aws

用户指南

AWS 云端 Red Hat OpenShift 服务

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 云端 Red Hat OpenShift 服务: 用户指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有其他非亚马逊拥有的商标均为其各自所有者的财产，这些所有者可能与亚马逊有关联、关联或赞助 Amazon.s

Table of Contents

什么是 AWS 云端 Red Hat OpenShift 服务？ 1
功能 1
正在访问 ROSA 1
如何开始 ROSA 2
定价 3
ROSA 服务费 3
AWS 基础设施费用 3
责任 3
概述 4
按区域责任共担任务 5
数据和应用程序的客户责任 21
架构 23
比较 ROSA 与 HCP 和 ROSA 经典版 23
开始使用 ROSA 25
设置 25
先决条件 25
启用 ROSA 和配置 AWS 先决条件 26
创建 ROSA HCP 集群-CLI 26
先决条件 27
创建 Amazon VPC 架构 27
创建所需的 IAM 角色和 OpenID Connect 配置 33
使用 C ROSA LI 创建带有 HCP 集群的 ROSA 和 AWS STS 35
配置身份提供商并授予 集群 访问权限 36
授予用户访问权限 集群 37
配置 cluster-admin 权限 38
配置 dedicated-admin 权限 38
集群 通过红帽混合云控制台访问 38
从开发者目录部署应用程序 39
撤销用户的 cluster-admin 权限 40
撤销用户的 dedicated-admin 权限 40
撤消用户对 a 的访问权限 集群 40
删除集群和 AWS STS 资源 40
创建 ROSA 经典集群-CLI 42
先决条件 42

使用 ROSA CLI 创建 ROSA 经典集群和 AWS STS 42
配置身份提供商并授予 集群 访问权限 44
向用户授予访问权限 集群 46
配置 cluster-admin 权限 46
配置 dedicated-admin 权限 47
集群 通过红帽混合云控制台访问 47
从开发者目录中部署应用程序 47
撤销用户的 cluster-admin 权限 48
撤销用户的 dedicated-admin 权限 49
撤消用户对 a 的访问权限 集群 49
删除集群和 AWS STS 资源 49
创建 ROSA 经典集群- AWS PrivateLink 50
先决条件 51
创建 Amazon VPC 架构 51
使用 ROSA CLI 创建 ROSA 经典集群和 AWS PrivateLink 56
配置 AWS PrivateLink DNS 转发 58
配置身份提供商并授予 集群 访问权限 59
向用户授予访问权限 集群 60
配置 cluster-admin 权限 61
配置 dedicated-admin 权限 61
集群 通过红帽混合云控制台访问 61
从开发者目录中部署应用程序 62
撤销用户的 cluster-admin 权限 63
撤销用户的 dedicated-admin 权限 63
撤消用户对 a 的访问权限 集群 63
删除集群和 AWS STS 资源 64
安全性 66
数据保护 66
数据加密 67
Identity and access management 70
受众 70
使用身份进行身份验证 71
使用策略管理访问 73
ROSA 基于身份的策略示例 75
AWS 托管策略 94
故障排除 118

恢复能力 120
AWS 全球基础设施弹性 120
ROSA 集群弹性 121
Customer-deployed 应用程序弹性 121
基础设施安全性 121
集群网络隔离 122
容器组（pod）网络隔离 122
仓储服务 123
存储的工作原理 123
永久容量、声明和存储类别 123
访问模式 124
默认情况下已安装存储驱动程序 125
AWS STS 和存储驱动程序权限 126
Amazon EBS 126
特性 126
卷类型 127
默认存储类别 127
加密 128
Permissions 128
Amazon EFS 128
特性 128
正在启用 Amazon EFS 129
权限和设置 129
接入点和文件所有权 129
加密 130
FSx for ONTAP 130
特性 131
安装三叉戟 131
加密 132
支撑模型 132
服务配额 133
使用其他服务 134
ROSA 和 AWS Marketplace 134
术语 134
ROSA 付款和账单 135
通过控制台订阅 ROSA Marketplace 商品信息 135

购买合 ROSA 同 136
Private Marketplace 140
问题排查 141
访问 ROSA 集群调试日志 141
ROSA 集群在 集群 创建期间未能通过 AWS 服务配额检查 141
ROSA CLI 过期的离线访问令牌疑难解答 142
创建失败 集群 ，但 osdCcsAdmin 出现错误 142
后续步骤 143
获取支持 143
打开一个 支持 case 143
打开 Red Hat Support 案例 143
文档历史记录 144
..... cliii

什么是 AWS 云端 Red Hat OpenShift 服务？

AWS 云端 Red Hat OpenShift 服务 (ROSA) 是一项托管服务，您可以使用它在红帽 OpenShift 企业 Kubernetes 平台上构建、扩展和部署容器化应用程序。 AWS ROSA 简化了将本地红帽 OpenShift 工作负载迁移到其他工作负载的流程 AWS，并提供了与其他 AWS 服务工作负载的紧密集成。

功能

ROSA 由和红帽联合支持 AWS 和运营。每个 ROSA 集群都提供红帽站点可靠性工程师 (SRE) 的全天候集群管理支持，并以红帽 99.95% 的正常运行时间服务级别协议 (SLA) 为后盾。有关该服务的支持模式的更多信息，请参阅the section called “获取支持”。

ROSA 还提供以下功能：

- Red Hat SRE 支持的集群安装、集群维护和集群升级。
- AWS 服务 集成包括 AWS 计算、数据库、分析、机器学习、网络和移动。
- 跨多个 AWS 可用区运行和扩展 Kubernetes 控制平面，以确保高可用性。
- 使用 OpenShift APIs 和开发人员生产力工具操作集群，包括服务网格、 CodeReady 工作空间和无服务器。

正在访问 ROSA

您可以使用以下接口定义和配置 ROSA 服务部署。

AWS

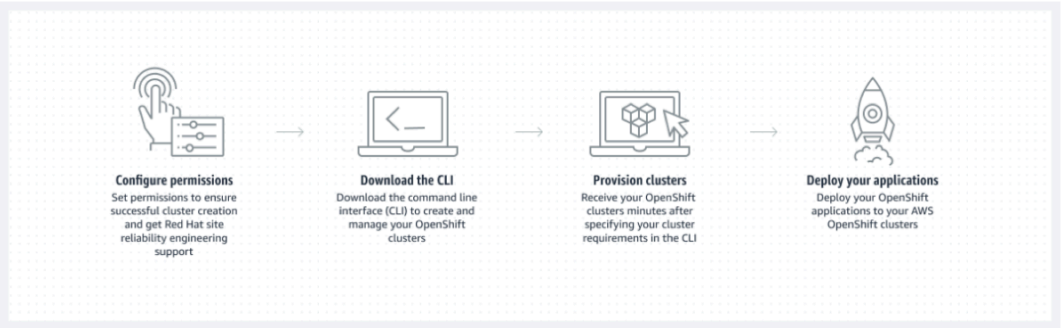
- ROSA 控制台-提供 Web 界面以启用 ROSA 订阅和购买 ROSA 软件合同。
- AWS Command Line Interface (AWS CLI) — 提供适用于各种各样的命令 AWS 服务 并在 Windows、macOS 和 Linux 上受支持。有关更多信息，请参阅 AWS Command Line Interface。

Red Hat OpenShift

- 红帽混合云控制台 — 提供一个 Web 界面，用于创建、更新和管理 ROSA 集群、安装集群插件以及创建和部署应用程序到 ROSA 集群。
- ROSA CLI (rosa)-提供创建、更新和管理 ROSA 集群的命令。

- OpenShift CLI (oc) — 提供用于创建应用程序和管理 OpenShift 容器平台项目的命令。
- Knative CLI (kn)-提供可用于与 OpenShift 无服务器组件（例如 Knative 服务和事件）交互的命令。
- 流水线 CLI (tkn)-提供使用终端与 OpenShift 管道交互的命令。
- opm CLI-提供帮助操作员开发人员和集群管理员从终端创建和维护 OpenShift 操作员目录的命令。
- 操作员 SDK CLI-提供操作员开发者可用于构建、测试和部署 OpenShift 操作员的命令。

如何开始 ROSA



以下总结了的入门流程 ROSA。有关详细的入门说明，请参阅开始使用 ROSA 。

AWS 管理控制台/AWS CLI

1. 为交付服务功能 AWS 服务 所 ROSA 依赖的权限进行配置。有关更多信息，请参阅 the section called “先决条件”。
2. 安装和配置最新的 AWS CLI 工具。有关更多信息，请参阅 AWS CLI 用户指南AWS CLI中的安装我们最新版本的。
3. 在ROSA 控制台 ROSA中启用。

红帽混合云控制台/ CLI ROSA

1. 从红帽混合云控制台下载最新版本的 OpenShift CL ROSA I 和 CLI。有关更多信息，请参阅红帽文档中的 ROSA CLI 入门。
2. 在红帽混合云控制台或 ROSA CLI 中创建 ROSA 集群。
3. 集群准备就绪后，配置身份提供商以授予用户对集群的访问权限。
4. 在 ROSA 集群上部署和管理工作负载的方式与在任何其他 OpenShift 环境中部署和管理工作负载的方式相同。

定价

的总成本由两个部分 ROSA 组成： ROSA 服务费和 AWS 基础设施费。有关定价的更多信息，请参阅AWS 云端 Red Hat OpenShift 服务 定价。

ROSA 服务费

默认情况下， ROSA 服务费用按工作节点每使用 4 个 vCPU 的小时费率按需累计。所有支持的 AWS 标准区域的服务费用是统一的。除了工作节点服务费外，使用托管控制平面 (HCP) 集群的 ROSA 还会按小时收取集群费用。

ROSA 提供 1 年和 3 年服务费合同，您可以购买这些合同以节省工作节点的按需服务费用。有关更多信息，请参阅 the section called “购买合 ROSA 同”。

AWS 基础设施费用

AWS 基础设施费用适用于 AWS 全球基础设施上托管的底层工作节点、基础设施节点、控制平面节点、存储和网络资源。 AWS 基础设施费用因而异 AWS 区域。

的职责概述 ROSA

本文档概述了 Amazon Web Services (AWS)、Red Hat 和客户对 AWS 云端 Red Hat OpenShift 服务 (ROSA) 托管服务的责任。有关 ROSA 及其组件的更多信息，请参阅 Red Hat 文档中的策略和服务定义。

分AWS 担责任模型定义了保护运行中提供的所有服务的基础设施的 AWS 责任 AWS Cloud，包括 ROSA。 AWS 基础架构包括运行 AWS Cloud 服务的硬件、软件、网络和设施。这种 AWS 责任通常被称为 “云安全”。为了 ROSA 作为一项完全托管的服务运营，红帽和客户应对 AWS 责任模型定义为 “云端安全” 的服务要素负责。

红帽负责 ROSA 集群基础架构、底层应用平台和操作系统的持续管理和安全。虽然 ROSA 集群托管在客户的 AWS 资源上 AWS 账户，但 ROSA 服务组件和红帽站点可靠性工程师 (SREs) 可以通过客户创建的 IAM 角色远程访问它们。Red Hat 使用此访问权限，来管理集群上所有控制面板和基础设施节点的部署和容量，并维护控制面板节点、基础设施节点和 Worker 节点的版本。

红帽和客户共同负责 ROSA 网络管理、集群日志、集群版本控制和容量管理。在红帽管理 ROSA 服务的同时，客户完全负责管理和保护部署到的任何应用程序、工作负载和数据 ROSA。

概述

下表概述 AWS了红帽及其客户责任 AWS 云端 Red Hat OpenShift 服务。

> **Note**
>
> 如果向用户添加了 `cluster-admin` 角色，请参阅 Red Hat Enterprise Agreement Appendix 4（Online Subscription Services）中的责任和免责声明。

资源	事件和运营管理	变更管理	访问和身份授权	安全和法规合规性	灾难恢复
客户数据	客户	客户	客户	客户	Customer
客户应用程序	客户	客户	客户	客户	Customer
开发人员服务	客户	客户	客户	客户	Customer
平台监控	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
日志记录	Red Hat	Red Hat 和客户	Red Hat 和客户	Red Hat 和客户	Red Hat
应用程序联网	Red Hat 和客户	Red Hat 和客户	Red Hat 和客户	Red Hat	Red Hat
集群联网	Red Hat	Red Hat 和客户	Red Hat 和客户	Red Hat	Red Hat
虚拟联网管理	Red Hat 和客户	Red Hat 和客户	Red Hat 和客户	Red Hat 和客户	Red Hat 和客户
虚拟计算管理（控制面板、基础设施和 Worker 节点）	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat

资源	事件和运营管理	变更管理	访问和身份授权	安全和法规合规性	灾难恢复
集群版本	Red Hat	Red Hat 和客户	Red Hat	Red Hat	Red Hat
容量管理	Red Hat	Red Hat 和客户	Red Hat	Red Hat	Red Hat
虚拟存储管理	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS 软件（公共 AWS 服务）	AWS	AWS	AWS	AWS	AWS
硬件/AWS 全球基础架构	AWS	AWS	AWS	AWS	AWS

按区域责任共担任务

AWS、Red Hat 和客户共同负责 ROSA 组件的监控和维护。本文档按领域和任务定义了 ROSA 服务职责。

事件和运营管理

AWS 负责保护运行中提供的所有服务的硬件基础架构 AWS Cloud。Red Hat 负责管理默认平台联网所需的服务组件。客户负责客户应用程序数据，以及客户可能配置的任何自定义联网的事件和运营管理。

资源	服务责任	客户责任
应用程序联网	Red Hat • 监控本地 OpenShift 路由器服务，并对警报做出响应。	客户 • 监控应用程序路由及其背后端点的运行状况。 • 向 AWS 红帽报告中断情况。
虚拟联网管理	Red Hat	客户

资源	服务责任	客户责任
	• 监控默认平台联 Amazon VPC 网所需的 AWS 负载均衡器、子网和 AWS 服务 组件。响应提醒。	• 监控 AWS 负载均衡器端点的运行状况。 • 监控可选通过到 Amazon VPC vPC 的连接、 Site-to-Site VPN 连接配置的网络流量，或者 Direct Connect 是否存在潜在问题或安全威胁。
虚拟存储管理	Red Hat • 监控用于群集节点的 Amazon EBS 卷以及用于 ROSA 服务内置容器映像注册表的 Amazon S3 存储桶。响应提醒。	客户 • 监控应用程序数据的运行状况。 • 如果使用客户托管 AWS KMS keys ，请创建和控制用于 Amazon EBS 加密的密钥生命周期和密钥策略。
AWS 软件（公共 AWS 服务）	AWS • 有关 AWS 事件和运营管理的信息，请参阅 AWS 白皮书中的如何 AWS 保持运营弹性和服务的连续性。	Customer • 监控客户账户中 AWS 资源的运行状况。 • 使用 IAM 工具对客户账户中的 AWS 资源应用适当的权限。
硬件/AWS 全球基础架构	AWS • 有关 AWS 事件和运营管理的信息，请参阅 AWS 白皮书中的如何 AWS 保持运营弹性和服务的连续性。	客户 • 配置、管理和监控客户应用程序和数据，以确保正确实施应用程序和数据安全控制。

变更管理

AWS 负责保护运行中提供的所有服务的硬件基础架构 AWS Cloud。Red Hat 负责对客户将控制的集群基础设施和服务进行更改，以及维护控制面板节点、基础设施节点和 Worker 节点的版本。客户负责启

动基础设施变更。客户还负责安装和维护可选服务、集群上的联网配置以及对客户数据和应用程序的更改。

资源	服务责任	客户责任
日志记录	Red Hat • 集中汇总和监控平台审计日志。 • 提供并维护日志记录操作员，使客户能够为默认应用程序日志记录部署日志记录堆栈。 • 根据客户要求提供审计日志。	客户 • 在集群上安装可选的默认应用程序日志记录操作员。 • 安装、配置和维护任何可选的应用程序日志记录解决方案，例如记录附加容器或第三方日志记录应用程序。 • 如果客户应用程序生成的应用程序日志影响日志记录堆栈或集群的稳定性，请调整其大小和频率。 • 通过支持案例索取平台审计日志，以研究特定事件。
应用程序联网	Red Hat • 设置公有负载均衡器。能够在需要时设置专用负载均衡器和最多一个附加负载均衡器。 • 设置本地 OpenShift 路由器服务。能够将路由器设置为私有并最多添加一个路由器分片。 • 安装、配置和维护默认内部 Pod 流量的 OpenShift SDN 组件。 • 能够客户提供托管 `NetworkPolicy` 和	客户 • 使用 `NetworkPolicy` 对象为项目和容器组（pod）网络、容器组（pod）入口和容器组（pod）出口配置非默认容器组（pod）网络权限。 • 使用 OpenShift 集群管理器为默认应用程序路由请求私有负载均衡器。 • 使用 OpenShift 集群管理器最多配置一个额外的公共或私有路由器分片以及相应的负载均衡器。 • 为特定服务请求并配置任何附加的服务负载均衡器。

资源	服务责任	客户责任
	`EgressNetworkPolicy` （防火墙）对象。	• 配置任何必需的 DNS 转发规则。
集群联网	Red Hat • 设置集群管理组件，例如公共或私有服务端点以及与 Amazon VPC组件的必要集成。 • 设置 Worker 节点、基础设施节点和控制面板节点之间进行内部集群通信所需的内部联网组件。	客户 • 在配置集群时，如果需要，可通过 OpenShift 集群管理器为计算机 CIDR、服务 CIDR 和 pod CIDR 提供可选的非默认 IP 地址范围。 • 在创建集群时或通过 OpenShift 集群管理器创建集群后，请求将 API 服务终端节点设为公开或私有。
虚拟联网管理	Red Hat • 设置和配置配置集群所需的 Amazon VPC 组件，例如子网、负载均衡器、Internet 网关和 NAT 网关。 • 让客户能够根据需要通过 OpenShift 集群管理 Site-to-Site VPN 器管理与本地资源的连接、 Direct Connect 到 Amazon VPC VPC 的连接。 • 使客户能够创建和部署 AWS 负载均衡器以与服务负载均衡器配合使用。	Customer • 设置和维护可选 Amazon VPC 组件，例如 Amazon VPC到 vPC 的 Site-to-Site VPN 连接、连接或 Direct Connect。 • 为特定服务请求并配置任何附加的负载均衡器。

资源	服务责任	客户责任
虚拟计算管理	Red Hat • 设置和配置 ROSA 控制平面和数据平面以使用 Amazon EC2 实例进行集群计算。 • 监控和管理集群上 Amazon EC2 控制平面和基础设施节点的部署。	Customer • 通过使用 OpenShift 集群管理器或 ROSA CLI 创建计算机池来监控和管理 Amazon EC2 工作节点。 • 管理对客户部署应用程序和应用程序数据的更改。
集群版本	Red Hat • 启用升级计划流程。 • 监控升级进度并修复遇到的任何问题。 • 发布次要升级和维护升级的变更日志和版本说明。	客户 • 可以立即安排维护版本升级，以备将来使用，也可以自动升级。 • 确认并安排次要版本升级。 • 确保集群版本保持为支持的次要版本。 • 在次要版本和维护版本上测试客户应用程序，以确保兼容性。
容量管理	Red Hat • 监控控制面板的使用情况。控制面板包括控制面板节点和基础设施节点。 • 扩展和调整控制面板节点的大小以保持服务质量。	客户 • 监控 Worker 节点利用率，并在适当时启用自动扩缩功能。 • 确定集群的扩展策略。 • 使用提供的 OpenShift 集群管理器控件根据需要添加或删除其他工作节点。 • 回复有关集群资源要求的 Red Hat 通知。

资源	服务责任	客户责任
虚拟存储管理	Red Hat • 设置和配置为 Amazon EBS 为集群配置本地节点存储和永久卷存储。 • 设置并配置内置图像注册表以使用存储 Amazon S3 桶存储。 • 定期修剪映像注册表资源 Amazon S3 ，以优化 Amazon S3 使用率和集群性能。	Customer • （可选）配置 Amazon EBS CSI 驱动程序或 Amazon EFS CSI 驱动程序以在集群上配置永久卷。

资源	服务责任	客户责任

AWS 软件（公共 AWS 服务）	AWS
	
	计算
	
	• 提供 Amazon EC2 服务，用于 ROSA 控制平面、基础架构和工作节点。
	
	存储
	
	• 提供 Amazon EBS 以允许该 ROSA 服务为集群配置本地节点存储和永久卷存储。
	
	联网
	
	• 提供以下 AWS Cloud 服务以满足 ROSA 虚拟网络基础架构的需求：
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• 提供以下可选 AWS 服务 集成： ROSA
	  • Site-to-Site VPN
	  • Direct Connect
	  • AWS PrivateLink
	  • AWS Transit Gateway
		Customer
		
		• 使用与 IAM 委托人或 AWS STS 临时安全证书关联的访问密钥 ID 和私有访问密钥签署请求。
		• 为集群指定在创建集群时要使用的 VPC 子网。
		• （可选）配置客户托管的 VPC 以用于 ROSA 集群。

资源	服务责任	客户责任
硬件/AWS 全球基础架构	AWS • 有关 AWS 数据中心管理控制的信息，请参阅 “ AWS Cloud 安全” 页面上的 “我们的控制措施”。 • 有关变更管理最佳做法的信息，请参阅 AWS 解决方案库 AWS中的变更管理指南。	Customer • 为托管在 AWS Cloud上的客户应用程序和数据实施变更管理最佳实践。

访问和身份授权

访问和身份授权包括管理对集群、应用程序和基础设施资源授权访问的责任。这包括提供访问控制机制、身份验证、授权和管理对资源的访问等任务。

资源	服务责任	客户责任
日志记录	Red Hat • 遵守基于行业标准的分层内部访问流程来访问平台审计日志。 • 提供原生 OpenShift RBAC 功能。	Customer • 配置 OpenShift RBAC 以控制对项目的访问权限，进而控制项目的应用程序日志。 • 对于第三方或自定义应用程序日志记录解决方案，客户负责访问管理。
应用程序联网	Red Hat • 提供原生 OpenShift RBAC 和功能。`dedicated-admin`	Customer • 根据需要配置 OpenShift `dedicated-admin` 和 RBAC 以控制对路由配置的访问。 • 管理红帽组织管理员，让红帽授予对 OpenShift 集群管理器的访问权限。集群管理

资源	服务责任	客户责任
		器用于配置路由器选项和提供服务负载均衡器配额。
集群联网	Red Hat • 通过 OpenShift 集群管理器提供客户访问控制。提供原生 OpenShift RBAC 和功能。`dedicated-admin`	Customer • 根据需要配置 OpenShift `dedicated-admin` 和 RBAC 以控制对路由配置的访问。 • 管理 Red Hat 账户的 Red Hat 组织成员资格。 • 管理红帽的组织管理员以授予对 OpenShift 集群管理器的访问权限。
虚拟联网管理	Red Hat • 通过 OpenShift 集群管理器提供客户访问控制。	Customer • 通过 OpenShift 集群管理器管理用户对 AWS 组件的可选访问权限。
虚拟计算管理	Red Hat • 通过 OpenShift 集群管理器提供客户访问控制。	Customer • 通过 OpenShift 集群管理器管理用户对 AWS 组件的可选访问权限。 • 创建启用 ROSA 服务访问所需的 IAM 角色和附加策略。
虚拟存储管理	Red Hat • 通过 OpenShift 集群管理器提供客户访问控制。	Customer • 通过 OpenShift 集群管理器管理用户对 AWS 组件的可选访问权限。 • 创建启用 ROSA 服务访问所需的 IAM 角色和附加策略。

资源	服务责任	客户责任
AWS 软件（公共 AWS 服务）	AWS 计算 • 提供 Amazon EC2 服务，用于 ROSA 控制平面、基础架构和工作节点。 存储 • 提供 Amazon EBS，用于允许 ROSA 为集群配置本地节点存储和永久卷存储。 • 提供 Amazon S3，用于服务的内置图像注册表。 联网 • Provide AWS Identity and Access Management (IAM)，供客户用来控制对客户账户上运行的 ROSA 资源的访问权限。	Customer • 创建启用 ROSA 服务访问所需的 IAM 角色和附加策略。 • 使用 IAM 工具对客户账户中的 AWS 资源应用适当的权限。 • 为了 ROSA 在整个 AWS 组织中启用，客户负责管理管理 AWS Organizations 员。 • 为了 ROSA 在整个 AWS 组织中启用，客户负责使用分配 ROSA 权利授予 AWS License Manager。
硬件/AWS 全球基础架构	AWS • 有关 AWS 数据中心物理访问控制的信息，请参阅 “AWS Cloud 安全” 页面上的 “我们的控制措施”。	Customer • 客户对 AWS 全球基础设施不承担任何责任。

安全和法规合规性

以下是与合规相关的责任和控制措施：

资源	服务责任	客户责任
日志记录	Red Hat • 将集群审计日志发送到 Red Hat SIEM 以分析安全事件。在规定的时间段内保留审计日志，以支持取证分析。	客户 • 分析应用程序日志的安全事件。 • 如果需要的保留时间比默认日志堆栈提供的时间长，则通过日志记录附加容器或第三方日志记录应用程序将应用程序日志发送到外部端点。
虚拟联网管理	Red Hat • 监控虚拟联网组件是否存在潜在问题和安全威胁。 • 使用公共 AWS 工具进行额外的监控和保护。	客户 • 监控可选配置的虚拟联网组件是否存在潜在问题和安全威胁。 • 根据需要配置任何必需的防火墙规则或客户数据中心保护。
虚拟计算管理	Red Hat • 监控虚拟计算组件是否存在潜在问题和安全威胁。 • 使用公共 AWS 工具进行额外的监控和保护。	客户 • 监控可选配置的虚拟联网组件是否存在潜在问题和安全威胁。 • 根据需要配置任何必需的防火墙规则或客户数据中心保护。
虚拟存储管理	Red Hat • 监控虚拟存储组件是否存在潜在问题和安全威胁。 • 使用公共 AWS 工具进行额外的监控和保护。	Customer • 配置 Amazon EBS 卷。 • 管理 Amazon EBS 卷存储，确保有足够的存储空间可供作为卷装入 ROSA。

资源	服务责任	客户责任
	• 使用提供的 AWS 托管 KMS 密钥将 ROSA 服务配置 Amazon EBS 为默认加密控制平面、基础设施和工作节点卷数据。 • 将该 ROSA 服务配置为使用默认存储类别的客户永久卷以及 Amazon EBS 提供的 AWS 托管 KMS 密钥进行加密。 • 让客户能够使用客户托管对永久卷 KMS key 进行加密。 • 将容器映像注册表配置为使用 Amazon S3 托管密钥的服务器端加密来加密静态图像注册表数据 (SSE-3)。 • 让客户能够创建公共或私有 Amazon S3 镜像注册表，以保护其容器镜像免遭未经授权的用户访问。	• 创建永久卷声明并通过 OpenShift 集群管理器生成永久卷。

