OpenShift Dedicated 4

OpenShift Dedicated 简介

OpenShift Dedicated 架构概述

Last Updated: 2024-07-03

OpenShift Dedicated 4 OpenShift Dedicated 简介

OpenShift Dedicated 架构概述

法律通告

摘要

本文档概述了 OpenShift Dedicated 中的平台和应用程序架构。

目录

第 1 章 了解 OPENSHIFT DEDICATED

OpenShift Dedicated 基于 Kubernetes 的基础，作为云服务提供完整的 OpenShift Container Platform 集群，配置为高可用性，专用于单个客户。

1.1. OPENSHIFT DEDICATED 概述

OpenShift Dedicated 主要由红帽管理，托管在 Amazon Web Services (AWS)或 Google Cloud Platform (GCP)上。每个 OpenShift Dedicated 集群都附带一个完全托管的 control plane (Control 和 Infrastructure 节点)、应用程序节点（由红帽站点可靠性工程师 (SRE) 安装和管理）、高级红帽支持以及集群服务，如日志记录、指标、监控、通知门户和集群门户。

OpenShift Dedicated 为 Kubernetes 带来企业级增强，具体包括以下所列：

- OpenShift Dedicated 集群部署在 AWS 或 GCP 环境中，可用混合型作应用程序管理方法的一部分。
- 集成了红帽技术。OpenShift Dedicated 中的主要组件源自 Red Hat Enterprise Linux 和相关红帽技术。OpenShift Dedicated 得益于红帽企业级优质软件的严格测试和认证计划。
- 开源开发模型。开发以开放方式完成，源代码可从公共软件存储库中获得。这种开放协作促进了快速创新和开发。

要了解在 OpenShift Container Platform 中构建和部署容器化 Kubernetes 应用程序时创建的资产选项，请参阅了解 OpenShift Container Platform 开发 。

1.1.1. 定制操作系统

OpenShift Dedicated 使用 Red Hat Enterprise Linux CoreOS (RHCOS)，这是一款面向容器的操作系统，结合了 CoreOS 和 Red Hat Atomic Host 操作系统的一些最佳特性和功能。RHCOS 是专门为从 OpenShift Dedicated 运行容器化应用程序而设计的，能够与新工具配合，提供快速安装、基于 Operator 的管理和简化的升级。

RHCOS 包括：

- Ignition，OpenShift Dedicated 将其用作首次启动系统配置来进行机器的初次上线和配置。
- CRI-O，Kubernetes 的原生容器运行时实现，可与操作系统紧密集成来提供高效和优化的 Kubernetes 体验。CRI-O，提供用于运行、停止和重启容器的工具。
- Kubelet，Kubernetes 的主要节点代理，负责启动和监视容器。

1.1.2. 其他主要功能

Operator 既是 OpenShift Dedicated 代码库的基本单元，又是部署供应用程序使用的应用程序和软件组件的便捷方式。在 OpenShift Dedicated 中，Operator 可充当平台的基础，不再需要手动升级操作系统和 control plane 应用程序。OpenShift Dedicated（如 Cluster Version Operator 和 Machine Config Operator）允许对这些关键组件进行简化的集群范围内管理。

Operator Lifecycle Manager (OLM) 和 OperatorHub 提供了相应的工具，可用于存储 Operator 并将其分发给开发和部署应用程序的人员。

Red Hat Quay Container Registry 是一个 Quay.io 容器 registry，为 OpenShift Dedicated 集群提供大多数容器镜像和 Operator。Quay.io 是 Red Hat Quay 的一个公共 registry 版本，可存储数百万镜像和标签。

OpenShift Dedicated 中的其他 Kubernetes 增强功能包括软件定义网络 (SDN)、身份验证、日志聚合、监视和路由方面的改进。OpenShift Dedicated 还提供功能齐全的 web 控制台和自定义 OpenShift CLI (**oc**) 界面。

1.1.3. OpenShift Dedicated 对互联网和 Telemetry 的访问

在 OpenShift Dedicated 中，您需要访问互联网来安装和升级您的集群。

通过 Telemetry 服务，从 OpenShift Dedicated 集群向红帽发送信息，以启用订阅管理自动化、监控集群的健康状态、协助支持并改进客户体验。

Telemetry 服务自动运行，集群已注册到 Red Hat OpenShift Cluster Manager。在 OpenShift Dedicated 中，远程健康报告总是被启用，您无法选择停用。Red Hat Site Reliability Engineering (SRE) 团队需要信息为您的 OpenShift Dedicated 集群提供有效的支持。

其他资源

- 如需有关 OpenShift Dedicated 集群的 Telemetry 和 远程健康监控的更多信息，请参阅关于远程健康监控

第 2 章 策略和服务定义

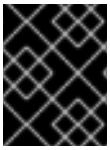
2.1. OPENSHIFT DEDICATED 服务定义

2.1.1. 帐户管理

2.1.1.1. 账单选项

客户可以选择购买 OpenShift Dedicated (OSD) 的年度订阅或通过云市场按需使用。客户可以决定使用自己的云基础架构帐户，称为客户云订阅(CCS)，或者在由红帽拥有的云供应商帐户中进行部署。下表提供有关计费的更多信息，以及相应的支持的部署选项。

OSD 订阅类型	云基础架构帐户	计费过程
红帽年度固定容量订阅	红帽云帐户	红帽可以消耗 OSD 订阅和云基础架构
	客户自己的云帐户	红帽使用 OSD 订阅的消耗 用于使用云基础架构的云供应商
通过 Google Cloud Marketplace 进行按需使用	客户自己的 Google Cloud 帐户	Google Cloud 用于云基础架构和 Red Hat OSD 订阅
通过 Red Hat Marketplace 进行按需使用	客户自己的云帐户	红帽使用 OSD 订阅的消耗 用于使用云基础架构的云供应商



重要

使用自己的云基础架构帐户（称为客户云订阅(CSS)）的客户负责预先购买或提供保留实例(RI)计算实例以确保云基础架构成本较低。

可以为 OpenShift Dedicated 集群购买其他资源，包括：

- 额外的节点（可以通过使用机器池的不同类型和大小）
- 中间件(JBoss EAP、JBoss Fuse 等)- 根据特定中间件组件的额外定价
- 以 500 GB 为单位递增的额外存储（仅限标准，包括 100 GB）
- 额外的 12 TiB 网络 I/O （仅包含标准，仅包含 12 TB）
- 服务的负载均衡器在 4 的捆绑包中可用；启用非标准端口（仅限标准）

