OpenShift Container Platform 4.8

关于

OpenShift Container Platform 简介

Last Updated: 2023-04-07

OpenShift Container Platform 4.8 关于

OpenShift Container Platform 简介

法律通告

摘要

本文档概述 OpenShift Container Platform 的功能。

目录

第 1 章 OPENSHIFT CONTAINER PLATFORM 4.8 文档

欢迎使用官方的 OpenShift Container Platform 4.8 文档，您可以在其中了解 OpenShift Container Platform 并开始了解其功能。

要浏览 OpenShift Container Platform 4.8 文档，您可以使用以下方法之一：

- 使用左侧导航栏浏览文档。
- 从此 Welcome 页面上的内容中选择您感兴趣的内容。

从架构和安全及合规性开始。然后请查看发行注记。

1.1. 集群安装程序操作

探索这些 OpenShift Container Platform 安装任务。

- **OpenShift Container Platform 安装概述**：您可以在安装程序置备或用户置备的基础架构上安装 OpenShift Container Platform。OpenShift Container Platform 安装程序提供了在各种不同平台上部署 OpenShift Container Platform 的灵活性。
- **在 AWS 上安装集群**：当您在 Amazon Web Services (AWS) 上部署集群时，有许多安装选项。您可以使用默认设置或自定义 AWS 设置部署集群。您还可以在您置备的 AWS 基础架构上安装集群。您可以修改提供的 AWS CloudFormation 模板，以满足您的需要。
- **在 Azure 上安装集群**：您可以使用默认设置、自定义 Azure 设置 或 Microsoft Azure 中的自定义网络设置部署集群。您还可以将 OpenShift Container Platform 安装到 Azure Virtual Network 中，或使用 Azure Resource Manager 模板置备自己的基础架构。
- **在 GCP 上安装集群**：您可以使用默认设置或自定义 GCP 设置在 Google Cloud Platform (GCP) 上部署集群。您还可以在置备自己的基础架构的情况下执行 GCP 安装。
- **在 VMware vSphere 上安装集群**：您可以在支持的 vSphere 版本上安装 OpenShift Container Platform。
- **在 IBM Z 和 LinuxONE 上使用 z/VM 安装集群**：您可以在用户置备的基础架构上的 IBM Z 和 LinuxONE 上安装带有 z/VM 的 OpenShift Container Platform。
- **在 IBM Z 和 LinuxONE 上使用 RHEL KVM 安装集群**：您可以在用户置备的基础架构上的 IBM Z 和 LinuxONE 上使用 RHEL KVM 安装 OpenShift Container Platform。
- **在 IBM Power Systems 上安装集群**：您可以在用户置备的基础架构的 IBM Power Systems 上安装 OpenShift Container Platform。
- **在裸机上安装安装程序置备的集群**：您可以使用安装程序置备的架构在裸机上安装 OpenShift Container Platform。
- **在裸机上安装用户置备的集群**：如果没有可用的平台和云供应商部署选项，您可以在用户置备的基础架构上安装 OpenShift Container Platform。
- **在 Red Hat OpenStack Platform (RHOSP) 上安装集群**：您可以使用 带有自定义的 RHOSP 上安装集群。
- **在 Red Hat Virtualization (RHV) 上安装集群**：您可以使用快速安装或使用自定义的安装在 Red Hat Virtualization (RHV) 上安装集群。

- **在受限网络中安装集群**: 如果您的集群使用 AWS, GCP, vSphere, IBM Z and LinuxONE with z/VM , IBM Z and LinuxONE with RHEL KVM , IBM Power Systems, 或裸机上的、无法完全访问互联网的用户置备的基础架构，使用以下方法之一 mirror OpenShift Container Platform 安装镜像，然后在这个受限的环境中进行安装。

- **在现有网络中安装集群** ：如果您使用 AWS 或 GCP 中的一个现存的 Virtual Private Cloud (VPC)，或使用 Azure 上的现存的 VNet，您可以安装集群。

- **安装一个私有集群**：如果集群不需要外部互联网访问，您可以在 AWS、Azure 或 GCP 上安装私有集群。要访问云 API 和安装介质时，仍需要访问互联网。

- **检查安装日志** ：检查安装日志，评估在 OpenShift Container Platform 4.8 安装过程中发生的问题。

- **访问 OpenShift Container Platform**：使用安装过程末尾的凭证输出，从命令行或 Web 控制台登录到 OpenShift Container Platform 集群。

- **安装 Red Hat OpenShift Container Storage**：您可以安装 Red Hat OpenShift Container Storage 作为 Operator，以便为容器提供高度集成和简化的持久性存储管理。

1.2. 开发人员活动

使用 OpenShift Container Platform 开发和部署容器化应用。OpenShift Container Platform 是一个用于开发和部署容器化应用程序的平台。OpenShift Container Platform 文档可帮助您：

- **了解 OpenShift Container Platform 开发** ：了解不同类型的容器化应用，从简单的容器到高级 Kubernetes 部署和 Operator。

- **使用项目** ：通过 OpenShift Container Platform Web 控制台或 OpenShift CLI(**oc**)创建项目以组织和共享您开发的软件。

- **使用应用程序** ：

使用 OpenShift Container Platform web 控制台的**开发者**视角创建并部署应用程序。

使用 **Topology** 视图查看 应用程序、监控状态、连接和组组件，以及修改您的代码库。

- **使用开发人员 CLI 工具(odo)** ： **odo** CLI 工具允许开发人员创建单个或多组件应用程序，并自动执行部署、构建和服务路由配置。它提取了复杂的 Kubernetes 和 OpenShift Container Platform 概念，允许您专注于开发应用程序。

- **创建 CI/CD 管道** ：管道是无服务器、云原生、持续集成和在隔离容器中运行的持续部署系统。它们使用标准的 Tekton 自定义资源来实现部署自动化，并为处理基于微服务的架构的非中心化团队设计。

- **部署 Helm chart**Helm 3 是一个软件包管理器，可帮助开发人员在 Kubernetes 中定义、安装和更新应用程序软件包。Helm Chart 是一个打包格式，用于描述可以使用 Helm CLI 部署的应用程序。

- **了解镜像构建** ：从不同的构建策略（Docker、S2I、自定义和管道）中选择可以包括不同类型的源资料（Git 存储库、本地二进制输入和外部工件）。然后，请参阅从基本构建到高级构建的构建类型示例。

- **创建容器镜像** ：容器镜像是 OpenShift Container Platform（和 Kubernetes）应用程序中最基本的构建块。通过定义镜像流，在继续开发镜像时，可让您在一个位置保存镜像的多个版本。S2I 容器允许您将源代码插入到基本容器中，该容器被设置为运行特定类型的代码，如 Ruby、Node.js 或 Python。

