OpenShift Container Platform 4.16

发行注记

OpenShift Container Platform 发行版本中的主要新功能及变化信息

Last Updated: 2024-07-03

OpenShift Container Platform 4.16 发行注记

OpenShift Container Platform 发行版本中的主要新功能及变化信息

法律通告

摘要

此发行注记介绍了 OpenShift Container Platform 的新功能、功能增强、重要的技术变化、以及对以前版本中的错误作出的主要修正。另外，还包括在此版本正式发行（GA）时存在的已知问题的信息。

目录

第 1 章 OPENSHIFT CONTAINER PLATFORM 4.16 发行注记

Red Hat OpenShift Container Platform 为开发人员和 IT 组织提供了一个混合云应用平台，以便以最少的配置和管理功能在安全、可扩展的资源上部署新的和现有应用程序。OpenShift Container Platform 支持大量编程语言和开发平台，如 Java、JavaScript、Python、Ruby 和 PHP。

OpenShift Container Platform 基于 Red Hat Enterprise Linux（RHEL）和 Kubernetes，为当今的企业级应用程序提供了一个更加安全、可扩展的多租户操作系统，同时提供了集成的应用程序运行时及程序库。OpenShift Container Platform 可以满足用户对安全性、隐私、合规性及监管的要求。

1.1. 关于此版本

OpenShift Container Platform (RHSA-2024:0041)现已正式发布。此发行版本使用 Kubernetes 1.29 和 CRI-O 运行时。OpenShift Container Platform 4.16 的新功能、改变以及已知的问题包括在此文档中。

OpenShift Container Platform 4.16 集群位于 https://console.redhat.com/openshift。使用 OpenShift Container Platform 的 Red Hat OpenShift Cluster Manager 应用程序，您可以将 OpenShift Container Platform 集群部署到内部环境或云环境中。

OpenShift Container Platform 4.16 在 Red Hat Enterprise Linux (RHEL) 8.8-8.10 和 Red Hat Enterprise Linux CoreOS 9.4 上被支持。

您必须将 RHCOS 机器用于 control plane，而 compute 系统可以使用 RHCOS 或 RHEL。RHEL 机器在 OpenShift Container Platform 4.16 中已弃用，并将在以后的发行版本中删除。

从 OpenShift Container Platform 4.14 开始，偶数版本延长的更新支持(EUS)阶段将所有支持的构架中的可用生命周期增加到 24 个月，包括 **x86_64**、64 位 ARM (**aarch64**)、IBM Power®(**ppc64le**)和 IBM Z®(**s390x**)架构。除此之外，红帽还提供 12 个月额外的 EUS 附加组件，以额外的 *EUS Term 2* 表示，将总可用生命周期从 24 个月延长至 36 个月。在 OpenShift Container Platform 的所有架构变体中提供了 Additional EUS Term 2。

有关所有版本支持的更多信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

从 4.16 版本开始，红帽简化了红帽所提供的集群 Operator 的管理和管理，它介绍了三个新的生命周期分类：平台 Aligned、平台 Agnostic 和 Rolling Stream。这些生命周期类别为集群管理员提供了额外的简易性和透明度，以更好地了解每个 Operator 的生命周期策略，并以可预测的支持界限来计划对集群进行维护和升级。如需更多信息，请参阅 OpenShift Operator 生命周期。

OpenShift Container Platform 专为 FIPS 设计。当以 FIPS 模式运行 Red Hat Enterprise Linux (RHEL) 或 Red Hat Enterprise Linux CoreOS (RHCOS)时，OpenShift Container Platform 核心组件使用 RHEL 加密库，在 **x86_64**、**ppc64le**、**s390x** 架构上提交给 NIST 的 FIPS 140-2/140-3 Validation。

有关 NIST 验证程序的更多信息，请参阅加密模块验证程序。有关为验证提交的 RHEL 加密库的单独版本的最新 NIST 状态，请参阅 Compliance Activities 和 Government Standards。

1.2. OPENSHIFT CONTAINER PLATFORM 层次和依赖组件支持和兼容性

OpenShift Container Platform 的层次组件和依赖组件的支持范围会独立于 OpenShift Container Platform 版本。要确定附加组件的当前支持状态和兼容性，请参阅其发行注记。如需更新相关信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