2.1.1.2. 集群自助服务

客户可以从 OpenShift Cluster Manager 创建、扩展和删除其集群，只要他们已经购买了必要的订阅。

Red Hat OpenShift Cluster Manager 中提供的操作不能直接从集群内直接执行，因为这可能导致负面影响，包括所有操作都自动恢复。

2.1.1.3. 云供应商

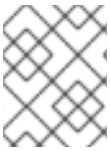
OpenShift Dedicated 在以下云供应商上将 OpenShift Container Platform 集群作为受管服务提供：

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

2.1.1.4. 实例类型

单个可用区集群至少需要 2 个 worker 节点才能将客户云订阅 (CCS) 集群部署到一个可用区。标准集群至少需要 4 个 worker 节点。这 4 个 worker 节点包含在基本订阅中。

多个可用区集群至少需要 3 个 worker 节点用于客户云订阅(CCS) 集群，3 个可用区的每个都部署 1 个。标准集群至少需要 9 个 worker 节点。这 9 个 worker 节点包含在基本订阅中，必须以 3 的倍数购买额外的节点才能保持正确的节点分布。



注意

单个 OpenShift Dedicated 机器池中的所有 worker 节点都必须有相同的类型和大小。但是，OpenShift Dedicated 集群中多个机器池的 worker 节点可以是不同的类型和大小。

control plane 和基础架构节点也由红帽提供。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 control plane 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。有关要在 worker 节点上部署的 Red Hat 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 1 个 vCPU 内核和 1 GiB 内存，并从可分配的资源中删除。这是运行底层平台所需的进程所必需的。这包括 udev、kubelet、容器运行时等系统守护进程，以及内核保留的帐户。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。

重要

从 OpenShift Dedicated 4.11 开始，默认的每个 pod PID 的限制为 **4096**。如果要启用此 PID 限制，您必须将 OpenShift Dedicated 集群升级到这些版本或更新版本。在 4.11 之前的版本上运行的 OpenShift Dedicated 集群使用默认的 PID 限制 **1024**。

您无法在任何 OpenShift Dedicated 集群中配置每个 pod PID 限制。

其它资源

- Red Hat Operator 支持

2.1.1.5. 客户订阅集群的 AWS 实例类型

OpenShift Dedicated 在 AWS 上提供以下 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)
- 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.metal (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, 128 GiB)
- m5d.12xlarge (48 vCPU, 192 GiB)
- m5d.16xlarge (64 vCPU, 256 GiB)
- m5d.24xlarge (96 vCPU, 384 GiB)

- m5n.metal (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)
- m5n.12xlarge (48 vCPU, 192 GiB)
- m5n.16xlarge (64 vCPU, 256 GiB)
- m5n.24xlarge (96 vCPU, 384 GiB)
- m5dn.metal (96 vCPU, 384 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)
- m5zn.metal (48 vCPU, 192 GiB)
- m5zn.xlarge (4 vCPU, 16 GiB)
- m5zn.2xlarge (8 vCPU, 32 GiB)
- m5zn.3xlarge (12 vCPU, 48 GiB)
- m5zn.6xlarge (24 vCPU, 96 GiB)
- m5zn.12xlarge (48 vCPU, 192 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)
- 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)

- m7i-flex.xlarge (4 vCPU, 16 GiB)
- m7i-flex.2xlarge (8 vCPU, 32 GiB)
- m7i-flex.4xlarge (16 vCPU, 64 GiB)
- m7i-flex.8xlarge (32 vCPU, 128 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)

2.4.4 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, 1952 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, 1024 GiB)
- x2idn.24xlarge (96 vCPU, 1536 GiB)
- x2idn.32xlarge (128 vCPU, 2048 GiB)
- x2iedn.xlarge (4 vCPU, 128 GiB)
- x2iedn.2xlarge (8 vCPU, 256 GiB)
- x2iedn.4xlarge (16 vCPU, 512 GiB)
- x2iedn.8xlarge (32 vCPU, 1024 GiB)
- x2iedn.16xlarge (64 vCPU, 2048 GiB)
- x2iedn.24xlarge (96 vCPU, 3072 GiB)
- x2iedn.32xlarge (128 vCPU, 4096 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)
- x2iezn.metal (48 vCPU, 1,536 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)
- 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.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)
- 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)
- 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, 1024 GiB)

2.4.4 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。

此实例类型在 24 个物理内核上提供 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.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)

例 2.7. 存储优化

- 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, 1024 GiB)
- i4i.metal (128 vCPU, 1024 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)

其它资源

- AWS 实例类型

2.1.1.6. 标准集群的 AWS 实例类型

OpenShift Dedicated 在 AWS 上提供以下 worker 节点类型和大小：

例 2.9. 常规目的

- m5.xlarge (4 vCPU, 16 GiB)
- m5.2xlarge (8 vCPU, 32 GiB)
- m5.4xlarge (16 vCPU, 64 GiB)

例 2.10. 内存优化

- r5.xlarge (4 vCPU, 32 GiB)
- r5.2xlarge (8 vCPU, 64 GiB)
- r5.4xlarge (16 vCPU, 128 GiB)

例 2.11. 计算优化

- c5.2xlarge (8 vCPU, 16 GiB)
- c5.4xlarge (16 vCPU, 32 GiB)

2.1.1.7. Google Cloud 计算类型

OpenShift Dedicated 在 Google Cloud 上提供以下 worker 节点类型和大小，它们选择具有与其他云实例类型相同的通用 CPU 和内存容量：

注意

e2 和 **a2** 计算类型仅适用于 CCS。

例 2.12. 常规目的

- custom-4-16384 (4 vCPU, 16 GiB)
- custom-8-32768 (8 vCPU, 32 GiB)
- custom-16-65536 (16 vCPU, 64 GiB)
- custom-32-131072 (32 vCPU, 128 GiB)
- custom-48-199608 (48 vCPU, 192 GiB)
- custom-64-262144 (64 vCPU, 256 GiB)
- custom-96-393216 (96 vCPU, 384 GiB)
- e2-standard-4 (4 vCPU, 16 GiB)
- n2-standard-4 (4 vCPU, 16 GiB)
- e2-standard-8 (8 vCPU, 32 GiB)
- n2-standard-8 (8 vCPU, 32 GiB)
- e2-standard-16 (16 vCPU, 64 GiB)
- n2-standard-16 (16 vCPU, 64 GiB)
- e2-standard-32 (32 vCPU, 128 GiB)
- n2-standard-32 (32 vCPU, 128 GiB)
- n2-standard-48 (48 vCPU, 192 GiB)
- n2-standard-64 (64 vCPU, 256 GiB)
- n2-standard-80 (80 vCPU, 320 GiB)
- n2-standard-96 (96 vCPU, 384 GiB)
- n2-standard-128 (128 vCPU, 512 GiB)

