Red Hat OpenStack Services on OpenShift 18.0

规划部署

在 Red Hat OpenShift Container Platform 集群上规划 Red Hat OpenStack Services on OpenShift 环境

Last Updated: 2024-12-11

Red Hat OpenStack Services on OpenShift 18.0 规划部署

在 Red Hat OpenShift Container Platform 集群上规划 Red Hat OpenStack Services on OpenShift 环境

OpenStack Team
rhos-docs@redhat.com

法律通告

摘要

在 OpenShift control plane 和数据平面上规划 Red Hat OpenStack Services。

目录

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。与我们分享您的成功秘诀。

在 JIRA 中提供文档反馈

使用 Create Issue 表单在 OpenShift (RHOSO)或更早版本的 Red Hat OpenStack Platform (RHOSP)上提供有关 Red Hat OpenStack Services 文档的反馈。当您为 RHOSO 或 RHOSP 文档创建问题时，这个问题将在 RHOSO Jira 项目中记录，您可以在其中跟踪您的反馈的进度。

要完成 Create Issue 表单，请确保您已登录到 JIRA。如果您没有红帽 JIRA 帐户，您可以在 https://issues.redhat.com 创建一个帐户。

1. 点击以下链接打开 **Create Issue** 页面： Create Issue
2. 完成 **Summary** 和 **Description** 字段。在 **Description** 字段中，包含文档 URL、章节号以及问题的详细描述。不要修改表单中的任何其他字段。
3. 点 **Create**。

第 1 章 RED HAT OPENSTACK SERVICES ON OPENSHIFT 概述

Red Hat OpenStack Services on OpenShift (RHOSO)提供了在 Red Hat Enterprise Linux 之上构建私有或公共基础设施即服务(IaaS)云的基础。它是用于开发支持云工作负载的可扩展、容错平台。

RHOSO control plane 作为 Red Hat OpenShift Container Platform (RHOCP)集群上的工作负载托管和管理。RHOSO 数据平面由托管 RHOSO 工作负载的 Red Hat Ansible Automation Platform 管理的外部 Red Hat Enterprise Linux (RHEL)节点组成。data plane 节点可以是 Compute 节点、存储节点、网络节点或其他节点类型。

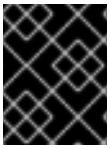
RHOSO IaaS 云通过一系列交互服务来实施，这些服务控制其计算、存储和网络资源。您可以通过基于 Web 的界面来管理云，以控制、配置和自动化 RHOSO 资源。另外，广泛的 API 控制 RHOSO 基础架构，此 API 也可供云的最终用户使用。

注意

RHOSO 仅支持基于 64 位 x86 硬件架构的 RHOCP master 和 worker 节点。

1.1. RHOSO 服务和 OPERATOR

Red Hat OpenStack Services on OpenShift (RHOSO) IaaS 服务作为在 Red Hat OpenShift Container Platform (RHOCP)集群上运行的一系列 Operator 实施。这些 Operator 管理 RHOSO 云的计算、存储、网络和其他服务。



重要

红帽建议使用 Red Hat OpenShift Container Platform (RHOCP) OperatorHub 获取所有 Operator。

OpenStack Operator (**openstack-operator**)安装 Services 表中详述的所有服务 Operator，是用于管理这些 Operator 的接口。OpenStack Operator 还安装和管理以下 Operator：

openstack-baremetal-operator

在裸机节点置备过程中由 OpenStack Operator 使用。

有关每个服务的功能的更多信息，请参阅 OpenShift 18.0 文档中的 Red Hat OpenStack Services 中的 特定于服务的文档。

表 1.1. 服务

service	Operator	default	描述
裸机置备(ironic)	**ironic-operator**	Disabled	支持各种带有特定于硬件驱动程序的硬件厂商的物理计算机。裸机调配与计算服务集成，以调配虚拟机的方式调配物理计算机，并为裸机到可信项目用例提供解决方案。
Block Storage (cinder)	**cinder-operator**	Enabled	为虚拟机实例提供和管理永久块存储卷。
Compute (nova)	**nova-operator**	Enabled	通过 **ironic** 驱动程序通过 **libvirt** 驱动程序或物理服务器提供计算资源的调配，如虚拟机。

service	Operator	default	描述
dashboard (horizon)	**Horizon-operator**	Disabled	提供基于浏览器的 GUI 仪表板，用于创建和管理云资源和用户访问权限。Dashboard 服务默认提供 Project、Admin 和 Settings 仪表板。您可以将仪表板配置为与其他产品（如计费、监控和其它管理工具）进行接口。
DNS （指定）	**designate-operator**	Enabled	提供 DNS 即服务(DNSaaS)，用于管理云中的 DNS 记录和区域。您可以部署 BIND 实例来包含 DNS 记录，也可以将 DNS 服务集成到现有的 BIND 基础架构中。也可以与 RHOSO 网络服务(neutron)集成，以自动为虚拟机实例、网络端口和浮动 IP 创建记录。
身份(keystone)	**keystone-operator**	Enabled	为所有 RHOSO 服务以及管理用户、项目和角色提供用户身份验证和授权。支持多种身份验证机制，包括用户名和密码凭证、基于令牌的系统以及 AWS 风格的日志。
Image (glance)	**glance-operator**	Enabled	用于存储虚拟机镜像和卷快照等资源的 registry 服务。云用户可以添加新镜像，也可以为现有实例生成快照以进行即时存储。您可以使用快照进行备份，或用作新实例的模板。
密钥管理(barbican)	**barbican-operator**	Enabled	提供安全存储、置备和管理 secret，如密码、加密密钥和 X.509 证书。这包括密钥材料，如 Symmetric Keys、Asymmetric Keys、Certificates 和 raw 二进制数据。
负载均衡(octavia)	**octavia-operator**	Disabled	为支持多个提供商驱动程序的云提供负载平衡即服务(LBaaS)。参考提供者驱动程序(Amphora 提供者驱动程序)是一个开源、可扩展和高可用性负载均衡供应商。它通过管理虚拟机（统称为 amphorae）来实现负载平衡服务的交付，它按需创建。
MariaDB	**mariadb-operator**	Enabled	提供部署和管理 MariaDB Galera 集群 的方法。
Memcached	**infra-operator**	Enabled	提供管理基础架构的方法。
networking (neutron)	**neutron-operator**	Enabled	通过虚拟计算环境中的软件定义型网络(SDN)提供联网即服务(NaaS)。处理云中虚拟网络基础架构的创建和管理，包括网络、子网和路由器。
Object Storage (swift)	**swift-operator**	Enabled	提供高效和持久化的数据存储，包括视频、图像、电子邮件消息、文件或实例镜像等静态实体。对象作为二进制文件存储在底层文件系统中，元数据存储在各个文件的扩展属性中。

service	Operator	default	描述
OVN	**ovn-operator**	Enabled	提供部署和管理 OVN 的方法。
Orchestration (heat)	**heat-operator**	Disabled	基于模板的编配引擎支持自动创建资源堆栈。提供模板以创建和管理云资源，如存储、网络、实例或应用。您可以使用模板来创建堆栈，这些堆栈是资源的集合。
放置（放置）	**placement-operator**	Enabled	提供安装和管理 OpenStack 放置安装的方法。
Telemetry (ceilometer、prometheus)	**telemetry-operator**	Enabled	为 RHOSO 云提供用户级使用情况数据。您可以将数据用于客户计费、系统监控或警报。Telemetry 可以从现有 RHOSO 组件（如计算使用事件）发送的通知收集数据，或者通过轮询 RHOSO 基础架构资源（如 libvirt ）来收集。
RabbitMQ	**rabbitmq-cluster-operator**	Enabled	提供部署和管理 RabbitMQ 集群的方法。
共享文件系统 (manila)	**manila-operator**	Disabled	调配可供多个虚拟机实例、裸机节点或容器使用的共享文件系统。

1.2. RHOSO 环境的特性

OpenShift (RHOSO)环境中 Red Hat OpenStack Services 的基本架构包括以下功能：

容器原生虚拟化应用程序交付

RHOSO 通过使用跨 Red Hat OpenShift Container Platform (RHOCP)和 RHEL 平台的容器原生虚拟化提供，以提供容器原生虚拟化的 RHOSO 部署。

RHOCP 托管服务

RHOCP 通过使用 RHOCP Operator 托管基础架构服务和 RHOSO 控制器服务，以提供生命周期管理。

Ansible 管理的 RHEL 托管服务

RHOSO 工作负载在由 OpenStack Operator 管理的 RHEL 节点上运行。OpenStack Operator 运行 Ansible 作业来配置 RHEL data plane 节点，如 Compute 节点。RHOCP 管理调配、DNS 和配置管理。

