Red Hat OpenShift Service on AWS 4

ROSA 简介

Red Hat OpenShift Service on AWS 架构概述

Last Updated: 2024-07-03

Red Hat OpenShift Service on AWS 4 ROSA 简介

Red Hat OpenShift Service on AWS 架构概述

法律通告

摘要

本文档介绍了 Red Hat OpenShift Service on AWS (ROSA) 中的平台和应用程序架构。

目录

第 1 章 了解 ROSA

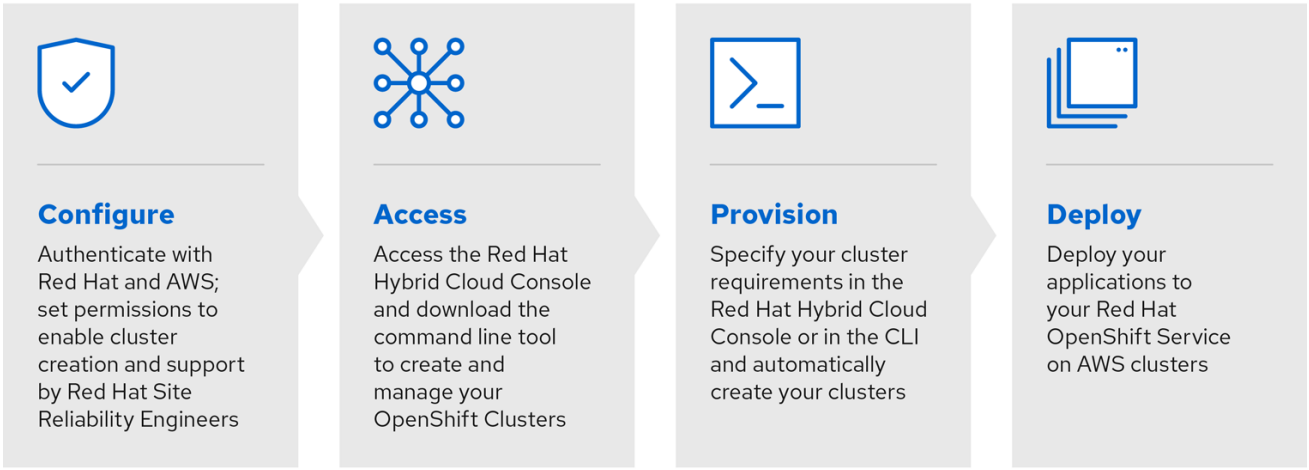
了解 Red Hat OpenShift Service on AWS (ROSA)，使用 Red Hat OpenShift Cluster Manager 和命令行界面(CLI)工具、消费体验以及与 Amazon Web Services (AWS)服务集成。

1.1. 关于 ROSA

ROSA 是一个完全被管理的应用平台，它使您可以专注于通过构建和部署应用程序来为客户创造价值。红帽站点可靠性工程(SRE)专家管理底层平台，因此您不必担心基础架构管理的复杂性。ROSA 提供与 Amazon CloudWatch、AWS Identity and Access Management (IAM)、Amazon Virtual Private Cloud (VPC)和各种额外 AWS 服务的无缝集成，以进一步加快为客户构建和交付不同体验。

您直接从 AWS 帐户订阅该服务。创建集群后，您可以使用 OpenShift Web 控制台、ROSA CLI 或 Red Hat OpenShift Cluster Manager 来运行集群。

您将使用新版本的新功能和共享源接收 OpenShift 更新，以便与 OpenShift Container Platform 保持一致。ROSA 支持与 Red Hat OpenShift Dedicated 和 OpenShift Container Platform 相同的 OpenShift 版本，以实现版本一致性。



有关 ROSA 安装的更多信息，请参阅在 AWS (ROSA)上安装 Red Hat OpenShift Service 。

1.2. 账单和定价

Red Hat OpenShift Service on AWS 会直接指向 Amazon Web Services (AWS)帐户。ROSA 定价基于使用，每年承诺或 3 年的承诺以便获得更大的折现。ROSA 的总成本由两个部分组成：

- ROSA 服务费用
- AWS 基础架构费用

如需更多详细信息，请访问 AWS 网站上的 Red Hat OpenShift Service on AWS 定价 页面。

1.3. 开始使用

要开始部署集群，请确保您的 AWS 帐户已满足先决条件，您有红帽帐户就绪，并按照 AWS 上开始使用 Red Hat OpenShift Service 中所述的步骤进行操作。

其他资源

- OpenShift Cluster Manager
- 关于使用 STS 的 ROSA 集群的 IAM 资源
- Getting started with Red Hat OpenShift Service on AWS
- AWS 定价页面

第 2 章 策略和服务定义

2.1. 关于 AWS 上的 RED HAT OPENSHIFT SERVICE 的可用性

可用性和灾难性对于任何应用平台至关重要。虽然 Red Hat OpenShift Service on AWS (ROSA) 在多个级别上提供很多保护措施，但必须为高可用性配置客户部署的应用程序。要考虑云提供商可能出现的中断，比如在多个可用区间部署集群并使用故障转移机制维护多个集群。

2.1.1. 潜在的故障点

Red Hat OpenShift Service on AWS (ROSA) 提供了多种功能，用于保护工作负载停机，但必须正确设计应用程序才能利用这些功能。

ROSA 通过添加红帽站点可靠性工程(SRE)支持以及部署多个可用区集群的选项，但可以通过多种方式使容器或基础架构仍失败的方法进一步保护。通过了解潜在的故障点，您可以了解应用程序和集群在各个特定级别上具有弹性的风险，并适当地进行架构。

注意

中断可能会在多个不同的基础架构和集群组件中发生。

2.1.1.1. 容器或 pod 失败

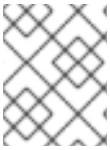
按照设计，Pod 将在短时间内存在。适当扩展服务，以便运行您的应用程序 pod 的多个实例可能会防止出现单个 pod 或容器的问题。OpenShift 节点调度程序还可确保这些工作负载在不同的 worker 节点上分布，以进一步提高弹性。

在考虑可能的 pod 故障时，了解存储如何附加到应用程序上非常重要。连接到单个 pod 的单个持久性卷无法利用 pod 扩展的完整优点，而复制的数据库、数据库服务或共享存储可以：

为了避免在计划维护（如升级）期间中断应用程序，定义 Pod Disruption Budget 非常重要。这些是 Kubernetes API 的一部分，可通过其他对象类型等 **oc** 命令进行管理。它们允许在操作过程中指定 pod 的安全约束，比如为维护而清空节点。

2.1.1.2. Worker 节点失败

Worker 节点是包含应用程序 pod 的虚拟机。默认情况下，ROSA 集群最少有两个 worker 节点用于单个可用区集群。如果 worker 节点失败，pod 会重新定位到可正常工作的 worker 节点，只要有足够的容量，直到现有节点出现任何问题解决或节点被替换。更多 worker 节点意味着可以更好地保护单节点停机，并确保在出现节点失败时重新调度 pod 容量。



注意

当对可能的节点故障进行核算时，了解存储如何影响程度也很重要。EFS 卷不受节点故障的影响。但是，如果 EBS 卷连接到失败的节点，则无法访问它。

2.1.1.3. 集群故障

单AZ ROSA 集群在专用子网中至少有三个 control plane 和两个基础架构节点。

根据您选择的集群类型，multi-AZ ROSA 集群至少有三个 control plane 节点，以及为高可用性（在一个区或多个区中）预先配置的三个基础架构节点。control plane 和基础架构节点具有与 worker 节点相同的弹性，并添加了由红帽完全管理的好处。

如果出现 control plane 完全中断的问题，OpenShift API 将无法正常工作，现有的 worker 节点 pod 不受影响。但是，如果同时存在 pod 或节点停机，则 control plane 必须先恢复，然后才能添加新 pod 或节点。

在基础架构节点上运行的所有服务都由红帽配置为高度可用，并分布到基础架构节点。如果出现完整的基础架构中断，则这些服务将不可用，直到节点恢复为止。

2.1.1.4. 区失败

AWS 的区故障会影响所有虚拟组件，如 worker 节点、块存储或共享存储以及特定于单个可用区的负载均衡器。为防止区故障，ROSA 为在三个可用区（称为多可用区）的集群提供选项。只要有足够的容量，在停机停机时将现有无状态工作负载重新分发到不受影响的区域。

2.1.1.5. 存储故障

如果您部署了有状态应用程序，则存储是一个关键组件，在考虑高可用性时必须考虑这一点。单个块存储 PV 无法发生中断，即使在 pod 级别上也是如此。维护存储的最佳方式是使用复制存储解决方案、不受中断影响的共享存储或独立于集群的数据库服务。

2.2. AWS 上的 RED HAT OPENSHIFT SERVICE 职责概述

本文档概述 Red Hat、Amazon Web Services (AWS)以及 Red Hat OpenShift Service on AWS (ROSA)托管服务的客户职责。

2.2.1. AWS 上的 Red Hat OpenShift Service 共享职责

虽然红帽和 Amazon Web Services (AWS)管理 Red Hat OpenShift Service on AWS 服务，但客户共享某些职责。Red Hat OpenShift Service on AWS 服务可远程访问，托管在公有云资源上，在客户拥有的 AWS 帐户中创建，并具有由红帽拥有的底层平台和数据安全性。

重要

如果已将 **cluster-admin** 角色添加到用户，请参阅 Red Hat Enterprise Agreement 附录 4（在线订阅服务） 中的职责和排除备注。

资源	事件和操作管理	变更管理	访问和身份授权	安全和合规性	灾难恢复
客户数据	客户	客户	客户	客户	客户
客户应用程序	客户	客户	客户	客户	客户
开发人员服务	客户	客户	客户	客户	客户
平台监控	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
日志记录	Red Hat	红帽和客户	红帽和客户	红帽和客户	Red Hat
应用程序网络	红帽和客户	红帽和客户	红帽和客户	Red Hat	Red Hat

资源	事件和操作管理	变更管理	访问和身份授权	安全和合规性	灾难恢复
集群网络	Red Hat	红帽和客户	红帽和客户	Red Hat	Red Hat
虚拟网络管理	红帽和客户	红帽和客户	红帽和客户	红帽和客户	红帽和客户
虚拟计算管理 (control plane、基础架构和 worker 节点)	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
集群版本	Red Hat	红帽和客户	Red Hat	Red Hat	Red Hat
容量管理	Red Hat	红帽和客户	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 全局基础架构	AWS	AWS	AWS	AWS	AWS

2.2.2. 按区域共享职责的任务

Red Hat、AWS 和客户都对 Red Hat OpenShift Service on AWS (ROSA)集群的监控、维护和总体健康状况共享责任。本文档演示了每个列出资源的职责，如下表所示。

2.2.3. 检查和操作集群通知

集群通知是有关集群状态、健康或性能的信息。

集群通知是 Red Hat Site Reliability Engineering (SRE)与您有关受管集群健康状况的主要方法。SRE 也可能使用集群通知来提示您执行操作，以解决或防止集群出现问题。

集群所有者和管理员必须定期检查和操作集群通知，以确保集群保持健康且受支持。

您可以在集群的 **Cluster history** 选项卡中查看 Red Hat Hybrid Cloud Console 中的集群通知。默认情况下，只有集群所有者接收集群通知作为电子邮件。如果其他用户需要接收集群通知电子邮件，请将每个用户添加为集群的通知联系人。

2.2.3.1. 集群通知策略

集群通知旨在让您了解集群的健康状况以及影响它的高影响事件。

大多数集群通知都会自动生成并自动发送，以确保您立即了解集群状态的问题或重要更改。

在某些情况下，Red Hat Site Reliability Engineering (SRE)创建并发送集群通知，以便为复杂的问题提供额外的上下文和指导。

集群通知不会针对低影响的事件、低风险安全更新、日常操作和维护，或由 SRE 快速解决的临时问题发送。

红帽服务在以下情况下自动发送通知：

- 远程健康监控或环境验证检查会检测集群中的问题，例如当 worker 节点有低磁盘空间时。
- 大量的集群生命周期事件（例如调度维护或升级时），或者集群操作会受到事件的影响，但不需要客户干预。
- 大量的集群管理更改，例如，当集群所有权或管理控制从一个用户转移到另一个用户时。
- 您的集群订阅会被更改或更新，例如，当红帽对集群进行订阅条款或功能的更新时。

SRE 在以下情况下创建和发送通知：

- 事件会导致降级或中断会影响集群的可用性或性能，例如，您的云供应商有区域中断。SRE 发送后续通知以告知您事件解析进度以及事件被解决的时间。
- 集群中检测到安全漏洞、安全漏洞或异常活动。
- 红帽检测到您所做的更改正在创建，或可能会导致集群不稳定。
- 红帽检测到您的工作负载会导致集群中的性能下降或不稳定。

2.2.4. 事件和操作管理

红帽负责查看默认平台网络所需的服务组件。AWS 负责保护运行 AWS 云中提供的所有服务的硬件基础架构。客户负责客户应用程序数据的事件和操作管理，以及客户为集群网络或虚拟网络配置的任何自定义网络。

资源	服务职责	客户职责
应用程序网络	**Red Hat** ● 监控原生 OpenShift 路由器服务，并响应警报。	● 监控应用程序路由的健康状况，以及其后面的端点。 ● 向红帽和 AWS 报告停机。

资源	服务职责	客户职责
虚拟网络管理	**Red Hat** ● 监控默认平台网络所需的 AWS 负载均衡器、Amazon VPC 子网和 AWS 服务组件。响应警报。	● 监控 AWS 负载均衡器端点的健康状况。 ● 监控可选通过 Amazon VPC-to-VPC 连接、AWS VPN 连接或 AWS Direct Connect 配置的网络流量，以了解潜在的问题或安全威胁。
虚拟存储管理	**Red Hat** ● 监控附加到集群节点的 Amazon EBS 卷，以及用于 ROSA 服务内置容器镜像 registry 的 Amazon S3 存储桶。响应警报。	● 监控应用数据的健康状况。 ● 如果使用客户管理的 AWS KMS 密钥，请为 Amazon EBS 加密创建和控制密钥生命周期和密钥策略。
平台监控	**Red Hat** ● 维护所有 ROSA 集群组件、站点可靠性工程师(SRE)服务和底层 AWS 帐户的集中式监控和警报系统。	
事件管理	**Red Hat** ● 创建和管理已知事件。 ● 与客户共享根本原因分析(RCA)草案。	● 通过支持问题单引发已知事件。
基础架构和数据弹性	**Red Hat** ● 没有红帽提供的用于带有 STS 的 ROSA 集群的备份方法。 ● 红帽不提交任何恢复点目标(RPO)或恢复时间目标(RTO)。	● 定期备份数据并部署带有 Kubernetes 最佳实践工作负载的 Multi-AZ 集群，以确保区域内的高可用性。 ● 如果整个云区域不可用，请在不同的区域安装新集群并使用备份数据恢复应用程序。
集群容量	**Red Hat** ● 管理集群中所有 control plane 和基础架构节点的容量。 ● 在升级过程中评估集群容量，并响应集群警报。	

资源	服务职责	客户职责
AWS 软件（公共 AWS 服务）	**AWS** • 有关 AWS 事件 和操作管理的信息，请参阅 AWS 中的如何保持操作弹性和服务的连续性。	• 监控客户帐户中 AWS 资源的运行状况。 • 使用 IAM 工具将适当的权限应用到客户账户中的 AWS 资源。
硬件/AWS 全局基础架构	**AWS** • 有关 AWS 事件 和操作管理的信息，请参阅 AWS 中的如何保持操作弹性和服务的连续性。	• 配置、管理和监控客户应用程序和数据，以确保正确强制实施应用程序和数据安全控制。

2.2.4.1. 平台监控

平台审计日志安全转发到集中式安全信息和事件监控 (SIEM) 系统，其中可能会触发 SRE 团队配置的警报，也可以手动查看。审计日志保留在 SIEM 系统中一年。当集群被删除时，给定集群的审计日志不会被删除。

2.2.4.2. 事件管理

事件是导致一个或多个红帽服务降级或中断的事件。事件可以由客户或客户体验与参与(CEE)成员通过支持问题单、直接由集中式监控和警报系统或由 SRE 团队的成员直接提升。

根据服务和客户的影响，事件会按照严重性进行分级。

在管理新事件时，红帽使用以下常规工作流：

1. SRE 第一次响应器会警告新的事件，并开始进行初始调查。
2. 在初始调查后，会为事件分配一个事件，领导事件协调恢复工作。
3. 事件线索管理关于恢复的所有通信和协调，包括相关的通知和支持问题单更新。
4. 事件已被恢复。
5. 其事件被记录，一个根本原因分析 (RCA) 在事件的 5 个工作日内进行。
6. 在事件 7 个工作日内将与客户共享 RCA 草案。

红帽还协助客户在支持问题单中引发的事件。红帽可以帮助活动，包括但不限于：

- Forensic 收集，包括隔离虚拟计算
- 指导计算镜像集合
- 提供收集的审计日志

2.2.4.3. 集群容量

集群升级对容量的影响会被评估为升级测试过程的一部分，以确保对集群的新添加添加的负面影响。在集群升级过程中，添加了额外的 worker 节点，以确保在升级过程中保留集群的总容量。

红帽 SRE 员工的容量评估也会在特定时间段内超过使用量阈值后对集群发出的警报。这些警报也可以产生给客户的通知。

2.2.5. 变更管理

本节论述了如何管理集群和配置更改、补丁和发行版本策略。

红帽负责启用客户控制的集群基础架构和服务，以及维护 control plane 节点、基础架构节点和服务以及 worker 节点的版本。AWS 负责保护运行 AWS 云中提供的所有服务的硬件基础架构。客户负责启动基础架构更改请求，并在集群中安装和维护可选服务和网络配置，以及客户数据和客户应用程序的所有更改。

2.2.5.1. 客户发起的更改

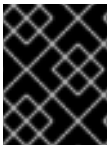
您可以使用自助服务功能（如集群部署、worker 节点扩展或集群删除）启动更改。

更改历史记录在 OpenShift Cluster Manager **Overview** 选项卡中的 **Cluster History** 部分中捕获，供您查看。更改历史记录包括但不仅限于，日志来自以下变化：

- 添加或删除身份提供程序
- 在 **dedicated-admins** 组中添加或移除用户
- 扩展集群计算节点
- 扩展集群负载均衡器
- 扩展集群持久性存储
- 升级集群

您可以通过避免以下组件的 OpenShift Cluster Manager 中的更改来实现维护排除：

- 删除集群
- 添加、修改或删除身份提供程序
- 从提升的组中添加、修改或删除用户
- 安装或删除附加组件
- 修改集群网络配置
- 添加、修改或删除机器池
- 启用或禁用用户工作负载监控
- 启动升级



重要

要强制实施维护排除，请确保禁用了机器池自动扩展或自动升级策略。在维护排除后，根据需要继续启用机器池自动扩展或自动升级策略。

2.2.5.2. 红帽发起的更改

红帽站点可靠性工程(SRE)使用 GitOps 工作流管理 Red Hat OpenShift Service 上的基础架构、代码和配置，并完全自动化的 CI/CD 管道。此过程可确保红帽可以持续地引入服务改进，而不影响客户。

每次建议的更改都会在检查后立即执行一系列自动验证。然后将更改部署到临时环境，在其中进行自动集成测试。最后，更改会部署到生产环境。每个步骤都完全自动化。

授权的 SRE 审查程序必须为每个步骤批准改进。建议者不能与提议更改的单独人员相同。所有更改和批准均作为 GitOps 工作流的一部分完全可审核。

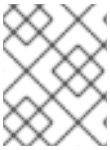
使用功能标记逐步将某些更改发布到生产环境，以控制新功能对指定集群或客户的可用性。

2.2.5.3. 补丁管理

OpenShift Container Platform 软件和底层不可变 Red Hat CoreOS (RHCOS)操作系统镜像对常规 z-stream 升级过程中的漏洞和漏洞进行补丁。在 OpenShift Container Platform 文档中了解更多有关 RHCOS 架构 的信息。

2.2.5.4. 发行管理

红帽不会自动升级集群。您可以使用 OpenShift Cluster Manager Web 控制台调度定期升级集群（周期性升级），或使用 OpenShift Cluster Manager web 控制台调度一次（计算升级）一次。只有在集群受严重影响 CVE 影响时，红帽才会强制将集群升级到新的 z-stream 版本。



注意

因为需要的权限可以在 y-stream 版本之间更改，所以可能需要更新策略，然后才能执行升级。因此，您无法使用 STS 在 ROSA 集群上调度重复升级。

您可以在 OpenShift Cluster Manager web 控制台中查看所有集群升级事件的历史记录。有关发行版本的更多信息，请参阅生命周期策略。

资源	服务职责	客户职责
日志记录	**Red Hat** • 集中聚合和监控平台审计日志。 • 提供和维护日志记录 Operator，使客户能够为默认应用程序日志部署日志记录堆栈。 • 根据客户请求提供审计日志。	• 在集群上安装可选的默认应用程序日志 Operator。 • 安装、配置和维护任何可选应用程序日志记录解决方案，如日志记录 sidecar 容器或第三方日志记录应用程序。 • 如果客户应用程序正在影响日志记录堆栈或集群的稳定性，调整应用程序日志的大小和频率。 • 通过支持问题单中研究特定事件请求平台审计日志。

资源	服务职责	客户职责
应用程序网络	**Red Hat** ● 设置公共负载均衡器。提供在需要时设置私有负载均衡器以及一个额外的负载均衡器的功能。 ● 设置原生 OpenShift 路由器服务。提供将路由器设置为私有的功能，并添加到额外的路由器分片。 ● 为默认内部 pod 流量安装、配置和维护 OpenShift SDN 组件（用于版本 4.11 之前创建的集群）。 ● 提供客户管理 **NetworkPolicy** 和 **EgressNetworkPolicy**（防火墙）对象的功能。	● 使用 **NetworkPolicy** 对象为项目和 pod 网络、pod 入口和 pod 出口配置非默认 pod 网络权限。 ● 使用 OpenShift Cluster Manager 为默认应用程序路由请求专用负载均衡器。 ● 使用 OpenShift Cluster Manager 将最多配置额外的公共或私有路由器分片和对应的负载均衡器。 ● 针对特定服务请求并配置任何其他服务负载均衡器。 ● 配置任何必要的 DNS 转发规则。
集群网络	**Red Hat** ● 设置集群管理组件，如公共或私有服务端点，以及与 Amazon VPC 组件集成的必要。 ● 设置 worker、基础架构和 control plane 节点之间内部集群通信所需的内部网络组件。	● 在置备集群时通过 OpenShift Cluster Manager 为机器 CIDR、服务 CIDR 和 pod CIDR 提供可选非默认 IP 地址范围。 ● 请求在创建集群时或通过 OpenShift Cluster Manager 创建集群或之后的 API 服务端点公开或私有。
虚拟网络管理	**Red Hat** ● 设置并配置置备集群所需的 Amazon VPC 组件，如子网、负载均衡器、互联网网关和 NAT 网关。 ● 为客户提供通过 OpenShift Cluster Manager 所需的与内部资源、Amazon VPC-to-VPC 连接和 AWS Direct Connect 的 AWS VPN 连接的功能。 ● 使客户能够创建和部署 AWS 负载均衡器以用于服务负载均衡器。	● 设置和维护可选的 Amazon VPC 组件，如 Amazon VPC-to-VPC 连接、AWS VPN 连接或 AWS Direct Connect。 ● 针对特定服务请求并配置任何其他服务负载均衡器。

资源	服务职责	客户职责
虚拟计算管理	**Red Hat** ● 设置并配置 ROSA control plane 和 data plane，以将 Amazon EC2 实例用于集群计算。 ● 监控和管理集群中 Amazon EC2 control plane 和基础架构节点的部署。	● 使用 OpenShift Cluster Manager 或 ROSA CLI (**rosa**) 创建机器池来监控和管理 Amazon EC2 worker 节点。 ● 管理对客户部署的应用程序和应用程序数据的更改。
集群版本	**Red Hat** ● 启用升级调度过程。 ● 监控升级进度并更正遇到的问题。 ● 为补丁版本升级发布更改日志和发行注记。	● 设置自动升级，或立即或计划补丁版本升级。 ● 确认并计划次要版本升级。 ● 在补丁版本中测试客户应用程序以确保兼容性。
容量管理	**Red Hat** ● 监控 control plane 的使用。control plane 包括 control plane 节点和基础架构节点。 ● 扩展和重新定义 control plane 节点的大小，以维护服务质量。	● 监控 worker 节点使用率，并在适当情况下启用自动扩展功能。 ● 确定集群的扩展策略。有关机器池的更多信息，请参阅其他资源。 ● 根据需要，使用提供的 OpenShift Cluster Manager 控制添加或删除额外的 worker 节点。 ● 根据集群资源要求响应红帽通知。
虚拟存储管理	**Red Hat** ● 设置并配置 Amazon EBS，为集群置备本地节点存储和持久性卷存储。 ● 设置并配置内置镜像 registry，以使用 Amazon S3 存储桶存储。 ● 定期修剪 Amazon S3 中的镜像 registry 资源，以优化 Amazon S3 使用和集群性能。	● （可选）配置 Amazon EBS CSI 驱动程序或 Amazon EFS CSI 驱动程序，以在集群中置备持久性卷。

资源	服务职责	客户职责
AWS 软件（公共 AWS 服务）	**AWS** **Compute：** 提供 Amazon EC2 服务，用于 ROSA control plane、基础架构和 worker 节点。 **Storage ：** 提供 Amazon EBS，供 ROSA 用于为集群置备本地节点存储和持久性卷存储。 **存储：** 提供 Amazon S3，用于 ROSA 服务的内置镜像 registry。 **网络：** 提供以下 AWS 云服务，供 ROSA 用于满足虚拟网络基础架构需求： ● Amazon VPC ● Elastic Load Balancing ● AWS IAM **网络：** 提供以下 AWS 服务，客户可以选择与 ROSA 集成： ● AWS VPN ● AWS Direct Connect ● AWS PrivateLink ● AWS Transit Gateway	● 使用与 IAM 主体或 STS 临时安全凭证关联的访问密钥 ID 和 secret 访问密钥签名请求。 ● 指定集群创建过程中使用的 VPC 子网。 ● （可选）配置客户管理的 VPC 以用于 ROSA 集群（对于 PrivateLink 和 HCP 集群是必需的）。
硬件/AWS 全局基础架构	**AWS** ● 有关 AWS 数据中心管理控制的详情，请参考 AWS Cloud Security 页面中的 Our Controls。 ● 有关更改管理最佳实践的详情，请参考 AWS 解决方案库中更改管理有关 AWS 的指南。	● 为 AWS 云上托管的客户应用程序和数据实施变更管理最佳实践。

2.2.6. 安全和合规性

下表概述了与安全性和监管合规性相关的职责：

资源	服务职责	客户职责
日志记录	**Red Hat** ● 将集群审计日志发送到红帽 SIEM 以分析安全事件。为定义的时间段内保留审计日志，以便支持诊断分析。	● 分析安全事件的应用程序日志。 ● 如果默认日志记录堆栈提供的时间较长，则通过日志记录 sidecar 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。
虚拟网络管理	**Red Hat** ● 监控虚拟网络组件以了解潜在的问题和安全隐患。 ● 使用公共 AWS 工具进行额外的监控和保护。	● 监控可选配置的虚拟网络组件，以了解潜在的问题和安全隐患。 ● 根据需要配置任何必要的防火墙规则或客户数据中心保护。
虚拟存储管理	**Red Hat** ● 监控虚拟存储组件以了解潜在的问题和安全威胁。 ● 使用公共 AWS 工具进行额外的监控和保护。 ● 使用 Amazon EBS 提供的 AWS 管理的密钥管理服务 (KMS)密钥，将 ROSA 服务配置为加密 control plane、基础架构和 worker 节点卷数据。 ● 配置 ROSA 服务，以使用默认存储类和 Amazon EBS 提供的 AWS 管理的 KMS 密钥的客户持久性卷。 ● 为客户提供使用客户管理的 AWS KMS 密钥加密持久性卷的功能。 ● 配置容器镜像 registry，以使用 Amazon S3 管理的密钥 (SSE-3)的服务器端加密来加密镜像 registry 数据。 ● 为客户提供创建公共或私有 Amazon S3 镜像 registry 的功能，以保护其容器镜像不受未授权用户访问。	● 置备 Amazon EBS 卷。 ● 管理 Amazon EBS 卷存储，以确保有足够的存储可以作为卷在 ROSA 中挂载。 ● 创建持久性卷声明，并通过 OpenShift Cluster Manager 生成持久性卷。