例 2.13. 内存优化

- custom-4-32768-ext (4 vCPU, 32 GiB)
- custom-8-65536-ext (8 vCPU, 64 GiB)
- custom-16-131072-ext (16 vCPU, 128 GiB)
- e2-highmem-4 (4 vCPU, 32 GiB)
- e2-highmem-8 (8 vCPU, 64 GiB)
- e2-highmem-16 (16 vCPU, 128 GiB)
- n2-highmem-4 (4 vCPU, 32 GiB)
- n2-highmem-8 (8 vCPU, 64 GiB)
- n2-highmem-16 (16 vCPU, 128 GiB)
- n2-highmem-32 (32 vCPU, 256 GiB)
- n2-highmem-48 (48 vCPU, 384 GiB)
- n2-highmem-64 (64 vCPU, 512 GiB)
- n2-highmem-80 (80 vCPU, 640 GiB)
- n2-highmem-96 (96 vCPU, 768 GiB)
- n2-highmem-128 (128 vCPU, 864 GiB)

例 2.14. 计算优化

- custom-8-16384 (8 vCPU, 16 GiB)
- custom-16-32768 (16 vCPU, 32 GiB)
- custom-36-73728 (36 vCPU, 72 GiB)
- custom-48-98304 (48 vCPU, 96 GiB)
- custom-72-147456 (72 vCPU, 144 GiB)
- custom-96-196608 (96 vCPU, 192 GiB)
- c2-standard-4 (4 vCPU, 16 GiB)
- c2-standard-8 (8 vCPU, 32 GiB)
- c2-standard-16 (16 vCPU, 64 GiB)
- c2-standard-30 (30 vCPU, 120 GiB)
- c2-standard-60 (60 vCPU, 240 GiB)

- e2-highcpu-8 (8 vCPU, 8 GiB)
- e2-highcpu-16 (16 vCPU, 16 GiB)
- e2-highcpu-32 (32 vCPU, 32 GiB)
- n2-highcpu-8 (8 vCPU, 8 GiB)
- n2-highcpu-16 (16 vCPU, 16 GiB)
- n2-highcpu-32 (32 vCPU, 32 GiB)
- n2-highcpu-48 (48 vCPU, 48 GiB)
- n2-highcpu-64 (64 vCPU, 64 GiB)
- n2-highcpu-80 (80 vCPU, 80 GiB)
- n2-highcpu-96 (96 vCPU, 96 GiB)

例 2.15. 加速计算

- a2-highgpu-1g (12 vCPU, 85 GiB)
- a2-highgpu-2g (24 vCPU, 170 GiB)
- a2-highgpu-4g (48 vCPU, 340 GiB)
- a2-highgpu-8g (96 vCPU, 680 GiB)
- a2-megagpu-16g (96 vCPU, 1.33 TiB)

2.1.1.8. 地区和可用性区域

OpenShift Container Platform 4 支持以下 AWS 区域，并受 OpenShift Dedicated 的支持：

- af-south-1 (Cape Town, AWS opt-in required)
- ap-east-1 (Hong Kong, AWS opt-in required)
- ap-northeast-1（东京）
- ap-northeast-2 （首尔）
- ap-northeast-3 (Osaka)
- ap-south-1（孟买）
- ap-south-2 (Hyderabad, 需要 AWS opt-in)
- ap-southeast-1（新加坡）
- ap-southeast-2（悉尼）
- ap-southeast-3(Jakarta, AWS opt-in required)

- ap-southeast-4 (Melbourne, AWS opt-in required)
- ca-central-1 (Central Canada)
- eu-central-1（法拉克福）
- eu-central-2 (Zurich, AWS opt-in required)
- eu-north-1（斯德哥尔摩）
- eu-south-1 (Milan、AWS opt-in required)
- eu-south-2 (Spain, AWS opt-in required)
- eu-west-1（爱尔兰）
- eu-west-2（伦敦）
- eu-west-3（巴黎）
- me-central-1 (UAE, AWS opt-in required)
- me-south-1 (Bahrain, AWS opt-in required)
- sa-east-1（圣保罗）
- 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）

目前支持以下 Google Cloud 区域：

- asia-east1, Changhua County, Taiwan
- asia-east2, Hong Kong
- asia-northeast1, Tokyo, Japan
- asia-northeast2, Osaka, Japan
- asia-south1, Mumbai, India
- asia-south2, Delhi, India
- asia-southeast1, Jurong West, Singapore
- australia-southeast1, Sydney, Australia
- australia-southeast2, Melbourne, Australia
- europe-north1, Hamina, Finland
- europe-west1, St. Ghislain, Belgium

- europe-west2, London, England, UK
- europe-west3, Frankfurt, Germany
- europe-west4, Eemshaven, Netherlands
- europe-west6, Zürich, Switzerland
- europe-west8, Milan, Italy
- europe-west12, Turin, Italy
- europe-southwest1, Madrid, Span
- northamerica-northeast1, Montréal, Québec, Canada
- southamerica-east1, Osasco (São Paulo), Brazil
- southamerica-west1, Santiago, Chile
- us-central1, Council Bluffs, Iowa, USA
- us-east1, Moncks Corner, South Carolina, USA
- us-east4, Ashburn, Northern Virginia, USA
- us-west1, The Dalles, Oregon, USA
- us-west2, Los Angeles, California, USA
- me-central1, Doha, Qatar
- me-central2, Dammam, Saudi Arabia

多 AZ 集群只能部署到至少有 3 个可用区的区域（请参阅 AWS 和 Google Cloud）。

每个新的 OpenShift Dedicated 集群都在单一区域的专用虚拟私有云(VPC)中安装，可选择部署到单个可用区(Single-AZ)或多个可用区(Multi-AZ)中。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。持久性卷由云块存储支持，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。

2.1.1.9. 服务级别协议 (SLA)

任何服务的 SLA 都在 红帽企业协议附录 4 （在线订阅服务）的附录 4 中定义。

2.1.1.10. 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 的请求。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

红帽不会在其结束日期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原生 OpenShift Dedicated 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。

2.1.1.11. 支持

OpenShift Dedicated 包括红帽高级支持，可以使用 红帽客户门户网站 访问。

如需了解有关 OpenShift Dedicated 包含的支持的更多详情，请参阅 覆盖范围页面。

如需支持响应时间，请参阅 OpenShift Dedicated SLA。

2.1.2. 日志记录

OpenShift Dedicated 为 Amazon CloudWatch （在 AWS）或 Google Cloud Logging （在 GCP 上）提供可选集成日志转发。

如需更多信息，请参阅关于日志收集和转发。

2.1.2.1. 集群日志记录

如果启用了集成，可通过 Amazon CloudWatch (AWS)或 Google Cloud Logging (GCP)提供集群审计日志。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。审计日志请求必须指定日期和时间范围，而不是超过 21 天。在请求审计日志时，客户应该注意审计日志的大小超过 GB。