1.3. 新功能及功能增强

此版本对以下方面进行了改进。

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. RHCOS 现在使用 RHEL 9.4

RHCOS 现在使用 OpenShift Container Platform 4.16 中的 Red Hat Enterprise Linux (RHEL) 9.4 软件包。这些软件包可确保 OpenShift Container Platform 实例收到最新的修复、功能、增强功能、硬件支持和驱动程序更新。作为延长更新支持(EUS)版本，OpenShift Container Platform 4.14 不包括在这个更改中，并将继续在整个生命周期中使用 RHEL 9.2 EUS 软件包。

1.3.1.2. 支持 iSCSI 引导卷

在这个版本中，您可以将 RHCOS 安装到小型计算机系统接口(iSCSI)引导设备。还支持 iSCSI 多路径。如需更多信息，请参阅在 iSCSI 引导设备上手动安装 RHCOS，以及使用 iBFT 在 iSCSI 引导设备上安装 RHCOS

1.3.1.3. 支持使用 CPU 上 Intel® 虚拟 RAID 的 RAID 存储(VROC)

在这个版本中，您可以将 RHCOS 安装到 Intel® VROC RAID 设备。有关将 RAID 配置为 Intel® VROC 设备的更多信息，请参阅在 CPU (VROC)数据卷中配置 Intel® 虚拟 RAID 。

1.3.2. 安装和更新

1.3.2.1. 集群 API 替换 AWS 安装的 Terraform

在 OpenShift Container Platform 4.16 中，安装程序使用 Cluster API 而不是 Terraform 在 Amazon Web Services 上安装时置备集群基础架构。由于这个变化，还有一些额外的权限。如需更多信息，请参阅 IAM 用户所需的 AWS 权限。

另外，对 control plane 和计算机器的 SSH 访问不再对机器网络开放，但仅限于与 control plane 和计算机器关联的安全组。

警告

使用 Cluster API 实现在 Amazon Web Services (AWS)上安装集群到 secret 或 top-secret 区域，还没有在 OpenShift Container Platform 4.16 版本中被测试。当测试到 secret 区域时，会更新本文档。Network Load Balancer 对 secret 或顶级 secret 区域中的安全组的支持存在一个已知问题，这会导致安装失败。如需更多信息，请参阅 **OCPBUGS-33311**。

1.3.2.2. 集群 API 替换 VMware vSphere 安装的 Terraform

在 OpenShift Container Platform 4.16 中，安装程序使用 Cluster API 而不是 Terraform 在 VMware vSphere 上安装时置备集群基础架构。

1.3.2.3. 集群 API 替换 Nutanix 安装的 Terraform

在 OpenShift Container Platform 4.16 中，安装程序使用 Cluster API 而不是 Terraform 在 Nutanix 上安装置备集群基础架构。

1.3.2.4. Cluster API 替换了 Google Cloud Platform (GCP)安装的 Terraform （技术预览）

在 OpenShift Container Platform 4.16 中，安装程序使用 Cluster API 而不是 Terraform 在 GCP 上安装时置备集群基础架构。此功能在 OpenShift Container Platform 4.16 中作为技术预览提供。要启用技术预览功能，请在安装前在 **install-config.yaml** 文件中设置 **featureSet: TechPreviewNoUpgrade** 参数。另外，在安装前将以下小节添加到 **install-config.yaml** 文件中，以启用 Cluster API 安装，而无需任何其他技术预览功能：

```
featureSet: CustomNoUpgrade
featureGates:
- ClusterAPIInstall=true
```

如需更多信息，请参阅 可选配置参数。

1.3.2.5. Ingress 功能

Ingress 功能现在是可配置的集群功能，对于 Red Hat HyperShift 是可选的。它不是可配置的，始终为独立的 OpenShift Container Platform 启用。

> **警告**
>
> 不要禁用 Ingress 功能。OpenShift Container Platform 集群不会在禁用 Ingress 功能的情况下运行。