- **创建部署** ：使用 **Deployment** 和 **DeploymentConfig** 对象对应用程序进行精细管理。使用 **Workloads** 页面或 OpenShift CLI (**oc**) 管理部署。了解 滚动、重新创建和自定义部署策略。
- **创建模板** ：使用现有模板或创建自己的模板来描述应用的构建或部署方式。模板可以将镜像与描述、参数、副本、公开端口和其他定义如何运行或构建的内容相结合。
- **了解 Operator**：Operator 是为 OpenShift Container Platform 4.8 创建集群应用程序的首选方法。了解 Operator Framework 以及如何使用已安装的 Operator 部署到项目中。
- **开发 Operator**：Operator 是为 OpenShift Container Platform 4.8 创建集群应用程序的首选方法。了解构建、测试和部署 Operator 的工作流。然后，基于 Ansible 或 Helm 创建自己的 Operator，或使用 Operator SDK 配置内置 Prometheus 监控。
- **REST API 参考** ：了解 OpenShift Container Platform 应用程序编程接口端点。

1.3. 集群管理员活动

管理虚拟机，向用户提供服务，并遵循监控和日志记录报告。本文档可帮助您：

- **了解 OpenShift Container Platform 管理** ：了解 OpenShift Container Platform 4.8 control plane 的组件。请参阅 OpenShift Container Platform control plane 和 worker 节点如何通过 Machine API 和 Operator 进行管理和更新。

1.3.1. 管理集群组件

- **管理机器** ：通过部署健康检查并将自动扩展应用到机器，在 AWS、Azure 或 GCP 上管理集群中的机器。
- **管理容器 registry** ：每个 OpenShift Container Platform 集群都包含一个内置容器 registry 来存储其镜像。您还可以配置用于 OpenShift Container Platform 的独立 Red Hat Quay registry。Quay.io 网站提供了一个公共容器 registry，用于存储 OpenShift Container Platform 容器和 Operator。
- **管理用户和组** ：添加具有不同级别的用户和组，以使用或修改集群。
- **管理身份验证** ：了解用户、组和 API 身份验证在 OpenShift Container Platform 中的工作方式。OpenShift Container Platform 支持多个身份提供程序，包括：
  - HTPasswd
  - Keystone
  - LDAP
  - 基本身份验证
  - 请求标头(Request header)
  - GitHub
  - GitLab
  - Google
  - openid

- **管理入口（ingress）、API 服务器和服务证书**：OpenShift Container Platform 默认为 Ingress Operator、API 服务器创建证书，以及需要加密的复杂中间件应用程序所需的服务。您可能需要更改、添加或轮转这些证书。

- **管理网络**：OpenShift Container Platform 中的集群网络由 Cluster Network Operator (CNO)管理。CNO 使用 kube-proxy 中的 iptables 规则用来处理在这些节点上运行的节点和 pod 间的网络流量。Multus Container Network Interface 添加了将 多网络接口附加到 pod 的功能。使用网络策略功能，您可以隔离 pod 或允许所选流量。

- **管理存储**：OpenShift Container Platform 允许管理员使用 Red Hat OpenShift Container Storage、AWS Elastic Block Store、NFS、iSCSI、Container Storage Interface(CSI) 配置持久性存储。您可以扩展持久性卷，配置 动态置备，并使用 CSI 配置、克隆，并使用持久性存储的快照。

- **管理 Operator**：Red Hat, ISV, 和社区 Operators 列表，集群管理员可对其进行审核并 在集群上进行安装。安装之后，您可以运行、升级、备份或者管理集群中的 Operator。

1.3.2. 更改集群组件

- **使用自定义资源定义(CRD)修改集群**：通过 Operator 实施的集群功能可使用 CRD 修改。了解 创建 CRD 以及从 CRD管理资源。

- **设置资源配额**：从 CPU、内存和其他系统资源中选择来设置配额。

- **修剪和回收资源**：通过修剪不需要的 Operator、组、部署、构建、镜像、registry 和 cron 作业来回收空间。

- **扩展和调优集群**：设置集群限制、调整节点、扩展集群监控和优化您的环境的网络、存储和路由。

- **更新集群**：使用 Cluster Version Operator (CVO) 升级 OpenShift Container Platform 集群。如果 OpenShift Update Service(OSUS)提供了更新，您可以通过 OpenShift Container Platform Web 控制台或 OpenShift CLI (**oc**) 应用该集群更新。

- **了解 OpenShift Update Service**：了解如何安装和管理本地 OpenShift Update Service，以便在断开连接的网络环境中推荐 OpenShift Container Platform 更新。

1.3.3. 监控集群

- **使用 OpenShift Logging**：了解 OpenShift Logging 并配置不同的 OpenShift Logging 类型，如 Elasticsearch、Fluentd 和 Kibana。

- **监控集群**：了解如何配置监控堆栈。配置监控后，使用 Web 控制台访问监控仪表板。除了基础架构指标外，您还可以提取和查看您自己的服务的指标。

- **远程健康监控**：OpenShift Container Platform 会收集有关集群的匿名汇总信息。通过使用 Telemetry 和 Insights Operator，红帽会接收这些数据，用于改进 OpenShift Container Platform。您可以查看远程健康监控收集的数据。

第 2 章 了解有关 OPENSHIFT CONTAINER PLATFORM 的更多信息

使用以下小节查找内容以帮助您了解和使用 OpenShift Container Platform。

2.1. 架构

了解 OpenShift Container Platform	规划 OpenShift Container Platform 部署	其他资源
Enterprise Kubernetes with OpenShift	经过测试的平台	OpenShift blog
架构	安全性与合规性	OpenShift Container Platform 新功能
	网络	OpenShift Container Platform 生命周期
	备份和恢复	

2.2. CLUSTER ADMINISTRATOR

了解 OpenShift Container Platform	部署 OpenShift Container Platform	管理 OpenShift Container Platform	其他资源
Enterprise Kubernetes with OpenShift	安装 OpenShift Container Platform	使用 Insights 发现集群中的问题	获得支持
架构	安装后配置	日志记录	OpenShift 知识库文章
OpenShift 互动学习门户	网络	监控	OpenShift Container Platform 生命周期
	存储		
	备份和恢复		
	更新集群		

2.3. 应用程序站点可靠性工程师 (APP SRE)

了解 OpenShift Container Platform	部署和管理应用程序	其他资源
OpenShift 互动学习门户	项目	获得支持
架构	Operator	OpenShift 知识库文章
	日志记录	OpenShift Container Platform 生命周期
	关于日志的博客	
	监控	

2.4. 开发者

在 OpenShift Container Platform 中了解应用程序开发	部署应用程序
OpenShift 入门供开发人员使用（交互式教程）	创建应用程序
Red Hat Developers 网站	Builds
Red Hat CodeReady Workspaces	Operator
	镜像
	以开发者为中心的 CLI

2.5. 了解 OPENSHIFT CONTAINER PLATFORM

OpenShift Container Platform 是一个 Kubernetes 环境，用于管理基于容器的应用程序及其对各种计算平台的依赖，如裸机、虚拟化、内部云等。OpenShift Container Platform 部署、配置和管理容器。OpenShift Container Platform 为其组件提供可用性、稳定性和自定义。

OpenShift Container Platform 利用多个计算资源，称为节点。节点有一个基于 Red Hat Enterprise Linux (RHEL) 的轻量级、安全的操作系统，称为 Red Hat Enterprise Linux CoreOS (RHCOS)。