2.1.2.2. 应用程序日志记录

如果已安装，发送到 **STDOUT** 的应用程序日志将通过集群日志记录堆栈转发到 Amazon CloudWatch （在 AWS 上）或 Google Cloud Logging （在 GCP 上）。

2.1.3. 监控

2.1.3.1. 集群指标

OpenShift Dedicated 集群附带了一个集成的 Prometheus/Grafana 堆栈，用于监控包括 CPU、内存和基于网络的指标。这可以通过 web 控制台访问，也可以通过 Grafana 仪表板查看集群级别状态和容量/使用情况。这些指标还允许 pod 横向自动扩展基于 OpenShift Dedicated 用户提供的 CPU 或内存指标。

2.1.3.2. 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。

2.1.4. 网络

2.1.4.1. 应用程序自定义域

警告

从 OpenShift Dedicated 4.14 开始，自定义域 Operator 已被弃用。要在 OpenShift Dedicated 4.14 或更高版本中管理 Ingress，请使用 Ingress Operator。对于 OpenShift Dedicated 4.13 及更早版本，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显示在 **Route Details** 页面中。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。

2.1.4.2. 集群服务的自定义域

自定义域和子域不适用于平台服务路由，如 API 或 Web 控制台路由，或用于默认应用程序路由。

2.1.4.3. 域验证证书

OpenShift Dedicated 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单独的 TLS 通配符证书，一个用于 Web 控制台，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。集群内的路由（如内部 API 端点 ）使用由集群内置证书颁发机构签名的 TLS 证书，并要求每个 pod 中的 CA 捆绑包信任 TLS 证书。

2.1.4.4. 构建的自定义证书颁发机构

OpenShift Dedicated 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。

2.1.4.5. 负载均衡器

OpenShift Dedicated 使用最多 5 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 Container Platform 和 Kubernetes API 的外部 control plane 负载均衡器。此负载均衡器可以在 Red Hat 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 以指向内部控制负载均衡器。

- 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，只有来自允许的堡垒主机的通信才可以进行。

- 默认路由器/入口负载均衡器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 'Label match'，则只有与此标签匹配的应用程序路由才会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：可映射到 OpenShift Dedicated 上运行的服务的负载均衡器，以启用高级入口功能，如非 HTTP/SNI 流量或使用非标准端口。对于标准集群，可以以 4 个为一组购买，或者可以在客户云订阅 (CCS) 集群中置备它们；但是，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。

2.1.4.6. 网络使用量

对于标准 OpenShift Dedicated 集群，网络使用量根据入站、VPC 对等、VPN 和 AZ 流量之间的数据传输来衡量。在标准的 OpenShift Dedicated 基础集群中，提供了 12TB 网络 I/O。用户可以购买额外的网络 I/O，最少单位是 12 TB。对于 CCS OpenShift Dedicated 集群，网络使用量不会被监控，由云供应商直接计费。

2.1.4.7. 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。

2.1.4.8. 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 OpenShift Dedicated 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 Dedicated 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。集群部署到接收不同的 NAT 网关的每个子网。对于在多个可用区的 AWS 上部署的集群，最多可有 3 个唯一的静态 IP 地址用于集群出口流量。对于在 Google Cloud 上部署的集群，无论可用区拓扑是什么，worker 节点出口流量都会有 1 个静态 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，因此客户在访问私有资源时不应依赖于允许列表中的单个 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.]+'"
```

2.1.4.9. 云网络配置

OpenShift Dedicated 允许通过几个云供应商管理的技术配置私有网络连接：

- VPN 连接
- AWS VPC 对等
- AWS Transit Gateway
- AWS Direct Connect
- Google Cloud VPC Network peering
- Google Cloud Classic VPN
- Google Cloud HA VPN

重要

Red Hat SREs 不监控私有网络连接。监控这些连接是客户的职责。

2.1.4.10. DNS 转发

对于具有私有云网络配置的 OpenShift Dedicated 集群，客户可以指定该私有连接上应查询的用于显式提供的域的内部 DNS 服务器。

2.1.4.11. 网络验证

当您将 OpenShift Dedicated 集群部署到现有的 Virtual Private Cloud (VPC) 或创建带有集群新子网的额外机器池时，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。

2.1.5. Storage

2.1.5.1. Encrypted-at-rest OS/node 存储

control plane 节点使用 encrypted-at-rest-EBS 存储。

2.1.5.2. encrypted-at-rest PV

默认情况下，用于持久性卷 (PV) 的 EBS 卷是 encrypted-at-rest。

2.1.5.3. 块存储 (RWO)

持久性卷 (PV) 由 AWS EBS 和 Google Cloud 持久磁盘块存储支持，该存储使用 ReadWriteOnce (RWO) 访问模式。在标准的 OpenShift Dedicated 基础集群中，为 PV 提供 100 GB 块存储，该块存储会根据应用程序请求动态置备和回收。额外的持久性存储可以 500 GB 的递增的形式购买。

PV 每次只能附加到一个节点，并特定于置备的可用区，但它们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 或 Google Cloud Platform 自定义机器类型 。

2.1.5.4. 共享存储 (RWX)

AWS CSI Driver 可用于为 AWS 上的 OpenShift Dedicated 提供 RWX 支持。提供了一个 community Operator，以简化设置。详情请参阅 OpenShift Dedicated and Red Hat OpenShift Service on AWS 上的 AWS EFS 配置。

2.1.6. 平台

2.1.6.1. 集群备份策略

重要

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 OpenShift Dedicated 服务的一部分。每个 OpenShift Dedicated 集群中的所有 Kubernetes 对象都会被备份，以便在不太可能的情况下进行提示恢复，因为集群无法正常运行。

备份存储在与集群相同的帐户的安全对象存储(Multi-AZ)存储桶中。节点根卷不会被备份，因为 Red Hat Enterprise Linux CoreOS 完全由 OpenShift Container Platform 集群管理，且没有有状态的数据应存储在节点的 root 卷中。

下表显示了备份的频率：

组件	快照频率	保留	备注
完整对象存储备份	每天 0100 UTC	7 天	这是所有 Kubernetes 对象的完整备份。在这个备份调度中没有备份持久性卷 (PV)。
完整对象存储备份	每周的周一 0200 UTC	30 天	这是所有 Kubernetes 对象的完整备份。这个备份调度中没有备份 PV。
完整对象存储备份	每小时的第 17 分钟	24 小时	这是所有 Kubernetes 对象的完整备份。这个备份调度中没有备份 PV。

2.1.6.2. 自动缩放

OpenShift Dedicated 上提供了节点自动扩展功能。如需有关在集群中自动扩展节点的更多信息，请参阅关于集群中的自动扩展节点。

2.1.6.3. 守护进程集

客户可以在 OpenShift Dedicated 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
...
```