资源	服务职责	客户职责
虚拟计算管理	**Red Hat** • 监控虚拟计算组件以了解潜在的问题和安全威胁。 • 使用公共 AWS 工具进行额外的监控和保护。	• 监控可选配置的虚拟网络组件，以了解潜在的问题和安全隐患。 • 根据需要配置任何必要的防火墙规则或客户数据中心保护。
AWS 软件（公共 AWS 服务）	**AWS** **compute：** 安全 Amazon EC2，用于 ROSA control plane、基础架构和 worker 节点。如需更多信息，请参阅 Amazon EC2 用户指南中的 Amazon EC2 中的基础架构安全性。 **存储：** 安全 Amazon Elastic Block Store (EBS)，用于 ROSA control plane、基础架构和 worker 节点卷，以及 Kubernetes 持久性卷。如需更多信息，请参阅 Amazon EC2 用户指南中的 Amazon EC2 中的数据保护。 **Storage ：** 提供 AWS KMS，ROSA 用于加密 control plane、基础架构和 worker 节点卷和持久性卷。如需更多信息，请参阅 Amazon EC2 用户指南中的 Amazon EBS 加密。 **存储：** 安全 Amazon S3，用于 ROSA 服务的内置容器镜像 registry。如需更多信息，请参阅 S3 用户指南中的 Amazon S3 安全性。 **网络：** 提供安全功能和服务，以提高 AWS 全局基础架构上的隐私和控制网络访问，包括建立在 Amazon VPC 中的网络防火墙、私有或专用网络连接，以及 AWS 安全设施之间所有流量自动加密。如需更多信息，请参阅 AWS 安全介绍中的 AWS 共享责任模型 和基础架构安全性。	• 确保遵循安全最佳实践和最小特权原则来保护 Amazon EC2 实例中的数据。如需更多信息，请参阅 Amazon EC2 中的基础架构安全性 和 Amazon EC2 中的数据保护。 • 监控可选配置的虚拟网络组件，以了解潜在的问题和安全隐患。 • 根据需要配置任何必要的防火墙规则或客户数据中心保护。 • 创建一个可选客户管理的 KMS 密钥，并使用 KMS 密钥加密 Amazon EBS 持久性卷。 • 监控虚拟存储中的客户数据，以了解潜在的问题和安全威胁。如需更多信息，请参阅 共享责任模型。

资源	服务职责	客户职责
硬件/AWS 全局基础架构	**AWS** • 提供 ROSA 用来提供服务功能的 AWS 全局基础架构。如需有关 AWS 安全控制的更多信息，请参阅 AWS 中的 AWS 基础架构安全性。 • 为客户提供管理合规需求的文档，并使用 AWS Artifact 和 AWS 安全 Hub 等工具在 AWS 中检查其安全状态。如需更多信息，请参阅 ROSA 用户指南中的 ROSA 验证。	• 配置、管理和监控客户应用程序和数据，以确保正确强制实施应用程序和数据安全控制。 • 使用 IAM 工具将适当的权限应用到客户账户中的 AWS 资源。

其他资源

- 有关客户或共享职责的更多信息，请参阅 ROSA 安全 文档。

2.2.7. 灾难恢复

灾难恢复包括数据和配置备份、将数据和配置复制到灾难恢复环境中，并在灾难恢复环境中进行故障转移。

Red Hat OpenShift Service on AWS (ROSA)为 pod、worker 节点、基础架构节点、control plane 节点和可用区级别的故障提供灾难恢复。

所有灾难恢复要求客户使用最佳实践来部署高可用性应用程序、存储和集群架构，如单区部署或多区部署等，以考虑所需的可用性级别。

当可用性区域或区域中断时，一个单区集群不会提供灾难避免或恢复。带有客户维护故障转移的多个单区集群可以在区域或区域级别考虑停机。

当完整区域中断时，一个多区集群不会提供灾难避免或恢复。多个带有客户维护故障转移的多区集群可以考虑区域级别的中断。

资源	服务职责	客户职责
虚拟网络管理	**Red Hat** • 恢复或重新创建平台正常工作所需的受影响的虚拟网络组件。	• 使用多个隧道配置虚拟网络连接，以防防公有云提供商建议中断。 • 如果使用多个集群的全局负载均衡器，请维护故障切换 DNS 和负载平衡。

资源	服务职责	客户职责
虚拟存储管理	**Red Hat** • 对于使用 IAM 用户凭证创建的 ROSA 集群，请通过每小时、每天和每周卷快照备份集群中的所有 Kubernetes 对象。每小时备份保留 24 小时(1 天)，为 168 小时(1 周)保留每日备份，每周备份会保留 720 hrs (30 天)。	• 备份客户应用程序和应用程序数据。
虚拟计算管理	**Red Hat** • 监控集群并替换失败的 Amazon EC2 control plane 或基础架构节点。 • 为客户提供手动或自动替换失败的 worker 节点的功能。	• 通过 OpenShift Cluster Manager 或 ROSA CLI 编辑机器池配置，替换失败的 Amazon EC2 worker 节点。
AWS 软件（公共 AWS 服务）	**AWS** **compute：** 提供支持数据弹性（如 Amazon EBS 快照和 Amazon EC2 自动扩展）的 Amazon EC2 功能。如需更多信息，请参阅 EC2 用户指南中的 Amazon EC2 中的弹性。 **Storage ：** 提供 ROSA 服务和客户通过 Amazon EBS 卷快照备份集群中的 Amazon EBS 卷的功能。 **存储：** 有关支持数据弹性的 Amazon S3 功能的信息，请参阅 Amazon S3 中的弹性。 **网络：** 有关支持数据弹性的 Amazon VPC 功能的信息，请参阅 Amazon VPC 用户指南中的 Amazon Virtual Private Cloud 中的 Resilience。	• 配置 ROSA 多AZ 集群，以提高容错和集群可用性。 • 使用 Amazon EBS CSI 驱动程序置备持久性卷以启用卷快照。 • 创建 Amazon EBS 持久性卷的 CSI 卷快照。

资源	服务职责	客户职责
硬件/AWS 全局基础架构	**AWS** • 提供 AWS 全局基础架构，允许 ROSA 在可用区间扩展 control plane、基础架构和 worker 节点。这个功能可让 ROSA 在区域间编配自动故障转移，而不中断。 • 有关灾难恢复最佳实践的更多信息，请参阅 AWS Well-Architected Framework 的云中的灾难恢复选项。	• 配置 ROSA 多AZ 集群，以提高容错和集群可用性。

其他资源

- 关于机器池

2.2.8. 额外的客户对数据和应用程序的职责

客户负责他们部署到 Red Hat OpenShift Service on AWS 上的应用程序、工作负载和数据。但是，红帽和 AWS 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	Red Hat 和 AWS	客户职责
客户数据	**Red Hat** • 保持平台级数据加密标准，如行业标准和合规标准所定义。 • 提供 OpenShift 组件以帮助管理应用数据，如机密。 • 启用与 Amazon RDS 等数据服务集成，以存储和管理集群和/或 AWS 之外的数据。 **AWS** • 提供 Amazon RDS，以便客户可以存储和管理集群和/或 AWS 之外的数据。	• 维护存储在平台上的所有客户数据的职责，以及客户应用程序如何使用和公开此数据。

资源	Red Hat 和 AWS	客户职责
客户应用程序	**Red Hat** • 调配安装了 OpenShift 组件的集群，以便客户可以访问 OpenShift 和 Kubernetes API 来部署和管理容器化应用。 • 使用镜像 pull secret 创建集群，以便客户部署可从 Red Hat Container Catalog registry 中拉取镜像。 • 提供对 OpenShift API 的访问，供客户用来设置 Operator 来向集群添加社区、第三方和红帽服务。 • 提供存储类和插件以支持用于客户应用程序的持久性卷。 • 提供容器镜像 registry，以便客户可以在集群上安全地存储应用程序容器镜像，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持久性卷。 • 提供 Amazon S3 以支持红帽置备容器镜像 registry。	• 为客户和第三方应用程序、数据及其完整生命周期维护责任。 • 如果客户使用 Operator 或外部镜像在集群中添加红帽、社区、第三方或其他服务，则客户负责这些服务并使用适当的供应商（包括红帽）来排除任何问题。 • 使用提供的工具和功能来配置和部署；保持最新；设置资源请求和限值；设置集群以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镜像流或模板；保存、备份和恢复数据；或者，管理其高可用性和弹性工作负载。 • 维护监控 Red Hat OpenShift Service on AWS 上运行的应用程序的职责，包括安装和操作软件来收集指标、创建警报以及保护应用程序中的 secret。

2.2.9. 其他资源

- 有关红帽站点可靠性工程(SRE)团队访问权限的更多信息，请参阅 身份和访问管理。

2.3. RED HAT OPENSHIFT SERVICE ON AWS 服务定义

本文档介绍了 概述了 Red Hat OpenShift Service on AWS (ROSA) 管理的服务的服务定义。

2.3.1. 帐户管理

本节提供有关 AWS 帐户管理上 Red Hat OpenShift Service 的服务定义的信息。

2.3.1.1. 账单和定价

Red Hat OpenShift Service on AWS 会直接指向 Amazon Web Services (AWS)帐户。ROSA 定价基于使用，每年承诺或 3 年的承诺以便获得更大的折现。ROSA 的总成本由两个部分组成：

- ROSA 服务费用
- AWS 基础架构费用

如需更多详细信息，请访问 AWS 网站上的 Red Hat OpenShift Service on AWS 定价 页面。

2.3.1.2. 集群自助服务

客户可以自助服务集群，包括但不限于：

- 创建集群
- 删除集群
- 添加或删除身份提供程序
- 从提升的组中添加或删除用户
- 配置集群隐私
- 添加或删除机器池并配置自动扩展
- 定义升级策略

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa** 执行这些自助服务任务。

2.3.1.3. 实例类型

单个可用区集群至少需要 3 个 control plane 节点、2 个基础架构节点和 2 个 worker 节点部署到一个可用区。

多个可用区集群至少需要 3 个 control plane 节点、3 个基础架构节点和 3 个 worker 节点。额外的节点必须购买到 3 的倍数才能保持适当的节点分布。

AWS 集群上的所有 Red Hat OpenShift Service 都支持最多 180 个 worker 节点。

control plane 和基础架构节点由红帽部署和管理。不支持通过云供应商控制台关闭底层基础架构，可能会导致数据丢失。至少 3 个 control plane 节点可以处理 etcd 和 API 相关的工作负载。至少 2 个基础架构节点来处理指标、路由、Web 控制台和其他工作负载。您不能在控制和基础架构节点上运行任何工作负载。任何您要运行的工作负载都必须部署到 worker 节点上。有关必须在 worker 节点上部署的红帽工作负载的更多信息，请参阅下面的 Red Hat Operator 支持部分。

注意

每个 worker 节点上都会保留一个 vCPU 内核和 1 GiB 内存，并从可分配的资源中删除。运行底层平台所需的进程需要保留资源。这些进程包括系统守护进程，如 udev、kubelet 和容器运行时。保留的资源也考虑内核保留。

OpenShift Container Platform 核心系统（如审计日志聚合、指标集合、DNS、镜像 registry、SDN 等）可能会消耗额外的可分配资源来保持集群的稳定性和可维护性。所消耗的额外资源可能会因使用情况而异。

如需更多信息，请参阅 Kubernetes 文档。

其它资源

- Red Hat Operator 支持
- 配置 PID 限制

2.3.1.4. AWS 实例类型

Red Hat OpenShift Service on AWS 提供了以下 worker 节点实例类型和大小：

例 2.1. 常规目的

- m5.metal (96† vCPU, 384 GiB)
- m5.xlarge (4 vCPU, 16 GiB)
- m5.2xlarge (8 vCPU, 32 GiB)
- m5.4xlarge (16 vCPU, 64 GiB)
- m5.8xlarge (32 vCPU, 128 GiB)
- m5.12xlarge (48 vCPU, 192 GiB)
- m5.16xlarge (64 vCPU, 256 GiB)
- m5.24xlarge (96 vCPU, 384 GiB)
- m5a.xlarge (4 vCPU, 16 GiB)
- m5a.2xlarge (8 vCPU, 32 GiB)
- m5a.4xlarge (16 vCPU, 64 GiB)
- m5a.8xlarge (32 vCPU, 128 GiB)
- m5a.12xlarge (48 vCPU, 192 GiB)
- m5a.16xlarge (64 vCPU, 256 GiB)
- m5a.24xlarge (96 vCPU, 384 GiB)
- m5dn.metal (96 vCPU, 384 GiB)
- m5zn.metal (48 vCPU, 192 GiB)
- m5d.metal (96† vCPU, 384 GiB)
- m5n.metal (96 vCPU, 384 GiB)
- m6a.metal (192 vCPU, 768 GiB)
- m6a.xlarge (4 vCPU, 16 GiB)
- m6a.2xlarge (8 vCPU, 32 GiB)
- m6a.4xlarge (16 vCPU, 64 GiB)
- m6a.8xlarge (32 vCPU, 128 GiB)
- m6a.12xlarge (48 vCPU, 192 GiB)
- m6a.16xlarge (64 vCPU, 256 GiB)

- m6a.24xlarge (96 vCPU, 384 GiB)
- m6a.32xlarge (128 vCPU, 512 GiB)
- m6a.48xlarge (192 vCPU, 768 GiB)
- m6i.metal (128 vCPU, 512 GiB)
- m6i.xlarge (4 vCPU, 16 GiB)
- m6i.2xlarge (8 vCPU, 32 GiB)
- m6i.4xlarge (16 vCPU, 64 GiB)
- m6i.8xlarge (32 vCPU, 128 GiB)
- m6i.12xlarge (48 vCPU, 192 GiB)
- m6i.16xlarge (64 vCPU, 256 GiB)
- m6i.24xlarge (96 vCPU，384 GiB)
- m6i.32xlarge (128 vCPU, 512 GiB)
- m6id.xlarge (4 vCPU, 16 GiB)
- m6id.2xlarge (8 vCPU, 32 GiB)
- m6id.4xlarge (16 vCPU, 64 GiB)
- m6id.8xlarge (32 vCPU, 128 GiB)
- m6id.12xlarge (48 vCPU, 192 GiB)
- m6id.16xlarge (64 vCPU, 256 GiB)
- m6id.24xlarge (96 vCPU, 384 GiB)
- m6id.32xlarge (128 vCPU, 512 GiB)
- m6id.metal (128 vCPU, 512 GiB)
- m6idn.xlarge (4 vCPU, 16 GiB)
- m6idn.2xlarge (8 vCPU, 32 GiB)
- m6idn.4xlarge (16 vCPU, 64 GiB)
- m6idn.8xlarge (32 vCPU, 128 GiB)
- m6idn.12xlarge (48 vCPU, 192 GiB)
- m6idn.16xlarge (64 vCPU, 256 GiB)
- m6idn.24xlarge (96 vCPU, 384 GiB)
- m6idn.32xlarge (128 vCPU, 512 GiB)

- m6in.xlarge (4 vCPU, 16 GiB)
- m6in.2xlarge (8 vCPU, 32 GiB)
- m6in.4xlarge (16 vCPU, 64 GiB)
- m6in.8xlarge (32 vCPU, 128 GiB)
- m6in.12xlarge (48 vCPU, 192 GiB)
- m6in.16xlarge (64 vCPU, 256 GiB)
- m6in.24xlarge (96 vCPU, 384 GiB)
- m6in.32xlarge (128 vCPU, 512 GiB)
- m7a.xlarge (4 vCPU, 16 GiB)
- m7a.2xlarge (8 vCPU, 32 GiB)
- m7a.4xlarge (16 vCPU, 64 GiB)
- m7a.8xlarge (32 vCPU, 128 GiB)
- m7a.12xlarge (48 vCPU, 192 GiB)
- m7a.16xlarge (64 vCPU, 256 GiB)
- m7a.24xlarge (96 vCPU, 384 GiB)
- m7a.32xlarge (128 vCPU, 512 GiB)
- m7a.48xlarge (192 vCPU, 768 GiB)
- m7a.metal-48xl (192 vCPU, 768 GiB)
- m7i-flex.2xlarge (8 vCPU, 32 GiB)
- m7i-flex.4xlarge (16 vCPU, 64 GiB)
- m7i-flex.8xlarge (32 vCPU, 128 GiB)
- m7i-flex.xlarge (4 vCPU, 16 GiB)
- m7i.xlarge (4 vCPU, 16 GiB)
- m7i.2xlarge (8 vCPU, 32 GiB)
- m7i.4xlarge (16 vCPU, 64 GiB)
- m7i.8xlarge (32 vCPU, 128 GiB)
- m7i.12xlarge (48 vCPU, 192 GiB)
- m7i.16xlarge (64 vCPU, 256 GiB)
- m7i.24xlarge (96 vCPU, 384 GiB)

- m7i.48xlarge (192 vCPU, 768 GiB)
- m7i.metal-24xl (96 vCPU, 384 GiB)
- m7i.metal-48xl (192 vCPU, 768 GiB)

这些实例类型在 48 个物理内核中提供 96 个逻辑处理器。它们在两个物理 Intel 插槽的单台服务器上运行。

例 2.2. Burstable 常规目的

- t3.xlarge (4 vCPU, 16 GiB)
- t3.2xlarge (8 vCPU, 32 GiB)
- t3a.xlarge (4 vCPU, 16 GiB)
- t3a.2xlarge (8 vCPU, 32 GiB)

例 2.3. 内存密集型

- x1.16xlarge (64 vCPU, 976 GiB)
- x1.32xlarge (128 vCPU, 1,952 GiB)
- x1e.xlarge (4 vCPU, 122 GiB)
- x1e.2xlarge (8 vCPU, 244 GiB)
- x1e.4xlarge (16 vCPU, 488 GiB)
- x1e.8xlarge (32 vCPU, 976 GiB)
- x1e.16xlarge (64 vCPU, 1,952 GiB)
- x1e.32xlarge (128 vCPU, 3,904 GiB)
- x2idn.16xlarge (64 vCPU, 1,024 GiB)
- x2idn.24xlarge (96 vCPU, 1,536 GiB)
- x2idn.32xlarge (128 vCPU, 2,048 GiB)
- x2iedn.xlarge (4 vCPU, 128 GiB)
- x2iedn.2xlarge (8 vCPU, 256 GiB)
- x2iedn.4xlarge (16 vCPU, 512 GiB)
- x2iedn.8xlarge (32 vCPU, 1,024 GiB)
- x2iedn.16xlarge (64 vCPU, 2,048 GiB)
- x2iedn.24xlarge (96 vCPU, 3,072 GiB)

- x2iedn.32xlarge (128 vCPU, 4,096 GiB)
- x2iezn.metal (48 vCPU, 1,536 GiB)
- x2iezn.2xlarge (8 vCPU, 256 GiB)
- x2iezn.4xlarge (16vCPU, 512 GiB)
- x2iezn.6xlarge (24vCPU, 768 GiB)
- x2iezn.8xlarge (32vCPU, 1,024 GiB)
- x2iezn.12xlarge (48vCPU, 1,536 GiB)
- x2idn.metal (128vCPU, 2,048 GiB)
- x2iedn.metal (128vCPU, 4,096 GiB)

例 2.4. 内存优化

- r4.xlarge (4 vCPU, 30.5 GiB)
- r4.2xlarge (8 vCPU, 61 GiB)
- r4.4xlarge (16 vCPU, 122 GiB)
- r4.8xlarge (32 vCPU, 244 GiB)
- r4.16xlarge (64 vCPU, 488 GiB)
- r5.metal (96† vCPU, 768 GiB)
- r5.xlarge (4 vCPU, 32 GiB)
- r5.2xlarge (8 vCPU, 64 GiB)
- r5.4xlarge (16 vCPU, 128 GiB)
- r5.8xlarge (32 vCPU, 256 GiB)
- r5.12xlarge (48 vCPU, 384 GiB)
- r5.16xlarge (64 vCPU, 512 GiB)
- r5.24xlarge (96 vCPU, 768 GiB)
- r5a.xlarge (4 vCPU, 32 GiB)
- r5a.2xlarge (8 vCPU, 64 GiB)
- r5a.4xlarge (16 vCPU, 128 GiB)
- r5a.8xlarge (32 vCPU, 256 GiB)
- r5a.12xlarge (48 vCPU, 384 GiB)
- r5a.16xlarge (64 vCPU, 512 GiB)

- r5a.24xlarge (96 vCPU, 768 GiB)
- r5ad.xlarge (4 vCPU, 32 GiB)
- r5ad.2xlarge (8 vCPU, 64 GiB)
- r5ad.4xlarge (16 vCPU, 128 GiB)
- r5ad.8xlarge (32 vCPU, 256 GiB)
- r5ad.12xlarge (48 vCPU, 384 GiB)
- r5ad.16xlarge (64 vCPU, 512 GiB)
- r5ad.24xlarge (96 vCPU, 768 GiB)
- r5b.metal (96 768 GiB)
- r5b.xlarge (4 vCPU, 32 GiB)
- r5b.2xlarge (8 vCPU, 364 GiB)
- r5b.4xlarge (16 vCPU, 3,128 GiB)
- r5b.8xlarge (32 vCPU, 3,256 GiB)
- r5b.12xlarge (48 vCPU, 3,384 GiB)
- r5b.16xlarge (64 vCPU, 3,512 GiB)
- r5b.24xlarge (96 vCPU, 3,768 GiB)
- r5d.metal (96† vCPU, 768 GiB)
- r5d.xlarge (4 vCPU, 32 GiB)
- r5d.2xlarge (8 vCPU, 64 GiB)
- r5d.4xlarge (16 vCPU, 128 GiB)
- r5d.8xlarge (32 vCPU, 256 GiB)
- r5d.12xlarge (48 vCPU, 384 GiB)
- r5d.16xlarge (64 vCPU, 512 GiB)
- r5d.24xlarge (96 vCPU, 768 GiB)
- r5n.metal (96 vCPU, 768 GiB)
- r5n.xlarge (4 vCPU, 32 GiB)
- r5n.2xlarge (8 vCPU, 64 GiB)
- r5n.4xlarge (16 vCPU, 128 GiB)
- r5n.8xlarge (32 vCPU, 256 GiB)

- r5n.12xlarge (48 vCPU, 384 GiB)
- r5n.16xlarge (64 vCPU, 512 GiB)
- r5n.24xlarge (96 vCPU, 768 GiB)
- r5dn.metal (96 vCPU, 768 GiB)
- r5dn.xlarge (4 vCPU, 32 GiB)
- r5dn.2xlarge (8 vCPU, 64 GiB)
- r5dn.4xlarge (16 vCPU, 128 GiB)
- r5dn.8xlarge (32 vCPU, 256 GiB)
- r5dn.12xlarge (48 vCPU, 384 GiB)
- r5dn.16xlarge (64 vCPU, 512 GiB)
- r5dn.24xlarge (96 vCPU, 768 GiB)
- r6a.xlarge (4 vCPU, 32 GiB)
- r6a.2xlarge (8 vCPU, 64 GiB)
- r6a.4xlarge (16 vCPU, 128 GiB)
- r6a.8xlarge (32 vCPU, 256 GiB)
- r6a.12xlarge (48 vCPU, 384 GiB)
- r6a.16xlarge (64 vCPU, 512 GiB)
- r6a.24xlarge (96 vCPU, 768 GiB)
- r6a.32xlarge (128 vCPU, 1,024 GiB)
- r6a.48xlarge (192 vCPU, 1,536 GiB)
- r6i.metal (128 vCPU, 1,024 GiB)
- r6i.xlarge (4 vCPU, 32 GiB)
- r6i.2xlarge (8 vCPU, 64 GiB)
- r6i.4xlarge (16 vCPU, 128 GiB)
- r6i.8xlarge (32 vCPU， 256 GiB)
- r6i.12xlarge (48 vCPU, 384 GiB)
- r6i.16xlarge (64 vCPU, 512 GiB)
- r6i.24xlarge (96 vCPU, 768 GiB)
- r6i.32xlarge (128 vCPU， 1,024 GiB)

- r6id.metal (128 vCPU, 1,024 GiB)
- r6id.xlarge (4 vCPU, 32 GiB)
- r6id.2xlarge (8 vCPU, 64 GiB)
- r6id.4xlarge (16 vCPU, 128 GiB)
- r6id.8xlarge (32 vCPU, 256 GiB)
- r6id.12xlarge (48 vCPU, 384 GiB)
- r6id.16xlarge (64 vCPU, 512 GiB)
- r6id.24xlarge (96 vCPU, 768 GiB)
- r6id.32xlarge (128 vCPU, 1,024 GiB)
- r6idn.12xlarge (48 vCPU, 384 GiB)
- r6idn.16xlarge (64 vCPU, 512 GiB)
- r6idn.24xlarge (96 vCPU, 768 GiB)
- r6idn.2xlarge (8 vCPU, 64 GiB)
- r6idn.32xlarge (128 vCPU, 1,024 GiB)
- r6idn.4xlarge (16 vCPU, 128 GiB)
- r6idn.8xlarge (32 vCPU, 256 GiB)
- r6idn.xlarge (4 vCPU, 32 GiB)
- r6in.12xlarge (48 vCPU, 384 GiB)
- r6in.16xlarge (64 vCPU, 512 GiB)
- r6in.24xlarge (96 vCPU, 768 GiB)
- r6in.2xlarge (8 vCPU, 64 GiB)
- r6in.32xlarge (128 vCPU, 1,024 GiB)
- r6in.4xlarge (16 vCPU, 128 GiB)
- r6in.8xlarge (32 vCPU, 256 GiB)
- r6in.xlarge (4 vCPU, 32 GiB)
- r7iz.xlarge (4 vCPU, 32 GiB)
- r7iz.2xlarge (8 vCPU, 64 GiB)
- r7iz.4xlarge (16 vCPU, 128 GiB)
- r7iz.8xlarge (32 vCPU, 256 GiB)

- r7iz.12xlarge (48 vCPU, 384 GiB)
- r7iz.16xlarge (64 vCPU, 512 GiB)
- r7iz.32xlarge (128 vCPU, 1024 GiB)
- r7iz.metal-16xl (64 vCPU, 512 GiB)
- r7iz.metal-32xl (128 vCPU, 1,024 GiB)
- z1d.metal (48 vCPU, 384 GiB)
- z1d.xlarge (4 vCPU, 32 GiB)
- z1d.2xlarge (8 vCPU, 64 GiB)
- z1d.3xlarge (12 vCPU, 96 GiB)
- z1d.6xlarge (24 vCPU, 192 GiB)
- z1d.12xlarge (48 vCPU, 384 GiB)

这些实例类型在 48 个物理内核中提供 96 个逻辑处理器。它们在两个物理 Intel 插槽的单台服务器上运行。

这个实例类型在 24 个物理内核中提供 48 个逻辑处理器。

例 2.5. 加速计算

- p3.2xlarge (8 vCPU, 61 GiB)
- p3.8xlarge (32 vCPU, 244 GiB)
- p3.16xlarge (64 vCPU, 488 GiB)
- p3dn.24xlarge (96 vCPU, 768 GiB)
- p4d.24xlarge (96 vCPU, 1,152 GiB)
- p4de.24xlarge (96 vCPU, 1,152 GiB)
- p5.48xlarge (192 vCPU, 2,048 GiB)
- g4dn.xlarge (4 vCPU, 16 GiB)
- g4dn.2xlarge (8 vCPU, 32 GiB)
- g4dn.4xlarge (16 vCPU, 64 GiB)
- g4dn.8xlarge (32 vCPU, 128 GiB)
- g4dn.12xlarge (48 vCPU, 192 GiB)
- g4dn.16xlarge (64 vCPU, 256 GiB)
- g4dn.metal (96 vCPU, 384 GiB)

