aws

用户指南

AWS 云端 Red Hat OpenShift 服务

AWS 云端 Red Hat OpenShift 服务: 用户指南

Table of Contents

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

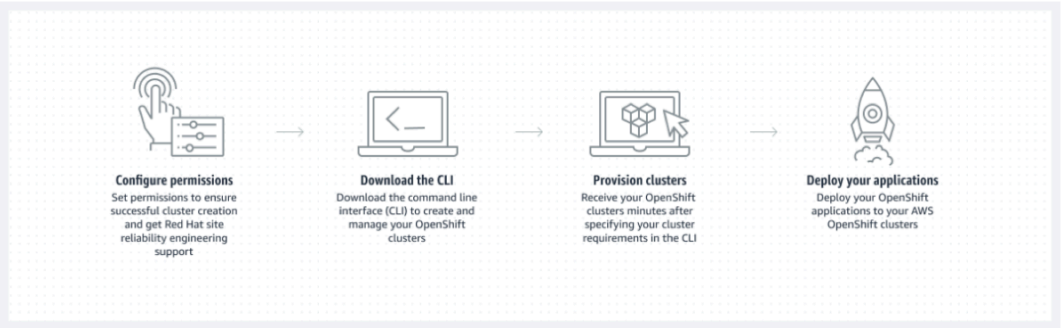
- ROSA 控制台-提供 Web 界面以启用 ROSA 订阅和购买 ROSA 软件合同。
- AWS Command Line Interface (AWS CLI) — 提供适用于各种各样的命令 AWS 服务 并在 Windows、macOS 和 Linux 上受支持。有关更多信息，请参阅 AWS Command Line Interface。

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 Management Console/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 服务控制策略拒绝所需的 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

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

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

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。

安全性 ROSA

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于的合规计划 ROSA，请参阅AWS 服务 按合规计划划分的范围。
- 云端安全 — 您的责任由您 AWS 服务 使用的内容决定。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。它向您展示了如何进行配置 ROSA 以满足您的安全和合规性目标。您还将学习如何使用其他方法 AWS 服务 来帮助您监控和保护您的 ROSA 资源。

内容

中的数据保护 ROSA

the section called “责任”文档和AWS 分担责任模型在中定义了数据保护 ROSA。 AWS 负责保护运行所有内容的全球基础设施 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。此内容包括您 AWS 服务 使用的的安全配置和管理任务。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 安全博客上的责任AWS 共担模型和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭据并使用 AWS Identity and Access Management (IAM) 设置个人用户。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）。

- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，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 Amazon Macie，例如，它有助于发现和保护存储在中的敏感数据 Amazon S3。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 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）。这包括您使用控制台、API ROSA 或以其他 AWS 服务 方式使用控制台 AWS CLI、API 或时 AWS SDKs。您输入的任何数据 ROSA 或其他服务都可能会被提取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

数据保护是指在传输（往返传输时 ROSA）和静态数据（存储在 AWS 数据中心的磁盘上时）保护数据。

AWS 云端 Red Hat OpenShift 服务 提供对连接到 ROSA 控制平面、基础架构和工作节点 Amazon EC2 实例的 Amazon Elastic Block Store (Amazon EBS) 存储卷以及用于持久存储的 Kubernetes 永久卷的安全访问。 ROSA 对静态和传输中的卷数据进行加密，并使用 AWS Key Management Service (AWS KMS) 来帮助保护您的加密数据。该服务 Amazon S3 用于容器镜像注册表存储，该存储默认处于静态加密状态。

> **Important**
>
> 因为 ROSA 是一项托管服务 AWS ，红帽负责管理所 ROSA 使用的基础架构。客户不应尝试通过 AWS 控制台或 CLI 手动关闭 ROSA 使用的 Amazon EC2 实例。此操作可能会导致客户数据丢失。

为 Amazon EBS支持的存储卷进行数据加密

AWS 云端 Red Hat OpenShift 服务 使用 Kubernetes 持久卷 (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由连接到 Amazon EC2 实例的 Amazon Elastic Block Store (Amazon EBS) 存储卷提供支持。

对于由支持的 ROSA 永久卷和节点 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实例与其连接存储之间传输的数据的安全性。有关更多信息，请参阅《Amazon EC2 用户指南》中的Amazon EBS 加密。

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

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

ROSA 还能够使用 Amazon EFS CSI 驱动程序和 Amazon EFS CSI 驱动程序操作员配置永久卷。Amazon EFS 驱动程序和操作员还允许您在 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。

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

> **Important**
>
> 使用 Amazon EFS CSI 驱动程序动态配置 ROSA 永久卷时，在评估文件系统权限时会 Amazon EFS 考虑访问点 IDs 的用户 ID、组 ID (GID) 和辅助组。 Amazon EFS 将文件 IDs 上的用户和组替换为接入点 IDs 上的用户和组，并忽略 NFS 客户端。 IDs因此， Amazon EFS 默默地忽略设置`fsGroup`。 ROSA 无法使用替换 o GIDs f 的文件`fsGroup`。任何可以访问已安装 Amazon EFS 的接入点的 pod 都可以访问该卷上的任何文件。有关更多信息，请参阅《Amazon EFS 用户指南》中的使用 Amazon EFS 接入点。

etcd 加密

ROSA 提供了在创建集群期间启用对`etcd`卷内`etcd`密钥值的加密的选项，从而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 ROSA 服务定义中的 etcd 加密。

密钥管理

ROSA 用于安全 KMS keys 地管理客户应用程序的控制平面、基础架构、工作人员数据量和永久卷。在创建集群期间，您可以选择使用 KMS key 提供的默认 AWS 托管密钥 Amazon EBS，也可以指定自己的客户托管密钥。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 提供了一个内置的容器镜像注册表，用于通过存储 Amazon S3 桶存储存储、检索和共享容器镜像。注册表由 OpenShift 映像注册表操作员配置和管理。它为用户提供了一种 out-of-the-box解决方案，用于管理运行其工作负载并在现有集群基础架构之上运行的映像。有关更多信息，请参阅 Red Hat 文档中的注册表。

ROSA 提供公共和私有图像注册库。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，默认情况下 ROSA 使用 Amazon S3 托管密钥的服务器端加密 (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《 Amazon S3 用户指南》中的使用 Amazon S3 托管加密密钥的服务器端加密保护数据 (SSE-S3)。

ROSA 使用传输层安全 (TLS) 协议来保护进出镜像注册表的数据的安全。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 ROSA 集群中的资源之间创建边界，并控制这些资源、您的本地网络和互联网之间的流量。有关 Amazon VPC 安全的更多信息，请参阅《 Amazon VPC 用户指南》 Amazon VPC中的互联网流量隐私。

