 红帽机构中的任何用户都可以创建并链接 **user-role** IAM 角色。
- 每个红帽机构的每个 AWS 帐户可以有多个 **user-role** IAM 角色。
- 红帽使用 **user-role** IAM 角色来识别用户。此 IAM 资源没有 AWS 帐户权限。
- 您的 AWS 帐户可以有多个 **user-role** IAM 角色，但您必须将每个 IAM 角色链接到红帽机构中每个用户。用户不能有多个链接的 **user-role** IAM 角色。



注意

"链接"或"与 AWS 帐户关联您的 IAM 资源"意味着，使用 **user-role** IAM 角色和 Red Hat OpenShift Cluster Manager AWS 角色创建信任策略。创建并连接此 IAM 资源后，您会看到 AWS 中的 **user-role** IAM 角色与 **arn:aws:iam::710019948333:role/RH-Managed-OpenShift-Installer** 资源之间的信任关系。

3.2.1. 创建 user-role IAM 角色

您可以使用命令行界面(CLI)创建 **user-role** IAM 角色。

前提条件

- 您有一个 AWS 帐户。
- 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

- 要使用基本权限创建 **user-role** IAM 角色，请运行以下命令：

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

此命令允许您通过指定特定属性来创建角色。以下示例输出显示选择了"自动模式"，它允许 ROSA CLI (**rosa**)创建 Operator 角色和策略。如需更多信息，请参阅附加资源中的"了解自动和手动部署模式"。

输出示例

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

```
? Link the 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' role with account '1AGE'? Yes 6
I: Successfully linked role ARN 'arn:aws:iam::2066:role/ManagedOpenShift-User.osdocs-Role' with account '1AGE'
```

1. 所有创建的 AWS 资源的前缀值。在本例中，**ManagedOpenShift** 会预先填充所有 AWS 资源。
2. 用于设置权限边界的策略的 Amazon 资源名称 (ARN)。
3. 指定用户名的 IAM 路径。
4. 选择创建 AWS 角色的方法。使用 **auto** 时，ROSA CLI 生成并链接角色和策略。在 **auto** 模式中，您收到一些不同的提示来创建 AWS 角色。
5. **auto** 方法询问您是否要使用您的前缀创建特定的 **user-role**。
6. 将创建的角色与 AWS 组织相关联。

重要

如果您在删除集群前取消链接或删除 **user-role** IAM 角色，则会阻止您删除集群。您必须创建或修改此角色才能继续删除过程。如需更多信息，请参阅修复无法删除的集群。

3.3. AWS 帐户关联

Red Hat OpenShift Service on AWS (ROSA)集群置备任务需要使用 Amazon Resource Name (ARN)将 **ocm-role** 和 **user-role** IAM 角色链接到 AWS 帐户。

ocm-role ARN 存储为红帽机构中的标签，而 **user-role** ARN 则作为标签存储在红帽用户帐户中。红帽使用这些 ARN 标签来确认用户是有效的帐户拥有者，并可使用正确的权限来执行 AWS 帐户中的必要任务。

3.3.1. 链接 AWS 帐户

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa** 将 AWS 帐户链接到现有的 IAM 角色。

前提条件

- 您有一个 AWS 帐户。
- 您可以使用 OpenShift Cluster Manager 创建集群。
- 您有安装 AWS 范围的角色所需的权限。如需更多信息，请参阅本节的"附加资源"。
- 您已在安装主机上安装和配置了最新的 AWS (**aws**) 和 ROSA (**rosa**) CLI。
- 您已创建了 **ocm-role** 和 **user-role** IAM 角色，但还没有将它们链接到 AWS 帐户。您可以运行以下命令来检查您的 IAM 角色是否已链接：

```
$ rosa list ocm-role
```

```
$ rosa list user-role
```