1.3.2.6. 使用 Assisted Installer 在 Alibaba Cloud 上安装（技术预览）

在这个版本中，OpenShift Container Platform 安装程序不再支持 Alibaba Cloud 平台上的安装程序置备的安装。您可以使用 Assisted Installer 在 Alibaba Cloud 上安装集群，它目前是一个技术预览功能。如需更多信息，请参阅在 Alibaba 云上安装。

1.3.2.7. 可选的云控制器管理器集群功能

在 OpenShift Container Platform 4.16 中，您可以在安装过程中禁用云控制器管理器功能。如需更多信息，请参阅 云控制器管理器功能。

1.3.2.8. OpenShift Container Platform 4.16 中的 FIPS 安装要求

在这个版本中，如果安装启用了 FIPS 的集群，则必须从配置为以 FIPS 模式运行的 RHEL 9 计算机运行安装程序，且必须使用安装程序支持的 FIPS 版本。如需更多信息，请参阅对 FIPS 加密的支持。

1.3.2.9. VMware vSphere 的可选额外标签

在 OpenShift Container Platform 4.16 中，您可以添加最多 10 个标签来附加到 VMware vSphere 集群置备的虚拟机(VM)。这些标签除了安装程序用来识别和删除集群时的相关虚拟机的唯一标签外。

您可以在 **install-config.yaml** 文件中的 VMware vSphere 虚拟机上定义标签。如需更多信息，请参阅 安装程序置备的 VMware vSphere 集群示例 **install-config.yaml** 文件。

您可以使用机器集为现有集群上的计算或 control plane 机器定义标签。如需更多信息，请参阅"为 compute 或 control plane 机器集使用机器集向机器添加标签"。

1.3.2.10. 从 OpenShift Container Platform 4.15 更新至 4.16 时所需的管理员确认

OpenShift Container Platform 4.16 使用 Kubernetes 1.29，它删除了几个 已弃用的 API。

集群管理员必须在从 OpenShift Container Platform 4.15 升级到 4.16 前提供手动确认。这有助于防止升级到 OpenShift Container Platform 4.16 后出现问题，其中已删除的 API 仍在由运行或与集群交互的工作负载、工具或其他组件使用。管理员必须针对将要删除的任何 API 评估其集群，并迁移受影响的组件，以使用适当的新 API 版本。完成此操作后，管理员可以向管理员提供确认。

所有 OpenShift Container Platform 4.15 集群都需要管理员确认，然后才能将其更新至 OpenShift Container Platform 4.16。

如需更多信息，请参阅 准备升级到 OpenShift Container Platform 4.16。

1.3.2.11. 保护 kubeadmin 密码在控制台中显示

在这个版本中，您可以在集群创建过程中使用- **-skip-password-print** 标志来防止在控制台中显示 **kubeadmin** 密码。密码仍然可在 **auth** 目录中访问。

1.3.2.12. 基于 OpenShift 的设备构建器（技术预览）

在这个版本中，基于 OpenShift 的 设备构建器作为技术预览提供。Appliance Builder 启用自包含的 OpenShift Container Platform 集群安装，这意味着它不依赖于互联网连接或外部 registry。它是一个基于容器的实用程序，用于构建包含基于代理的安装程序的磁盘镜像，然后用于安装多个 OpenShift Container Platform 集群。

如需更多信息，请参阅 基于 OpenShift 的设备构建器用户指南。

1.3.2.13. 为在 AWS 上安装启用自己的 IPv4 (BYOIP)功能

在这个版本中，您可以使用 **publicIpv4Pool** 字段在 Amazon Web Services (AWS)上安装时启用自己的公共 IPv4 地址(BYOIP)功能来分配 Elastic IP 地址(EIPs)。您必须确保具有启用 BYOIP 所需的权限。如需更多信息，请参阅 可选 AWS 配置参数。

1.3.2.14. 在 Dammam (Saudi Arabia)和 Johannesburg (South Africa)区域部署 GCP

您可以在 Dammam、Saudi Arabia (**me-central2**)区域和 Johannesburg, South Africa (**africa-south1**)区域中的 Google Cloud Platform (GCP)上部署 OpenShift Container Platform 4.16。如需更多信息，请参阅支持的 GCP 区域。