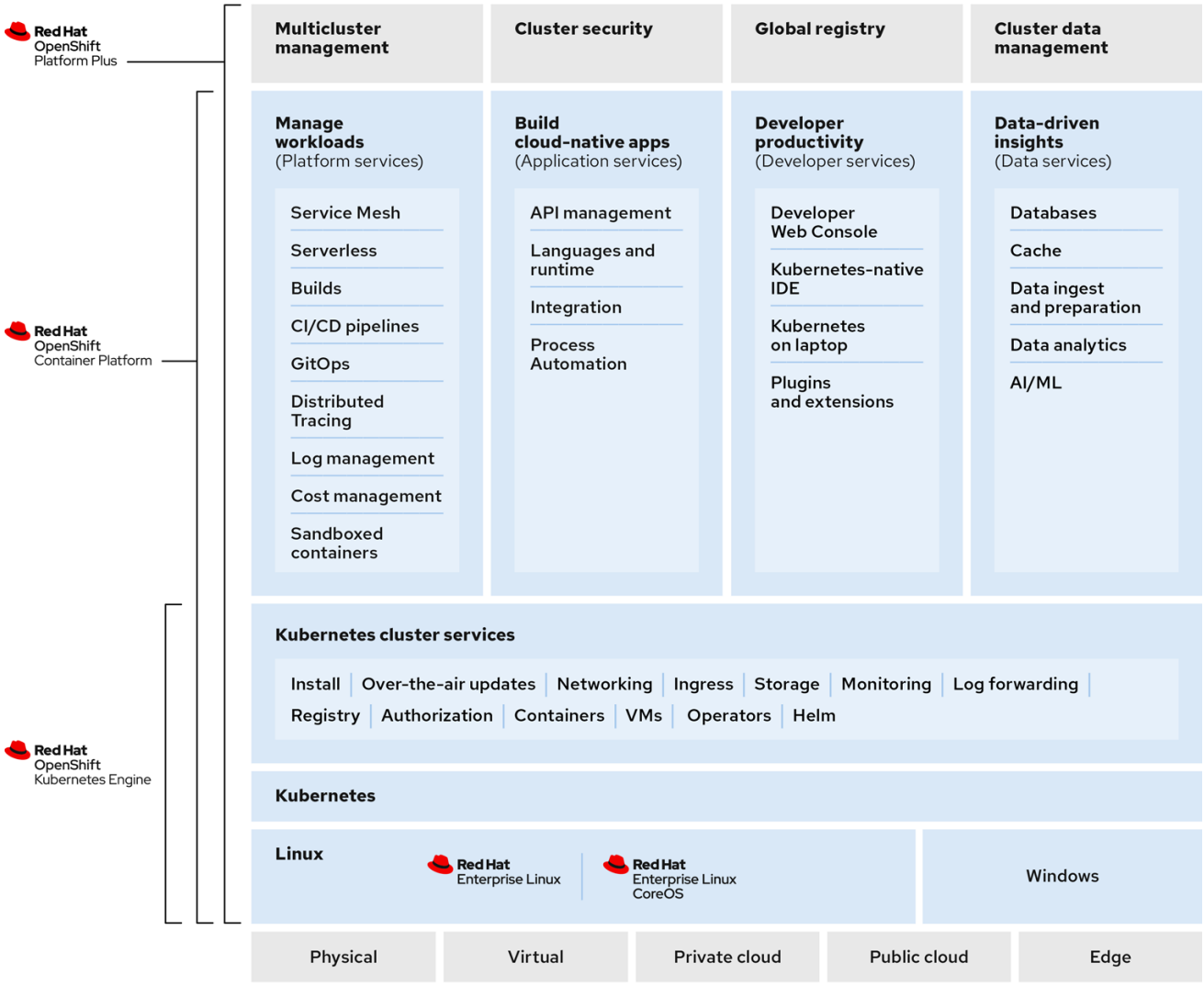
引导并配置节点后，它会获取容器运行时，如 CRI-O 或 Docker，用于管理和运行调度到其中的容器工作负载的镜像。Kubernetes 代理或 kubelet 会在节点上调度容器工作负载。kubelet 负责将节点注册到集群并接收容器工作负载的详情。

OpenShift Container Platform 配置并管理集群的网络、负载均衡和路由。OpenShift Container Platform 添加了集群服务来监控集群健康和性能、日志记录和管理升级。

容器镜像 registry 和 OperatorHub 提供红帽认证的产品和社区构建的软件，用于在集群中提供各种应用程序服务。这些应用程序和服务管理集群中部署的应用程序、数据库、前端和用户界面、应用程序运行时和业务自动化，以及用于开发和测试容器应用的开发人员服务。

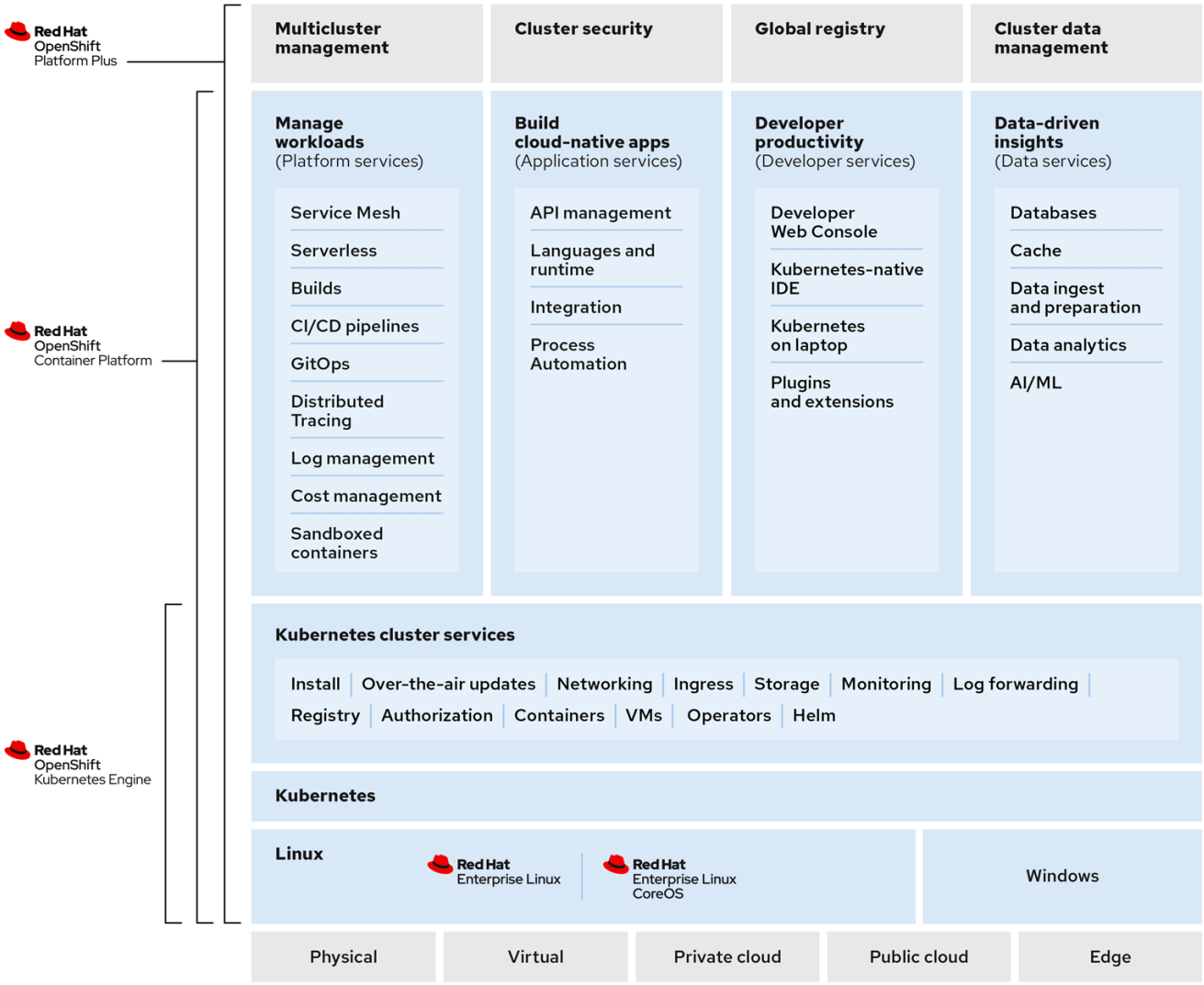
您可以通过配置从预构建镜像运行的容器部署或通过称为 Operator 的资源来手动管理集群中的应用程序。您可以通过预先构建的镜像和源代码构建自定义镜像，并将这些自定义镜像存储在本地内部、私有或公共 registry 中。