安装程序置备的基础架构

RHOSO 安装程序启用使用安装程序置备的基础架构，它使用 RHOSO 裸机机器管理为 RHOSO 云置备 Compute 节点。

用户置备的基础架构

如果您有自己的机器ingest 和置备工作流，您可以使用 RHOSO 预置备模型将预置备硬件添加到 RHOSO 环境中，同时获得容器原生虚拟化的优势。

托管 RHOSO 客户端

RHOSO 提供了一个主机 **openstackclient** pod，它预先配置了对所部署的 RHOSO 环境的管理员访问权限。

1.3. RHOSO 18.0 已知的限制

以下列表详细介绍了 Red Hat OpenStack Services on OpenShift (RHOSO)的限制。已知的限制是 RHOSO 不支持的功能。

计算服务(nova)：

- RHOSO 18.0 不支持非路径网络后端。如需更多信息，请参阅使用 离线路径网络后端集成。
- 不支持自定义策略。如果您需要自定义策略，请联系红帽以获得支持例外。
- RHOSO 不支持以下软件包：
  - **nova-serialproxy**
  - **nova-spicehtml5proxy**
- 文件注入个人文件，将用户数据注入到虚拟机实例中。作为临时解决方案，用户可以使用 **--user-data** 选项在实例启动期间运行脚本，或者在启动实例时使用- **property** 选项设置实例元数据。如需更多信息，请参阅创建自定义实例。
- 实例的持久内存(vPMEM)。您只能在具有 NVDIMM 硬件的 Compute 节点上创建持久内存命名空间。对于 Intel Corporation on 2022 年 7 月 28 日的宣布，红帽已从 RHOSP 17.0 及之后的版本中删除对持久内存的支持，它们不再对其 Intel® Optane™ 商业投资。如需更多信息，请参阅 Intel® Optane™ Business Update: Does This Mean for Warranty and Support 。
- 非原生架构的 QEMU 模拟。
- LVM 不支持作为镜像后端。
- 不支持 **ploop** 镜像格式。
- 早于 4 的 NFS 版本。

镜像服务(glance)：

- RHOSO 只支持一个架构 x86_64。没有需要为 RHOSO 云设置它的有效用例，因此所有主机都将是 x86_64。
- 早于 4 的 NFS 版本。

块存储服务(cinder)：

- Cinder 复制。
- LVM 驱动程序。
- 早于 4 的 NFS 版本。

如果您需要支持任何这些功能，请联系红帽客户 体验和参与团队 来讨论支持例外（如果适用）或其他选项。

1.4. RHOSO 环境支持的拓扑

Red Hat OpenStack Services on OpenShift (RHOSO)支持紧凑 control plane 拓扑和专用节点 control plane 拓扑。

在紧凑拓扑中，RHOSO control plane 和 Red Hat OpenShift Container Platform (RHOCP) control plane 共享相同的物理节点。

在专用节点拓扑中，RHOCP control plane 在一组物理节点上运行，RHOSO 控制平面在另一组物理节点上运行。

1.4.1. 紧凑拓扑

紧凑的 RHOSO 拓扑是默认值，它由以下组件组成：

OpenShift 紧凑集群

托管 RHOSO 和 RHOCP control plane 的 Red Hat OpenShift 集群。
RHOSO 控制平面由 OpenStack 控制器服务 pod 组成，它们由计算服务(nova)、网络服务(neutron)等服务组成。

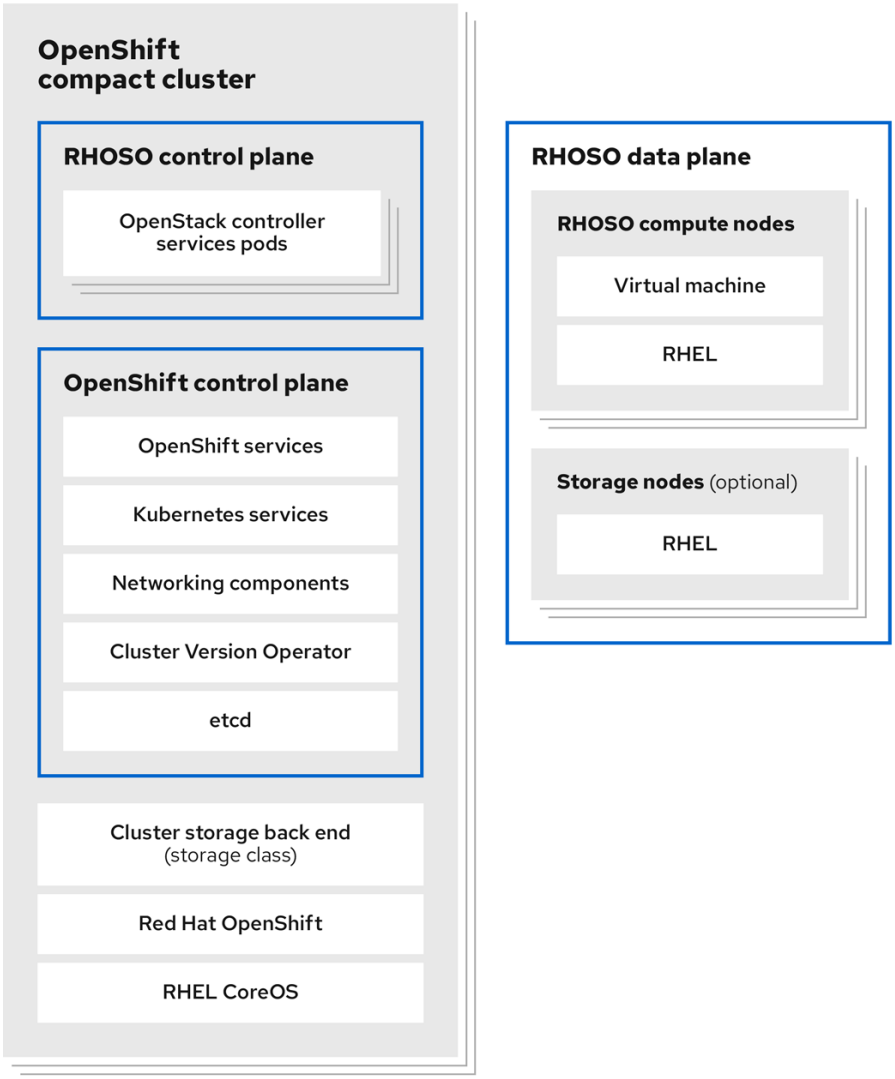
OpenShift control plane 托管运行 RHOCP 所需的以下服务的 pod：OpenShift 服务、Kubernetes 服务、网络组件、Cluster Version Operator 和 etcd。