1.3.2.15. 在 Google Cloud Platform (GCP)上的 NVIDIA H100 实例类型上安装

在这个版本中，您可以在 GCP 上安装集群时，在启用了 GPU 的 NVIDIA H100 机器上部署计算节点。如需更多信息，请参阅 为 GCP 和 Google 文档测试 实例类型。

1.3.3. 安装后配置

1.3.3.1. 使用 Multiarch Tuning Operator 管理多架构集群中的工作负载（技术预览）

在这个版本中，您可以使用 Multiarch Tuning Operator 在多架构集群中管理工作负载。此 Operator 增强了多架构集群中的操作体验，以及迁移到多架构计算配置的单架构集群。它实施 **ClusterPodPlacementConfig** 自定义资源(CR)以支持架构感知的工作负载调度。

如需更多信息，请参阅使用 Multiarch Tuning Operator 在多架构集群中管理工作负载。

重要

Multiarch Tuning Operator 只是一个技术预览功能。它不支持带有受限网络场景的集群。

1.3.3.2. 支持将 64 位 x86 计算机器添加到具有 64 位 ARM control plane 机器的集群中

此功能支持将 64 位 x86 计算机器添加到具有 64 位 ARM control plane 机器的多架构集群中。在这个版本中，您可以将 64 位 x86 计算机器添加到使用 64 位 ARM control plane 机器的集群，且已经包含 64 位 ARM 计算机器。

1.3.3.3. 支持使用多有效负载安装基于代理的安装程序集群

此功能支持使用 **多** 有效负载安装基于代理的安装程序集群。使用 **多** 有效负载安装基于代理的安装程序集群后，您可以将具有不同架构的计算机器添加到集群中。

1.3.4. Web 控制台

1.3.4.1. 对法语和西班牙语的语言支持

在这个版本中，Web 控制台中支持法语和西班牙语。您可以从 **User Preferences** 页面上的 **Language** 列表更新 web 控制台中的语言。

1.3.4.2. PatternFly 4 现已弃用 4.16

在这个版本中，Web 控制台中弃用了 Patternfly 4 和 React Router 5。所有插件都应尽快迁移到 Patternfly 5 和 React Router 6。

1.3.4.3. Administrator perspective （管理员视角）

此发行版本对 web 控制台的 **Administrator** 视角包括以下更新：

- Google Cloud Platform (GCP)令牌授权、**Auth Token GCP** 和 **Configurable TLS 密码** 过滤器被添加到 OperatorHub 中的 **Infrastructure features** 过滤器中。
- 新的快速启动(I **mpersoning the system:admin 用户**)提供了模拟 **system:admin** 用户的信息。
- pod 的最后一个终止状态现在可以在 **容器列表和容器 详情**页**面中**查**看**。
- 现在，在 **Groups** 和 Group **详情**页**中提供了 Impersonate Group** 操作，而无需搜索适当的 **RoleBinding**。

1.3.4.3.1. OpenShift Container Platform Web 控制台中的节点 CSR 处理

在这个版本中，OpenShift Container Platform Web 控制台支持节点证书签名请求(CSR)。

1.3.4.3.2. 跨存储类克隆和恢复

在这个版本中，您可以在完成克隆或恢复操作时从同一供应商选择一个存储类。这种灵活性允许在具有不同副本数的存储类之间进行无缝转换。例如，从具有 3 个副本的存储类移到 2/1 副本。

1.3.4.4. Developer Perspective (开发者视角)

此发行版本在 web 控制台的 **Developer** 视角包括以下更新：

- 搜索时，会在 Search 页面上的 Resources 列表中添加一个新部分，以显示最近搜索的项目，按搜索的顺序显示。
- 在这个版本中，您可以折叠并展开 Getting started 部分。

1.3.4.4.1. 控制台 Telemetry

在这个版本中，如果也启用了集群遥测，则启用匿名用户分析。这是大多数集群的默认设置，红帽提供了如何使用 Web 控制台的指标。集群管理员可以在每个集群中更新它，并选择选择、选择或禁用前端遥测。

1.3.5. OpenShift CLI (oc)

1.3.5.1. oc-mirror 插件 v2 （技术预览）

OpenShift Container Platform 的 oc-mirror 插件 v2 包括新的特性和功能，改进 Operator 镜像和其他 OpenShift Container Platform 内容的镜像过程。