如果这两个角色的 **Linked** 列中显示了 **Yes**，您已将角色链接到 AWS 帐户。

流程

1. 在 CLI 中，使用 Amazon 资源名称(ARN)将 **ocm-role** 资源链接到您的红帽机构：

注意

您必须具有红帽机构管理员权限才能运行 **rosa link** 命令。将 **ocm-role** 资源与 AWS 帐户链接后，对机构的所有用户可见。

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

输出示例

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

2. 在 CLI 中，使用 Amazon 资源名称(ARN)将您的 **user-role** 资源链接到您的红帽用户帐户：

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

输出示例

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

3.3.2. 将多个 AWS 帐户与红帽机构相关联

您可以将多个 AWS 帐户与红帽机构相关联。通过关联多个帐户，您可以从红帽机构在 AWS (ROSA)集群上创建 Red Hat OpenShift Service。

使用此功能，您可以使用多个 AWS 配置集作为区域密集型环境在不同的 AWS 区域中创建集群。

前提条件

- 您有一个 AWS 帐户。
- 您可以使用 OpenShift Cluster Manager 创建集群。
- 您有安装 AWS 范围的角色所需的权限。
- 您已在安装主机上安装和配置了最新的 AWS (**aws**) 和 ROSA (**rosa**) CLI。
- 您已创建了 **ocm-role** 和 **user-role** IAM 角色。

流程

要关联一个额外的 AWS 帐户，首先在本地 AWS 配置中创建配置集。然后，通过在其他 AWS 帐户中创建 **ocm-role**、用户帐户角色，将帐户与您的红帽机构相关联。

要在附加区域中创建角色，在运行 **rosa create** 命令时指定 **--profile <aws-profile>** 参数，将 **<aws_profile>** 替换为附加帐户配置集名称：

- 在创建 OpenShift Cluster Manager 角色时指定 AWS 帐户配置集：

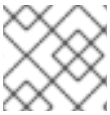
```
$ rosa create --profile <aws_profile> ocm-role
```

- 在创建用户角色时指定 AWS 帐户配置集：

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

- 在创建帐户角色时指定 AWS 帐户配置集：

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



注意

如果没有指定配置集，则使用默认 AWS 配置集。

3.4. 安装程序角色的权限边界

您可以将策略作为 *权限边界* 应用到安装程序角色。您可以使用 AWS 管理的策略或客户管理的策略为 Amazon Web Services (AWS)身份和访问管理(user 或 role)实体(user 或 role)设置边界。策略和边界策略的组合限制了用户或团队的最大权限。ROSA 包含三个准备的权限边界策略文件，您可以限制安装程序角色的权限，因为不支持更改安装程序策略本身。

注意

这个功能只在 Red Hat OpenShift Service on AWS （经典架构）集群中被支持。

权限边界策略文件如下：

- *Core* 边界策略文件包含 ROSA （经典架构）安装程序在 AWS 集群上安装 Red Hat OpenShift Service 所需的最小权限。安装程序没有创建虚拟私有云(VPC)或 PrivateLink (PL)的权限。需要提供 VPC。

- *VPC* 边界策略文件包含创建/管理 VPC 所需的 ROSA （经典架构）安装程序所需的最小权限。它不包括 PL 或 core 安装的权限。如果您需要安装具有足够权限的集群，以便安装程序安装集群并创建/管理 VPC，但您不需要设置 PL，然后将 core 和 VPC 边界文件与安装程序角色一起使用。

- *PrivateLink (PL)* 边界策略文件包含 ROSA （经典架构）安装程序使用集群创建 AWS PL 所需的最小权限。它不包括 VPC 或核心安装的权限。在安装过程中，为所有 PL 集群提供预先创建的 VPC。