如需更多信息，请参阅 RHOCP *架构指南中的 OpenShift Container Platform 简介*

RHOSO 数据平面

RHOSO 数据平面由 OpenStack Compute 节点组成。专用于存储的节点是可选的。

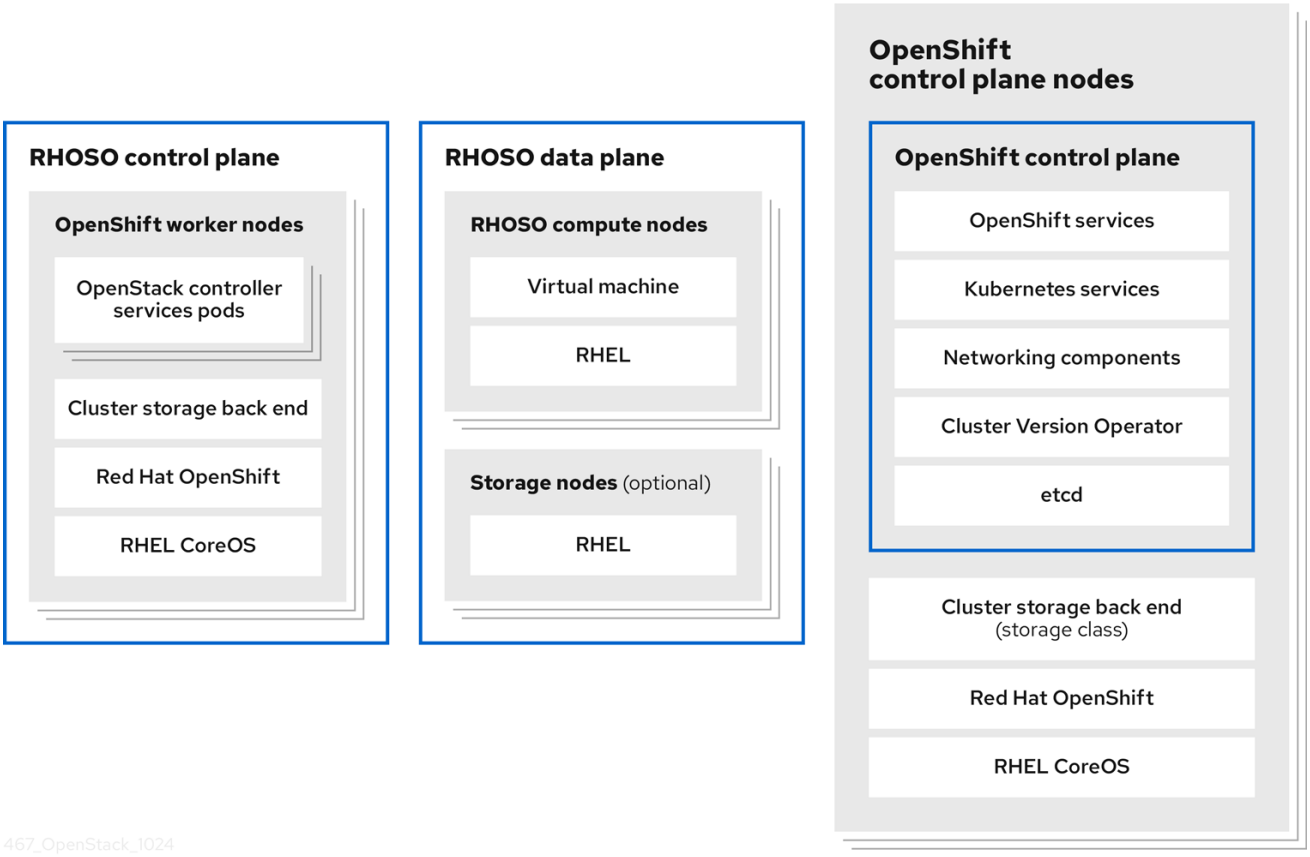
图 1.1. 紧凑 RHOSO 拓扑



1.4.2. 专用节点拓扑

专用节点 RHOSO 拓扑与紧凑拓扑不同，因为 RHOSO control plane 有一个单独的节点集群，以及用于 OpenShift control plane 的独立节点集群。

图 1.2. 专用节点 RHOSO 拓扑



第 2 章 规划部署

要在 OpenShift (RHOSO)环境中部署和操作 Red Hat OpenStack Services，请使用 Red Hat OpenShift Container Platform (RHOCP)提供的工具和容器基础架构。

RHOCP 使用 Operator 的模块化系统来扩展 RHOCP 集群的功能。RHOSO OpenStack Operator (**openstack-operator**)在 RHOCP 中安装并运行 RHOSO 控制平面，并自动执行 RHOSO 数据平面的部署。data plane 是托管 RHOSO 工作负载的节点集合。OpenStack Operator 使用托管 RHOSO 服务和工作负载所需的操作系统配置准备节点。

OpenStack Operator 管理一组自定义资源定义(CRD)，用于定义如何部署和管理 RHOSO control plane 和数据平面节点的基础架构和配置。要使用 RHOCP 托管 control plane 创建 RHOSO 云，您可以使用 OpenStack Operator CRD 创建一组自定义资源(CR)来配置 control plane 和数据平面。

2.1. 如何部署云基础架构

要使用 RHOCP 托管 control plane 创建 RHOSO 云，您必须完成以下任务：

1. 在可正常工作的 RHOCP 集群上安装 OpenStack Operator (**openstack-operator**)。
2. 提供对 RHOSO 服务的安全访问。
3. 创建并配置 control plane 网络。
4. 创建并配置 data plane 网络。
5. 为您的环境创建一个 control plane。
6. 为您的环境自定义 control plane。
7. 创建和配置 data plane 节点。
8. 可选：为 RHOSO 部署配置存储解决方案。

您可以在可访问 RHOCP 集群的工作站上执行 control plane 安装任务和所有数据平面创建任务。

在可正常工作的 RHOCP 集群上安装 OpenStack Operator (openstack-operator)

RHOSO 管理员在 RHOCP 集群上安装 OpenStack Operator。有关如何安装 OpenStack Operator 的详情，请参考在 OpenShift *上部署 Red Hat OpenStack Services* 指南中的 安装和准备 Operator。

提供对 RHOSO 服务的安全访问

您必须创建一个 Secret 自定义资源(CR)来提供对 RHOSO 服务 pod 的安全访问。如需更多信息，请参阅在 OpenShift *上部署 Red Hat OpenStack Services 指南中的提供对 Red Hat OpenStack* Platform 服务的安全访问。

创建并配置 control plane 网络

您可以使用 RHOCP Operator 为 RHOSO control plane 网络准备 RHOCP 集群。如需更多信息，请参阅在 *OpenShift 上部署 Red Hat OpenStack Services* 指南中的 为 RHOSP 网络准备 RHOCP。

创建并配置 data plane 网络

您可以使用 RHOCP Operator 为 RHOSO 数据平面网络准备 RHOCP 集群。如需更多信息，*请参阅在 OpenShift 上部署 Red Hat OpenStack Services* 指南中的 配置 data plane 网络。

为您的环境创建一个 control plane

您可以使用每个服务的建议配置配置和创建初始 control plane。如需更多信息，*请参阅在 OpenShift 上部署 Red Hat OpenStack Services* 指南中的创建 control plane。

为您的环境自定义 control plane

您可以使用环境所需的服务自定义部署的 control plane。如需更多信息，请参阅 自定义 *Red Hat OpenStack Services on OpenShift 部署指南中的自定义* control plane。

创建并配置 data plane 节点

您可以使用最小功能配置和创建一个简单的数据平面。如需更多信息，*请参阅在 OpenShift 上部署 Red Hat OpenStack Services 指南中的创建数据平面*。https://docs.redhat.com/en/documentation/red_hat_openstack_services_on_openshift/18.0/html/the-data-plane

为您的环境自定义数据平面

您可以使用环境所需的功能和配置自定义部署的数据平面。如需更多信息，请参阅 自定义 *Red Hat OpenStack Services on OpenShift 部署指南中的自定义* 数据平面。

为 RHOSO 部署配置存储解决方案

您可以选择为 RHOSO 部署配置存储解决方案。如需更多信息，请参阅 配置持久性存储 指南。

2.2. 自定义资源定义(CRD)

OpenStack Operator 包含一组可用于创建和管理 RHOSP 资源的自定义资源定义(CRD)。

- 使用以下命令查看 RHOSP CRD 的完整列表：
  $ oc get crd | grep "^openstack"
- 使用以下命令查看特定 CRD 的定义：

```
$ oc describe crd openstackcontrolplane
Name:         openstackcontrolplane.openstack.org
Namespace:
Labels:       operators.coreos.com/operator.openstack=
Annotations:  cert-manager.io/inject-ca-from:
$(CERTIFICATE_NAMESPACE)/$(CERTIFICATE_NAME)
              controller-gen.kubebuilder.io/version: v0.3.0
API Version:  apiextensions.k8s.io/v1
Kind:         CustomResourceDefinition
...
```

- 使用以下命令查看可用于配置特定 CRD 的字段的描述：

```
$ oc explain openstackcontrolplane.spec
KIND:     OpenStackControlPlane
VERSION:  core.openstack.org/v1beta1

RESOURCE: spec <Object>

DESCRIPTION:
    <empty>

FIELDS:
  ceilometer   <Object>
  cinder       <Object>
  dns  <Object>
  extraMounts  <[]Object>
...
```

其他资源

- 管理自定义资源定义中的资源

2.2.1. CRD 命名约定

每个 CRD 在 **spec.names** 部分中包含多个名称。根据操作的上下文使用这些名称：

- 在创建并与资源清单交互时使用 **kind** ：

```
apiVersion: core.openstack.org/v1beta1
kind: OpenStackControlPlane
...
```

  资源清单中的 **kind** 名称与对应 CRD 中的 **kind** 名称关联。

- 与单个资源进行交互时使用 **singular**

```
$ oc describe openstackcontrolplane/compute
```

第 3 章 系统要求

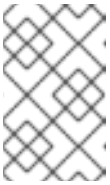
您必须在 OpenShift (RHOSO)部署中规划 Red Hat OpenStack Services，以确定您的环境的系统要求。

3.1. RED HAT OPENSHIFT CONTAINER PLATFORM 集群要求

在 OpenShift (RHOSO) control plane 上托管 Red Hat OpenStack Services 的 Red Hat OpenShift Container Platform (RHOCP)集群的最低要求如下：

硬件

- 一个可预置备的 3 节点 RHOCP 紧凑集群，版本 4.16。
- 紧凑集群中的每个节点都必须具有以下资源：
  - 64 GB RAM
  - 16 个 CPU 内核
  - 根磁盘加上 250 GB 存储（强烈建议使用 NVMe 或 SSD）的 120GB NVMe 或 SSD。



注意

部署环境中运行的虚拟机实例的卷、卷和根磁盘托管在专用的外部存储节点上。但是，服务日志、数据库和元数据存储在 RHOCP 持久性卷声明(PVC)中。测试至少需要 150 GB。