多集群管理层可以使用一个控制台管理多个集群，包括它们的部署、配置、合规性和工作负载分布。



第 3 章 关于 OPENSHIFT KUBERNETES ENGINE

从 2020 年 4 月 27 日，红帽决定将 Red Hat OpenShift Container Engine 重命名为 Red Hat OpenShift Kubernetes Engine，以更好地反映产品所提供的值。



Red Hat OpenShift Kubernetes Engine 是红帽的一个产品，可让您使用企业级 Kubernetes 平台作为启动容器的生产环境平台。下载和安装 OpenShift Container Platform 的方式与 OpenShift Container Platform 相同，但 OpenShift Kubernetes Engine 只提供了 OpenShift Container Platform 所提供的功能的一个子集。

3.1. 相同和不同的地方

您可以在下表中看到 OpenShift Kubernetes Engine 和 OpenShift Container Platform 之间的相似性和不同之处：

表 3.1. OpenShift Kubernetes Engine 和 OpenShift Container Platform 的产品比较

	OpenShift Kubernetes Engine	OpenShift Container Platform
完全自动化安装程序	是	是

	OpenShift Kubernetes Engine	OpenShift Container Platform
无线智能升级	是	是
企业集安全 Kubernetes	是	是
kubectl 和 oc 自动命令行	是	是
Operator Lifecycle Manager (OLM)	是	是
管理员 Web 控制台	是	是
OpenShift Virtualization	是	是
用户工作负载监控		是
Metering 和成本管理 SaaS 服务		是
平台日志记录		是
开发人员 Web 控制台		是
开发人员应用程序目录		是
Source to Image 和 Builder Automation (Tekton)		是
OpenShift Service Mesh（Maistra、Kiali 和 Jaeger）		是
OpenShift distributed tracing(Jaeger)		是
OpenShift Serverless (Knative)		是
OpenShift Pipelines (Jenkins 和 Tekton)		是
IBM Cloud Pak 和 RHT MW Bundles 的嵌入式组件		是

3.1.1. 核心 Kubernetes 和容器编配

OpenShift Kubernetes Engine 提供了对一个企业级 Kubernetes 环境的完整访问权限，该环境易于安装，并提供了您的数据中心中可能使用的许多软件元素的广泛兼容性测试。

OpenShift Kubernetes Engine 提供与 OpenShift Container Platform 相同的服务级别协议、错误修复和常见漏洞和错误保护。OpenShift Kubernetes Engine 包括了一个 Red Hat Enterprise Linux (RHEL) Virtual Datacenter 和 Red Hat Enterprise Linux CoreOS (RHCOS) 权利，可让您使用集成的 Linux 操作系统与来自相同技术供应商的容器运行时。

OpenShift Kubernetes Engine 订阅与 Red Hat OpenShift support for Windows Containers 订阅兼容。

3.1.2. 企业级就绪配置

OpenShift Kubernetes Engine 使用与 OpenShift Container Platform 相同的安全选项和默认设置。默认安全性上下文约束、Pod 安全策略、最佳实践网络和存储设置、服务帐户配置、SELinux 集成、HAproxy 边缘路由配置以及 OpenShift Container Platform 提供的所有其他标准保护。OpenShift Kubernetes Engine 提供对 OpenShift Container Platform 使用的集成监控解决方案的完整访问权限，该解决方案基于 Prometheus，并为常见 Kubernetes 问题提供深入的覆盖范围和警报。

OpenShift Kubernetes Engine 使用与 OpenShift Container Platform 相同的安装和升级自动化。

3.1.3. 标准基础架构服务

通过 OpenShift Kubernetes Engine 订阅，您可以获得 OpenShift Container Platform 支持的所有存储插件支持。

在网络方面，OpenShift Kubernetes Engine 完全支持对 Kubernetes Container Network Interface (CNI) 的访问，因此您可以使用任何支持 OpenShift Container Platform 的第三方 SDN。它还允许您使用提供的 Open vSwitch 软件定义网络来进行完整扩展。OpenShift Kubernetes Engine 允许您充分利用在 OpenShift Container Platform 中支持的 OVN Kubernetes overlay、Musus 和 Multus 插件。OpenShift Kubernetes Engine 允许用户使用 Kubernetes 网络策略在集群上部署的应用程序服务之间创建微分段。

您还可以使用 OpenShift Container Platform 中发现的 **Route** API 对象，包括其与 HAproxy 边缘路由层集成在一起的 Kubernetes Ingress Controller。

3.1.4. 核心用户体验

OpenShift Kubernetes Engine 用户对 Kubernetes Operator、pod 部署策略、Helm 和 OpenShift Container Platform 模板具有完全访问权限。OpenShift Kubernetes Engine 用户可以使用 **oc** 和 **kubectl** 命令行界面。OpenShift Kubernetes Engine 还提供基于 Web 的管理员控制台，它显示了部署容器服务的所有方面并提供容器即服务体验。OpenShift Kubernetes Engine 授予对 Operator 生命周期管理器的访问权限，以帮助您控制您使用的集群和支持生命周期的服务中的内容。使用 OpenShift Kubernetes Engine 订阅，您可以访问 Kubernetes 命名空间、OpenShift **Project** API 对象和集群级 Prometheus 监控指标和事件的访问权限。

3.1.5. 维护和策展的内容

使用 OpenShift Kubernetes Engine 订阅，您可从红帽生态系统目录和红帽 Connect ISV 市场访问 OpenShift Container Platform 内容。您可以访问 OpenShift Container Platform 生态环境所提供的所有维护和策展的内容。