在使用权限边界策略时，会应用以下组合：

- 没有权限边界策略意味着，完整的安装程序策略权限应用到集群。

- **core** 仅为安装程序角色设置最受限的权限。VPC 和 PL 权限不包括在 **Core only** boundary 策略中。

    - 安装程序无法创建和管理 VPC 或 PL

- 安装程序无法创建和管理 VPC 或 PL。
- 您必须具有客户提供的 VPC，而 PrivateLink (PL)不可用。

- **Core + VPC** 为安装程序角色设置 core 和 VPC 权限。
  - 安装程序无法创建和管理 PL。
  - 假设您没有使用 custom/BYO-VPC。
  - 假设安装程序将创建和管理 VPC。
- **Core + PrivateLink (PL)**意味着安装程序可以置备 PL 基础架构。
  - 您必须具有客户提供的 VPC。
  - 这适用于带有 PL 的私有集群。

这个示例步骤适用于具有最多权限限制的安装程序角色和策略，只使用 ROSA *的核心* 安装程序权限边界策略。您可以使用 AWS 控制台或 AWS CLI 完成此项。本例使用 AWS CLI 和以下策略：

例 3.1. sts_installer_core_permission_boundary_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
  "autoscaling:DescribeAutoScalingGroups",
  "ec2:AllocateAddress",
  "ec2:AssociateAddress",
  "ec2:AttachNetworkInterface",
  "ec2:AuthorizeSecurityGroupEgress",
  "ec2:AuthorizeSecurityGroupIngress",
  "ec2:CopyImage",
  "ec2:CreateNetworkInterface",
  "ec2:CreateSecurityGroup",
  "ec2:CreateTags",
  "ec2:CreateVolume",
  "ec2:DeleteNetworkInterface",
  "ec2:DeleteSecurityGroup",
  "ec2:DeleteSnapshot",
  "ec2:DeleteTags",
  "ec2:DeleteVolume",
  "ec2:DeregisterImage",
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeAddresses",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeDhcpOptions",
  "ec2:DescribeImages",
  "ec2:DescribeInstanceAttribute",
  "ec2:DescribeInstanceCreditSpecifications",
  "ec2:DescribeInstances",
  "ec2:DescribeInstanceStatus",
  "ec2:DescribeInstanceTypeOfferings",
  "ec2:DescribeInstanceTypes",
```

```
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetConsoleOutput",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
```

```
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile",
        "iam:TagInstanceProfile",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:PassRole",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:SimulatePrincipalPolicy",
        "iam:TagRole",
        "iam:UntagRole",
        "route53:ChangeResourceRecordSets",
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:GetAccountLimit",
        "route53:GetChange",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53:UpdateHostedZoneComment",
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetAccelerateConfiguration",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
```

```
            "s3:PutBucketTagging",
            "s3:PutEncryptionConfiguration",
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:PutObjectTagging",
            "servicequotas:GetServiceQuota",
            "servicequotas:ListAWSDefaultServiceQuotas",
            "sts:AssumeRole",
            "sts:AssumeRoleWithWebIdentity",
            "sts:GetCallerIdentity",
            "tag:GetResources",
            "tag:UntagResources",
            "kms:DescribeKey",
            "cloudwatch:GetMetricData",
            "ec2:CreateRoute",
            "ec2:DeleteRoute",
            "ec2:CreateVpcEndpoint",
            "ec2:DeleteVpcEndpoints",
            "ec2:CreateVpcEndpointServiceConfiguration",
            "ec2:DeleteVpcEndpointServiceConfigurations",
            "ec2:DescribeVpcEndpointServiceConfigurations",
            "ec2:DescribeVpcEndpointServicePermissions",
            "ec2:DescribeVpcEndpointServices",
            "ec2:ModifyVpcEndpointServicePermissions"
                ],
                "Resource": "*"
            },
            {
                "Effect": "Allow",
                "Action": [
                    "secretsmanager:GetSecretValue"
                ],
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "aws:ResourceTag/red-hat-managed": "true"
                    }
                }
            }
        ]
    }
```

重要

要使用权限边界，您需要准备权限边界策略，并将其添加到 AWS IAM 中的相关安装程序角色中。虽然 ROSA (**rosa**) CLI 提供了权限边界功能，但它适用于所有角色，而不仅适用于安装程序角色，这意味着它不可用于提供的权限边界策略（仅适用于安装程序角色）。

前提条件

- 您有一个 AWS 帐户。
- 您有管理 AWS 角色和策略所需的权限。

- 您已在工作站上安装和配置了最新的 AWS (**aws**)和 ROSA (**rosa**) CLI。
- 您已准备了 ROSA 集群范围的角色，包括安装程序角色和对应的策略。如果 AWS 帐户中不存在它们，*请参阅附加资源* 中的"创建账户范围的 STS 角色和策略"。

流程

1. 在 **rosa** CLI 中输入以下命令来准备策略文件：