  - 2 个物理 NIC

注意

在带有 3 个控制器和 3 个 worker 的 6 节点集群中，只有 worker 节点需要 2 个物理 NIC。

- 集群中的持久性卷声明(PVC)存储：
  - 用于服务日志、数据库、文件导入转换和元数据的 150 GB 持久性卷(PV)池。

注意

- 您必须根据 RHOSO 工作负载规划 RHOSO pod 所需的 PV 池的大小。例如，镜像服务镜像转换 PVC 应该足以托管最大镜像，并在转换后的镜像以及任何其他并发转换。如果您的 RHOSO 部署使用对象存储服务(swift)，则必须对存储要求进行类似注意事项。
- 镜像服务需要 PV 池，但实际的镜像存储在镜像服务后端，如 Red Hat Ceph Storage 或 SAN。

  - 5 GB 可用的 PV 必须由本地 SSD 支持用于 control plane 服务，如 Galera、OVN 和 RabbitMQ 数据库。

软件

- RHOCP 环境支持 Multus CNI。
- 以下 Operator 安装在 RHOCP 集群中：
  - Kubernetes NMState Operator。此 Operator 必须通过创建 **nmstate** 实例来启动。如需更多信息，请参阅 RHOCP *网络指南中的* 安装 Kubernetes NMState Operator。
  - MetalLB Operator。此 Operator 必须通过创建 **metallb** 实例来启动。如需更多信息，请参阅 RHOCP *网络指南中的* 安装 MetalLB Operator。

注意

当使用 MetalLB Operator 启动 MetalLB 时，Operator 会在集群中的每个节点上启动一个 **speaker** pod 实例。在使用 3 个 OCP 控制器/master 和 3 个 OCP 计算/workers 等扩展架构时，如果您的 OCP 控制器无法访问 **ctlplane** 和 **internalapi** 网络，您必须将 **speaker** pod 限制到 OCP 计算/worker 节点。有关 speaker pod 的更多信息，请参阅将 speaker pod 限制到特定的节点。

  - cert-manager Operator。如需更多信息，请参阅 RHOCP *安全和合规性* 指南中的 Red Hat OpenShift 的 cert-manager Operator。
  - Cluster Observability Operator。如需更多信息，请参阅安装 Cluster Observability Operator。
  - Cluster Baremetal Operator (CBO)。CBO 部署 Bare Metal Operator (BMO)组件，这是在 data plane 部署过程中置备裸机节点所必需的。有关规划裸机置备的更多信息，请参阅 为裸机数据平面节点规划置备。
- 集群工作站上安装了以下工具：
  - **oc** 命令行工具。
  - **podman** 命令行工具。
- RHOCP 存储后端已配置。
- RHOCP 存储类已定义，可以访问类型为 **ReadWriteOnce** 的持久性卷。
- 对于安装程序置备的基础架构，必须准备操作系统镜像以用于裸机置备。您可以使用以下镜像作为裸机镜像：https://catalog.redhat.com/software/containers/rhel9/rhel-guest-image/6197bdceb4dcabca7fe351d5?container-tabs=overview

其他资源

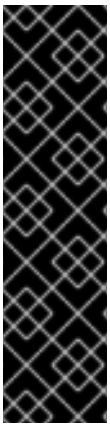
- 存储和 安装后存储配置

3.2. DATA PLANE 节点要求

您可以使用预置备节点或未置备的裸机节点来创建数据平面。data plane 节点的最低要求如下：

- 预置备节点：
  - RHEL 9.4.

- 被配置为使用在 data plane 创建过程中生成的 SSH 密钥进行 SSH 访问。SSH 用户必须是 **root** 用户，或者启用了不受限制且无密码的 sudo。如需更多信息，*请参阅在 OpenShift 上部署 Red Hat OpenStack Services* 指南中的创建 数据平面 secret。
- control plane 网络上的可路由 IP 地址，通过 SSH 启用 Ansible 访问。



重要

有些网络架构可能需要以下网络功能：

- RHOCP worker 节点上的专用 NIC 用于 RHOSP 隔离网络。
- 使用所需隔离网络的 VLAN 端口交换机。

请参考您的 RHOCP 和网络管理员，了解它们在部署中是否要求。

有关所需隔离网络的详情，请参考在 *OpenShift 上部署 Red Hat OpenStack Services 指南中的默认 Red Hat OpenStack Platform 网络*。

3.3. COMPUTE 节点要求

Compute 节点负责在启动虚拟机实例后运行虚拟机实例。Compute 节点需要支持硬件虚拟化的裸机系统。Compute 节点还必须有足够的内存和磁盘空间来支持其托管的虚拟机实例的要求。

注意

Red Hat OpenStack Services on OpenShift (RHOSO) 18.0 不支持使用 QEMU 架构模拟。

处理器

支持 Intel 64 或 AMD64 CPU 扩展并启用了 AMD-V 或 Intel VT 硬件虚拟扩展的 64 位 x86 处理器。我们推荐所使用的处理器最少有 4 个内核。

内存

主机操作系统最小 6 GB RAM，以及以下事项可容纳的额外内存：

- 添加您要提供给虚拟机实例的额外内存。
- 添加附加内存以便在主机上运行特殊功能或其他资源，如额外的内核模块、虚拟交换机、监控解决方案和其他额外的后台任务。
- 如果要使用非统一内存访问(NUMA)，红帽建议每个 CPU 插槽节点使用 8GB，如果超过 256 GB 的物理 RAM，则建议每个套接字节点使用 16GB。
- 至少配置 4 GB 交换空间。

有关规划 Compute 节点内存配置的更多信息，请参阅 为实例创建配置 Compute 服务。

磁盘空间

最少具有 50GB 可用磁盘空间。

网络接口卡

最少一个 1 Gbps 网络接口卡。对绑定的接口使用额外的网络接口卡，或代理标记的 VLAN 流量。

平台管理

安装程序置备的计算节点需要在服务器的主板上有一个受支持的平台管理界面，如智能平台管理接口(IPMI)功能。预置备节点不需要这个接口。

第 4 章 为裸机数据平面节点规划置备

您可以在 OpenShift (RHOSO)数据平面上的 Red Hat OpenStack Services 中使用预置备节点或未置备的裸机节点：

- 预置备的节点 ：在将操作系统添加到数据平面前，您使用自己的工具在节点上安装操作系统。
- unprovisioned 节点：在将操作系统添加到数据平面前，该节点没有安装操作系统。节点使用 Red Hat OpenShift Container Platform (RHOCP) Cluster Baremetal Operator (CBO)作为 data plane 创建和部署过程的一部分来置备。

RHOSO 环境支持所有远程硬件管理协议技术和裸机[3] 支持的引导方法。有关支持的硬件的详情，请参考 *Metal[3] 用户指南中的支持的硬件*。https://book.metal3.io/bmo/supported_hardware.html?highlight=boot%20method#vendor-specific-protocols但是，用于安装 RHOCP 集群的安装方法限制了 RHOSO 环境可用的技术和引导方法。

RHOCP 安装方法决定了 CBO 的可用性以及创建调配网络的功能，它决定了 RHOSO 部署可用于置备裸机数据平面节点的技术和引导方法。因此，您必须规划 RHOSO 部署，以确保支持置备裸机数据平面节点所需的技术和引导方法。

注意

红帽建议使用虚拟介质而不是 iPXE 启动进行置备，因为 RHOCP 集群中可能不提供 iPXE 引导。

4.1. RED HAT OPENSHIFT CONTAINER PLATFORM 安装注意事项

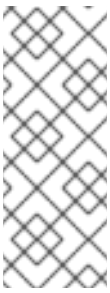
用于安装 RHOCP 集群的方法决定了 Cluster Baremetal Operator (CBO)的可用性以及创建 provisioning 网络的能力。网络引导需要 provisioning 网络。

支持的安装程序

您可以在使用 Assisted Installer 安装的集群中启用 CBO，您可以在安装后手动将用于网络引导部署的 provisioning 网络添加到 Assisted Installer 集群中。

裸机上的安装程序置备的基础架构

在使用裸机安装程序置备的基础架构安装的 RHOCP 集群上默认启用 CBO。您可以使用置备网络配置安装程序置备的集群，以启用虚拟介质和网络引导安装。



注意

- 如果您在没有 provisioning 网络的情况下配置安装程序置备的集群，则只有虚拟介质置备才可用。
- 如果您在不是裸机的平台上安装了带有 IPI 的 RHOCP，您的集群可能无法启用 CBO。有关在不是裸机的平台上安装 RHOCP 的详情，请参考 RHOCP 安装指南。