- g5.xlarge (4 vCPU, 16 GiB)
- g5.2xlarge (8 vCPU, 32 GiB)
- g5.4xlarge (16 vCPU, 64 GiB)
- g5.8xlarge (32 vCPU, 128 GiB)
- g5.16xlarge (64 vCPU, 256 GiB)
- g5.12xlarge (48 vCPU, 192 GiB)
- g5.24xlarge (96 vCPU, 384 GiB)
- g5.48xlarge (192 vCPU, 768 GiB)
- dl1.24xlarge (96 vCPU, 768 GiB)

† 特定于 Intel；不被 Nvidia 支持

对 GPU 实例类型软件堆栈的支持由 AWS 提供。确保您的 AWS 服务配额可以容纳所需的 GPU 实例类型。

例 2.6. 计算优化

- c5.metal (96 vCPU, 192 GiB)
- c5.xlarge (4 vCPU, 8 GiB)
- c5.2xlarge (8 vCPU, 16 GiB)
- c5.4xlarge (16 vCPU, 32 GiB)
- c5.9xlarge (36 vCPU, 72 GiB)
- c5.12xlarge (48 vCPU, 96 GiB)
- c5.18xlarge (72 vCPU, 144 GiB)
- c5.24xlarge (96 vCPU, 192 GiB)
- c5d.metal (96 vCPU, 192 GiB)
- c5d.xlarge (4 vCPU, 8 GiB)
- c5d.2xlarge (8 vCPU, 16 GiB)
- c5d.4xlarge (16 vCPU, 32 GiB)
- c5d.9xlarge (36 vCPU, 72 GiB)
- c5d.12xlarge (48 vCPU, 96 GiB)
- c5d.18xlarge (72 vCPU, 144 GiB)
- c5d.24xlarge (96 vCPU, 192 GiB)

- c5a.xlarge (4 vCPU, 8 GiB)
- c5a.2xlarge (8 vCPU, 16 GiB)
- c5a.4xlarge (16 vCPU, 32 GiB)
- c5a.8xlarge (32 vCPU, 64 GiB)
- c5a.12xlarge (48 vCPU, 96 GiB)
- c5a.16xlarge (64 vCPU, 128 GiB)
- c5a.24xlarge (96 vCPU, 192 GiB)
- c5ad.xlarge (4 vCPU, 8 GiB)
- c5ad.2xlarge (8 vCPU, 16 GiB)
- c5ad.4xlarge (16 vCPU, 32 GiB)
- c5ad.8xlarge (32 vCPU, 64 GiB)
- c5ad.12xlarge (48 vCPU, 96 GiB)
- c5ad.16xlarge (64 vCPU, 128 GiB)
- c5ad.24xlarge (96 vCPU, 192 GiB)
- c5n.metal (72 vCPU, 192 GiB)
- c5n.xlarge (4 vCPU, 10.5 GiB)
- c5n.2xlarge (8 vCPU, 21 GiB)
- c5n.4xlarge (16 vCPU, 42 GiB)
- c5n.9xlarge (36 vCPU, 96 GiB)
- c5n.18xlarge (72 vCPU, 192 GiB)
- c6a.xlarge (4 vCPU, 8 GiB)
- c6a.2xlarge (8 vCPU, 16 GiB)
- c6a.4xlarge (16 vCPU, 32 GiB)
- c6a.8xlarge (32 vCPU, 64 GiB)
- c6a.12xlarge (48 vCPU, 96 GiB)
- c6a.16xlarge (64 vCPU, 128 GiB)
- c6a.24xlarge (96 vCPU, 192 GiB)
- c6a.32xlarge (128 vCPU, 256 GiB)
- c6a.48xlarge (192 vCPU, 384 GiB)

- c6i.metal (128 vCPU, 256 GiB)
- c6i.xlarge (4 vCPU, 8 GiB)
- c6i.2xlarge (8 vCPU, 16 GiB)
- c6i.4xlarge (16 vCPU, 32 GiB)
- c6i.8xlarge (32 vCPU, 64 GiB)
- c6i.12xlarge (48 vCPU，96 GiB)
- c6i.16xlarge (64 vCPU, 128 GiB)
- c6i.24xlarge (96 vCPU, 192 GiB)
- c6i.32xlarge (128 vCPU, 256 GiB)
- c6id.metal (128 vCPU, 256 GiB)
- c6id.xlarge (4 vCPU, 8 GiB)
- c6id.2xlarge (8 vCPU, 16 GiB)
- c6id.4xlarge (16 vCPU, 32 GiB)
- c6id.8xlarge (32 vCPU, 64 GiB)
- c6id.12xlarge (48 vCPU, 96 GiB)
- c6id.16xlarge (64 vCPU, 128 GiB)
- c6id.24xlarge (96 vCPU, 192 GiB)
- c6id.32xlarge (128 vCPU, 256 GiB)
- c6in.12xlarge (48 vCPU, 96 GiB)
- c6in.16xlarge (64 vCPU, 128 GiB)
- c6in.24xlarge (96 vCPU, 192 GiB)
- c6in.2xlarge (8 vCPU, 16 GiB)
- c6in.32xlarge (128 vCPU, 256 GiB)
- c6in.4xlarge (16 vCPU, 32 GiB)
- c6in.8xlarge (32 vCPU, 64 GiB)
- c6in.xlarge (4 vCPU, 8 GiB)
- m5zn.12xlarge (48 vCPU, 192 GiB)
- m5zn.2xlarge (8 vCPU, 32 GiB)
- m5zn.3xlarge (16 vCPU, 48 GiB)

- m5zn.6xlarge (32 vCPU, 96 GiB)
- m5zn.xlarge (4 vCPU, 16 GiB)

例 2.7. 存储优化

- c5ad.12xlarge (48 vCPU, 96 GiB)
- c5ad.16xlarge (64 vCPU, 128 GiB)
- c5ad.24xlarge (96 vCPU, 192 GiB)
- c5ad.2xlarge (8 vCPU, 16 GiB)
- c5ad.4xlarge (16 vCPU, 32 GiB)
- c5ad.8xlarge (32 vCPU, 64 GiB)
- c5ad.xlarge (4 vCPU, 8 GiB)
- i3.metal (72† vCPU, 512 GiB)
- i3.xlarge (4 vCPU, 30.5 GiB)
- i3.2xlarge (8 vCPU, 61 GiB)
- i3.4xlarge (16 vCPU, 122 GiB)
- i3.8xlarge (32 vCPU, 244 GiB)
- i3.16xlarge (64 vCPU, 488 GiB)
- i3en.metal (96 vCPU, 768 GiB)
- i3en.xlarge (4 vCPU, 32 GiB)
- i3en.2xlarge (8 vCPU, 64 GiB)
- i3en.3xlarge (12 vCPU, 96 GiB)
- i3en.6xlarge (24 vCPU, 192 GiB)
- i3en.12xlarge (48 vCPU, 384 GiB)
- i3en.24xlarge (96 vCPU, 768 GiB)
- i4i.xlarge (4 vCPU, 32 GiB)
- i4i.2xlarge (8 vCPU, 64 GiB)
- i4i.4xlarge (16 vCPU, 128 GiB)
- i4i.8xlarge (32 vCPU, 256 GiB)
- i4i.12xlarge (48 vCPU, 384 GiB)
- i4i.16xlarge (64 vCPU, 512 GiB)

- i4i.24xlarge (96 vCPU, 768 GiB)
- i4i.32xlarge (128 vCPU, 1,024 GiB)
- i4i.metal (128 vCPU, 1,024 GiB)
- m5ad.xlarge (4 vCPU, 16 GiB)
- m5ad.2xlarge (8 vCPU, 32 GiB)
- m5ad.4xlarge (16 vCPU, 64 GiB)
- m5ad.8xlarge (32 vCPU, 128 GiB)
- m5ad.12xlarge (48 vCPU, 192 GiB)
- m5ad.16xlarge (64 vCPU, 256 GiB)
- m5ad.24xlarge (96 vCPU, 384 GiB)
- m5d.xlarge (4 vCPU, 16 GiB)
- m5d.2xlarge (8 vCPU, 32 GiB)
- m5d.4xlarge (16 vCPU, 64 GiB)
- m5d.8xlarge (32 vCPU, 28 GiB)
- m5d.12xlarge (48 vCPU, 192 GiB)
- m5d.16xlarge (64 vCPU, 256 GiB)
- m5d.24xlarge (96 vCPU, 384 GiB)

这个实例类型在 36 个物理内核中提供 72 个逻辑处理器。

注意

虚拟实例类型初始化速度快于 ".metal" 实例类型。

例 2.8. 高内存

- U-3tb1.56xlarge (224 vCPU, 3,072 GiB)
- U-6tb1.56xlarge (224 vCPU, 6,144 GiB)
- U-6tb1.112xlarge (448 vCPU, 6,144 GiB)
- u-6tb1.metal (448 vCPU, 6,144 GiB)
- U-9tb1.112xlarge (448 vCPU, 9,216 GiB)
- U-9tb1.metal (448 vCPU, 9,216 GiB)
- U-12tb1.112xlarge (448 vCPU, 12,288 GiB)

- U-12tb1.metal (448 vCPU, 12,288 GiB)
- u-18tb1.metal (448 vCPU, 18,432 GiB)
- U-24tb1.metal (448 vCPU, 24,576 GiB)
- U-24tb1.112xlarge (448 vCPU, 24,576 GiB)

例 2.9. 网络优化

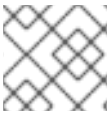
- c5n.xlarge (4 vCPU, 10.5 GiB)
- c5n.2xlarge (8 vCPU, 21 GiB)
- c5n.4xlarge (16 vCPU, 42 GiB)
- c5n.9xlarge (36 vCPU, 96 GiB)
- c5n.18xlarge (72 vCPU, 192 GiB)
- m5dn.xlarge (4 vCPU, 16 GiB)
- m5dn.2xlarge (8 vCPU, 32 GiB)
- m5dn.4xlarge (16 vCPU, 64 GiB)
- m5dn.8xlarge (32 vCPU, 128 GiB)
- m5dn.12xlarge (48 vCPU, 192 GiB)
- m5dn.16xlarge (64 vCPU, 256 GiB)
- m5dn.24xlarge (96 vCPU, 384 GiB)
- m5n.12xlarge (48 vCPU, 192 GiB)
- m5n.16xlarge (64 vCPU, 256 GiB)
- m5n.24xlarge (96 vCPU, 384 GiB)
- m5n.xlarge (4 vCPU, 16 GiB)
- m5n.2xlarge (8 vCPU, 32 GiB)
- m5n.4xlarge (16 vCPU, 64 GiB)
- m5n.8xlarge (32 vCPU, 128 GiB)

其它资源

- AWS 实例类型

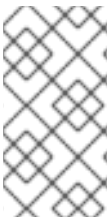
2.3.1.5. 地区和可用性区域

以下 AWS 区域目前可用于 Red Hat OpenShift 4，并受 Red Hat OpenShift Service on AWS 的支持。



注意

中国的区域不受支持，无论它们对 OpenShift 4 的支持是什么。



注意

对于 GovCloud (US)区域，您必须提交 Red Hat OpenShift Service on AWS (ROSA) FedRAMP 的访问请求。

GovCloud (US)区域只在 ROSA Classic 集群中被支持。

例 2.10. AWS 区域

- us-east-1（北弗吉尼亚）
- us-east-2（俄亥俄）
- us-west-1（北加利福尼亚）
- us-west-2（俄勒冈）
- af-south-1 (Cape Town, AWS opt-in required)
- ap-east-1 (Hong Kong, AWS opt-in required)
- ap-south-2 (Hyderabad, AWS opt-in required)
- ap-southeast-3(Jakarta, AWS opt-in required)
- ap-southeast-4 (Melbourne, AWS opt-in required)
- ap-south-1（孟买）
- ap-northeast-3 (Osaka)
- ap-northeast-2 （首尔）
- ap-southeast-1（新加坡）
- ap-southeast-2（悉尼）
- ap-northeast-1（东京）
- ca-central-1 (Central Canada)
- eu-central-1（法拉克福）
- eu-north-1（斯德哥尔摩）
- eu-west-1（爱尔兰）
- eu-west-2（伦敦）
- eu-south-1 (Milan、AWS opt-in required)

- eu-west-3（巴黎）
- eu-south-2 (Spain)
- eu-central-2 (Zurich, AWS opt-in required)
- me-south-1 (Bahrain, AWS opt-in required)
- me-central-1 (UAE, AWS opt-in required)
- sa-east-1 （圣保罗）
- us-gov-east-1 (AWS GovCloud - US-East)
- us-gov-west-1 (AWS GovCloud - US-West)

多个可用区集群只能部署到至少 3 个可用区的区域。如需更多信息，请参阅 AWS 文档中的 Regions 和 Availability Zones 部分。

AWS 集群上的每个新的 Red Hat OpenShift Service 都会在一个区域创建或已存在的虚拟私有云 (VPC) 内安装，可以选择部署到单一可用区(Single-AZ) 或多可用区 (Multi-AZ)。这提供了集群级别的网络和资源隔离，并启用 cloud-provider VPC 设置，如 VPN 连接和 VPC Peering。持久性卷(PV)由 Amazon Elastic Block Storage (Amazon EBS)支持，并特定于置备的可用区。在将关联的 pod 资源分配给特定的可用区前，持久性卷声明(PVC)不会绑定到卷，以防止不可调度的 pod。特定于可用区的资源只可供同一可用区中的资源使用。

警告

部署集群后，无法更改一个或多个可用区的区域和选择。

其它资源

- Red Hat OpenShift Service on AWS 端点和配额

2.3.1.6. 本地区域

Red Hat OpenShift Service on AWS 支持使用 AWS Local Zones，这些区域会满足集中式可用区，客户可以放置对延迟敏感的应用程序工作负载。本地区域是有其自身互联网连接的 AWS 区域扩展。有关 AWS 区域的更多信息，请参阅 AWS 文档 Local Zones 的工作原理。

有关启用 AWS Local Zones 并将 Local Zone 添加到机器池的步骤，请参阅 为机器池配置 Local Zones。

2.3.1.7. 服务等级协议 (SLA)

服务本身的任何 SLA 在 Red Hat Enterprise Agreement 附录 4 （在线订阅服务）的附录 4 中定义。

2.3.1.8. 有限支持状态

当集群过渡到 *有限支持状*态时，红帽不再主动监控集群，SLA 将不再适用，并拒绝对 SLA 请求的学分。这并不意味着您不再有产品支持。在某些情况下，如果您修复了违反因素，集群可以返回完全支持的状态。但是，在其他情况下，您可能需要删除并重新创建集群。

集群可能会因为许多原因移至有限支持状态，包括以下情况：

如果您没有在生命周期结束前将集群升级到支持的版本

红帽不会在其生命周期结束后为版本提供任何运行时或 SLA 保证。要继续获得支持，请在生命周期结束前将集群升级到受支持的版本。如果您没有在生命周期结束前升级集群，集群会过渡到有限支持状态，直到升级到一个支持版本。
红帽提供了合理的商业支持，从不受支持的版本升级到受支持的版本。但是，如果支持的升级路径不再可用，您可能需要创建新集群并迁移您的工作负载。

如果您删除或替换任何由红帽安装和管理的 Red Hat OpenShift Service on AWS 组件或任何其他组件

如果使用了集群管理员权限，红帽不负责您的任何或授权用户的操作，包括影响基础架构服务、服务可用性或数据丢失的人。如果红帽检测到此类操作，集群可能会过渡到有限支持状态。红帽通知您的状态变化，您应该恢复操作或创建支持问题单来探索可能需要删除和重新创建集群的补救步骤。

如果您对可能造成集群移至有限支持状态或需要进一步帮助的特定操作有疑问，请打开支持票据。

2.3.1.9. 支持

Red Hat OpenShift Service on AWS 包括红帽高级支持，可以使用 红帽客户门户网站 访问。

如需支持响应时间，请参阅 AWS SLA 上的 Red Hat OpenShift Service。

AWS 支持取决于客户对 AWS 的现有支持合同。

2.3.2. 日志记录

Red Hat OpenShift Service on AW 为 Amazon (AWS) CloudWatch 提供可选集成日志转发。

2.3.2.1. 集群日志记录

如果启用了集成，可以通过 AWS CloudWatch 集群审计日志。如果没有启用集成，您可以通过打开支持问题单来请求审计日志。

2.3.2.2. 应用程序日志记录

发送到 **STDOUT** 的应用程序日志由 Fluentd 收集，并通过集群日志记录堆栈转发到 AWS CloudWatch（如果已安装）。

2.3.3. 监控

本节提供有关 Red Hat OpenShift Service on AWS 监控的服务定义信息。

2.3.3.1. 集群指标

Red Hat OpenShift Service on AWS 集群上带有集成 Prometheus 堆栈，用于集群监控，包括 CPU、内存和基于网络的指标。这可以通过 Web 控制台访问。这些指标还允许由 Red Hat OpenShift Service on AWS 用户提供的 CPU 或内存指标进行 pod 横向自动扩展。

2.3.3.2. 集群通知

集群通知是有关集群状态、健康或性能的信息。

集群通知是 Red Hat Site Reliability Engineering (SRE)与您有关受管集群健康状况的主要方法。SRE 也可能使用集群通知来提示您执行操作，以解决或防止集群出现问题。

集群所有者和管理员必须定期检查和操作集群通知，以确保集群保持健康且受支持。

您可以在集群的 **Cluster history** 选项卡中查看 Red Hat Hybrid Cloud Console 中的集群通知。默认情况下，只有集群所有者接收集群通知作为电子邮件。如果其他用户需要接收集群通知电子邮件，请将每个用户添加为集群的通知联系人。

2.3.4. 网络

本节提供有关 Red Hat OpenShift Service on AWS 网络服务定义信息。

2.3.4.1. 应用程序自定义域

警告

从 Red Hat OpenShift Service on AWS 4.14 开始，自定义域 Operator 已被弃用。要在 AWS 4.14 或更高版本的 Red Hat OpenShift Service 中管理 Ingress，请使用 Ingress Operator。对于 Red Hat OpenShift Service on AWS 4.13 及更早的版本，这个功能不会改变。

要将自定义主机名用于路由，您必须通过创建规范名称 (CNAME) 记录来更新 DNS 供应商。您的 CNAME 记录应当将 OpenShift 规范路由器主机名映射到您的自定义域。OpenShift 规范路由器主机名在创建路由后在 *Route Details* 页面中显示。或者，也可以创建通配符 CNAME 记录，以将给定主机名的所有子域路由到集群的路由器。

2.3.4.2. 域验证证书

Red Hat OpenShift Service on AWS 包括集群中内部和外部服务所需的 TLS 安全证书。对于外部路由，每个集群中都提供并安装了两个不同的 TLS 通配符证书：一个用于 Web 控制台和路由默认主机名，另一个用于 API 端点。我们来加密是证书使用的证书颁发机构。集群内路由（如内部 API 端点）使用集群内置证书颁发机构签名的 TLS 证书，并需要每个 pod 中的 CA 捆绑包信任 TLS 证书。

2.3.4.3. 构建的自定义证书颁发机构

Red Hat OpenShift Service on AWS 支持在从镜像 registry 中拉取镜像时，使用自定义证书颁发机构来被构建信任。

2.3.4.4. 负载均衡器

Red Hat OpenShift Service on AWS 使用最多五个不同的负载均衡器：

- 集群内部的 control plane 负载均衡器，用于平衡内部集群通信的流量。

- 用于访问 OpenShift 和 Kubernetes API 的外部 control plane 负载均衡器。此负载均衡器可以在 OpenShift Cluster Manager 中被禁用。如果禁用了这个负载均衡器，红帽会重新配置 API DNS 以指向内部 control plane 负载均衡器。

- 为红帽保留由红帽保留的外部 control plane 负载均衡器。访问是严格控制的，只有来自白名单的堡垒主机的通信才可以进行。

- 默认外部路由器/入口负载均衡器，它是默认应用程序负载均衡器，由 URL 中的 **apps** 表示。默认负载均衡器可以在 OpenShift Cluster Manager 中配置，以便可以通过互联网公开访问，或者只有通过已存在的私有连接来私有访问。集群上的所有应用程序路由都会在这个默认路由器负载均衡器上公开，包括日志记录 UI、指标 API 和 registry 等集群服务。

- 可选：一个作为二级应用程序负载均衡器的二级路由器/入口负载均衡器，由 URL 中的 **apps2** 表示。辅助负载均衡器可以在 OpenShift Cluster Manager 中配置，以便可以通过互联网公开访问，或者只有通过已存在的私有连接来私有访问。如果为这个路由器负载均衡器配置了 **标签匹配**，则只有与此标签匹配的应用程序路由在此路由器负载均衡器上公开；否则，所有应用程序路由也会在此路由器负载均衡器上公开。

- 可选：服务的负载均衡器。为服务启用非 HTTP/SNI 流量和非标准端口。这些负载均衡器可以映射到在 AWS 上运行的服务，以启用高级入口功能，如非 HTTP/SNI 流量或使用非标准端口。每个 AWS 帐户都有一个配额，用于限制每个集群中可以使用的 Classic Load Balancer 数量。

2.3.4.5. 集群入口

项目管理员可以为许多不同的用途添加路由注解，包括通过 IP 允许列表进行入口控制。

也可以使用 **NetworkPolicy** 对象来更改 Ingress 策略，这利用了 **ovs-networkpolicy** 插件。这允许对入口网络策略进行完全控制到 pod 级别，包括在同一集群中的 pod 间，甚至在同一命名空间中。

所有集群入口流量都将通过定义的负载均衡器。云配置阻止对所有节点的直接访问。

2.3.4.6. 集群出口

通过 **EgressNetworkPolicy** 对象进行 Pod 出口流量控制可用于防止或限制 Red Hat OpenShift Service on AWS 中的出站流量。

需要来自 control plane 和基础架构节点的公共出站流量，并需要维护集群镜像安全性和集群监控。这要求 **0.0.0.0/0** 路由仅属于互联网网关；无法通过专用连接路由此范围。

OpenShift 4 集群使用 NAT 网关为离开集群的任何公共出站流量提供一个公共静态 IP。每个可用区都部署到接收不同的 NAT 网关，因此集群出口流量最多可存在 3 个唯一的静态 IP 地址。在集群中或未离开公共互联网的任何流量都不会通过 NAT 网关，并且具有属于源自于流量的来源 IP 地址的源 IP 地址。节点 IP 地址是动态的；因此，在访问私有资源时，客户不得依赖白名单各个 IP 地址。

客户可以通过在群集上运行 pod 并查询外部服务来确定其公共静态 IP 地址。例如：

```
$ oc run ip-lookup --image=busybox -i -t --restart=Never --rm -- /bin/sh -c "/bin/nslookup -type=a
myip.opendns.com resolver1.opendns.com | grep -E 'Address: [0-9.]+'"
```

2.3.4.7. 云网络配置

Red Hat OpenShift Service on AWS 允许通过 AWS 管理的技术配置私有网络连接，例如：

- VPN 连接

- VPC 对等

- 传输网关
- 直接连接

重要

红帽站点可靠性工程师(SRE)不监控私有网络连接。监控这些连接是客户的职责。

2.3.4.8. DNS 转发

对于具有私有云网络配置的 Red Hat OpenShift Service on AWS 集群的客户可以指定该专用连接上可用的内部 DNS 服务器，该服务器应查询用于明确提供的域。

2.3.4.9. 网络验证

当您将 Red Hat OpenShift Service on AWS 集群部署到现有的 Virtual Private Cloud (VPC)中，或使用对集群的新子网创建额外的机器池时，网络验证检查会自动运行。检查会验证您的网络配置并突出显示错误，允许您在部署前解决配置问题。

您还可以手动运行网络验证检查以验证现有集群的配置。

其他资源

- 有关网络验证检查的更多信息，请参阅 网络验证。

2.3.5. 存储

本节提供有关 Red Hat OpenShift Service on AWS 存储服务定义信息。

2.3.5.1. Encrypted-at-rest OS 和节点存储

control plane、基础架构和 worker 节点使用 encrypted-at-rest Amazon Elastic Block Store (Amazon EBS)存储。

2.3.5.2. encrypted-at-rest PV

默认情况下，用于 PV 的 EBS 卷是 encrypted-at-rest。

2.3.5.3. 块存储 (RWO)

持久性卷(PV)由 Amazon Elastic Block Store (Amazon EBS)支持，它们是 Read-Write-Once。

PV 每次只能附加到一个节点，并特定于置备的可用区。但是，PV 可以附加到可用区中的任何节点。

每个云供应商都有自己的限制，用于把 PV 附加到单一节点。详情请参阅 AWS 实例类型限值。

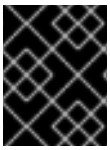
2.3.5.4. 共享存储 (RWX)

AWS CSI Driver 可用于为 Red Hat OpenShift Service on AWS 提供 RWX 支持。提供了一个 community Operator，以简化设置。详情请参阅 OpenShift Dedicated 和 Red Hat OpenShift Service on AWS 的 Amazon Elastic File Storage 设置。

2.3.6. 平台

本节提供有关 Red Hat OpenShift Service on AWS （ROSA）平台的定义信息。

2.3.6.1. 集群备份策略



重要

红帽不提供带有 STS 的 ROSA 集群的备份方法，这是默认设置。客户对应用程序和应用程序数据进行备份计划至关重要。下表只适用于使用 IAM 用户凭证创建的集群。

应用程序和应用程序数据备份不是 Red Hat OpenShift Service 的一部分。下表概述集群备份策略。

组件	快照频率	保留	备注
完整对象存储备份	每日	7 天	这是所有 Kubernetes 对象（如 etcd）的完整备份。在这个备份调度中没有备份持久性卷 (PV)。
	每周	30 天	
完整对象存储备份	每小时	24 小时	这是所有 Kubernetes 对象（如 etcd）的完整备份。这个备份调度中没有备份 PV。
节点根卷	Never	N/A	节点被视为是短期的。节点的 root 卷应当不重要。

2.3.6.2. 自动缩放

Red Hat OpenShift Service on AWS 提供了节点自动扩展功能。您可以配置自动扩展选项，以自动扩展集群中的机器数量。

其他资源

- 关于集群中的自动扩展节点

2.3.6.3. Daemonset

客户可以在 Red Hat OpenShift Service on AWS 上创建并运行 daemonset。要将 daemonset 限制为仅在 worker 节点上运行，请使用以下 **nodeSelector** ：

```
...
spec:
  nodeSelector:
    role: worker
...
```

2.3.6.4. 多个可用区

在多个可用区集群中，control plane 节点在可用区间分布，每个可用区需要至少一个 worker 节点。

2.3.6.5. 节点标签

红帽会在创建节点时创建自定义节点标签，目前无法在 Red Hat OpenShift Service on AWS 集群上更改。但是，创建新机器池时支持自定义标签。

2.3.6.6. OpenShift version

Red Hat OpenShift Service on AWS 作为服务运行，并与最新的 OpenShift Container Platform 版本保持最新状态。将计划升级到最新版本。

2.3.6.7. 升级

可以使用 ROSA CLI、**rosa** 或 OpenShift Cluster Manager 调度升级。

有关升级策略和步骤的更多信息，请参阅 AWS 生命周期的 Red Hat OpenShift Service 。

2.3.6.8. Windows 容器

目前，Red Hat OpenShift support for Windows Containers 在 Red Hat OpenShift Service on AWS 上不可用。