2.1.6.4. 多个可用区

在多个可用区集群中，控制节点分布在可用区中，每个可用区需要至少三个 worker 节点。

2.1.6.5. 节点标签

红帽会在节点创建过程中创建自定义节点标签，目前无法在 OpenShift Dedicated 集群中更改。

2.1.6.6. OpenShift version

OpenShift Dedicated 作为服务运行，并与最新的 OpenShift Container Platform 版本保持最新状态。

2.1.6.7. 升级

有关升级策略和步骤的更多信息，请参阅 OpenShift Dedicated 生命周期。

2.1.6.8. Windows 容器

目前，OpenShift Dedicated 不提供 Windows 容器。

2.1.6.9. 容器引擎

OpenShift Dedicated 在 OpenShift 4 上运行，并使用 CRI-O 作为唯一可用的容器引擎。

2.1.6.10. 操作系统

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

2.1.6.11. 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，且必须在 worker 节点上部署。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

2.1.6.12. Kubernetes Operator 支持

OperatorHub 市场中列出的所有 Operator 都应该可用于安装。从 OperatorHub 安装的 Operator （包括 Red Hat Operator）不会作为 OpenShift Dedicated 服务的一部分进行管理。如需有关给定 Operator 的支持性的更多信息，请参阅红帽客户门户网站。

2.1.7. 安全性

本节提供有关 OpenShift Dedicated 安全的服务定义的信息。

2.1.7.1. 身份验证供应商

集群的身份验证被配置为 Red Hat OpenShift Cluster Manager 集群创建过程的一部分。OpenShift 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。支持置备同时置备的多个身份提供程序。支持以下身份提供程序：

- GitHub 或 GitHub Enterprise OAuth
- GitLab OAuth
- Google OAuth
- LDAP
- OpenID 连接

2.1.7.2. 特权容器

默认情况下，OpenShift Dedicated 上无法使用特权容器。**dedicated-admins** 组的成员可以使用 **anyuid** 和 **nonroot**，这应该可以满足多种用例。特权容器仅适用于 **cluster-admin** 用户。

2.1.7.3. 客户管理员用户

除了普通用户外，OpenShift Dedicated 还提供对名为 **dedicated-admin** 的 OpenShift Dedicated 特定组的访问。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。
- 可以安装来自 OperatorHub 的 Operator (* verbs在所有 ***.operators.coreos.com** API 组中)。

2.1.7.4. 集群管理角色

作为具有客户云订阅 (CCS) 的 OpenShift Dedicated 的管理员，您可以访问 **cluster-admin** 角色。使用 **cluster-admin** 角色登录到帐户时，用户最多具有控制和配置集群的不受限制的访问权限。Webhook 会阻止一些配置以防止集群的更改，或者由于它们被 OpenShift Cluster Manager 管理，所以任何集群内的更改都会被覆盖。