以下是 oc-mirror 插件 v2 中的主要改进和功能：

- **自动生成 IDMS 和 ITMS 对象** ：
  oc-mirror 插件 v2 每次运行后自动生成 **ImageDigestMirrorSet** (IDMS)和 **ImageTagMirrorSet** (ITMS)对象的完整列表。这些对象替换 oc-mirror 插件 v1 中使用的 **ImageContentSourcePolicy** (ICSP)。此功能增强无需手动合并并清理操作器镜像，并确保包含所有必要的镜像。
- **CatalogSource 对象** ：
  CatalogSource 对象创建，其中插件现在为所有相关目录索引生成 CatalogSource 对象，以便将 oc-mirror 的输出工件应用到断开连接的集群的应用程序。
- **改进了验证** ：
  oc-mirror 插件 v2 验证镜像设置配置中指定的完整镜像集是否已镜像到 registry，无论镜像是否之前被镜像。这样可确保全面可靠的镜像。
- **缓存系统** ：
  新的缓存系统通过仅将新镜像合并到存档中来替换元数据，从而维护最小归档大小。这会优化存储并提高性能。
- **按日期选择** 的镜像：
  用户现在可以根据镜像日期生成镜像存档，允许选择包含新镜像。
- **增强的镜像删除控制** ：
  Delete 功能的引入可替换自动修剪功能，为用户提供对镜像删除更大的控制。
- **支持 registry.conf** ：
  oc-mirror 插件 v2 支持 **registry.conf** 文件，它有助于使用相同的缓存镜像到多个 enclaves。这提高了管理已镜像镜像的灵活性和效率。
- **Operator 版本过滤** ：
  用户可以根据捆绑包名称过滤 Operator 版本，从而更加精确地控制镜像流程中包含的版本。

oc-mirror v1 和 v2 之间的区别

虽然 oc-mirror 插件 v2 提供了很多改进，但 oc-mirror 插件 v1 中的一些功能还没有出现在 oc-mirror 插件 v2 中。

- Helm Charts：oc-mirror 插件 v2 中不存在 Helm chart。

- **ImageSetConfig v1alpha2**: API 版本 **v1alpha2** 不可用，用户必须更新到 **v2alpha1**。
- 存储元数据(**storageConfig**)： oc-mirror 插件 v2 **ImageSetConfiguration** 没有使用存储元数据。
- 自动修剪 ：使用 oc-mirror 插件 v2 中的新的 **Delete** 功能替换。
- 发行签名：发行签名不会在 oc-mirror 插件 v2 中生成。
- 有些命令：oc-mirror 插件 v2 中不提供 **init**、**list** 和 **describe** 命令。

使用 oc-mirror 插件 v2

要使用 oc-mirror 插件 v2，请在 oc-mirror 命令行中添加-- **v2** 标志。

oc-mirror OpenShift CLI (**oc**)插件用于将所有所需的 OpenShift Container Platform 内容和其他镜像(mirror)镜像到您的镜像 registry，简化了断开连接的集群的维护。

1.3.5.2. oc adm upgrade status 命令简介（技术预览）

在以前的版本中，**oc adm upgrade** 命令提供有关集群更新状态的有限信息。此发行版本添加了 **oc adm upgrade status** 命令，该命令与 **oc adm upgrade** 命令分离状态信息，并提供有关集群更新的特定信息，包括 control plane 和 worker 节点更新的状态。

1.3.5.3. 对重复的资源短名称的警告

在这个版本中，如果您使用其短名称查询资源，如果集群中存在多个具有相同短名称的自定义资源定义(CRD)，则 OpenShift CLI (**oc**)会返回警告。

警告示例

```
Warning: short name "ex" could also match lower priority resource examples.test.com
```

1.3.5.4. 删除资源时需要确认的新标志（技术预览）

此发行版本为 **oc delete** 命令引入了一个新的 **--interactive** 标志。当 **--interactive** 标志被设置为 **true** 时，只有在用户确认删除时才会删除该资源。这个标志作为技术预览提供。