2.3.6.9. 容器引擎

Red Hat OpenShift Service on AWS 在 OpenShift 4 上运行，并使用 CRI-O 作为唯一可用的容器引擎。

2.3.6.10. 操作系统

Red Hat OpenShift Service on AWS 在 OpenShift 4 上运行，并使用 Red Hat CoreOS 作为所有 control plane 和 worker 节点的操作系统。

2.3.6.11. Red Hat Operator 支持

红帽工作负载通常是指通过 Operator Hub 提供的红帽提供的 Operator。红帽工作负载不由红帽 SRE 团队管理，必须部署到 worker 节点上。这些 Operator 可能需要额外的红帽订阅，并可能产生额外的云基础架构成本。这些红帽提供的 Operator 示例包括：

- Red Hat Quay
- Red Hat Advanced Cluster Management
- Red Hat Advanced Cluster Security
- Red Hat OpenShift Service Mesh
- OpenShift Serverless
- Red Hat OpenShift Logging
- Red Hat OpenShift Pipelines

2.3.6.12. Kubernetes Operator 支持

OperatorHub 市场中列出的所有 Operator 都应该可用于安装。这些 Operator 被视为客户工作负载，不受 Red Hat SRE 监控。

2.3.7. 安全性

本节提供有关 Red Hat OpenShift Service on AWS 安全服务定义信息。

2.3.7.1. 身份验证供应商

可以使用 OpenShift Cluster Manager 或集群创建过程或使用 ROSA CLI **rosa** 配置集群的身份验证。ROSA 不是一个身份提供程序，对集群的所有访问都必须由客户管理，作为其集成解决方案的一部分。支持同时使用同时调配的多个身份提供程序。支持以下身份提供程序：

- Github 或 GitHub Enterprise
- GitLab
- Google
- LDAP
- OpenID Connect
- htpasswd

2.3.7.2. 特权容器

特权容器可供具有 **cluster-admin** 角色的用户使用。使用特权容器作为 **cluster-admin** 取决于 Red Hat Enterprise Agreement 附录 4 (在线订阅服务)中的职责和排除备注。

2.3.7.3. 客户管理员用户

除了普通用户外，Red Hat OpenShift Service on AWS 还提供对名为 **dedicated-admin** 的 ROSA 特定组的访问权限。属于 **dedicated-admin** 组成员的任何用户：

- 具有集群中所有客户创建项目的管理员访问权限。
- 可以管理集群的资源配额和限值。
- 可以添加和管理 **NetworkPolicy** 对象。
- 可以查看集群中特定节点和 PV 的信息，包括调度程序信息。
- 可以访问集群上保留的 **dedicated-admin** 项目，它允许使用提升的特权创建服务帐户，同时还能够为集群上的项目更新默认限值和配额。
- 可以从 OperatorHub 安装 Operator，并执行所有 If **operators.coreos.com** API 组中的所有操作动词。

2.3.7.4. 集群管理角色

Red Hat OpenShift Service on AWS 管理员可对您的机构的集群具有 **cluster-admin** 角色的默认访问权限。使用 **cluster-admin** 角色登录到帐户时，用户可以增加运行特权安全上下文的权限。

2.3.7.5. 项目自助服务

默认情况下，所有用户都可以创建、更新和删除他们的项目。如果 **dedicated-admin** 组的成员从经过身份验证的用户移除 **self-provisioner** 角色，则可以受限制：

```
$ oc adm policy remove-cluster-role-from-group self-provisioner system:authenticated:oauth
```

通过应用可以恢复限制：

```
$ oc adm policy add-cluster-role-to-group self-provisioner system:authenticated:oauth
```

2.3.7.6. 法规合规性

有关最新合规性信息，*请参阅了解 ROSA 的进程和安全性* 中的 *Compliance* 表。

2.3.7.7. 网络安全性

使用 Red Hat OpenShift Service on AWS 时，AWS 对所有负载均衡器（即 AWS Shield）提供标准的 DDoS 保护。这对 Red Hat OpenShift Service on AWS 使用的所有面向公共的负载均衡器的用户级别为 3 和 4 的攻击提供了 95% 的保护。为来自 **haproxy** 路由器的 HTTP 请求添加 10 秒超时，以接收响应或连接关闭，以提供额外的保护。

2.3.7.8. etcd 加密

Red Hat OpenShift Service on AWS 中，control plane 存储会默认加密，这包括 etcd 卷的加密。这种存储级别加密通过云供应商的存储层提供。

您还可以启用 etcd 加密，加密 etcd 中的密钥值，而不是密钥。如果启用 etcd 加密，则会加密以下 Kubernetes API 服务器和 OpenShift API 服务器资源：

- Secrets
- 配置映射
- Routes
- OAuth 访问令牌
- OAuth 授权令牌

默认情况下不启用 etcd 加密功能，它只能在集群安装过程中启用。即使启用了 etcd 加密，则有权访问 control plane 节点或 **cluster-admin** 权限的任何人都可以访问 etcd 密钥值。

重要

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

2.3.8. 其他资源

- 有关最新合规性信息，请参阅了解 ROSA 的进程和安全性。
- 请参阅 ROSA 生命周期

2.4. RED HAT OPENSHIFT SERVICE ON AWS 更新生命周期

2.4.1. 概述

红帽为 Red Hat OpenShift Service on AWS 公布了它的产品生命周期，以便客户和合作伙伴有效地规划、部署和支持其应用程序。红帽发布这个生命周期，以尽可能提供透明性，并可能会在出现冲突时从这些政策做例外。

Red Hat OpenShift Service on AWS 是一个 Red Hat OpenShift 的受管实例，并维护一个独立的发行计划。有关受管产品的更多详细信息，请参阅 Red Hat OpenShift Service on AWS 服务定义。特定版本的安全公告和程序错误修复公告的可用性取决于 Red Hat OpenShift Container Platform 生命周期政策，并遵循 Red Hat OpenShift Service on AWS 维护计划。

其他资源

- Red Hat OpenShift Service on AWS 服务定义

2.4.2. 定义

表 2.1. 版本参考

版本格式	主	次	Patch	Major.minor.patch
	x	y	z	x.y.z
示例	4	5	21	4.5.21

主发行版本或 X-releases

称为*主发行版本*或 *X-releases* (X.y.z)。

例子

- "Major release 5" → 5.y.z
- "Major release 4" → 4.y.z
- "Major release 3" → 3.y.z

次发行版本或 Y-releases

称为*次发行版本*或 *Y-releases* (x.Y.z)。

例子

- "Minor release 4" → 4.4.z
- "次版本 5" → 4.5.z
- "Minor release 6" → 4.6.z

补丁版本或 Z-releases

称为*补丁版本*或*Z-releases* (x.y.Z)。

例子

- "Patch release 14 of minor release 5" → 4.5.14

- "Patch release 25 of minor release 5" → 4.5.25
- "Patch release 26 of minor release 6" → 4.6.26

2.4.3. 主发行版本 (X.y.z)

Red Hat OpenShift Service on AWS 的主版本（如版本 4）在后续主版本或产品停用后，支持一年。

示例

- 如果 Red Hat OpenShift Service on AWS 版本 5 在 1 月 1 日发布，则版本 4 可以在受管集群上持续运行 12 个月，直到 12 月 31 日为止。在这段时间后，集群需要升级或迁移到版本 5。

2.4.4. 次版本(x.Y.z)

从 4.8 OpenShift Container Platform 次版本开始，红帽会在给定次版本的正式发布后至少支持所有次版本的 16 个月。补丁版本不受支持周期的影响。

在支持期结束前，客户会收到 60、30 和 15 天通知。在支持周期结束前，集群必须升级到最旧支持的次版本的最新补丁版本，或者集群将进入 "Limited Support" 状态。

示例

1. 客户的集群当前在 4.13.8 上运行。4.13 次版本在 2023 年 5 月 17 日正式发布。
2. 2024 年 7 月 19 日、8 月 16 日和 9 月 2 日，客户会收到通知，如果集群还没有升级到受支持的次版本，则其集群将在 2024 年 9 月 17 日进入"有限支持"状态。
3. 集群必须在 2024 年 9 月 17 日前升级到 4.14 或更高版本。
4. 如果还没有执行升级，集群将标记为 "Limited Support" 状态。

其他资源

- Red Hat OpenShift Service on AWS 的有限支持状态

2.4.5. 补丁版本(x.y.Z)

在支持次版本的期间，红帽支持所有 OpenShift Container Platform 补丁版本，除非另有指定。

出于平台安全性和稳定性的原因，补丁版本可能会被弃用，这会阻止安装该版本并触发该发行版本的强制升级。

示例

1. 4.7.6 可发现包含关键 CVE。
2. 受 CVE 影响的任何发行版本都将从支持的补丁版本列表中删除。另外，任何运行 4.7.6 的集群都会被调度在 48 小时内自动升级。

2.4.6. 有限支持状态

当集群过渡到 *有限支持状*态时，红帽不再主动监控集群，SLA 将不再适用，并拒绝对 SLA 请求的学分。这并不意味着您不再有产品支持。在某些情况下，如果您修复了违反因素，集群可以返回完全支持的状态。但是，在其他情况下，您可能需要删除并重新创建集群。

集群可能会因为许多原因移至有限支持状态，包括以下情况：

如果您没有在生命周期结束前将集群升级到支持的版本

红帽不会在其生命周期结束后为版本提供任何运行时或 SLA 保证。要继续获得支持，请在生命周期结束前将集群升级到受支持的版本。如果您没有在生命周期结束前升级集群，集群会过渡到有限支持状态，直到升级到受支持的版本。
红帽提供了合理的商业支持，从不受支持的版本升级到受支持的版本。但是，如果支持的升级路径不再可用，您可能需要创建新集群并迁移您的工作负载。

如果您删除或替换任何由红帽安装和管理的 Red Hat OpenShift Service on AWS 组件或任何其他组件

如果使用了集群管理员权限，红帽不负责您的任何或授权用户的操作，包括影响基础架构服务、服务可用性或数据丢失的人。如果红帽检测到此类操作，集群可能会过渡到有限支持状态。红帽通知您的状态变化，您应该恢复操作或创建支持问题单来探索可能需要删除和重新创建集群的补救步骤。

如果您对可能造成集群移至有限支持状态或需要进一步帮助的特定操作有疑问，请打开支持票据。

2.4.7. 支持的版本例外策略

红帽保留添加或删除新的或现有版本的权利，或延迟即将发布的次版本，这些版本已确定有一个或多个关键生产影响了漏洞或安全问题，而不会提前通知。

2.4.8. 安装策略

虽然红帽建议安装最新的支持版本，但 Red Hat OpenShift Service on AWS 支持安装任何受支持的版本，如前面的策略所述。

2.4.9. 必须升级

如果一个关键(Critical)或重要的 CVE，或其他由红帽识别的错误有严重影响集群的安全性或稳定性，则客户必须在两个 工作日内 升级到下一个支持的补丁版本。

在极端情况下，基于红帽对环境的 CVE 的评估，红帽会通知客户有 两个工作日 来调度或手动将集群更新至最新的安全补丁版本。如果在两个工作日后没有执行更新，红帽会自动将集群升级到最新的安全补丁版本，以缓解潜在的安全漏洞或不稳定。https://access.redhat.com/articles/2623321如果客户通过 支持问题单 请求，红帽可能会自行决定临时延迟自动更新。

2.4.10. 生命周期日期

版本	公开发行（GA）	生命周期结束
4.15	2024 年 2 月 27 日	2025 年 6 月 30 日
4.14	2023 年 10 月 31 日	2025 年 2 月 28 日
4.13	2023 年 5 月 17 日	2024 年 9 月 17 日
4.12	2023 年 1 月 17 日	2024 年 7 月 17 日

版本	公开发行（GA）	生命周期结束
4.11	2022 年 8 月 10 日	2023 年 12 月 10 日
4.10	2022 年 3 月 10 日	2023 年 9 月 10 日
4.9	2021 年 10 月 18 日	2022 年 12 月 18 日
4.8	2021 年 7 月 27 日	2022 年 9 月 27 日

2.5. 带有托管 CONTROL PLANE (HCP)服务定义的 RED HAT OPENSHIFT SERVICE ON AWS (ROSA)

本文档概述了带有托管 control plane (HCP)管理的服务的 Red Hat OpenShift Service on AWS (ROSA)的服务定义。

2.5.1. 帐户管理

本节提供有关 AWS 帐户管理上 Red Hat OpenShift Service 的服务定义的信息。

2.5.1.1. 账单和定价

Red Hat OpenShift Service on AWS 会直接指向 Amazon Web Services (AWS)帐户。ROSA 定价基于使用，每年承诺或 3 年的承诺以便获得更大的折现。ROSA 的总成本由两个部分组成：

- ROSA 服务费用
- AWS 基础架构费用

如需更多详细信息，请访问 AWS 网站上的 Red Hat OpenShift Service on AWS 定价 页面。

2.5.1.2. 集群自助服务

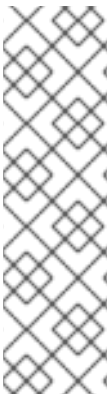
客户可以自助服务集群，包括但不限于：

- 创建集群
- 删除集群
- 添加或删除身份提供程序
- 从提升的组中添加或删除用户
- 配置集群隐私
- 添加或删除机器池并配置自动扩展
- 定义升级策略

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa** 执行这些自助服务任务。

2.5.1.3. 实例类型

所有带有 HCP 集群的 ROSA 至少需要 2 个 worker 节点。所有带有 HCP 集群的 ROSA 都支持最多 90 个 worker 节点。不支持通过云供应商控制台关闭底层基础架构，可能会导致数据丢失。



注意

每个 worker 节点上都会保留一个 vCPU 内核和 1 GiB 内存，并从可分配的资源中删除。运行底层平台所需的进程需要保留资源。这些进程包括系统守护进程，如 udev、kubelet 和容器运行时。保留的资源也考虑内核保留。

OpenShift Container Platform 核心系统（如审计日志聚合、指标集合、DNS、镜像 registry、SDN 等）可能会消耗额外的可分配资源来保持集群的稳定性和可维护性。所消耗的额外资源可能会因使用情况而异。

如需更多信息，请参阅 Kubernetes 文档。

其它资源

- Red Hat Operator 支持

2.5.1.4. AWS 实例类型

Red Hat OpenShift Service on AWS 提供了以下 worker 节点实例类型和大小：

例 2.11. 常规目的

- m5.metal (96† vCPU, 384 GiB)
- m5.xlarge (4 vCPU, 16 GiB)
- m5.2xlarge (8 vCPU, 32 GiB)
- m5.4xlarge (16 vCPU, 64 GiB)
- m5.8xlarge (32 vCPU, 128 GiB)
- m5.12xlarge (48 vCPU, 192 GiB)
- m5.16xlarge (64 vCPU, 256 GiB)
- m5.24xlarge (96 vCPU, 384 GiB)
- m5a.xlarge (4 vCPU, 16 GiB)
- m5a.2xlarge (8 vCPU, 32 GiB)
- m5a.4xlarge (16 vCPU, 64 GiB)
- m5a.8xlarge (32 vCPU, 128 GiB)
- m5a.12xlarge (48 vCPU, 192 GiB)
- m5a.16xlarge (64 vCPU, 256 GiB)
- m5a.24xlarge (96 vCPU, 384 GiB)

- m5dn.metal (96 vCPU, 384 GiB)
- m5zn.metal (48 vCPU, 192 GiB)
- m5d.metal (96† vCPU, 384 GiB)
- m5n.metal (96 vCPU, 384 GiB)
- m6a.metal (192 vCPU, 768 GiB)
- m6a.xlarge (4 vCPU, 16 GiB)
- m6a.2xlarge (8 vCPU, 32 GiB)
- m6a.4xlarge (16 vCPU, 64 GiB)
- m6a.8xlarge (32 vCPU, 128 GiB)
- m6a.12xlarge (48 vCPU, 192 GiB)
- m6a.16xlarge (64 vCPU, 256 GiB)
- m6a.24xlarge (96 vCPU, 384 GiB)
- m6a.32xlarge (128 vCPU, 512 GiB)
- m6a.48xlarge (192 vCPU, 768 GiB)
- m6i.metal (128 vCPU, 512 GiB)
- m6i.xlarge (4 vCPU, 16 GiB)
- m6i.2xlarge (8 vCPU, 32 GiB)
- m6i.4xlarge (16 vCPU, 64 GiB)
- m6i.8xlarge (32 vCPU, 128 GiB)
- m6i.12xlarge (48 vCPU, 192 GiB)
- m6i.16xlarge (64 vCPU, 256 GiB)
- m6i.24xlarge (96 vCPU， 384 GiB)
- m6i.32xlarge (128 vCPU, 512 GiB)
- m6id.xlarge (4 vCPU, 16 GiB)
- m6id.2xlarge (8 vCPU, 32 GiB)
- m6id.4xlarge (16 vCPU, 64 GiB)
- m6id.8xlarge (32 vCPU, 128 GiB)
- m6id.12xlarge (48 vCPU, 192 GiB)
- m6id.16xlarge (64 vCPU, 256 GiB)

- m6id.24xlarge (96 vCPU, 384 GiB)
- m6id.32xlarge (128 vCPU, 512 GiB)
- m6id.metal (128 vCPU, 512 GiB)
- m6idn.xlarge (4 vCPU, 16 GiB)
- m6idn.2xlarge (8 vCPU, 32 GiB)
- m6idn.4xlarge (16 vCPU, 64 GiB)
- m6idn.8xlarge (32 vCPU, 128 GiB)
- m6idn.12xlarge (48 vCPU, 192 GiB)
- m6idn.16xlarge (64 vCPU, 256 GiB)
- m6idn.24xlarge (96 vCPU, 384 GiB)
- m6idn.32xlarge (128 vCPU, 512 GiB)
- m6in.xlarge (4 vCPU, 16 GiB)
- m6in.2xlarge (8 vCPU, 32 GiB)
- m6in.4xlarge (16 vCPU, 64 GiB)
- m6in.8xlarge (32 vCPU, 128 GiB)
- m6in.12xlarge (48 vCPU, 192 GiB)
- m6in.16xlarge (64 vCPU, 256 GiB)
- m6in.24xlarge (96 vCPU, 384 GiB)
- m6in.32xlarge (128 vCPU, 512 GiB)
- m7a.xlarge (4 vCPU, 16 GiB)
- m7a.2xlarge (8 vCPU, 32 GiB)
- m7a.4xlarge (16 vCPU, 64 GiB)
- m7a.8xlarge (32 vCPU, 128 GiB)
- m7a.12xlarge (48 vCPU, 192 GiB)
- m7a.16xlarge (64 vCPU, 256 GiB)
- m7a.24xlarge (96 vCPU, 384 GiB)
- m7a.32xlarge (128 vCPU, 512 GiB)
- m7a.48xlarge (192 vCPU, 768 GiB)
- m7a.metal-48xl (192 vCPU, 768 GiB)

- m7i-flex.2xlarge (8 vCPU, 32 GiB)
- m7i-flex.4xlarge (16 vCPU, 64 GiB)
- m7i-flex.8xlarge (32 vCPU, 128 GiB)
- m7i-flex.xlarge (4 vCPU, 16 GiB)
- m7i.xlarge (4 vCPU, 16 GiB)
- m7i.2xlarge (8 vCPU, 32 GiB)
- m7i.4xlarge (16 vCPU, 64 GiB)
- m7i.8xlarge (32 vCPU, 128 GiB)
- m7i.12xlarge (48 vCPU, 192 GiB)
- m7i.16xlarge (64 vCPU, 256 GiB)
- m7i.24xlarge (96 vCPU, 384 GiB)
- m7i.48xlarge (192 vCPU, 768 GiB)
- m7i.metal-24xl (96 vCPU, 384 GiB)
- m7i.metal-48xl (192 vCPU, 768 GiB)

这些实例类型在 48 个物理内核中提供 96 个逻辑处理器。它们在两个物理 Intel 插槽的单台服务器上运行。

例 2.12. Burstable 常规目的

- t3.xlarge (4 vCPU, 16 GiB)
- t3.2xlarge (8 vCPU, 32 GiB)
- t3a.xlarge (4 vCPU, 16 GiB)
- t3a.2xlarge (8 vCPU, 32 GiB)

例 2.13. 内存密集型

- x1.16xlarge (64 vCPU, 976 GiB)
- x1.32xlarge (128 vCPU, 1,952 GiB)
- x1e.xlarge (4 vCPU, 122 GiB)
- x1e.2xlarge (8 vCPU, 244 GiB)
- x1e.4xlarge (16 vCPU, 488 GiB)
- x1e.8xlarge (32 vCPU, 976 GiB)

- x1e.16xlarge (64 vCPU, 1,952 GiB)
- x1e.32xlarge (128 vCPU, 3,904 GiB)
- x2idn.16xlarge (64 vCPU, 1,024 GiB)
- x2idn.24xlarge (96 vCPU, 1,536 GiB)
- x2idn.32xlarge (128 vCPU, 2,048 GiB)
- x2iedn.xlarge (4 vCPU, 128 GiB)
- x2iedn.2xlarge (8 vCPU, 256 GiB)
- x2iedn.4xlarge (16 vCPU, 512 GiB)
- x2iedn.8xlarge (32 vCPU, 1,024 GiB)
- x2iedn.16xlarge (64 vCPU, 2,048 GiB)
- x2iedn.24xlarge (96 vCPU, 3,072 GiB)
- x2iedn.32xlarge (128 vCPU, 4,096 GiB)
- x2iezn.metal (48 vCPU, 1,536 GiB)
- x2iezn.2xlarge (8 vCPU, 256 GiB)
- x2iezn.4xlarge (16vCPU, 512 GiB)
- x2iezn.6xlarge (24vCPU, 768 GiB)
- x2iezn.8xlarge (32vCPU, 1,024 GiB)
- x2iezn.12xlarge (48vCPU, 1,536 GiB)
- x2idn.metal (128vCPU, 2,048 GiB)
- x2iedn.metal (128vCPU, 4,096 GiB)

例 2.14. 内存优化

- r4.xlarge (4 vCPU, 30.5 GiB)
- r4.2xlarge (8 vCPU, 61 GiB)
- r4.4xlarge (16 vCPU, 122 GiB)
- r4.8xlarge (32 vCPU, 244 GiB)
- r4.16xlarge (64 vCPU, 488 GiB)
- r5.metal (96† vCPU, 768 GiB)
- r5.xlarge (4 vCPU, 32 GiB)
- r5.2xlarge (8 vCPU, 64 GiB)

- r5.4xlarge (16 vCPU, 128 GiB)
- r5.8xlarge (32 vCPU, 256 GiB)
- r5.12xlarge (48 vCPU, 384 GiB)
- r5.16xlarge (64 vCPU, 512 GiB)
- r5.24xlarge (96 vCPU, 768 GiB)
- r5a.xlarge (4 vCPU, 32 GiB)
- r5a.2xlarge (8 vCPU, 64 GiB)
- r5a.4xlarge (16 vCPU, 128 GiB)
- r5a.8xlarge (32 vCPU, 256 GiB)
- r5a.12xlarge (48 vCPU, 384 GiB)
- r5a.16xlarge (64 vCPU, 512 GiB)
- r5a.24xlarge (96 vCPU, 768 GiB)
- r5ad.xlarge (4 vCPU, 32 GiB)
- r5ad.2xlarge (8 vCPU, 64 GiB)
- r5ad.4xlarge (16 vCPU, 128 GiB)
- r5ad.8xlarge (32 vCPU, 256 GiB)
- r5ad.12xlarge (48 vCPU, 384 GiB)
- r5ad.16xlarge (64 vCPU, 512 GiB)
- r5ad.24xlarge (96 vCPU, 768 GiB)
- r5b.metal (96 768 GiB)
- r5b.xlarge (4 vCPU, 32 GiB)
- r5b.2xlarge (8 vCPU, 364 GiB)
- r5b.4xlarge (16 vCPU, 3,128 GiB)
- r5b.8xlarge (32 vCPU, 3,256 GiB)
- r5b.12xlarge (48 vCPU, 3,384 GiB)
- r5b.16xlarge (64 vCPU, 3,512 GiB)
- r5b.24xlarge (96 vCPU, 3,768 GiB)
- r5d.metal (96† vCPU, 768 GiB)
- r5d.xlarge (4 vCPU, 32 GiB)

- r5d.2xlarge (8 vCPU, 64 GiB)
- r5d.4xlarge (16 vCPU, 128 GiB)
- r5d.8xlarge (32 vCPU, 256 GiB)
- r5d.12xlarge (48 vCPU, 384 GiB)
- r5d.16xlarge (64 vCPU, 512 GiB)
- r5d.24xlarge (96 vCPU, 768 GiB)
- r5n.metal (96 vCPU, 768 GiB)
- r5n.xlarge (4 vCPU, 32 GiB)
- r5n.2xlarge (8 vCPU, 64 GiB)
- r5n.4xlarge (16 vCPU, 128 GiB)
- r5n.8xlarge (32 vCPU, 256 GiB)
- r5n.12xlarge (48 vCPU, 384 GiB)
- r5n.16xlarge (64 vCPU, 512 GiB)
- r5n.24xlarge (96 vCPU, 768 GiB)
- r5dn.metal (96 vCPU, 768 GiB)
- r5dn.xlarge (4 vCPU, 32 GiB)
- r5dn.2xlarge (8 vCPU, 64 GiB)
- r5dn.4xlarge (16 vCPU, 128 GiB)
- r5dn.8xlarge (32 vCPU, 256 GiB)
- r5dn.12xlarge (48 vCPU, 384 GiB)
- r5dn.16xlarge (64 vCPU, 512 GiB)
- r5dn.24xlarge (96 vCPU, 768 GiB)
- r6a.xlarge (4 vCPU, 32 GiB)
- r6a.2xlarge (8 vCPU, 64 GiB)
- r6a.4xlarge (16 vCPU, 128 GiB)
- r6a.8xlarge (32 vCPU, 256 GiB)
- r6a.12xlarge (48 vCPU, 384 GiB)
- r6a.16xlarge (64 vCPU, 512 GiB)
- r6a.24xlarge (96 vCPU, 768 GiB)

- r6a.32xlarge (128 vCPU, 1,024 GiB)
- r6a.48xlarge (192 vCPU, 1,536 GiB)
- r6i.metal (128 vCPU, 1,024 GiB)
- r6i.xlarge (4 vCPU, 32 GiB)
- r6i.2xlarge (8 vCPU, 64 GiB)
- r6i.4xlarge (16 vCPU, 128 GiB)
- r6i.8xlarge (32 vCPU，256 GiB)
- r6i.12xlarge (48 vCPU, 384 GiB)
- r6i.16xlarge (64 vCPU, 512 GiB)
- r6i.24xlarge (96 vCPU, 768 GiB)
- r6i.32xlarge (128 vCPU，1,024 GiB)
- r6id.metal (128 vCPU, 1,024 GiB)
- r6id.xlarge (4 vCPU, 32 GiB)
- r6id.2xlarge (8 vCPU, 64 GiB)
- r6id.4xlarge (16 vCPU, 128 GiB)
- r6id.8xlarge (32 vCPU, 256 GiB)
- r6id.12xlarge (48 vCPU, 384 GiB)
- r6id.16xlarge (64 vCPU, 512 GiB)
- r6id.24xlarge (96 vCPU, 768 GiB)
- r6id.32xlarge (128 vCPU, 1,024 GiB)
- r6idn.12xlarge (48 vCPU, 384 GiB)
- r6idn.16xlarge (64 vCPU, 512 GiB)
- r6idn.24xlarge (96 vCPU, 768 GiB)
- r6idn.2xlarge (8 vCPU, 64 GiB)
- r6idn.32xlarge (128 vCPU, 1,024 GiB)
- r6idn.4xlarge (16 vCPU, 128 GiB)
- r6idn.8xlarge (32 vCPU, 256 GiB)
- r6idn.xlarge (4 vCPU, 32 GiB)
- r6in.12xlarge (48 vCPU, 384 GiB)