3.1.6. 兼容 OpenShift Container Storage

OpenShift Kubernetes Engine 与 OpenShift Container Storage 兼容并提供支持。

3.1.7. Red Hat Middleware 兼容

OpenShift Kubernetes Engine 与独立的 Red Hat Middleware 产品解决方案兼容并提供支持。包括 OpenShift 的 Red Hat Middleware Bundles 仅包含 OpenShift Container Platform。

3.1.8. OpenShift Serverless

OpenShift Kubernetes Engine 不包括对 OpenShift Serverless 的支持。使用 OpenShift Container Platform 用于这个支持。

3.1.9. Quay 集成兼容

OpenShift Kubernetes Engine 兼容并支持 Red Hat Quay。

3.1.10. OpenShift Virtualization

OpenShift Kubernetes Engine 包括对来自 kubevirt.io 开源项目提供的红帽产品产品支持。

3.1.11. 高级集群管理

OpenShift Kubernetes Engine 与额外购买的 Red Hat Advanced Cluster Management (RHACM) 兼容。OpenShift Kubernetes Engine 订阅不提供集群范围的日志聚合解决方案，或支持 Elasticsearch、Fluentd 或基于 Kibana 的日志记录解决方案。同样，OpenShift Container Platform 或 console.redhat.com Cost Management SaaS 服务中的计费功能也不支持 OpenShift Kubernetes Engine。OpenShift Kubernetes Engine 不支持来自开源 istio.io 和 kiali.io 项目的 Red Hat Service Mesh 功能，为 OpenShift Container Platform 上的容器化服务提供 OpenTracing 可观察性。

3.1.12. 高级网络

OpenShift Container Platform 中的标准网络解决方案支持 OpenShift Kubernetes Engine 订阅。OpenShift Container Platform 的 Kubernetes CNI 插件可用于自动化 OpenShift Container Platform 项目之间的多租户网络分段。OpenShift Kubernetes Engine 提供对集群中应用程序服务使用的源 IP 地址的所有细粒度控制。这些出口 IP 地址控制可以与 OpenShift Kubernetes Engine 搭配使用。当没有通过 OpenShift Container Platform 中的 VIP pod 使用的公共云供应商时，OpenShift Container Platform 在集群服务上提供入口路由。OpenShift Kubernetes Engine 支持该入口解决方案。OpenShift Kubernetes Engine 用户支持 Kubernetes ingress 控制对象，它提供与公共云提供商的集成。OpenShift Kubernetes Engine 不支持来自 istio.io 开源项目的 Red Hat Service Mesh。另外，OpenShift Kubernetes Engine 不支持 OpenShift Serverless 中找到的 Kourier Ingress Controller。

3.1.13. 开发者体验

在 OpenShift Kubernetes Engine 中，不支持以下功能：

- CodeReady 开发人员体验工具，如 CodeReady Workspaces。
- OpenShift Container Platform 的管道功能将启用 Kubernetes 的简化 Jenkins 和 Tekton 体验整合到用户的项目空间中。
- OpenShift Container Platform 的 source-to-image 功能，可让您在集群中轻松部署源代码、dockerfiles 或容器镜像。
- 用于最终用户容器部署的构建策略、构建器 Pod 或 Tekton。
- **odo** developer 命令行。
- OpenShift Container Platform Web 控制台中的开发人员用户角色。

3.1.14. 功能概述

下表是 OpenShift Kubernetes Engine 和 OpenShift Container Platform 中功能可用性的摘要。如果适用，它包括启用功能的 Operator 名称。

表 3.2. OpenShift Kubernetes Engine 和 OpenShift Container Platform 中的功能

功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
完全自动化安装程序 (IPI)	包括	包括	N/A
可自定义的安装程序 (UPI)	包括	包括	N/A
断开连接的安装	包括	包括	N/A
Red Hat Enterprise Linux (RHEL) 或 Red Hat Enterprise Linux CoreOS (RHCOS) 权利	包括	包括	N/A
将现有 RHEL 手动附加到集群 (BYO)	包括	包括	N/A
CRIO 运行时	包括	包括	N/A
无线智能升级和 Operating System (RHCOS) 管理	包括	包括	N/A
企业集安全 Kubernetes	包括	包括	N/A
kubectl 和 oc 自动命令行	包括	包括	N/A
Auth Integrations, RBAC, SCC, Multi-Tenancy Admission 控制器	包括	包括	N/A
Operator Lifecycle Manager (OLM)	包括	包括	N/A
管理员 Web 控制台	包括	包括	N/A
OpenShift Virtualization	包括	包括	OpenShift Virtualization Operator
红帽提供的 Compliance Operator	包括	包括	Compliance Operator
File Integrity Operator	包括	包括	File Integrity Operator

功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
Gatekeeper Operator	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Gatekeeper Operator
Klusterlet	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	N/A
由红帽提供的 kube Descheduler Operator	包括	包括	kube Descheduler Operator
由红帽提供的本地存储	包括	包括	Local Storage Operator
红帽提供的节点功能发现	包括	包括	Node Feature Discovery Operator
Performance Add-on Operator	包括	包括	Performance Add-on Operator
红帽提供的 PTP Operator	包括	包括	PTP Operator
红帽提供的 Service Telemetry Operator	包括	包括	Service Telemetry Operator
Cluster Network Operator	包括	包括	Cluster Network Operator
Vertical Pod Autoscaler	包括	包括	Vertical Pod Autoscaler
集群监控 (Prometheus)	包括	包括	集群监控
设备管理器（例如 GPU）	包括	包括	N/A
日志转发（使用 fluentd）	包括	包括	Red Hat OpenShift Logging Operator（用于带有 fluentd 的日志转发）
Telemeter 和 Insights 连接体验	包括	包括	N/A
功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
OpenShift Cloud Manager SaaS Service	包括	包括	N/A
OVS 和 OVN SDN	包括	包括	N/A

功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
MetalLB	包括	包括	MetalLB Operator
HAProxy Ingress Controller	包括	包括	N/A
Red Hat OpenStack Platform (RHOSP) Kuryr 集成	包括	包括	N/A
Ingress 集群范围的防火墙	包括	包括	N/A
Egress Pod 和命名空间颗粒控制	包括	包括	N/A
Ingress 非标准端口	包括	包括	N/A
Multus 和 Available Multus 插件	包括	包括	N/A
网络策略	包括	包括	N/A
IPv6 单栈和双栈	包括	包括	N/A
CNI 插件 ISV 兼容性	包括	包括	N/A
CSI 插件 ISV 兼容性	包括	包括	N/A
按需购买 RHT 和 IBM 中间件（没有包括在 OpenShift Container Platform 或 OpenShift Kubernetes Engine 中）	包括	包括	N/A
ISV 或合作伙伴的 Operator 和容器兼容性（没有包括在 OpenShift Container Platform 或 OpenShift Kubernetes Engine 中）	包括	包括	N/A
嵌入式 OperatorHub	包括	包括	N/A
嵌入式市场	包括	包括	N/A