资源	服务责任	客户责任
AWS 软件（公共 AWS 服务）	AWS 计算 • 提供 Amazon EC2，用于 ROSA 控制平面、基础架构和工作节点。有关更多信息，请参阅《 Amazon EC2 用户指南》Amazon EC2中的基础设施安全。 存储 • 提供 Amazon EBS，用于 ROSA 控制平面、基础设施和工作节点卷，以及 Kubernetes 永久卷。有关更多信息，请参阅《 Amazon EC2 用户指南》Amazon EC2中的数据保护。 • Pro AWS KMS vid ROSA e，用于加密控制平面、基础架构、工作节点卷和永久卷。有关更多信息，请参阅《 Amazon EC2 用户指南》中的Amazon EBS 加密。 • 提供 Amazon S3，用于 ROSA 服务的内置容器镜像注册表。有关更多信息，请参阅《 Amazon S3 用户指南》中的Amazon S3 安全性。 联网	Customer • 确保遵循安全最佳实践和最小权限原则，以保护 Amazon EC2 实例上的数据。有关更多信息，请参阅Amazon EC2中的基础设施安全性和 Amazon EC2中的数据保护。 • 监控可选配置的虚拟联网组件是否存在潜在问题和安全威胁。 • 根据需要配置任何必需的防火墙规则或客户数据中心保护。 • 创建可选的客户托管 KMS 密钥并使用 KMS 密钥加密 Amazon EBS 永久卷。 • 监控虚拟存储中的客户数据是否存在潜在问题和安全威胁。有关更多信息，请参阅AWS 责任共担模式。

资源	服务责任	客户责任
	• 提供安全功能和服务，以增强隐私并控制 AWS 全球基础设施上的网络访问，包括内置的网络防火墙 Amazon VPC、私有或专用网络连接，以及自动加密 AWS 安全设施之间 AWS 全球和区域网络上的所有流量。有关更多信息，请参阅《安全简介》白皮书中的AWS 分担责任模型和基础设施 AWS 安全。	
硬件/AWS 全球基础架构	AWS • 提供 ROSA 用于提供服务功能的 AWS 全球基础架构。有关 AWS 安全控制的更多信息，请参阅 AWS 白皮书中的 AWS 基础设施安全。 • 为客户提供文档，以管理合规需求并 AWS 使用诸如 AWS Artifact 和 Security Hub 之类的工具检查其 AWS 安全状态。	客户 • 配置、管理和监控客户应用程序和数据，以确保正确实施应用程序和数据安全控制。 • 使用 IAM 工具对客户账户中的 AWS 资源应用适当的权限。

灾难恢复

灾难恢复包括数据和配置备份、灾难恢复环境的数据复制和配置，以及灾难事件的失效转移。

资源	服务责任	客户责任
虚拟联网管理	Red Hat	客户

资源	服务责任	客户责任
	• 还原或重新创建平台正常运行所必需的受影响虚拟网络组件。	• 尽可能使用多个隧道配置虚拟网络连接，以防止中断。 • 如果使用具有多个集群的全局负载均衡器，请保持失效转移 DNS 和负载均衡。
虚拟计算管理	Red Hat • 监控集群并更换出现故障的 Amazon EC2 控制平面或基础架构节点。 • 使客户能够手动或自动更换故障 Worker 节点。	客户 • 通过 OpenShift 集群管理器或 ROSA CLI 编辑计算机池配置来替换出现故障 Amazon EC2 的工作节点。
虚拟存储管理	Red Hat • 对于 AWS IAM 使用用户凭证创建的 ROSA 集群，请通过每小时、每日和每周的卷快照备份集群上的所有 Kubernetes 对象。	客户 • 备份客户应用程序和应用程序数据。

资源	服务责任	客户责任
AWS 软件（公共 AWS 服务）	AWS 计算 • 提供支持数据弹性的 Amazon EC2 功能，例如 Amazon EBS 快照和。 Amazon EC2 Auto Scaling 有关更多信息，请参阅《 Amazon EC2 用户指南》Amazon EC2中的弹性。 存储 • 使 ROSA 服务和客户能够通过卷快照备份集群上的 Amazon EBS Amazon EBS 卷。 • 有关支持数据弹性的 Amazon S3 功能的信息，请参阅中的弹性。 Amazon S3 联网 • 有关支持数据弹性的 Amazon VPC 功能的信息，请参阅《 Amazon VPC 用户指南》Amazon Virtual Private Cloud中的弹性。	Customer • 配置 ROSA 多可用区集群以提高容错能力和集群可用性。 • 使用 Amazon EBS CSI 驱动程序配置永久卷以启用卷快照。 • 创建 Amazon EBS 永久卷的 CSI 卷快照。

资源	服务责任	客户责任
硬件/AWS 全球基础架构	AWS • 提供 AWS 全球基础架构，ROSA 允许跨可用区扩展控制平面、基础设施和工作节点。此功能 ROSA 允许在不中断的情况下协调区域之间的自动故障转移。 • 有关灾难恢复最佳实践的更多信息，请参阅 Well-Architected F ramework 中的 AWS 云端灾难恢复选项。	Customer • 配置 ROSA 多可用区集群以提高容错能力和集群可用性。

数据和应用程序的客户责任

客户应对他们部署到的应用程序、工作负载和数据负责 AWS 云端 Red Hat OpenShift 服务。但是 AWS ，红帽提供了各种工具来帮助客户管理平台上的数据和应用程序。

资源	红帽如何 AWS 提供帮助	客户责任
客户数据	Red Hat • 维护行业安全和合规性标准所定义的平台级数据加密标准。 • 提供 OpenShift 组件以帮助管理应用程序数据，例如密钥。 • 启用与数据服务的集成 Amazon RDS ，例如存储和管理集群外部的数据和/或 AWS。 AWS	客户 • 对存储在平台上的所有客户数据以及客户应用程序如何使用和公开这些数据负责。

资源	红帽如何 AWS 提供帮助	客户责任
	• Amazon RDS 允许客户在集群之外存储和管理数据。	
客户应用程序	Red Hat • 配置已安装 OpenShift 组件的集群，以便客户可以访问 OpenShift 和 Kubernetes APIs 来部署和管理容器化应用程序。 • 使用映像拉取密钥创建集群，以便客户部署可以从 Red Hat 容器目录注册表中拉取映像。 • 提供客户可以用来设置运营商的访问权限，以便向集群添加社区 AWS、第三方和红帽服务。 OpenShift APIs • 提供存储类和插件以支持用于客户应用程序的持久性卷。 • 提供容器映像注册表，以便客户可以将应用程序容器映像安全地存储在集群上以部署和管理应用程序。 AWS • 提供 Amazon EBS 以支持用于客户应用程序的永久卷。 • 提供 Amazon S3 以支持红帽配置容器镜像注册表。	客户 • 对客户和第三方应用程序、数据以及整个应用程序生命周期负责。 • 如果客户使用操作员或外部映像将 Red Hat、社区、第三方、其自己或其他服务添加到集群，则客户应对这些服务负责，并负责与相应的提供商（包括 Red Hat）合作解决任何问题。 • 使用提供的工具和功能来配置和部署；保持最新状态；设置资源请求和限制；调整集群规模以拥有足够的资源来运行应用程序；设置权限；与其他服务集成；管理客户部署的任何映像流或模板；外部服务；保存、备份和还原数据；以其他方式管理其高可用性和弹性的工作负载。 • 负责监控运行的应用程序 AWS 云端 Red Hat OpenShift 服务，包括安装和操作软件以收集指标、创建警报和保护应用程序中的机密信息。

ROSA 建筑

AWS 云端 Red Hat OpenShift 服务 (ROSA) 具有以下集群拓扑：

- 托管控制平面 (HCP)-控制平面托管在红帽内部 AWS 账户 并由红帽管理。工作节点部署在客户的节点中 AWS 账户。
- Classic — 控制平面和工作节点部署在客户的控制平面和工作节点中 AWS 账户。

ROSA with HCP 提供了更高效的控制平面架构，有助于减少运行时产生的 AWS 基础设施费用，ROSA 并缩短集群创建时间。带有 HCP 的 ROSA 和 ROSA 经典版都可以在 AWS ROSA 控制台中启用。使用 ROSA CLI 配置 ROSA 集群时，您可以选择要使用的架构。

> **Note**
>
> - ROSA 在经典和托管控制平面架构上均提供 FedRAMP High 和 HIPAA 合格合规认证 AWS GovCloud 。有关更多信息，请参阅 Red Hat 文档中的 Compliance。
> - ROSA 在经典和托管控制平面架构中 AWS GovCloud 提供联邦信息处理标准 (FIPS) 端点。

比较 ROSA 与 HCP 和 ROSA 经典版

下表将 ROSA 与 HCP 和 ROSA 经典架构模型进行了比较。

	带 HCP 的 ROSA	ROSA 经典版
集群基础设施托管	控制平面组件，例如 etcd、API 服务器和 oauth，托管在红帽旗下的公司中。 AWS 账户	诸如 etcd、API 服务器和 oauth 之类的控制平面组件托管在客户拥有的服务器中。 AWS 账户
Amazon VPC	工作节点通过控制平面与控制平面通信AWS PrivateLink。	工作节点和控制平面节点部署在客户的 VPC 中。
AWS Identity and Access Management	使用 AWS 托管策略。	使用由服务定义的客户托管策略。

	带 HCP 的 ROSA	ROSA 经典版
多区域部署	控制平面跨多个可用区部署 (AZs)。	控制平面可以在单个可用区内部署，也可以跨多个可用区部署 AZs。
基础架构节点	不使用专用的基础设施节点。平台组件部署到工作节点上。	使用两个单可用区或三个多可用区专用节点来托管平台组件。
OpenShift 能力	平台监控、镜像注册表和入口控制器部署在工作节点中。	平台监控、镜像注册表和入口控制器部署在专用的基础设施节点中。
集群升级	控制平面和每个机器池可以单独升级。	必须同时升级整个集群。
Amazon EC2 占地面积最小	创建集群需要两个 Amazon EC2 实例。	创建集群需要七个单可用区 Amazon EC2 实例或九个多可用区实例。
AWS 区域	有关 AWS 区域 可用性，请参阅《 AWS 通用参考指南》中的AWS 云端 Red Hat OpenShift 服务 终端节点和配额。	有关 AWS 区域 可用性，请参阅《 AWS 通用参考指南》中的AWS 云端 Red Hat OpenShift 服务 终端节点和配额。

开始使用 ROSA

AWS 云端 Red Hat OpenShift 服务 (ROSA) 是一项托管服务，您可以使用它在红帽 OpenShift 企业 Kubernetes 平台上构建、扩展和部署容器化应用程序。 AWS

您可以使用以下指南创建您的第一个 ROSA 集群、授予用户访问权限、部署您的第一个应用程序，以及了解如何撤消用户访问权限和删除集群。

- the section called “创建 ROSA HCP 集群-CLI”-使用 AWS STS 和 C ROSA LI 使用 HCP 集群创建您的第一个 ROSA。
- the section called “创建 ROSA 经典集群- AWS PrivateLink ”-使用创建您的第一个 ROSA 经典集群 AWS PrivateLink。
- the section called “创建 ROSA 经典集群-CLI”-使用 AWS STS 和 ROSA CLI 创建您的第一个 ROSA 经典集群。

设置为使用 ROSA

要为创建 ROSA 集群做好环境准备，您需要完成以下操作。

先决条件

必须满足以下先决条件才能启用 ROSA 集群创建。

- 安装并配置最新版本 AWS CLI。有关更多信息，请参阅安装或更新 AWS CLI的最新版本。
- 安装和配置最新的 ROSA CLI 和 OpenShift 容器平台 CLI。有关更多信息，请参阅 ROSA CLI 入门。
- 必须为 Amazon EC2、 Amazon VPC Amazon EBS、和设置所需的服务配额 Elastic Load Balancing。 AWS 或者，红帽可能会根据需要代表您申请增加服务配额，以解决问题。要查看所需的服务配额 ROSA，请参阅《 AWS 一般参考》中的AWS 云端 Red Hat OpenShift 服务 终端节点和配额。
- 要获得 AWS 支持 ROSA，您必须启用 AWS 商业、企业入门计划或企业支持计划。红帽可能会根据需要代表您请求 AWS 支持，以解决问题。有关更多信息，请参阅 the section called “获取支持”。要启用 支持，请参阅支持 页面。
- 如果您使用 AWS Organizations 管理托管 ROSA 服务的 AWS 账户 ，则必须将组织的服务控制策略 (SCP) 配置为允许红帽不受限制地执行 SCP 中列出的策略操作。有关更多信息，请参阅the

section called “AWS Organizations 服务控制策略要求拒绝 AWS Marketplace 权限”。有关的更多信息 SCPs，请参阅服务控制策略 (SCPs)。

- 如果 AWS STS 将 ROSA 集群 带部署到默认处于禁 AWS 区域 用的启用状态，则必须 AWS 账户 使用以下命令将中所有区域的安全令牌更新为版本 2。

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

有关启用区域的更多信息，请参阅链接：accounts/latest/reference/manage

启用 ROSA 和配置 AWS 先决条件

要创建 ROSA 集群，您必须在 AWS ROSA 控制台中启用该 ROSA 服务。 AWS ROSA 控制台会验证您是否 AWS 账户 拥有必要的 AWS Marketplace 权限、服务配额以及名为 Elastic Load Balancing (ELB) 的服务相关角色。`AWSServiceRoleForElasticLoadBalancing`如果缺少这些先决条件中的任何一个，控制台将提供有关如何配置您的账户以满足先决条件的指导。

1. 导航至 ROSA 控制台。
2. 选择开始。
3. 在 “验证 ROSA 先决条件” 页面上，选择 “我同意与红帽共享我的联系信息”。
4. 选择启用 ROSA 。
5. 在该页面验证您的服务配额满足 ROSA 先决条件并创建了 ELB 服务相关角色后，请打开一个新的终端会话， ROSA 集群 使用 CLI ROSA 创建您的第一个终端会话。

使用 C ROSA LI 创建带有 HCP 集群的 ROSA

以下各节介绍如何使用托管控制平面（带有 HCP 的 ROSA） AWS STS 和 C ROSA LI 开始使用 ROSA。有关使用 Terraform 创建带有 HCP 集群的 ROSA 的步骤，请参阅红帽文档。要了解有关用于创建 ROSA 集群的 Terraform 提供程序的更多信息，请参阅 Terraform 文档。

ROSA CLI 使用`auto`模式或`manual`模式来创建所需 IAM 资源和 OpenID Connect (OIDC) 配置。 ROSA 集群`auto`模式会自动创建所需的 IAM 角色和策略以及 OIDC 提供者。 `manual`模式输出手动创建 IAM 资源所需的 AWS CLI 命令。通过使用`manual`模式，您可以在手动运行生成的 AWS CLI 命令之前查看这些命令。在 `manual` 模式下，您还可以将命令传递给组织中的其他管理员或组，以便其可以创建资源。

本文档中的过程使用 ROSA CLI `auto` 模式为使用 HCP 的 ROSA 创建所需的 IAM 资源和 OIDC 配置。有关入门的更多选项，请参阅开始使用 ROSA 。

主题

- 先决条件
- 创建 Amazon VPC 架构
- 创建所需的 IAM 角色和 OpenID Connect 配置
- 使用 C ROSA LI 创建带有 HCP 集群的 ROSA 和 AWS STS
- 配置身份提供商并授予 集群 访问权限
- 授予用户访问权限 集群
- 配置 cluster-admin 权限
- 配置 dedicated-admin 权限
- 集群 通过红帽混合云控制台访问
- 从开发者目录部署应用程序
- 撤销用户的 cluster-admin 权限
- 撤销用户的 dedicated-admin 权限
- 撤消用户对 a 的访问权限 集群
- 删除集群和 AWS STS 资源

先决条件

完成中列出的先决条件操作the section called “设置”。

创建 Amazon VPC 架构

以下过程创建了可用于托管集群的 Amazon VPC 架构。所有 集群 资源都托管在私有子网中。公有子网将来自私有子网的出站流量通过 NAT 网关路由到公有互联网。此示例使用 Amazon VPC的 CIDR 块 `10.0.0.0/16`。但您可以选择其他 CIDR 块。有关更多信息，请参阅 VPC 大小调整。

> **Important**
>
> 如果不 Amazon VPC 满足要求，集群创建将失败。

Example

Terraform

1. 安装 Terraform CLI。有关更多信息，请参阅 Terraform 文档中的安装说明。
2. 打开终端会话并克隆 Terraform VPC 存储库。

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

3. 导航到创建的目录。

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

4. 启动 Terraform 文件。

```
terraform init
```

完成后，CLI 会返回一条消息，说明 Terraform 已成功初始化。

5. 要基于现有模板构建 Terraform 计划，请运行以下命令。 AWS 区域 必须指定。或者，您可以选择指定集群名称。

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

命令运行后，会向hypershift-tf目录中添加一个rosa.tfplan文件。有关更多详细选项，请参阅 Terraform VPC 存储库的自述文件。

6. 应用计划文件来构建 VPC。

```
terraform apply rosa.tfplan
```

完成后，CLI 会返回一条成功消息，验证添加的资源。

a. （可选）为由 Terraform 配置的私有、公有和机器池子网创建环境变量， IDs 以便在使用 HCP 集群创建 ROSA 时使用。

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

b. （可选）验证环境变量设置是否正确。

```
echo $SUBNET_IDS
```

Amazon VPC console

1. 打开 Amazon VPC 控制台。
2. 在 VPC 控制面板上，选择创建 VPC。
3. 对于要创建的资源，选择 VPC 等。
4. 保持选中自动生成名称标签以为 VPC 资源创建名称标签，或者清除此选项以为 VPC 资源提供您自己的名称标签。
5. 在 IPv4 CIDR 块中，输入 VPC IPv4 的地址范围。VPC 必须有 IPv4 地址范围。
6. （可选）要支持 IPv6 流量，请选择 IPv6 CIDR 块，即亚马逊提供 IPv6 的 CIDR 块。
7. 将租赁保留为. `Default`
8. 在可用区数量 (AZs) 中，选择所需的数量。对于多可用区部署， ROSA 需要三个可用区。要 AZs 为您的子网选择，请展开自定义 AZs。

   > **Note**
   >
   > 某些 ROSA 实例类型仅在部分可用区域中可用。您可以使用 ROSA CLI `rosa list instance-types` 命令列出所有可用的 ROSA 实例类型。要检查某个实例类型是否适用于给定可用区，请使用 AWS CLI 命令`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`。

9. 要配置子网，请选择公有子网的数量和私有子网的数量的值。要选择子网的 IP 地址范围，请展开自定义子网 CIDR 块。

   > **Note**
   >
   > 带 HCP 的 ROSA 要求客户为每个可用区至少配置一个公有子网和私有子网，用于创建集群。

10. 要授予私有子网中的资源访问公有互联网的权限 IPv4，对于 NAT 网关，请选择要 AZs 在其中创建 NAT 网关的数量。在生产环境中，我们建议您在每个可用区部署一个 NAT 网关，其中包含需要访问公共互联网的资源。
11. （可选）如果您需要 Amazon S3 直接从 VPC 进行访问，请选择 VP C 终端节点，即 S3 网关。
12. 保留默认 DNS 选项处于选中状态。 ROSA 需要 VPC 上支持 DNS 主机名。

13展开其他标签，选择添加新标签，然后添加以下标签密钥。 ROSA 使用自动预检来验证是否使用了这些标签。

- 键：kubernetes.io/role/elb
- 键：kubernetes.io/role/internal-elb

14选择创建 VPC。

AWS CLI

1. 创建具有 10.0.0.0/16 CIDR 块的 VPC。

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

前面的命令返回 VPC ID。下面是一个示例输出。

```
vpc-1234567890abcdef0
```

2. 将 VPC ID 存储在环境变量中。

```
export VPC_ID=vpc-1234567890abcdef0
```

3. 使用VPC_ID环境变量为 VPC 创建Name标签。

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. 在 VPC 上启用 DNS 主机名支持。

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. 在 VPC 中创建公有和私有子网，指定应在其中创建资源的可用区。

> **Important**
>
> 带 HCP 的 ROSA 要求客户为每个可用区至少配置一个公有子网和私有子网，用于创建集群。对于多可用区部署，需要三个可用区。如果未满足这些要求，则集群创建失败。

> **Note**
>
> 某些 ROSA 实例类型仅在部分可用区域中可用。您可以使用 ROSA CLI `rosa list instance-types` 命令列出所有可用的 ROSA 实例类型。要检查某个实例类型是否适用于给定可用区，请使用 AWS CLI 命令`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`。

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. 将公有和私有子网存储 IDs 在环境变量中。

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. 为您的 VPC 子网创建以下标签。 ROSA 使用自动预检来验证是否使用了这些标签。

> **Note**
>
> 您必须至少标记一个私有子网，如果适用，还必须标记一个公有子网。

```
aws ec2 create-tags --resources $PUBLIC_SUB --tags Key=kubernetes.io/role/
elb,Value=1
aws ec2 create-tags --resources $PRIVATE_SUB --tags Key=kubernetes.io/role/
internal-elb,Value=1
```

8. 为出站流量创建互联网网关和路由表。为私有流量创建路由表和弹性 IP 地址。

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

9. 将环境变量存储 IDs 在环境中。

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

10.将互联网网关连接到 VPC。

```
aws ec2 attach-internet-gateway \
    --vpc-id $VPC_ID \
    --internet-gateway-id $IGW
```

11.将公有路由表关联到公有子网，并将流量配置为路由到 Internet 网关。

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

12.创建 NAT 网关并将其与弹性 IP 地址关联以启用流向私有子网的流量。

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

13.将私有路由表关联到私有子网，并将流量配置为路由到 NAT 网关。

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

14.（可选）对于多可用区部署，请重复上述步骤，再配置两个包含公有子网和私有子网的可用区。

创建所需的 IAM 角色和 OpenID Connect 配置

在使用 HCP 集群创建 ROSA 之前，必须创建必要的 IAM 角色和策略以及 OpenID Connect (OIDC) 配置。有关使用 HCP 的 ROSA 的 IAM 角色和策略的更多信息，请参阅the section called “ AWS 托管策略”。

此过程使用 ROSA CLI `auto` 模式自动创建带有 HCP 集群的 ROSA 所需的 OIDC 配置。

1. 创建所需的 IAM 账户角色和策略。该`--force-policy-creation`参数更新存在的所有现有角色和策略。如果没有任何角色和策略，则该命令会改为创建这些资源。

```
rosa create account-roles --force-policy-creation
```

> **Note**
>
> 如果您的离线访问令牌已过期，ROSA CLI 会输出一条错误消息，指出您的授权令牌需要更新。有关故障排除的步骤，请参阅the section called “ROSA CLI 过期的离线访问令牌疑难解答”。

2. 创建 OpenID Connect（OIDC）配置，以启用对集群的用户身份验证。此配置已注册为与 OpenShift 集群管理器 (OCM) 配合使用。

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

3. 复制 CL ROSA I 输出中提供的 OIDC 配置 ID。稍后需要提供 OIDC 配置 ID 才能创建带 HCP 的 ROSA 集群。
4. 要验证与您的用户组织相关联集群可用的 OIDC 配置，请运行以下命令。

```
rosa list oidc-config
```

5. 创建所需的 IAM 操作员角色，<OIDC_CONFIG_ID>替换为之前复制的 OIDC 配置 ID。

   Example

> **Important**
>
> 创建操作员角色时，必须在 <PREFIX_NAME> 中提供前缀。否则会产生错误。

```
rosa create operator-roles --prefix <PREFIX_NAME> --oidc-config-id <OIDC_CONFIG_ID>
 --hosted-cp
```

6. 要验证 IAM 操作员角色是否已创建，请运行以下命令：

```
rosa list operator-roles
```

使用 C ROSA LI 创建带有 HCP 集群的 ROSA 和 AWS STS

您可以 集群 使用 AWS Security Token Service (AWS STS) 和 C ROSA LI 中提供的`auto`模式创建 HCP 的 ROSA。您可以选择使用公共 API 和 Ingress 或私有 API 和 Ingress 创建集群。

您可以创建 集群 具有单个可用区（单可用区）或多个可用区（多可用区）的。无论哪种情况，您的计算机的 CIDR 值都必须匹配 VPC 的 CIDR 值。

以下过程使用`rosa create cluster --hosted-cp`命令创建带有 HCP 集群的单可用区 ROSA。要创建多可用区 集群，请在命令`multi-az`中指定要部署到 IDs 的每个私有子网的私有子网。

1. 使用以下命令之一，创建带 HCP 的 ROSA 集群。
   - 使用公共 API 和 Ingress 创建带有 HCP 集群的 ROSA，指定集群名称、操作员角色前缀、OIDC 配置 ID 以及公有和私有子网。 IDs

     ```
     rosa create cluster --cluster-name=<CLUSTER_NAME> --sts --mode=auto --hosted-cp --
     operator-roles-prefix <OPERATOR_ROLE_PREFIX> --oidc-config-id <OIDC_CONFIG_ID> --
     subnet-ids=<PUBLIC_SUBNET_ID>,<PRIVATE_SUBNET_ID>
     ```

   - 使用私有 API 和 Ingress 创建带有 HCP 集群的 ROSA，指定集群名称、操作员角色前缀、OIDC 配置 ID 和私有子网。 IDs

     ```
     rosa create cluster --private --cluster-name=<CLUSTER_NAME> --sts --mode=auto --
     hosted-cp --subnet-ids=<PRIVATE_SUBNET_ID>
     ```

2. 检查您的状态 集群。

   ```
   rosa describe cluster -c <CLUSTER_NAME>
   ```

   > **Note**
   >
   > 如果创建过程失败或`State`字段在 10 分钟后仍未变为就绪状态，请参阅问题排查。要联系 支持 我们的红帽支持部门寻求帮助，请参阅the section called “获取支持”。

3. 通过查看 OpenShift 安装程序日志来跟踪 集群 创建进度。

   ```
   rosa logs install -c <CLUSTER_NAME> --watch
   ```

配置身份提供商并授予 集群 访问权限

ROSA 包括内置 OAuth 服务器。创建 集群 完成后，必须配置 OAuth 为使用身份提供商。然后，您可以将用户添加到您配置的身份提供商，以授予其访问 集群的权限。您可以根据需要授予这些用户 `cluster-admin` 或 `dedicated-admin` 权限。

您可以为自己 ROSA 集群配置不同的身份提供商类型。支持的类型包括 GitHub En GitHub terprise、Google GitLab、LDAP、OpenID Connect 和 HTPasswd 身份提供商。

> **Important**
>
> 包含 HTPasswd 身份提供者只是为了允许创建单个静态管理员用户。 HTPasswd 不支持作为通用身份提供商。 ROSA

以下过程以配置 GitHub 身份提供者为例。有关如何配置每种支持的身份提供商类型的说明，请参阅为 AWS STS配置身份提供商。

1. 导航到 github.com 并登录到你的 GitHub 账户。
2. 如果您没有 GitHub 组织可以用于您的身份配置 集群，请创建一个组织。有关更多信息，请参阅 GitHub 文档中的步骤。
3. 使用 ROSA CLI 的交互模式，为您的集群配置身份提供商。