在 VPC 中，您可以将 ROSA 集群配置为使用 HTTP 或 HTTPS 代理服务器来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 ROSA 集群中 Pod。有关更多信息，请参阅 the section called “基础结构安全性”。

使用 KMS 进行数据加密

ROSA AWS KMS 用于安全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 KMS key 提供的 AWS 托管卷进行加密 Amazon EBS。这 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。

新创建的 ROSA 集群配置为使用默认 gp3 存储类来加密永久卷。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 ROSA 预建存储类的更多信息，请参阅 Red Hat 文档中的配置永久存储。

在创建集群期间，您可以选择使用默认 Amazon EBS提供的密钥对集群中的永久卷进行加密，也可以指定自己的客户托管对称 KMS key。有关创建密钥的更多信息，请参阅 AWS KMS 开发人员指南中的创建对称加密 KMS 密钥。

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准则时，这很有用 AWS。有关更多信息，请参阅 Red Hat 文档 KMS key中的AWS 使用加密容器永久卷。

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 加密与自己的密钥一起使用时 KMS key，密钥必须与您的集群 AWS 区域 相同。
- 创建和使用自己的作品会产生一定的成本 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) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。 IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 ROSA 资源。 IAM 无需支付额外费用即可使用。 AWS 服务

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
- 对 ROSA 身份和访问进行故障排除

受众

你使用 AWS Identity and Access Management (IAM) 的方式会有所不同，具体取决于你所做的工作 ROSA。

服务用户-如果您使用该 ROSA 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当你使用更多 ROSA 功能来完成工作时，你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，请参阅the section called “问题排查”。

服务管理员-如果您负责公司的 ROSA 资源，则可能拥有完全访问权限 ROSA。您的工作是确定您的服务用户应访问哪些 ROSA 功能和资源。然后，您必须向 IAM 管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念 IAM。

IAM 管理员-如果您是 IAM 管理员，则可能需要了解有关用于管理访问权限的策略的详细信息 ROSA。要查看可在中使用的 ROSA 基于身份的策略示例 IAM，请参阅。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 AWS 使用身份凭证登录的方式。您必须 AWS 账户 以 root 用户身份进行身份验证（登录 AWS） IAM 用户，或者通过扮 IAM 演角色进行身份验证。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 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 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员之前使用 IAM 角色设置了联合身份。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《登录用户指南》中的如何 AWS 登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

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 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅 AWS IAM Identity Center（ AWS 单点登录的继任者）用户指南中的多重身份验证和 IAM 用户指南AWS中的使用多重身份验证 (MFA)。

AWS 账户 root 用户

创建时 AWS 账户，您首先要使用一个单一登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。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。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的 “需要根用户凭据的 IAM 任务”。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity Center 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，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，以便在您的所有 AWS 账户 和应用程序中使用。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（ AWS 单点登录的继任者）用户指南中。

IAM 用户 和群组

IAM 用户是指您内部 AWS 账户 对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时证书，而不是创建 IAM 用户 谁拥有长期证书，例如密码和访问密钥。但是，如果您有需要长期凭证的特定用例 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。

IAM 群组是指定集合的身份 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，您可以拥有一个名为的组，IAMAdmins并授予该组管理 IAM 资源的权限。

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 IAM 用户指南中的何时创建 IAM 用户 （ 而不是角色 ）。

IAM 角色

IAM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定的人无关。您可以通过切换 IAM 角色 AWS Management Console 来临时担任中的角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南中的使用 IAM 角色。

IAM 具有临时证书的角色在以下情况下很有用：

- 联合用户访问权限-要向联合身份分配权限，您需要创建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，请参阅 AWS IAM Identity Center（ AWS 单点登录的继任者）用户指南中的权限集。

- 临时 IAM 用户 权限- IAM 用户 可以代入一个 IAM 角色来临时获得特定任务的不同权限。
- 跨账户访问-您可以使用 IAM 角色允许其他账户中的某人（受信任的委托人）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，对于某些资源 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 IAM 用户指南中的 IAM 角色与基于资源的策略的区别。
- 跨服务访问-有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中进行调用时，该服务通常会在其中运行应用程序 Amazon EC2 或在其中存储对象 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)-当您使用 IAM 用户 或角色在中执行操作时 AWS，您被视为委托人。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 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。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 IAM 角色是服务代替您执行操作的角色。 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。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色显示在您的 IAM 账户中，并归服务所有。 IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在上运行的应用程序 Amazon EC2 -您可以使用 IAM 角色管理在 Amazon EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 Amazon EC2 实例中存储访问密钥更可取。要为 Amazon EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要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允许在 Amazon EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是使用 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发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。大多数策略都以 JSON 文档的 AWS 形式存储在中。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 JSON 策略来指定谁有权访问什么。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。要授予用户对其所需资源执行操作的权限， IAM 管理员可以创建 IAM 策略。然后，管理员可以将 IAM 策略添加到角色中，用户可以代入角色。

IAM 无论您使用何种方法执行操作，策略都会定义该操作的权限。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 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是您可以附加到身份（例如、角色或群组）的 JSON 权限策略文档。 IAM 用户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策略，请参阅 IAM 用户 IAM 指南中的创建策略。

基于身份的策略可以进一步归类为内联策略或托管式策略。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，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。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。

基于资源的策略

基于资源的策略是附加到资源的 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。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略 IAM 中使用 AWS 托管策略。

访问控制列表 (ACLs)

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

Amazon S3 AWS WAF、和 Amazon VPC 都是支持的服务示例 ACLs。要了解更多信息 ACLs，请参阅《亚马逊简单存储服务用户指南》中的访问控制列表 (ACL) 概述。

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向 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。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 IAM 用户指南中的IAM 实体的权限边界。
- 服务控制策略 (SCPs)- SCPs 是 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中实体的权限，包括每个 AWS 账户 root 用户。有关 Organization SCPs s 和的更多信息，请参阅《 AWS Organizations 用户指南》中的服务控制策略 (SCPs)。
- 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。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

ROSA 基于身份的策略示例

默认情况下 IAM 用户 ，角色无权创建或修改 AWS 资源。他们也无法使用 AWS Management Console AWS CLI、或 AWS API 执行任务。 IAM 管理员必须创建 IAM 策略，授予用户和角色对其所需的指定资源执行特定 API 操作的权限。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户 或群组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅 IAM 用户指南中的 “在 JSON” 选项卡上创建策略。