2.1.7.5. 项目自助服务

默认情况下，所有用户都能够创建、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
```

2.1.7.6. 法规合规性

OpenShift Dedicated 遵循常见的安全和控制最佳实践。下表中概述了认证。

表 2.1. OpenShift Dedicated 的安全性和控制认证

Compliance	AWS 上的 OpenShift Dedicated	GCP 上的 OpenShift Dedicated
HIPAA 认证的	是（仅限客户云订阅）	是（仅限客户云订阅）
ISO 27001	是	是
PCI DSS	是	是
SOC 2 类型 2	是	是

2.1.7.7. 网络安全性

每个 OpenShift Dedicated 集群都由云基础架构级别的安全网络配置使用防火墙规则(AWS 安全组或 Google Cloud Compute Engine 防火墙规则)进行保护。AWS 上的 OpenShift Dedicated 客户也会保护对 AWS Shield Standard 的 DDoS 攻击。同样，OpenShift Dedicated 在 GCP 上使用的所有 GCP 负载均衡器和公共 IP 地址都可以通过 Google Cloud Armor Standard 保护 DDoS 的攻击。

2.1.7.8. etcd 加密

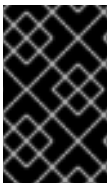
在 OpenShift Dedicated 中，control plane 存储默认加密，这包括 etcd 卷的加密。这种存储级别加密通过云供应商的存储层提供。

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。

2.2. 责任分配列表

了解 OpenShift Dedicated 托管服务的红帽、云供应商和客户职责。

2.2.1. OpenShift Dedicated 职责概述

虽然红帽会管理 OpenShift Dedicated 服务，但在某些方面客户需要共享责任。OpenShift Dedicated 服务被远程访问，托管在公有云资源上，由红帽或客户拥有的云服务供应商帐户中创建，并具有由红帽拥有的底层平台和数据安全。

重要

如果集群中启用了 **cluster-admin** 角色，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	身份和访问管理	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	共享	共享	共享	Red Hat
应用程序网络	共享	共享	共享	Red Hat	Red Hat
集群网络	Red Hat	共享	共享	Red Hat	Red Hat
虚拟网络	共享	共享	共享	共享	共享

资源	事件和操作管理	变更管理	身份和访问管理	安全和合规性	灾难恢复
control plane 和基础架构节点	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
Worker 节点	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
集群版本	Red Hat	共享	Red Hat	Red Hat	Red Hat
容量管理	Red Hat	共享	Red Hat	Red Hat	Red Hat
虚拟存储	红帽和云供应商	红帽和云供应商	红帽和云供应商	红帽和云供应商	红帽和云供应商
物理基础结构和安全	云供应商	云供应商	云供应商	云供应商	云供应商

2.2.2. 共享责任列表

客户和红帽共享负责 OpenShift Dedicated 集群的监控和维护。本文档演示了按区域和任务划分职责。

2.2.2.1. 事件和操作管理

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	红帽职责	客户职责
应用程序网络	监控云负载平衡器和原生 OpenShift 路由器服务，并响应警报。	• 监控服务负载均衡器端点的健康状况 • 监控应用程序路由的健康状况，以及其后面的端点。 • 向红帽报告出现的问题。
虚拟网络	监控默认平台网络所需的云负载均衡器、子网和公有云组件，并响应警报。	监控（可选）通过 VPC 配置为 VPC 连接、VPN 连接或直接连接，以了解潜在问题或安全威胁的网络流量。

2.2.2.2. 变更管理

红帽负责启用客户控制的集群基础架构和服务，以及维护控制平面节点、基础架构节点和服务以及 worker 节点的版本。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。

资源	红帽职责	客户职责

资源	红帽职责	客户职责
日志记录	• 集中聚合和监控平台审计日志。 • 提供和维护日志记录操作器，以便客户能够为默认应用程序日志部署日志堆栈。 • 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记录 Operator。 • 安装、配置和维护任何可选的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。
应用程序网络	• 设置公有云负载均衡器。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。 • 安装、配置和维护 OpenShift SDN 组件，以实现默认内部 pod 流量。 • 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 Red Hat OpenShift Cluster Manager 为默认应用程序路由请求私有负载均衡器。 • 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	• 设置集群管理组件，如公共或私有服务端点，以及与虚拟网络组件集成的必要。 • 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。

资源	红帽职责	客户职责
虚拟网络	• 设置并配置置备集群所需的虚拟网络组件，包括虚拟私有云、子网、负载均衡器、互联网网关、NAT 网关等。 • 为客户提供与内部资源、VPC 到 VPC 连接以及 OpenShift Cluster Manager 所需的直接连接管理 VPN 连接的功能。 • 使客户能够创建和部署公有云负载均衡器以用于服务负载均衡器。	• 设置和维护可选公有云网络组件，如 VPC 到 VPC 连接、VPN 连接或直接连接。 • 针对特定服务请求并配置任何其他服务负载均衡器。
集群版本	• 启用升级调度过程。 • 监控升级进度并更正遇到的问题。 • 为次版本和维护升级发布更改日志和发行注记。	• 可立即计划维护版本升级、未来升级或进行自动升级。 • 确认并计划次要版本升级。 • 确保集群版本保持在受支持的次版本中。 • 在次版本和维护版本中测试客户应用程序以确保兼容性。
容量管理	• 监控 control plane 的利用率 (control plane 节点和基础架构节点)。 • 扩展或重新定义 control plane 节点的大小，以维护服务质量。 • 监控客户资源的利用率，包括网络、存储和计算容量。如果无法启用自动扩展功能，客户就需要集群资源（例如，扩展新的计算节点、额外存储等）更改。	• 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。

2.2.2.3. 访问和身份授权

访问和身份授权列表包括管理对集群、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	红帽职责	客户职责

资源	红帽职责	客户职责
日志记录	• 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	提供原生 OpenShift RBAC 和 **dedicated-admin** 功能。	• 配置 OpenShift dedicated-admins 和 RBAC，以控制对路由配置的访问。 • 管理红帽机构的机构管理员，以授予 OpenShift Cluster Manager 的访问权限。OpenShift Cluster Manager 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	• 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。 • 管理红帽机构的机构管理员，以授予 OpenShift Cluster Manager 的访问权限。 • 配置 OpenShift dedicated-admins 和 RBAC，以控制对路由配置的访问。
虚拟网络	通过 OpenShift Cluster Manager 提供客户访问控制。	通过 OpenShift Cluster Manager 管理对公有云组件的可选用户访问。

2.2.2.4. 安全和合规性

以下是与合规相关的职责和控制相关：

资源	红帽职责	客户职责
日志记录	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。

资源	红帽职责	客户职责
虚拟网络	• 监控虚拟网络组件以了解潜在的问题和安全隐患。 • 利用其他公有云提供商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威胁。 • 根据需要配置任何必要的防火墙规则或数据中心保护。

2.2.2.5. 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。

资源	红帽职责	客户职责
虚拟网络	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。

2.2.3. 客户对数据和应用程序的职责

客户负责他们部署到 OpenShift Dedicated 中的应用程序、工作负载和数据。但是，红帽提供各种工具来帮助客户管理平台上的数据和应用程序。

资源	红帽职责	客户职责
客户数据	• 维护平台级数据加密标准。 • 提供 OpenShift 组件以帮助管理应用数据，如机密。 • 启用与第三方数据库服务（如 AWS RDS 或 Google Cloud SQL）集成，以存储和管理集群和/或云供应商之外的数据。	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	红帽职责	客户职责
客户应用程序	• 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 以将社区、第三方和红帽服务添加到集群中。 • 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。	• 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处理适当的提供程序（包括红帽）来排查任何问题。 • 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 OpenShift Dedicated 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并创建警报。