- r6in.16xlarge (64 vCPU, 512 GiB)
- r6in.24xlarge (96 vCPU, 768 GiB)
- r6in.2xlarge (8 vCPU, 64 GiB)
- r6in.32xlarge (128 vCPU, 1,024 GiB)
- r6in.4xlarge (16 vCPU, 128 GiB)
- r6in.8xlarge (32 vCPU, 256 GiB)
- r6in.xlarge (4 vCPU, 32 GiB)
- r7iz.xlarge (4 vCPU, 32 GiB)
- r7iz.2xlarge (8 vCPU, 64 GiB)
- r7iz.4xlarge (16 vCPU, 128 GiB)
- r7iz.8xlarge (32 vCPU, 256 GiB)
- r7iz.12xlarge (48 vCPU, 384 GiB)
- r7iz.16xlarge (64 vCPU, 512 GiB)
- r7iz.32xlarge (128 vCPU, 1024 GiB)
- r7iz.metal-16xl (64 vCPU, 512 GiB)
- r7iz.metal-32xl (128 vCPU, 1,024 GiB)
- z1d.metal (48 vCPU, 384 GiB)
- z1d.xlarge (4 vCPU, 32 GiB)
- z1d.2xlarge (8 vCPU, 64 GiB)
- z1d.3xlarge (12 vCPU, 96 GiB)
- z1d.6xlarge (24 vCPU, 192 GiB)
- z1d.12xlarge (48 vCPU, 384 GiB)

这些实例类型在 48 个物理内核中提供 96 个逻辑处理器。它们在两个物理 Intel 插槽的单台服务器上运行。

这个实例类型在 24 个物理内核中提供 48 个逻辑处理器。

例 2.15. 加速计算

- p3.2xlarge (8 vCPU, 61 GiB)
- p3.8xlarge (32 vCPU, 244 GiB)
- p3.16xlarge (64 vCPU, 488 GiB)

- p3dn.24xlarge (96 vCPU, 768 GiB)
- p4d.24xlarge (96 vCPU, 1,152 GiB)
- p4de.24xlarge (96 vCPU, 1,152 GiB)
- p5.48xlarge (192 vCPU, 2,048 GiB)
- g4dn.xlarge (4 vCPU, 16 GiB)
- g4dn.2xlarge (8 vCPU, 32 GiB)
- g4dn.4xlarge (16 vCPU, 64 GiB)
- g4dn.8xlarge (32 vCPU, 128 GiB)
- g4dn.12xlarge (48 vCPU, 192 GiB)
- g4dn.16xlarge (64 vCPU, 256 GiB)
- g4dn.metal (96 vCPU, 384 GiB)
- g5.xlarge (4 vCPU, 16 GiB)
- g5.2xlarge (8 vCPU, 32 GiB)
- g5.4xlarge (16 vCPU, 64 GiB)
- g5.8xlarge (32 vCPU, 128 GiB)
- g5.16xlarge (64 vCPU, 256 GiB)
- g5.12xlarge (48 vCPU, 192 GiB)
- g5.24xlarge (96 vCPU, 384 GiB)
- g5.48xlarge (192 vCPU, 768 GiB)
- dl1.24xlarge (96 vCPU, 768 GiB)

† 特定于 Intel；不被 Nvidia 支持

对 GPU 实例类型软件堆栈的支持由 AWS 提供。确保您的 AWS 服务配额可以容纳所需的 GPU 实例类型。

例 2.16. 计算优化

- c5.metal (96 vCPU, 192 GiB)
- c5.xlarge (4 vCPU, 8 GiB)
- c5.2xlarge (8 vCPU, 16 GiB)
- c5.4xlarge (16 vCPU, 32 GiB)
- c5.9xlarge (36 vCPU, 72 GiB)

- c5.12xlarge (48 vCPU, 96 GiB)
- c5.18xlarge (72 vCPU, 144 GiB)
- c5.24xlarge (96 vCPU, 192 GiB)
- c5d.metal (96 vCPU, 192 GiB)
- c5d.xlarge (4 vCPU, 8 GiB)
- c5d.2xlarge (8 vCPU, 16 GiB)
- c5d.4xlarge (16 vCPU, 32 GiB)
- c5d.9xlarge (36 vCPU, 72 GiB)
- c5d.12xlarge (48 vCPU, 96 GiB)
- c5d.18xlarge (72 vCPU, 144 GiB)
- c5d.24xlarge (96 vCPU, 192 GiB)
- c5a.xlarge (4 vCPU, 8 GiB)
- c5a.2xlarge (8 vCPU, 16 GiB)
- c5a.4xlarge (16 vCPU, 32 GiB)
- c5a.8xlarge (32 vCPU, 64 GiB)
- c5a.12xlarge (48 vCPU, 96 GiB)
- c5a.16xlarge (64 vCPU, 128 GiB)
- c5a.24xlarge (96 vCPU, 192 GiB)
- c5ad.xlarge (4 vCPU, 8 GiB)
- c5ad.2xlarge (8 vCPU, 16 GiB)
- c5ad.4xlarge (16 vCPU, 32 GiB)
- c5ad.8xlarge (32 vCPU, 64 GiB)
- c5ad.12xlarge (48 vCPU, 96 GiB)
- c5ad.16xlarge (64 vCPU, 128 GiB)
- c5ad.24xlarge (96 vCPU, 192 GiB)
- c5n.metal (72 vCPU, 192 GiB)
- c5n.xlarge (4 vCPU, 10.5 GiB)
- c5n.2xlarge (8 vCPU, 21 GiB)
- c5n.4xlarge (16 vCPU, 42 GiB)

- c5n.9xlarge (36 vCPU, 96 GiB)
- c5n.18xlarge (72 vCPU, 192 GiB)
- c6a.xlarge (4 vCPU, 8 GiB)
- c6a.2xlarge (8 vCPU, 16 GiB)
- c6a.4xlarge (16 vCPU, 32 GiB)
- c6a.8xlarge (32 vCPU, 64 GiB)
- c6a.12xlarge (48 vCPU, 96 GiB)
- c6a.16xlarge (64 vCPU, 128 GiB)
- c6a.24xlarge (96 vCPU, 192 GiB)
- c6a.32xlarge (128 vCPU, 256 GiB)
- c6a.48xlarge (192 vCPU, 384 GiB)
- c6i.metal (128 vCPU, 256 GiB)
- c6i.xlarge (4 vCPU, 8 GiB)
- c6i.2xlarge (8 vCPU, 16 GiB)
- c6i.4xlarge (16 vCPU, 32 GiB)
- c6i.8xlarge (32 vCPU, 64 GiB)
- c6i.12xlarge (48 vCPU， 96 GiB)
- c6i.16xlarge (64 vCPU, 128 GiB)
- c6i.24xlarge (96 vCPU, 192 GiB)
- c6i.32xlarge (128 vCPU, 256 GiB)
- c6id.metal (128 vCPU, 256 GiB)
- c6id.xlarge (4 vCPU, 8 GiB)
- c6id.2xlarge (8 vCPU, 16 GiB)
- c6id.4xlarge (16 vCPU, 32 GiB)
- c6id.8xlarge (32 vCPU, 64 GiB)
- c6id.12xlarge (48 vCPU, 96 GiB)
- c6id.16xlarge (64 vCPU, 128 GiB)
- c6id.24xlarge (96 vCPU, 192 GiB)
- c6id.32xlarge (128 vCPU, 256 GiB)

- c6in.12xlarge (48 vCPU, 96 GiB)
- c6in.16xlarge (64 vCPU, 128 GiB)
- c6in.24xlarge (96 vCPU, 192 GiB)
- c6in.2xlarge (8 vCPU, 16 GiB)
- c6in.32xlarge (128 vCPU, 256 GiB)
- c6in.4xlarge (16 vCPU, 32 GiB)
- c6in.8xlarge (32 vCPU, 64 GiB)
- c6in.xlarge (4 vCPU, 8 GiB)
- m5zn.12xlarge (48 vCPU, 192 GiB)
- m5zn.2xlarge (8 vCPU, 32 GiB)
- m5zn.3xlarge (16 vCPU, 48 GiB)
- m5zn.6xlarge (32 vCPU, 96 GiB)
- m5zn.xlarge (4 vCPU, 16 GiB)

例 2.17. 存储优化

- c5ad.12xlarge (48 vCPU, 96 GiB)
- c5ad.16xlarge (64 vCPU, 128 GiB)
- c5ad.24xlarge (96 vCPU, 192 GiB)
- c5ad.2xlarge (8 vCPU, 16 GiB)
- c5ad.4xlarge (16 vCPU, 32 GiB)
- c5ad.8xlarge (32 vCPU, 64 GiB)
- c5ad.xlarge (4 vCPU, 8 GiB)
- i3.metal (72† vCPU, 512 GiB)
- i3.xlarge (4 vCPU, 30.5 GiB)
- i3.2xlarge (8 vCPU, 61 GiB)
- i3.4xlarge (16 vCPU, 122 GiB)
- i3.8xlarge (32 vCPU, 244 GiB)
- i3.16xlarge (64 vCPU, 488 GiB)
- i3en.metal (96 vCPU, 768 GiB)
- i3en.xlarge (4 vCPU, 32 GiB)

- i3en.2xlarge (8 vCPU, 64 GiB)
- i3en.3xlarge (12 vCPU, 96 GiB)
- i3en.6xlarge (24 vCPU, 192 GiB)
- i3en.12xlarge (48 vCPU, 384 GiB)
- i3en.24xlarge (96 vCPU, 768 GiB)
- i4i.xlarge (4 vCPU, 32 GiB)
- i4i.2xlarge (8 vCPU, 64 GiB)
- i4i.4xlarge (16 vCPU, 128 GiB)
- i4i.8xlarge (32 vCPU, 256 GiB)
- i4i.12xlarge (48 vCPU, 384 GiB)
- i4i.16xlarge (64 vCPU, 512 GiB)
- i4i.24xlarge (96 vCPU, 768 GiB)
- i4i.32xlarge (128 vCPU, 1,024 GiB)
- i4i.metal (128 vCPU, 1,024 GiB)
- m5ad.xlarge (4 vCPU, 16 GiB)
- m5ad.2xlarge (8 vCPU, 32 GiB)
- m5ad.4xlarge (16 vCPU, 64 GiB)
- m5ad.8xlarge (32 vCPU, 128 GiB)
- m5ad.12xlarge (48 vCPU, 192 GiB)
- m5ad.16xlarge (64 vCPU, 256 GiB)
- m5ad.24xlarge (96 vCPU, 384 GiB)
- m5d.xlarge (4 vCPU, 16 GiB)
- m5d.2xlarge (8 vCPU, 32 GiB)
- m5d.4xlarge (16 vCPU, 64 GiB)
- m5d.8xlarge (32 vCPU, 28 GiB)
- m5d.12xlarge (48 vCPU, 192 GiB)
- m5d.16xlarge (64 vCPU, 256 GiB)
- m5d.24xlarge (96 vCPU, 384 GiB)

这个实例类型在 36 个物理内核中提供 72 个逻辑处理器。

注意

虚拟实例类型初始化速度快于 ".metal" 实例类型。

例 2.18. 高内存

- U-3tb1.56xlarge (224 vCPU, 3,072 GiB)
- U-6tb1.56xlarge (224 vCPU, 6,144 GiB)
- U-6tb1.112xlarge (448 vCPU, 6,144 GiB)
- u-6tb1.metal (448 vCPU, 6,144 GiB)
- U-9tb1.112xlarge (448 vCPU, 9,216 GiB)
- U-9tb1.metal (448 vCPU, 9,216 GiB)
- U-12tb1.112xlarge (448 vCPU, 12,288 GiB)
- U-12tb1.metal (448 vCPU, 12,288 GiB)
- u-18tb1.metal (448 vCPU, 18,432 GiB)
- U-24tb1.metal (448 vCPU, 24,576 GiB)
- U-24tb1.112xlarge (448 vCPU, 24,576 GiB)

例 2.19. 网络优化

- c5n.xlarge (4 vCPU, 10.5 GiB)
- c5n.2xlarge (8 vCPU, 21 GiB)
- c5n.4xlarge (16 vCPU, 42 GiB)
- c5n.9xlarge (36 vCPU, 96 GiB)
- c5n.18xlarge (72 vCPU, 192 GiB)
- m5dn.xlarge (4 vCPU, 16 GiB)
- m5dn.2xlarge (8 vCPU, 32 GiB)
- m5dn.4xlarge (16 vCPU, 64 GiB)
- m5dn.8xlarge (32 vCPU, 128 GiB)
- m5dn.12xlarge (48 vCPU, 192 GiB)
- m5dn.16xlarge (64 vCPU, 256 GiB)
- m5dn.24xlarge (96 vCPU, 384 GiB)
- m5n.12xlarge (48 vCPU, 192 GiB)

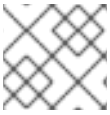
- m5n.16xlarge (64 vCPU, 256 GiB)
- m5n.24xlarge (96 vCPU, 384 GiB)
- m5n.xlarge (4 vCPU, 16 GiB)
- m5n.2xlarge (8 vCPU, 32 GiB)
- m5n.4xlarge (16 vCPU, 64 GiB)
- m5n.8xlarge (32 vCPU, 128 GiB)

其它资源

- AWS 实例类型

2.5.1.5. 地区和可用性区域

以下 AWS 区域目前可用于使用 HCP 的 ROSA。



注意

中国的区域不受支持，无论它们对 OpenShift 4 的支持是什么。

注意

对于 GovCloud (US)区域，您必须提交 Red Hat OpenShift Service on AWS (ROSA) FedRAMP 的访问请求。

GovCloud (US)区域只在 ROSA Classic 集群中被支持。

例 2.20. AWS 区域

- us-east-1（北弗吉尼亚）
- us-east-2（俄亥俄）
- us-west-2（俄勒冈）
- af-south-1 (Cape Town, AWS opt-in required)
- ap-east-1 (Hong Kong, AWS opt-in required)
- ap-south-2 (Hyderabad, AWS opt-in required)
- ap-southeast-3(Jakarta, AWS opt-in required)
- ap-southeast-4 (Melbourne, AWS opt-in required)
- ap-south-1（孟买）
- ap-northeast-3 (Osaka)
- ap-northeast-2 （首尔）

- ap-southeast-1（新加坡）
- ap-southeast-2（悉尼）
- ap-northeast-1（东京）
- ca-central-1 (Central Canada)
- eu-central-1（法拉克福）
- eu-north-1（斯德哥尔摩）
- eu-west-1（爱尔兰）
- eu-west-2（伦敦）
- eu-south-1 (Milan、AWS opt-in required)
- eu-west-3（巴黎）
- eu-south-2 (Spain)
- eu-central-2 (Zurich, AWS opt-in required)
- me-south-1 (Bahrain, AWS opt-in required)
- me-central-1 (UAE, AWS opt-in required)
- sa-east-1 （圣保罗）

多个可用区集群只能部署到至少 3 个可用区的区域。如需更多信息，请参阅 AWS 文档中的 Regions 和 Availability Zones 部分。

每个带有 HCP 集群的新 ROSA 安装在一个区域中已存在的虚拟私有云(VPC)中，可以选择部署到给定区域的可用区总数。这提供了集群级别的网络和资源隔离，并启用 cloud-provider VPC 设置，如 VPN 连接和 VPC Peering。持久性卷(PV)由 Amazon Elastic Block Storage (Amazon EBS)支持，并特定于置备的可用区。在将关联的 pod 资源分配给特定的可用区前，持久性卷声明(PVC)不会绑定到卷，以防止不可调度的 pod。特定于可用区的资源只可供同一可用区中的资源使用。

警告

部署集群后无法更改区域。

其它资源

- Red Hat OpenShift Service on AWS 端点和配额

2.5.1.6. 本地区域

带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)不支持使用 AWS Local Zones。

2.5.1.7. 服务等级协议 (SLA)

服务本身的任何 SLA 在 Red Hat Enterprise Agreement 附录 4（在线订阅服务）的附录 4 中定义。

2.5.1.8. 有限支持状态

当集群过渡到 *有限支持状态*时，红帽不再主动监控集群，SLA 将不再适用，并拒绝对 SLA 请求的学分。这并不意味着您不再有产品支持。在某些情况下，如果您修复了违反因素，集群可以返回完全支持的状态。但是，在其他情况下，您可能需要删除并重新创建集群。

集群可能会因为许多原因移至有限支持状态，包括以下情况：

如果您删除或替换任何由红帽安装和管理的 Red Hat OpenShift Service on AWS 组件或任何其他组件

如果使用了集群管理员权限，红帽不负责您的任何或授权用户的操作，包括影响基础架构服务、服务可用性或数据丢失的人。如果红帽检测到此类操作，集群可能会过渡到有限支持状态。红帽通知您的状态变化，您应该恢复操作或创建支持问题单来探索可能需要删除和重新创建集群的补救步骤。

如果您对可能造成集群移至有限支持状态或需要进一步帮助的特定操作有疑问，请打开支持票据。
：!rosa-with-hcp:

2.5.1.9. 支持

Red Hat OpenShift Service on AWS 包括红帽高级支持，可以使用 红帽客户门户网站 访问。

如需支持响应时间，请参阅 AWS SLA 上的 Red Hat OpenShift Service。

AWS 支持取决于客户对 AWS 的现有支持合同。

2.5.2. 日志记录

Red Hat OpenShift Service on AW 为 Amazon (AWS) CloudWatch 提供可选集成日志转发。

2.5.2.1. 集群日志记录

如果启用了集成，可以通过 AWS CloudWatch 集群审计日志。如果没有启用集成，您可以通过打开支持问题单来请求审计日志。

2.5.2.2. 应用程序日志记录

发送到 **STDOUT** 的应用程序日志由 Fluentd 收集，并通过集群日志记录堆栈转发到 AWS CloudWatch（如果已安装）。

2.5.3. 监控

本节提供有关 Red Hat OpenShift Service on AWS 监控的服务定义信息。

2.5.3.1. 集群指标

Red Hat OpenShift Service on AWS 集群上带有集成 Prometheus 堆栈，用于集群监控，包括 CPU、内存和基于网络的指标。这可以通过 Web 控制台访问。这些指标还允许由 Red Hat OpenShift Service on AWS 用户提供的 CPU 或内存指标进行 pod 横向自动扩展。

2.5.3.2. 集群通知

集群通知是有关集群状态、健康或性能的信息。

集群通知是 Red Hat Site Reliability Engineering (SRE)与您有关受管集群健康状况的主要方法。SRE 也可能使用集群通知来提示您执行操作，以解决或防止集群出现问题。

集群所有者和管理员必须定期检查和操作集群通知，以确保集群保持健康且受支持。

您可以在集群的 **Cluster history** 选项卡中查看 Red Hat Hybrid Cloud Console 中的集群通知。默认情况下，只有集群所有者接收集群通知作为电子邮件。如果其他用户需要接收集群通知电子邮件，请将每个用户添加为集群的通知联系人。

2.5.4. 网络

本节提供有关 Red Hat OpenShift Service on AWS 网络服务定义信息。

2.5.4.1. 应用程序自定义域

警告

从 Red Hat OpenShift Service on AWS 4.14 开始，自定义域 Operator 已被弃用。要在 AWS 4.14 或更高版本的 Red Hat OpenShift Service 中管理 Ingress，请使用 Ingress Operator。对于 Red Hat OpenShift Service on AWS 4.13 及更早的版本，这个功能不会改变。

要将自定义主机名用于路由，您必须通过创建规范名称 (CNAME) 记录来更新 DNS 供应商。您的 CNAME 记录应当将 OpenShift 规范路由器主机名映射到您的自定义域。OpenShift 规范路由器主机名在创建路由后在 *Route Details* 页面中显示。或者，也可以创建通配符 CNAME 记录，以将给定主机名的所有子域路由到集群的路由器。

2.5.4.2. 域验证证书

Red Hat OpenShift Service on AWS 包括集群中内部和外部服务所需的 TLS 安全证书。对于外部路由，每个集群中都提供并安装了两个不同的 TLS 通配符证书：一个用于 Web 控制台和路由默认主机名，另一个用于 API 端点。我们来加密是证书使用的证书颁发机构。集群内路由（如内部 API 端点）使用集群内置证书颁发机构签名的 TLS 证书，并需要每个 pod 中的 CA 捆绑包信任 TLS 证书。

2.5.4.3. 构建的自定义证书颁发机构

Red Hat OpenShift Service on AWS 支持在从镜像 registry 中拉取镜像时，使用自定义证书颁发机构来被构建信任。

2.5.4.4. 负载均衡器

带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)只会从默认入口控制器部署负载均衡器。客户可以选择为二级入口控制器或服务负载均衡器部署所有其他负载均衡器。

2.5.4.5. 集群入口

项目管理员可以为许多不同的用途添加路由注解，包括通过 IP 允许列表进行入口控制。

也可以使用 **NetworkPolicy** 对象来更改 Ingress 策略，这利用了 **ovs-networkpolicy** 插件。这允许对入口网络策略进行完全控制到 pod 级别，包括在同一集群中的 pod 间，甚至在同一命名空间中。

所有集群入口流量都将通过定义的负载均衡器。云配置阻止对所有节点的直接访问。

2.5.4.6. 集群出口

通过 **EgressNetworkPolicy** 对象进行 Pod 出口流量控制可用于防止或限制带有托管 control plane (HCP) 的 Red Hat OpenShift Service on AWS (ROSA)中的出站流量。

2.5.4.7. 云网络配置

Red Hat OpenShift Service on AWS 允许通过 AWS 管理的技术配置私有网络连接，例如：

- VPN 连接
- VPC 对等
- 传输网关
- 直接连接

重要

红帽站点可靠性工程师(SRE)不监控私有网络连接。监控这些连接是客户的职责。

2.5.4.8. DNS 转发

对于具有私有云网络配置的 Red Hat OpenShift Service on AWS 集群的客户可以指定该专用连接上可用的内部 DNS 服务器，该服务器应查询用于明确提供的域。

2.5.4.9. 网络验证

当您将 Red Hat OpenShift Service on AWS 集群部署到现有的 Virtual Private Cloud (VPC)中，或使用对集群的新子网创建额外的机器池时，网络验证检查会自动运行。检查会验证您的网络配置并突出显示错误，允许您在部署前解决配置问题。

您还可以手动运行网络验证检查以验证现有集群的配置。：!rosa-with-hcp:

其他资源

- 有关网络验证检查的更多信息，请参阅 网络验证。

2.5.5. 存储

本节提供有关带有托管 control plane (HCP)存储的 Red Hat OpenShift Service on AWS (ROSA)的服务定义信息。

2.5.5.1. Encrypted-at-rest OS 和节点存储

Worker 节点使用 encrypted-at-rest Amazon Elastic Block Store (Amazon EBS)存储。

2.5.5.2. encrypted-at-rest PV

默认情况下，用于 PV 的 EBS 卷是 encrypted-at-rest。

2.5.5.3. 块存储 (RWO)

持久性卷(PV)由 Amazon Elastic Block Store (Amazon EBS)支持，它们是 Read-Write-Once。

PV 每次只能附加到一个节点，并特定于置备的可用区。但是，PV 可以附加到可用区中的任何节点。

每个云供应商都有自己的限制，用于把 PV 附加到单一节点。详情请参阅 AWS 实例类型限值。

2.5.5.4. 共享存储 (RWX)

AWS CSI Driver 可用于为带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)提供 RWX 支持。提供了一个 community Operator，以简化设置。详情请参阅 OpenShift Dedicated 和 Red Hat OpenShift Service on AWS 的 Amazon Elastic File Storage 设置。

2.5.6. 平台

本节提供有关带有托管 control plane (HCP)平台的 Red Hat OpenShift Service on AWS (ROSA)的服务定义信息。

2.5.6.1. 集群备份策略

重要

红帽不提供带有 STS 的 ROSA 集群的备份方法，这是默认设置。客户对应用程序和应用程序数据进行备份计划至关重要。

应用程序和应用程序数据备份不是带有托管 control plane (HCP)服务的 Red Hat OpenShift Service on AWS (ROSA)的一部分。

2.5.6.2. 自动缩放

节点自动扩展可在带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)上提供。您可以配置自动扩展选项，以自动扩展集群中的机器数量。

其他资源

- 关于集群中的自动扩展节点

2.5.6.3. Daemonset

客户可以使用托管的 control plane (HCP)在 Red Hat OpenShift Service on AWS (ROSA)上创建并运行 daemonset。

2.5.6.4. 多个可用区

无论客户的 worker 节点配置是什么，control plane 组件始终在多个可用区间部署。

2.5.6.5. 节点标签

红帽在节点创建过程中创建自定义节点标签，目前无法在带有托管 control plane (HCP)集群的 Red Hat OpenShift Service on AWS (ROSA)上更改。但是，创建新机器池时支持自定义标签。

2.5.6.6. OpenShift version

带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)作为服务运行，并与最新的 OpenShift Container Platform 版本保持最新状态。将计划升级到最新版本。

2.5.6.7. 升级

可以使用 ROSA CLI、**rosa** 或 OpenShift Cluster Manager 调度升级。

有关升级策略和步骤的更多信息，请参阅 AWS 生命周期的 Red Hat OpenShift Service 。

2.5.6.8. Windows 容器

目前，Red Hat OpenShift support for Windows Containers 在 Red Hat OpenShift Service on AWS 上不可用。

2.5.6.9. 容器引擎

带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)在 OpenShift 4 上运行，并使用 CRI-O 作为唯一可用的容器引擎。

2.5.6.10. 操作系统

带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)在 OpenShift 4 上运行，并使用 Red Hat CoreOS 作为所有 control plane 和 worker 节点的操作系统。

2.5.6.11. Red Hat Operator 支持

红帽工作负载通常是指通过 Operator Hub 提供的红帽提供的 Operator。红帽工作负载不由红帽 SRE 团队管理，必须部署到 worker 节点上。这些 Operator 可能需要额外的红帽订阅，并可能产生额外的云基础架构成本。这些红帽提供的 Operator 示例包括：

- Red Hat Quay
- Red Hat Advanced Cluster Management
- Red Hat Advanced Cluster Security
- Red Hat OpenShift Service Mesh
- OpenShift Serverless
- Red Hat OpenShift Logging
- Red Hat OpenShift Pipelines

2.5.6.12. Kubernetes Operator 支持

OperatorHub 市场中列出的所有 Operator 都应该可用于安装。这些 Operator 被视为客户工作负载，不受 Red Hat SRE 监控。

2.5.7. 安全性

本节提供有关带有托管 control plane (HCP)安全性的 Red Hat OpenShift Service on AWS (ROSA)的服务定义信息。

2.5.7.1. 身份验证供应商

可以使用 OpenShift Cluster Manager 或集群创建过程或使用 ROSA CLI **rosa** 配置集群的身份验证。ROSA 不是一个身份提供程序，对集群的所有访问都必须由客户管理，作为其集成解决方案的一部分。支持同时使用同时调配的多个身份提供程序。支持以下身份提供程序：

- Github 或 GitHub Enterprise
- GitLab
- Google
- LDAP
- OpenID Connect
- htpasswd

2.5.7.2. 特权容器

特权容器可供具有 **cluster-admin** 角色的用户使用。使用特权容器作为 **cluster-admin** 取决于 Red Hat Enterprise Agreement 附录 4 (在线订阅服务)中的职责和排除备注。

2.5.7.3. 客户管理员用户

除了普通用户外，带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)提供了对带有 HCP 特定组的 ROSA 的访问，名为 **dedicated-admin**。属于 **dedicated-admin** 组成员的任何用户：

- 具有集群中所有客户创建项目的管理员访问权限。
- 可以管理集群的资源配额和限值。
- 可以添加和管理 **NetworkPolicy** 对象。
- 可以查看集群中特定节点和 PV 的信息，包括调度程序信息。
- 可以访问集群上保留的 **dedicated-admin** 项目，它允许使用提升的特权创建服务帐户，同时还能够为集群上的项目更新默认限值和配额。
- 可以从 OperatorHub 安装 Operator，并执行所有 If **operators.coreos.com** API 组中的所有操作动词。