功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
Quay 兼容性（不包含）	包括	包括	N/A
RHEL Software Collections 和 RHT SSO Common Service（包括）	包括	包括	N/A
嵌入式 Registry	包括	包括	N/A
Helm	包括	包括	N/A
用户工作负载监控	未包含	包括	N/A
Metering 和成本管理 SaaS 服务	未包含	包括	N/A
平台日志记录	未包含	包括	Red Hat OpenShift Logging Operator
红帽提供的 OpenShift Elasticsearch Operator	未包含	无法独立运行	N/A
开发人员 Web 控制台	未包含	包括	N/A
开发人员应用程序目录	未包含	包括	N/A
Source to Image 和 Builder Automation (Tekton)	未包含	包括	N/A
OpenShift Service Mesh	未包含	包括	OpenShift Service Mesh Operator
Service Binding Operator	未包含	包括	Service Binding Operator
功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
Red Hat OpenShift Serverless	未包含	包括	OpenShift Serverless Operator
红帽提供的 Web 终端	未包含	包括	Web Terminal Operator
红帽提供的 Jenkins Operator	未包含	包括	Jenkins Operator

功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
Red Hat OpenShift Pipelines Operator	未包含	包括	OpenShift Pipelines Operator
IBM Cloud Pak 和 RHT MW Bundles 的嵌入式组件	未包含	包括	N/A
Red Hat OpenShift GitOps	未包含	包括	OpenShift GitOps
Red Hat CodeReady Workspaces	未包含	包括	CodeReady Workspaces
Red Hat CodeReady Containers	未包含	包括	N/A
红帽提供的 Quay Bridge Operator	未包含	包括	Quay Bridge Operator
红帽提供的 Quay Container Security	未包含	包括	Quay Operator
Red Hat OpenShift distributed tracing Platform	未包含	包括	Red Hat OpenShift 分布式跟踪平台 Operator
Red Hat OpenShift Kiali	未包含	包括	Kiali Operator
由红帽提供的 metering（已弃用）	未包含	包括	N/A
Containers Operator 的 Migration Toolkit	未包含	包括	Containers Operator 的 Migration Toolkit
OpenShift 的成本管理	不包括	包括	N/A
Red Hat JBoss Web Server	不包括	包括	JWS Operator
红帽构建的 Quarkus	不包括	包括	N/A
Kourier Ingress 控制器	不包括	包括	N/A

功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
RHT Middleware Bundles Sub 兼容性（不包括在 OpenShift Container Platform 中）	不包括	包括	N/A
IBM Cloud Pak Sub 兼容性（不包括在 OpenShift Container Platform 中）	不包括	包括	N/A
OpenShift Do (odo)	不包括	包括	N/A
Source to Image 和 Tekton Builders	不包括	包括	N/A
OpenShift Serverless FaaS	不包括	包括	N/A
IDE 集成	不包括	包括	不适用
Windows Machine Config Operator	包括的社区 Windows Machine Config Operator - 不需要订阅	包括的 Red Hat Windows Machine Config Operator - 需要单独的订阅	Windows Machine Config Operator
Red Hat Quay	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Quay Operator
Red Hat Advanced Cluster Management	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Advanced Cluster Management for Kubernetes
Red Hat Advanced Cluster Security	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	不适用
OpenShift Container Storage	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	OpenShift Container Storage
功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
Ansible Automation Platform Resource Operator	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Ansible Automation Platform Resource Operator
红帽提供的业务自动化	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Network Automation Operator

功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
由红帽提供的数据网格	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Data Grid Operator
由红帽提供的 Red Hat Integration	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Red Hat Integration Operator
Red Hat Integration - 由红帽提供的 3Scale	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	3scale
Red Hat Integration - 由红帽提供的 3Scale APICast 网关	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	3scale APIcast
Red Hat Integration - AMQ Broker	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	AMQ Broker
Red Hat Integration - AMQ Broker LTS	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	
Red Hat Integration - AMQ Interconnect	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	AMQ Interconnect
Red Hat Integration - AMQ Online	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	
Red Hat Integration - AMQ Streams	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	AMQ Streams
Red Hat Integration - Camel K	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Camel K
Red Hat Integration - Fuse Console	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Fuse 控制台
Red Hat Integration - Fuse Online	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Fuse Online
Red Hat Integration - Service Registry Operator	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Service Registry
红帽提供的 API Designer	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	API Designer
红帽提供的 JBoss EAP	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	JBoss EAP

功能	OpenShift Kubernetes Engine	OpenShift Container Platform	Operator 名称
红帽提供的 JBoss Web Server	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	JBoss Web Server
Smart Gateway Operator	未包括 - 需要单独的订阅	未包括 - 需要单独的订阅	Smart Gateway Operator
Kubernetes NMState Operator	包括	包括	N/A

3.2. 订阅限制

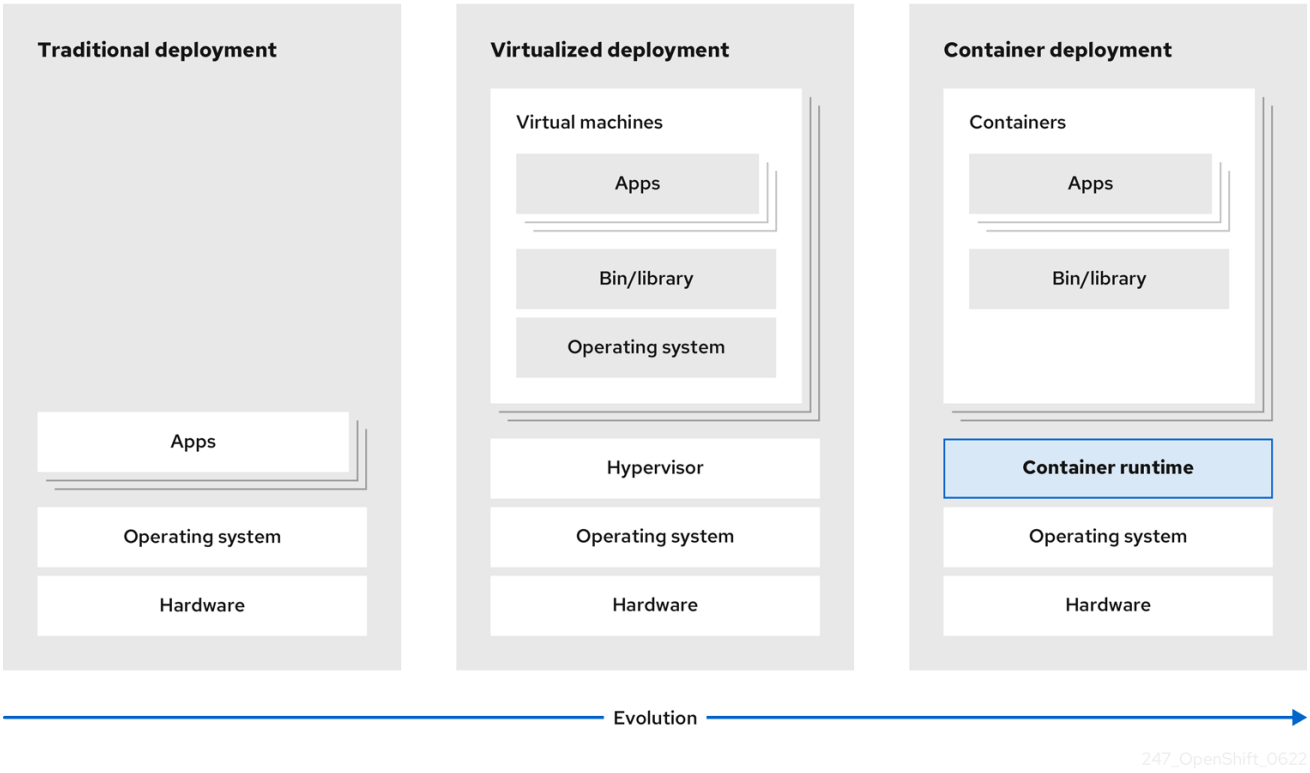
OpenShift Kubernetes Engine 是一个订阅产品，它提供了 OpenShift Container Platform 中的一组有限的功能，其价格较低。OpenShift Kubernetes Engine 和 OpenShift Container Platform 是相同的产品，所有软件和功能都会在这两个服务中提供。因此，它们使用同一个下载 - OpenShift Container Platform。OpenShift Kubernetes Engine 使用 OpenShift Container Platform 文档并支持服务和程序错误修复。