1.3.6. IBM Z 和 IBM LinuxONE

在这个版本中，IBM Z® 和 IBM® LinuxONE 与 OpenShift Container Platform 4.16 兼容。您可以使用 z/VM、LPAR 或 Red Hat Enterprise Linux (RHEL) 基于内核的虚拟机 (KVM) 执行安装。有关安装说明，请参阅准备在 IBM Z 和 IBM LinuxONE 上安装 。

重要

Compute 节点必须运行 Red Hat Enterprise Linux CoreOS (RHCOS)。

IBM Z 和 IBM LinuxONE 主要改进
OpenShift Container Platform 4.16 上的 IBM Z® 和 IBM® LinuxONE 版本为 OpenShift Container Platform 组件和概念增加了改进和新功能。

此发行版本引进了对 IBM Z® 和 IBM® LinuxONE 中的以下功能的支持：

- 基于代理的 RHEL KVM 安装程序 ISO 引导
- Ingress Node Firewall Operator
- LPAR 中的多架构计算机器
- z/VM 和 LPAR 的安全引导

1.3.7. IBM Power

IBM Power® 现在与 OpenShift Container Platform 4.16 兼容。有关安装说明，请参阅以下文档：

- 在 IBM Power® 上安装集群。
- 在受限网络中的 IBM Power® 上安装集群

重要

Compute 节点必须运行 Red Hat Enterprise Linux CoreOS (RHCOS)。

IBM Power 主要改进
OpenShift Container Platform 4.16 上的 IBM Power® 发行版本为 OpenShift Container Platform 组件添加了改进和新功能。

此发行版本引进了对 IBM Power® 的以下功能的支持：

- CPU Manager
- Ingress Node Firewall Operator

IBM Power、IBM Z 和 IBM LinuxONE 支持列表
从 OpenShift Container Platform 4.14 开始，延长更新支持 (EUS) 已扩展到 IBM Power® 和 IBM Z® 平台。如需更多信息，请参阅 OpenShift EUS 概述。

表 1.1. OpenShift Container Platform 功能

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
备用身份验证供应商	支持	支持
基于代理的安装程序	支持	支持
支持的安装程序	支持	支持
使用 Local Storage Operator 自动设备发现	不支持	支持
使用机器健康检查功能自动修复损坏的机器	不支持	不支持
IBM Cloud® 的云控制器管理器。	支持	不支持
在节点上控制过量使用和管理容器密度	不支持	不支持

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
Cron 作业	支持	支持
Descheduler	支持	支持
Egress IP	支持	支持
加密数据存储在 etcd 中	支持	支持
FIPS 加密	支持	支持
Helm	支持	支持
Pod 横向自动扩展	支持	支持
托管 control plane（技术预览）	支持	支持
IBM 安全执行	不支持	支持
IBM Power® Virtual Server 的安装程序置备的基础架构支持	支持	不支持
在单一节点上安装	支持	支持
IPv6	支持	支持
用户定义项目的监控	支持	支持
多架构计算节点	支持	支持
多架构 control plane	支持	支持
多路径（Multipathing）	支持	支持
网络绑定磁盘加密 - 外部 Tang 服务器	支持	支持
非易失性内存表达驱动器(NVMe)	支持	不支持
NX-gzip for Power10 （硬件加速）	支持	不支持
oc-mirror 插件	支持	支持
OpenShift CLI (**oc**) 插件	支持	支持
Operator API	支持	支持

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
OpenShift Virtualization	不支持	不支持
OVN-Kubernetes，包括 IPsec 加密	支持	支持
PodDisruptionBudget	支持	支持
精度时间协议 (PTP) 硬件	不支持	不支持
Red Hat OpenShift Local	不支持	不支持
Scheduler 配置集	支持	支持
安全引导	不支持	支持
流控制传输协议 (SCTP)	支持	支持
支持多个网络接口	支持	支持
openshift-install 工具支持 IBM Power® 上的各种 SMT 级别 (Hardware Acceleration)	支持	支持
三节点集群支持	支持	支持
拓扑管理器	支持	不支持
SCSI 磁盘中的 z/VM 模拟 FBA 设备	不支持	支持
4K FCP 块设备	支持	支持