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 按照输出中的配置提示限制 GitHub 组织成员的 集群 访问权限。

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
```

```
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 在输出中打开 URL，<GITHUB_ORG_NAME>替换为您的 GitHub 组织名称。
6. 在 GitHub 网页上，选择注册应用程序以在您的 GitHub 组织中注册新 OAuth 应用程序。
7. 运行以下命令，使用 GitHub OAuth 页面中的信息填充剩余的`rosa create idp`交互式提示。用 GitHub OAuth 应用程序中的<GITHUB_CLIENT_SECRET>凭据替换<GITHUB_CLIENT_ID>和。

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> 身份提供商配置可能需要大约两分钟才能生效。如果您配置了`cluster-admin`用户，则可以运行`oc get pods -n openshift-authentication --watch`观看 OAuth pod 使用更新的配置重新部署。

8. 确认身份提供商已正确配置。

```
rosa list idps --cluster=<CLUSTER_NAME>
```

授予用户访问权限 集群

您可以通过将用户添加到已配置的身份提供商 集群 来授予他们对您的访问权限。

以下过程将用户添加到已配置为向集群配置身份的 GitHub 组织。

1. 导航到 github.com 并登录到你的 GitHub 账户。
2. 邀请需要 集群 访问您的 GitHub 组织的用户。有关更多信息，请参阅 GitHub 文档中的邀请用户加入您的组织。

配置 cluster-admin 权限

1. 通过运行以下命令授予 cluster-admin 权限。将 <IDP_USER_NAME> 和 <CLUSTER_NAME> 替换为您的用户名和集群名。

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户是否已列为 cluster-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

配置 dedicated-admin 权限

1. 通过使用以下命令授予 dedicated-admin 权限。运行以下命令<CLUSTER_NAME>，用您的用户集群 名和名称替换<IDP_USER_NAME>和。

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户是否已列为 cluster-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

集群 通过红帽混合云控制台访问

集群 通过红帽混合云控制台登录您的。

1. 集群 使用以下命令获取您的控制台 URL。<CLUSTER_NAME>用你的名字替换 集群。

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 导航到输出中的控制台 URL 并登录。

   在登录方式... 对话框中，选择身份提供商名称，然后完成提供商提出的任何授权请求。

从开发者目录部署应用程序

在 Red Hat Hybrid Cloud Console 中，您可以部署开发人员目录测试应用程序，并通过路由将其公开。

1. 导航到 Red Hat Hybrid Cloud Console，然后选择要将应用程序部署到的集群。
2. 在集群的页面上，选择 Open console。
3. 在 Administrator 视角中，选择 Home > Projects > Create Project。
4. 输入项目的名称，然后添加 Display Name 和 Description（可选）。
5. 选择 Create 以创建项目。
6. 切换到 Developer 视角并选择 +Add。确保所选的项目是刚刚创建的项目。
7. 在 Developer Catalog 对话框中，选择 All services。
8. 在 “开发者目录” 页面中，JavaScript从菜单中选择 “语言” >。
9. 选择 Node.js，然后选择 “创建应用程序” 以打开 “创建 Source-to-Image应用程序” 页面。

> **Note**
>
> 您可能需要选择 Clear All Filters 才能显示 Node.js 选项。

10. 在 Git 部分中，选择 Try Sample。
11. 在 Name 字段中，添加一个唯一的名称。
12. 选择创建。

> **Note**
>
> 部署新应用程序需要几分钟时间。

13. 部署完成后，选择应用程序的路由 URL。

    浏览器中将打开一个新选项卡，并显示与以下内容类似的一则消息。

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

14. （可选）删除应用程序并清理资源：
    a. 在 Administrator 视角中，选择 Home > Projects。
    b. 打开项目的操作菜单，然后选择 Delete Project。

撤销用户的 cluster-admin 权限

1. 使用以下命令撤销 cluster-admin 权限。<CLUSTER_NAME>用您的用户名<IDP_USER_NAME>和集群 名称替换和。

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户未列为 cluster-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

撤销用户的 dedicated-admin 权限

1. 通过使用以下命令，撤销 dedicated-admin 权限。<CLUSTER_NAME>用您的用户名<IDP_USER_NAME>和 集群 名称替换和。

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户未列为 dedicated-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

撤消用户对 a 的访问权限 集群

您可以通过将身份提供商用户从已配置的身份提供商中移除来撤消其 集群 访问权限。

您可以为自己的 集群配置不同类型的身份提供商。以下过程将撤消 GitHub 组织成员的 集群 访问权限。

1. 导航到 github.com 并登录到你的 GitHub 账户。
2. 将该用户从您的 GitHub 组织中移除。有关更多信息，请参阅 GitHub 文档中的从组织中移除成员。

删除集群和 AWS STS 资源

您可以使用 ROSA CLI 删除使用 AWS Security Token Service (AWS STS) 集群 的。您也可以使用 ROSA CLI 删除由创建的 IAM 角色和 OIDC 提供者。 ROSA要删除由创建的 IAM 策略 ROSA，您可以使用 IAM 控制台。

> **Note**
>
> IAM 由创建的角色和策略 ROSA 可能会被同一账户中的其他 ROSA 集群使用。

1. 删除 集群 并查看日志。将 <CLUSTER_NAME> 替换为 集群的名称或 ID。

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> 必须等待完全删除， 集群 然后才能移除 IAM 角色、策略和 OIDC 提供商。删除安装程序创建的资源需要账户 IAM 角色。需要操作员 IAM 角色才能清理 OpenShift 操作员创建的资源。操作员使用 OIDC 提供商进行身份验证。

2. 运行以下命令，删除 集群 操作员用来进行身份验证的 OIDC 提供商。

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. 删除特定于集群的操作员 IAM 角色。

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 使用以下命令删除账户的 IAM 角色。将 <PREFIX> 替换为要删除的账户 IAM 角色的前缀。如果您在创建账户 IAM 角色时指定了自定义前缀，请指定默认的 `ManagedOpenShift` 前缀。

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. 删除由创建的 IAM 策略 ROSA。
   a. 登录 IAM 控制台。
   b. 在左侧菜单的访问管理下，选择策略。
   c. 选择要删除的策略，然后选择操作 > 删除。
   d. 输入策略名称，然后选择删除。
   e. 重复此步骤以删除 集群的每个 IAM policy。

使用 ROSA CLI 创建 ROSA 经典集群

以下各节介绍如何使用 AWS STS 和 ROSA CLI 开始使用 ROSA classic。有关使用 Terraform 创建 ROSA 经典集群的步骤，请参阅红帽文档。要了解有关用于创建 ROSA 集群的 Terraform 提供程序的更多信息，请参阅 Terraform 文档。

C ROSA LI 使用automanual模式或模式来创建置备所需的 IAM 资源 ROSA 集群。 auto模式会立即创建所需的 IAM 角色和策略以及 OpenID Connect (OIDC) 提供程序。 manual模式输出创建 IAM 资源所需的 AWS CLI 命令。通过使用manual模式，您可以在手动运行生成的 AWS CLI 命令之前查看这些命令。在 manual 模式下，您还可以将命令传递给组织中的其他管理员或组，以便其可以创建资源。

有关入门的更多选项，请参阅开始使用 ROSA 。

主题

- 先决条件
- 使用 ROSA CLI 创建 ROSA 经典集群和 AWS STS
- 配置身份提供商并授予 集群 访问权限
- 向用户授予访问权限 集群
- 配置 cluster-admin 权限
- 配置 dedicated-admin 权限
- 集群 通过红帽混合云控制台访问
- 从开发者目录中部署应用程序
- 撤销用户的 cluster-admin 权限
- 撤销用户的 dedicated-admin 权限
- 撤消用户对 a 的访问权限 集群
- 删除集群和 AWS STS 资源

先决条件

完成中列出的先决条件操作the section called “设置”。

使用 ROSA CLI 创建 ROSA 经典集群和 AWS STS

您可以 集群 使用 ROSA CLI 和创建 ROSA 经典版 AWS STS。

1. 使用`--mode auto`或创建所需的 IAM 账户角色和策略`--mode manual`。

   -
     ```
     rosa create account-roles --classic --mode auto
     ```
   -
     ```
     rosa create account-roles --classic --mode manual
     ```

     > **Note**
     >
     > 如果您的离线访问令牌已过期，ROSA CLI 会输出一条错误消息，指出您的授权令牌需要更新。有关故障排除的步骤，请参阅the section called “ROSA CLI 过期的离线访问令牌疑难解答”。

2. 集群 使用`--mode auto`或创建一个`--mode manual`。 automode 允许您更快地创建集群。manualmode 会提示您为集群指定自定义设置。

   -
     ```
     rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode auto
     ```

     > **Note**
     >
     > 当您指定时`--mode auto`，该`rosa create cluster`命令会自动创建特定于集群的操作员 IAM 角色和 OIDC 提供者。操作员使用 OIDC 提供商进行身份验证。

     > **Note**
     >
     > 使用`--mode auto`默认值时，将安装最新的稳定 OpenShift 版本。

   -
     ```
     rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode manual
     ```

     > **Important**
     >
     > 如果您在`manual`模式下启用 etcd 加密，则会产生大约 20% 的性能开销。除了对 etcd 卷进行加密的默认 Amazon EBS 加密之外，还引入了第二层加密，从而产生了开销。

> **Note**
>
> 运行`manual`模式以创建集群后，您需要手动创建集群特定的操作员 IAM 角色和集群操作员用来进行身份验证的 OpenID Connect 提供程序。

3. 检查您的状态 集群。

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> 如果置备过程失败或`State`字段在 40 分钟后仍未更改为就绪状态，请参阅问题排查。要联系我们 支持 的 Red Hat 支持部门寻求帮助，请参阅the section called “获取支持”。

4. 通过查看 OpenShift 安装程序日志来跟踪 集群 创建进度。

```
rosa logs install -c <CLUSTER_NAME> --watch
```

配置身份提供商并授予 集群 访问权限

ROSA 包括内置 OAuth 服务器。创建 集群 完成后，必须配置 OAuth 为使用身份提供商。然后，您可以将用户添加到您配置的身份提供商，以授予其访问 集群的权限。您可以根据需要授予这些用户 `cluster-admin` 或 `dedicated-admin` 权限。

您可以为自己 ROSA 集群配置不同的身份提供商类型。支持的类型包括 GitHub En GitHub terprise、Google GitLab、LDAP、OpenID Connect 和 HTPasswd 身份提供商。

> **Important**
>
> 包含 HTPasswd 身份提供者只是为了允许创建单个静态管理员用户。 HTPasswd 不支持作为通用身份提供商。 ROSA

以下过程以配置 GitHub 身份提供者为例。有关如何配置每种支持的身份提供商类型的说明，请参阅为 AWS STS配置身份提供商。

1. 导航到 github.com 并登录到你的 GitHub 账户。
2. 如果您没有 GitHub 组织可以用于您的身份配置 集群，请创建一个组织。有关更多信息，请参阅 GitHub 文档中的步骤。
3. 使用 ROSA CLI 的交互模式，为您的集群配置身份提供商。

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 按照输出中的配置提示限制 GitHub 组织成员的 集群 访问权限。

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 在输出中打开 URL，<GITHUB_ORG_NAME>替换为您的 GitHub 组织名称。
6. 在 GitHub 网页上，选择注册应用程序以在您的 GitHub 组织中注册新 OAuth 应用程序。
7. 运行以下命令，使用 GitHub OAuth 页面中的信息填充剩余的`rosa create idp`交互式提示。用 GitHub OAuth 应用程序中的<GITHUB_CLIENT_SECRET>凭据替换<GITHUB_CLIENT_ID>和。

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
```

```
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> 身份提供商配置可能需要大约两分钟才能生效。如果您配置了`cluster-admin`用户，则可以运行`oc get pods -n openshift-authentication --watch`观看 OAuth pod 使用更新的配置重新部署。

8. 确认身份提供商已正确配置。

```
rosa list idps --cluster=<CLUSTER_NAME>
```

向用户授予访问权限 集群

您可以通过将用户添加到已配置的身份提供商 集群 来授予他们对您的访问权限。

以下过程将用户添加到已配置为向集群配置身份的 GitHub 组织。

1. 导航到 github.com 并登录到你的 GitHub 账户。
2. 邀请需要 集群 访问您的 GitHub 组织的用户。有关更多信息，请参阅 GitHub 文档中的邀请用户加入您的组织。

配置 `cluster-admin` 权限

1. 通过运行以下命令授予 `cluster-admin` 权限。将 <IDP_USER_NAME> 和 <CLUSTER_NAME> 替换为您的用户名和集群名。

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户是否已列为 `cluster-admins` 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

配置 dedicated-admin 权限

1. 通过使用以下命令授予 dedicated-admin 权限。运行以下命令<CLUSTER_NAME>，用您的用户集群 名和名称替换<IDP_USER_NAME>和。

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户是否已列为 cluster-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

集群 通过红帽混合云控制台访问

在创建 集群 管理员用户或向配置的身份提供商添加用户后，您可以 集群 通过红帽混合云控制台登录您的。

1. 集群 使用以下命令获取您的控制台 URL。<CLUSTER_NAME>用你的名字替换 集群。

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 导航到输出中的控制台 URL 并登录。
   - 如果您创建了 cluster-admin 用户，请使用提供的凭证登录。
   - 如果您为配置了身份提供商 集群，请在 “登录方式...” 对话框中选择身份提供商名称，然后完成您的提供商提出的任何授权请求。

从开发者目录中部署应用程序

在 Red Hat Hybrid Cloud Console 中，您可以部署开发人员目录测试应用程序，并通过路由将其公开。

1. 导航到 Red Hat Hybrid Cloud Console，然后选择要将应用程序部署到的集群。
2. 在集群的页面上，选择 Open console。
3. 在 Administrator 视角中，选择 Home > Projects > Create Project。
4. 输入项目的名称，然后添加 Display Name 和 Description（可选）。
5. 选择 Create 以创建项目。
6. 切换到 Developer 视角并选择 +Add。确保所选的项目是刚刚创建的项目。

7. 在 Developer Catalog 对话框中，选择 All services。
8. 在 “开发者目录” 页面中，JavaScript从菜单中选择 “语言” >。
9. 选择 Node.js，然后选择 “创建应用程序” 以打开 “创建 Source-to-Image应用程序” 页面。

> **Note**
> 您可能需要选择 Clear All Filters 才能显示 Node.js 选项。

10. 在 Git 部分中，选择 Try Sample。
11. 在 Name 字段中，添加一个唯一的名称。
12. 选择创建。

> **Note**
> 部署新应用程序需要几分钟时间。

13. 部署完成后，选择应用程序的路由 URL。

浏览器中将打开一个新选项卡，并显示与以下内容类似的一则消息。

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

14. (可选) 删除应用程序并清理资源：
    a. 在 Administrator 视角中，选择 Home > Projects。
    b. 打开项目的操作菜单，然后选择 Delete Project。

撤销用户的 `cluster-admin` 权限

1. 使用以下命令撤销 `cluster-admin` 权限。<CLUSTER_NAME>用您的用户名<IDP_USER_NAME>和集群 名称替换和。

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户未列为 `cluster-admins` 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

撤销用户的 dedicated-admin 权限

1. 通过使用以下命令，撤销 dedicated-admin 权限。<CLUSTER_NAME>用您的用户名<IDP_USER_NAME>和 集群 名称替换和。

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户未列为 dedicated-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

撤消用户对 a 的访问权限 集群

您可以通过将身份提供商用户从已配置的身份提供商中移除来撤消其 集群 访问权限。

您可以为自己的 集群配置不同类型的身份提供商。以下过程将撤消 GitHub 组织成员的 集群 访问权限。

1. 导航到 github.com 并登录到你的 GitHub 账户。
2. 将该用户从您的 GitHub 组织中移除。有关更多信息，请参阅 GitHub 文档中的从组织中移除成员。

删除集群和 AWS STS 资源

您可以使用 ROSA CLI 删除使用 AWS Security Token Service (AWS STS) 集群 的。您也可以使用 ROSA CLI 删除由创建的 IAM 角色和 OIDC 提供者。 ROSA要删除由创建的 IAM 策略 ROSA，您可以使用 IAM 控制台。

> **Important**
>
> IAM 由创建的角色和策略 ROSA 可能会被同一账户中的其他 ROSA 集群使用。

1. 删除 集群 并查看日志。将 <CLUSTER_NAME> 替换为 集群的名称或 ID。

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> 必须等待完全删除， 集群 然后才能移除 IAM 角色、策略和 OIDC 提供商。删除安装程序创建的资源需要账户 IAM 角色。需要操作员 IAM 角色才能清理 OpenShift 操作员创建的资源。操作员使用 OIDC 提供商进行身份验证。

2. 运行以下命令，删除 集群 操作员用来进行身份验证的 OIDC 提供商。

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. 删除特定于集群的操作员 IAM 角色。

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 使用以下命令删除账户的 IAM 角色。将 <PREFIX> 替换为要删除的账户 IAM 角色的前缀。如果您在创建账户 IAM 角色时指定了自定义前缀，请指定默认的 ManagedOpenShift 前缀。

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. 删除由创建的 IAM 策略 ROSA。
   a. 登录 IAM 控制台。
   b. 在左侧菜单的访问管理下，选择策略。
   c. 选择要删除的策略，然后选择操作 > 删除。
   d. 输入策略名称，然后选择删除。
   e. 重复此步骤以删除 集群的每个 IAM policy。

创建使用的 ROSA 经典集群 AWS PrivateLink

ROSA 经典集群可以通过几种不同的方式部署：公共集群、私有集群或私有集群 AWS PrivateLink。有关 ROSA 经典版的更多信息，请参阅the section called “架构”。对于公共配置和私 OpenShift 集群 有集群 配置，都可以访问互联网，并且在应用程序层对应用程序工作负载设置了隐私。

如果您要求 集群 和应用程序工作负载均为私有工作负载，则可以使用 ROSA classic AWS PrivateLink 进行配置。 AWS PrivateLink 是一种高度可用、可扩展的 ROSA 技术，用于在 ROSA 服务与 AWS 客户账户中的群集资源之间创建私有连接。借助 AWS PrivateLink，红帽站点可靠性工程 (SRE) 团队可以使用连接到集群 AWS PrivateLink 终端节点的私有子网访问集群以获得支持和补救。

有关的更多信息 AWS PrivateLink，请参阅什么是 AWS PrivateLink？

主题

- 先决条件
- 创建 Amazon VPC 架构
- 使用 ROSA CLI 创建 ROSA 经典集群和 AWS PrivateLink
- 配置 AWS PrivateLink DNS 转发
- 配置身份提供商并授予 集群 访问权限
- 向用户授予访问权限 集群
- 配置 cluster-admin 权限
- 配置 dedicated-admin 权限
- 集群 通过红帽混合云控制台访问
- 从开发者目录中部署应用程序
- 撤销用户的 cluster-admin 权限
- 撤销用户的 dedicated-admin 权限
- 撤消用户对 a 的访问权限 集群
- 删除集群和 AWS STS 资源

先决条件

完成中列出的先决条件操作the section called “设置”。

创建 Amazon VPC 架构

以下过程创建了可用于托管集群的 Amazon VPC 架构。所有 集群 资源都托管在私有子网中。公有子网将来自私有子网的出站流量通过 NAT 网关路由到公有互联网。此示例使用 Amazon VPC的 CIDR 块 `10.0.0.0/16`。但您可以选择其他 CIDR 块。有关更多信息，请参阅 VPC 大小调整。

> **Important**
>
> 如果不 Amazon VPC 满足要求，集群创建将失败。

Example

Amazon VPC console

1. 打开 Amazon VPC 控制台。
2. 在 VPC 控制面板上，选择创建 VPC。
3. 对于要创建的资源，选择 VPC 等。
4. 保持选中自动生成名称标签以为 VPC 资源创建名称标签，或者清除此选项以为 VPC 资源提供您自己的名称标签。
5. 在 IPv4 CIDR 块中，输入 VPC IPv4 的地址范围。VPC 必须有 IPv4 地址范围。
6. （可选）要支持 IPv6 流量，请选择 IPv6 CIDR 块，即亚马逊提供 IPv6 的 CIDR 块。
7. 将租赁保留为. `Default`
8. 在可用区数量 (AZs) 中，选择所需的数量。对于多可用区部署， ROSA 需要三个可用区。要 AZs 为您的子网选择，请展开自定义 AZs。

   > **Note**
   >
   > 某些 ROSA 实例类型仅在部分可用区域中可用。您可以使用 ROSA CLI `rosa list instance-types` 命令列出所有可用的 ROSA 实例类型。要检查某个实例类型是否适用于给定可用区，请使用 AWS CLI 命令`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`。

9. 要配置子网，请选择公有子网的数量和私有子网的数量的值。要选择子网的 IP 地址范围，请展开自定义子网 CIDR 块。

   > **Note**
   >
   > ROSA 要求客户为每个可用区配置至少一个用于创建集群的私有子网。

10. 要授予私有子网中的资源访问公有互联网的权限 IPv4，对于 NAT 网关，请选择要 AZs 在其中创建 NAT 网关的数量。在生产环境中，我们建议您在每个可用区部署一个 NAT 网关，其中包含需要访问公共互联网的资源。
11. （可选）如果您需要 Amazon S3 直接从 VPC 进行访问，请选择 VP C 终端节点，即 S3 网关。
12. 保留默认 DNS 选项处于选中状态。 ROSA 需要 VPC 上支持 DNS 主机名。

13选择创建 VPC。

AWS CLI

1. 创建具有 10.0.0.0/16 CIDR 块的 VPC。

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

前面的命令返回 VPC ID。下面是一个示例输出。

```
vpc-1234567890abcdef0
```

2. 将 VPC ID 存储在环境变量中。

```
export VPC_ID=vpc-1234567890abcdef0
```

3. 使用VPC_ID环境变量为 VPC 创建Name标签。

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. 在 VPC 上启用 DNS 主机名支持。

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. 在 VPC 中创建公有和私有子网，指定应在其中创建资源的可用区。

> **Important**
>
> ROSA 要求客户为每个可用区配置至少一个用于创建集群的私有子网。对于多可用区部署，需要三个可用区。如果未满足这些要求，则集群创建失败。

> **Note**
>
> 某些 ROSA 实例类型仅在部分可用区域中可用。您可以使用 ROSA CLI `rosa list instance-types` 命令列出所有可用的 ROSA 实例类型。要检查某个实例类型是否适用于给定可用区，请使用 AWS CLI 命令`aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`。

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. 将公有子网和私有子网存储 IDs 在环境变量中。

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. 为出站流量创建互联网网关和路由表。为私有流量创建路由表和弹性 IP 地址。

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
```

```
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

8. 将环境变量存储 IDs 在环境中。

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

9. 将互联网网关连接到 VPC。

```
aws ec2 attach-internet-gateway \
    --vpc-id $VPC_ID \
    --internet-gateway-id $IGW
```

10.将公有路由表关联到公有子网，并将流量配置为路由到 Internet 网关。

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

11.创建 NAT 网关并将其与弹性 IP 地址关联以启用流向私有子网的流量。

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

12.将私有路由表关联到私有子网，并将流量配置为路由到 NAT 网关。

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
```

```
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

13. (可选) 对于多可用区部署，请重复上述步骤，再配置两个包含公有子网和私有子网的可用区。

使用 ROSA CLI 创建 ROSA 经典集群和 AWS PrivateLink

您可以使用 ROSA CLI 和 AWS PrivateLink 创建 集群 具有单个可用区 (单可用区) 或多个可用区 (多可用区) 的。无论哪种情况，您的计算机的 CIDR 值都必须匹配 VPC 的 CIDR 值。

以下过程使用`rosa create cluster`命令创建 ROSA 经典版 集群。要创建多可用区 集群，请在命令`--multi-az`中指定，然后在出现提示时选择要 IDs 使用的私有子网。

> **Note**
>
> 如果您使用防火墙，则必须对其进行配置，使其 ROSA 能够访问其运行所需的站点。
> 有关更多信息，请参阅 Red Hat 文档中的AWS PrivateLink 集群使用要求。

1. 使用`--mode auto`或创建所需的 IAM 账户角色和策略`--mode manual`。

   -
     ```
     rosa create account-roles --classic --mode auto
     ```
   -
     ```
     rosa create account-roles --classic --mode manual
     ```

     > **Note**
     >
     > 如果您的离线访问令牌已过期， ROSA CLI 会输出一条错误消息，指出您的授权令牌需要更新。有关故障排除的步骤，请参阅the section called “ROSA CLI 过期的离线访问令牌疑难解答”。

2. 集群 通过运行以下命令之一来创建。

   - 单可用区

```
rosa create cluster --private-link --cluster-name=<CLUSTER_NAME> --machine-
cidr=10.0.0.0/16 --subnet-ids=<PRIVATE_SUBNET_ID>
```

- 多可用区

```
rosa create cluster --private-link --multi-az --cluster-name=<CLUSTER_NAME> --
machine-cidr=10.0.0.0/16
```

> **Note**
>
> 要创建使用 AWS PrivateLink with AWS Security Token Service (AWS STS) 短期凭证的集群，请在命令末尾追加`--sts --mode auto`或`--sts --mode manual`。`rosa create cluster`

3. 按照交互式提示创建 集群 操作员 IAM 角色。

```
rosa create operator-roles --interactive -c <CLUSTER_NAME>
```

4. 创建 集群 操作员用来进行身份验证的 OpenID Connect (OIDC) 提供程序。

```
rosa create oidc-provider --interactive -c <CLUSTER_NAME>
```

5. 检查您的状态 集群。

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> 该 集群 `State`字段最多可能需要 40 分钟才能显示`ready`状态。如果配置失败或`ready`在 40 分钟后未显示为，请参阅问题排查。要联系我们 支持 的 Red Hat 支持部门寻求帮助，请参阅the section called “获取支持”。

6. 通过查看 OpenShift 安装程序日志来跟踪 集群 创建进度。

```
rosa logs install -c <CLUSTER_NAME> --watch
```

配置 AWS PrivateLink DNS 转发

使用的集群在中 AWS PrivateLink 创建公共托管区域和私有托管区域 Route 53。 Route 53 私有托管区域内的记录只能从其分配到的 VPC 内部进行解析。

Let's Encrypt DNS-01 验证需要一个公有区域，以便能为该域颁发有效且公开信任的证书。在 Let's Encrypt 验证完成后，将删除验证记录。颁发和续订这些证书仍然需要使用该区域，通常每 60 天需要使用一次。尽管这些区域通常显示为空，但公有区域在验证过程中起着至关重要的作用。

有关 AWS 私有托管区域的更多信息，请参阅使用私有区域。有关公有托管区域更多信息，请参阅使用公有托管区域。

配置入 Route 53 Resolver 站终端节点

1. 要允许在 VPC 外部解析等记录`api.<cluster_domain>`和`*.apps.<cluster_domain>`解析，请配置 Route 53 Resolver 入站终端节点。

   > **Note**
   >
   > 配置入站终端节点时，需要至少指定两个 IP 地址以实现冗余。我们建议您在至少两个可用区中指定 IP 地址。您可以选择在这些可用区或其他可用区中指定其他 IP 地址。