```
$ curl -o ./rosa-installer-core.json https://raw.githubusercontent.com/openshift/managed-cluster-config/master/resources/sts/4.16/sts_installer_core_permission_boundary_policy.json
```

2. 在 AWS 中创建策略，并输入以下命令收集其 Amazon 资源名称(ARN)：

```
$ aws iam create-policy \
--policy-name rosa-core-permissions-boundary-policy \
--policy-document file://./rosa-installer-core.json \
--description "ROSA installer core permission boundary policy, the minimum permission set, allows BYO-VPC, disallows PrivateLink"
```

输出示例

```
{
    "Policy": {
        "PolicyName": "rosa-core-permissions-boundary-policy",
        "PolicyId": "<Policy ID>",
        "Arn": "arn:aws:iam::<account ID>:policy/rosa-core-permissions-boundary-policy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "<CreateDate>",
        "UpdateDate": "<UpdateDate>"
    }
}
```

3. 输入以下命令在您要限制的安装程序角色中添加权限边界策略：

```
$ aws iam put-role-permissions-boundary \
--role-name ManagedOpenShift-Installer-Role \
--permissions-boundary arn:aws:iam::<account ID>:policy/rosa-core-permissions-boundary-policy
```

4. 在 **rosa** CLI 中输入以下命令来显示安装程序角色以验证附加策略（包括权限边界）：

```
$ aws iam get-role --role-name ManagedOpenShift-Installer-Role \
--output text | grep PERMISSIONSBOUNDARY
```

输出示例

```
PERMISSIONSBOUNDARY arn:aws:iam::<account ID>:policy/rosa-core-permissions-boundary-policy Policy
```

有关 PL 和 VPC 权限边界策略的更多示例，请参阅：

例 3.2. sts_installer_privatelink_permission_boundary_policy.json