2.3. 了解 OPENSHIFT DEDICATED 的进程和安全性

2.3.1. 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。

2.3.1.1. 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。

2.3.2. 事件和操作管理

本文档详细介绍了 OpenShift Dedicated 管理服务的职责。云提供商负责保护运行云提供商所提供的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。

2.3.2.1. 平台监控

红帽站点可靠性工程师(SRE)为所有 OpenShift Dedicated 集群组件、SRE 服务和底层云供应商帐户维护集中监控和警报系统。平台审计日志可以安全地转发到集中式 SIEM （安全信息和事件监控）系统，其中可能会触发 SRE 团队配置的警报，也可以手动审核。审计日志保留在 SIEM 中一年。当集群被删除时，给定集群的审计日志不会被删除。

2.3.2.2. 事件管理

事件是导致一个或多个红帽服务降级或中断事件。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。

如何由红帽管理新事件的一般工作流：

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，一个根本原因分析在事件的 5 个工作日内进行。
6. 根本原因分析 (RCA) 草案文档在事件的 7 个工作日内与客户共享。

2.3.2.3. 备份和恢复

所有 OpenShift Dedicated 集群都使用云供应商快照备份。值得注意的是，这不包括存储在持久性卷 (PV) 上的客户数据。所有快照都使用适当的云供应商快照 API，并上传到与集群相同的帐户中的安全对象存储桶(AWS 中的S3 和 Google Cloud 中的 GCS)中。

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。这个备份调度中没有备份 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。

- 红帽不提交任何恢复点目标 (RPO) 或恢复时间目标 (RTO)。
- 客户负责对其数据的定期备份
- 客户应部署带有 Kubernetes 最佳实践工作负载的 multi-AZ 集群，以确保在区域内高可用性。
- 如果整个云区域不可用，客户必须在不同的区域安装新集群，并使用备份数据恢复其应用程序。

2.3.2.4. 集群容量

评估和管理集群容量是由红帽和客户之间共享的责任。Red Hat SRE 负责集群中所有 control plane 和基础架构节点的容量。

红帽 SRE 还会评估升级过程中的集群容量，并响应集群警报。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。

SRE 人员的容量评估也会在响应集群中的警报时发生，在一定时间段内超过使用量阈值。这些警报也可以产生给客户的通知。

2.3.3. 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。

2.3.3.1. 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。

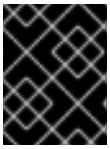
更改历史记录在 OpenShift Cluster Manager **Overview** 选项卡中的 **Cluster History** 部分中捕获，供您查看。更改历史记录包括但不仅限于，日志来自以下变化：

- 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。

2.3.3.2. 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 OpenShift Dedicated 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。

2.3.3.3. 补丁管理

OpenShift Container Platform 软件和底层不可变 Red Hat Enterprise Linux CoreOS (RHCOS) 操作系统镜像针对常规 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。

2.3.3.4. 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。只有集群受严重影响 CVE 的影响时，红帽才会强制将集群升级到新的 z-stream 版本。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。

2.3.4. 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。

2.3.4.1. 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，并强调所收集、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。

2.3.4.2. 数据管理

OpenShift Dedicated 使用 AWS 密钥管理服务(KMS)和 Google Cloud KMS 等云供应商服务，以帮助安全地管理持久数据的加密密钥。这些密钥用于加密所有 control plane、基础架构和 worker 节点根卷。客户可在安装时为加密根卷指定自己的 KMS 密钥。持久性卷(PV)也使用 KMS 进行密钥管理。通过创建一个新的 **StorageClass** 引用 KMS 密钥 Amazon Resource Name (ARN)或 ID，用户可以指定自己的 KMS 密钥进行加密 PV。

当客户删除其 OpenShift Dedicated 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)。

2.3.4.3. 漏洞管理

红帽使用行业标准工具对 OpenShift Dedicated 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。

2.3.4.4. 网络安全性

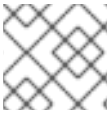
2.3.4.4.1. 防火墙和 DDoS 保护

每个 OpenShift Dedicated 集群都由云基础架构级别的安全网络配置使用防火墙规则(AWS 安全组或 Google Cloud Compute Engine 防火墙规则)进行保护。AWS 上的 OpenShift Dedicated 客户也会保护对 AWS Shield Standard 的 DDoS 攻击。同样，OpenShift Dedicated 在 GCP 上使用的所有 GCP 负载均衡器和公共 IP 地址都可以通过 Google Cloud Armor Standard 保护 DDoS 的攻击。

2.3.4.4.2. 私有集群和网络连接

客户可以选择配置其 OpenShift Dedicated 集群端点(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 或应用程序。

对于 AWS，用户可以通过 AWS VPC 对等、AWS VPN 或 AWS Direct Connect 配置私有网络连接。



注意

目前，Google Cloud 上的 OpenShift Dedicated 集群不支持私有集群。

2.3.4.4.3. 集群网络访问控制

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

2.3.4.5. penetration 测试

红帽对 OpenShift Dedicated 执行定期测试。测试由独立的内部团队使用行业标准工具和最佳实践进行。

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

2.3.4.6. Compliance

OpenShift Dedicated 遵循常见的安全和控制最佳实践。下表中概述了认证。

表 2.2. OpenShift Dedicated 的安全性和控制认证

Compliance	AWS 上的 OpenShift Dedicated	GCP 上的 OpenShift Dedicated
HIPAA 认证的	是（仅限客户云订阅）	是（仅限客户云订阅）
ISO 27001	是	是
PCI DSS	是	是
SOC 2 类型 2	是	是

其他资源

- 有关 SRE 驻留的信息，请参阅 Red Hat Subprocessor 列表。

2.3.5. 灾难恢复

OpenShift Dedicated 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（例如，单区部署与多区部署）来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。

2.3.6. 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。

2.4. SRE 和服务帐户访问

2.4.1. 身份和访问管理

红帽站点可靠性工程 (SRE) 团队的大部分访问是通过自动化配置管理的集群 Operator 来完成。

2.4.1.1. 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。

2.4.1.2. SRE 访问所有 OpenShift Dedicated 集群

SREs 通过代理访问 OpenShift Dedicated 集群。代理会在 OpenShift Dedicated 集群中登录时为 SREs 使用服务帐户进行 mint。因为没有为 OpenShift Dedicated 集群配置身份提供程序，因此 SREs 通过运行本地 Web 控制台容器来访问代理。SRE 无法直接访问集群 Web 控制台。SRE 必须以单独的用户身份进行身份验证以确保可审核性。所有验证尝试都会记录到安全信息和事件管理 (SIEM) 系统。

2.4.1.3. OpenShift Dedicated 中的特权访问控制

Red Hat SRE 在访问 OpenShift Dedicated 和公有云供应商组件时遵循最小特权原则。SRE 访问有四个基本类别：

- SRE 管理员通过带有正常双因素身份验证的红帽客户门户网站访问，且没有特权提升。