2. 配置入站终端节点时，请选择创建集群时使用的 VPC 和私有子网。

为集群配置 DNS 转发

关联 Route 53 Resolver 内部终端节点并运行后，配置 DNS 转发，以便网络上的指定服务器可以处理 DNS 查询。

1. 将您的公司网络配置为将 DNS 查询转发到顶级域的 IP 地址，例如 `drow-pl-01.htno.p1.openshiftapps.com`。
2. 如果要将 DNS 查询从一个 VPC 转发到另一个 VPC，请按照管理转发规则中的说明进行操作。
3. 如果您要配置远程网络 DNS 服务器，请参阅特定的 DNS 服务器文档，为已安装的集群域配置选择性 DNS 转发。

配置身份提供商并授予 集群 访问权限

ROSA 包括内置 OAuth 服务器。创建 ROSA 集群 完成后，必须配置 OAuth 为使用身份提供商。然后，您可以将用户添加到您配置的身份提供商，以授予其访问 集群的权限。您可以根据需要授予这些用户 `cluster-admin` 或 `dedicated-admin` 权限。

您可以为自己的 集群配置不同的身份提供商类型。支持的类型包括 En GitHub terprise GitHub、Google GitLab、LDAP、OpenID Connect 和 HTPasswd 身份提供商。

> **Important**
>
> 包含 HTPasswd 身份提供者只是为了允许创建单个静态管理员用户。 HTPasswd 不支持作为通用身份提供商。 ROSA

以下过程以配置 GitHub 身份提供者为例。有关如何配置每种支持的身份提供商类型的说明，请参阅为 AWS STS配置身份提供商。

1. 导航到 github.com 并登录到你的 GitHub 账户。
2. 如果您没有 GitHub 组织可以用于您的身份配置 ROSA 集群，请创建一个组织。有关更多信息，请参阅 GitHub 文档中的步骤。
3. 使用 ROSA CLI 的交互模式，通过运行以下命令为您的集群配置身份提供商。

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 按照输出中的配置提示限制 GitHub 组织成员的 集群 访问权限。

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
```

```
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 在输出中打开 URL，<GITHUB_ORG_NAME>替换为您的 GitHub 组织名称。
6. 在 GitHub 网页上，选择注册应用程序以在您的 GitHub 组织中注册新 OAuth 应用程序。
7. 使用 GitHub OAuth 页面中的信息填充剩余的rosa create idp交互式提示，用 GitHub OAuth 应用程序中的<GITHUB_CLIENT_SECRET>凭据替换<GITHUB_CLIENT_ID>和。

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> 身份提供商配置可能需要大约两分钟才能生效。如果您配置了cluster-admin用户，则可以运行oc get pods -n openshift-authentication --watch命令来观察使用更新的配置重新部署 p OAuth od。

8. 确认身份提供商已正确配置。

```
rosa list idps --cluster=<CLUSTER_NAME>
```

向用户授予访问权限 集群

您可以通过将用户添加到已配置的身份提供商 集群 来授予他们对您的访问权限。

以下过程将用户添加到已配置为向集群配置身份的 GitHub 组织。

1. 导航到 github.com 并登录到你的 GitHub 账户。
2. 邀请需要 集群 访问您的 GitHub 组织的用户。有关更多信息，请参阅 GitHub 文档中的邀请用户加入您的组织。

配置 cluster-admin 权限

1. 使用以下命令授予 cluster-admin 权限。将 <IDP_USER_NAME> 和 <CLUSTER_NAME> 替换为您的用户名和集群名。

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户是否已列为 cluster-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

配置 dedicated-admin 权限

1. 使用以下命令授予 dedicated-admin 权限。<CLUSTER_NAME>用您的用户名<IDP_USER_NAME>和 集群 名称替换和。

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户是否已列为 cluster-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

集群 通过红帽混合云控制台访问

在您创建 集群 管理员用户或向配置的身份提供商添加用户后，您可以 集群 通过红帽混合云控制台登录您的。

1. 集群 使用以下命令获取您的控制台 URL。<CLUSTER_NAME>用你的名字替换 集群。

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 导航到输出中的控制台 URL 并登录。

- 如果您创建了 `cluster-admin` 用户，请使用提供的凭证登录。
- 如果您为配置了身份提供商 集群，请在 “登录方式...” 对话框中选择身份提供商名称，然后完成您的提供商提出的任何授权请求。

从开发者目录中部署应用程序

在 Red Hat Hybrid Cloud Console 中，您可以部署开发人员目录测试应用程序，并通过路由将其公开。

1. 导航到 Red Hat Hybrid Cloud Console，然后选择要将应用程序部署到的集群。
2. 在集群的页面上，选择 Open console。
3. 在 Administrator 视角中，选择 Home > Projects > Create Project。
4. 输入项目的名称，然后添加 Display Name 和 Description（可选）。
5. 选择 Create 以创建项目。
6. 切换到 Developer 视角并选择 +Add。确保所选的项目是刚刚创建的项目。
7. 在 Developer Catalog 对话框中，选择 All services。
8. 在 “开发者目录” 页面中，JavaScript从菜单中选择 “语言” >。
9. 选择 Node.js，然后选择 “创建应用程序” 以打开 “创建 Source-to-Image应用程序” 页面。

> **Note**
>
> 您可能需要选择 Clear All Filters 才能显示 Node.js 选项。

10. 在 Git 部分中，选择 Try Sample。
11. 在 Name 字段中，添加一个唯一的名称。
12. 选择创建。

> **Note**
>
> 部署新应用程序需要几分钟时间。

13. 部署完成后，选择应用程序的路由 URL。

浏览器中将打开一个新选项卡，并显示与以下内容类似的一则消息。

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

14. (可选) 删除应用程序并清理资源。
    a. 在 Administrator 视角中，选择 Home > Projects。
    b. 打开项目的操作菜单，然后选择 Delete Project。

撤销用户的 **cluster-admin** 权限

1. 使用以下命令撤销 cluster-admin 权限。<CLUSTER_NAME>用您的用户名<IDP_USER_NAME>和集群 名称替换和。

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户未列为 cluster-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

撤销用户的 **dedicated-admin** 权限

1. 使用以下命令撤销 dedicated-admin 权限。<CLUSTER_NAME>用您的用户名<IDP_USER_NAME>和 集群 名称替换和。

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 确认该用户未列为 dedicated-admins 组的成员。

```
rosa list users --cluster=<CLUSTER_NAME>
```

撤消用户对 a 的访问权限 集群

您可以通过将身份提供商用户从已配置的身份提供商中移除来撤消其 集群 访问权限。

您可以为自己的 集群配置不同类型的身份提供商。以下过程将撤消 GitHub 组织成员的 集群 访问权限。

1. 导航到 github.com 并登录到你的 GitHub 账户。

2. 将该用户从您的 GitHub 组织中移除。有关更多信息，请参阅 GitHub 文档中的从组织中移除成员。

删除集群和 AWS STS 资源

您可以使用 ROSA CLI 删除使用 AWS Security Token Service (AWS STS) 集群 的。您也可以使用 ROSA CLI 删除由创建的 IAM 角色和 OIDC 提供者。 ROSA要删除由创建的 IAM 策略 ROSA，您可以使用 IAM 控制台。

> **Important**
>
> IAM 由创建的角色和策略 ROSA 可能会被同一账户中的其他 ROSA 集群使用。

1. 删除 集群 并查看日志。将 <CLUSTER_NAME> 替换为 集群的名称或 ID。

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> 必须等待完全删除， 集群 然后才能移除 IAM 角色、策略和 OIDC 提供商。删除安装程序创建的资源需要账户 IAM 角色。需要操作员 IAM 角色才能清理 OpenShift 操作员创建的资源。操作员使用 OIDC 提供商进行身份验证。

2. 运行以下命令，删除 集群 操作员用来进行身份验证的 OIDC 提供商。

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. 删除特定于集群的操作员 IAM 角色。

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 使用以下命令删除账户的 IAM 角色。将 <PREFIX> 替换为要删除的账户 IAM 角色的前缀。如果您在创建账户 IAM 角色时指定了自定义前缀，请指定默认的 `ManagedOpenShift` 前缀。

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. 删除由创建的 IAM 策略 ROSA。

   a. 登录 IAM 控制台。

b. 在左侧菜单的访问管理下，选择策略。

c. 选择要删除的策略，然后选择操作 > 删除。

d. 输入策略名称，然后选择删除。

e. 重复此步骤以删除 集群的每个 IAM policy。

中的安全性 ROSA

云安全位于 AWS 是最高优先级。作为一个 AWS 客户，您将受益于专为满足最安全敏感组织的要求而构建的数据中心和网络架构。

安全是双方的共同责任 AWS 还有你。责任共担模型将其描述为云的安全性和云中的安全性：

- 云的安全 — AWS 负责保护正在运行的基础架构 AWS 中的服务 AWS Cloud。 AWS 还为您提供可以安全使用的服务。 Third-party 审计师定期测试和验证我们的安全有效性，这是其中的一部分 AWS 合规计划。了解适用于的合规计划 ROSA，参见 AWS 服务 按合规计划划分的范围。
- 云端安全 — 您的责任由 AWS 服务 你用的。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用时如何应用分担责任模型 ROSA。它向你展示了如何配置 ROSA 以实现您的安全与合规性目标。你还将学习如何使用其他 AWS 服务 这可以帮助您监控和保护您的 ROSA 资源。

内容

- 中的数据保护 ROSA
- 的身份和访问管理 ROSA
- 弹性在 ROSA
- 中的基础设施安全 ROSA

中的数据保护 ROSA

这个 the section called “责任” 文档和 AWS 责任共担模式 在中定义数据保护 ROSA。 AWS 负责保护运行所有网络的全球基础设施 AWS Cloud。Red Hat 负责保护集群基础设施和底层服务平台。客户负责维护对托管在此基础设施上的内容的控制。此内容包括的安全配置和管理任务 AWS 服务 你用的。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 责任共担模式和 GDPR 上的博客文章 AWS 安全博客。

出于数据保护的目的，我们建议您保护 AWS 账户 凭据并使用以下方式设置个人用户 AWS Identity and Access Management （ IAM ）。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（ MFA ）。

- 使用 SSL/TLS 与之沟通 AWS 资源。我们要求使用 TLS 1.2，并建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案，以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务，例如 Amazon Macie，这有助于发现和保护存储在 Amazon S3。
- 如果您在访问时需要经过 FIPS 140-2 验证的加密模块 AWS 通过命令行接口或 API，使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅美国联邦信息处理标准（FIPS）第 140-2 版。

我们强烈建议您切勿将敏感的可识别信息（例如您客户的账号）放入自由格式字段（例如名称字段）。这包括当你与之合作时 ROSA 或者其他 AWS 服务 使用控制台、API、 AWS CLI，或 AWS 软件开发工具包。您输入的任何数据 ROSA 或者其他服务可能会被选中以包含在诊断日志中。当您向外部服务器提供 URL 时，请勿在 URL 中包含凭证信息来验证您对该服务器的请求。

主题

- 使用加密保护数据

使用加密保护数据

数据保护是指在数据传输过程中（往返传输时）保护数据 ROSA）和静止状态（当它存储在磁盘上时） AWS 数据中心）。

AWS 云端 Red Hat OpenShift 服务 提供安全访问 Amazon Elastic Block Store （Amazon EBS) 连接的存储卷 Amazon EC2 的实例 ROSA 控制平面、基础架构和工作节点，以及用于永久存储的 Kubernetes 永久卷。 ROSA 对静态和传输中的海量数据进行加密，并使用 AWS Key Management Service （AWS KMS) 以帮助保护您的加密数据。该服务使用 Amazon S3 用于容器镜像注册表存储，默认情况下处于静态加密状态。

> **Important**
>
> 因为 ROSA 是一项托管服务， AWS 而红帽则负责管理基础架构 ROSA 使用。客户不应尝试手动关闭 Amazon EC2 这样的实例 ROSA 的用途 AWS 控制台或 CLI。此操作可能会导致客户数据丢失。

的数据加密 Amazon EBS-支持的存储卷

AWS 云端 Red Hat OpenShift 服务 使用 Kubernetes 永久卷 (PV) 框架允许集群管理员为集群配置永久存储。永久卷以及控制平面、基础架构和工作节点均由 Amazon Elastic Block Store （ Amazon EBS) 连接的存储卷 Amazon EC2 实例。

对于 ROSA 永久卷和节点由 Amazon EBS，加密操作发生在托管 EC2 实例的服务器上，从而确保静态数据和在实例与其附加存储之间传输的数据的安全。有关更多信息，请参阅 Amazon EBS 加密 在 Amazon EC2 用户指南。

的数据加密 Amazon EBS CSI 驱动程序和 Amazon EFS CSI 驱动程序

ROSA 默认为使用 Amazon EBS 要配置的 CSI 驱动程序 Amazon EBS 存储。这个 Amazon EBS CSI 驱动程序和 Amazon EBS 默认情况下，CSI 驱动程序操作员安装在集群上 `openshift-cluster-csi-drivers` 命名空间。这个 Amazon EBS CSI 驱动程序和操作员允许您动态配置永久卷和创建卷快照。

ROSA 还能够使用配置永久卷 Amazon EFS CSI 驱动程序和 Amazon EFS CSI 司机操作员。这个 Amazon EFS 驱动程序和操作员还允许你在 pod 之间或与 Kubernetes 内部或外部的其他应用程序共享文件系统数据。

两者的体积数据在传输过程中都是安全的 Amazon EBS CSI 驱动程序和 Amazon EFS CSI 驱动程序。有关更多信息，请参阅 Red Hat 文档中的使用 Container Storage Interface （ CSI ）。

> **Important**
>
> 动态配置时 ROSA 使用永久音量 Amazon EFS CSI 驱动程序， Amazon EFS 评估文件系统权限时，会考虑接入点的用户 ID、群组 ID (GID) 和辅助组 ID。 Amazon EFS 将文件上的用户和群组 ID 替换为接入点上的用户和群组 ID，并忽略 NFS 客户端 ID。结果， Amazon EFS 默默地忽略 `fsGroup` 设置。 ROSA 无法使用替换文件的 GID `fsGroup`。任何可以访问已安装的 pod Amazon EFS 接入点可以访问卷上的任何文件。有关更多信息，请参阅 与... 合作 Amazon EFS 接入点 在 Amazon EFS 用户指南。

etcd 加密

ROSA 提供了启用加密的选项 `etcd` 中的键值 `etcd` 创建集群期间的容量，增加了额外的加密层。加密 `etcd` 后，您将额外产生大约 20% 的性能开销。我们建议您仅在用例特别需要的情况下启用 `etcd` 加密。有关更多信息，请参阅 etcd 加密 在 ROSA 服务定义。

密钥管理

ROSA 使用 KMS keys 安全地管理控制平面、基础架构和工作人员数据量以及客户应用程序的永久容量。在创建集群期间，您可以选择使用默认 AWS 管理 KMS key 提供者 Amazon EBS，或者指定您自己的客户管理密钥。有关更多信息，请参阅 the section called “密钥管理”。

内置映像注册表的数据加密

ROSA 提供内置容器镜像注册表，用于存储、检索和共享容器镜像 Amazon S3 桶存储。注册表由配置和管理 OpenShift 图像注册管理运营商。它为用户提供了一个开箱即用的解决方案，用于管理运行其工作负载并在现有集群基础设施之上运行的映像。有关更多信息，请参阅 Red Hat 文档中的注册表。

ROSA 提供公共和私有镜像注册表。对于企业应用程序，我们建议使用私有注册表来保护您的映像不被未经授权的用户使用。为了保护注册表的静态数据， ROSA 默认使用服务器端加密 Amazon S3 管理密钥（SSE-S3）。这不需要您采取任何行动，且不会另外收取费用。有关更多信息，请参阅 使用服务器端加密保护数据 Amazon S3 托管加密密钥 (SSE-S3) 在 Amazon S3 用户指南。

ROSA 使用传输层安全 (TLS) 协议来保护传入和传出映像注册表的数据。有关更多信息，请参阅 Red Hat 文档中的注册表。

互联网络流量隐私

AWS 云端 Red Hat OpenShift 服务 使用 Amazon Virtual Private Cloud （Amazon VPC) 在您的资源之间创建边界 ROSA 集群并控制它们、您的本地网络和互联网之间的流量。有关以下内容的更多信息 Amazon VPC 安全，请参阅 网际流量隐私 Amazon VPC 在 Amazon VPC 用户指南。

在 VPC 中，您可以配置您的 ROSA 集群使用 HTTP 或 HTTPS 代理服务器拒绝直接访问互联网。如果您是集群管理员，则还可以在容器级别定义网络策略，将网际流量限制到您的 Pod ROSA 集群。有关更多信息，请参阅 the section called “基础设施安全性”。

使用 KMS 进行数据加密

ROSA 使用 AWS KMS 安全地管理加密数据的密钥。默认情况下，控制平面、基础设施和工作节点卷使用加密 AWS 管理 KMS key 提供者 Amazon EBS。这个 KMS key 有别名 `aws/ebs`。默认情况下，使用默认 gp3 存储类的持久性卷也会使用此 KMS key进行加密。

新创建 ROSA 集群配置为使用默认 gp3 存储类对永久卷进行加密。只有将存储类别配置为进行加密时，才会对使用任何其他存储类创建的持久性卷进行加密。有关以下内容的更多信息 ROSA 预建存储类，请参阅 配置永久存储 在红帽文档中。

在创建集群期间，您可以选择使用默认值对集群中的永久卷进行加密 Amazon EBS-提供密钥，或指定您自己的客户管理对称密钥 KMS key。有关创建密钥的更多信息，请参阅 创建对称加密 KMS 密钥 在 AWS KMS 开发者指南。

您还可以通过定义 KMS key来加密集群中各个容器的持久性卷。当您在部署到时有明确的合规性和安全指导时，这很有用 AWS。有关更多信息，请参阅 开启对容器永久卷进行加密 AWS 用 KMS key 在红帽文档中。

在使用自己的 KMS keys加密持久性卷时，应考虑以下要点：

- 当您将 KMS 加密与自己的加密一起使用时 KMS key，密钥必须存在于同一个密钥中 AWS 区域 作为您的集群。
- 创建和使用自己的内容需要付费 KMS keys。有关更多信息，请参阅AWS Key Management Service 定价。

的身份和访问管理 ROSA

AWS Identity and Access Management （ IAM) 是一个 AWS 服务 这可以帮助管理员安全地控制访问权限 AWS 资源。 IAM 管理员控制谁能成为 身份验证 （ 已登录 ）和 授权 （ 有权限 ）使用 ROSA 资源。 IAM 是一个 AWS 服务 您无需额外付费即可使用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- ROSA 基于身份的策略示例
- AWS 的托管策略 ROSA
- 故障排除 ROSA 身份和访问权限

受众

你怎么用 AWS Identity and Access Management （ IAM) 有所不同，具体取决于你所做的工作 ROSA。

服务用户 -如果你使用 ROSA 服务来完成您的工作，然后您的管理员会为您提供所需的证书和权限。当你使用更多时 ROSA 功能要完成工作，您可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问中的功能 ROSA，参见 the section called “故障排除”。

服务管理员 -如果你负责 ROSA 贵公司的资源，你可能有完全访问权限 ROSA。你的工作是决定哪个 ROSA 您的服务用户应访问的功能和资源。然后，您必须向您提交请求 IAM 管理员来更改您的服务用户的权限。查看此页面上的信息，了解以下内容的基本概念 IAM。

IAM 管理员 -如果你是一个 IAM 管理员，您可能想了解有关用于管理访问权限的策略的详细信息 ROSA。查看示例 ROSA 您可以在中使用的基于身份的策略 IAM，参见 the section called “ ROSA 基于身份的策略示例”。

使用身份进行身份验证

身份验证是您登录的方式 AWS 使用您的身份凭证。你一定是 身份验证 （ 已登录到 AWS) 作为 AWS 账户 root 用户，一个 IAM 用户，或者假设 IAM 角色。

你可以登录 AWS 使用通过身份源提供的凭证作为联邦身份。 AWS IAM Identity Center （ IAM Identity Center) 用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据都是联邦身份的示例。当您以联合身份登录时，您的管理员之前使用设置了联合身份 IAM 角色。当你访问时 AWS 通过使用联邦，你间接扮演了一个角色。

根据您的用户类型，您可以登录 AWS 管理控制台 或者 AWS 访问门户。有关登录的更多信息 AWS，参见 如何登录您的 AWS 账户 在 AWS Sign-In 用户指南。

如果你访问 AWS 以编程方式， AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，用于使用您的证书对您的请求进行加密签名。如果你不使用 AWS 工具，你必须自己签署请求。有关使用推荐方法自行签署请求的更多信息，请参阅 签名 AWS API 请求 在 IAM 用户指南。

无论使用何种身份验证方法，您可能还需要提供其它安全信息。例如， AWS 建议您使用多因素身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅 Multi-factor 身份验证 在 AWS IAM 身份中心（继任者 AWS 单身 Sign-On) 用户指南 和 在中使用多因素身份验证 (MFA) AWS 在 IAM 用户指南。

AWS 账户 根用户

当你创建一个 AWS 账户，您首先要使用对所有人具有完全访问权限的单一登录身份 AWS 服务 以及账户中的资源。这个身份被称为 AWS 账户 root 用户，使用创建帐户时使用的电子邮件地址和密码登录即可访问。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要你以 root 用户身份登录的任务的完整列表，请参阅 需要根用户证书的任务 在 IAM 用户指南。

联合身份

最佳做法是，要求人类用户（包括需要管理员访问权限的用户）使用联合身份提供商进行访问 AWS 服务 通过使用临时证书。

联合身份是来自您的企业用户目录的用户、Web 身份提供商、 AWS Directory Service、身份中心目录或任何访问的用户 AWS 服务 使用通过身份源提供的证书。当联合身份访问时 AWS 账户，他们扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以供您的所有用户和群组使用 AWS 账户 和应用程序。有关 IAM 身份中心的信息，请参阅 什么是 IAM 身份中心？ 在 AWS IAM 身份中心（继任者 AWS 单身 Sign-On) 用户指南。

IAM 用户 和群组

一个 IAM 用户 是你内在的身份 AWS 账户 对个人或应用程序具有特定权限。在可能的情况下，我们建议依赖临时证书而不是创建 IAM 用户 拥有密码和访问密钥等长期凭证的人。但是，如果您有需要长期证书的特定用例 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用案例，应在需要时更新访问密钥。

一个 IAM 组 是一个身份，它指定了一个集合 IAM 用户。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，你可以有一个名为的群组 iamAdmins 并授予该群组的管理权限 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 何时创建 IAM 用户（而不是角色） 在 IAM 用户指南。

IAM 角色

一个 IAM 角色 是你内在的身份 AWS 账户 具有特定权限。它类似于 IAM 用户，但与特定人员无关。你可以暂时假设 IAM 中的角色 AWS 管理控制台 通过 切换角色。你可以通过调用来代入角色 AWS CLI 要么 AWS API 操作或使用自定义 URL。有关使用角色的方法的更多信息，请参阅 使用 IAM 角色 在 IAM 用户指南。

IAM 具有临时证书的角色在以下情况下很有用：

- 联邦用户访问权限 -要为联合身份分配权限，您需要创建一个角色并为该角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供者创建角色。如果您使用 IAM Identity

Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 会将权限集与 IAM中的角色相关联。有关权限集的信息，请参见 权限集 在 AWS IAM 身份中心（继任者 AWS 单身 Sign-On) 用户指南。

- 暂时的 IAM 用户 许可 -一个 IAM 用户 可以假设 IAM 角色可暂时为特定任务承担不同的权限。
- Cross-account 访问 -你可以使用 IAM 角色允许其他账户中的某人（可信委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，有些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅 怎么样 IAM 角色不同于基于资源的策略 在 IAM 用户指南。
- Cross-service 访问 -一些 AWS 服务 使用其他功能 AWS 服务。例如，当您在服务中进行调用时，该服务通常会在中运行应用程序 Amazon EC2 或者将对象存储在 Amazon S3。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS)-当你使用 IAM 用户 或者要在其中执行操作的角色 AWS，你被视为校长。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用委托人的权限调用 AWS 服务，再加上请求 AWS 服务 向下游服务发出请求。仅当服务收到需要与其他服务进行交互的请求时，才会发出 FAS 请求 AWS 服务 或需要完成的资源。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 -服务角色是 IAM 服务为代表您执行操作而承担的角色。一个 IAM 管理员可以在内部创建、修改和删除服务角色 IAM。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - Service-linked 角色 -服务相关角色是一种链接到的服务角色 AWS 服务。该服务可以代替您执行操作。 Service-linked 角色显示在您的 IAM 帐户，归该服务所有。一个 IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 正在运行的应用程序 Amazon EC2 -你可以使用 IAM 角色用于管理在上运行的应用程序的临时证书 Amazon EC2 实例和制作 AWS CLI 要么 AWS API 请求。这比将访问密钥存储在 Amazon EC2 实例。要分配 AWS 角色改为 Amazon EC2 实例并将其提供给其所有应用程序，您可以创建一个附加到该实例的实例配置文件。实例配置文件包含角色并启用在上运行的程序 Amazon EC2 获取临时证书的实例。有关更多信息，请参阅 使用 IAM 角色为在其上运行的应用程序授予权限 Amazon EC2 实例 在 IAM 用户指南。

要了解是否使用 IAM 角色或 IAM 用户，请参阅 何时创建 IAM 角色（而不是用户） 在 IAM 用户指南。

使用策略管理访问

您可以控制访问权限 AWS 通过创建策略并将其附加到 AWS 身份或资源。策略是其中的一个对象 AWS 当与身份或资源关联时，它定义了他们的权限。 AWS 当委托人（用户、根用户或角色会话）提

出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略存储在 AWS 作为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 AWS 用于指定谁有权访问什么的 JSON 策略。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限， IAM 管理员可以创建 IAM 政策。然后，管理员可以添加 IAM 策略到角色，用户可以代入角色。

IAM 无论您使用哪种方法执行操作，策略都会定义操作的权限。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从中获取角色信息 AWS 管理控制台， AWS CLI，或者 AWS API。

Identity-based 策略

Identity-based 策略是您可以附加到身份的 JSON 权限策略文档，例如 IAM 用户、角色或群组。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的政策，请参阅 正在创建 IAM 策略 在 IAM 用户指南。

Identity-based 政策可以进一步归类为 内联策略 要么 托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到您的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户管理策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南中的在托管式策略与内联策略之间进行选择。