```
{
"Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "route53:ListHostedZonesByVPC",
        "route53:CreateVPCAssociationAuthorization",
        "route53:AssociateVPCWithHostedZone",
        "route53:DeleteVPCAssociationAuthorization",
        "route53:DisassociateVPCFromHostedZone",
        "route53:ChangeResourceRecordSets"
      ],
      "Resource": "*"
    }
  ]
}
```

例 3.3. sts_installer_vpc_permission_boundary_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
      "ec2:AssociateDhcpOptions",
      "ec2:AssociateRouteTable",
      "ec2:AttachInternetGateway",
      "ec2:CreateDhcpOptions",
      "ec2:CreateInternetGateway",
      "ec2:CreateNatGateway",
      "ec2:CreateRouteTable",
      "ec2:CreateSubnet",
      "ec2:CreateVpc",
      "ec2:DeleteDhcpOptions",
      "ec2:DeleteInternetGateway",
      "ec2:DeleteNatGateway",
      "ec2:DeleteRouteTable",
      "ec2:DeleteSubnet",
      "ec2:DeleteVpc",
      "ec2:DetachInternetGateway",
      "ec2:DisassociateRouteTable",
      "ec2:ModifySubnetAttribute",
      "ec2:ModifyVpcAttribute",
      "ec2:ReplaceRouteTableAssociation"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

3.5. 其他资源

- 请参阅 IAM 实体(AWS 文档)的权限界限。
- 请参阅创建集群范围的 STS 角色和策略。
- 请参阅 IAM 角色故障排除。
- 如需创建 集群所需的 IAM 角色列表，请参阅帐户范围的 IAM 角色和策略引用。

第 4 章 限制和可扩展性

本文档详细描述了在 AWS (ROSA) 集群上为 Red Hat OpenShift Service 测试的集群最大值，以及用于测试最大测试环境和配置的信息。另外还提供了有关 control plane 和基础架构节点大小和扩展的信息。

4.1. 集群最大限制

在规划 Red Hat OpenShift Service on AWS (ROSA)集群安装时，请考虑以下测试的对象最大值。表指定 (ROSA)集群中每个测试类型的最大限值。

这些指南基于多个可用区配置中 102 计算（也称为 worker）节点的集群。对于较小的集群，最大值限制会较低。

注意

所有测试中使用的 OpenShift Container Platform 版本都是 OCP 4.8.0。

表 4.1. 测试的集群最大值

最大类型	4.8 测试的最大值
节点数	102
pod 数量 [1]	20,400
每个节点的 pod 数量	250
每个内核的 pod 数量	没有默认值
命名空间数量 [2]	3,400
每个命名空间的 pod 数量 [3]	20,400
服务数 [4]	10,000
每个命名空间的服务数	10,000
每个服务中的后端数	10,000
每个命名空间的部署数量 [3]	1,000

1. 这里的 pod 数量是 test pod 的数量。实际的 pod 数量取决于应用程序的内存、CPU 和存储要求。
2. 当有大量活跃的项目时，如果键空间增长过大并超过空间配额，etcd 的性能将会受到影响。强烈建议您定期维护 etcd 存储（包括整理碎片）来释放 etcd 存储。

3. 系统中有一些控制循环，它们必须对给定命名空间中的所有对象进行迭代，以作为对一些状态更改的响应。在单一命名空间中有大量给定类型的对象可使这些循环的运行成本变高，并降低对给定状态变化的处理速度。限制假设系统有足够的 CPU 、内存和磁盘来满足应用程序的要求。

4. 每个服务端口和每个服务后端在 iptables 中都有对应条目。给定服务的后端数量会影响端点对象的大小，这会影响到整个系统发送的数据大小。

在 OpenShift Container Platform 4.8 中，与以前的 OpenShift Container Platform 版本相比，系统会保留半个 CPU 内核(500 millicore)。

4.2. OPENSHIFT CONTAINER PLATFORM 测试环境和配置

下表列出了为 AWS 云平台测试集群最大值的 OpenShift Container Platform 环境和配置。