使用控制 ROSA 台

要 ROSA 从控制台订阅，您的 IAM 委托人必须具有所需的 AWS Marketplace 权限。这些权限允许委托人订阅和取消订阅中的 ROSA 产品列表 AWS Marketplace 以及查看 AWS Marketplace 订阅。要添加所需的权限，请转到ROSA 控制台并将 AWS 托管策略附加`ROSAManageSubscription`到您的 IAM 委托人。有关 `ROSAManageSubscription`的更多信息，请参阅the section called “AWS 托管策略： ROSAManage订阅”。

授权 ROSA 与 HCP 一起管理资源 AWS

带有托管控制平面 (HCP) 的 ROSA 使用具有服务操作和支持所需权限的 AWS 托管策略。您可以使用 ROSA CLI 或 IAM 控制台将这些策略附加到中的服务角色 AWS 账户。

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

授权 ROSA 经典版管理资源 AWS

ROSA classic 使用客户托管的 IAM 策略，其权限由服务预先定义。您可以使用 ROSA CLI 创建这些策略并将其附加到中的服务角色 AWS 账户。 ROSA 要求按照服务定义配置这些策略，以确保持续的操作和服务支持。

> **Note**
>
> 在未事先咨询红帽之前，您不应更改 ROSA 的经典政策。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。带有托管控制平面的 ROSA 使用权限集更有限的 AWS 托管策略。有关更多信息，请参阅 the section called “ AWS 托管策略”。

有两种类型的客户托管政策 ROSA：账户策略和运营商政策。账户策略附加到该服务用来与红帽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的 IAM 角色。操作员策略附加到 OpenShift 操作员用于与入口、存储、图像注册表和节点管理相关的集群操作的 IAM 角色。每个集群只能创建一次账户策略 AWS 账户，而每个集群只能创建一次操作员策略。