第 4 章 KUBERNETES 概述

Kubernetes 是由 Google 开发的开源容器编排工具。您可以使用 Kubernetes 运行和管理基于容器的工作负载。最常见的 Kubernetes 用例是部署一系列互联微服务，以云原生方式构建应用。您可以创建 Kubernetes 集群，跨越内部部署、公共云、私有云或混合云中的主机。

传统上，应用程序部署在单一操作系统之上。通过虚拟化，您可以将物理主机分成几个虚拟主机。在共享资源中使用虚拟实例并非是实现运行效率和可扩展性的最佳选择。因为虚拟机 (VM) 和物理主机一样会消耗尽可能多的资源，因此为虚拟机提供资源（如 CPU、RAM 和存储）的成本会比较高。另外，您可能会看到，因为使用共享资源，导致虚拟实例中运行的应用程序的性能下降。

图 4.1. 用于类部署的容器技术的演进



要解决这个问题，您可以使用容器化技术，在一个容器化环境中隔离应用程序。与虚拟机类似，容器具有自己的文件系统、vCPU、内存、进程空间、依赖项等。容器与底层基础架构分离，可跨云和操作系统分布移植。与一个功能齐全的操作系统相比，容器是一个更加轻量的系统，它会在操作系统上隔离进程。虚拟机的启动速度较慢，它是物理硬件的抽象概念。虚拟机在一台机器上运行，由一个虚拟机监控程序（hypervisor）处理。

您可以使用 Kubernetes 执行以下操作：

- 共享资源
- 在多个主机间编排容器
- 安装新的硬件配置
- 运行健康检查和自我修复应用程序
- 扩展容器化应用程序

4.1. KUBERNETES 组件

表 4.1. Kubernetes 组件

组件	目的
kube-proxy	在集群的每个节点上运行，并维护 Kubernetes 资源之间的网络流量。
kube-controller-manager	监管集群的状态。
kube-scheduler	将 pod 分配给节点。
etcd	存储集群数据。
kube-apiserver	验证并配置 API 对象的数据。
kubelet	在节点上运行并读取容器清单。确保定义的容器已启动且正在运行。
kubectl	您可以定义如何运行工作负载。使用 **kubectl** 命令与 **kube-apiserver** 进行交互。
节点	节点是 Kubernetes 集群中的物理机器或虚拟机。控制平面（control plane）管理每个节点，并在 Kubernetes 集群中的节点之间调度 pod。
容器运行时	容器运行时在主机操作系统上运行容器。您必须在每个节点上安装容器运行时，以便 pod 能够在该节点上运行。
持久性存储	即便在设备关闭后也存储数据。Kubernetes 使用持久性卷来存储应用程序数据。
container-registry	存储和访问容器镜像。
Pod	pod 是 Kubernetes 中的最小逻辑单元。pod 包含一个或多个在 worker 节点上运行的容器。

4.2. KUBERNETES 资源

自定义资源是 Kubernetes API 的扩展。您可以使用自定义资源自定义 Kubernetes 集群。Operator 是一个软件扩展，它通过自定义资源来管理应用程序及其组件。当您希望在处理集群资源时具有固定的结果，则 Kubernetes 会使用声明性模型。通过使用 Operator，Kubernetes 以声明性方式定义其状态。您可以使用必需命令修改 Kubernetes 集群资源。Operator 充当控制循环，它可以持续将所需的资源状态与资源的实际状态进行比较，并将操作与所需的状态保持一致。