节点	类型	vCPU	RAM(GiB)	磁盘类型	磁盘大小(GiB)/IOPS	数量	区域
control plane/etcd [1]	m5.4xlarge	16	64	gp3	350 / 1,000	3	us-west-2
基础架构节点 [2]	r5.2xlarge	8	64	gp3	300 / 900	3	us-west-2
Workload [3]	m5.2xlarge	8	32	gp3	350 / 900	3	us-west-2
Compute 节点	m5.2xlarge	8	32	gp3	350 / 900	102	us-west-2

1. io1 磁盘用于 4.10 之前的版本中的 control plane/etcd 节点。

2. 基础架构节点用于托管监控组件，因为 Prometheus 可以根据使用情况模式声明大量内存。

3. 工作负载节点专用于运行性能和可扩展工作负载生成器。

更大的集群大小和更高的对象数量可能可以被访问。但是，基础架构节点的大小限制 Prometheus 可用的内存量。在创建、修改或删除对象时，Prometheus 会将指标存储在其内存中，时长大约 3 小时，然后再在磁盘上保留指标。如果创建、修改或删除对象的速率过高，Prometheus 可能会因为缺少内存资源而造成问题问题。

4.3. CONTROL PLANE 和基础架构节点大小和扩展

当您在 AWS (ROSA)集群上安装 Red Hat OpenShift Service 时，control plane 和基础架构节点的大小由计算节点计数自动决定。

如果您在安装后更改集群中的计算节点数量，Red Hat Site Reliability Engineering (SRE)团队会根据需要扩展 control plane 和基础架构节点，以保持集群稳定性。

4.3.1. 安装过程中的节点大小

在安装过程中，control plane 和基础架构节点的大小会被动态计算。大小计算基于集群中计算节点的数量。

下表列出了在安装过程中应用的 control plane 和基础架构节点大小。

计算节点数量	control plane 大小	基础架构节点大小
1 到 25	m5.2xlarge	r5.xlarge
26 到 100	m5.4xlarge	r5.2xlarge
101 到 180	m5.8xlarge	r5.4xlarge

注意

ROSA 上的最大计算节点数量为 180。

4.3.2. 安装后节点扩展

如果您在安装后更改计算节点数量，则 control plane 和基础架构节点会根据需要由 Red Hat Site Reliability Engineering (SRE)团队扩展。节点已扩展以保持平台稳定性。

control plane 和基础架构节点安装后扩展要求会根据具体情况进行评估。考虑使用节点资源消耗和接收的警报。

control plane 节点重新定义警报大小的规则

在以下情况下，会为集群中的 control plane 节点触发重新定义大小警报：

- control plane 节点在典型的 ROSA 集群中平均保持 66% 的利用率。

注意

ROSA 上的最大计算节点数量为 180。

基础架构节点大小警报的规则

当具有高 CPU 或内存使用率时，会为集群中的基础架构节点触发重新定义警报的大小。这个高影响的利用率状态为：

- 基础架构节点在典型的 ROSA 集群中平均保持 50% 的利用率，其具有使用 2 个基础架构节点的单一可用区。
- 基础架构节点平均在带有 3 个基础架构节点的多个可用区的经典 ROSA 集群中保持 66% 的利用率。

注意

ROSA 上的最大计算节点数量为 180。

调整大小的警报仅在达到高利用率时显示。短使用量激增（如节点暂时关闭导致其他节点扩展）不会触发这些警报。

SRE 团队可能会因为其他原因扩展 control plane 和基础架构节点，例如管理节点上资源消耗的增加。

应用缩放时，通过服务日志条目通知客户。有关服务日志的更多信息，请参阅 *访问 ROSA 集群的服务日志*。

4.3.3. 较大的集群的大小注意事项

对于较大的集群，基础架构节点大小可能会严重影响可扩展性。很多因素会影响指定的阈值，包括 etcd 版本或者存储数据格式。

超过这些限制并不一定意味着集群将失败。在大多数情况下，超过这些限制会降低整体性能。

4.4. 后续步骤

- 规划您的环境

4.5. 其他资源

- 访问 ROSA 集群的服务日志

第 5 章 规划您的环境

5.1. 根据经过测试的集群限制规划您的环境

本文档论述了如何根据经过测试的集群最大值规划 Red Hat OpenShift Service on AWS 环境。

在节点中过度订阅物理资源会影响在 pod 放置过程中对 Kubernetes 调度程序的资源保证。了解可以采取什么措施避免内存交换。

某些限制只在单一维度中扩展。当很多对象在集群中运行时，它们会有所不同。

本文档中给出的数字基于红帽测试方法、设置、配置和调整。这些数字会根据您自己的设置和环境而有所不同。

在规划您的环境时，使用以下公式决定每个节点应该有多少个 pod：

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

每个节点上的 Pod 数量做多为 250。而在某个节点中运行的 pod 的具体数量取决于应用程序本身。参照*根据应用程序要求规划您的环境*的内容，考虑应用程序的内存、CPU 和存储要求。

示例情境

如果想把集群的规模限制在没有集群可以有 2200 个 pod，则需要至少有九个节点，假设每个节点最多有 250 个 pod：