有关裸机上安装程序置备的集群的更多信息，请参阅在 *裸机上的 RHOCP 部署安装程序置备的集群*。

用户置备的基础架构

您可以通过创建一个 **Provisioning** CR，在使用用户置备的基础架构安装的 RHOCP 集群上启用 CBO。

注意

您不能在用户置备的集群中添加 provisioning 网络。这意味着您无法在使用用户置备的基础架构安装的 RHOCP 集群上启用 PXE 网络引导。您只能在使用用户置备的基础架构安装的 RHOCP 集群中使用虚拟介质置备裸机数据平面节点。

有关如何创建 **Provisioning** CR 的更多信息，请参阅 RHOCP *Installing on metal* 指南中的使用 Bare Metal Operator 扩展用户置备的集群。

4.2. BARE METAL OPERATOR (BMO)

Red Hat OpenShift Container Platform (RHOCP) Cluster Baremetal Operator (CBO)在 data plane 上置备裸机节点。CBO 部署在 RHOCP 集群中置备裸机节点所需的组件，包括 Bare Metal Operator (BMO) 和 Ironic 容器。

BMO 管理集群中的可用主机并执行以下操作：

- 检查节点硬件详情并将其报告给对应的 **BareMetalHost** CR。这包括 CPU、RAM、磁盘和 NIC 的信息。
- 使用特定镜像置备节点。
- 在置备前后清理节点磁盘内容。

如需有关 Bare Metal Operator 以及如何配置 **BareMetalHost** CR 的更多信息，请参阅 RHOCP *安装后配置* 指南中的 裸机配置。

第 5 章 规划您的网络

在部署 RHOSO 之前，请仔细检查您的网络要求和整个环境，以告知您的网络设计决策。

5.1. 默认物理网络

以下物理数据中心网络通常为 OpenShift (RHOSO)部署上的 Red Hat OpenStack 服务实现：

- control plane 网络
- 外部网络（可选）
- 内部 API 网络
- 存储网络
- 租户（项目）网络
- 存储管理网络（可选）

如需更多信息，请参阅 *部署 Red Hat OpenStack Services on OpenShift 指南中的默认 Red Hat OpenStack Services on OpenShift 网络*。

5.2. RHOSO 网络隔离

您必须规划您的部署如何隔离托管特定类型的网络流量。这包括规划 IP 范围、子网和虚拟 IP，以及配置 NIC 布局。

OpenShift (RHOSO) control plane 服务上的 Red Hat OpenStack Services 作为 Red Hat OpenShift Container Platform (RHOCP)工作负载运行。在 control plane 上，您可以使用 NMState Operator 将 worker 节点连接到所需的隔离网络。您可以根据需要，为每个隔离网络创建一个 NetworkAttachmentDefinition (nad)自定义资源(CR)来将服务 pod 附加到隔离的网络中。您可以使用 MetalLB Operator 在隔离的网络上公开内部服务端点。默认情况下，公共服务端点作为 RHOCP 路由公开。

您还必须创建一个 **L2Advertisement** 资源来定义如何宣布 VIP，以及 **IpAddressPool** 资源来配置哪些 IP 可用作 VIP。在第 2 层模式中，一个节点假定将服务公告给本地网络。

如需更多信息，请参阅在 *OpenShift 上部署 Red Hat OpenStack Services* 指南中的 为 RHOSO 网络隔离准备 RHOCP。

要创建 data plane 网络，请定义一个 NetConfig 自定义资源(CR)并为 data plane 网络指定所有子网。您必须为您的数据平面至少定义一个 control plane 网络。您还可以定义 VLAN 网络，为可组合网络创建网络隔离，如 InternalAPI、Storage 和 External。每个网络定义必须包含 IP 地址分配。

如需更多信息，*请参阅在 OpenShift 上部署 Red Hat OpenStack Services* 指南中的创建 data plane 网络。

5.3. NIC

紧凑的 RHOSO 部署需要每个 RHOSO control plane worker 节点上至少有两个 NIC。

每个 worker 节点上的一个 NIC 为 OpenShift 服务。它提供了 OpenShift 集群网络中的 OpenShift 组件之间的连接。

另一个 NIC 为 OpenStack 服务。它将 worker 节点上运行的 OpenStack 服务连接到 RHOSO 数据平面上的隔离网络。

5.3.1. NIC 和扩展注意事项

网络要求因环境和业务需求而异。例如，您可能需要以下网络功能：

- RHOCP worker 节点上的专用 NIC 用于特定的 RHOSP 隔离网络。
- 使用所需隔离网络的 VLAN 端口交换机。

请参考您的 RHOCP 和网络管理员，了解它们在部署中是否要求。每个 Compute 节点都需要至少一个 NIC。您可以纵向扩展，以提供隔离网络的连接。

5.4. 存储网络规划注意事项

如需更多信息，请参阅本指南中的 *存储网络*。

5.5. 网络功能虚拟化(NFV)

网络功能虚拟化(NFV)是一种基于软件的解决方案，可帮助通信服务提供商(CSP)超越传统专有硬件，实现更高的效率和灵活性，降低操作成本。

在 OpenShift (RHOSO)环境中的 Red Hat OpenStack Services 中使用 NFV，通过提供虚拟化基础架构来虚拟化在硬件设备（如交换机、路由器和存储）上运行的网络功能(VNF)，从而支持 IT 和网络聚合。NFV 环境利用数据平面开发套件(DPDK)和单根 I/O 虚拟化(SR-IOV)技术来提高数据包处理速度。

如果选择了 NFV 部署，则必须使用 部署网络功能虚拟化环境 作为部署指南，*而不是在 OpenShift 上部署 Red Hat OpenStack Services*。

5.6. RHOSO 网络规划的其他资源

- Kubernetes NMState Operator
- Kubernetes NMState 项目
- 使用 MetalLB 进行负载平衡
- MetalLB 文档
- MetalLB 在第 2 层模式中
- 指定 LB IP 可以从中宣布的网络接口
- 多网络
- 在 OpenShift 中使用 Multus CNI
- macvlan plugin
- Whereabouts IPAM CNI 插件 - 扩展配置
- 关于 IP 地址池的广告

第 6 章 RED HAT OPENSTACK SERVICES ON RED HAT OPENSTACK SERVICES ON OPENSHIFT 的联邦信息处理标准

联邦信息处理标准(FIPS)是由国家标准与技术研究院(NIST)开发的一系列安全要求。在 Red Hat Enterprise Linux 9 中，支持的标准是 FIPS 出版物 140-3： *Cryptographic 模块的安全要求*。有关支持的标准的详情，请查看 联邦信息处理标准 140-3。

FIPS 140-3 验证的加密模块是已完成的 NIST CMVP 进程的加密库，并且已经从 NIST 收到了证书。有关 Red Hat FIPS 140 验证模块的当前信息，请参阅 Compliance Activities 和 Government Standards。

当在启用了 FIPS 的 Red Hat OpenShift Container Platform (RHOCP)集群中安装 RHOSO 时，OpenShift (RHOSO)上的 Red Hat OpenStack Services 中默认启用 FIPS。您必须在 RHOCP 的初始安装中启用 FIPS。有关以 FIPS 模式安装 RHOCP 集群的更多信息，请参阅 在 FIPS 模式中安装集群。

当您使用系统范围的加密策略时，**FIPS 140 模式**、RHEL 和 CoreOS 被设计为将核心加密模块和库的使用限制为 FIPS 验证的已验证。但是，paramiko 在代码中实施加密功能，且未经过 FIPS 验证。RHOSO 核心组件使用提交到 NIST 进行 FIPS 验证的 RHEL 加密库，除非它们调用 paramiko。

6.1. 准备在 OPENSHIFT CONTROL PLANE 上安装启用了 FIPS 的 RED HAT OPENSTACK SERVICES

在 OpenShift (RHOSO) control plane 上安装 Red Hat OpenStack Services 前，您必须修改 **iscsi.conf** 以删除 MD5 和 SHA1。control plane 的 iSCSId 配置不是由 RHOSO operator 处理，因此您必须在 Red Hat OpenShift Container Platform (RHOCP)集群上完成此步骤。

先决条件

- 您有一个已存在的 RHOCP 集群，启用了 FIPS。有关 RHOCP 上的 FIPS 的更多信息，请参阅对 FIPS 加密的支持。

流程

- 在每个节点上，确保 **/etc/iscsi/iscsi.conf** 文件中的 **node.session.auth.chap_algs** 的值设置为 **SHA3-256,SHA256**。

6.2. FIPS 状态的验证

您可以检查 RHOCP 或部署的 worker 节点的 FIPS 状态。

流程

1. 使用具有 cluster-admin 权限的账户登录 Red Hat OpenShift Container Platform (RHOCP)集群。
2. 获取集群中的节点列表：

```
$ oc get nodes
```

输出示例：

```
NAME   STATUS   ROLES                  AGE VERSION
master1   Ready control-plane,master   7d1h   v1.28.6+6216ea1
master2   Ready control-plane,master   7d1h   v1.28.6+6216ea1
```

```
master3   Ready control-plane,master   7d1h   v1.28.6+6216ea1
worker1   Ready worker                 7d1h   v1.28.6+6216ea1
worker2   Ready worker                 7d1h   v1.28.6+6216ea1
worker3   Ready worker
```