2.5.7.4. 集群管理角色

带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)的管理员对您的机构集群的 **cluster-admin** 角色具有默认访问权限。使用 **cluster-admin** 角色登录到帐户时，用户可以增加运行特权安全上下文的权限。

2.5.7.5. 项目自助服务

默认情况下，所有用户都可以创建、更新和删除他们的项目。如果 **dedicated-admin** 组的成员从经过身份验证的用户移除 **self-provisioner** 角色，则可以受限制：

```
$ oc adm policy remove-cluster-role-from-group self-provisioner system:authenticated:oauth
```

通过应用可以恢复限制：

```
$ oc adm policy add-cluster-role-to-group self-provisioner system:authenticated:oauth
```

2.5.7.6. 法规合规性

有关最新合规性信息，*请参阅了解 ROSA 的进程和安全性* 中的 *Compliance* 表。

2.5.7.7. 网络安全性

使用 Red Hat OpenShift Service on AWS 时，AWS 对所有负载均衡器（即 AWS Shield）提供标准的 DDoS 保护。这对 Red Hat OpenShift Service on AWS 使用的所有面向公共的负载均衡器的用户级别为 3 和 4 的攻击提供了 95% 的保护。为来自 **haproxy** 路由器的 HTTP 请求添加 10 秒超时，以接收响应或连接关闭，以提供额外的保护。

2.5.7.8. etcd 加密

在带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)中，control plane 存储默认加密，这包括 etcd 卷的加密。这种存储级别加密通过云供应商的存储层提供。

默认情况下，etcd 数据库始终加密。客户可能会选择提供自己的自定义 AWS KMS 密钥来加密 etcd 数据库。

etcd 加密将加密以下 Kubernetes API 服务器和 OpenShift API 服务器资源：

- Secrets
- 配置映射
- Routes
- OAuth 访问令牌
- OAuth 授权令牌

2.5.8. 其他资源

- 有关最新合规性信息，请参阅了解 ROSA 的进程和安全性。
- 请参阅 ROSA 生命周期

2.6. 使用 HCP 更新生命周期的 ROSA

2.6.1. 概述

红帽为 Red Hat OpenShift Service on AWS 公布了它的产品生命周期，以便客户和合作伙伴有效地规划、部署和支持其应用程序。红帽发布这个生命周期，以尽可能提供透明性，并可能会在出现冲突时从这些政策做例外。

Red Hat OpenShift Service on AWS 是一个 Red Hat OpenShift 的受管实例，并维护一个独立的发行计划。有关受管产品的更多详细信息，请参阅 Red Hat OpenShift Service on AWS 服务定义。特定版本的安全公告和程序错误修复公告的可用性取决于 Red Hat OpenShift Container Platform 生命周期政策，并遵循 Red Hat OpenShift Service on AWS 维护计划。

其他资源

- Red Hat OpenShift Service on AWS 服务定义

2.6.2. 定义

表 2.2. 版本参考

版本格式	主	次	Patch	Major.minor.patch
	x	y	z	x.y.z
示例	4	5	21	4.5.21

主发行版本或 X-releases

称为*主发行版本*或 *X-releases* (X.y.z)。

例子

- "Major release 5" → 5.y.z
- "Major release 4" → 4.y.z
- "Major release 3" → 3.y.z

次发行版本或 Y-releases

称为*次发行版本*或 *Y-releases* (x.Y.z)。

例子

- "Minor release 4" → 4.4.z
- "次版本 5" → 4.5.z
- "Minor release 6" → 4.6.z

补丁版本或 Z-releases

称为*补丁版本*或*Z-releases* (x.y.Z)。

例子

- "Patch release 14 of minor release 5" → 4.5.14
- "Patch release 25 of minor release 5" → 4.5.25
- "Patch release 26 of minor release 6" → 4.6.26

2.6.3. 主发行版本 (X.y.z)

Red Hat OpenShift Service on AWS 的主版本（如版本 4）在后续主版本或产品停用后，支持一年。

示例

- 如果 Red Hat OpenShift Service on AWS 版本 5 在 1 月 1 日发布，则版本 4 可以在受管集群上持续运行 12 个月，直到 12 月 31 日为止。在这段时间后，集群需要升级或迁移到版本 5。

2.6.4. 次版本(x.Y.z)

从 4.8 OpenShift Container Platform 次版本开始，红帽会在给定次版本的正式发布后至少支持所有次版本的 16 个月。补丁版本不受支持周期的影响。

在支持期结束前，客户会收到 60、30 和 15 天通知。在支持周期结束前，集群必须升级到最老支持的次版本的最新补丁版本，或者红帽会自动将 control plane 升级到下一个支持的次版本。

示例

1. 客户的集群当前在 4.13.8 上运行。4.13 次版本在 2023 年 5 月 17 日正式发布。
2. 2024 年 7 月 19 日、8 月 16 日和 9 月 2 日，客户会收到通知，如果集群还没有升级到受支持的次版本，则其集群将在 2024 年 9 月 17 日进入"有限支持"状态。
3. 集群必须在 2024 年 9 月 17 日前升级到 4.14 或更高版本。
4. 如果没有执行升级，集群的 control plane 会自动升级到 4.14.26，且对集群的 worker 节点没有自动升级。

其他资源

- Red Hat OpenShift Service on AWS 的有限支持状态

2.6.5. 补丁版本(x.y.Z)

在支持次版本的期间，红帽支持所有 OpenShift Container Platform 补丁版本，除非另有指定。

出于平台安全性和稳定性的原因，补丁版本可能会被弃用，这会阻止安装该版本并触发该发行版本的强制升级。

示例

1. 4.7.6 可发现包含关键 CVE。
2. 受 CVE 影响的任何发行版本都将从支持的补丁版本列表中删除。另外，任何运行 4.7.6 的集群都会被调度在 48 小时内自动升级。

2.6.6. 有限支持状态

当集群过渡到 *有限支持状态*时，红帽不再主动监控集群，SLA 将不再适用，并拒绝对 SLA 请求的学分。这并不意味着您不再有产品支持。在某些情况下，如果您修复了违反因素，集群可以返回完全支持的状态。但是，在其他情况下，您可能需要删除并重新创建集群。

集群可能会因为许多原因移至有限支持状态，包括以下情况：

如果您删除或替换任何由红帽安装和管理的 Red Hat OpenShift Service on AWS 组件或任何其他组件

如果使用了集群管理员权限，红帽不负责您的任何或授权用户的操作，包括影响基础架构服务、服务可用性或数据丢失的人。如果红帽检测到此类操作，集群可能会过渡到有限支持状态。红帽通知您的状态变化，您应该恢复操作或创建支持问题单来探索可能需要删除和重新创建集群的补救步骤。

如果您对可能造成集群移至有限支持状态或需要进一步帮助的特定操作有疑问，请打开支持票据。

2.6.7. 支持的版本例外策略

红帽保留添加或删除新的或现有版本的权利，或延迟即将发布的次版本，这些版本已确定有一个或多个关键生产影响了漏洞或安全问题，而不会提前通知。

2.6.8. 安装策略

虽然红帽建议安装最新的支持版本，但 Red Hat OpenShift Service on AWS 支持安装任何受支持的版本，如前面的策略所述。

2.6.9. 必须升级

如果一个关键(Critical)或重要的 CVE，或其他由红帽识别的错误有严重影响集群的安全性或稳定性，则客户必须在两个 工作日内 升级到下一个支持的补丁版本。

在极端情况下，基于红帽对环境的 CVE 的评估，红帽会通知客户有 两个工作日 来调度或手动将集群更新至最新的安全补丁版本。如果在两个工作日后没有执行更新，红帽会自动将集群的 control plane 更新到最新的、安全补丁版本，以缓解潜在的安全漏洞或不稳定。https://access.redhat.com/articles/2623321如果客户通过 支持问题单 请求，红帽可能会自行决定临时延迟自动更新。

2.6.10. 生命周期日期

版本	公开发行（GA）	生命周期结束
4.15	2024 年 2 月 27 日	2025 年 6 月 30 日
4.14	2023 年 12 月 4 日	2025 年 2 月 28 日

2.7. 了解 RED HAT OPENSHIFT SERVICE ON AWS 的安全性

本文档详细介绍了 Red Hat、Amazon Web Services (AWS)和托管 Red Hat OpenShift Service on AWS (ROSA)的客户安全职责。

缩写和术语

- **AWS** - Amazon Web Services
- **CEE** - 客户体验与参与（红帽支持）
- **CI/CD** - Continuous Integration / Continuous Delivery
- **CVE** - 常见漏洞和风险
- **PVs** - 持久性卷
- **ROSA** - Red Hat OpenShift Service on AWS
- **SRE** - Red Hat Site Reliability Engineering
- **VPC** - Virtual Private Cloud

2.7.1. 安全和合规性

安全和合规性和合规性包括实施安全控制和合规认证等任务。

2.7.1.1. 数据分类

红帽定义并遵循一个数据分类标准，以确定数据的敏感度，并强调收集、使用、传输、存储和处理数据的保密性和完整性的固有风险。客户拥有的数据被分类为最高水平的敏感度和处理要求。

2.7.1.2. 数据管理

Red Hat OpenShift Service on AWS (ROSA)使用 AWS 密钥管理服务 (KMS) 来帮助安全地管理加密的数据密钥。这些密钥用于默认加密的 control plane、基础架构和 worker 数据卷。客户应用程序的持久性卷 (PV) 也使用 AWS KMS 进行密钥管理。

当客户删除其 ROSA 集群时，所有集群数据都会被永久删除，包括 control plane 数据卷和客户应用程序数据卷，如持久性卷 (PV)。

2.7.1.3. 漏洞管理

红帽使用行业标准工具对 ROSA 执行定期漏洞扫描。识别的漏洞将根据严重性的时间表跟踪其补救。记录漏洞扫描和修复活动，以供在合规认证审计课程中由第三方评估商进行验证。

2.7.1.4. 网络安全性

2.7.1.4.1. 防火墙和 DDoS 保护

每个 ROSA 集群都由使用 AWS 安全组的防火墙规则的安全网络配置进行保护。ROSA 客户还可保护对 AWS Shield Standard 的 DDoS 攻击。

2.7.1.4.2. 私有集群和网络连接

客户可以选择配置其 ROSA 集群端点，如 Web 控制台、API 和应用程序路由器，以便无法从互联网访问集群 control plane 和应用程序。Red Hat SRE 仍然需要通过 IP allow-lists 保护的端点。

AWS 客户可通过 AWS VPC 对等、AWS VPN 或 AWS Direct Connect 等技术配置私有网络连接到其 ROSA 集群。

2.7.1.4.3. 集群网络访问控制

客户可以使用 **NetworkPolicy** 对象和 OpenShift SDN 配置细粒度网络访问控制规则。

2.7.1.5. penetration 测试

红帽对 ROSA 执行定期测试。通过使用行业标准工具和最佳实践，由独立内部团队执行测试。

发现的任何问题会根据严重性进行优先级排序。属于开源项目的所有问题都与社区共享以解决问题。

2.7.1.6. Compliance

Red Hat OpenShift Service on AWS 在安全性和控制方面遵循常见的行业最佳实践。下表中概述了认证。

表 2.3. Red Hat OpenShift Service on AWS 的安全性和控制认证

Compliance	Red Hat OpenShift Service on AWS (ROSA)	带有托管 control plane (HCP)的 Red Hat OpenShift Service on AWS (ROSA)
HIPAA Qualified	是	否
ISO 27001	是	是
ISO 27017	是	是
ISO 27018	是	是
PCI DSS	是	是
SOC 1 类型 2	是	是
SOC 2 类型 2	是	是
SOC 3	是	是
FedRAMP High[1]	是(GovCloud requisite)	否

1. 有关 GovCloud 上的 ROSA 的更多信息，请参阅 FedRAMP Marketplace ROSA Agency 和 ROSA JAB 列表。

其他资源

- 有关 SRE 驻留的信息，请参阅 Red Hat Subprocessor 列表。
- 有关客户或共享职责的更多信息，请参阅 ROSA 响应文档。
- 有关 ROSA 及其组件的更多信息，请参阅 ROSA 服务定义。

2.8. SRE 和服务帐户访问

通过身份和访问管理，概述了对 Red Hat OpenShift Service on AWS (ROSA)集群的 Red Hat 站点可靠性工程(SRE)访问。

2.8.1. 身份和访问管理

Red Hat SRE 团队的大部分访问是通过自动化配置管理使用集群 Operator 进行的。

子处理器

有关可用子处理器列表，请查看红帽客户门户网站上的 红帽子处理器列表。

2.8.2. SRE 集群访问

SRE 访问 Red Hat OpenShift Service on AWS (ROSA)集群通过多个所需身份验证层控制，所有这些集群都由严格的公司策略管理。所有身份验证尝试访问集群以及集群中所做的更改都会记录在审计日志中，以

及负责这些操作的 SRE 的特定帐户身份。这些审计日志有助于确保 SREs 对客户集群进行的所有更改遵循组成红帽受管服务指南的严格的策略和步骤。

以下是 SRE 必须执行的进程的概述，以访问客户的集群。

- SRE 从 Red Hat SSO （云服务）请求刷新的 ID 令牌。此请求经过身份验证。令牌在十五分钟内有效。令牌过期后，您可以再次刷新令牌并接收新令牌。刷新到新令牌的功能存在冲突；但是，在 30 天不活动后，会撤销刷新到新令牌的功能。

- SRE 连接到红帽 VPN。VPN 身份验证由 Red Hat Corporate Identity and Access Management system (RH IAM)完成。使用 RH IAM 时，SRE 是多因素，可以根据组和现有载入和关闭进程在内部管理。当 SRE 进行身份验证并连接后，SRE 可以访问云服务团队管理 plane。对云服务团队管理平面的更改需要许多层的批准，并由严格的公司策略维护。

- 授权完成后，SRE 会登录到 fleet management plane，并接收由 fleet management plane 创建的服务帐户令牌。令牌有效 15 分钟。当令牌不再有效后，它会被删除。

- 在授予 fleet management plane 的访问权限后，SRE 会使用各种方法访问集群，具体取决于网络配置。

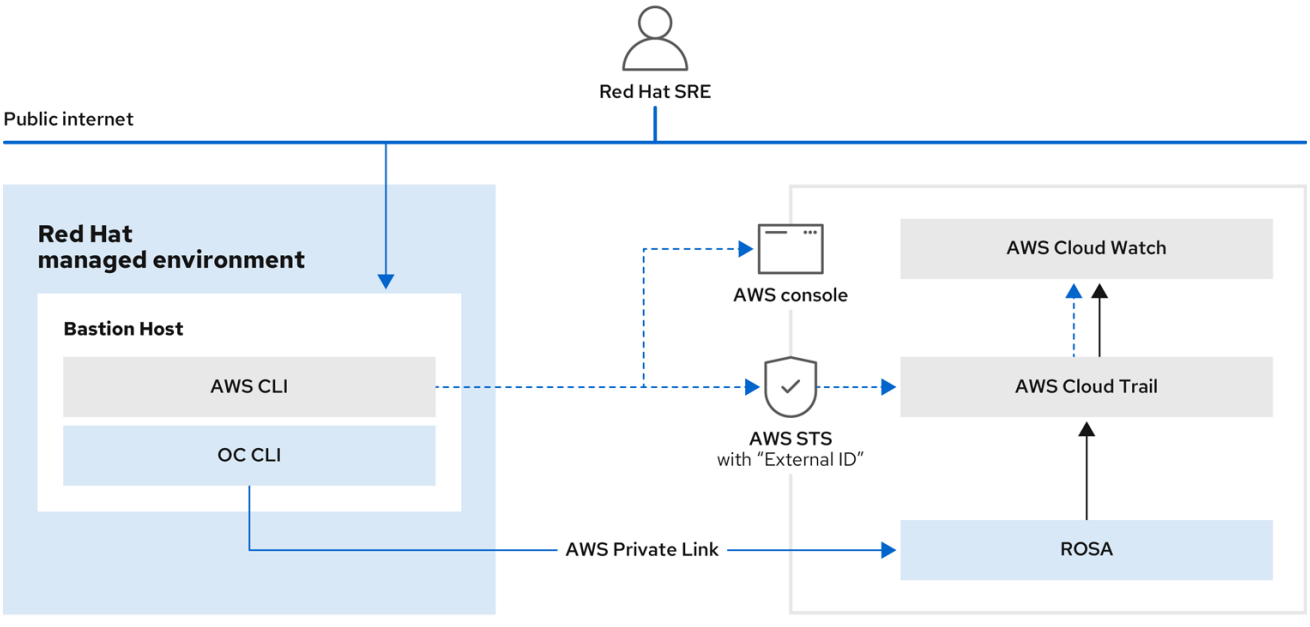
    - 访问私有或公共集群 ： 请求通过特定的 Network Load Balancer (NLB)发送，方法是使用端口 6443 上的加密 HTTP 连接。

    - 访问 PrivateLink 集群 ： 请求发送到红帽 Transit 网关，然后连接到每个区域的 Red Hat VPC。接收请求的 VPC 将依赖于目标私有集群的区域。在 VPC 中，有一个专用子网，其中包含到客户的 PrivateLink 集群 的 PrivateLink 端点。

SREs 通过 Web 控制台或命令行界面(CLI)工具访问 ROSA 集群。身份验证需要多因素身份验证 (MFA)，对密码复杂性和帐户锁定要求具有行业标准的要求。SRE 必须作为个人进行身份验证以确保可审核。所有验证尝试都会记录到安全信息和事件管理 (SIEM) 系统。

SREs 使用加密 HTTP 连接访问私有集群。只有通过 IP 允许列表或私有云供应商链接，才能从安全的红帽网络获得连接。

图 2.1. SRE 对 ROSA 集群的访问



2.8.2.1. ROSA 中的特权访问控制

SRE 在访问 ROSA 和 AWS 组件时遵循最小特权的原则。SRE 访问有四个基本类别：

- SRE 管理通过红帽门户访问，具有正常双因素身份验证，且无特权的 elevation。
- SRE 管理通过带有正常双因素身份验证的 Red Hat Enterprise SSO 访问，且没有特权升级。
- OpenShift elevation，这是使用红帽 SSO 的手动提升。访问时间被限制为 2 小时，经过全面审核，需要进行管理批准。
- AWS 访问或提升，这是 AWS 控制台或 CLI 访问的手动传播。访问仅限于 60 分钟，并且完全审核。

每种访问类型对组件具有不同的访问权限级别：

组件	典型的 SRE 管理访问权限（红帽门户）	典型的 SRE 管理员访问权限（红帽 SSO）	OpenShift elevation	云供应商访问或提升信息
OpenShift Cluster Manager	R/W	无权限	无权限	无权限
OpenShift console	无权限	R/W	R/W	无权限
节点操作系统	无权限	提升 OS 和网络权限的特定列表。	提升 OS 和网络权限的特定列表。	无权限
AWS 控制台	无权限	没有访问权限，但这是用于请求云供应商访问的帐户。	无权限	使用 SRE 身份的所有云供应商权限。

2.8.2.2. SRE 对 AWS 帐户的访问

在日常的 Red Hat OpenShift Service on AWS 操作中，Red Hat 人员不会访问 AWS 账户。出于紧急的故障排除目的，SRE 定义了并可审计的程序来访问云基础架构帐户。

SRE 使用 AWS 安全令牌服务 (STS) 为保留角色生成简短的 AWS 访问令牌。对 STS 令牌的访问会被审核，可追溯到各个用户。STS 和非STS 集群都使用 AWS STS 服务进行 SRE 访问。对于非STS 集群，**BYOCAdminAccess** 角色附加了 **AdministratorAccess** IAM 策略，此角色用于管理。对于 STS 集群，**ManagedOpenShift-Support-Role** 带有 **ManagedOpenShift-Support-Access** 策略，这个策略用于管理。

2.8.2.3. AWS 帐户的 SRE STS 视图

当 SREs 通过双因素身份验证进行 VPN 时，它们和红帽支持可以假定 AWS 帐户中的 **ManagedOpenShift-Support-Role**。**ManagedOpenShift-Support-Role** 具有 SREs 所需的所有权限，直接排除故障和管理 AWS 资源。假设 **ManagedOpenShift-Support-Role**，SRE 使用 AWS 安全令牌服务(STS)为其帐户生成唯一的、时间过期 URL。然后 SREs 可以执行多个故障排除操作，其中包括：

- 查看 CloudTrail 日志
- 关闭有问题的 EC2 实例

SRE 执行的所有活动都来自红帽 IP 地址，并登录到 CloudTrail 以便审核和查看所有活动。只有在需要访问 AWS 服务才能协助时，才会使用此角色。大多数权限都是只读的。但是，选择几个权限具有更多访问权限，包括重启实例或启动新实例。SRE 访问仅限于附加到 **ManagedOpenShift-Support-Role** 的策略权限。

有关权限的完整列表，请参阅 About IAM resources for ROSA cluster using STS 用户指南中的 sts_support_permission_policy.json。

2.8.2.4. SRE 通过 PrivateLink VPC 端点服务访问

PrivateLink VPC 端点服务作为 ROSA 集群创建的一部分创建。

当您有一个 PrivateLink ROSA 集群时，其 Kubernetes API 服务器会通过一个负载均衡器公开，该负载均衡器默认只能从 VPC 内访问。红帽站点可靠性工程(SRE)可以通过在红帽拥有的 AWS 帐户中有一个关联的 VPC 端点的 VPC 端点连接到这个负载均衡器。此端点服务包含集群名称，它也在 ARN 中。

在 **Allow principals** 选项卡下，会列出红帽拥有的 AWS 帐户。这个特定用户可确保其他实体无法创建到 PrivateLink 集群的 Kubernetes API 服务器的 VPC 端点连接。

当 Red Hat SREs 访问 API 时，这个 fleet management plane 可以通过 VPC 端点服务连接到内部 API。

2.8.3. 红帽支持访问

红帽客户体验与参与(CEE)团队的成员通常对集群的部分具有只读访问权限。具体来说，CEE 对核心和产品命名空间具有有限访问权限，且无法访问客户命名空间。

角色	Core 命名空间	层次产品命名空间	Customer 命名空间	AWS 帐户*
OpenShift SRE	Read: All Write: Very 有限 [1]	Read: All Write: None	Read: None[2] Write: None	Read: All [3] Write: All [3]
CEE	Read: All Write: None	Read: All Write: None	Read: None[2] Write: None	Read: None Write: None
客户管理员	Read: None Write: None	Read: None Write: None	Read: All Write: All	Read: All Write: All
客户用户	Read: None Write: None	Read: None Write: None	Read: Limited[4] Write: Limited[4]	Read: None Write: None
其他人	Read: None Write: None	Read: None Write: None	Read: None Write: None	Read: None Write: None

1. 仅限于解决常见用例，如部署失败、升级集群并替换错误的 worker 节点。
2. 默认情况下，红帽人员无法访问客户数据。
3. SRE 对 AWS 帐户的访问是在记录的事件期间进行出色的故障排除紧急步骤。
4. 限制为通过 RBAC 授予的内容，以及用户创建的命名空间。

2.8.4. 客户访问权限

客户访问权限仅限于由客户管理员角色使用 RBAC 授予权限创建的命名空间。通常不允许访问底层基础架构或产品命名空间，而无需 **cluster-admin** 访问。有关客户访问和身份验证的更多信息，请参阅文档中的"了解身份验证"部分。

2.8.5. 访问批准及审核

新的 SRE 用户访问需要管理批准。通过自动过程将经过隔离或传输的 SRE 帐户作为授权用户删除。另外，SRE 会执行定期访问审核，包括授权用户列表的管理登录。

访问和身份授权表包括管理对集群、应用程序和基础架构资源的授权访问权限的职责。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	服务职责	客户职责
日志记录	**Red Hat** • 遵循行业标准内平台审计日志的内部访问过程。 • 提供原生 OpenShift RBAC 功能。	• 配置 OpenShift RBAC 以控制对项目的访问，并扩展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。
应用程序网络	**Red Hat** • 提供原生 OpenShift RBAC 和 **dedicated-admin** 功能。	• 配置 OpenShift **dedicated-admin** 和 RBAC，以控制对路由配置的访问。 • 管理红帽机构管理员以授予 OpenShift Cluster Manager 访问权限。集群管理器用于配置路由器选项，并提供服务负载均衡器配额。
集群网络	**Red Hat** • 通过 OpenShift Cluster Manager 提供客户访问控制。 • 提供原生 OpenShift RBAC 和 **dedicated-admin** 功能。	• 管理红帽帐户的机构成员资格。 • 管理红帽机构管理员以授予 OpenShift Cluster Manager 访问权限。 • 配置 OpenShift **dedicated-admin** 和 RBAC，以控制对路由配置的访问。

资源	服务职责	客户职责
虚拟网络管理	**Red Hat** • 通过 OpenShift Cluster Manager 提供客户访问控制。	• 通过 OpenShift Cluster Manager 管理对 AWS 组件的可选用户访问。
虚拟存储管理	**Red Hat** • 通过 Red Hat OpenShift Cluster Manager 提供客户访问控制。	• 通过 OpenShift Cluster Manager 管理对 AWS 组件的可选用户访问。 • 创建启用 ROSA 服务访问所需的 AWS IAM 角色和附加策略。
虚拟计算管理	**Red Hat** • 通过 Red Hat OpenShift Cluster Manager 提供客户访问控制。	• 通过 OpenShift Cluster Manager 管理对 AWS 组件的可选用户访问。 • 创建启用 ROSA 服务访问所需的 AWS IAM 角色和附加策略。
AWS 软件（公共 AWS 服务）	**AWS** **Compute：** 提供 Amazon EC2 服务，用于 ROSA control plane、基础架构和 worker 节点。 **Storage ：** 提供 Amazon EBS，允许 ROSA 为集群置备本地节点存储和持久性卷存储。 **Storage：** 提供 Amazon S3，用于服务的内置镜像 registry。 **网络 ：** 提供 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。	• 创建启用 ROSA 服务访问所需的 AWS IAM 角色和附加策略。 • 使用 IAM 工具将适当的权限应用到客户账户中的 AWS 资源。 • 要在 AWS 机构中启用 ROSA，客户负责管理 AWS 机构管理员。 • 要在 AWS 机构中启用 ROSA，客户负责使用 AWS 许可证管理器分发 ROSA 授权。
硬件和 AWS 全局基础架构	**AWS** • 有关 AWS 数据中心的物理访问控制的详情，请参考 AWS Cloud Security 页面中的 Our Controls。	• 客户不负责 AWS 全局基础架构。