```
2200 / 250 = 8.8
```

如果将节点数量增加到 20，那么 pod 的分布情况将变为每个节点有 110 个 pod：

```
2200 / 20 = 110
```

其中：

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

5.2. 根据应用程序要求规划您的环境

本文档论述了如何根据应用程序要求规划 Red Hat OpenShift Service on AWS 环境。

考虑应用程序环境示例：

pod 类型	pod 数量	最大内存	CPU 内核	持久性存储
Apache	100	500 MB	0.5	1 GB
node.js	200	1 GB	1	1 GB
postgresql	100	1 GB	2	10 GB
JBoss EAP	100	1 GB	1	1 GB

额外要求：550 个 CPU 内核、450 GB RAM 和 1.4 TB 存储。

根据您的具体情况，节点的实例大小可以被增大或降低。在节点上通常会使用资源过度分配。在这个部署场景中，您可以选择运行多个额外的较小节点，或数量更少的较大节点来提供同样数量的资源。在做出决定前应考虑一些因素，如操作的灵活性以及每个实例的成本。

节点类型	数量	CPU	RAM (GB)
节点（选择 1）	100	4	16
节点（选择 2）	50	8	32
节点（选择 3）	25	16	64

有些应用程序很适合于过度分配的环境，有些则不适合。大多数 Java 应用程序以及使用巨页的应用程序都不允许使用过度分配功能。它们的内存不能用于其他应用程序。在上面的例子中，环境大约会出现 30% 过度分配的情况，这是一个常见的比例。

应用程序 pod 可以使用环境变量或 DNS 访问服务。如果使用环境变量，当 pod 在节点上运行时，对于每个活跃服务，则 kubelet 的变量都会注入。集群感知 DNS 服务器监视 Kubernetes API 提供了新服务，并为每个服务创建一组 DNS 记录。如果整个集群中启用了 DNS，则所有 pod 都应自动根据其 DNS 名称解析服务。如果您必须超过 5000 服务，可以使用 DNS 进行服务发现。当使用环境变量进行服务发现时，如果参数列表超过命名空间中 5000 服务后允许的长度，则 pod 和部署将失败。

要解决这个问题，请禁用部署的服务规格文件中的服务链接：

示例

```
Kind: Template
apiVersion: template.openshift.io/v1
metadata:
  name: deploymentConfigTemplate
  creationTimestamp:
  annotations:
    description: This template will create a deploymentConfig with 1 replica, 4 env vars and a service.
    tags: ''
objects:
  - kind: DeploymentConfig
    apiVersion: apps.openshift.io/v1
    metadata:
      name: deploymentconfig${IDENTIFIER}
    spec:
      template:
        metadata:
          labels:
            name: replicationcontroller${IDENTIFIER}
        spec:
          enableServiceLinks: false
          containers:
          - name: pause${IDENTIFIER}
            image: "${IMAGE}"
            ports:
            - containerPort: 8080
```

```
            protocol: TCP
          env:
          - name: ENVVAR1_${IDENTIFIER}
            value: "${ENV_VALUE}"
          - name: ENVVAR2_${IDENTIFIER}
            value: "${ENV_VALUE}"
          - name: ENVVAR3_${IDENTIFIER}
            value: "${ENV_VALUE}"
          - name: ENVVAR4_${IDENTIFIER}
            value: "${ENV_VALUE}"
          resources: {}
          imagePullPolicy: IfNotPresent
          capabilities: {}
          securityContext:
            capabilities: {}
            privileged: false
        restartPolicy: Always
        serviceAccount: ''
    replicas: 1
    selector:
      name: replicationcontroller${IDENTIFIER}
    triggers:
    - type: ConfigChange
    strategy:
      type: Rolling
- kind: Service
  apiVersion: v1
  metadata:
    name: service${IDENTIFIER}
  spec:
    selector:
      name: replicationcontroller${IDENTIFIER}
    ports:
    - name: serviceport${IDENTIFIER}
      protocol: TCP
      port: 80
      targetPort: 8080
    portalIP: ''
    type: ClusterIP
    sessionAffinity: None
  status:
    loadBalancer: {}
parameters:
- name: IDENTIFIER
  description: Number to append to the name of resources
  value: '1'
  required: true
- name: IMAGE
  description: Image to use for deploymentConfig
  value: gcr.io/google-containers/pause-amd64:3.0
  required: false
- name: ENV_VALUE
  description: Value to use for environment variables
  generate: expression
  from: "[A-Za-z0-9]{255}"
```