3. 在上一步输出中显示的一个节点上打开一个 debug pod:

```
$ oc debug node/worker2
```

输出示例：

```
Temporary namespace openshift-debug-rq2m8 is created for debugging node...
Starting pod/worker2-debug-5shqt ...
To use host binaries, run `chroot /host`
Pod IP: 192.168.50.112
If you don't see a command prompt, try pressing enter.
sh-5.1#
```

4. 检查 /**proc**中的 **fips_enabled**

```
sh-5.1# cat /proc/sys/crypto/fips_enabled
```

示例输出。**1** 显示为已启用，**0** 代表禁用：

```
1
```

有关在 FIPS 模式中安装 Red Hat OpenShift Cluster Platform 的更多信息，请参阅 RHOCP 安装指南中的 FIPS 加密支持。

第 7 章 规划存储和共享文件系统

Red Hat OpenStack Services on OpenShift (RHOSO) 使用临时存储和持久存储来满足部署的存储需求。

临时存储与特定 Compute 实例关联。当此实例终止时，即关联的临时存储。临时存储可用于运行时要求，如存储实例的操作系统。

持久性存储独立于任何正在运行的实例。持久存储可用于存储可重复使用的数据，如数据卷、磁盘镜像和可共享文件系统。

在开始部署前，应考虑和仔细规划部署的存储要求。这包括如下注意事项：

- 支持的功能和拓扑
- 存储技术
- 网络
- 可扩展性
- 可访问性
- 性能
- 成本
- 安全性
- 冗余和灾难恢复
- 存储管理

7.1. 支持的存储功能和拓扑

RHOSO 支持以下存储和网络功能：

- Red Hat Ceph Storage 集成：
  - Ceph 块设备(RBD)，带有用于持久存储、镜像服务(glance)的块存储服务(cinder)，以及临时存储的计算服务(nova)。
  - 使用共享文件系统服务(manila)通过 NFS 提供 Ceph 文件系统(Native CephFS 或 CephFS)。
  - Object Storage 服务与 Ceph 对象网关(RGW)集成
  - 超融合基础架构(HCI)：超融合基础架构由超融合节点组成。超融合节点是外部数据平面节点，其计算和 Red Hat Ceph Storage 服务在同一节点上在一起，以优化硬件占用。
- 带有适当配置和驱动程序的块存储服务的传输协议：
  - NVMe over TCP
  - RBD
  - NFS
  - FC

注意

您必须在使用块存储服务和光纤通道(FC)后端的任何部署中的所有 Compute 和 OCP worker 节点上安装主机总线适配器(HBA)。

- *iSCSI*

- *使用 iSCSI、FC 和 NVMe over TCP 进行多路径，可在带有适当的 RHOCP MachineConfig 的 control plane 上提供。*
- *带有适当配置和驱动程序的共享文件系统服务的传输协议：*
  - *CephFS*
  - *NFS*
  - *CIFS*
- *通过原生 Swift 或 Amazon S3 兼容 API 的对象存储*

RHOSO 支持以下存储服务：

service	后端
Image 服务 (glance)	• Red Hat Ceph Storage RBD • Block Storage (cinder) • Object Storage (swift) • NFS
计算服务(nova)	• 本地文件存储 • Red Hat Ceph Storage RBD
Block Storage 服务 (cinder)	• Red Hat Ceph Storage RBD • Fiber Channel • iSCSI • NFS • NVMe over TCP  **注意** 通过第三方驱动程序提供支持。

service	后端
共享文件系统服务(manila)	• Red Hat Ceph Storage CephFS • Red Hat Ceph Storage CephFS-NFS • 通过第三方供应商存储系统进行 NFS 或 CIFS
Object Storage 服务 (swift)	• 外部数据平面节点上的磁盘 • OpenShift 节点上的 PersistentVolume (PV)（默认） • 与 Ceph RGW 集成

要按项目管理系统资源消耗，您可以为块存储服务(cinder)和共享文件系统服务(manila)配置配额。您可以覆盖默认配额，以便单个项目具有不同的消耗限制。

7.2. 存储技术

RHOSO 支持多种可单独或组合使用的存储技术，为您的部署提供存储解决方案。

7.2.1. Red Hat Ceph Storage

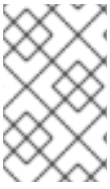
Red Hat Ceph Storage 是一个分布式数据对象存储，专为性能、可靠性和可扩展性而设计。分布式对象存储使用非结构化数据来同时服务现代和传统的对象接口。它提供对块、文件和对象存储的访问。

Red Hat Ceph Storage 作为一个集群部署。集群由两个主要的守护进程组成：

- *Ceph Object Storage Daemon (CephOSD)- CephOSD 执行数据存储、数据复制、重新平衡、恢复、监控和报告任务。*
- *Ceph monitor (CephMon)- CephMon 使用集群的当前状态维护 cluster map 的主要副本。*

在以下部署场景中，RHOSO 支持 Red Hat Ceph Storage 7：

- *与外部部署的 Red Hat Ceph Storage 7 集群集成。*
- *一个超融合基础架构(HCI)环境，它由外部数据平面节点组成，这些节点将计算和 Red Hat Ceph Storage 服务在同一节点上在一起，用于优化资源使用。*



注意

Red Hat OpenStack Services on OpenShift (RHOSO) 18.0 支持使用 Red Hat Ceph Storage Object Gateway (RGW)的纠删代码。目前不支持使用 Red Hat Ceph Storage Block Device (RDB)的纠删代码。

有关 Red Hat Ceph Storage 架构的更多信息，请参阅 Red Hat Ceph Storage 7 架构指南 。

7.2.2. 块存储(cinder)

块存储服务(cinder)允许用户在后端调配块存储卷。用户可以将卷附加到实例，以使用通用持久性存储来增强其临时存储。您可以将卷分离和重新关联到实例，但您只能通过附加的实例访问这些卷。

您还可以配置实例，使其不使用临时存储。您可以配置块存储服务来将镜像写入卷，而不使用临时存储。然后，您可以使用卷作为实例的可引导根卷。卷还通过备份和快照提供固有冗余和灾难恢复。但是，只有在部署可选块存储备份服务时，才会提供备份。另外，您可以加密卷以提高安全性。

7.2.3. 镜像(glance)

Image 服务(glance)为实例镜像提供发现、注册和交付服务。它还提供存储实例临时磁盘快照以满足克隆或恢复目的的功能。您可以将存储的镜像用作模板，比安装服务器操作系统和单独配置服务，快速、一致地编写新的服务器。

7.2.4. Object Storage (swift)

Object Storage 服务(swift)提供了一个完全分布式的存储解决方案，可用于存储任何类型的静态数据或二进制对象；如介质文件、大型数据集和磁盘镜像。对象存储服务使用对象容器来组织对象，该容器类似于文件系统中的目录，但不能嵌套。您可以使用对象存储服务作为云中各个服务的存储库。

Red Hat Ceph Storage RGW 可用作对象存储服务的替代选择。

7.2.5. 共享文件系统(manila)

共享文件系统服务(manila)提供了置备远程、可共享的文件系统的方法。这些称为共享。共享允许云中的项目共享 POSIX 兼容存储，它们可以被多个实例同时使用。

共享用于实例使用，可通过读/写访问模式同时被多个实例使用。

7.3. 存储网络

在 RHOSO 安装过程中配置两个默认存储相关网络：存储和存储管理网络。这些隔离网络遵循最佳实践，以便在存储组件和部署之间进行网络连接。

存储网络用于数据存储访问和检索。

RHOSO 服务使用存储管理网络来访问存储解决方案中的特定接口，允许访问管理控制台。例如，Red Hat Ceph Storage 在超融合基础架构(HCI)环境中使用存储管理网络作为 cluster_network 复制数据。

下表列出了默认存储相关网络的属性。

网络名称	VLAN	CIDR	NetConfig allocationRange	MetalLB IPAddressPool 范围	NAD ipam range	OCP worker nncp 范围
storage	21	172.18.0.0/24	172.18.0.100 - 172.18.0.250	N/A	172.18.0.30 - 172.18.0.70	172.18.0.10 - 172.18.0.20

网络名称	VLAN	CIDR	NetConfig allocationRange	MetalLB IPAddressPool 范围	NAD ipam range	OCP worker nncp 范围
storageMgmt	23	172.20.0.0/24	172.20.0.100 - 172.20.0.250	N/A	172.20.0.30 - 172.20.0.70	172.20.0.10 - 172.20.0.20