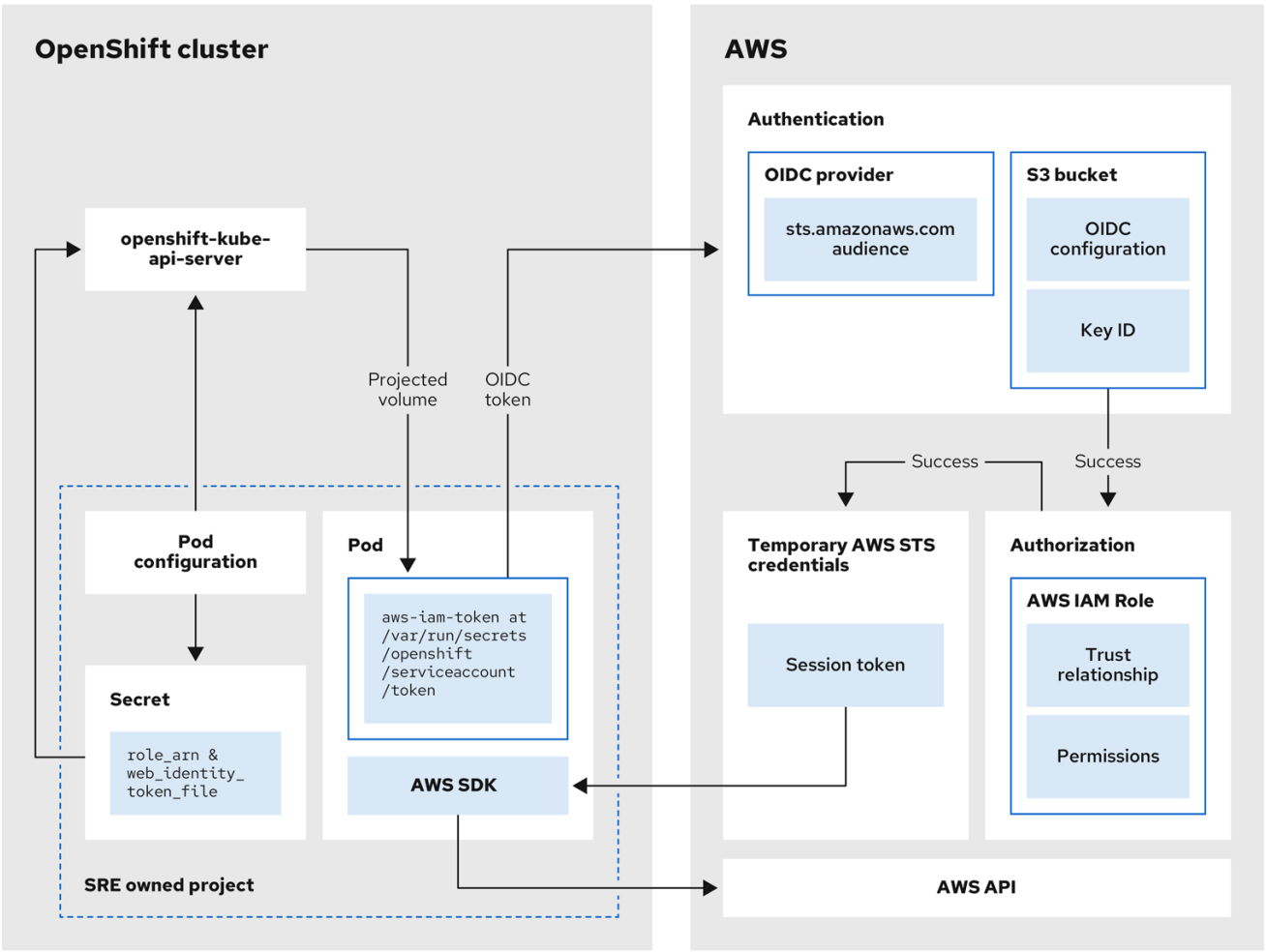
2.8.6. 服务帐户如何假定 SRE 拥有的项目中的 AWS IAM 角色

当使用 AWS 安全令牌服务(STS)的 AWS 集群上安装 Red Hat OpenShift Service 时，会创建特定于集群的 Operator AWS Identity and Access Management (IAM)角色。这些 IAM 角色允许 Red Hat OpenShift Service on AWS 集群 Operator 运行核心 OpenShift 功能。

集群 Operator 使用服务帐户假设 IAM 角色。当服务帐户假设 IAM 角色时，会为集群 Operator 的 pod 中使用的服务帐户提供临时 STS 凭证。如果假设角色具有所需的 AWS 权限，则服务帐户可以在 pod 中运行 AWS SDK 操作。

在 SRE 拥有的项目中假设 AWS IAM 角色的工作流
下图演示了在 SRE 拥有的项目中假设 AWS IAM 角色的工作流：

图 2.2. 在 SRE 拥有的项目中假设 AWS IAM 角色的工作流



工作流有以下阶段：

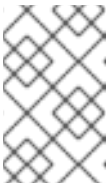
1. 在集群 Operator 运行的每个项目中，Operator 的部署 spec 具有投射服务帐户令牌的卷挂载，以及包含 pod 的 AWS 凭证配置的 secret。令牌是面向使用者和限时的。每小时，Red Hat OpenShift Service on AWS 会生成新的令牌，AWS SDK 会读取包含 AWS 凭证配置的挂载的 secret。此配置具有到挂载令牌的路径和 AWS IAM 角色 ARN。secret 的凭证配置包括：

    - 一个 **$AWS_ARN_ROLE** 变量，其中包含具有运行 AWS SDK 操作所需的权限的 IAM 角色的 ARN。
    - **$AWS_WEB_IDENTITY_TOKEN_FILE** 变量，在 pod 中具有到服务帐户的 OpenID Connect (OIDC)令牌的完整路径。完整路径为 **/var/run/secrets/openshift/serviceaccount/token**。

2. 当集群 Operator 需要假设 AWS IAM 角色访问 AWS 服务（如 EC2）时，Operator 上运行的 AWS SDK 客户端代码会调用 **AssumeRoleWithWebIdentity** API 调用。

3. OIDC 令牌从 pod 传递给 OIDC 供应商。如果满足以下要求，供应商会验证服务帐户身份：

   - 身份签名由私钥有效并签名。
   - **sts.amazonaws.com** 使用者列在 OIDC 令牌中，并与 OIDC 供应商中配置的 audience 匹配。

   注意

   在带有 STS 集群的 Red Hat OpenShift Service on AWS 中，OIDC 供应商会在安装过程中创建，并默认设置为服务帐户签发者。**sts.amazonaws.com** 使用者默认在 OIDC 供应商中设置。

   - OIDC 令牌没有过期。
   - 令牌中的签发者值具有 OIDC 供应商的 URL。

4. 如果项目和服务帐户位于被假定的 IAM 角色的信任策略范围内，则授权会成功。

5. 成功身份验证和授权后，临时 AWS STS 凭证以 AWS 访问令牌、secret 密钥和会话令牌的形式传递给 pod，供服务帐户使用。通过使用凭证，服务帐户会临时授予 IAM 角色中启用的 AWS 权限。

6. 当集群 Operator 运行时，使用 pod 中的 AWS SDK 的 Operator 会消耗具有投射服务帐户和 AWS IAM 角色 ARN 的 secret，以针对 OIDC 供应商进行身份验证。OIDC 供应商返回临时 STS 凭证，用于针对 AWS API 进行身份验证。

其他资源

- 如需有关集群 Operator 使用的 AWS IAM 角色的更多信息，请参阅 特定于集群的 Operator IAM 角色参考。
- 有关集群 Operator 所需的策略和权限的更多信息，请参阅 集群范围的角色创建方法。

第 3 章 关于使用 STS 的 ROSA 集群的 IAM 资源

要部署使用 AWS 安全令牌服务(STS) 的 Red Hat OpenShift Service on AWS (ROSA) 集群，您必须创建以下 AWS Identity Access Management (IAM)资源：

- 特定的帐户范围的 IAM 角色和策略，它们提供 ROSA 支持、安装、control plane 和计算功能所需的 STS 权限。这包括集群范围的 Operator 策略。
- 特定于集群的 Operator IAM 角色，允许 ROSA 集群 Operator 执行核心 OpenShift 功能。
- 集群 Operator 用于进行身份验证的 OpenID Connect (OIDC)供应商。
- 如果使用 OpenShift Cluster Manager 部署 ROSA，必须创建额外的资源：
  - 一个 OpenShift Cluster Manager IAM 角色来在集群中完成安装。
  - 没有任何权限来验证 AWS 帐户身份的用户角色。

本文档提供有关您在创建使用 STS 的 ROSA 集群时必须要部署的 IAM 资源的引用信息。它还包含在 **rosa create** 命令中使用 **手动**模式时生成的 **aws** CLI 命令。

其他资源

- 有关快速创建带有 STS 的 ROSA 集群的步骤，包括 AWS IAM 资源，请参阅 使用默认选项创建带有 STS 的 ROSA 集群。
- 有关使用自定义创建带有 STS 的 ROSA 集群的步骤，包括 AWS IAM 资源，请参阅使用自定义创建带有 STS 的 ROSA 集群。

3.1. OPENSHIFT CLUSTER MANAGER 角色和权限

如果使用 OpenShift Cluster Manager 创建 ROSA 集群，则必须具有链接到 AWS 帐户的以下 AWS IAM 角色来创建和管理集群。有关将 IAM 角色链接到 AWS 帐户的更多信息，请参阅 关联 AWS 帐户。

提示

如果您只使用 ROSA CLI (**rosa**)，则不需要创建这些 IAM 角色。

这些 AWS IAM 角色如下：

- ROSA 用户角色是由红帽用来验证客户的 AWS 身份的 AWS 角色。此角色没有额外的权限，该角色与 Red Hat 安装程序帐户具有信任关系。
- **ocm-role** 资源授予在 OpenShift Cluster Manager 中安装 ROSA 集群所需的权限。您可以将基本或管理权限应用到 **ocm-role** 资源。如果创建一个管理 **ocm-role** 资源，OpenShift Cluster Manager 可以创 建所需的 AWS Operator 角色和 OpenID Connect (OIDC)供应商。此 IAM 角色还与 Red Hat 安装程序帐户建立信任关系。

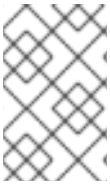
注意

ocm-role IAM 资源引用 IAM 角色以及创建必要策略的组合。

如果要在 OpenShift Cluster Manager 中使用自动模式，创建此用户角色以及管理 **ocm-role** 资源，以创建 Operator 角色策略和 OIDC 供应商。

3.1.1. 了解 OpenShift Cluster Manager 角色

在 OpenShift Cluster Manager 中创建 ROSA 集群需要 **ocm-role** IAM 角色。通过基本的 **ocm-role** IAM 角色权限，您可以在 OpenShift Cluster Manager 中执行集群维护。要自动创建 operator 角色和 OpenID Connect (OIDC) 供应商，您必须在 **rosa create** 命令中添加 **--admin** 选项。此命令使用管理任务所需的额外权限创建 **ocm-role** 资源。



注意

此提升的 IAM 角色允许 OpenShift Cluster Manager 在集群创建过程中自动创建特定于集群的 Operator 角色和 OIDC 供应商。有关此自动角色和策略创建的更多信息，请参阅附加资源中的"客户范围内的角色创建"链接。

3.1.1.1. 了解用户角色

除了 **ocm-role** IAM 角色外，还需要创建一个用户角色，以便 Red Hat OpenShift Service on AWS 可以验证 AWS 身份。此角色没有权限，它仅用于在安装程序帐户和 **ocm-role** 资源之间建立信任关系。

下表显示了 **ocm-role** 资源的相关基本和管理权限。

表 3.1. 基本 ocm-role 资源的相关权限

资源	描述
iam:GetOpenIDConnectProvider	此权限允许基本角色检索有关指定 OpenID Connect (OIDC) 供应商的信息。
iam:GetRole	此权限允许基本角色检索指定角色的任何信息。返回的一些数据包括角色的路径、GUID、ARN 以及授予角色权限的信任策略。
iam:ListRoles	此权限允许基本角色列出路径前缀中的角色。
iam:ListRoleTags	此权限允许基本角色列出指定角色上的标签。
ec2:DescribeRegions	此权限允许基本角色返回有关您帐户上所有启用区域的信息。
ec2:DescribeRouteTables	此权限允许基本角色返回有关所有路由表的信息。
ec2:DescribeSubnets	此权限允许基本角色返回有关所有子网的信息。
ec2:DescribeVpcs	此权限允许基本角色返回有关所有虚拟私有云 (VPC) 的信息。
sts:AssumeRole	此权限允许基本角色检索临时安全凭证来访问超出一般权限的 AWS 资源。
sts:AssumeRoleWithWebIdentity	此权限允许基本角色通过 Web 身份提供程序检索对其帐户进行身份验证的临时安全凭据。

表 3.2. admin ocm-role 资源的额外权限

资源	描述
iam:AttachRolePolicy	此权限允许 admin 角色将指定的策略附加到所需的 IAM 角色。
iam:CreateOpenIDConnectProvider	此权限会创建一个描述身份提供程序的资源，它支持 OpenID Connect (OIDC)。当您创建具有此权限的 OIDC 供应商时，此供应商在供应商和 AWS 之间建立信任关系。
iam:CreateRole	此权限允许 admin 角色为您的 AWS 帐户创建角色。
iam:ListPolicies	此权限允许 admin 角色列出与 AWS 帐户关联的任何策略。
iam:ListPolicyTags	此权限允许 admin 角色列出指定策略上的任何标签。
iam:PutRolePermissionsBoundary	此权限允许 admin 角色根据指定的策略更改用户的权限边界。
iam:TagRole	此权限允许 admin 角色向 IAM 角色添加标签。

其他资源

- 集群范围的角色创建方法

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

前提条件

- 您有一个 AWS 帐户。
- 在 OpenShift Cluster Manager 机构中具有 Red Hat Organization Administrator 权限。
- 您有安装 AWS 范围的角色所需的权限。
- 您已在安装主机上安装并配置了最新的 Red Hat OpenShift Service on AWS (ROSA) CLI **rosa**。

流程

- 要使用基本权限创建 ocm-role IAM 角色，请运行以下命令：

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

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

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

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

输出示例

```
I: Creating ocm role
? Role prefix: ManagedOpenShift 1
? Enable admin capabilities for the OCM role (optional): No 2
? Permissions boundary ARN (optional): 3
? Role Path (optional): 4
? Role creation mode: auto 5
I: Creating role using 'arn:aws:iam::<ARN>:user/<UserName>'
? Create the 'ManagedOpenShift-OCM-Role-182' role? Yes 6
I: Created role 'ManagedOpenShift-OCM-Role-182' with ARN  'arn:aws:iam::
<ARN>:role/ManagedOpenShift-OCM-Role-182'
I: Linking OCM role
? OCM Role ARN: arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182 7
? Link the 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' role with organization
'<AWS ARN>'? Yes 8
I: Successfully linked role-arn 'arn:aws:iam::<ARN>:role/ManagedOpenShift-OCM-Role-182' with
organization account '<AWS ARN>'
```

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

   注意

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

AWS IAM 角色链接到 AWS 帐户，以创建和管理集群。有关将 IAM 角色链接到 AWS 帐户的更多信息，请参阅 关联 AWS 帐户。

其他资源

- AWS Identity and Access Management 数据类型
- Amazon Elastic Computer Cloud 数据类型
- AWS 令牌安全服务数据类型
- 集群范围的角色创建方法

3.2. 帐户范围的 IAM 角色和策略参考

本节详细介绍了使用 STS 的 ROSA 部署所需的帐户范围 IAM 角色和策略，包括 Operator 策略。它还包括定义策略的 JSON 文件。

集群范围的角色和策略特定于 OpenShift 次版本，如 OpenShift 4.16，并且兼容。您可以为同一次版本的多个集群重复使用 account-wide 角色和策略来最小化所需的 STS 资源，而不考虑补丁版本。

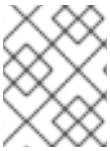
3.2.1. 集群范围的角色创建方法

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI、**rosa** 或 OpenShift Cluster Manager 指导安装来创建集群范围的角色。您可以手动创建角色，或者使用为这些角色和策略使用预定义名称的自动过程来创建角色。

手动 ocm-role 资源创建
如果您有必要的 CLI 访问在系统上创建这些角色，您可以使用手动创建方法。您可以在所需 CLI 工具或从 OpenShift Cluster Manager 运行这个选项。在开始手动创建过程后，CLI 会显示一系列命令，供您运行用于创建角色并将其链接到所需策略。

自动 ocm-role 资源创建
如果您使用管理权限创建 **ocm-role** 资源，您可以使用 OpenShift Cluster Manager 的自动创建方法。ROSA CLI 不要求您具有此 admin **ocm-role** IAM 资源，以自动创建这些角色和策略。选择此方法会创建使用默认名称的角色和策略。

如果您在 OpenShift Cluster Manager 上使用 ROSA 指导安装，则必须在引导的集群安装的第一个步骤中使用管理权限创建 **ocm-role** 资源。如果没有此角色，则无法使用自动 Operator 角色和策略创建选项，但您仍然可以使用手动过程创建集群及其角色和策略。



注意

sts_installer_trust_policy.json 和 **sts_support_trust_policy.json** 样本中存在的帐户号代表允许假定所需角色的红帽帐户。

表 3.3. ROSA 安装程序角色、策略和策略文件

资源	描述
ManagedOpenShift-Installer-Role	ROSA 安装程序使用的 IAM 角色。
ManagedOpenShift-Installer-Role-Policy	提供了一个 IAM 策略，它为 ROSA 安装程序提供完成集群安装任务所需的权限。

例 3.1. sts_installer_trust_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::710019948333:role/RH-Managed-OpenShift-Installer"
                ]
            },
```

```
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

例 3.2. sts_installer_permission_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "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:PassRole",
"iam:RemoveRoleFromInstanceProfile",
"iam:SimulatePrincipalPolicy",
"iam:TagRole",
"iam:UntagRole",
"route53:ChangeResourceRecordSets",
"route53:ChangeTagsForResource",
"route53:CreateHostedZone",
"route53:DeleteHostedZone",
"route53:GetAccountLimit",
"route53:GetChange",
"route53:GetHostedZone",
"route53:ListHostedZones",
"route53:ListHostedZonesByName",
"route53:ListResourceRecordSets",
"route53:ListTagsForResource",
"route53:UpdateHostedZoneComment",
"s3:CreateBucket",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:GetAccelerateConfiguration",
"s3:GetBucketAcl",
"s3:GetBucketCORS",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketObjectLockConfiguration",
```

```
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3: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"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

表 3.4. ROSA control plane 角色、策略和策略文件

资源	描述
ManagedOpenShift-ControlPlane-Role	ROSA control plane 使用的 IAM 角色。
ManagedOpenShift-ControlPlane-Role-Policy	提供了一个 IAM 策略，它为 ROSA control plane 提供管理其组件所需的权限。

例 3.3. sts_instance_controlplane_trust_policy.json

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": [
               "ec2.amazonaws.com"
            ]
         },
         "Action": [
            "sts:AssumeRole"
         ]
      }
   ]
}
```

例 3.4. sts_instance_controlplane_permission_policy.json

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

表 3.5. ROSA 计算节点角色、策略和策略文件

资源	描述
ManagedOpenShift-Worker-Role	ROSA 计算实例使用的 IAM 角色。
ManagedOpenShift-Worker-Role-Policy	提供了一个 IAM 策略，该策略为 ROSA 计算实例提供管理其组件所需的权限。

例 3.5. sts_instance_worker_trust_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            },
            "Action": [
                "sts:AssumeRole"
```

```
        ]
      }
    ]
}
```

例 3.6. sts_instance_worker_permission_policy.json

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

表 3.6. ROSA 支持角色、策略和策略文件

资源	描述
ManagedOpenShift-Support-Role	Red Hat Site Reliability Engineering (SRE)支持团队使用的 IAM 角色。
ManagedOpenShift-Support-Role-Policy	提供 Red Hat SRE 支持团队的 IAM 策略，以及支持 ROSA 集群所需的权限。

例 3.7. sts_support_trust_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::710019948333:role/RH-Technical-Support-Access"
                ]
            },
            "Action": [
                "sts:AssumeRole"
            ]
        }
    ]
}
```

例 3.8. sts_support_permission_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "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:DescribeVolumeStatus",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcEndpoints",
                "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"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::managed-velero*",
            "arn:aws:s3:::*image-registry*"
        ]
```

```
        }
    ]
}
```

表 3.7. ROSA OCM 角色和策略文件

资源	描述
ManagedOpenShift-OCM-Role	您可以使用此 IAM 角色在 OpenShift Cluster Manager 中创建和维护 ROSA 集群。

例 3.9. **sts_ocm_role_trust_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::710019948333:role/RH-Managed-OpenShift-Installer"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "<OCM_account_ID>"
                }
            }
        }
    ]
}
```

表 3.8. ROSA 用户角色和策略文件

资源	描述
ManagedOpenShift-User-<OCM_user>-Role	红帽用来验证客户的 AWS 身份的 IAM 角色。

例 3.10. **sts_user_role_trust_policy.json**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::710019948333:role/RH-Managed-OpenShift-Installer"
            },
            "Action": "sts:AssumeRole",
```

```
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "<OCM_account_ID>"
                }
            }
        }
    ]
}
```

表 3.9. ROSA Ingress Operator IAM 策略和策略文件

资源	描述
ManagedOpenShift-openshift-ingress-operator-cloud-credentials	提供了一个 IAM 策略，为 ROSA Ingress Operator 提供管理集群外部访问所需的权限。

例 3.11. openshift_ingress_operator_cloud_credentials_policy.json

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

表 3.10. ROSA 后端存储 IAM 策略和策略文件

资源	描述
ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credentials	ROSA 需要一个 IAM 策略，以通过 Container Storage Interface (CSI)管理后端存储。

例 3.12. openshift_cluster_csi_drivers_ebs_cloud_credentials_policy.json

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

```
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DetachVolume",
        "ec2:ModifyVolume"
      ],
      "Resource": "*"
    }
  ]
}
```

表 3.11. ROSA Machine Config Operator 策略和策略文件

资源	描述
ManagedOpenShift-openshift-machine-api-aws-cloud-credentials	提供了一个 IAM 策略，该策略为 ROSA Machine Config Operator 提供执行核心集群功能所需的权限。

例 3.13. openshift_machine_api_aws_cloud_credentials_policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
```

```
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "iam:PassRole",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlainText",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:RevokeGrant",
        "kms:CreateGrant",
        "kms:ListGrants"
      ],
      "Resource": "*",
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}
```

表 3.12. ROSA Cloud Credential Operator 策略和策略文件

资源	描述
ManagedOpenShift-openshift-cloud-credential-operator-cloud-credentials	提供了一个 IAM 策略，它为 ROSA Cloud Credential Operator 提供管理云供应商凭证所需的权限。

例 3.14. openshift_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

表 3.13. ROSA Image Registry Operator 策略和策略文件

资源	描述
ManagedOpenShift-openshift-image-registry-installer-cloud-credentials	提供了一个 IAM 策略，它为 ROSA Image Registry Operator 提供管理集群 AWS S3 中的 OpenShift 镜像 registry 存储所需的权限。

例 3.15. openshift_image_registry_installer_cloud_credentials_policy.json

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

其他资源

- 有关 OpenShift 主要、次版本和补丁版本的定义，请参阅 Red Hat OpenShift Service on AWS 更新生命周期。

3.2.2. 帐户范围的 IAM 角色和策略 AWS CLI 参考

本节列出了 **rosa** 命令在终端中生成的 **aws** CLI 命令。您可以使用手动或自动模式运行该命令。

使用手动模式创建帐户角色
manual 角色创建模式为您生成 **aws** 命令，供您查看并运行。以下命令启动该进程，其中 &lt **;openshift_version&** gt; 是指 AWS (ROSA)上的 Red Hat OpenShift Service 版本，如 **4.16**。

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

注意

提供的命令示例包括 **ManagedOpenShift** 前缀。如果没有使用 **--prefix** 选项指定自定义前缀，则 **ManagedOpenShift** 前缀是默认值。

命令输出

```
aws iam create-role \
 --role-name ManagedOpenShift-Installer-Role \
 --assume-role-policy-document file://sts_installer_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=rosa_role_type,Value=installer

aws iam put-role-policy \
 --role-name ManagedOpenShift-Installer-Role \
 --policy-name ManagedOpenShift-Installer-Role-Policy \
 --policy-document file://sts_installer_permission_policy.json

aws iam create-role \
 --role-name ManagedOpenShift-ControlPlane-Role \
 --assume-role-policy-document file://sts_instance_controlplane_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=rosa_role_type,Value=instance_controlplane

aws iam put-role-policy \
 --role-name ManagedOpenShift-ControlPlane-Role \
 --policy-name ManagedOpenShift-ControlPlane-Role-Policy \
 --policy-document file://sts_instance_controlplane_permission_policy.json

aws iam create-role \
 --role-name ManagedOpenShift-Worker-Role \
 --assume-role-policy-document file://sts_instance_worker_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=rosa_role_type,Value=instance_worker

aws iam put-role-policy \
 --role-name ManagedOpenShift-Worker-Role \
 --policy-name ManagedOpenShift-Worker-Role-Policy \
 --policy-document file://sts_instance_worker_permission_policy.json

aws iam create-role \
```

```
 --role-name ManagedOpenShift-Support-Role \
 --assume-role-policy-document file://sts_support_trust_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=rosa_role_type,Value=support

aws iam put-role-policy \
 --role-name ManagedOpenShift-Support-Role \
 --policy-name ManagedOpenShift-Support-Role-Policy \
 --policy-document file://sts_support_permission_policy.json

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-ingress-operator-cloud-credentials \
 --policy-document file://openshift_ingress_operator_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=operator_namespace,Value=openshift-ingress-
operator Key=operator_name,Value=cloud-credentials

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-cluster-csi-drivers-ebs-cloud-credent \
 --policy-document file://openshift_cluster_csi_drivers_ebs_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=operator_namespace,Value=openshift-cluster-
csi-drivers Key=operator_name,Value=ebs-cloud-credentials

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-machine-api-aws-cloud-credentials \
 --policy-document file://openshift_machine_api_aws_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=operator_namespace,Value=openshift-
machine-api Key=operator_name,Value=aws-cloud-credentials

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-cloud-credential-operator-cloud-crede \
 --policy-document
file://openshift_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=operator_namespace,Value=openshift-cloud-
credential-operator Key=operator_name,Value=cloud-credential-operator-iam-ro-creds

aws iam create-policy \
 --policy-name ManagedOpenShift-openshift-image-registry-installer-cloud-creden \
 --policy-document file://openshift_image_registry_installer_cloud_credentials_policy.json \
 --tags Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value=ManagedOpenShift Key=operator_namespace,Value=openshift-image-
registry Key=operator_name,Value=installer-cloud-credentials
```

使用 auto 模式创建角色

添加 **--mode auto** 参数时，Red Hat OpenShift Service on AWS (ROSA) CLI，**rosa** 会创建您的角色和策略。以下命令启动该进程：

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

注意

提供的命令示例包括 **ManagedOpenShift** 前缀。如果没有使用 **--prefix** 选项指定自定义前缀，则 **ManagedOpenShift** 前缀是默认值。

命令输出