Resource-based 策略

Resource-based 策略是您附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

Resource-based 策略是位于该服务中的内联策略。你不能用 AWS 来自的托管策略 IAM 在基于资源的政策中。

访问控制列表（ACL）

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，但它们不使用 JSON 策略文档格式。

Amazon S3， AWS WAF，以及 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述 在 亚马逊简单存储服务用户指南。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 -权限边界是一项高级功能，您可以在其中设置基于身份的策略可以授予的最大权限 IAM 实体（IAM 用户 或角色）。您可为实体设置权限边界。由此产生的权限是实体基于身份的策略及其权限边界的交叉点。 Resource-based 在中指定用户或角色的策略 `Principal` 字段不受权限边界的限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 的权限边界 IAM 实体 在 IAM 用户指南。
- 服务控制策略 (SCP) -SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限 AWS Organizations。 AWS Organizations 是一项用于对多个进行分组和集中管理的服务 AWS 账户 您的企业拥有的。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略（SCP）。SCP 限制成员账户中实体的权限，包括每个实体的权限 AWS 账户 root 用户。有关组织和 SCP 的更多信息，请参阅 服务控制策略 (SCP) 在 AWS Organizations 用户指南。
- 会话策略 - 会话策略是高级策略，在以编程方式为角色或联合身份用户创建临时会话时，这些策略将作为参数进行传递。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解如何做 AWS 确定在涉及多种策略类型时是否允许请求，请参阅 策略评估逻辑 在 IAM 用户指南。

ROSA 基于身份的策略示例

默认情况下， IAM 用户 而且角色没有权限创建或修改 AWS 资源。他们也无法使用执行任务 AWS 管理控制台， AWS CLI，或 AWS API。一个 IAM 管理员必须创建 IAM 策略授予用户和角色对他们所需的特定资源执行特定 API 操作的权限。然后，管理员必须将这些策略附加到 IAM 用户 或需要这些权限的群组。

要学习如何创建 IAM 使用这些示例 JSON 策略文档的基于身份的策略，请参阅 在 JSON 选项卡上创建策略 在 IAM 用户指南。

使用 ROSA 控制台

订阅 ROSA 在控制台中，您的 IAM 委托人必须具备所需的 AWS Marketplace 权限。权限允许委托人订阅和取消订阅 ROSA 中的产品清单 AWS Marketplace 并查看 AWS Marketplace 订阅。要添加所需

的权限，请转到 ROSA 控制台 并附上 AWS 托管策略 ROSAManageSubscription 致您的 IAM 负责人。有关 ROSAManageSubscription的更多信息，请参阅the section called “AWS 管理策略：ROSAManageSubscription”。

授权 ROSA 让 HCP 进行管理 AWS 资源

使用托管控制平面 (HCP) 的 ROSA AWS 具有服务操作和支持所需权限的托管策略。你使用 ROSA CLI 或 IAM 控制台将这些策略附加到您的服务角色 AWS 账户。

有关更多信息，请参阅 the section called “ AWS 托管策略”。

授权 ROSA classic 进行管理 AWS 资源

ROSA classic 使用客户管理的 IAM 策略，其权限由服务预先定义。你使用 ROSA 使用 CLI 创建这些策略并将其附加到您的中的服务角色 AWS 账户。 ROSA 要求按照服务定义配置这些策略，以确保持续运行和服务支持。

> **Note**
>
> 在未事先咨询红帽之前，您不应更改 ROSA 经典政策。这样做可能会使红帽99.95%的集群正常运行时间服务级别协议失效。带有托管控制飞机的罗莎用途 AWS 权限更有限的托管策略。有关更多信息，请参阅 the section called “ AWS 托管策略”。

有两种类型的客户管理策略 ROSA: 账户政策和运营商政策。账户政策附于 IAM 该服务使用这些角色与 Red Hat 建立信任关系，以提供站点可靠性工程师 (SRE) 支持、集群创建和计算功能。运营商政策附于 IAM 那个角色 OpenShift 操作员用于与入口、存储、映像注册表和节点管理相关的集群操作。账户政策每次创建一次 AWS 账户，而运营商策略是为每个集群创建一次的。

有关更多信息，请参阅the section called “ROSA 经典账户政策”和the section called “ROSA 经典运营商政策”。

允许用户查看他们自己的权限

此示例说明如何创建允许的策略 IAM 用户 查看附加到其用户身份的内联和托管策略。此策略包括在控制台上完成此操作的权限，或使用编程方式完成此操作的权限 AWS CLI。

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Effect": "Allow",
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

ROSA 经典账户政策

本节提供有关 ROSA 经典版所需的账户政策的详细信息。ROSA classic 需要这些权限才能管理 AWS 集群运行的资源，支持红帽站点可靠性工程师对集群的支持。您可以为策略名称分配自定义前缀，但应按照此页面上的定义命名这些策略（例如， `ManagedOpenShift-Installer-Role-Policy`）。

账户政策特定于 OpenShift 次要版本并且向后兼容。在创建或升级集群之前，应通过运行来验证策略版本和集群版本是否相同 `rosa list account-roles`。如果策略版本低于集群版本，请运行 `rosa upgrade account-roles` 升级角色和附加的策略。您可以对相同次要版本的多个集群使用相同的账户策略和角色。

[前缀]-Installer-Role-Policy

您可以将 [Prefix]-Installer-Role-Policy 附加到 IAM 实体。在创建 ROSA 经典集群之前，必须先将此策略附加到名为的 IAM 角色 [Prefix]-Installer-Role。此策略授予所需的权限，允许 ROSA 安装程序来管理 AWS 创建集群所需的资源。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:AssociateDhcpOptions",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CopyImage",
                "ec2:CreateDhcpOptions",
                "ec2:CreateInternetGateway",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteDhcpOptions",
                "ec2:DeleteInternetGateway",
                "ec2:DeleteNatGateway",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DeleteSecurityGroup",
```

```
                "ec2:DeleteSnapshot",
                "ec2:DeleteSubnet",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeleteVpc",
                "ec2:DeleteVpcEndpoints",
                "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:DetachInternetGateway",
                "ec2:DisassociateRouteTable",
                "ec2:GetConsoleOutput",
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
```

```
                "ec2:ModifyVpcAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRouteTableAssociation",
                "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:DescribeAccountLimits",
                "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: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:DeleteObjectVersion",
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketAcl",
                "s3:GetBucketCORS",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetReplicationConfiguration",
                "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:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListAWSDefaultServiceQuotas",
                "sts:AssumeRole",
                "sts:AssumeRoleWithWebIdentity",
                "sts:GetCallerIdentity",
                "tag:GetResources",
                "tag:UntagResources",
                "ec2:CreateVpcEndpointServiceConfiguration",
                "ec2:DeleteVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:ModifyVpcEndpointServicePermissions",
                "kms:DescribeKey",
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
```

```
}
```

[前缀]-ControlPlane-Role-Policy

您可以将 [Prefix]-ControlPlane-Role-Policy 附加到 IAM 实体。在创建 ROSA 经典集群之前，必须先将此策略附加到名为的 IAM 角色 [Prefix]-ControlPlane-Role。此政策向 ROSA classic 授予管理所需的权限 Amazon EC2 和 Elastic Load Balancing 托管的资源 ROSA 控制平面，以及读取 KMS keys。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteVolume",
                "ec2:Describe*",
                "ec2:DetachVolume",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyVolume",
                "ec2:RevokeSecurityGroupIngress",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerPolicy",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteLoadBalancerListeners",
                "elasticloadbalancing:DeleteTargetGroup",
```

```
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:Describe*",
                "elasticloadbalancing:DetachLoadBalancerFromSubnets",
                "elasticloadbalancing:ModifyListener",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[前缀]-Worker-Role-Policy

您可以将 `[Prefix]-Worker-Role-Policy` 附加到 IAM 实体。在创建 ROSA 经典集群之前，必须先将此策略附加到名为的 IAM 角色 `[Prefix]-Worker-Role`。此策略向 ROSA classic 授予描述作为工作节点运行的 EC2 实例所需的权限。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[前缀]-Support-Role-Policy

您可以将 [Prefix]-Support-Role-Policy 附加到 IAM 实体。在创建 ROSA 经典集群之前，必须先将此策略附加到名为的 IAM 角色 [Prefix]-Support-Role。该政策授予红帽站点可靠性工程所需的权限，以观察、诊断和支持 AWS ROSA 经典集群使用的资源，包括更改群集节点状态的能力。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:LookupEvents",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:CopySnapshot",
                "ec2:CreateNetworkInsightsPath",
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:DeleteTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAddressesAttribute",
                "ec2:DescribeAggregateIdFormat",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeCarrierGateways",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeCoipPools",
```

```
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeIdFormat",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLocalGatewayRouteTables",
                "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
                "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
                "ec2:DescribeLocalGateways",
                "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
                "ec2:DescribeLocalGatewayVirtualInterfaces",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInsightsAnalyses",
                "ec2:DescribeNetworkInsightsPaths",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePlacementGroups",
                "ec2:DescribePrefixLists",
                "ec2:DescribePrincipalIdFormat",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeRouteTables",
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshotAttribute",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeStaleSecurityGroups",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGatewayAttachments",
                "ec2:DescribeTransitGatewayConnectPeers",
                "ec2:DescribeTransitGatewayConnects",
                "ec2:DescribeTransitGatewayMulticastDomains",
                "ec2:DescribeTransitGatewayPeeringAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeVolumeAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetAssociatedIpv6PoolCidrs",
                "ec2:GetConsoleOutput",
                "ec2:GetManagedPrefixListEntries",
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:GetTransitGatewayAttachmentPropagations",
                "ec2:GetTransitGatewayMulticastDomainAssociations",
                "ec2:GetTransitGatewayPrefixListReferences",
                "ec2:GetTransitGatewayRouteTableAssociations",
                "ec2:GetTransitGatewayRouteTablePropagations",
                "ec2:ModifyInstanceAttribute",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:SearchLocalGatewayRoutes",
                "ec2:SearchTransitGatewayMulticastGroups",
                "ec2:SearchTransitGatewayRoutes",
                "ec2:StartInstances",
                "ec2:StartNetworkInsightsAnalysis",
```

```
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListenerCertificates",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeRules",
                "elasticloadbalancing:DescribeSSLPolicies",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GetRole",
                "iam:ListRoles",
                "kms:CreateGrant",
                "route53:GetHostedZone",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "s3:GetBucketTagging",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListAllMyBuckets",
                "sts:DecodeAuthorizationMessage",
                "tiros:CreateQuery",
                "tiros:GetQueryAnswer",
                "tiros:GetQueryExplanation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::managed-velero*",
```

```
                "arn:aws:s3:::*image-registry*"
            ]
        }
    ]
}
```

ROSA 经典运营商政策

本节详细介绍了ROSA classic所需的运营商政策。在创建 ROSA 经典集群之前，必须先将这些策略附加到相关的操作员角色。每个集群都需要一组独有的操作员角色。

需要这些权限才能允许 OpenShift 操作员来管理 ROSA 经典集群节点。您可以为策略名称分配自定义前缀以简化策略管理（例如，`ManagedOpenShift-openshift-ingress-operator-cloud-credentials`）。

[前缀]-openshift-ingress-operator-cloud凭证

您可以将 `[Prefix]-openshift-ingress-operator-cloud-credentials` 附加到 IAM 实体。此策略向 Ingress 运营商授予所需的权限，以配置和管理负载均衡器和 DNS 配置以进行外部集群访问。该政策还允许入口操作员读取和过滤 Route 53 用于发现托管区域的资源标签值。有关操作员的更多信息，请参阅 OpenShift 入口操作员 在 OpenShift GitHub 文档。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "elasticloadbalancing:DescribeLoadBalancers",
                "route53:ListHostedZones",
                "route53:ListTagsForResources",
                "route53:ChangeResourceRecordSets",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[前缀]-openshift-cluster-csi-drivers-ebs-cloud凭证

您可以将 `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` 附加到 IAM 实体。此政策向... 授予所需的权限 Amazon EBS CSI 驱动程序操作员负责安装和维护 Amazon EBS ROSA 经典集群上的 CSI 驱动程序。有关操作员的更多信息，请参阅 aws-ebs-csi 驱动程序操作员 在 OpenShift GitHub 文档。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateSnapshot",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DetachVolume",
                "ec2:EnableFastSnapshotRestores",
                "ec2:ModifyVolume"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

[前缀]-openshift-machine-api-aws-cloud证书

您可以将 `[Prefix]-openshift-machine-api-aws-cloud-credentials` 附加到 IAM 实体。此策略向计算机配置操作员授予描述、运行和终止所需的权限 Amazon EC2 实例作为工作节点进行管

理。此策略还授予权限，允许使用以下方法对工作节点根卷进行磁盘加密 AWS KMS keys。有关操作员的更多信息，请参阅 机器配置操作员 在 OpenShift GitHub 文档。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:DescribeKey"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

[前缀]-openshift-cloud凭据-操作员云凭证

您可以将 `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` 附加到 IAM 实体。此政策向云凭据运营商授予检索所需的权限 IAM 用户 详细信息，包括访问密钥 ID、随附的内联政策文档、用户的创建日期、路径、用户 ID 和亚马逊资源名称 (ARN)。有关操作员的更多信息，请参阅 云凭证运营商 在 OpenShift GitHub 文档。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

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

```
    ]
}
```

[前缀]-openshift-镜像注册表安装程序云凭证

您可以将 `[Prefix]-openshift-image-registry-installer-cloud-credentials` 附加到 IAM 实体。该政策向映像注册管理运营商授予必要的权限，允许其为 ROSA classic 的集群内映像注册表和相关服务预置和管理资源，包括 Amazon S3。这是必需的，这样操作员才能安装和维护 ROSA 经典集群的内部注册表。有关该操作员的更多信息，请参阅 图像注册管理运营商 在 OpenShift GitHub 文档。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketTagging",
                "s3:GetBucketTagging",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucketMultipartUploads",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

[前缀]-openshift-cloud-network-cr-cr-cr配置控制器

您可以将 `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` 附加到 IAM 实体。此政策向云网络配置控制器操作员授予所需的权限，以配置和管理网络资源，供 ROSA 经典集群网络叠加层使用。操作员使用这些权限来管理私有 IP 地址 Amazon EC2 实例作为 ROSA 经典集群的一部分。有关该操作员的更多信息，请参阅 Cloud-network-config-controller 在 OpenShift GitHub 文档。

权限策略

本策略文档中定义的权限指定了允许或拒绝哪些操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignIpv6Addresses",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 的托管策略 ROSA

一个 AWS 托管策略是一个独立的策略，由创建和管理 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、群组和角色分配权限。

请记住 AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们适用于所有人 AWS 可供客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改中定义的权限 AWS 托管策略。如果 AWS 更新中定义的权限 AWS 托管策略，此更新会影响该策略所关联的所有主体身份（用户、组和角色）。 AWS 最有可能更新 AWS 新建时采用托管策略 AWS 服务 已启动或新的 API 操作可用于现有服务。有关更多信息，请参阅 AWS 托管策略 在 IAM 用户指南。

AWS 管理策略： ROSAManageSubscription

你可以附上 `ROSAManageSubscription` 对你的政策 IAM 实体。在启用之前 ROSA 在 AWS ROSA 控制台，您必须先将此策略附加到 IAM 角色。

该政策授予 AWS Marketplace 您需要的权限才能管理 ROSA 订阅。

权限详细信息

该策略包含以下权限。

- `aws-marketplace:Subscribe` -授予订阅权限 AWS Marketplace 产品用于 ROSA。
- `aws-marketplace:Unsubscribe` -允许负责人删除订阅 AWS Marketplace 产品。
- `aws-marketplace:ViewSubscriptions` -允许校长查看来自的订阅 AWS Marketplace。这是必需的，这样 IAM 校长可以查看可用的 AWS Marketplace 订阅。

要查看完整的 JSON 策略文档，请参阅 ROSAManageSubscription 在 AWS 托管策略参考指南。

具有 HCP 账户政策的 ROSA

本节提供有关使用托管控制平面 (HCP) 的 ROSA 所需的账户策略的详细信息。这些 AWS 托管策略添加了 ROSA 在 HCP IAM 角色中使用的权限。Red Hat 站点可靠性工程（SRE）技术支持、集群安装以及控制面板和计算功能需要这些权限。

> **Note**
>
> AWS 托管策略专供 ROSA 与托管控制平面 (HCP) 一起使用。ROSA 经典集群使用客户管理的 IAM 策略。有关 ROSA 经典策略的更多信息，请参阅 the section called “ROSA 经典账户政策” 和 the section called “ROSA 经典运营商政策”。

AWS 管理策略： ROSAWorkerInstancePolicy

你可以附上 `ROSAWorkerInstancePolicy` 给你的 IAM 实体。在创建集群之前，您必须拥有一个附加了此策略的 IAM 角色。ROSA 服务向其他人拨打电话 AWS 服务 以你的名义。他们这样做是为了管理您在每个集群上使用的资源。

权限详细信息

此策略包括以下权限，允许 ROSA 工作节点完成以下任务：

- `ec2` — 评估 AWS 区域 和 Amazon EC2 实例详细信息作为 ROSA 集群工作节点生命周期管理的一部分。
- `ecr` -评估并从中获取图像 ROSA-managed 集群安装和工作节点生命周期管理所必需的 ECR 存储库。

要查看完整的 JSON 策略文档，请参阅 ROSAWorkerInstancePolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSASRESupportPolicy

您可以将 `ROSASRESupportPolicy` 附加到 IAM 实体。

在使用托管控制平面集群创建 ROSA 之前，必须先将此策略附加到 IAM 角色。该政策向红帽站点可靠性工程师 (SRE) 授予直接观察、诊断和支持所需的权限 AWS 与之相关的资源 ROSA 集群，包括变更能力 ROSA 群集节点状态。

权限详细信息

此策略包含允许 Red Hat SRE 完成以下任务的以下权限：

- `cloudtrail` — 阅读 AWS CloudTrail 与集群相关的事件和线索。
- `cloudwatch` — 阅读 Amazon CloudWatch 与集群相关的指标。
- `ec2` — 阅读、描述和审查 Amazon EC2 与集群运行状况相关的组件，例如安全组、VPC 终端节点连接和卷状态。启动、停止、重启和终止 Amazon EC2 实例。
- `elasticloadbalancing` — 阅读、描述和审查 Elastic Load Balancing 与集群运行状况相关的参数。
- `iam` — 评估 IAM 与集群运行状况相关的角色。
- `route53` – 查看与集群运行状况相关的 DNS 设置。

- sts — DecodeAuthorizationMessage — 阅读 IAM 用于调试目的的消息。

要查看完整的 JSON 策略文档，请参阅 ROSASRESupportPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSAInstallerPolicy

你可以附上 ROSAInstallerPolicy 给你的 IAM 实体。

在使用托管控制平面集群创建 ROSA 之前，必须先将此策略附加到名为的 IAM 角色 [Prefix]-ROSA-Worker-Role。此策略允许实体将任何遵循 [Prefix]-ROSA-Worker-Role 模式的角色添加到实例配置文件。此策略向安装程序授予必要的管理权限 AWS 支持的资源 ROSA 群集安装。

权限详细信息

此策略包含允许安装程序完成以下任务的以下权限：

- ec2 — 跑 Amazon EC2 使用托管的 AMI 的实例 AWS 账户 由红帽拥有和管理。描述 Amazon EC2 与之相关的实例、卷和网络资源 Amazon EC2 节点。此权限是必需的，这样 Kubernetes 控制平面才能将实例加入集群，并且集群可以评估其在集群中的存在 Amazon VPC。查看 Amazon EC2 容量预留以支持 ROSA 中的新容量预留功能。使用标签密钥匹配标记和删除子网上的标签 "kubernetes.io/cluster/*"。这是确保仅在适用的子网中创建用于集群入口的负载均衡器以及管理 Kubernetes 集群标识标签所必需的。
- elasticloadbalancing – 向集群上的目标节点添加负载均衡器。从集群上的目标节点移除负载均衡器。此权限是必需的，这样 Kubernetes 控制平面才能动态配置 Kubernetes 服务请求的负载均衡器，并且 OpenShift 应用程序服务。
- kms — 阅读 AWS KMS 密钥、创建和管理拨款 Amazon EC2，并返回一个唯一的对称数据密钥以供在外部使用 AWS KMS。如果在创建集群时启用了 etcd 加密，则使用加密的 etcd 数据需要此项。
- iam – 验证 IAM 角色和策略。动态配置和管理 Amazon EC2 与集群相关的实例配置文件。使用 iam:TagInstanceProfile 权限向 IAM 实例配置文件添加标签。当由于缺少客户指定的集群 OIDC 提供商而导致群集安装失败时，提供安装程序错误消息。
- route53 — 管理 Route 53 创建集群所需的资源。
- servicequotas – 评估创建集群所需的服务限额。
- sts — 创建临时的 AWS STS 的证书 ROSA 组件。承担创建集群的凭证。
- secretsmanager – 读取密钥值以安全地允许客户托管的 OIDC 配置作为集群预置的一部分。

要查看完整的 JSON 策略文档，请参阅 ROSAInstallerPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSASharedVPCRoute53Policy

你可以附上 ROSASharedVPCRoute53Policy 给你的 IAM 实体。您必须将此策略附加到 IAM 角色以允许 ROSA 集群调用其他集群 AWS 服务 在共享 VPC 环境中。

此策略允许 ROSA 安装程序配置 Route 53 记录。此政策旨在用于共享 VPC，并提供针对共享 VPC 用例量身定制的 Route 53 权限子集。

权限详细信息

此策略包括以下权限，允许 ROSA 安装程序完成以下任务：

- route53 — 阅读 DNS 区域信息和现有 DNS 记录以了解当前 DNS 配置。创建、修改和删除 DNS 记录，但仅限于特定的 ROSA-related 域名模式包括 .hypershift.local，.openshiftapps.com， .devshift.org， .openshiftusgov.com，以及 .devshiftusgov.com。在 Route 53 资源上添加、修改或移除标签，以进行资源管理和组织。
- tag — 发现并列出 AWS 基于标签的资源，这对于识别由 ROSA 管理的资源很有用。

要查看有关该策略的更多详细信息，包括最新版本的 JSON 策略文档，请参阅 ROSASharedVPCRoute53Policy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSASharedVPCEndpointPolicy

你可以附上 ROSASharedVPCEndpointPolicy 给你的 IAM 实体。您必须将此策略附加到 IAM 角色以允许 ROSA 集群调用其他集群 AWS 服务 在共享 VPC 环境中。

此策略允许 ROSA 安装程序在共享 VPC 环境中配置 VPC 终端节点和安全组。

权限详细信息

此策略包括以下权限，允许 ROSA 安装程序完成以下任务：

- ec2 — Read-only 描述权限 VPC-related 资源包括 VPC 终端节点、VPC 和安全组，用于了解网络环境。创建、删除和修改具有基于标签的限制的安全组，使得 ROSA 能够为集群网络创建和管理安全组，同时将操作限制为仅限 ROSA-tagged 资源。创建、修改和删除具有基于标签的限制的 VPC 终端节点，允许 ROSA 创建和管理用于私有连接的 VPC 终端节点 AWS 服务 在共享 VPC 环境中。在创建过程中对新创建的 VPC 终端节点和安全组应用标签，以便正确识别和管理资源。

要查看有关该策略的更多详细信息，包括最新版本的 JSON 策略文档，请参阅 ROSASharedVPCEndpointPolicy 在 AWS 托管策略参考指南。

ROSA 采用 HCP 运营商政策

本节提供有关使用托管控制平面 (HCP) 的 ROSA 所需的运营商策略的详细信息。你可以附上这些 AWS 托管策略适用于在 HCP 中使用 ROSA 所需的操作员角色。需要这些权限才能允许 OpenShift 操作员使用 HCP 集群节点管理 ROSA。

> **Note**
>
> AWS 托管策略专供 ROSA 与托管控制平面 (HCP) 一起使用。ROSA 经典集群使用客户管理的 IAM 策略。有关 ROSA 经典策略的更多信息，请参阅 the section called “ROSA 经典账户政策” 和 the section called “ROSA 经典运营商政策”。

AWS 管理策略： ROSAAmazonEBSCSIDriverOperatorPolicy

你可以附上 `ROSAAmazonEBSCSIDriverOperatorPolicy` 给你的 IAM 实体。您必须将此策略附加到操作员 IAM 角色，以允许具有托管控制平面集群的 ROSA 向其他人拨打电话 AWS 服务。每个集群都需要一组独有的操作员角色。

此政策向以下用户授予必要的权限 Amazon EBS CSI 驱动程序操作员负责安装和维护 Amazon EBS CSI 驱动程序上的 ROSA 集群。有关该操作员的更多信息，请参阅 aws-ebs-csi-driver 操作员 在 OpenShift GitHub 文档。

权限详细信息

此策略包括以下权限，这些权限允许 Amazon EBS 驾驶员需要完成以下任务：

- `ec2` — 创建、修改、附加、分离和删除 Amazon EBS 音量开启 Amazon EC2 实例。创建、删除和复制 Amazon EBS 卷快照。锁定快照以查看不变性和合规性用例。启用快速快照还原，以便更快地从快照创建卷。在上添加和移除标签 ROSA-由客户管理并由客户指定 Amazon EBS 卷、快照和实例。描述 Amazon EC2 实例、卷、快照、实例类型和可用区。
- `kms` — 阅读 AWS KMS 加密密钥 Amazon EBS 卷。解密并重新加密 Amazon EBS 使用客户管理的海量数据 AWS KMS 钥匙。为新的加密卷生成数据加密密钥。创建委托补助金 AWS KMS 操作到 Amazon EC2 用于卷和快照生命周期管理。这些权限仅适用于 AWS KMS 您为其指定的密钥 ROSA 使用。

要查看完整的 JSON 策略文档，请参阅 ROSAAmazonEBSCSIDriverOperatorPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSAIngressOperatorPolicy

你可以附上 ROSAIngressOperatorPolicy 给你的 IAM 实体。您必须将此策略附加到操作员 IAM 角色，以允许具有托管控制平面集群的 ROSA 向其他人拨打电话 AWS 服务。每个集群都需要一组独有的操作员角色。

此策略向入口运营商授予所需的权限，以预置和管理负载均衡器和 DNS 配置 ROSA 集群。该策略允许对标签值进行读取访问。然后，运算符筛选标签值 Route 53 用于发现托管区域的资源。有关该操作员的更多信息，请参阅 OpenShift 入口操作员 在 OpenShift GitHub 文档。

权限详细信息

此策略包含允许 Ingress Operator 完成以下任务的以下权限：

- elasticloadbalancing – 描述预置的负载均衡器的状态。
- route53 — 清单 Route 53 托管区域和编辑记录，用于管理由 ROSA 集群控制的 DNS。
- tag – 使用 tag:GetResources 权限管理带标签的资源。

要查看完整的 JSON 策略文档，请参阅 ROSAIngressOperatorPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSAImageRegistryOperatorPolicy

你可以附上 ROSAImageRegistryOperatorPolicy 给你的 IAM 实体。您必须将此策略附加到操作员 IAM 角色，以允许具有托管控制平面集群的 ROSA 向其他人拨打电话 AWS 服务。每个集群都需要一组独有的操作员角色。

此政策向映像注册管理运营商授予所需的权限，允许他们为... 预置和管理资源 ROSA 集群内映像注册表和依赖服务，包括 S3。这是操作员安装和维护内部注册表所必需的 ROSA 集群。有关该操作员的更多信息，请参阅 图像注册管理运营商 在 OpenShift GitHub 文档。