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查看附加 IAM 用户 到其用户身份的内联和托管策略的策略。此策略包括在控制台上或使用以编程方式完成此操作的 AWS CLI权限。

```
{
    "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 classic 所需的账户政策的详细信息。ROSA classic 需要这些权限来管理集群运行的 AWS 资源并为集群启用红帽站点可靠性工程师支持。您可以为策略名称分配自定义前缀，但这些策略应按照本页上的定义命名（例如，`ManagedOpenShift-Installer-Role-Policy`）。

账户政策特定于 OpenShift 次要发行版本，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，`rosa upgrade account-roles`请运行升级角色和附加的策略。您可以为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]-安装程序角色策略

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 安装程序管理创建集群所需的 AWS 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-角色政策

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。此策略向 ROSA classic 授予所需的管理 Amazon EC2 权限、托 ROSA 管控制层面的 Elastic Load Balancing 资源以及读取权限 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]-工作人员角色政策

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]-支持角色政策

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 ROSA 经典集群使用的 AWS 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

本节提供有关 ROSA classic 所需的运营商策略的详细信息。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 操作员管理 ROSA 经典群集节点。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-证书

您可以将 `[Prefix]-openshift-ingress-operator-cloud-credentials` 附加到 IAM 实体。此策略向 Ingress 操作员授予必要的权限，以配置和管理用于外部集群访问的负载均衡器和 DNS 配置。该政策还允许 Ingress 操作员读取和筛选 Route 53 资源标签值以发现托管区域。有关运算符的更多信息，请参阅 OpenShift GitHub 文档中的 OpenShift Ingress Operator。

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-credentials

您可以将 `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` 附加到 IAM 实体。此策略向 Amazon EBS CSI 驱动程序操作员授予在 ROSA 经典集群上安装和维护 Amazon

EBS CSI 驱动程序所需的权限。有关运算符的更多信息，请参阅 OpenShift GitHub 文档中的 aws-ebs-csi-driver-operator。

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-云凭证

您可以将 `[Prefix]-openshift-machine-api-aws-cloud-credentials` 附加到 IAM 实体。此策略向 Machine Config 操作员授予描述、运行和终止作为工作节点管理的 Amazon EC2 实例所需的权限。此策略还授予允许使用对工作节点根卷进行磁盘加密的权限 AWS KMS keys。有关运算符的更多信息，请参阅 OpenShift GitHub 文档machine-config-operator中的。

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-credential-operator-云凭证

您可以将 `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` 附加到 IAM 实体。此政策向云凭证操作员授予检索 IAM 用户 详细信息的必要权限，包括访问密钥 IDs、附加的内联策略文档、用户的创建日期、路径、用户 ID 和 Amazon 资源名称 (ARN)。有关运算符的更多信息，请参阅 OpenShift GitHub 文档cloud-credential-operator中的。

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-image-registry-installer-云凭证

您可以将 `[Prefix]-openshift-image-registry-installer-cloud-credentials` 附加到 IAM 实体。该策略向映像注册表操作员授予所需的权限，以配置和管理ROSA classic的集群内映像注册表和相关服务的资源，包括 Amazon S3。这是必需的，这样操作员才能安装和维护 ROSA classic 集群的内部注册表。有关该运算符的更多信息，请参阅 OpenShift GitHub 文档中的图像注册表运算符。

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-config-controller-cloud-cr

您可以将 `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` 附加到 IAM 实体。此策略向 Cloud Network Config Config Config Controller 操作员授予配置和管理网络资源以供 ROSA 经典集群网络覆盖层使用的必要权限。操作员使用这些权限来管理作为 ROSA 经典集群一部分的 Amazon EC2 实例的私有 IP 地址。有关运算符的更多信息，请参阅 OpenShift GitHub 文档loud-network-config-controller中的 C。

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

AWS 托管策略是由创建和管理的独立策略 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、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，因为它们可供所有 AWS 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 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。有关更多信息，请参阅《 IAM 用户指南》中的AWS 托管策略。

AWS 托管策略： ROSAManage订阅

您可以将该ROSAManageSubscription策略附加到您的 IAM 实体。在 AWS ROSA 控制台 ROSA 中启用之前，必须先将此策略附加到 IAM 角色。

此策略授予您管理 ROSA 订阅所需的 AWS Marketplace 权限。

权限详细信息

该策略包含以下权限。

- `aws-marketplace:Subscribe`-授予订阅 AWS Marketplace 产品的权限 ROSA。
- `aws-marketplace:Unsubscribe`-允许委托人删除对 AWS Marketplace 产品的订阅。
- `aws-marketplace:ViewSubscriptions`-允许委托人查看来自的订阅。 AWS Marketplace这是必需的，这样 IAM 委托人才能查看可用的 AWS Marketplace 订阅。

要查看完整的 JSON 策略文档，请参ROSAManage阅《 AWS 托管策略参考指南》中的订阅。

采用 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 托管策略旨在由 ROSA 与托管控制平面 (HCP) 一起使用。ROSA 经典集群使用客户托管 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 托管策略： ROSAWorkerInstancePolicy

你可以附加ROSAWorkerInstancePolicy到你的 IAM 实体。在创建集群之前，您必须拥有一个附加此策略的 IAM 角色。ROSA 服务代表您拨打他人的 AWS 服务 电话。他们这样做是为了管理您在每个集群中使用的资源。

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— 作为 ROSA 集群工作节点生命周期管理的一部分，评估 AWS 区域 和 Amazon EC2 实例详细信息。
- ecr-评估并从 Rosa 管理的 ECR 存储库中获取镜像，这些镜像是集群安装和工作节点生命周期管理所必需的。

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

AWS 托管策略： ROSASRESupport策略

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。此策略向红帽站点可靠性工程师 (SREs) 授予直接观察、诊断和支持与 ROSA 集群相关的 AWS 资源所需的权限，包括更改 ROSA 群集节点状态的能力。

权限详细信息

此策略包括以下权限，允许红帽 SREs 完成以下任务：

- cloudtrail— 读取与集群相关 AWS CloudTrail 的事件和跟踪。
- cloudwatch— 读取与集群相关的 Amazon CloudWatch 指标。
- ec2— 阅读、描述和查看与集群运行状况相关的 Amazon EC2 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、描述和查看与集群运行状况相关的 Elastic Load Balancing 参数。
- iam— 评估与集群运行状况相关的 IAM 角色。
- route53 – 查看与集群运行状况相关的 DNS 设置。

- `stsDecodeAuthorizationMessage`— 阅读 IAM 消息以进行调试。

要查看完整的 JSON 策略文档，请参阅ROSASRESupport《 AWS 托管策略参考指南》中的策略。

AWS 托管策略： ROSAInstaller策略

你可以附加`ROSAInstallerPolicy`到你的 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管理支持 ROSA 群集安装的 AWS 资源的必要权限。

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`— 使用 AMIs 由红帽 AWS 账户 拥有和管理的托管方式运行 Amazon EC2 实例。描述与 Amazon EC2 节点关联的 Amazon EC2 实例、卷和网络资源。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检查 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`"kubernetes.io/cluster/*"`来标记和删除子网上的标签。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 服务和应用程序服务请求的负载均衡器。 OpenShift
- `kms`— 读取 AWS KMS 密钥，创建和管理授权 Amazon EC2，并返回唯一的对称数据密钥以供外部使用。 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。动态配置和管理与集群相关的 Amazon EC2 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 提供程序而导致集群安装失败时，提供安装程序错误消息。
- `route53`— 管理创建集群所需的 Route 53 资源。
- `servicequotas` – 评估创建集群所需的服务限额。
- `sts`— 为 ROSA 组件创建临时 AWS STS 证书。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ROSAInstaller《 AWS 托管策略参考指南》中的策略。

AWS 托管策略： ROSASharedVPCRoute53策略

你可以附加ROSASharedVPCRoute53Policy到你的 IAM 实体。您必须将此策略附加到 IAM 角色才能允许 ROSA 集群 AWS 服务 在共享 VPC 环境中向其他群集进行调用。

此策略允许 ROSA 安装程序配置 Route 53 记录。此策略旨在用于共享 VPC，并提供为共享 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 区域信息和现有的 DNS 记录以了解当前 DNS 配置。创建、修改和删除 DNS 记录，但仅适用于与 Rosa 相关的特定域名模式.hypershift.local，包括、.openshiftapps.com、.devshift.org.openshiftusgov.com、和。.devshiftusgov.com在 Route 53 资源上添加、修改或移除标签，用于资源管理和组织。
- tag— 根据 AWS 资源的标签发现和列出资源，这对于识别由 ROSA 管理的资源非常有用。

要查看有关策略的更多详细信息，包括最新版本的 JSON 策略文档，请参阅 ROSASharedVPCRoute53 AWS 托管策略参考指南中的策略。

AWS 托管策略： ROSASharedVPCEndpoint策略

你可以附加ROSASharedVPCEndpointPolicy到你的 IAM 实体。您必须将此策略附加到 IAM 角色才能允许 ROSA 集群 AWS 服务 在共享 VPC 环境中向其他群集进行调用。