您的存储解决方案可能需要额外的网络配置。这些默认值为构建完整部署提供了基础。

*所有带有后端(**cinder-volume** 和 **cinder-backup**)的块存储服务需要访问所有存储网络，这些存储网络可能不包括基于后端的存储管理网络。使用后端的块存储服务仅需要访问其存储管理网络。在大多数部署中，只有一个管理网络，但如果有多个存储管理网络，每个服务后端对都需要访问其相应的管理网络。*

您必须在使用块存储服务和光纤通道(FC)后端的任何部署中的所有 OCP worker 节点上安装主机总线适配器(HBA)。

7.3.1. 为块存储服务规划网络

存储最佳实践建议使用两个不同的网络：

- *一个网络用于数据 I/O*
- *一个用于存储管理的网络*

*这些网络称为 **存储和 存储。** 如果您的部署与两个网络的架构分离，请根据需要调整记录的示例。例如，如果存储网络上有存储系统的管理界面，请在只有一个网络时将 **storageMgmt** 替换为 **存储**，并在存储网络已存在时删除 **storageMgmt**。*

*Red Hat OpenStack Services on OpenShift (RHOSO) 中的存储服务（除 Object Storage 服务(swift)除外）需要访问存储和 **storage Mgmt** 网络。您可以在 **OpenStackControlPlane** CR 的 **networkAttachments** 字段中配置 **storage** 和 **storageMgmt** 网络。**networkAttachments** 字段接受字符串列表，其中包含组件需要访问的所有网络。不同的组件可以有不同的网络要求，例如，块存储服务 (cinder) API 组件不需要访问任何存储网络。*

*以下示例显示了 Block Storage 卷的 **networkAttachments** ：*

```
apiVersion: core.openstack.org/v1beta1
kind: OpenStackControlPlane
metadata:
  name: openstack
spec:
  cinder:
    template:
      cinderVolumes:
        iscsi:
          networkAttachments:
          - storage
          - storageMgmt
```

7.3.2. 为共享文件系统服务规划网络

规划云上的网络，以确保云用户可以将其共享连接到在 OpenShift (RHOSO)虚拟机、裸机服务器和容器上运行的工作负载。

根据云用户所需的安全性和隔离级别，您可以将 **driver_handles_share_servers** 参数设置为 **true** 或 **false**。

7.3.2.1. 将 DHSS 设置为 true

如果将 DHSS 参数设置为 **true**，您可以使用共享文件系统服务将共享导出到带有隔离的共享服务器的最终用户定义的共享网络。用户可以在自助服务共享网络上调配工作负载，以确保专用网络片段上的隔离 NAS 文件服务器导出其共享。

作为项目管理员，您必须确保将隔离网络映射到您的存储基础架构的物理网络。您还必须确保您使用的存储系统支持网络段。存储系统（如 NetApp ONTAP 和 Dell EMC PowerMax、unity 和 VNX）不支持虚拟覆盖分段风格，如 GENEVE 或 VXLAN。

作为覆盖网络的替代方案，您可以执行以下操作之一：

- 将 VLAN 网络用于项目网络。
- 在共享提供商网络上允许 VLAN 段。
- 提供对已连接到您的存储系统的预先存在的片段网络的访问权限。

7.3.2.2. 将 DHSS 设置为 false

如果将 DHSS 参数设置为 **false**，则云用户无法在自己的共享网络上创建共享。您可以创建专用的共享存储网络，云用户必须将客户端连接到配置的网络访问其共享。

不是所有共享文件系统服务存储驱动程序都支持 **DHSS=true** 和 **DHSS=false**。**DHSS=true** 和 **DHSS=false** 确保数据路径多租户隔离。但是，如果您需要租户工作负载的网络路径多租户隔离作为自助服务模型的一部分，您必须使用支持 **DHSS=true** 的后端部署共享文件系统服务(manila)。

7.3.2.3. 确保与共享的网络连接

要连接到文件共享，客户端必须有连接到该共享的一个或多个导出位置的网络连接。

当管理员将共享类型的 **driver_handles_share_servers** 参数(DHSS)设置为 **true** 时，云用户可以创建共享网络，其中包含计算实例附加的网络详情。然后，云用户可以在创建共享时引用共享网络。

当管理员将共享类型的 DHSS 参数设置为 **false** 时，云用户必须将其 Compute 实例连接到为 OpenShift (RHOSO)部署中配置的共享存储网络。有关如何配置并验证到共享网络的网络连接的更多信息，请参阅*连接到共享网络以访问 存储操作中 的共享*。

7.4. 可扩展性和后端存储

通常，集群存储解决方案提供更大的后端可扩展性和弹性。例如，当您将 Red Hat Ceph Storage 用作 Block Storage (cinder)后端时，您可以通过添加更多 Ceph Object Storage Daemon (OSD) 节点来扩展存储容量和冗余。块存储、对象存储(swift)和共享文件系统服务(manila)服务支持 Red Hat Ceph Storage 作为后端。

块存储服务可以将多个存储解决方案用作离散后端。在服务级别，您可以通过添加更多后端来扩展容量。

默认情况下，对象存储服务通过在 OpenShift 底层基础架构中分配持久性卷来消耗空间。它可以配置为在专用存储节点上使用文件系统，并且可以使用尽可能多的空间。对象存储服务支持 XFS 和 ext4 文件系

统，您可以扩展这两个文件系统，使其消耗尽可能多的底层块存储。您还可以通过向存储节点添加更多存储设备来扩展容量。

共享文件系统服务从由 Red Hat Ceph Storage 或其他后端存储系统管理的指定存储池中置备文件共享。您可以通过增加服务可用的大小或添加更多后端存储系统来扩展此共享存储。每个后端存储系统都与专用服务集成，用于与存储系统交互并管理存储系统。

7.5. 存储可访问性和管理

卷仅通过实例使用。用户可以扩展、创建卷的快照并使用快照克隆或将卷恢复到以前的状态。

您可以使用 Block Storage 服务(cinder)创建卷类型，以聚合卷设置。您可以将卷类型与加密和服务质量(QoS)规格相关联，为您的云用户提供不同级别的性能。您的云用户可以指定创建新卷时所需的卷类型。例如，使用高性能 QoS 规格的卷可能会为用户提供更多的 IOPS，或者您的用户可以为使用较低性能 QoS 规格的卷分配更轻的工作负载来节省资源。共享可以被一个或多个实例、裸机节点或容器同时使用。共享文件系统服务(manila)还支持共享调整大小、快照和克隆，管理员可以创建共享类型来聚合设置。

用户可以使用 Object Storage 服务(swift) API 访问容器中的对象，管理员可以让对象可以被云中的实例和服务访问。此可访问性使对象是理想的服务存储库；例如，您可以将镜像服务(glance)镜像存储在由对象存储服务管理的容器中。

7.6. 存储安全性

块存储服务通过密钥管理器服务(barbican)提供数据安全性。块存储服务使用一对一键，使用由密钥管理器服务管理的密钥进行卷映射。在配置卷类型时定义加密类型。

也可以通过加密控制和/或数据流量（例如使用 Red Hat Ceph Storage）在后端级别提高安全性，这可以通过启用 messengerv2 安全模式来实现。这样，在 Ceph 服务以及 OpenStack 计算节点之间的网络流量会被加密。

您可以在服务和节点级别配置对象和容器安全性。Object Storage 服务(swift)没有为容器和对象提供原生加密。但是，启用了 Key Manager 服务后，对象存储服务可以透明地加密和解密您存储的(at-rest)对象。at-rest 加密与传输中的加密不同，因为它指的是在磁盘上存储过程中加密的对象。

共享文件系统服务(manila)可以通过访问限制（根据实例 IP、用户或组还是 TLS 证书）保护共享。有些共享文件系统服务部署可以独立共享服务器，以管理共享网络和共享之间的关系。某些共享服务器支持，甚至需要其他网络安全性。例如，CIFS 共享服务器需要部署 LDAP、Active Directory 或 Kerberos 身份验证服务。

有些后端也支持加密数据 AT REST。这通过加密后端磁盘本身实现额外的安全性，防止出现物理安全威胁，如失窃或未擦除磁盘。

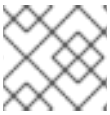
有关为块存储服务、对象存储服务和共享文件系统服务配置安全选项的更多信息，请参阅配置安全服务。

7.7. 存储冗余和灾难恢复

如果您部署可选的 Block Storage 备份服务，则块存储服务(cinder)为用户存储的基本灾难恢复提供卷备份和恢复。您可以使用备份来保护卷内容。块存储服务还支持快照。除了克隆外，您还可以使用快照将卷恢复到以前的状态。

如果您的环境包含多个后端，您也可以在这些后端之间迁移卷。如果您需要使后端离线进行维护，这将非常有用。备份通常存储在与源卷分开的存储后端中，以帮助保护数据。快照无法实现，因为快照依赖于其源卷。