图 4.2. Kubernetes 集群概述

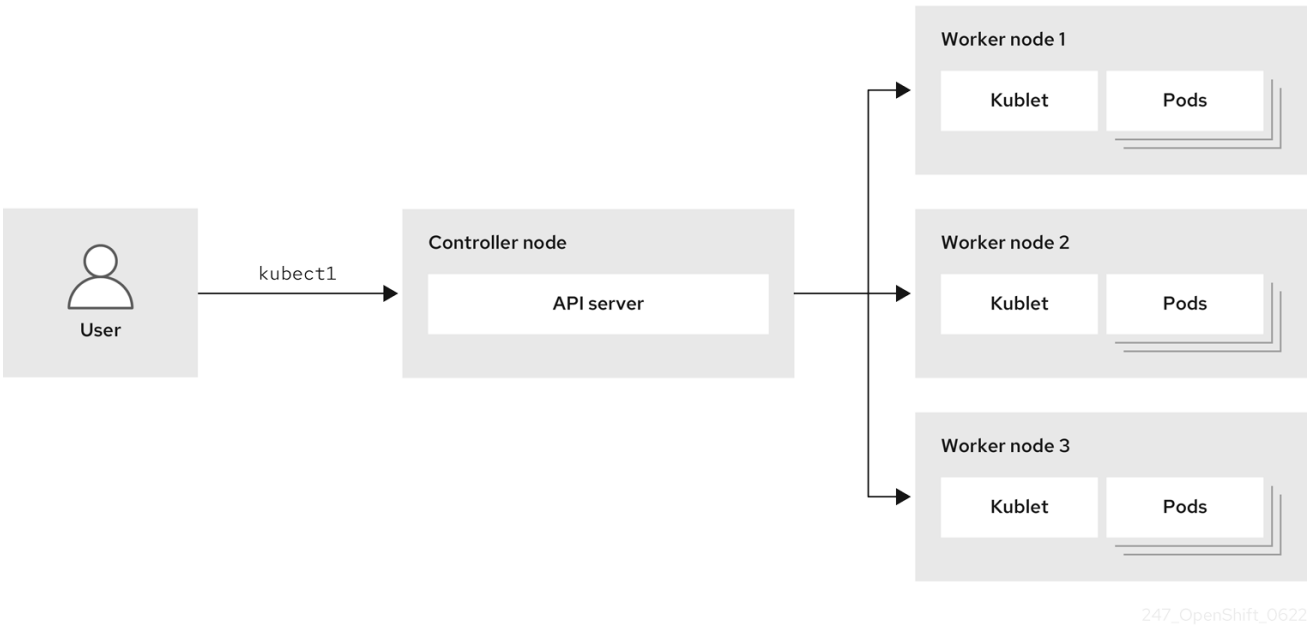
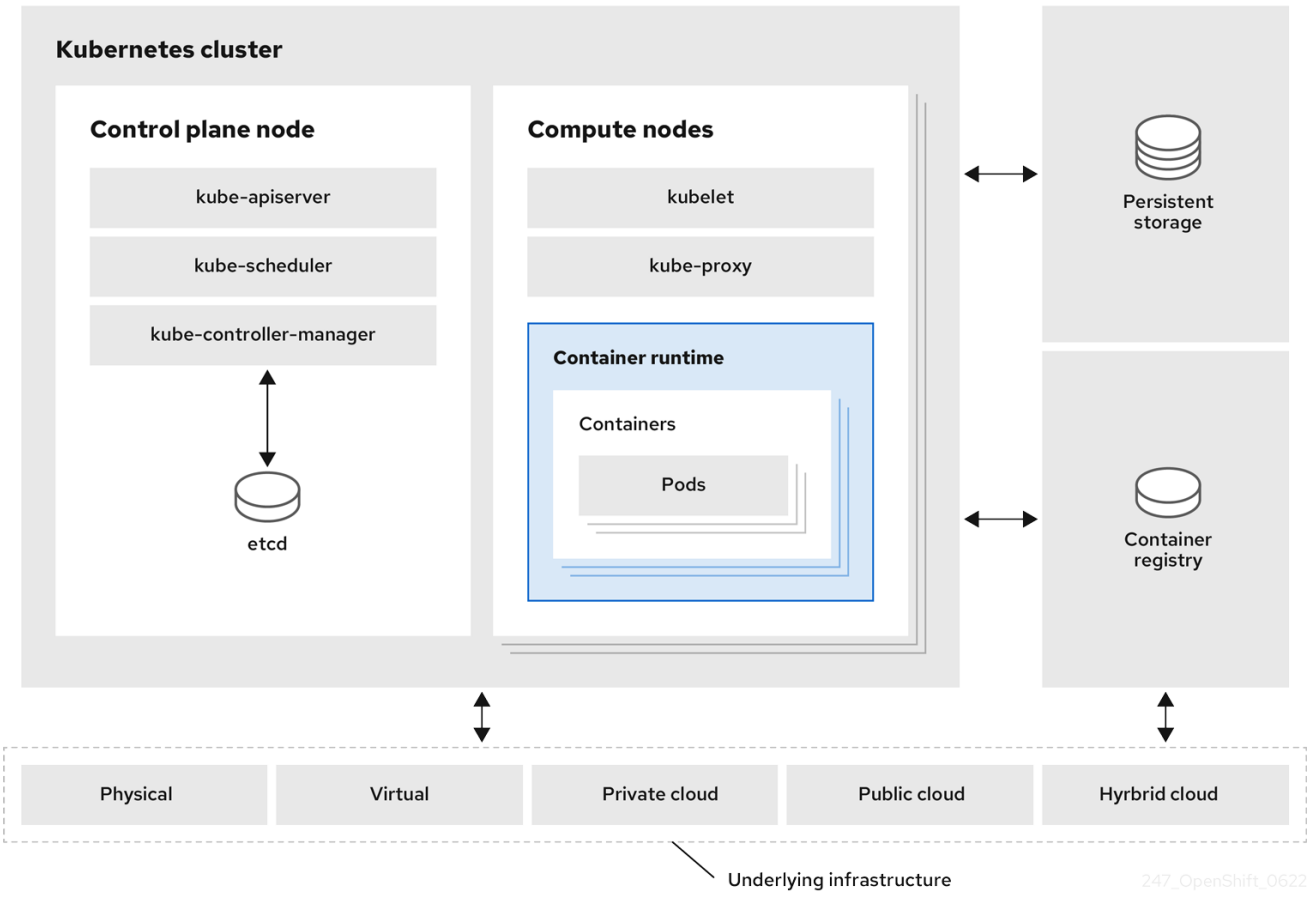


表 4.2. Kubernetes 资源

资源	目的
服务	Kubernetes 使用服务在一组 pod 上公开正在运行的应用程序。
ReplicaSet	Kubernetes 使用 **ReplicaSet** 来维护恒定的 pod 号。
Deployment	维护应用程序生命周期的资源对象。

Kubernetes 是 OpenShift Container Platform 的核心组件。您可以使用 OpenShift Container Platform 开发和运行容器化应用程序。OpenShift Container Platform 以 Kubernetes 为基础，为大规模电信、流视频、游戏、银行和其他应用提供引擎技术。您可以使用 OpenShift Container Platform 将容器化应用程序扩展至内部和多云环境中的容器化应用程序。

图 4.3. Kubernetes 构架



集群是一个计算单元，由云环境中的多个节点组成。Kubernetes 集群包含一个 control plane 和 worker 节点。您可以在各种机器和环境中运行 Kubernetes 容器。control plane 节点控制和维护集群的状态。您可以使用 worker 节点运行 Kubernetes 应用程序。您可以使用 Kubernetes 命名空间来区分集群中的集群资源。命名空间范围适用于资源对象，如部署、服务和 pod。您不能将命名空间用于集群范围的资源对象，如存储类、节点和持久性卷。

4.3. KUBERNETES 概念指南

在 OpenShift Container Platform 入门前，请考虑以下 Kubernetes 概念指南：

- 从一个或多个 worker 节点开始，以运行容器工作负载。
- 从一个或多个 control plane 节点管理这些工作负载的部署。
- 将容器嵌套到名为 pod 的部署单元中。使用 pod 可以为容器提供额外的元数据，并可在单个部署实体中对多个容器进行分组。
- 创建特殊种类的资产。例如，服务由一组 pod 及定义了访问方式的策略来表示。此策略可使容器连接到所需的服务，即便容器没有用于服务的特定 IP 地址。复制控制器（replication controller）是另一种特殊资产，用于指示一次需要运行多少个 pod 副本。您可以使用此功能来自动扩展应用程序，以适应其当前的需求。

OpenShift Container Platform 集群的 API 是 100% Kubernetes。在任何 Kubernetes 上运行的容器之间没有变化，并在 OpenShift Container Platform 上运行。没有对应用的更改。OpenShift Container Platform 提供附加值功能，为 Kubernetes 提供企业级的增强。OpenShift Container Platform CLI 工具 (**oc**)与 **kubectl** 兼容。虽然 Kubernetes API 100% 可在 OpenShift Container Platform 中使用，但 **kubectl** 命令行缺少了很多用户友好的功能。OpenShift Container Platform 提供了一组功能和命令行工

具，如 **oc**。虽然 Kubernetes 擅长管理应用程序，但它并未指定或管理平台级要求或部署过程。强大而灵活的平台管理工具和流程是 OpenShift Container Platform 具备的重要优势。您必须将身份验证、网络、安全、监控和日志管理添加到容器化平台中。