权限详细信息

此策略包含允许 Image Registry Operator 完成以下操作的以下权限：

- s3 — 管理和评估 Amazon S3 存储桶作为容器映像内容和集群元数据的永久存储。

要查看完整的 JSON 策略文档，请参阅 ROSAImageRegistryOperatorPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSACloudNetworkConfigOperatorPolicy

你可以附上 `ROSACloudNetworkConfigOperatorPolicy` 给你的 IAM 实体。您必须将此策略附加到操作员 IAM 角色，以允许具有托管控制平面集群的 ROSA 向其他人拨打电话 AWS 服务。每个集群都需要一组独有的操作员角色。

此政策向云网络配置控制器操作员授予所需的权限，以配置和管理网络资源 ROSA 集群网络叠加层。操作员使用这些权限来管理私有 IP 地址 Amazon EC2 实例作为其中的一部分 ROSA 集群。有关该操作员的更多信息，请参阅 Cloud-network-config-controller 在 OpenShift GitHub 文档。

权限详细信息

此策略包含允许 Cloud Network Config Controller Operator 完成以下任务的以下权限：

- `ec2` — 读取、分配和描述连接配置 Amazon EC2 实例， Amazon VPC 中的子网和弹性网络接口 ROSA 集群。

要查看完整的 JSON 策略文档，请参阅 ROSACloudNetworkConfigOperatorPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSAKubeControllerPolicy

你可以附上 `ROSAKubeControllerPolicy` 给你的 IAM 实体。您必须将此策略附加到操作员 IAM 角色，以允许具有托管控制平面集群的 ROSA 向其他人拨打电话 AWS 服务。每个集群都需要一组独有的操作员角色。

此策略向 kube 控制器授予管理所需的权限 Amazon EC2， Elastic Load Balancing，以及 AWS KMS 带有托管控制平面集群的 ROSA 的资源。有关此控制器的更多信息，请参见 控制器架构 在 OpenShift 文档。

权限详细信息

此策略包含允许 kube 控制器完成以下任务的以下权限：

- `ec2` — 创建、删除和添加标签到 Amazon EC2 实例安全组。将入站规则添加到安全组。描述可用区、 Amazon EC2 实例、路由表、安全组、VPC 和子网。
- `elasticloadbalancing` — 创建和管理负载均衡器及其策略。创建和管理负载均衡器监听器。向目标组注册和取消注册目标并管理目标组。注册和注销 Amazon EC2 带有负载均衡器的实例，并为负载均衡器添加标签。

- kms — 检索有关某项的详细信息 AWS KMS 钥匙。如果在创建集群时启用了 etcd 加密，则使用加密的 etcd 数据需要此项。

要查看完整的 JSON 策略文档，请参阅 ROSAKubeControllerPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSANodePoolManagementPolicy

你可以附上 ROSANodePoolManagementPolicy 给你的 IAM 实体。您必须将此策略附加到操作员 IAM 角色，以允许具有托管控制平面集群的 ROSA 向其他人拨打电话 AWS 服务。每个集群都需要一组独有的操作员角色。

此政策向以下用户授予所需的权限 NodePool 用于描述、运行和终止的控制器 Amazon EC2 实例作为工作节点进行管理。此策略还授予权限，允许使用以下方法对工作节点根卷进行磁盘加密 AWS KMS 密钥，标记连接到工作节点的弹性网络接口，以及访问 Amazon EC2 容量预留。有关此控制器的更多信息，请参见 控制器架构 在 OpenShift 文档。

权限详细信息

此策略包括以下权限，这些权限允许 NodePool 控制器完成以下任务：

- ec2 — 跑 Amazon EC2 使用托管的 AMI 的实例 AWS 账户 由红帽拥有和管理。在中管理 EC2 生命周期 ROSA 集群。使用动态创建和集成工作节点 Elastic Load Balancing， Amazon VPC， Route 53， Amazon EBS，以及 Amazon EC2。访问和描述容量预留以支持 ROSA 中的容量预留功能。描述 Amazon EC2 支持与工作负载相适应的节点大小决策的实例类型。从工作实例中移除标签， Amazon EBS 容量和承载的弹性网络接口 red-hat-managed: "true" 标签。 Tag-removal 来自的请求 NodePool 控制器需要至少一个标签密钥并排除 red-hat-managed 钥匙。修改带有 Worker 实例的实例元数据选项 red-hat-managed: "true" 标签。
- iam — 使用 Elastic Load Balancing 通过名为的服务相关角色 AWSServiceRoleForElasticLoadBalancing。将角色分配给 Amazon EC2 实例配置文件。
- kms — 阅读一篇文章 AWS KMS 密钥、创建和管理拨款 Amazon EC2，并返回一个唯一的对称数据密钥以供在外部使用 AWS KMS。允许对 Worker 节点根卷进行磁盘加密需要此项。
- sqs — 从客户管理的 Amazon SQS 队列中接收和删除带有以下内容的消息 red-hat: "true" 资源标签。这个 NodePool 控制器使用这些权限来使用竞价实例中断通知，并在回收之前优雅地耗尽工作节点。

要查看完整的 JSON 策略文档，请参阅 ROSANodePoolManagementPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSAKMSProviderPolicy

你可以附上 `ROSAKMSProviderPolicy` 给你的 IAM 实体。您必须将此策略附加到操作员 IAM 角色，以允许具有托管控制平面集群的 ROSA 向其他人拨打电话 AWS 服务。每个集群都需要一组独有的操作员角色。

此策略向内置版本授予所需的权限 AWS 要管理的加密提供商 AWS KMS 支持的密钥 `etcd` 数据加密。此政策允许 Amazon EC2 要使用 KMS 密钥 AWS 加密提供商提供加密和解密功能 `etcd` 数据。有关该提供商的更多信息，请参阅 AWS 加密提供商 在 Kubernetes 中 GitHub 文档。

权限详细信息

此策略包括以下权限，这些权限允许 AWS 加密提供商完成以下任务：

- `kms` — 加密、解密和检索 AWS KMS 钥匙。如果在创建集群时启用了 `etcd` 加密，则使用加密的 `etcd` 数据需要此项。

要查看完整的 JSON 策略文档，请参阅 ROSAKMSProviderPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSAControlPlaneOperatorPolicy

你可以附上 `ROSAControlPlaneOperatorPolicy` 给你的 IAM 实体。您必须将此策略附加到操作员 IAM 角色，以允许具有托管控制平面集群的 ROSA 向其他人拨打电话 AWS 服务。每个集群都需要一组独有的操作员角色。

此政策向控制平面操作员授予管理所需的权限 Amazon EC2 和 Route 53 带有托管控制平面集群的 ROSA 资源。有关此运算符的更多信息，请参阅 控制器架构 在 OpenShift 文档。

权限详细信息

此策略包含允许 Control Plane Operator 完成以下任务的以下权限：

- `ec2` — 创建和管理 Amazon VPC 端点。
- `route53` — 列出并更改 Route 53 记录集并列出托管区域。创建、检查、标记和删除托管集群 DNS 的托管区域。记录更改仅限于红色 Hat-managed 域名。托管区域权限适用于整个账户中的托管区域。
- 在 Red 上添加和移除标签 Hat-managed 安全组：控制平面操作员可以标记和取消标记 Red Hat-managed 用于适当管理和清理资源生命周期的安全组。该政策禁止运营商删除 `red-hat-managed` 标签，它将这些资源标识为红色 Hat-managed。

- 管理引用安全组的 VPC 终端节点：控制平面运营商可以修改引用安全组的 VPC 终端节点。集群升级期间的 VPC 终端节点协调需要此权限。

要查看完整的 JSON 策略文档，请参阅 ROSAControlPlaneOperatorPolicy 在 AWS 托管策略参考指南。

AWS 管理策略： ROSAKarpenterControllerPolicy

你可以附上 `ROSAKarpenterControllerPolicy` 给你的 IAM 实体。将此策略附加到操作员 IAM 角色，这样具有托管控制平面集群的 ROSA 就可以向其他人拨打电话 AWS 服务。每个集群都需要一组独特的操作员角色。

ROSA Karpenter 控制器使用此策略根据实时集群工作负载需求动态配置、扩展和管理 EC2 工作节点。该策略授予 EC2 实例生命周期管理（启动、标记和终止实例）、队列创建和启动模板管理的权限。该政策还涵盖通过定价 API 选择成本感知型实例、使用客户管理的 KMS 密钥进行 EBS 批量加密，以及节点角色的 IAM 实例配置文件管理。严格的服务边界，通过以下方式强制执行 `red-hat-managed: "true"` 资源和请求标签，限定所有可变操作的范围，因此控制器只能创建、修改或终止属于的资源 ROSA-managed 基础设施。

该政策限制 EC2 映像仅限经批准的红帽和 AWS AMI 发布商账户，将 IAM 实例配置文件限制为 ROSA-specific 命名模式 (`rosa-service-managed-`)，并允许控制器仅传递 ROSA 工作节点角色 ( ) 到 EC2 服务。该政策是对现有政策的补充 ROSANodePoolManagementPolicy 通过添加动态，Karpenter-driven 自动缩放功能，同时保持ROSA的既定安全模型和最低权限原则。

权限详细信息

此策略包括以下权限，允许 ROSA Karpenter 控制器完成以下任务：

- `ec2` — 描述和发现可用区、实例类型、映像、启动模板、安全组、子网、VPC、快照、现货价格历史记录和容量预留。创建和管理 EC2 队列、实例、卷、启动模板和竞价型实例请求。标记和终止带有标签的资源 `red-hat-managed: true`。
- `pricing` — 查询 EC2 实例定价信息，以选择成本优化的节点。
- `kms` — 使用标有客户管理的 KMS 密钥描述、解密、重新加密和生成数据密钥 `red-hat: true` 用于 EBS 卷加密。创建范围有限的 KMS 授权，将这些操作委托给 EC2 服务。
- `iam` — 将 ROSA 工作节点角色传递给 EC2 服务以启动实例。创建、读取、标记和管理与之匹配的实例配置文件 ROSA-specific 命名模式 (`rosa-service-managed-*`)。

要查看完整的 JSON 策略文档，请参阅 ROSAKarpenterControllerPolicy 在 AWS 托管策略参考指南。

ROSA 更新到 AWS 托管策略

查看有关更新的详细信息 AWS 的托管策略 ROSA 自从该服务开始跟踪这些更改以来。要获得有关此页面更改的自动提示，请订阅 文档历史记录 页面上的 RSS 源。

更改	描述	日期
ROSAControlPlaneOperatorPolicy — 政策已更新	通过此政策更新，您可以使用控制平面操作员创建、检查、标记和删除 Route 53 托管区域。操作员可以在附加红色下管理记录 Hat-managed 托管集群 DNS 的域名。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAControlPlaneOperatorPolicy”。	2026 年 11 月 12 日
ROSANodePoolManagementPolicy — 政策已更新	通过此策略更新，您可以从工作实例中移除过时的标签，Amazon EBS 容量和弹性网络接口，使用 NodePool 控制器。您还可以使用控制器修改现有工作实例上的实例元数据选项。您只能对带有以下内容的资源使用这两个权限 `red-hat-managed: "true"` 标签。要了解更多信息，请参阅the section called “AWS 管理策略： ROSANodePoolManagementPolicy”。	2026年11月5日
ROSAAmazonEBSCSIDriverOperatorPolicy — 政策已更新	我们更新了 ROSAAmazonEBSCSIDriverOperatorPolicy 扩展 Amazon EBS 1.61 版本功能集的 CSI 驱动程序。在这	2026 年 8 月 18 日

更改	描述	日期
	次更新中，Amazon EBS CSI 驱动程序操作员可以复制和锁定 Amazon EBS 快照并启用快速快照恢复。它也可以使用客户管理的 AWS KMS 加密卷操作的密钥。要了解更多信息，请参阅the section called “AWS 管理策略：ROSAAmazonEBSCSIDriverOperatorPolicy”。	
ROSANodePoolManagementPolicy — 政策已更新	AWS 已更新 ROSANodePoolManagementPolicy 所以 NodePool 控制器可以描述 EC2 实例类型并处理来自客户标记的 Amazon SQS 队列的现货实例中断消息。这些 SQS 操作仅适用于携带的队列 `red-hat: "true"` 资源标签。要了解更多信息，请参阅the section called “AWS 管理策略：ROSANodePoolManagementPolicy”。	2026 年 7 月 28 日

更改	描述	日期
ROSAControlPlaneOperatorPolicy — 政策已更新	AWS 已更新 ROSAControlPlaneOperatorPolicy。通过此更新，控制平面操作员可以在 Red 上添加和移除标签 Hat-managed 安全组（`ec2:DeleteTags` ）。保护措施可防止操作员移除 `red-hat-managed` 标记本身。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAControlPlaneOperatorPolicy”。	2026 年 7 月 28 日
ROSAKarpenterControllerPolicy — 添加了新政策	AWS 发布了一项新政策，允许 Karpenter 控制器使用托管控制平面集群为 ROSA 动态配置、扩展和管理 EC2 工作节点。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAKarpenterControllerPolicy”。	2026年7月22日
ROSAControlPlaneOperatorPolicy — 政策已更新	ROSA 更新了政策，允许标记红色 Hat-managed 安全组用于适当的资源生命周期管理并将安全组/* 添加到 ManageVPCEndpointWithCondition 修复集群升级期间的 VPCE 协调失败问题。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAControlPlaneOperatorPolicy”。	2026 年 4 月 9 日

更改	描述	日期
ROSAKubeControllerPolicy — 政策已更新	ROSA 更新了政策，明确了向目标组注册和注销目标的弹性负载平衡权限。要了解更多信息，请参阅the section called “AWS 管理策略：ROSAKubeControllerPolicy”。	2026 年 3 月 5 日
ROSANodePoolManagementPolicy — 政策已更新	ROSA 更新了政策，增加了对亚马逊 EC2 容量预留的资源访问权限。此更改允许 NodePool 控制器访问和描述容量预留以改善资源管理。要了解更多信息，请参阅the section called “AWS 管理策略：ROSANodePoolManagementPolicy”。	2025 年 9 月 3 日
ROSASharedVPCEndpointPolicy — 添加了新政策	ROSA 添加了一项新政策，允许 ROSA 安装程序用于在共享 VPC 环境中配置 VPC 终端节点和安全组。该策略提供了一部分专为共享 VPC 用例量身定制的 EC2 权限。要了解更多信息，请参阅the section called “AWS 管理策略：ROSASharedVPCEndpointPolicy”。	2025 年 8 月 7 日

更改	描述	日期
ROSASharedVPCRoute53Policy — 添加了新政策	ROSA 添加了一项新政策，允许 ROSA 安装程序用于在共享 VPC 环境中配置 Route 53 记录。该策略提供了一部分专为共享 VPC 用例量身定制的 Route 53 权限。要了解更多信息，请参阅the section called “AWS 管理策略： ROSASharedVPCRoute53Policy”。	2025 年 8 月 7 日
ROSAInstallerPolicy — 政策已更新	ROSA 更新了政策，允许 ROSA 安装程序检查亚马逊 EC2 容量预留以支持 ROSA 中的新容量预留功能。此更新还允许安装程序使用标签密钥匹配来删除子网上的标签 `"kubernetes.io/cluster/*"` 用于改进 Kubernetes 集群标签管理。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAInstallerPolicy”。	2025 年 8 月 7 日
ROSAImageRegistryOperatorPolicy — 政策已更新	ROSA 更新了策略，将权限范围缩小到 S3 存储桶资源级别。此更改满足了两者的 ROSA 存储要求 AWS 商业和 GovCloud 地区。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAImageRegistryOperatorPolicy”。	2025 年 5 月 19 日

更改	描述	日期
ROSANodePoolManagementPolicy — 政策已更新	ROSA 更新了政策，允许标记连接到工作节点的弹性网络接口。要了解更多信息，请参阅the section called “AWS 管理策略： ROSANodePoolManagementPolicy”。	2025 年 5 月 5 日
ROSAImageRegistryOperatorPolicy — 政策已更新	ROSA 更新了允许使用红帽的政策 OpenShift 映像注册运营商，用于在中预置和管理 Amazon S3 存储桶和对象 AWS GovCloud ROSA 集群内映像注册表使用的区域。此更改满足了 ROSA 的存储要求 AWS GovCloud 地区。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAImageRegistryOperatorPolicy”。	2025 年 4 月 16 日
ROSAWorkerInstancePolicy — 政策已更新	ROSA 更新了政策，允许工作节点评估并从中获取图像 ROSA-managed 集群安装和工作节点生命周期管理所必需的 ECR 存储库。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAWorkerInstancePolicy”。	2025 年 3 月 3 日

更改	描述	日期
ROSANodePoolManagementPolicy — 政策已更新	ROSA 更新了政策，仅允许在 ec2 期间对弹性网络接口进行与 EC2 实例类似的标记：RunInstances 当请求包含标签时调用 `red-hat-managed: true`。这些权限是在 HCP 4.17 集群中支持 ROSA 所必需的。要了解更多信息，请参阅the section called “AWS 管理策略： ROSANodePoolManagementPolicy”。	2025 年 2 月 24 日
ROSAAmazonEBSCSIDriverOperatorPolicy — 政策已更新	ROSA 更新了政策以支持新政策 Amazon EBS 快照授权 API。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAAmazonEBSCSIDriverOperatorPolicy”。	2025 年 1 月 17 日
ROSANodePoolManagementPolicy — 政策已更新	ROSA 更新了政策，允许 ROSA 节点池管理器来描述 DHCP 选项集，以便设置正确的私有 DNS 名称。要了解更多信息，请参阅the section called “AWS 管理策略： ROSANodePoolManagementPolicy”。	2024 年 5 月 2 日

更改	描述	日期
ROSAInstallerPolicy — 政策已更新	ROSA 更新了政策，允许 ROSA 安装程序使用标签密钥匹配向子网添加标签 `"kubernetes.io/cluster/*"` 。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAInstallerPolicy”。	2024 年 4 月 24 日
ROSASRESupportPolicy — 政策已更新	ROSA 更新了策略，允许 SRE 角色检索已标记的实例配置文件信息 ROSA 如同 `red-hat-managed` 。要了解更多信息，请参阅the section called “AWS 管理策略： ROSASRESupportPolicy”。	2024 年 4 月 10 日
ROSAInstallerPolicy — 政策已更新	ROSA 更新了政策，允许 ROSA 安装程序来验证这一点 AWS 的托管策略 ROSA 已连接到 IAM 使用的角色 ROSA。此更新还允许安装程序识别是否已将客户管理策略附加到 ROSA 角色。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAInstallerPolicy”。	2024 年 4 月 10 日

更改	描述	日期
ROSAInstallerPolicy — 政策已更新	ROSA 更新了策略，允许该服务在由于缺少客户指定的集群 OIDC 提供商而导致群集安装失败时提供安装程序警报消息。此更新还允许该服务检索现有的 DNS 域名服务器，从而使集群配置操作具有等效性。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAInstallerPolicy”。	2024 年 1 月 26 日
ROSASRESupportPolicy — 政策已更新	ROSA 更新了策略，允许该服务使用对安全组执行读取操作 DescribeSecurityGroups API。要了解更多信息，请参阅the section called “AWS 管理策略： ROSASRESupportPolicy”。	2024 年 1 月 22 日
ROSAImageRegistryOperatorPolicy — 政策已更新	ROSA 更新了政策，允许映像注册运营商对之采取行动 Amazon S3 名称包含 14 个字符的区域中的存储桶。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAImageRegistryOperatorPolicy”。	2023 年 12 月 12 日

更改	描述	日期
ROSAKubeControllerPolicy — 政策已更新	ROSA 更新了策略，允许 kube-controller-manager 描述可用区， Amazon EC2 实例、路由表、安全组、VPC 和子网。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAKubeControllerPolicy”。	2023 年 10 月 16 日
ROSAManageSubscription — 政策已更新	ROSA 更新了政策，添加了带有托管控制平面的 ROSA ProductId。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAManageSubscription”。	2023 年 8 月 1 日
ROSAKubeControllerPolicy — 政策已更新	ROSA 更新了策略，允许 kube-controller-manager 将网络负载均衡器创建为 Kubernetes 服务负载均衡器。网络负载均衡器提供了更强的能力来处理不稳定的工作负载并支持负载均衡器的静态 IP 地址。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAKubeControllerPolicy”。	2023 年 7 月 13 日

更改	描述	日期
ROSANodePoolManagementPolicy — 添加了新政策	ROSA 添加了新策略以允许 NodePool 用于描述、运行和终止的控制器 Amazon EC2 实例作为工作节点进行管理。此策略还允许使用以下方法对工作节点根卷进行磁盘加密 AWS KMS 钥匙。要了解更多信息，请参阅the section called “AWS 管理策略： ROSANodePoolManagementPolicy”。	2023 年 6 月 8 日
ROSAInstallerPolicy — 添加了新政策	ROSA 添加了允许安装程序管理的新策略 AWS 支持群集安装的资源。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAInstallerPolicy”。	2023 年 6 月 6 日
ROSASRESupportPolicy — 添加了新政策	ROSA 添加了一项新政策，允许红帽 SRE 直接观察、诊断和支持 AWS 与之相关的资源 ROSA 集群，包括变更能力 ROSA 群集节点状态。要了解更多信息，请参阅the section called “AWS 管理策略： ROSASRESupportPolicy”。	2023 年 6 月 1 日

更改	描述	日期
ROSAKMSProviderPolicy — 添加了新政策	ROSA 添加了一个新策略以允许内置 AWS 要管理的加密提供商 AWS KMS 支持 etcd 数据加密的密钥。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAKMSProviderPolicy”。	2023 年 4 月 27 日
ROSAKubeControllerPolicy — 添加了新政策	ROSA 添加了允许 kube 控制器管理的新策略 Amazon EC2， Elastic Load Balancing ，以及 AWS KMS 的资源 ROSA 使用托管的控制平面集群。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAKubeControllerPolicy”。	2023 年 4 月 27 日
ROSAImageRegistryOperatorPolicy — 添加了新政策	ROSA 添加了一项新政策，允许映像注册管理运营商为预置和管理资源 ROSA 集群内映像注册表和依赖服务，包括 S3。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAImageRegistryOperatorPolicy”。	2023 年 4 月 27 日

更改	描述	日期
ROSAControlPlaneOperatorPolicy — 添加了新政策	ROSA 添加了一项新策略以允许控制平面操作员进行管理 Amazon EC2 和 Route 53 的资源 ROSA 使用托管的控制平面集群。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAControlPlaneOperatorPolicy”。	2023 年 4 月 24 日
ROSACloudNetworkConfigOperatorPolicy — 添加了新政策	ROSA 添加了一项新政策，允许云网络配置控制器操作员为云网络配置和管理网络资源 ROSA 集群网络叠加层。要了解更多信息，请参阅the section called “AWS 管理策略： ROSACloudNetworkConfigOperatorPolicy”。	2023 年 4 月 20 日
ROSAIngressOperatorPolicy — 添加了新政策	ROSA 添加了一项新政策，允许入口运营商预置和管理负载均衡器和 DNS 配置 ROSA 集群。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAIngressOperatorPolicy”。	2023 年 4 月 20 日
ROSAAmazonEBSCSIDriverOperatorPolicy — 添加了新政策	ROSA 添加了新策略以允许 Amazon EBS CSI 驱动程序操作员负责安装和维护 Amazon EBS CSI 驱动程序上的 ROSA 集群。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAAmazonEBSCSIDriverOperatorPolicy”。	2023 年 4 月 20 日

更改	描述	日期
ROSAWorkerInstancePolicy — 添加了新政策	ROSA 添加了允许该服务管理群集资源的新策略。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAWorkerInstancePolicy”。	2023 年 4 月 20 日
ROSAManageSubscription — 添加了新政策	ROSA 添加了一项新政策来授予 AWS Marketplace 管理所需的权限 ROSA 订阅。要了解更多信息，请参阅the section called “AWS 管理策略： ROSAManageSubscription”。	2022 年 4 月 11 日
AWS 云端 Red Hat OpenShift 服务 已开始跟踪更改	AWS 云端 Red Hat OpenShift 服务 开始跟踪其更改 AWS 托管策略。	2022 年 3 月 2 日

故障排除 ROSA 身份和访问权限

使用以下信息来帮助您诊断和修复在使用时可能遇到的常见问题 ROSA 和 IAM。

AWS Organizations 服务控制策略要求拒绝 AWS Marketplace 权限

如果你的 AWS Organizations 服务控制策略 (SCP) 不允许所需的 AWS Marketplace 尝试启用时的订阅权限 ROSA，则出现以下控制台错误。

```
An error occurred while enabling ROSA, because a service control policy (SCP) is
 denying required permissions. Contact your management account administrator, and
 consult the documentation for troubleshooting.
```

如果您收到此错误，则必须联系管理员寻求帮助。您的管理员是管理组织帐户的人。要求该人执行以下操作：

1. 将 SCP 配置为允许 `aws-marketplace:Subscribe`， `aws-marketplace:Unsubscribe`，以及 `aws-marketplace:ViewSubscriptions` 权限。有关更多信息，请参阅 更新 SCP 在 AWS Organizations 用户指南。
2. 启用 ROSA 在组织的管理账户中。
3. 分享 ROSA 订阅组织内需要访问权限的成员账户。有关更多信息，请参阅 在组织中共享订阅 在 AWS Marketplace 买家指南。

用户或角色没有必填项 AWS Marketplace 权限

如果你的 IAM 校长没有必填项 AWS Marketplace 尝试启用时的订阅权限 ROSA，则出现以下控制台错误。

```
An error occurred while enabling ROSA, because your user or role does not have the
 required permissions.
```

要解决该问题，请完成以下步骤：

1. 前往 IAM 控制台 并附上 AWS 托管策略 `ROSAManageSubscription` 转到您的 IAM 身份。有关更多信息，请参阅 ROSAManageSubscription 在 AWS 托管策略参考指南。
2. 按照the section called “启用 ROSA 和配置 AWS 先决条件”中的程序操作。

如果您没有权限查看或更新您在中设置的权限 IAM 或者您收到错误，则必须联系管理员寻求帮助。让那个人附上 `ROSAManageSubscription` 给你的 IAM 识别并按照中的程序进行操作 the section called “启用 ROSA 和配置 AWS 先决条件”。管理员执行此操作时，它会启用 ROSA 通过更新所有人的权限集 IAM 下的身份 AWS 账户。

必填 AWS Marketplace 权限被管理员封锁

如果您的账户管理员封锁了所需的 AWS Marketplace 订阅权限，尝试启用时会出现以下控制台错误 ROSA。

```
An error occurred while enabling ROSA because required permissions have been blocked by
 an administrator. ROSAManageSubscription includes the permissions required to enable
 ROSA. Consult the documentation and try again.
```