- 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。它经过全面审核，每个操作 SREs 都需要管理批准。
- 云供应商访问或提升，这是云供应商控制台或 CLI 访问的手动提升。访问仅限于 60 分钟，并且完全审核。

每种访问类型对组件有不同的访问权限级别：

组件	典型的 SRE 管理访问权限（红帽客户门户）	典型的 SRE 管理员访问权限（红帽 SSO）	OpenShift elevation	云供应商访问
OpenShift Cluster Manager	R/W	无权限	无权限	无权限
OpenShift web 控制台	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。

2.4.1.4. SRE 对云基础架构帐户的访问

红帽人员在日常 OpenShift Dedicated 操作中无法访问云基础架构帐户。出于紧急故障排除目的，Red Hat SRE 具有定义并可审核的流程来访问云基础架构帐户。

在 AWS 中，SRE 使用 AWS 安全令牌服务(STS)为 **BYOCAdminAccess** 用户生成简短的 AWS 访问令牌。对 STS 令牌的访问会被记录，可追溯到单个用户。**BYOCAdminAccess** 附加了 **AdministratorAccess** IAM 策略。

在 Google Cloud 中，SRES 在针对 Red Hat SAML 身份提供程序(IDP)进行身份验证后访问资源。IDP 授权有生存时间过期的令牌。令牌的颁发由企业红帽 IT 进行审核，并链接到个人用户。

2.4.1.5. 红帽支持访问

红帽 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	云基础架构帐户*
OpenShift SRE	Read: All Write: Very Limited [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: Limited[4] Write: Limited[4]
客户用户	Read: None Write: None	Read: None Write: None	Read: Limited[5] Write: Limited[5]	Read: None Write: None
其他人	Read: None Write: None	Read: None Write: None	Read: None Write: None	Read: None Write: None

Cloud Infrastructure Account 指的是底层 AWS 或 Google Cloud 帐户

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 对云基础架构帐户的访问是一个"break-glass"过程，用于在记录的事件期间进行故障排除。
4. 客户管理员通过 Cloud Infrastructure Access 限制对云基础架构帐户控制台的访问权限。
5. 限制为通过 RBAC 授予的内容，以及用户创建的命名空间。

2.4.1.6. 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"观察身份验证"部分。

2.4.1.7. 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。

2.4.2. SRE 集群访问

SRE 对 OpenShift Dedicated 集群的访问是通过多个所需身份验证层控制的，它们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。刷新到一个新令牌的能力是无限的，但刷新到一个新令牌的能力会在 30 不活跃后被撤销。

- 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 是多因素的，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平面。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。

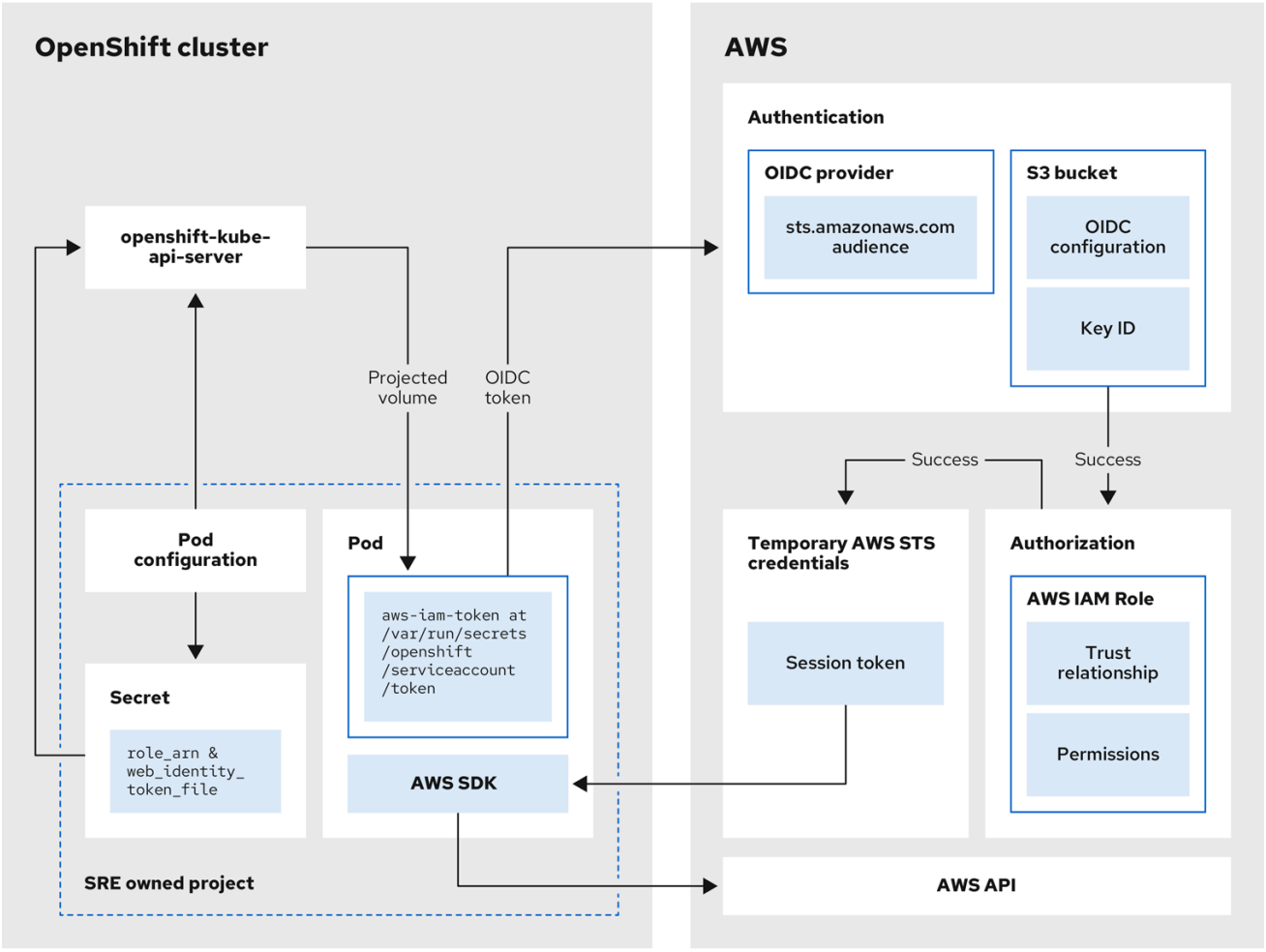
2.4.3. 服务帐户如何假定 SRE 拥有的项目中的 AWS IAM 角色

安装使用 AWS 安全令牌服务 (STS) 的 OpenShift Dedicated 集群时，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 OpenShift Dedicated 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 2.1. 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，OpenShift Dedicated 会生成新令牌，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 OpenShift Dedicated 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。

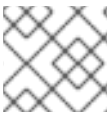
2.5. 了解 OPENSHIFT DEDICATED 的可用性

可用性和灾难性对于任何应用平台至关重要。OpenShift Dedicated 在多个级别为故障提供了许多保护，但必须为高可用性配置客户部署的应用程序。另外，要考虑可能会出现云供应商中断，可以使用其他选项，例如在多个可用区间部署集群或使用故障转移机制维护多个集群。

2.5.1. 潜在的故障点

OpenShift Container Platform 为防止您的工作负载停机提供了许多功能和选项，但必须正确设计应用程序才能利用这些功能。

OpenShift Dedicated 通过添加 Red Hat Site Reliability engineers (SRE) 支持以及部署多区集群的选项，但存在许多容器或基础架构仍失败的方法，您可以进一步保护您出现常见的 Kubernetes 问题。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。

2.5.1.1. 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，以便运行应用程序 pod 的多个实例可防止任何 pod 或容器的问题。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 中断预算非常重要。这些是 Kubernetes API 的一部分，可以像其他对象类型一样通过 OpenShift CLI (**oc**)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。

2.5.1.2. 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，对于单个可用区集群，OpenShift Dedicated

集群至少有四个 worker 节点。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。

2.5.1.3. 集群故障

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

如果出现完整的 control plane 节点中断，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 或节点中断，则 control plane 节点必须在添加新 pod 或节点前恢复。

在基础架构节点上运行的所有服务都由红帽配置成高度可用，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。

2.5.1.4. 区失败

来自公有云供应商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。为了防止区故障，OpenShift Dedicated 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。

2.5.1.5. 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。

2.6. OPENSHIFT DEDICATED 更新生命周期

2.6.1. 概述

红帽为 OpenShift Dedicated 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。

OpenShift Dedicated 是 Red Hat OpenShift 的受管实例，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 OpenShift Dedicated 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 OpenShift Dedicated 维护计划。

其他资源

- OpenShift Dedicated 服务定义

2.6.2. 定义

表 2.3. 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)

OpenShift Dedicated 的主版本（如版本 4）自发布后续主版本或产品停用后的一年内被支持。

示例

- 如果 OpenShift Dedicated 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 天的通知。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。

Example

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。

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原生 OpenShift Dedicated 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 OpenShift Dedicated 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。

2.6.10. 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 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
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