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

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— 描述与 VPC 相关的资源（包括 VPC 终端节点）的只读权限 VPCs，以及用于了解网络环境的安全组。创建、删除和修改具有基于标签的限制的安全组，使 ROSA 能够创建和管理集群网络的安全组，同时将操作限制为仅限带有 Rosa 标签的资源。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 AWS 服务 在共享 VPC 环境中创建和管理用于私有连接的 VPC 终端节点。在新创建的 VPC 终端节点和安全组的创建过程中应用标签，以便正确识别和管理资源。

要查看有关策略的更多详细信息，包括最新版本的 JSON 策略文档，请参阅 ROSASharedVPCEndpoint AWS 托管策略参考指南中的策略。

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 所需的操作员策略的详细信息。您可以将这些 AWS 托管策略附加到在 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 托管策略旨在由 ROSA 与托管控制平面 (HCP) 一起使用。ROSA 经典集群使用客户托管 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 托管策略： ROSAAmazonEBSCSIDriverOperatorPolicy

你可以附加`ROSAAmazonEBSCSIDriverOperatorPolicy`到你的 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 向其他角色发出呼叫 AWS 服务。每个集群都需要一组独有的操作员角色。

此策略向 Amazon EBS CSI 驱动程序操作员授予在 ROSA 集群上安装和维护 Amazon EBS CSI 驱动程序所需的权限。有关运算符的更多信息，请参阅 OpenShift GitHub 文档中的aws-ebs-csi-driver 运算符。

权限详细信息

此策略包括以下权限，允许 Amazon EBS 驾驶员操作员完成以下任务：

- `ec2`— 创建、修改、连接、分离和删除连接到 Amazon EC2 实例的 Amazon EBS 卷。创建和删除 Amazon EBS 卷快照并列出 Amazon EC2 实例、卷和快照。

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

AWS 托管策略： ROSAIngressOperatorPolicy

你可以附加`ROSAIngressOperatorPolicy`到你的 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 向其他角色发出呼叫 AWS 服务。每个集群都需要一组独有的操作员角色。

此策略向 Ingress 操作员授予为集群配置和管理负载均衡器和 DNS 配置所需的 ROSA 权限。该策略允许对标签值进行读取访问。然后，操作员筛选 Route 53 资源的标签值以发现托管区域。有关运算符的更多信息，请参阅 OpenShift GitHub 文档中的 OpenShift Ingress Operator。

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`— 列出 Route 53 托管区域并编辑管理由 ROSA 集群控制的 DNS 的记录。
- `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 AWS 托管策略参考指南ROSAIngressOperatorPolicy中的。

AWS 托管策略： ROSAImageRegistryOperatorPolicy

你可以附加`ROSAImageRegistryOperatorPolicy`到你的 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 向其他角色发出呼叫 AWS 服务。每个集群都需要一组独有的操作员角色。

此策略向映像注册表操作员授予为 ROSA 集群内映像注册表和依赖服务（包括 S3）配置和管理资源所需的权限。这是必需的，这样操作员才能安装和维护 ROSA 集群的内部注册表。有关该运算符的更多信息，请参阅 OpenShift GitHub 文档中的图像注册表运算符。

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 AWS 托管策略参考指南ROSAImageRegistryOperatorPolicy中的。

AWS 托管策略： ROSACloudNetworkConfigOperatorPolicy

你可以附加`ROSACloudNetworkConfigOperatorPolicy`到你的 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 向其他角色发出呼叫 AWS 服务。每个集群都需要一组独有的操作员角色。

此策略向 Cloud Network Config Config Config Controller 操作员授予为 ROSA 集群网络覆盖层配置和管理网络资源所需的权限。操作员使用这些权限来管理作为 ROSA 集群一部分的 Amazon EC2 实例的

私有 IP 地址。有关运算符的更多信息，请参阅 OpenShift GitHub 文档loud-network-config-controller 中的 C。

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— 阅读、分配和描述用于连接 ROSA 集群中 Amazon EC2 实例、 Amazon VPC 子网和弹性网络接口的配置。

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

AWS 托管策略： ROSAKubeControllerPolicy

你可以附加ROSAKubeControllerPolicy到你的 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 向其他角色发出呼叫 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，以及具有托管控制平面集群的 ROSA 的 AWS KMS 资源。有关此控制器的更多信息，请参阅 OpenShift 文档中的控制器架构。

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 Amazon EC2 实例安全组并向其添加标签。将入站规则添加到安全组。描述可用区、 Amazon EC2 实例、路由表、安全组和子网。 VPCs
- 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。使用负载均衡器注册和注销 Amazon EC2 实例，并向负载均衡器添加标签。
- kms— 检索有关 AWS KMS 密钥的详细信息。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 AWS 托管策略参考指南ROSAKubeControllerPolicy中的。

AWS 托管策略： ROSANodePoolManagementPolicy

你可以附加ROSANodePoolManagementPolicy到你的 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 调用其他 AWS 服务。每个集群都需要一组独有的操作员角色。

此策略向 NodePool 控制器授予描述、运行和终止作为工作节点管理的 Amazon EC2 实例所需的权限。该策略还授予允许使用 AWS KMS 密钥对工作节点根卷进行磁盘加密、标记连接到工作节点的 elastic network interface 以及访问 Amazon EC2 容量预留的权限。有关此控制器的更多信息，请参阅 OpenShift 文档中的控制器架构。

权限详细信息

此策略包括以下权限，允许 NodePool 控制器完成以下任务：

- ec2— 使用 AMIs 由红帽 AWS 账户 拥有和管理的托管方式运行 Amazon EC2 实例。管理集群中的 EC2 生命周期。 ROSA 使用、、 Elastic Load Balancing Amazon VPC Route 53、 Amazon EBS和动态创建和集成工作节点 Amazon EC2。访问和描述容量预留以支持 ROSA 中的容量预留功能。
- iam— Elastic Load Balancing 通过名AWSServiceRoleForElasticLoadBalancing为的服务相关角色使用。为 Amazon EC2 实例配置文件分配角色。
- kms— 读取 AWS KMS 密钥，创建和管理授权 Amazon EC2，并返回唯一的对称数据密钥以供外部使用。 AWS KMS允许对 Worker 节点根卷进行磁盘加密需要此项。

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

AWS 托管策略： ROSAKMSProvider策略

你可以附加ROSAKMSProviderPolicy到你的 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 向其他角色发出呼叫 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 AWS 加密提供商授予管理支持etcd数据加密的 AWS KMS 密钥所需的权限。此策略 Amazon EC2 允许使用 AWS 加密提供商提供的 KMS 密钥来加密和解密etcd数据。有关此提供商的更多信息，请参阅 Kubernetes GitHub 文档中的AWS 加密提供商。

权限详细信息

此策略包括以下权限，允许 AWS 加密提供商完成以下任务：

- kms— 加密、解密和检索密钥。 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。

要查看完整的 JSON 策略文档，请参阅ROSAKMSProvider《 AWS 托管策略参考指南》中的策略。

AWS 托管策略： ROSAControlPlaneOperatorPolicy

你可以附加ROSAControlPlaneOperatorPolicy到你的 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 向其他角色发出呼叫 AWS 服务。每个集群都需要一组独有的操作员角色。

此策略向控制平面操作员授予管理托管控制平面集群的 ROSA 所需的权限 Amazon EC2 和 Route 53 资源。有关此运算符的更多信息，请参阅 OpenShift 文档中的控制器架构。

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— 列出和更改 Route 53 记录集并列出托管区域。
- 为以下内容添加了标签 RedHatManagedSecurityGroups：允许控制平面操作员在创建后标记红帽管理的安全组。这是正确管理资源生命周期以及清理与 ROSA 和 HCP 群集关联的安全组所必需的。
- 在管理中添加了安全组/* VPCEndpointWithCondition：修复了集群升级期间的 VPCE 协调失败。操作员需要权限才能修改引用安全组的 VPC 终端节点。

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

ROSA AWS 托管策略的更新

查看 ROSA 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。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	ROSA 更新了政策，允许标记红帽管理的安全组以实现适当的资源生命周期管理，并	2026 年 4 月 9 日

更改	描述	日期
	在 Manage 中添加了安全组/*，VPCEndpointWithCondition 以修复集群升级期间的 VPCE 协调失败。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAControlPlaneOperatorPolicy”。	
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 Elastic Load Balancing 权限。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAKubeControllerPolicy”。	2026 年 3 月 5 日
ROSANodePoolManagementPolicy — 政策已更新	ROSA 更新了政策，增加了对 Amazon 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，以改进资源管理。要了解更多信息，请参阅the section called “AWS 托管策略： ROSANodePoolManagementPolicy”。	2025 年 9 月 3 日
ROSASharedVPCEndpoint策略-已添加新政策	ROSA 添加了一项新策略，允许 ROSA 安装程序在共享 VPC 环境中配置 VPC 端点和安全组。该策略提供了为共享 VPC 用例量身定制的 EC2 权限子集。要了解更多信息，请参阅the section called “AWS 托管策略： ROSASharedVPCEndpoint策略”。	2025 年 8 月 7 日

更改	描述	日期
ROSASharedVPCRoute53策略-已添加新政策	ROSA 添加了一项新策略，允许 ROSA 安装程序在共享 VPC 环境中配置 Route 53 记录。该策略提供了为共享 VPC 用例量身定制的 Route 53 权限子集。要了解更多信息，请参阅the section called “AWS 托管策略： ROSASharedVPCRoute53策略”。	2025 年 8 月 7 日