块存储服务还支持创建一致性组，来同时将卷分组在一起。这在多个卷间提供了更高的数据一致性。



注意

红帽目前不支持块存储服务复制。

Object Storage 服务(swift)不提供内置备份功能。您必须在文件系统或节点级别执行所有备份。但是，对象存储服务具有强大的冗余性和容错能力。即使是对象存储服务的最基本的部署多次复制对象。您可以使用设备映射器多路径(DM 多路径)等故障切换功能来增强冗余。

共享文件系统服务(manila)不提供共享的内置备份功能，但您可以创建用于克隆和恢复的快照。

7.8. 管理存储解决方案

您可以使用 RHOSO 仪表板(horizon)或 RHOSO 命令行界面(CLI)来管理您的 RHOSO 配置。您可以使用任何方法执行大多数流程，但一些高级流程只能通过 CLI 来完成。

您可以使用存储供应商提供的专用管理界面来管理您的存储解决方案配置。

7.9. 调整 RED HAT OPENSHIFT 存储的大小

镜像和对象存储服务可以配置为在 Red Hat OpenShift 后备存储中分配空间。在这种情况下，应该根据这些服务的预期使用 Red Hat OpenShift 存储大小来估算。

7.9.1. 镜像服务注意事项

镜像服务(glance)需要一个暂存区域在导入操作过程中操作数据。镜像数据可以复制到多个存储中，以便镜像服务需要一些持久性。虽然 PVC 代表镜像服务的主要存储模型，但也可以选择外部模型。

外部模型

如果选择了 External，则不会创建 PVC，镜像服务的行为与没有提供持久性的无状态实例类似。在本实例中，必须使用 **extraMounts** 提供持久性。NFS 通常用于提供持久性。它可以映射到 **/var/lib/glance** ：

```
...
default:
  storage:
    external: true
...
...
extraMounts:
- extraVol:
  - extraVolType: NFS
    mounts:
    - mountPath: /var/lib/glance/os_glance_staging_store
      name: nfs
    volumes:
    - name: nfs
      nfs:
        path: <nfs_export_path>
        server: <nfs_ip_address>
```

- 将 **<nfs_export_path>** 替换为 NFS 共享的导出路径。
- 将 **<nfs_ip_address>** 替换为 NFS 共享的 IP 地址。此 IP 地址必须是覆盖网络的一部分，该网络可由镜像服务访问。

应该注意的是，配置示例与分布式镜像导入功能冲突。分布式镜像导入需要 RWO 存储插入到特定实例中；它拥有数据，并在上传操作需要暂存数据时接收请求。当采用外部模型时，如果将 Red Hat Ceph Storage 用作后端，并且镜像转换操作在其中一个现有副本中运行，则 **glance-operator** 不必对与 staging 区域关联的底层存储进行任何假设，并且使用 **os_glance_staging_store** 目录的转换操作（具有 Pod）与 RWX NFS 后端交互。**在这种情况下，不能请求镜像缓存 PVC 并挂载到 subPath，因为它应该是管理员使用 extraMounts 来计划持久性的责任。**

PVC 模型

PVC 模型是默认的。部署 GlanceAPI 实例时，会根据 storageClass 和 storageRequest 传递，创建 PVC 并绑定到 /var/lib/glance。

```
...
default:
  replicas: 3
  storage:
    storageRequest: 10G
...
```

在这个模型中，如果将 Red Hat Ceph Storage 设置为后端，则不会创建专用镜像转换 PVC。管理员必须提前考虑 PVC 大小；PVC 的大小应至少为最大转换的镜像大小。同一 Pod 中的并发转换在 PVC 大小方面可能会有问题。如果 PVC 已满且没有足够的空间，转换将失败或无法进行。在之前的转换超过并释放了暂存区域空间后，应重试上传。但是，在不同 Pod 中可能会发生并发转换操作。您应该为特定的 glanceAPI 部署至少 3 个副本。这有助于处理大量操作，如镜像转换。

对于基于 PVC 的布局，以副本形式横向扩展的 glanceAPI 受 storageClass 提供的可用存储的限制，并依赖于 storageRequest。storageRequest 是一个关键参数，可以为所有 glanceAPI 全局定义，或者为每个 API 使用不同的值定义。它会影响每个操作的横向扩展操作。除了 staging 区域所需的本地 PVC 外，也可以启用镜像缓存，它转换为绑定到每个 glanceAPI 实例的额外 PVC。glance-cache PVC 绑定到 /var/lib/glance/image-cache。glance-operator 相应地配置 glanceAPI 实例，同时设置 image_cache_max_size 和 image_cache_dir 参数。镜像缓存 PVC 的数量遵循与本地 PVC 描述的规则相同，请求的 PVC 数量与副本数成比例。

7.9.2. 对象存储服务注意事项

对象存储服务需要存储设备进行数据。这些设备必须在其生命周期内使用相同的主机名或 IP 地址访问。如何实现带有无标头服务的 StatefulSet 的配置。

如果要使用存储卷为工作负载提供持久性，您可以使用 StatefulSet 作为解决方案的一部分。虽然 StatefulSet 中的单个 Pod 容易失败，但持久性 Pod 标识符可以更轻松地将现有卷与替换任何失败的 Pod 匹配。

对象存储服务需要很少的服务来访问这些 PV，并且所有这些 PV 都在单个 pod 中运行。

另外，如果 StatefulSet 被删除，卷不会被删除。不必要的删除 StatefulSet （或整个部署）不会立即造成灾难性数据丢失，但可以从管理员交互中恢复。

无头服务使可以使用 DNS 名称直接访问存储 pod。例如，如果 pod 名称为 swift-storage-0，并且 SwiftStorage 实例命名为 swift-storage，它可以通过 swift-storage-0.swift-storage 访问。这使得它可在对象存储服务环中轻松使用，IP 更改现在为透明的，不需要更新环。

并行 pod 管理会告知 StatefulSet 控制器并行启动或终止所有 Pod，且不会等待 Pod 变为 Running，并在启动或终止另一个 Pod 前完全终止。这个选项只会影响扩展操作的行为。更新不会受到影响。

这需要多个扩展；包括有多个副本的新部署。需要同时创建所有 pod，否则将有没有绑定的 PVC，且无法创建对象存储服务环，最终阻塞这些 pod 的启动。

存储 pod 应该分布到不同的节点上，以避免出现单点故障。具有 preferredDuringSchedulingIgnoredDuringExecution 的 podAntiAffinity 规则用于尽可能将 pod 分发到不同的节点。使用位于不同节点上的单独 storageClass 和 PersistentVolume，可用于强制实施进一步的发布。

对象存储服务后端服务必须只能被其他后端服务和对象存储服务代理访问。要限制访问，添加了 NetworkPolicy 来只允许这些 pod 之间的流量。NetworkPolicy 本身依赖于标签，它们必须与允许流量匹配。因此，标签不能唯一；相反，所有 pod 都必须使用相同的标签才能允许访问。这也是 swift-operator 没有使用 lib-common 中的标签的原因。

对象存储服务 ring 需要有关要使用的磁盘的信息，这包括大小和主机名或 IP。当使用 PVC 启动 StatefulSet 时，大小未知，大小要求是一个较低限制，但实际的 PV 可能非常大。

但是，StatefulSet 在 ConfigMap 可用前创建 PVC，并只等待启动 pod，直到这些 pod 可用为止。SwiftRing 协调器正在监视 SwiftStorage 实例，并迭代 PVC 来获取有关使用磁盘的实际信息。绑定这些大小后，会知道大小，swift-ring-rebalance 作业将创建 Swift 环，最终是 ConfigMap。ConfigMap 变为可用后，StatefulSet 将启动服务 pod。

Ring 存储在 SwiftProxy 和 SwiftStorage 实例使用投射卷的 ConfigMap 中。这样便可同时挂载所有必需的文件，而不会将其与其他位置合并。更新的 ConfigMap 将更新这些文件，并且这些更改由 Swift 服务最终重新加载它们。

有些 Operator 使用 customServiceConfig 选项来自定义设置。但是，SwiftRing 实例部署多个后端服务，各自需要自定义特定的文件。因此，在使用 swift-operator 时，只支持将特定密钥用作文件名的

defaultConfigOverwrite。

第 8 章 集成

您可以将 Red Hat OpenStack Services on OpenShift (RHOSO)与以下第三方软件（经过测试和批准的软件）集成

您可以在可信云供应商上部署 RHOSO。有关已认证产品列表，请参阅 Hardware - Tested and Approved。

第 9 章 订阅

要在 OpenShift (RHOSO)上安装 Red Hat OpenStack Services，您必须使用 Red Hat Subscription Manager 在 RHOSO 环境中注册所有系统，并订阅所需的频道。

如需有关 OpenShift 订阅上的 Red Hat OpenStack Services 的更多信息，请参阅 Red Hat OpenStack Services on OpenShift FAQ。