如果您收到此错误，则必须联系管理员寻求帮助。要求该人执行以下操作：

1. 前往 ROSA 控制台 并附上 AWS 托管策略 ROSAManageSubscription 转到您的 IAM 身份。有关更多信息，请参阅 ROSAManageSubscription 在 AWS 托管策略参考指南。
2. 按照中的步骤操作 the section called “启用 ROSA 和配置 AWS 先决条件” 启用 ROSA。此过程启用 ROSA 通过更新所有人的权限集 IAM 下的身份 AWS 账户。

创建负载均衡器时出错： AccessDenied

如果您尚未创建负载均衡器， AWSServiceRoleForElasticLoadBalacing 您的账户中可能不存在服务相关角色。如果您尝试创建，则会出现以下错误 ROSA 集群 没有 AWSServiceRoleForElasticLoadBalacing 在您的账户中扮演的角色。

```
Error creating network Load Balancer: AccessDenied
```

要解决该问题，请完成以下步骤：

1. 检查您的账户是否有 AWSServiceRoleForElasticLoadBalancing 角色。

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

2. 如果您没有此角色，请按照中的说明创建角色 创建服务相关角色 在 Elastic Load Balancing 用户指南。

弹性在 ROSA

AWS 全球基础设施弹性

这个 AWS 全球基础设施是围绕它建立的 AWS 区域 和可用区。 AWS 区域 提供多个物理上分隔和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

ROSA 为客户提供了在单个中运行 Kubernetes 控制平面和数据平面的选项 AWS 可用区，或跨多个可用区。而 Single-AZ 集群可用于实验，鼓励客户在多个可用区中运行其工作负载。这样可以确保应用程序甚至可以承受整个可用区故障（非常罕见的事件）。

有关以下内容的更多信息 AWS 区域 和可用区，请参阅 AWS 全球基础设施。

ROSA 集群弹性

这个 ROSA 控制平面至少由三个组成 OpenShift 控制平面节点。每个控制面板节点都由一个 API 服务器实例、一个 `etcd` 实例和控制器组成。如果控制面板节点出现故障，所有 API 请求都会自动路由到其他可用节点，以确保集群可用性。

这个 ROSA 数据平面由至少两个组成 OpenShift 基础架构节点和两个 OpenShift 工作节点。基础设施节点运行支持的 pod OpenShift 集群基础架构组件，例如默认路由器、内置 OpenShift 注册表，以及用于集群指标和监控的组件。 OpenShift 工作节点运行最终用户应用程序 pod。

Red Hat 站点可靠性工程师（SRE）全面管理控制面板和基础设施节点。红帽 SRes 主动监控 ROSA 集群，并负责更换所有出现故障的控制平面节点和基础架构节点。有关更多信息，请参阅 the section called “责任”。

> **Important**
>
> 因为 ROSA 是一项托管服务，红帽负责管理底层 AWS 基础架构 ROSA 使用。客户不应尝试手动关闭 Amazon EC2 这样的实例 ROSA 的用途 AWS 控制台或 AWS CLI。此操作可能会导致客户数据丢失。

如果 Worker 节点在数据面板上出现故障，则控制面板会将未调度的容器组（pod）重新定位到正常运行的 Worker 节点，直到故障节点恢复或替换。可以手动替换故障的 Worker 节点，也可以通过启用集群中计算机的自动扩展来自动替换。有关更多信息，请参阅 Red Hat 文档中的集群自动扩展。

Customer-deployed 应用程序弹性

虽然 ROSA 提供多种保护措施以确保服务的高可用性，客户有责任构建已部署的应用程序以实现高可用性，以保护工作负载免受停机影响。有关更多信息，请参阅 Red Hat 文档中的关于 ROSA的可用性。

中的基础设施安全 ROSA

作为一项托管服务， AWS 云端 Red Hat OpenShift 服务 受到 AWS 全球网络安全。如需了解以下信息 AWS 安全服务及其方法 AWS 保护基础架构，请参阅 AWS 云安全。设计你的 AWS 使用基础设施安全最佳实践的环境，请参阅 基础架构保护 在 安全支柱 — AWS Well-Architected 框架。

你用 AWS 已发布用于访问的 API 调用 ROSA 通过 AWS 网络。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，并建议使用 TLS 1.3。
- 具有完美向前保密 (PFS) 的密码套件，例如 DHE（临时保密） Diffie-Hellman) 或 ECDHE（椭圆曲线短暂的 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

集群网络隔离

Red Hat 站点可靠性工程师（SRE）负责集群和底层应用平台的持续管理和网络安全。有关红帽在以下方面的职责的更多信息 ROSA，参见 the section called “责任”。

当你创建新集群时， ROSA 提供了创建公共 Kubernetes API 服务器端点和应用程序路由或私有 Kubernetes API 端点和应用程序路由的选项。此连接用于与您的集群通信（使用 OpenShift 管理工具，例如 ROSA CLI 和 OpenShift CLI）。私有连接允许节点与 API 服务器之间的所有通信都留在 VPC 内。如果您启用对 API 服务器和应用程序路由的私有访问，则必须使用现有的 VPC 和 AWS PrivateLink 将 VPC 连接到 OpenShift 后端服务。

Kubernetes API 服务器访问权限使用以下组合来保护 AWS Identity and Access Management （IAM）和原生 Kubernetes 基于角色的访问控制 (RBAC)。有关 Kubernetes RBAC 的更多信息，请参阅 Kubernetes 文档中的使用 RBAC 鉴权。

ROSA 允许您使用多种类型的 TLS 终止来创建安全的应用程序路由，以便向客户端提供证书。有关更多信息，请参阅 Red Hat 文档中的安全路由。

如果你创建一个 ROSA 集群在现有 VPC 中，您可以为集群指定 VPC 子网和可用区。您还可以定义集群网络要使用的 CIDR 范围，并将这些 CIDR 范围与 VPC 子网进行匹配。有关更多信息，请参阅 Red Hat 文档中的 CIDR 范围定义。

对于使用公有 API 终端节点的集群， ROSA 要求您的 VPC 为要将集群部署到的每个可用区配置公有和私有子网。对于使用私有 API 端点的集群，只需要私有子网。

如果您使用现有 VPC，则可以配置 ROSA 集群在创建集群期间或之后使用 HTTP 或 HTTPS 代理服务器来加密集群 Web 流量，从而为您的数据增加另一层安全性。启用代理后，将拒绝核心集群组件直接访问互联网。代理不会拒绝用户工作负载访问互联网。有关更多信息，请参阅 Red Hat 文档中的配置集群范围代理。

容器组（pod）网络隔离

如果您是集群管理员，则可以在容器级别定义网络策略，限制流向您的 Pod 的流量 ROSA 集群。

存储在 ROSA

AWS 云端 Red Hat OpenShift 服务 集群将永久数据存储在 AWS 通过 Kubernetes 永久卷框架和容器存储接口 (CSI) 提供存储服务。本节介绍可用于您的工作负载的存储选项、何时使用每种存储选项以及它们在工作负载上的行为 ROSA。

以下存储后端可用：

- Amazon Elastic Block Store（Amazon EBS) — 用于单节点、一次读写工作负载的块存储。您的集群包括 Amazon EBS CSI 驱动程序和用途 Amazon EBS 默认存储。有关更多信息，请参阅 the section called “Amazon EBS”。
- Amazon Elastic File System（Amazon EFS) — 共享的弹性文件存储，用于跨多个 Pod 和可用区进行多次读写的工作负载。您可以安装和配置 Amazon EFS 使用前的 CSI 驱动程序。有关更多信息，请参阅 the section called “Amazon EFS”。
- 亚马逊 FSx for NetApp ONTAP（适用于 ONTAP 的 FSx） — 高性能、多协议共享文件和块存储，通过配置 NetApp 三叉戟 CSI 驱动程序。 NetApp 提供并支持三叉戟。你安装和配置它。有关更多信息，请参阅 the section called “FSx for ONTAP”。

在选择存储后端之前，请查看 the section called “存储的工作原理” 要明白怎么做 ROSA 提供存储空间以及如何提供 AWS STS 会影响每个存储驱动程序所需的权限。

主题

- 存储的工作原理 ROSA
- 块存储 Amazon Elastic Block Store
- 共享文件存储空间与 Amazon Elastic File System
- Multi-protocol 使用亚马逊 FSx 进行存储 NetApp ONTAP

存储的工作原理 ROSA

和 ROSA，您可以使用 Kubernetes 持久卷框架为应用程序提供比单个 Pod 寿命更长的持久存储空间。存储空间通过容器存储接口 (CSI) 消耗，该标准允许 ROSA 使用 AWS 存储服务，无需为平台中的每项服务提供支持。

永久容量、声明和存储类别

ROSA 应用程序使用三个 Kubernetes 存储对象：

PersistentVolume (PV)

集群中的一块存储器，由 AWS 存储资源，例如 Amazon EBS 音量或 Amazon EFS 文件系统。PV 的生命周期独立于使用它的任何 Pod。

PersistentVolumeClaim （聚氯乙烯）

工作负载提出的存储请求。PVC 指定工作负载所需的存储量和访问模式。 ROSA 将 PVC 绑定到满足请求的 PV。

StorageClass (SC)

描述存储类别的模板，包括哪个 CSI 驱动程序为其配置以及要使用的参数（例如 Amazon EBS 卷类型）。存储类别启用 动态配置。

您可以通过两种方式预置永久卷：

- 动态配置 — 当 PVC 引用存储类时， ROSA 按需自动配置匹配的 PV。这是最常见的方法。
- 静态配置 — 集群管理员提前创建 PV，并且 PVC 绑定到匹配的现有 PV。

只有当请求的容量和访问模式都匹配时，PVC 才会绑定到 PV。绑定 PV 一次只能为一个 PVC 提供服务。删除 PVC 时，该 PV 的回收策略决定了底层存储的变化。默认情况下， ROSA 删除动态配置的卷。

访问模式

卷的访问模式决定了有多少节点可以挂载该卷以及它们是否可以写入该卷。下表显示了访问模式以及每种访问模式支持的存储后端。

访问模式	说明	支持的后端
ReadWrite Once （两个）	该卷可以由单个节点以读写方式挂载。	Amazon EBS， Amazon EFS，亚马逊 FSx NetApp ONTAP
ReadWrite Many (RWX)	该卷可以由多个节点同时以读写方式挂载。	Amazon EFS，适用于 ONTAP 的 FSx

访问模式	说明	支持的后端
ReadOnlyMany（罗克斯）	许多节点可以将该卷安装为只读状态。	Amazon EFS

> **⚠ EBS 不支持 ReadWriteMany**
>
> Amazon EBS 无法共享卷以供多个节点同时写入。如果您的工作量需要 ReadWriteMany (RWX) 访问、使用 Amazon EFS 或者改为适用于 ONTAP 的 FSx。

默认情况下已安装存储驱动程序

ROSA 为你安装一些 CSI 驱动程序，并要求你启用其他 CSI 驱动程序。下表显示了默认情况下安装了哪些 CSI 驱动程序。

存储后端	默认情况下已安装	注意
Amazon EBS（EBS CSI 驱动程序）	是	您的集群包括 Amazon EBS CSI 驱动程序和操作员在 `openshift-cluster-csi-drivers` 命名空间和用途 Amazon EBS 默认情况下预置永久音量。
Amazon EFS（EFS CSI 驱动程序）	否	你安装 Amazon EFS CSI 驱动程序操作员并创建所需的 AWS 使用前的身份和访问管理 (IAM) 资源。
适用于 ONTAP 的 FSx (NetApp 三叉戟）	否	三叉戟是一个 NetApp-provided 您安装和操作的 CSI 驱动程序。它不是 AWS 或红帽插件。

您的集群是使用准备好的 Amazon EBS 存储类别和用途 Amazon EBS 默认情况下，节点根卷和永久卷均适用。在责任共担模式下，您可以安装和配置任何额外的存储。要使用 Amazon EFS 或者第三方 CSI 驱动程序，你可以安装该驱动程序并创建它 IAM 资源。

AWS STS 和存储驱动程序权限

ROSA 集群使用 AWS Security Token Service （ AWS STS ）。集群组件假设的不是长期的证书 IAM 角色通过 OpenID Connect (OIDC) 身份提供商获取短期证书。这会影响向每个存储驱动程序授予访问权限的方式 AWS API：

- 这个 Amazon EBS CSI 司机操作员 从... 接收其权限 AWS 托管策略 `ROSAAmazonEBSCSIDriverOperatorPolicy`，以及它的 IAM 角色是在您创建集群时自动创建的。这个 Amazon EBS 默认情况下已安装 CSI 驱动程序，其作用是标准的一部分 ROSA 操作员角色。结果， Amazon EBS 无需任何额外存储即可使用 IAM 设置。
- 这个 Amazon EFS CSI 驱动程序 和 NetApp 三叉戟 要求你额外创建一个 IAM 角色和策略，并在驱动程序调用之前将其与集群的 OIDC 提供商关联起来 AWS API。

> **ROSA HCP 和 ROSA Classic 之间的 IAM**
>
> 这个 IAM HCP 和 ROSA classic 的模型不同。用于 HCP 的 ROSA AWS 管理 IAM 策略，ROSA classic 使用该服务定义和管理的策略。有关两种架构的比较，请参见 比较 ROSA 与 HCP 和 ROSA 经典版。

有关永久卷和集群数据加密的更多信息，请参阅 中的数据保护 ROSA。

块存储 Amazon Elastic Block Store

Amazon Elastic Block Store （ Amazon EBS) 提供块存储容量供您使用 ROSA 工作负载。 Amazon EBS 是的默认存储后端 ROSA。您的集群包括 Amazon EBS CSI 驱动程序和 Amazon EBS CSI 司机操作员。除非你配置另一个后端， Amazon EBS 预置所有永久卷。

使用 Amazon EBS 适用于需要低延迟块存储的单 Pod 读写工作负载，例如数据库和其他不在 pod 之间共享文件系统的有状态应用程序。

特性

- 存储类型 — 块存储。每个卷都连接到一个节点。
- 访问模式 — ReadWriteOnce （ 两个 ）。一个 Amazon EBS 多个节点不能同时写入卷。
- 可用区范围 — 一个 Amazon EBS 卷存在于单个可用区中，只能连接到同一可用区中的节点。如果该节点出现故障，则该卷不会自动可供其他可用区中的节点使用。

- 动态配置 — 支持，包括卷快照。

> **EBS 卷的可用区限制**
>
> 一个 Amazon EBS 卷绑定到单个可用区，连接后无法在区域之间移动。使用 `Recreate` 依赖的工作负载的部署策略 Amazon EBS 卷。设置 `volumeBindingMode: WaitForFirstConsumer` 在存储类上。这可确保该卷与使用该卷的容器在同一个可用区中进行配置。

卷类型

这个 Amazon EBS CSI 驱动程序 (`ebs.csi.aws.com`) 支持很多 Amazon EBS 卷类型，包括 `gp3`，`gp2`，`io1`，`io2`，`st1`，以及 `sc1`。您可以使用设置音量类型 `type` 存储类中的参数。

ROSA 提供两种使用通用 SSD 类型的存储类别：

- `gp3-csi` 供给 `gp3` 音量，是集群的默认值。
- `gp2-csi` 供给 `gp2` 卷。

要使用其他卷类型，例如，`io1` 适用于高 IOPS 工作负载或 `st1` 用于优化吞吐量的 HDD — 创建自定义存储类来指定卷的类型 `parameters.type` 领域。我们推荐 `gp3` 结束了 `gp2` 适用于大多数工作负载。

的常用存储类参数 Amazon EBS CSI 驱动程序包括 `type`，`iops`，`throughput`，`encrypted`，以及 `kmsKeyId`。设定 `allowVolumeExpansion: true` 在存储类上启用在线卷大小调整。

默认存储类别

新创建 ROSA 集群（版本 4.10 及更高版本）配置为默认值 `gp3-csi` 由... 支持的存储类别 Amazon EBS CSI 驱动程序。当 PVC 未命名存储类时，ROSA 使用 `gp3-csi` 调配音量。一个 `gp2-csi` 类也适用于需要的工作负载 `gp2` 卷类型。

现代 ROSA 集群仅使用 CSI-backed 存储类别。树中的遗产 AWS EBS 卷插件及其关联存储类已从底层中移除 OpenShift 平台。不要引用传统的树内类名，例如 `gp2` 要么 `gp3` 没有 `-csi` 后缀-在存储类配置中。

加密

Amazon EBS 加密可保护静态和传输中的永久容量数据。

静态加密

使用默认 `gp3-csi` 存储类，您的永久卷在静态时使用加密 AWS 管理 `aws/ebs` AWS KMS 钥匙。从其他存储类别配置的卷仅在等级设置时才会加密 `encrypted: "true"`。

传输中加密

用于加密 Amazon EBS 体积， Amazon EBS 加密保护两者之间传输的数据 Amazon EC2 实例及其附加卷。加密操作在 Amazon EC2 主机。

密钥管理

创建集群时，可以选择加密 Amazon EBS 默认音量 AWS KMS 密钥或由客户管理，对称 AWS KMS 钥匙。客户管理的密钥必须在同一密钥中 AWS 区域 作为集群。要将客户管理的密钥用于从自定义存储类配置的卷，请使用以下命令指定密钥 `kmsKeyId`。

有关以下内容的更多信息 AWS KMS 密钥和加密已开启 ROSA，参见 使用加密保护数据。

Permissions

这个 Amazon EBS CSI 驱动程序操作员从... 获得权限 AWS 托管策略 `ROSAAmazonEBSCSIDriverOperatorPolicy`。运营商的 IAM 角色是在您创建集群时自动创建的，因此无需额外创建 IAM 需要配置才能使用 Amazon EBS 存储。有关如何操作的更多信息 AWS STS 影响存储驱动程序权限，请参阅 the section called “AWS STS 和存储驱动程序权限”。

共享文件存储空间与 Amazon Elastic File System

和 Amazon Elastic File System （ Amazon EFS ），你可以安装共享的弹性， POSIX-compliant 文件系统同时跨越多个 pod。 Amazon EFS 是 ROSA 的选项 ReadWriteMany (RWX) 工作负载，例如内容管理系统、共享应用程序数据以及由许多 pod 读取的机器学习训练数据。

不像 Amazon EBS，的 Amazon EFS CSI 驱动程序是 默认情况下未安装。你必须安装 Amazon EFS CSI 驱动程序操作员并创建所需的 AWS 在您使用之前的身份和访问管理 (IAM) 资源。

特性

- 存储类型 — 共享文件存储。

- 访问模式 — ReadWriteMany （ RWX ） ， ReadWriteOnce (RWO)，以及 ReadOnlyMany （ 罗克斯 ）。
- 可用区范围 — Amazon EFS 是一个可从多个可用区域访问的区域文件系统。一个 Amazon EFS 文件系统不受单个节点或可用区故障的影响。
- 资源调配 — 支持静态和动态配置。动态配置用途 Amazon EFS 接入点。

正在启用 Amazon EFS

要使用 Amazon EFS 上 ROSA，你安装 Amazon EFS 为红帽提供的 CSI 驱动程序操作员 OpenShift。操作员可从以下地址获得 OperatorHub 在 OpenShift Web 控制台，是手动安装的。安装操作员后，您可以创建一个引用 Operator 的存储类 Amazon EFS CSI 驱动程序。

> ⚠ 仅使用红帽 OpenShift EFS CSI 驱动程序
>
> 只有红帽 OpenShift Amazon EFS 支持 CSI 驱动程序和操作员 ROSA。上游社区 Amazon EFS 不支持 CSI 驱动程序。

权限和设置

因为 ROSA 使用 AWS STS，你必须创建一个 IAM 的角色和政策 Amazon EFS CSI 驱动程序并将其与集群的 OIDC 提供商关联以便驱动程序可以调用 Amazon EFS API。与之相比，这是一个额外的步骤 Amazon EBS，其角色是自动创建的。有关 OIDC 凭证模型的更多信息，请参阅 the section called “AWS STS 和存储驱动程序权限”。

这个 IAM 使用 HCP 和 ROSA classic 的 ROSA 的配置步骤相同。在这两种架构中，工作节点都在你的架构中运行 AWS 账户并进行身份验证 AWS 通过集群的 OIDC 发行者获得资源。

正在设置 Amazon EFS 还涉及配置 Amazon EFS 文件系统策略，允许工作节点安全组中的 NFS 流量，并创建存储类。有关详细步骤，请参阅红帽文档以了解如何使用 Amazon EFS 带有 CSI 驱动程序 ROSA。

接入点和文件所有权

当您使用动态配置时， Amazon EFS CSI 驱动程序创建了一个 Amazon EFS 每个卷的接入点。请注意以下行为：

- Amazon EFS 评估接入点的用户 ID 和群组 ID。然后，它将文件用户和群组 ID 替换为接入点的 ID。结果， ROSA 无法使用 `fsGroup` 控制文件组所有权 Amazon EFS 体积； `fsGroup` 设置被静默忽略。
- 任何可以访问已挂载接入点的 pod 都可以访问该卷上的任何文件。

在上设计多租户工作负载时，请考虑这些特征 Amazon EFS。

加密

Amazon EFS 支持使用对静态数据进行加密 AWS KMS 以及使用 TLS 对传输中的数据进行加密。

静态加密

Amazon EFS 静态加密是在文件系统本身上配置的，而不是通过存储类参数配置的。这个 Amazon EFS CSI 驱动程序无法动态配置 Amazon EFS 文件系统。您必须在中预置文件系统 AWS 启用静态加密。然后，您可以在您的文件系统中引用预置的文件系统 PersistentVolume 通过将文件系统 ID 设置为 `volumeHandle`。

传输中加密

In-transit 默认情况下未启用加密。要启用它，请添加 `tls` 到 `mountOptions` 你的数组 PersistentVolume 要么 StorageClass 定义。什么时候 `tls` 已设置， Amazon EFS CSI 驱动程序通过 TLS 挂载文件系统。

密钥管理

指定 AWS KMS 配置时的密钥 Amazon EFS 文件系统。

Multi-protocol 使用亚马逊 FSx 进行存储 NetApp ONTAP

使用亚马逊 FSx NetApp ONTAP，您可以预置基于构建的高性能文件和块存储 NetApp ONTAP 文件系统。开启 ROSA，您可以通过以下方式为 ONTAP 存储配置 FSx NetApp 三叉戟 （ 也称为 Astra Trident ），来自的开源 CSI 驱动程序 NetApp 适用于 Kubernetes。

如果您需要高性能共享存储，或同时需要来自同一文件系统的 NFS 文件卷和 iSCSI 数据块卷，请使用 FSx for ONTAP。它还适合需要使用 ONTAP 数据管理功能的企业工作负载，例如数据库和业务应用程序。

> **NetApp 三叉戟不是 AWS 或红帽服务**
>
> NetApp 三叉戟是一个 NetApp 产品。它不是 AWS 或红帽服务或附加组件。您可以自己安装、配置和操作 Trident，然后 NetApp 支持 Trident 驱动程序。

特性

- 存储类型 — Multi-protocol 文件和块存储。三叉戟可以回来 ROSA FSx 对 ONTAP NFS 或 iSCSI 卷的永久卷容量声明。
- 访问模式 — NFS 卷支持 ReadWriteMany (RWX) 和 ReadWriteOnce (RWO)。iSCSI 数据块卷支持 ReadWriteMany (RWX) 和 ReadWriteOnce （两个）。
- 可用区范围 — FSx for ONTAP 支持 Single-AZ 和 Multi-AZ 部署。 Multi-AZ 文件系统通过文件协议的透明故障转移和 iSCSI 的多路径故障转移提供高可用性。
- Multi-protocol 访问 — Trident 可以从同一 FSx 为 ONTAP 文件系统配置 NFS 文件卷和 iSCSI 数据块卷。

安装三叉戟

您可以使用 Helm Chart (Helm v3) 或 Trident Operator 部署三叉戟 `tridentctl` 命令行工具。你可以自己安装和操作 Trident。Trident 使用基于日历的版本架构（例如 26.06）。 NetApp 通常支持两到三个最新的次要版本。对于与您的兼容的特定版本 ROSA 还有红帽 OpenShift 版本，请参阅 要求 在 NetApp 三叉戟文档。

因为 ROSA 使用 AWS STS，三叉戟需要一个 IAM FSx API 访问的角色。此角色必须连接到集群的 OIDC 提供商，类似于 Amazon EFS CSI 驱动程序。

用于部署和 IAM 设置说明，请参阅 初始设置 在 NetApp的 ROSA 解决方案指南。

> **运行 iSCSI 时从多路径中排除 EBS 设备**
>
> 如果您将适用于 ONTAP iSCSI 卷的 FSx 与 Amazon EBS 相同节点上的 CSI 驱动程序，不包括 Amazon EBS 节点中的设备 `multipath.conf` 配置。这可以防止多路径管理 Amazon EBS 卷。这个 NetApp 部署指南包括已准备好的 `multipath.conf`。

加密

FSx for ONTAP 提供静态和传输中的加密。

静态加密

FSx for ONTAP 使用自动加密所有静态数据和所有备份 AES-256 分组密码和 AWS KMS。

传输中加密

FSx for ONTAP 支持对其文件和数据块协议进行传输加密。

密钥管理

您可以选择两个关键选项之一：

- AWS 托管密钥 — 默认选项。 AWS 无需额外费用即可管理密钥。
- 客户管理的密钥 — 提供你自己的对称模型 AWS KMS 加强控制的关键。使用客户管理的密钥，您可以定义跨账户密钥策略和细粒度的密钥授予，并启用由以下机构管理的年度自动密钥轮换 AWS KMS。

> **FSx for ONTAP 需要对称的 KMS 密钥**
>
> FSx for ONTAP 仅接受对称的 AWS KMS 加密密钥。不支持非对称密钥。

支撑模型

使用 Trident 的 ONTAP 的 FSx 的责任由双方共同承担 AWS 和 NetApp:

- AWS 支持 FSx for ONTAP 后端，包括文件系统、存储虚拟机、卷、逻辑接口和 ONTAP 数据路径。
- NetApp 支持 Trident CSI 驱动程序代码和配置。

ROSA 服务配额

AWS 云端 Red Hat OpenShift 服务 (ROSA) 使用 Amazon EC2、 Amazon Virtual Private Cloud Amazon Elastic Block Store、和的服务配额 Elastic Load Balancing 来配置集群。有关更多信息，请参阅《 AWS 通用参考指南》中的AWS 云端 Red Hat OpenShift 服务 终端节点和配额。

AWS 服务与集成 ROSA

ROSA 与其他 AWS 服务 人合作，为您的业务挑战提供其他解决方案。本主题列出了用于 ROSA 添加功能的服务或 ROSA 用于执行任务的服务。

主题

- ROSA 如何使用 AWS Marketplace

ROSA 如何使用 AWS Marketplace

AWS Marketplace 是一个精心策划的数字目录，可用于查找、购买、部署和管理构建解决方案和运营业务所需的第三方软件、数据和服务。 AWS Marketplace 通过灵活的定价选项和多种部署方法简化软件许可和采购。

ROSA AWS Marketplace 用于服务计量和计费。ROSA classic 通过基于 AWS Marketplace 亚马逊机器映像 (AMI) 的产品进行计量和计费，而带有托管控制平面 (HCP) 的 ROSA 则通过基于 AWS Marketplace 软件即服务 (SaaS) 的产品进行计量和计费。