ROSAInstaller政策-政策已更新	ROSA 更新了政策，允许 ROSA 安装程序检查 Amazon 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键匹配`"kubernetes.io/cluster/*"` 来删除子网上的标签，从而改进 Kubernetes 集群标签管理。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAInstaller策略”。	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 ROSA 对 AWS 商业和 GovCloud 区域存储的要求。要了解更多信息，请参阅the section called “AWS 托管策略： 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，允许对连接到工作节点的 elastic network interface 进行标记。要了解更多信息，请参阅the section called “AWS 托管策略： ROSANodePoolManagementPolicy”。	2025 年 5 月 5 日
ROSAImageRegistryOperatorPolicy — 政策已更新	ROSA 更新了政策，允许红帽 OpenShift 图像注册管理运营商在 AWS GovCloud 区域中预配置和管理 Amazon S3 存储桶和对象，供 ROSA 集群内映像注册表使用。此更改满足了 ROSA 对 AWS GovCloud 区域的存储要求。要了解更多信息，请参阅the section called “AWS 托管策略： 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 Rosa 管理的 ECR 存储库中获取镜像，这些镜像是集群安装和工作节点生命周期管理所必需的。要了解更多信息，请参阅the section called “AWS 托管策略： 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，允许仅在请求包含标签的 ec2:RunInstances 调用期间使用与 EC2 实例类似的标签来标记弹性网络接口`red-hat-managed: true` 。这些权限是支持 ROSA 的 HCP 4.17 集群所必需的。要了解更多信息，请参阅the section called “AWS 托管策略： ROSANodePoolManagementPolicy”。	2025 年 2 月 24 日
ROSAAmazonEBSCSIDriverOperatorPolicy — 政策已更新	ROSA 更新了政策以支持新的 Amazon EBS 快照授权 API。要了解更多信息，请参阅the section called “AWS 托管策略： 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 托管策略： ROSANodePoolManagementPolicy”。	2024 年 5 月 2 日

更改	描述	日期
ROSAInstaller政策-政策已更新	ROSA 更新了政策，允许 ROSA 安装程序使用匹配"kubernetes.io/cluster/*" 的标签密钥向子网添加标签。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAInstaller策略”。	2024 年 4 月 24 日
ROSASRESupport政策-政策已更新	ROSA 更新了政策，允许 SRE 角色检索已标记 ROSA 为的实例配置文件的信息red-hat-managed 。要了解更多信息，请参阅the section called “AWS 托管策略： ROSASRESupport策略”。	2024 年 4 月 10 日
ROSAInstaller政策-政策已更新	ROSA 更新了策略，允许 ROSA 安装程序验证的 AWS 托管策略 ROSA 是否已附加到所使用的 IAM 角色 ROSA。此更新还允许安装程序识别客户托管策略是否已附加到 ROSA 角色。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAInstaller策略”。	2024 年 4 月 10 日

更改	描述	日期
ROSAInstaller政策-政策已更新	ROSA 更新了政策，允许该服务在由于缺少客户指定的集群 OIDC 提供程序而导致集群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 名称服务器，从而使集群配置操作具有等性。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAInstaller策略”。	2024 年 1 月 26 日
ROSASRESupport政策-政策已更新	ROSA 更新了政策，允许该服务使用 DescribeSecurityGroups API 对安全组执行读取操作。要了解更多信息，请参阅the section called “AWS 托管策略： ROSASRESupport策略”。	2024 年 1 月 22 日
ROSAImageRegistryOperatorPolicy — 政策已更新	ROSA 更新了政策，允许图像注册管理运营商对名称为 14 个字符的区域中的 Amazon S3 存储桶采取操作。要了解更多信息，请参阅the section called “AWS 托管策略： 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， kube-controller-manager允许描述可用区、 Amazon EC2 实例、路由表、安全组和子网。 VPCs 要了解更多信息，请参阅the section called “AWS 托管策略： ROSAKubeControllerPolicy”。	2023 年 10 月 16 日
ROSAManage订阅-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 托管策略： ROSAManage订阅”。	2023 年 8 月 1 日
ROSAKubeControllerPolicy — 政策已更新	ROSA 更新了政策，允许创建网络负载均衡器作为 Kubernetes 服务负载均衡器。kube-controller-manager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 托管策略： ROSAKubeControllerPolicy”。	2023 年 7 月 13 日

更改	描述	日期
ROSANodePoolManagementPolicy — 添加了新政策	ROSA 添加了一个新策略，允许 NodePool 控制器描述、运行和终止作为工作节点管理的 Amazon EC2 实例。此策略还允许使用密 AWS KMS 钥对工作节点根卷进行磁盘加密。要了解更多信息，请参阅the section called “AWS 托管策略： ROSANodePoolManagementPolicy”。	2023 年 6 月 8 日
ROSAInstaller策略-已添加新政策	ROSA 添加了一项新策略，允许安装程序管理支持群集安装的 AWS 资源。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAInstaller策略”。	2023 年 6 月 6 日
ROSASRESupport策略-已添加新政策	ROSA 添加了一项新政策，允许红帽 SREs 直接观察、诊断和支持与 ROSA 集群相关的 AWS 资源，包括更改 ROSA 群集节点状态的能力。要了解更多信息，请参阅the section called “AWS 托管策略： ROSASRESupport策略”。	2023 年 6 月 1 日
ROSAKMSProvider策略-已添加新政策	ROSA 添加了一项新策略，允许内置 AWS 加密提供商管理支持 etcd 数据加密的 AWS KMS 密钥。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAKMSProvider策略”。	2023 年 4 月 27 日

更改	描述	日期
ROSAKubeControllerPolicy — 添加了新政策	ROSA 添加了一项新策略，允许 kube 控制器管理托管控制平面集群的 Amazon EC2 Elastic Load Balancing ROSA 、和 AWS KMS 资源。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAKubeControllerPolicy”。	2023 年 4 月 27 日
ROSAImageRegistryOperatorPolicy — 添加了新政策	ROSA 添加了一项新策略，允许图像注册管理器操作员为 ROSA 集群内映像注册表和依赖服务（包括 S3）配置和管理资源。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAImageRegistryOperatorPolicy”。	2023 年 4 月 27 日
ROSAControlPlaneOperatorPolicy — 添加了新政策	ROSA 添加了一项新政策，允许控制平面操作员对托管的控制平面集群 ROSA 进行 Amazon EC2 管理和 Route 53 资源。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAControlPlaneOperatorPolicy”。	2023 年 4 月 24 日

更改	描述	日期
ROSACloudNetworkConfigOperatorPolicy — 添加了新政策	ROSA 添加了一项新政策，允许 Cloud Network Config Config Controller 操作员为 ROSA 集群网络覆盖层配置和管理网络资源。要了解更多信息，请参阅the section called “AWS 托管策略： 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 Ingress 运营商为集群配置和管理负载均衡器和 DNS 配置。 ROSA 要了解更多信息，请参阅the section called “AWS 托管策略： ROSAIngressOperatorPolicy”。	2023 年 4 月 20 日
ROSAAmazonEBSCSIDriverOperatorPolicy — 添加了新政策	ROSA 添加了一项新政策，允许 Amazon EBS CSI 驱动程序操作员在 ROSA 集群上安装和维护 Amazon EBS CSI 驱动程序。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAAmazonEBSCSIDriverOperatorPolicy”。	2023 年 4 月 20 日
ROSAWorkerInstancePolicy — 添加了新政策	ROSA 添加了一个新策略以允许该服务管理群集资源。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAWorkerInstancePolicy”。	2023 年 4 月 20 日

更改	描述	日期
ROSAManage订阅-已添加新政策	ROSA 添加了一项新策略来授予管理 ROSA 订阅所需的 AWS Marketplace 权限。要了解更多信息，请参阅the section called “AWS 托管策略： ROSAManage订阅”。	2022 年 4 月 11 日
AWS 云端 Red Hat OpenShift 服务 开始跟踪更改	AWS 云端 Red Hat OpenShift 服务 开始跟踪其 AWS 托管策略的更改。	2022 年 3 月 2 日

对 ROSA 身份和访问进行故障排除

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

AWS Organizations 服务控制策略拒绝所需的 AWS Marketplace 权限

如果您的 AWS Organizations 服务控制策略 (SCP) 在您尝试启用时不允许所需的 AWS Marketplace 订阅权限 ROSA，则会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。您的管理员是管理您组织帐户的人。要求该人执行以下操作：

1. 将 SCP 配置为允许`aws-marketplace:Subscribe`、`aws-marketplace:Unsubscribe`、和`aws-marketplace:ViewSubscriptions`权限。有关更多信息，请参阅 AWS Organizations 用户指南中的更新 SCP。
2. ROSA 在组织的管理账户中启用。
3. 在组织内共享需要访问权限的成员账户的 ROSA 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。

用户或角色没有所需的 AWS Marketplace 权限

如果您尝试启用时您的 IAM 委托人没有所需的 AWS Marketplace 订阅权限 ROSA，则会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，将 AWS 托管策略附加ROSAManageSubscription到您的 IAM 身份。有关更多信息，请参ROSAManage阅《 AWS 托管策略参考指南》中的订阅。
2. 按照the section called “启用 ROSA 和配置 AWS 先决条件”中的程序操作。

如果您无权查看或更新您的权限集， IAM 或者收到错误消息，则必须联系管理员寻求帮助。请该人附上您的ROSAManageSubscription身 IAM 份，然后按照中的步骤进行操作the section called “启用 ROSA 和配置 AWS 先决条件”。当管理员执行此操作时，它会 ROSA 通过更新下所有 IAM 身份的权限集来启用 AWS 账户。

管理员屏蔽了所需的 AWS Marketplace 权限

如果您的账户管理员屏蔽了所需的 AWS Marketplace 订阅权限，则在您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，将 AWS 托管策略附加ROSAManageSubscription到您的 IAM 身份。有关更多信息，请参ROSAManage阅《 AWS 托管策略参考指南》中的订阅。
2. 按照中的步骤启the section called “启用 ROSA 和配置 AWS 先决条件”用 ROSA。此过程 ROSA 通过更新下所有 IAM 身份的权限集来启用 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，则您的账户中可能不存在AWSServiceRoleForElasticLoadBalacing服务相关角色。如果您尝试创建账户中 ROSA 集群没有该AWSServiceRoleForElasticLoadBalacing角色的，则会出现以下错误。