```
    required: false
  labels:
template: deploymentConfigTemplate
```

可在命名空间中运行的应用程序 pod 数量取决于服务数量以及环境变量用于服务发现时的服务名称长度。系统上的 **ARG_MAX** 定义新进程的最大参数长度，默认设置为 2097152 字节 (2 MiB)。kubelet 将环境变量注入到要在命名空间中运行的每个 pod，包括：

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

如果参数长度超过允许的值，服务名称中的字符数会受到影响，命名空间中的 pod 将开始失败。

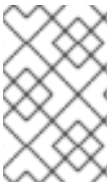
第 6 章 所需的 AWS 服务配额

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。

6.1. 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 6.1. 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。

配额名称	服务代码	配额代码	AWS 默认	最低要求	描述
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。
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 6.2. 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。

配额名称	服务代码	配额代码	AWS 默认	最低要求	描述
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。
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。

配额名称	服务代码	配额代码	AWS 默认	最低要求	描述

6.1.1. 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

6.2. 后续步骤

- 设置环境并安装 ROSA

第 7 章 为使用 STS 设置环境

满足 AWS 的先决条件后，设置您的环境并安装 Red Hat OpenShift Service on AWS (ROSA)。

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。

7.1. 为 STS 设置环境

在创建使用 AWS 安全令牌服务 (STS) 的 Red Hat OpenShift Service on AWS (ROSA) 集群前，请完成以下步骤来设置您的环境。

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。
   建议您使用专用 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，则这些策略必须比集群所需的角色和策略更严格。

2. 在 AWS 管理控制台中启用 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

   您可以使用环境变量设置默认的 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
```

4. 安装最新版本的 ROSA CLI (**rosa**)。

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** 的文件，并使文件可执行。本文档使用 **rosa** 参考可执行文件。

```
$ chmod +x rosa
```

c. 可选：在路径中添加 **rosa**。

```
$ 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. 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. 提供脚本，以从现有终端中启用 **rosa** 命令完成。以下示例在 Linux 机器上提供 **rosa** 的 Bash 完成脚本：

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

5. 使用 ROSA CLI 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

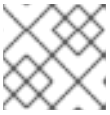
```
I: Logged in as '<rh-rosa-user>' on 'https://api.openshift.com'
```

6. 验证您的 AWS 帐户是否有部署 ROSA 集群所需的配额。

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

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 管理控制台，并为失败的服务请求配额增加。

在配额检查成功后，继续下一步。

7. 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 OpenShift Cluster Manager 开始的行。

   ```
   $ rosa whoami
   ```

   输出示例

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

8. 通过 ROSA (**rosa**) CLI 安装 OpenShift CLI (**oc**)、版本 4.7.9 或更高版本。

   a. 输入这个命令下载 **oc** CLI 的最新版本：

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

   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 openshift-client
   ```

创建角色

完成这些步骤后，就可以设置 IAM 和 OIDC 访问的角色。

7.2. 后续步骤

- 快速创建使用 STS 的 ROSA 集群，或使用自定义创建集群。

7.3. 其他资源

- AWS 先决条件

- 所需的 AWS 服务配额并增加请求