本页说明了 ROSA 如何使用付 AWS Marketplace 款、账单、订阅和合同购买。

术语

本页在讨论 ROSA 与的集成时使用了以下术语 AWS Marketplace。

亚马逊机器映像 (AMI)

服务器的映像，包括 AWS上运行的操作系统和其他软件。

AMI 订阅

在中 AWS Marketplace，基于 AMI 的软件产品（例如 ROSA classic）使用按小时计费和按年订阅的定价模式。按小时定价是默认的定价模式，但您可以选择为一种 Amazon EC2 实例类型预先购买一年的使用量。

SaaS 订阅

在中 AWS Marketplace，诸如带有 HCP 的 ROSA 之类的 software-as-a-service（SaaS）产品采用基于使用量的订阅模式。软件卖家可以跟踪您的使用情况，您只需按实际使用量付费。

公开报价

公开优惠允许您直接从中购买 AWS Marketplace 软件和服务 AWS 管理控制台。

专属优惠

私人报价是一项购买计划，允许买卖双方就购买的自定义价格和最终用户许可协议 (EULA) 条款进行协商。 AWS Marketplace

ROSA 服务费

红帽站点可靠性工程师对 OpenShift 软件和集群管理 ROSA 收取的费用（SREs）。 ROSA 服务费按量计费， AWS Marketplace 并显示在您的 AWS 账单上。

AWS 基础设施费用

对 AWS 服务 底层 ROSA 集群 AWS 收取的标准费用 Amazon EC2，包括 Amazon EBS、Amazon S3、和 Elastic Load Balancing。费用按使用量计量 AWS 服务 并显示在 AWS 账单上。

ROSA 付款和账单

ROSA 与集成 AWS Marketplace ，以实现 ROSA 服务费的计量和计费。 ROSA 服务费包括红帽站点可靠性工程师访问 OpenShift 软件和集群管理的权限（SREs）。 ROSA 所有支持的 AWS 标准区域的服务费是统一的。默认情况下，带有 HCP 服务费的 ROSA 按需计费，根据这些集群中正在运行的集群和工作节点 v CPUs 的数量，按固定小时费率计算。ROSA 经典服务费用根据工作节点的数量按需累计 vCPUs. ROSA classic 不对控制平面或所需的基础设施节点收取服务费。

ROSA 客户还要为 AWS 服务 底层 ROSA 集群支付标准 AWS 基础设施费用 Amazon EC2，包括 Amazon EBS、 Amazon S3、和 Elastic Load Balancing。 AWS 基础设施费用是与计量 ROSA 服务费分开的计费项目。 AWS Marketplace AWS 默认情况下 AWS 区域 ，基础架构费用因小时使用量而异。为了进一步节省 AWS 基础设施成本，您可以购买 Amazon EC2 节省计划或预留实例。有关更多信息，请参阅 Amazon EC2 用户指南中的 Compute Savings Plans 和预留实例。

ROSA 在您创建 ROSA 集群或购买 ROSA 合约之前，不会收取费用。有关更多信息，请参阅AWS 云端 Red Hat OpenShift 服务 定价。

您可以在AWS Billing 控制台中查看 ROSA 服务费和 AWS 基础设施费用并管理付款。您还可以免费使用该 AWS Cost Explorer Service 界面查看费用并监控使用情况。有关更多信息，请参阅《 AWS 账单与成本管理 用户指南》中的 “查看账单” 和 “成本管理用户指南” AWS Cost Explorer Service中的 “使用分析 AWS成本”。

通过控制台订阅 ROSA Marketplace 商品信息

当你在ROSA 控制台 ROSA中启用时，你订阅了 ROSA class AWS 账户 ic 和 ROSA，HCP 列表处于开 AWS Marketplace启状态。启用 ROSA 订阅不收取任何费用。

对于 AWS Organizations 用户， ROSA 允许您与组织中的其他帐户共享 ROSA classic 订阅。有关更多信息，请参阅《 AWS Marketplace 买家指南》中的在组织中共享订阅。

购买合 ROSA 同

ROSA 用于 AWS Marketplace 为 ROSA 提供 HCP 和 ROSA classic 的可选合同。合同可以节省 ROSA 工作节点的服务费用。 ROSA 合同不影响 AWS 基础设施收取的费用。

12 个月合约

你可以通过 ROSA 控制台购买 ROSA classic 和 ROSA with HCP 的 12 个月公开发行合约。

> **Note**
>
> 必须首先在您的账户上启用 ROSA 经典版，才能从控制台购买 12 个月合约。

> **Note**
>
> 12 个月合约不能转入到专属优惠中。

购买 ROSA 经典版 12 个月合约

当您购买 ROSA 经典版 12 个月合约时，需要预先支付一年期的费用，在接下来的 12 个月内无需为所涵盖的实例支付每小时服务费。合同费用取决于您选择的 Amazon EC2 实例类型和实例数量。该合同不包括对所用标的资产 ROSA AWS 服务 收取的 AWS 基础设施费用。有关更多信息，请参阅AWS 云端 Red Hat OpenShift 服务 定价。

合约仅涵盖您在创建合约时指定的实例类型（例如 m5.xlarge）。您可以购买额外的 12 个月合同，以节省多种 Amazon EC2 实例类型的成本。在您的 12 个月合同之外使用会产生按需费率收取 ROSA 服务费。

> **Note**
>
> ROSA 经典版 12 个月合约不会自动续订。

要为 ROSA 经典版购买 12 个月合约

> **Note**
>
> 如果您在尚不支持 ROSA 和 HCP 的地区使用 ROSA 控制台，则此工作流程尚不可用。有关通过 HCP 支持 ROSA 的地区列表，请参阅the section called “比较 ROSA 与 HCP 和 ROSA 经典版”。
> 要在不支持带 HCP 的 ROSA 的区域中购买 ROSA 经典版合约，请转到 ROSA 控制台并选择购买软件合约和查看现有合约。

1. 转到 ROSA 控制台。
2. 在左侧导航窗格中，选择合约。
3. 选择 ROSA 经典版合约。
4. 选择购买合约。
5. 选择您需要的 EC2 实例类型和实例数量。
6. 选择查看合约。
7. 查看合约详细信息并选择购买合约。

> **Note**
>
> ROSA 使用控制台创建 12 个月的合同后，无法降级或取消。如果需要在有效合约期限内降级或取消合约，请转到 支持 中心并创建一个支持案例。

购买带 HCP 的 ROSA 12 个月合约

当在控制台中启用带 HCP 的 ROSA 时，最初会在您的账户上创建一份免费的带 HCP 的 ROSA 12 个月合约，以方便按需计费。如果您选择购买 ROSA with HCP 合同以节省工作节点服务费，则会修改初始合同以涵盖您指定的工作节点 v CPUs 和控制平面的使用成本。

当您购买ROSA worker with HCP的12个月合同时，您需要预先支付年度期限的费用，并且在接下来的12个月中无需为受保的工作节点v CPUs 和控制平面支付每小时使用费。合同成本基于您选择的工作节点 v CPUs 和控制平面的数量。合约仅涵盖您在创建合约时指定的工作节点 v CPUs 和控制平面。该合同不包括对所用标的资产 ROSA AWS 服务 收取的 AWS 基础设施费用。有关更多信息，请参阅AWS 云端 Red Hat OpenShift 服务 定价。

每月使用量配额

购买后，您的预付费 v CPUs 和控制平面将转换为每月使用配额。超过每月配额的 vCPU 和控制面板使用情况按每小时按需使用费率计费。带 HCP 的 ROSA 使用以下公式计算与合约相关的每月配额：

- 工作节点 vCPUs：v 的数量 CPUs x 24 小时 x 365 天/12 个月
- 控制面板：控制面板数量 x 24 小时 x 365 天/12 个月

例如，购买 4,000 个工作节点 v CPUs 和 8 个控制平面将转换为每月配额 2,920,000 个工作节点 vCPU 小时和每月可消耗的 5,840 个控制平面小时。

要购买带 HCP 的 ROSA 12 个月合约

> **Note**
>
> 如果您在尚不支持 ROSA 托管 AWS 云端 Red Hat OpenShift 服务 控制平面的地区使用控制台，则此工作流程尚不可用。有关通过 HCP 支持 ROSA 的地区列表，请参阅the section called “比较 ROSA 与 HCP 和 ROSA 经典版”。

1. 转到 ROSA 控制台。
2. 在左侧导航窗格中，选择合约。
3. 选择带 HCP 的 ROSA 的合约。
4. 选择购买合约。
5. 输入CPUs 要购买的 v 数。以 4 的倍数指定。
6. 输入要购买的控制面板的数量。
7. 选择查看合约。
8. 查看合约详细信息并选择购买合约。

> **Note**
>
> ROSA 使用控制台创建 12 个月的合同后，无法降级或取消。如果需要在有效合约期限内降级或取消合约，请转到 支持 中心并创建一个支持案例。

升级带 HCP 的 ROSA 12 个月合约

您可以随时使用额外的工作节点 v CPUs 和控制平面升级您的活跃 ROSA 和 HCP 12 个月合同。当升级带 HCP 的 ROSA 12 个月合约时，您需要为增加的资源按比例支付预付款。按比例分摊的费用根据合约的剩余天数计算。合约仅涵盖您在创建合约时指定的工作节点 v CPUs 和控制平面。合同升级不会影响 AWS 基础设施收取的费用。

升级后，使用CPUs 与原始合同购买相同的公式，将添加的 v 和控制平面转换为每月使用配额。超过每月配额的 vCPU 和控制面板使用情况按每小时按需使用费率计费。有关更多信息，请参阅 the section called “每月使用量配额”。

要升级带 HCP 的 ROSA 12 个月合约

1. 转到 ROSA 控制台。
2. 在左侧导航窗格中，选择合约。
3. 选择带 HCP 的 ROSA 的合约。
4. 选择 Upgrade。
5. 输入CPUs 要添加的 v 数。以 4 的倍数指定。
6. 输入要为合约增加的控制面板的数量。
7. 选择查看升级。
8. 查看合约详细信息并选择购买升级。

> **Note**
>
> 无法升级 ROSA 经典版 12 个月合约。您可以随时使用 ROSA 主机购买额外的 12 个月的 ROSA 经典版合约。

获取专属优惠

您可以通过 HCP 或 ROSA classic 向 ROSA 申请 AWS Marketplace 私有报价，以获得与红帽协商的产品定价和最终用户许可协议 (EULA) 条款。有关更多信息，请参阅《 AWS Marketplace 买家指南》中的私人报价。

获取 ROSA 私人报价

> **Note**
>
> 如果您是 AWS Organizations 用户，并且收到了发给您的付款人和成员账户的私人报价，请按照以下步骤 ROSA 直接在组织中的每个账户上订阅。
> 如果您收到仅向 AWS Organizations 付款人账户发放的 ROSA classic 私人优惠，则需要与组织中的成员账户共享订阅。有关更多信息，请参阅《 AWS Marketplace 买家指南》中的在组织中共享订阅。

1. 发出专属优惠之后，登录到 AWS Marketplace 控制台。
2. 打开带有 ROSA 私人报价链接的电子邮件。
3. 单击此链接，以直接访问专属优惠。

> **Note**
>
> 当在登录到正确的账户之前单击此链接时，将产生一个找不到页面 (404) 错误。

4. 查看条款和条件。
5. 选择接受条款。

> **Note**
>
> 如果不接受 AWS Marketplace 私人报价， ROSA 则 AWS Marketplace 将继续按公开小时费率计费。

6. 要验证优惠详细信息，请选择产品列表中的显示详细信息。
7. 要开始使用 ROSA，请选择 “继续配置”。您将被重定向到 ROSA 控制台。

Private Marketplace

Private Marketplace使管理员能够为来自 AWS Marketplace的已批准产品建立定制的数字目录。管理员可以创建独特的经过审查的软件集， AWS Marketplace 供 AWS 组织单位或组织 AWS 账户 内的其他部门购买。

如果您的组织使用私有市场，则管理员必须先将的 AWS Marketplace ROSA 商品添加到私有市场，然后用户才能启用该服务。有关更多信息，请参阅《 AWS Marketplace 买家指南》中的私有市场入门。

问题排查

以下页面详细介绍了在创建或管理 ROSA 集群时遇到的一些常见问题。

主题

- 访问 ROSA 集群调试日志
- ROSA 集群在 集群 创建期间未能通过 AWS 服务配额检查
- ROSA CLI 过期的离线访问令牌疑难解答
- 创建失败 集群 ，但 osdCcsAdmin 出现错误
- 后续步骤
- 获取 ROSA 支持

访问 ROSA 集群调试日志

要开始对应用程序问题进行故障排除，请先查看调试日志。C ROSA LI 调试日志提供了有关创建 集群失败时产生的错误消息的详细信息。

要显示 集群 调试信息，请运行以下 ROSA CLI 命令。在命令中，<cluster_name>用你的名字替换集群。

```
rosa describe cluster -c <cluster_name> --debug
```

ROSA 集群在 集群 创建期间未能通过 AWS 服务配额检查

要使用 ROSA，可能需要增加您账户的服务配额。有关更多信息，请参阅 AWS 云端 Red Hat OpenShift 服务 终端节点和限额。

1. 运行以下命令确定您账户的配额。

```
rosa verify quota
```

> **Note**
>
> 不同 AWS 区域的配额有所不同。请务必确认每个所在区域的配额。

2. 如果您需要增加配额，请导航到 服务配额 控制台。
3. 在导航窗格上，选择 AWS 服务。
4. 选择需要增加配额的服务。
5. 选择需要增加的配额，然后选择请求增加配额。
6. 在请求增加配额中，输入您想要的配额总量，然后选择请求。

ROSA CLI 过期的离线访问令牌疑难解答

如果你使用 ROSA CLI 并且你的 api.openshift.com 离线访问令牌过期，则会出现一条错误消息。当 sso.redhat.com 使令牌失效时，就会发生这种情况。

1. 导航到OpenShift 集群管理器 API 令牌页面，然后选择加载令牌。
2. 复制以下身份验证命令并将其粘贴到终端中。

```
rosa login --token="<api_token>"
```

创建失败 集群 ，但 osdCcsAdmin 出现错误

> **Note**
>
> 仅当您使用非 STS 配置 ROSA 集群的方法时，才会发生此错误。为避免出现此问题，请使用配置您的 ROSA 集群 AWS STS。有关更多信息，请参阅 the section called “创建 ROSA 经典集群-CLI”。

如果创建 集群 失败，则可能会收到以下错误消息：

```
Failed to create cluster: Unable to create cluster spec: Failed to get access keys for
 user 'osdCcsAdmin': NoSuchEntity: The user with name osdCcsAdmin cannot be found.
```

1. 删除 堆栈。

```
rosa init --delete-stack
```

2. 重新初始化您的账户。

```
rosa init
```

后续步骤

- 请访问OpenShift 文档。
- 打开支持 案例或 Red Hat Support 案例。
- 查找有关以下常见问题的答案 AWS 云端 Red Hat OpenShift 服务。
- 有关 ROSA 支持模式的更多信息，请参阅the section called “获取支持”。

获取 ROSA 支持

借助 ROSA，您可以获得红帽支持团队的支持。 支持 可以向任一组织提出支持案例，然后转到正确的团队以解决您的问题。

打开一个 支持 case

需要 AWS 开发者支持计划才能打开 ROSA 技术案例，但建议使用 AWS 商业、企业或企业 On-Ramp 支持计划，以便持续获得 ROSA 技术支持和架构指导。必要时，红帽使用该 支持 API 为客户打开案例。 AWS 商业、企业和企业 On-Ramp 支持计划允许支持工程师持续访问电话、网络和聊天。有关 支持 计划的更多信息，请参阅支持。

有关启用 支持 套餐的步骤，请参阅如何注册 支持 套餐？

有关创建 支持 案例的信息，请参阅创建支持案例和案例管理。

打开 Red Hat Support 案例

ROSA 包括红帽 Premium Support。要获得 Red Hat Premium Support，请导航到 Red Hat Customer Portal，然后使用支持案例工具创建支持问题单。有关更多信息，请参阅如何与红帽支持联系。

文档历史记录

下表介绍了对 文档的一些重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

变更	说明	日期
已更新 ROSAControlPlaneOperatorPolicy	此更新为 `ROSAControlPlaneOperatorPolicy` 添加创建、检查、标记和删除的权限 Route 53 托管区域。您可以使用控制平面操作员管理集群 DNS 区域和附加红色下的记录 Hat-managed 域名。有关更多信息，请参阅 ROSAControlPlaneOperatorPolicy。	2026 年 11 月 12 日
已更新 ROSANodePoolManagementPolicy	更新后的 `ROSANodePoolManagementPolicy` 支持中的工作节点维护 ROSA 集群。 AWS 云端 Red Hat OpenShift 服务（ROSA) 是一项托管的 Kubernetes 服务。此更新适用于保持长时间运行的管理员 ROSA 集群。 该政策现在包括启动后管理现有工作人员资源的额外权限。此更新有助于保持工作线程资源与集群配置保持一致，而无需更换工作节点。 要了解更多信息，请参阅 ROSANodePoolManagementPolicy 在 ROSA 用户指南。	2026年11月5日

新的存储章节	我们添加了 “存储” 章节，描述了以下内容的永久存储选项 ROSA 集群。本章介绍如何做 ROSA 通过容器存储接口 (CSI) 配置存储。它还涵盖了块存储 Amazon Elastic Block Store，与共享文件存储 Amazon Elastic File System，以及使用 Amazon FSx 的多协议存储 NetApp ONTAP 直通 NetApp 三叉戟。有关更多信息，请参阅 存储在 ROSA。	2026 年 10 月 1 日
已更新 ROSAAmazonEBSCSIDriverOperatorPolicy	我们更新了管理政策 `ROSAAmazonEBSCSIDriverOperatorPolicy` 扩展 Amazon EBS 1.61 版本功能集的 CSI 驱动程序。在这次更新中， Amazon EBS CSI 驱动程序操作员可以复制和锁定 Amazon EBS 快照并启用快速快照恢复。它也可以使用客户管理的 AWS KMS 加密卷操作的密钥。有关更多信息，请参阅 ROSA 更新到 AWS 托管策略。	2026 年 8 月 18 日

已更新 ROSANodePoolManagementPolicy	更新了 AWS 托管策略 ROSANodePoolManagementPolicy 允许 NodePool 用于描述 EC2 实例类型的控制器。控制器还可以接收和删除客户管理的 Amazon SQS 队列中携带的竞价实例中断消息 `red-hat: "true"` 资源标签。有关更多信息，请参阅 ROSA 更新到 AWS 托管策略。	2026 年 7 月 28 日
已更新 ROSAControlPlaneOperatorPolicy	更新了 AWS 托管策略 ROSAControlPlaneOperatorPolicy。通过此更新，控制平面操作员可以在 Red 上添加和移除标签 Hat-managed 安全组（`ec2:DeleteTags`）。保护措施可防止操作员移除 `red-hat-managed` 标记本身。有关更多信息，请参阅 ROSA 更新到 AWS 托管策略。	2026 年 7 月 28 日
New ROSAKarpenterControllerPolicy	AWS 发布了新的管理策略 `ROSAKarpenterControllerPolicy` 使 Karpenter 控制器能够使用托管控制平面集群为 ROSA 动态配置、扩展和管理 EC2 工作节点。有关更多信息，请参阅 ROSA 更新到 AWS 托管策略。	2026年7月22日

已更新 ROSAControlPlaneOperatorPolicy	更新了 AWS 托管策略 ROSAControlPlaneOperatorPolicy 允许标记红色 Hat-managed 安全组用于适当的资源生命周期管理并将安全组/* 添加到 ManageVPCEndpointWithCondition 修复集群升级期间的 VPCE 协调失败问题。有关更多信息，请参阅 ROSA 更新到 AWS 托管策略。	2026 年 4 月 9 日
已更新 ROSAKubeControllerPolicy	更新了 AWS 托管策略 ROSAKubeControllerPolicy 阐明向目标组注册和取消注册目标的弹性负载平衡权限。有关更多信息，请参阅 ROSA 更新到 AWS 托管策略。	2026 年 3 月 5 日
已更新 ROSANodePoolManagementPolicy	ROSA 已更新管理策略 `ROSANodePoolManagementPolicy` 为容量预留添加资源访问权限以支持容量预留功能。有关信息，请参见 ROSA 更新到 AWS 托管策略。	2025 年 9 月 3 日
已更新 ROSAInstallerPolicy	更新了 AWS 托管策略 ROSAInstallerPolicy 支持 ROSA 中的新容量预留功能并改进 Kubernetes 集群标签管理。有关信息，请参见 ROSA 更新到 AWS 托管策略。	2025 年 8 月 7 日

New ROSASharedVPCRoute53Policy	ROSA 已经发布了新的管理策略 ROSASharedVPCRoute53Policy 允许 ROSA 安装程序在共享 VPC 环境中配置 Route 53 记录。有关信息，请参见 ROSA 更新到 AWS 托管策略。	2025 年 8 月 7 日
New ROSASharedVPCEndpointPolicy	ROSA 已经发布了新的管理策略 ROSASharedVPCEndpointPolicy 允许 ROSA 安装程序在共享 VPC 环境中配置 VPC 终端节点和安全组。该策略提供了一部分专为共享 VPC 用例量身定制的 EC2 权限。有关信息，请参见 ROSA 更新到 AWS 托管策略。	2025 年 8 月 7 日
已更新 ROSAImageRegistryOperatorPolicy	更新了 AWS 托管策略 ROSAImageRegistryOperatorPolicy。	2025 年 5 月 19 日
已更新 ROSANodePoolManagementPolicy	更新了 AWS 托管策略 ROSANodePoolManagementPolicy 。	2025 年 5 月 5 日
已更新 ROSAImageRegistryOperatorPolicy	更新了 AWS 托管策略 ROSAImageRegistryOperatorPolicy。	2025 年 4 月 16 日
已更新 ROSAWorkerInstancePolicy	更新了 AWS 托管策略 ROSAWorkerInstancePolicy。	2025 年 3 月 3 日
已更新 ROSANodePoolManagementPolicy	更新了 AWS 托管策略 ROSANodePoolManagementPolicy。	2025 年 2 月 24 日

已更新 ROSAAmazonEBSCSIDriverOperatorPolicy	更新了 AWS 托管策略 ROSAAmazonEBSCSIDriverOperatorPolicy。	2025 年 1 月 17 日
ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在中东（阿联酋）上市 AWS 区域。	2024 年 5 月 13 日
ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在欧洲（巴黎）上市 AWS 区域。	2024 年 5 月 6 日
已更新 ROSANodePoolManagementPolicy	更新了 AWS 托管策略 ROSANodePoolManagementPolicy。	2024 年 5 月 2 日
ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在欧洲（西班牙）上市 AWS 区域。	2024 年 4 月 29 日
已更新 ROSAInstallerPolicy	更新了 AWS 托管策略 ROSAInstallerPolicy。	2024 年 4 月 24 日
ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在欧洲（苏黎世）上市 AWS 区域。	2024 年 4 月 19 日
ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在亚太地区（大阪）上市 AWS 区域。	2024 年 4 月 17 日
已更新 ROSAInstallerPolicy 和 ROSASRESupportPolicy	更新了 AWS 托管策略 ROSAInstallerPolicy 和 ROSASRESupportPolicy。	2024 年 4 月 10 日
ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在亚太地区（香港）上市 AWS 区域。	2024 年 4 月 8 日

ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在南美洲（圣保罗）上市 AWS 区域。	2024 年 4 月 1 日
ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在中东（巴林）上市 AWS 区域。	2024 年 3 月 25 日
ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在亚太地区（首尔）上市 AWS 区域。	2024 年 3 月 14 日
ROSA 和 HCP AWS 区域 扩张	带有托管控制飞机 (HCP) 的 ROSA 现已在非洲（开普敦）上市 AWS 区域。	2024 年 3 月 5 日
已更新 ROSAInstallerPolicy	更新了 AWS 托管策略 ROSAInstallerPolicy。	2024 年 1 月 26 日
已更新 ROSASRESupportPolicy	更新了 AWS 托管策略 ROSASRESupportPolicy。	2024 年 1 月 22 日
已更新 ROSAImageRegistryOperatorPolicy	更新了 AWS 托管策略 ROSAImageRegistryOperatorPolicy。	2023 年 12 月 12 日
已更新 ROSAKubeControllerPolicy	更新了 AWS 托管策略 ROSAKubeControllerPolicy。	2023 年 10 月 16 日
已更新 ROSAManageSubscription	更新了 AWS 托管策略 ROSAManageSubscription。	2023 年 8 月 1 日
已更新 ROSAKubeControllerPolicy	更新了 AWS 托管策略 ROSAKubeControllerPolicy。	2023 年 7 月 13 日
添加了 ROSA 安全页面	添加了 ROSA 中的故障恢复能力、ROSA 中的基础设施安全和 ROSA 中的数据保护等页面。	2023 年 6 月 30 日

添加了部署选项页面	添加了部署选项页面。	2023 年 6 月 9 日
添加了新的 AWS 托管策略 ROSANodePoolManagementPolicy	全新 AWS 托管策略 ROSANodePoolManagementPolicy 已添加。	2023 年 6 月 8 日
添加了新的 AWS 托管策略 ROSAInstallerPolicy	全新 AWS 托管策略 ROSAInstallerPolicy 已添加。	2023 年 6 月 6 日
添加了新的 AWS 托管策略 ROSASRESupportPolicy	全新 AWS 托管策略 ROSASRESupportPolicy 已添加。	2023 年 6 月 1 日
添加了 ROSA 责任概述	添加了 ROSA 责任概述页面。	2023 年 5 月 26 日
更新了什么 AWS 云端 Red Hat OpenShift 服务？	更新了“是什么” AWS 云端 Red Hat OpenShift 服务 页面。	2023 年 5 月 24 日
添加了新的 AWS ROSA 操作员角色的管理策略	全新 AWS 托管策略 ROSAImageRegistryOperatorPolicy， ROSAKubeControllerPolicy，以及 ROSAKMSProviderPolicy 已添加。	2023 年 4 月 27 日
添加了新的 AWS 托管策略 ROSAControlPlaneOperatorPolicy	全新 AWS 托管策略 ROSAControlPlaneOperatorPolicy 已添加。	2023 年 4 月 24 日
添加了新的 AWS ROSA 账户角色的管理策略	全新 AWS 添加了 ROSA 账户的管理策略页面和操作员角色页面。	2023 年 4 月 20 日
添加了 ROSA 服务限额页面	添加了 ROSA 服务配额页面。	2022 年 12 月 22 日
添加了故障排除页面	添加了疑难解答页面。	2022 年 11 月 1 日
添加了开始使用页面	添加了入门页面。	2022 年 8 月 12 日

添加了新的 AWS 托管策略 ROSAManageSubscription	全新 AWS 托管策略 ROSAManageSubscription 已添加。	2022 年 4 月 11 日
初始版本	的初始版本 AWS 云端 Red Hat OpenShift 服务 用户指南。	2021 年 3 月 24 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。