```
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 Elastic Load Balancing 用户指南中创建服务相关角色中的说明创建角色。

韧性在 ROSA

AWS 全球基础设施弹性

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理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 AWS 可用区或跨多个可用区运行 Kubernetes 控制平面和数据平面的选项。虽然单可用区集群可用于实验，但我们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 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

ROSA 集群弹性

ROSA 控制平面由至少三个 OpenShift 控制平面节点组成。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。

ROSA 数据平面由至少两个 OpenShift 基础架构节点和两个 OpenShift 工作节点组成。基础设施节点运行的 pod 支持 OpenShift 集群基础设施组件，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。

红帽站点可靠性工程师 (SREs) 全面管理控制平面和基础架构节点。红帽会 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设施节点。有关更多信息，请参阅 the section called “责任”。

> **Important**
>
> 由于 ROSA 是一项托管服务，因此红帽负责管理所 ROSA 使用的底层 AWS 基础架构。客户不应尝试通过 AWS 控制台或手动关闭 ROSA 使用的 Amazon EC2 实例 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。

客户部署的应用程序恢复能力

尽管 ROSA 提供了许多保护措施来确保服务的高可用性，但客户有责任构建其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 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅安全支柱中的基础设施保护 — Well-Architecte AWS d Framew ork。

您可以使用 AWS 已发布的 API 调用 ROSA 通过 AWS 网络进行访问。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，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 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

红帽站点可靠性工程师 (SREs) 负责集群和底层应用平台的持续管理和网络安全。有关红帽责任的更多信息 ROSA，请参阅the section called “责任”。

创建新集群时， ROSA 可以选择创建公共 Kubernetes API 服务器端点和应用程序路由，或者创建私有 Kubernetes API 终端节点和应用程序路由。此连接用于与您的集群通信（使用 ROSA CLI 和 OpenShift CLI 等 OpenShift 管理工具）。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 VPC 并将该 VPC AWS PrivateLink 连接到 OpenShift 后端服务。