```
I: Creating roles using 'arn:aws:iam::<ARN>:user/<UserID>'
? Create the 'ManagedOpenShift-Installer-Role' role? Yes
I: Created role 'ManagedOpenShift-Installer-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-Installer-Role'
? Create the 'ManagedOpenShift-ControlPlane-Role' role? Yes
I: Created role 'ManagedOpenShift-ControlPlane-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-ControlPlane-Role'
? Create the 'ManagedOpenShift-Worker-Role' role? Yes
I: Created role 'ManagedOpenShift-Worker-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-Worker-Role'
? Create the 'ManagedOpenShift-Support-Role' role? Yes
I: Created role 'ManagedOpenShift-Support-Role' with ARN 'arn:aws:iam::
<ARN>:role/ManagedOpenShift-Support-Role'
? Create the operator policies? Yes
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-machine-api-
aws-cloud-credentials'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-cloud-
credential-operator-cloud-crede'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-image-registry-
installer-cloud-creden'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-ingress-
operator-cloud-credentials'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-cluster-csi-
drivers-ebs-cloud-credent'
I: Created policy with ARN 'arn:aws:iam::<ARN>:policy/ManagedOpenShift-openshift-cloud-network-
config-controller-cloud'
I: To create a cluster with these roles, run the following command:
rosa create cluster --sts
```

3.3. 安装程序角色的权限边界

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

注意

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

权限边界策略文件如下：

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

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

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

在使用权限边界策略时，会应用以下组合：

- 没有权限边界策略意味着，完整的安装程序策略权限应用到集群。

- **core** 仅为安装程序角色设置最受限的权限。VPC 和 PL 权限不包括在 **Core only** boundary 策略中。
  - 安装程序无法创建和管理 VPC 或 PL。
  - 您必须具有客户提供的 VPC，而 PrivateLink (PL)不可用。

- **Core + VPC** 为安装程序角色设置 core 和 VPC 权限。
  - 安装程序无法创建和管理 PL。
  - 假设您没有使用 custom/BYO-VPC。
  - 假设安装程序将创建和管理 VPC。

- **Core + PrivateLink (PL)**意味着安装程序可以置备 PL 基础架构。
  - 您必须具有客户提供的 VPC。
  - 这适用于带有 PL 的私有集群。

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

例 3.16. sts_installer_core_permission_boundary_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
  "autoscaling:DescribeAutoScalingGroups",
  "ec2:AllocateAddress",
  "ec2:AssociateAddress",
  "ec2:AttachNetworkInterface",
  "ec2:AuthorizeSecurityGroupEgress",
  "ec2:AuthorizeSecurityGroupIngress",
  "ec2:CopyImage",
  "ec2:CreateNetworkInterface",
  "ec2:CreateSecurityGroup",
  "ec2:CreateTags",
  "ec2:CreateVolume",
  "ec2:DeleteNetworkInterface",
  "ec2:DeleteSecurityGroup",
```

```
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetConsoleOutput",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
```

```
"elasticloadbalancing:DeregisterTargets",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:ModifyLoadBalancerAttributes",
"elasticloadbalancing:ModifyTargetGroup",
"elasticloadbalancing:ModifyTargetGroupAttributes",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
"iam:AddRoleToInstanceProfile",
"iam:CreateInstanceProfile",
"iam:DeleteInstanceProfile",
"iam:GetInstanceProfile",
"iam:TagInstanceProfile",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:ListAttachedRolePolicies",
"iam:ListInstanceProfiles",
"iam:ListInstanceProfilesForRole",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:PassRole",
"iam:RemoveRoleFromInstanceProfile",
"iam:SimulatePrincipalPolicy",
"iam:TagRole",
"iam:UntagRole",
"route53:ChangeResourceRecordSets",
"route53:ChangeTagsForResource",
"route53:CreateHostedZone",
"route53:DeleteHostedZone",
"route53:GetAccountLimit",
"route53:GetChange",
"route53:GetHostedZone",
"route53:ListHostedZones",
"route53:ListHostedZonesByName",
"route53:ListResourceRecordSets",
"route53:ListTagsForResource",
"route53:UpdateHostedZoneComment",
"s3:CreateBucket",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:GetAccelerateConfiguration",
"s3:GetBucketAcl",
"s3:GetBucketCORS",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketObjectLockConfiguration",
```

```
        "s3:GetBucketPolicy",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectTagging",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "sts:AssumeRole",
        "sts:AssumeRoleWithWebIdentity",
        "sts:GetCallerIdentity",
        "tag:GetResources",
        "tag:UntagResources",
        "kms:DescribeKey",
        "cloudwatch:GetMetricData",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:ModifyVpcEndpointServicePermissions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

重要

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

前提条件

- 您有一个 AWS 帐户。
- 您有管理 AWS 角色和策略所需的权限。
- 您已在工作站上安装和配置了最新的 AWS (**aws**)和 ROSA (**rosa**) CLI。
- 您已准备了 ROSA 集群范围的角色，包括安装程序角色和对应的策略。如果 AWS 帐户中不存在它们，*请参阅附加资源* 中的"创建账户范围的 STS 角色和策略"。

流程

1. 在 **rosa** CLI 中输入以下命令来准备策略文件：

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

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

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

输出示例

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

3. 输入以下命令在您要限制的安装程序角色中添加权限边界策略：

```
$ aws iam put-role-permissions-boundary \
```

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

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

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

输出示例

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

有关 PL 和 VPC 权限边界策略的更多示例，请参阅：

例 3.17. sts_installer_privatelink_permission_boundary_policy.json

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

例 3.18. sts_installer_vpc_permission_boundary_policy.json

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
      "ec2:AssociateDhcpOptions",
      "ec2:AssociateRouteTable",
      "ec2:AttachInternetGateway",
      "ec2:CreateDhcpOptions",
      "ec2:CreateInternetGateway",
      "ec2:CreateNatGateway",
      "ec2:CreateRouteTable",
```

```
            "ec2:CreateSubnet",
            "ec2:CreateVpc",
            "ec2:DeleteDhcpOptions",
            "ec2:DeleteInternetGateway",
            "ec2:DeleteNatGateway",
            "ec2:DeleteRouteTable",
            "ec2:DeleteSubnet",
            "ec2:DeleteVpc",
            "ec2:DetachInternetGateway",
            "ec2:DisassociateRouteTable",
            "ec2:ModifySubnetAttribute",
            "ec2:ModifyVpcAttribute",
            "ec2:ReplaceRouteTableAssociation"
                ],
                "Resource": "*"
            }
        ]
    }
```

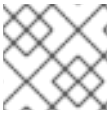
其他资源

- 如需更多信息，请参阅 IAM 实体(AWS 文档)的权限边界。
- 有关创建所需的帐户范围 STS 角色和策略的更多信息，请参阅创建集群范围的 STS 角色和策略。

3.4. 集群特定 OPERATOR IAM 角色参考

本节详细介绍了使用 STS 的 AWS (ROSA) 部署的 Red Hat OpenShift Service 所需的 Operator IAM 角色。集群 Operator 使用 Operator 角色获取执行集群操作所需的临时权限，如管理后端存储、云供应商凭证和对集群的外部访问权限。

在创建 Operator 角色时，匹配的集群版本的 account-wide Operator 策略会附加到角色中。Operator 策略使用 Operator 标记，以及它们与之兼容的版本。Operator 角色的正确策略通过使用标签来决定。



注意

如果您的帐户中有多个匹配策略，则创建 Operator 时会提供一个交互式选项列表。

表 3.14. ROSA 集群特定 Operator 角色

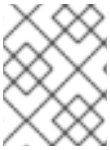
资源	描述
<cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credentials	ROSA 需要的 IAM 角色，以通过 Container Storage Interface (CSI) 管理后端存储。
<cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials	ROSA Machine Config Operator 所需的 IAM 角色，以执行核心集群功能。

资源	描述
<cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-credentials	ROSA Cloud Credential Operator 所需的 IAM 角色来管理云供应商凭证。
<cluster_name>-<hash>-openshift-cloud-network-config-controller-credentials	云网络配置控制器所需的 IAM 角色来管理集群的云网络配置。
<cluster_name>-<hash>-openshift-image-registry-installer-cloud-credentials	ROSA Image Registry Operator 所需的 IAM 角色，用于管理集群的 AWS S3 中的 OpenShift 镜像 registry 存储。
<cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials	ROSA Ingress Operator 所需的 IAM 角色来管理集群的外部访问。
<cluster_name>-<hash>-openshift-cloud-network-config-controller-cloud-credentials	云网络配置控制器所需的 IAM 角色来管理集群的云网络凭证。

3.4.1. Operator IAM 角色 AWS CLI 参考

本节列出了在使用手动模式运行以下 **rosa** 命令时在终端中显示的 **aws** CLI 命令：

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



注意

使用手动模式时，**aws** 命令会被打印到终端中，供您查看。查看 **aws** 命令后，您必须手动运行它们。另外，您可以使用 **rosa create** 命令指定 **--mode auto** 来立即运行 **aws** 命令。

命令输出

```
aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credent \
 --assume-role-policy-document file://operator_cluster_csi_drivers_ebs_cloud_credentials_policy.json
\
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-cluster-csi-drivers
Key=operator_name,Value=ebs-cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-cluster-csi-drivers-ebs-cloud-credent \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-cluster-csi-drivers-
ebs-cloud-credent

aws iam create-role \
```

```
 --role-name <cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials \
 --assume-role-policy-document file://operator_machine_api_aws_cloud_credentials_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-machine-api
Key=operator_name,Value=aws-cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-machine-api-aws-cloud-credentials \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-machine-api-aws-
cloud-credentials

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-crede \
 --assume-role-policy-document
file://operator_cloud_credential_operator_cloud_credential_operator_iam_ro_creds_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-cloud-credential-operator
Key=operator_name,Value=cloud-credential-operator-iam-ro-creds

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-cloud-credential-operator-cloud-crede \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-cloud-credential-
operator-cloud-crede

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-image-registry-installer-cloud-creden \
 --assume-role-policy-document file://operator_image_registry_installer_cloud_credentials_policy.json
\
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-image-registry
Key=operator_name,Value=installer-cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-image-registry-installer-cloud-creden \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-image-registry-
installer-cloud-creden

aws iam create-role \
 --role-name <cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials \
 --assume-role-policy-document file://operator_ingress_operator_cloud_credentials_policy.json \
 --tags Key=rosa_cluster_id,Value=<id> Key=rosa_openshift_version,Value=<openshift_version>
Key=rosa_role_prefix,Value= Key=operator_namespace,Value=openshift-ingress-operator
Key=operator_name,Value=cloud-credentials

aws iam attach-role-policy \
 --role-name <cluster_name>-<hash>-openshift-ingress-operator-cloud-credentials \
 --policy-arn arn:aws:iam::<aws_account_id>:policy/ManagedOpenShift-openshift-ingress-operator-
cloud-credentials
```

注意

表中提供的命令示例包括使用 **ManagedOpenShift** 前缀的 Operator 角色。如果您在创建集群范围的角色和策略（包括 Operator 策略）时定义了自定义前缀，您必须在创建 Operator 角色时使用 **--prefix <prefix_name>** 选项来引用它。

3.4.2. 关于自定义 Operator IAM 角色前缀

每个使用 AWS 安全令牌服务 (STS) 的 Red Hat OpenShift Service on AWS (ROSA)都需要集群特定的 Operator IAM 角色。

默认情况下，Operator 角色名称使用集群名称和随机 4 位的哈希作为前缀。例如，名为 **mycluster** 的集群的 Cloud Credential Operator IAM 角色具有默认名称 **mycluster-<hash>-openshift-cloud-credential-operator-cloud-credentials**，其中 **<hash>** 是一个随机 4 位字符串。

通过这个默认命名惯例，您可以在 AWS 帐户中轻松识别集群的 Operator IAM 角色。

当您为集群创建 Operator 角色时，您可以选择指定要使用的自定义前缀，而不是 **<cluster_name>-<hash>**。通过使用自定义前缀，您可以在 Operator 角色名称前添加逻辑标识符来满足您的环境的要求。例如，您可以为集群名称和环境类型添加前缀，如 **mycluster-dev**。在本例中，带有自定义前缀的 Cloud Credential Operator 角色名称为 **mycluster-dev-openshift-cloud-credential-operator-cloud-credenti**。

注意

角色名称被截断为 64 个字符。

其他资源

> For steps to create the cluster-specific Operator IAM roles using a custom prefix, see link:https://docs.redhat.com/en/documentation/red_hat_openshift_service_on_aws/4/html-single/install_rosa_classic_clusters/#rosa-sts-creating-cluster-customizations-cli_rosa-sts-creating-a-cluster-with-customizations[Creating a cluster with customizations using the CLI] or link:https://docs.redhat.com/en/documentation/red_hat_openshift_service_on_aws/4/html-single/install_rosa_classic_clusters/#rosa-sts-creating-cluster-customizations-ocm_rosa-sts-creating-a-cluster-with-customizations[Creating a cluster with customizations by using {cluster-manager}].

3.5. 为 OPERATOR 身份验证打开 ID CONNECT (OIDC)要求

对于使用 STS 的 ROSA 安装，您必须创建一个特定于集群的 OIDC 供应商，供集群 Operator 为您自己的 OIDC 供应商进行身份验证或创建自己的 OIDC 配置。

3.5.1. 使用 CLI 创建 OIDC 供应商

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI 创建托管在 AWS 帐户中的 OIDC 供应商 **rosa**。

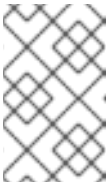
前提条件

- 已安装最新版本的 ROSA CLI。

流程

- 要创建 OIDC 供应商，使用未注册或注册的 OIDC 配置。
  - 取消注册的 OIDC 配置要求您通过集群创建 OIDC 供应商。运行以下命令来创建 OIDC 供应商：

```
$ rosa create oidc-provider --mode manual --cluster <cluster_name>
```



注意

使用手动模式时，**aws** 命令会被打印到终端中，供您查看。查看 **aws** 命令后，您必须手动运行。另外，您可以使用 **rosa create** 命令指定 **--mode auto** 来立即运行 **aws** 命令。

命令输出

```
aws iam create-open-id-connect-provider \
 --url https://oidc.op1.openshiftapps.com/<oidc_config_id> \ 1
 --client-id-list openshift sts.<aws_region>.amazonaws.com \
 --thumbprint-list <thumbprint> 2
```

1. 在集群创建后用于访问 OpenID Connect (OIDC)身份提供程序的 URL。
2. 在运行 **rosa create oidc-provider** 命令时，会自动生成 thumbprint。有关在 AWS Identity and Access Management (IAM) OIDC 身份提供程序中使用 thumbprints 的更多信息，请参阅 AWS 文档。

- 注册的 OIDC 配置使用 OIDC 配置 ID。使用您的 OIDC 配置 ID 运行以下命令：

```
$ rosa create oidc-provider --oidc-config-id <oidc_config_id> --mode auto -y
```

命令输出

```
I: Creating OIDC provider using 'arn:aws:iam::4540112244:user/userName'
I: Created OIDC provider with ARN 'arn:aws:iam::4540112244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/241rh9ql5gpu99d7leokhvkp8icnalpf'
```

3.5.2. 创建 OpenID 连接配置

当使用由红帽托管的集群时，您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa** 创建受管或非受管 OpenID Connect (OIDC)配置。受管 OIDC 配置存储在红帽的 AWS 帐户中，而生成的非受管 OIDC 配置存储在 AWS 帐户中。OIDC 配置已注册到 OpenShift Cluster Manager。在创建非受管 OIDC 配置时，CLI 为您提供了私钥。

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

前提条件

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

流程

1. 要创建 OIDC 配置和 AWS 资源，请运行以下命令：

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

此命令返回以下信息：

输出示例

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

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

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

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

1 在上面的示例输出中，OIDC 配置 ID 是 13cdr6b。

- 运行以下命令，查看变量的值：

```
$ echo $OIDC_ID
```

输出示例

```
13cdr6b
```

验证

- 您可以列出与用户机构关联的集群可用的 OIDC 配置。运行以下命令：

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

输出示例

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

创建自己的 OpenID Connect 配置的参数选项

以下选项可以添加到 **rosa create oidc-config** 命令中。所有这些参数都是可选的。运行没有参数的 **rosa create oidc-config** 命令会创建一个非受管 OIDC 配置。

注意

您需要通过 OpenShift Cluster Manager 将请求发布到 **/oidc_configs** 来注册非受管 OIDC 配置。您在响应中收到 ID。使用此 ID 创建集群。

raw-files
允许您为私有 RSA 密钥提供原始文件。这个密钥名为 **rosa-private-key-oidc-<random_label_of_length_4>.key**。您还收到名为 **discovery-document-oidc-<random_label_of_length_4>.json** 的发现文档，以及名为 **jwks-oidc-<random_label_of_length_4>.json** 的发现文档。

您可以使用这些文件来设置端点。此端点会响应 **/.well-known/openid-configuration**，它带有发现文档和带有 JSON Web Key Set 的 **keys.json**。私钥以纯文本形式存储在 Amazon Web Services (AWS) Secrets Manager Service (SMS)中。

示例

```
$ rosa create oidc-config --raw-files
```

模式
允许您指定模式来创建 OIDC 配置。使用 **manual** 选项，您可以接收在 S3 存储桶中设置 OIDC 配置的 AWS 命令。这个选项将私钥存储在 Secrets Manager 中。使用 **手动** 选项，OIDC Endpoint URL 是 S3 存储桶的 URL。您必须检索 Secret Manager ARN，以便在 OpenShift Cluster Manager 中注册 OIDC 配置。

在使用 **auto** 选项时，您会收到与 **手动模式** 相同的 OIDC 配置和 AWS 资源。两个选项之间的显著区别在于，在使用 **auto** 选项时，ROSA 调用 AWS，因此您不需要采取任何进一步的操作。OIDC 端点 URL 是 S3 存储桶的 URL。CLI 检索 Secrets Manager ARN，将 OIDC 配置注册到 OpenShift Cluster Manager，并报告用户可以运行的第二个 **rosa** 命令继续创建 STS 集群。

示例

```
$ rosa create oidc-config --mode=<auto|manual>
```

Managed
创建一个托管在红帽 AWS 帐户下的 OIDC 配置。这个命令会创建一个私钥，它直接使用 OIDC 配置 ID 响应，供您在创建 STS 集群时使用。

示例

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

输出示例

```
W: For a managed OIDC Config only auto mode is supported. However, you may choose the
provider creation mode
? OIDC Provider creation mode: auto
I: Setting up managed OIDC configuration
I: Please run the following command to create a cluster with this oidc config
rosa create cluster --sts --oidc-config-id 233jnu62i9aphpucsj9kueqlkr1vcgra
I: Creating OIDC provider using 'arn:aws:iam::242819244:user/userName'
? Create the OIDC provider? Yes
I: Created OIDC provider with ARN 'arn:aws:iam::242819244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/233jnu62i9aphpucsj9kueqlkr1vcgra'
```

3.6. 服务控制策略的最小有效权限集(SCP)

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

注意

在使用 AWS 安全令牌服务(STS)时，您必须确保服务控制策略不会阻止以下资源：

- **ec2:{}**
- **iam:{}**
- **tag:***

验证您的服务控制策略(SCP)是否不限制任何这些所需的权限。

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

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

其他资源

- 服务控制策略
- SCP 对权限的影响

3.7. 客户管理的策略

Red Hat OpenShift Service on AWS (ROSA)用户可以将客户管理的策略附加到运行和维护 ROSA 集群所需的 IAM 角色。AWS IAM 角色不常见此功能。将这些策略附加到 ROSA 特定的 IAM 角色会扩展 ROSA 集群的权限功能；例如，允许集群组件访问不属于 ROSA 的 IAM 策略的额外 AWS 资源。

为确保任何依赖客户策略的关键客户应用程序在集群或角色升级过程中以任何方式修改，ROSA 会使用 **ListAttachedRolesPolicies** 权限从角色中检索权限策略列表，以及 **ListRolePolicies** 权限从 ROSA 特定角色检索策略列表。此信息可确保，客户管理的策略在集群事件过程中不会受到影响，并允许 Red Hat SRE 监控附加到 ROSA 特定 IAM 角色的 ROSA 和客户管理的策略，从而更有效地对集群问题进行故障排除。

警告

不支持将权限边界策略附加到用于限制 ROSA 的策略的 IAM 角色，因为这些策略可能会中断成功运行和维护 ROSA 集群所需的基本权限的功能。ROSA （经典架构）安装程序角色准备了权限边界策略。如需更多信息，请参阅附加资源部分。

其他资源

- 安装程序角色的权限界限
- IAM 实体的权限界限

第 4 章 OPENID CONNECT 概述

OpenID Connect (OIDC)使用安全令牌服务(STS)来允许客户端提供 Web 身份令牌来访问多个服务。当客户端使用 STS 登录到服务时，会根据 OIDC 身份提供程序验证令牌。

OIDC 协议使用配置 URL，其中包含验证客户端身份的必要信息。该协议使用供应商所需的凭证来响应提供程序，以验证客户端并登录。

Red Hat OpenShift Service on AWS 集群使用 STS 和 OIDC 来授予集群内 Operator 对所需 AWS 资源的访问权限。

4.1. 了解 OIDC 验证选项

OIDC 验证有三个选项：

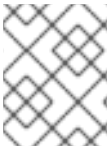
- 未注册，管理的 OIDC 配置
  在集群安装过程中会为您创建未注册、管理的 OIDC 配置。该配置托管在红帽的 AWS 帐户下。这个选项不为您提供链接到 OIDC 配置的 ID，因此您只能在单个集群中使用这种类型的 OIDC 配置。

- 注册、管理的 OIDC 配置
  在开始创建集群前，您可以创建注册的、管理的 OIDC 配置。此配置托管在红帽的 AWS 帐户下，如取消注册的受管 OIDC 配置。当您将这个选项用于 OIDC 配置时，您会收到到 OIDC 配置链接的 ID。红帽使用此 ID 来识别签发者 URL 和私钥。然后，您可以使用此 URL 和私钥创建身份提供程序和 Operator 角色。这些资源通过使用 Identity and Access Management (IAM) AWS 服务在 AWS 帐户下创建。您还可以在集群创建过程中使用 OIDC 配置 ID。

- registered, 非受管 OIDC 配置
  在开始创建集群前，您可以创建注册的、非受管 OIDC 配置。此配置托管在您的 AWS 帐户下。使用这个选项时，您需要管理私钥。您可以使用 AWS Secrets Manager (SM)服务和托管配置的签发者 URL 将私钥存储在 AWS secret 文件中，将配置注册到 Red Hat OpenShift Cluster Manager。您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa**, 使用 **rosa create oidc-config --managed=false** 命令创建注册的、非受管 OIDC 配置。此命令在您的帐户下创建并托管配置，并创建必要的文件和私钥。此命令还会将配置注册到 OpenShift Cluster Manager。

注册的选项可用于在开始创建集群前创建所需的 IAM 资源。这个选项会导致安装时间更快，因为集群创建过程中有一个等待周期，安装会暂停，直到创建 OIDC 供应商和 Operator 角色为止。

对于 ROSA Classic，您可以使用任何 OIDC 配置选项。如果您使用带有 HCP 的 ROSA，您必须创建注册的 OIDC 配置，可以是受管或非受管。您可以与其他集群共享注册的 OIDC 配置。通过共享配置，您还可以共享 provider 和 Operator 角色。



注意

不建议在生产环境集群中重复使用 OIDC 配置、OIDC 供应商和 Operator 角色，因为在整个集群中都使用了验证验证。红帽建议仅在非生产环境测试环境中重复使用资源。

4.2. 创建 OPENID 连接配置

当使用由红帽托管的集群时，您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI, **rosa** 创建受管或非受管 OpenID Connect (OIDC)配置。受管 OIDC 配置存储在红帽的 AWS 帐户中，而生成的非受管 OIDC 配置存储在 AWS 帐户中。OIDC 配置已注册到 OpenShift Cluster Manager。在创建非受管 OIDC 配置时，CLI 为您提供了私钥。

创建 OpenID 连接配置

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

前提条件

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

流程

1. 要创建 OIDC 配置和 AWS 资源，请运行以下命令：

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

此命令返回以下信息：

输出示例

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

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

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

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

1 在上面的示例输出中，OIDC 配置 ID 是 13cdr6b。

- 运行以下命令，查看变量的值：

```
$ echo $OIDC_ID
```

输出示例

```
13cdr6b
```

验证

- 您可以列出与用户机构关联的集群可用的 OIDC 配置。运行以下命令：

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

输出示例

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

创建自己的 OpenID Connect 配置的参数选项
以下选项可以添加到 **rosa create oidc-config** 命令中。所有这些参数都是可选的。运行没有参数的 **rosa create oidc-config** 命令会创建一个非受管 OIDC 配置。

注意

您需要通过 OpenShift Cluster Manager 将请求发布到 **/oidc_configs** 来注册非受管 OIDC 配置。您在响应中收到 ID。使用此 ID 创建集群。

raw-files
允许您为私有 RSA 密钥提供原始文件。这个密钥名为 **rosa-private-key-oidc-<random_label_of_length_4>.key**。您还收到名为 **discovery-document-oidc-<random_label_of_length_4>.json** 的发现文档，以及名为 **jwks-oidc-<random_label_of_length_4>.json** 的发现文档。

您可以使用这些文件来设置端点。此端点会响应 **/.well-known/openid-configuration**，它带有发现文档和带有 JSON Web Key Set 的 **keys.json**。私钥以纯文本形式存储在 Amazon Web Services (AWS) Secrets Manager Service (SMS)中。

示例

```
$ rosa create oidc-config --raw-files
```

模式
允许您指定模式来创建 OIDC 配置。使用 **manual** 选项，您可以接收在 S3 存储桶中设置 OIDC 配置的 AWS 命令。这个选项将私钥存储在 Secrets Manager 中。使用 **手动** 选项，OIDC Endpoint URL 是 S3 存储桶的 URL。您必须检索 Secret Manager ARN，以便在 OpenShift Cluster Manager 中注册 OIDC 配置。

在使用 **auto** 选项时，您会收到与 **手动模式** 相同的 OIDC 配置和 AWS 资源。两个选项之间的显著区别在于，在使用 **auto** 选项时，ROSA 调用 AWS，因此您不需要采取任何进一步的操作。OIDC 端点 URL 是 S3 存储桶的 URL。CLI 检索 Secrets Manager ARN，将 OIDC 配置注册到 OpenShift Cluster Manager，并报告用户可以运行的第二个 **rosa** 命令继续创建 STS 集群。

示例

```
$ rosa create oidc-config --mode=<auto|manual>
```

Managed
创建一个托管在红帽 AWS 帐户下的 OIDC 配置。这个命令会创建一个私钥，它直接使用 OIDC 配置 ID 响应，供您在创建 STS 集群时使用。

示例

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

输出示例

```
W: For a managed OIDC Config only auto mode is supported. However, you may choose the
provider creation mode
? OIDC Provider creation mode: auto
I: Setting up managed OIDC configuration
I: Please run the following command to create a cluster with this oidc config
rosa create cluster --sts --oidc-config-id 233jnu62i9aphpucsj9kueqlkr1vcgra
I: Creating OIDC provider using 'arn:aws:iam::242819244:user/userName'
? Create the OIDC provider? Yes
I: Created OIDC provider with ARN 'arn:aws:iam::242819244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/233jnu62i9aphpucsj9kueqlkr1vcgra'
```

4.3. 使用 CLI 创建 OIDC 供应商

您可以使用 Red Hat OpenShift Service on AWS (ROSA) CLI 创建托管在 AWS 帐户中的 OIDC 供应商 **rosa**。

前提条件

- 已安装最新版本的 ROSA CLI。

流程

- 要创建 OIDC 供应商，使用未注册或注册的 OIDC 配置。
  - 取消注册的 OIDC 配置要求您通过集群创建 OIDC 供应商。运行以下命令来创建 OIDC 供应商：

    ```
    $ rosa create oidc-provider --mode manual --cluster <cluster_name>
    ```

    注意

    使用手动模式时，**aws** 命令会被打印到终端中，供您查看。查看 **aws** 命令后，您必须手动运行。另外，您可以使用 **rosa create** 命令指定 **--mode auto** 来立即运行 **aws** 命令。

    命令输出

    ```
    aws iam create-open-id-connect-provider \
     --url https://oidc.op1.openshiftapps.com/<oidc_config_id> \ 1
     --client-id-list openshift sts.<aws_region>.amazonaws.com \
     --thumbprint-list <thumbprint> 2
    ```

    1 在集群创建后用于访问 OpenID Connect (OIDC)身份提供程序的 URL。

    2 在运行 **rosa create oidc-provider** 命令时，会自动生成 thumbprint。有关在 AWS Identity and Access Management (IAM) OIDC 身份提供程序中使用 thumbprints 的更多信息，请参阅 AWS 文档。

  - 注册的 OIDC 配置使用 OIDC 配置 ID。使用您的 OIDC 配置 ID 运行以下命令：

    ■

```
$ rosa create oidc-provider --oidc-config-id <oidc_config_id> --mode auto -y
```

命令输出

```
I: Creating OIDC provider using 'arn:aws:iam::4540112244:user/userName'
I: Created OIDC provider with ARN 'arn:aws:iam::4540112244:oidc-
provider/dvbwgdztaeq9o.cloudfront.net/241rh9ql5gpu99d7leokhvkp8icnalpf'
```

4.4. 其他资源

- 请参阅 为 ROSA Classic 创建 OpenID Connect 配置。
- 请参阅为使用 HCP 的 ROSA 创建 OpenID Connect 配置。