Kubernetes API 服务器访问是使用 AWS Identity and Access Management (IAM) 和原生 Kubernetes 基于角色的访问控制 (RBAC) 的组合来保护的。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 终止创建安全的应用程序路由，为客户端提供证书。有关更多信息，请参阅 Red Hat 文档中的安全路由。

如果您在现有 VPC 中创建 ROSA 集群，则需要为集群指定要使用的 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 为要部署集群的每个可用区配置公有子网和私有子网。对于使用私有 API 端点的集群，只需要私有子网。

如果您使用的是现有 VPC，则可以将 ROSA 集群配置为在集群创建期间或之后使用 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保护。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 ROSA 集群中 Pod 的流量。

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

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 Management Console。

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

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”。

获得 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 案子

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 Support 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	更新了 AWS 托管策略，ROSAControlPlaneOperatorPolicy 允许标记 Red Hat 管理的安全组以实现适当的资源生命周期管理，并将安全组/* 添加到 Manage VPCEndpoint WithCondition 以修复集群升级期间的 VPCE 协调失败。有关更多信息，请参阅AWS 托管策略的ROSA 更新。	2026 年 4 月 9 日
已更新 ROSAKubeControllerPolicy	更新了 AWS 托管策略，明确了 ROSAKubeControllerPolicy 向目标组注册和注销目标的 Elastic Load Balancing 权限。有关更多信息，请参阅AWS 托管策略的ROSA 更新。	2026 年 3 月 5 日
已更新 ROSANodePoolManagementPolicy	ROSA 已更新托管策略`ROSANodePoolManagementPolicy` 以添加容量预留的资源访问权限以支持容量预留功能。有关信息，请参阅AWS 托管策略的ROSA 更新。	2025 年 9 月 3 日
更新后的 ROSAInstaller政策	更新了 AWS 托管策略 ROSAInstaller策略以支持 ROSA 中的新容量预留功能并改进 Kubernetes 集群标签管	2025 年 8 月 7 日

	理。有关信息，请参阅AWS 托管策略的ROSA 更新。	
新 ROSASharedVPCRoute53 政策	ROSA 发布了一项新的托管策略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，请参阅AWS 托管策略的ROSA 更新。	2025 年 8 月 7 日
新 ROSASharedVPCEndpoint 政策	ROSA 发布了一项新的托管策略ROSASharedVPCEndpointPolicy ，允许 ROSA 安装程序在共享 VPC 环境中配置 VPC 端点和安全组。该策略提供了为共享 VPC 用例量身定制的 EC2 权限子集。有关信息，请参阅AWS 托管策略的 ROSA 更新。	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 通过 HCP AWS 区域扩展	带有托管控制平面 (HCP) 的 ROSA 现已在中东（阿联酋）上市 AWS 区域。	2024 年 5 月 13 日
ROSA 通过 HCP AWS 区域扩展	带有托管控制平面 (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 通过 HCP AWS 区域扩展	带有托管控制平面 (HCP) 的 ROSA 现已在欧洲（西班牙）上市 AWS 区域。	2024 年 4 月 29 日
更新后的 ROSAInstaller政策	更新了 AWS 托管策略 ROSAInstaller策略。	2024 年 4 月 24 日
ROSA 通过 HCP AWS 区域扩展	带有托管控制平面 (HCP) 的 ROSA 现已在欧洲（苏黎世）上市 AWS 区域。	2024 年 4 月 19 日
ROSA 通过 HCP AWS 区域扩展	带有托管控制平面 (HCP) 的 ROSA 现已在亚太地区（大阪）上市 AWS 区域。	2024 年 4 月 17 日
更新的 ROSAInstaller政策和 ROSASRESupport政策	更新了 AWS 托管策略 ROSAInstaller策略和 ROSASRESupport策略。	2024 年 4 月 10 日

ROSA 通过 HCP AWS 区域 扩展	带有托管控制平面 (HCP) 的 ROSA 现已在亚太地区（香港 AWS 区域）上市。	2024 年 4 月 8 日
ROSA 通过 HCP AWS 区域 扩展	带有托管控制平面 (HCP) 的 ROSA 现已在南美洲（圣保罗）上市 AWS 区域。	2024 年 4 月 1 日
ROSA 通过 HCP AWS 区域 扩展	带有托管控制平面 (HCP) 的 ROSA 现已在中东（巴林 AWS 区域）上市。	2024 年 3 月 25 日
ROSA 通过 HCP AWS 区域 扩展	带有托管控制平面 (HCP) 的 ROSA 现已在亚太地区（首尔）上市 AWS 区域。	2024 年 3 月 14 日
ROSA 通过 HCP AWS 区域 扩展	带有托管控制平面 (HCP) 的 ROSA 现已在非洲（开普敦）上市 AWS 区域。	2024 年 3 月 5 日
更新后的 ROSAInstaller政策	更新了 AWS 托管策略 ROSAInstaller策略。	2024 年 1 月 26 日
更新后的 ROSASRESupport政策	更新了 AWS 托管策略 ROSASRESupport策略。	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
更新的 ROSAManage订阅	更新了 AWS 托管策略 ROSAManage订阅。	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 ROSANode PoolManagementPolicy	添加 AWS ROSANodePoolManagementPolicy 了新的托管策略。	2023 年 6 月 8 日
添加了新的 AWS 托管策略 ROSAInstaller策略	添加 AWS 了新的托管 ROSAInstaller策略策略。	2023 年 6 月 6 日
添加了新的 AWS 托管策略 ROSASRESupport策略	添加 AWS 了新的托管 ROSASRESupport策略策略。	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
更新了什么是 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
为 ROSA 操作员角色添加了新的 AWS 托管策略	添加 AWS 了新的托管 ROSAKMSProvider策略 ROSAImageRegistryOperatorPolicy和策略。 ROSAKube ControllerPolicy	2023 年 4 月 27 日
添加了新的 AWS 托管策略 ROSAControl PlaneOperatorPolicy	添加 AWS ROSAControlPlaneOperatorPolicy 了新的托管策略。	2023 年 4 月 24 日
为 ROSA 账户角色添加了新的 AWS 托管策略	添加了 ROSA 账户和操作员角色页面的新 AWS 托管策略页面。	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	已添加疑难解答页面。	2022 年 11 月 1 日

添加了开始使用页面	已添加入门页面。	2022 年 8 月 12 日
添加了新的 AWS 托管策略 ROSAManage订阅	添加 AWS 了新的托管策略 ROSAManage订阅。	2022 年 4 月 11 日
初始版本	《 AWS 云端 Red Hat OpenShift 服务 用户指南》的初始版本。	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。