表 1.2. 持久性存储选项

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
使用 iSCSI 的持久性存储	支持 [1]	支持 [1],[2]
使用本地卷 (LSO) 的持久性存储	支持 [1]	支持 [1],[2]
使用 hostPath 的持久性存储	支持 [1]	支持 [1],[2]
使用 Fibre Channel 持久性存储	支持 [1]	支持 [1],[2]

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
使用 Raw Block 的持久性存储	支持 [1]	支持 [1],[2]
使用 EDEV/FBA 的持久性存储	支持 [1]	支持 [1],[2]

1. 必须使用 Red Hat OpenShift Data Foundation 或其他支持的存储协议来置备持久性共享存储。
2. 必须使用本地存储（如 iSCSI、FC 或者带有 DASD、FCP 或 EDEV/FBA 的 LSO）来置备持久性非共享存储。

表 1.3. Operator

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
cert-manager Operator for Red Hat OpenShift	支持	支持
Cluster Logging Operator	支持	支持
Cluster Resource Override Operator	支持	支持
Compliance Operator	支持	支持
Cost Management Metrics Operator	支持	支持
File Integrity Operator	支持	支持
HyperShift Operator	技术预览	技术预览
IBM Power® Virtual Server Block CSI Driver Operator	支持	不支持
Ingress Node Firewall Operator	支持	支持
Local Storage Operator	支持	支持
MetalLB Operator	支持	支持
Network Observability Operator	支持	支持
NFD Operator	支持	支持
NMState Operator	支持	支持
OpenShift Elasticsearch Operator	支持	支持

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
Vertical Pod Autoscaler Operator	支持	支持

表 1.4. Multus CNI 插件

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
Bridge	支持	支持
Host-device	支持	支持
IPAM	支持	支持
IPVLAN	支持	支持

表 1.5. CSI 卷

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
克隆	支持	支持
扩展	支持	支持
Snapshot	支持	支持

1.3.8. 认证和授权

1.3.8.1. 在现有集群中启用 Microsoft Entra Workload ID

在本发行版本中，您可以启用 Microsoft Entra Workload ID，以便在现有 Microsoft Azure OpenShift Container Platform 集群上使用简短凭证。此功能现在在 OpenShift Container Platform 的 4.14 和 4.15 版本中被支持。如需更多信息，请参阅启用基于令牌的身份验证。

1.3.9. 网络

1.3.9.1. OpenShift SDN 网络插件会阻止将来的主要升级

作为 OpenShift Container Platform 的一部分，作为唯一支持的网络插件，从 OpenShift Container Platform 4.16 开始，如果集群使用 OpenShift SDN 网络插件，在没有迁移到 OVN-Kubernetes 的情况下，您无法升级到将来的 OpenShift Container Platform 主版本。有关迁移到 OVN-Kubernetes 的更多信息，请参阅从 OpenShift SDN 网络插件 迁移。

如果尝试升级，Cluster Network Operator 会报告以下状态：

```
- lastTransitionTime: "2024-04-11T05:54:37Z"
  message: Cluster is configured with OpenShiftSDN, which is not supported in the
    next version. Please follow the documented steps to migrate from OpenShiftSDN
    to OVN-Kubernetes in order to be able to upgrade. https://docs.openshift.com/container-
platform/4.16/networking/ovn_kubernetes_network_provider/migrate-from-openshift-sdn.html
  reason: OpenShiftSDNConfigured
  status: "False"
  type: Upgradeable
```

1.3.9.2. 双 NIC Intel E810 Westport Channel 作为 PTP grandmaster 时钟（正式发布）

将 **linuxptp** 服务配置为双 Intel E810 Westport Channel 网络接口控制器(NIC)的 grandmaster 时钟(T-GM)现在是 OpenShift Container Platform 中的通用功能。主机系统时钟从连接到 Global Navigation Satellite Systems (GNSS)时间源的 NIC 同步。第二个 NIC 同步到由连接到 GNSS 的 NIC 提供的 1PPS 时间输出。如需更多信息，请参阅 将 linuxptp 服务配置为双 E810 Westport Channel NIC 的 grandmaster 时钟。

1.3.9.3. 带有高可用性系统时钟的双 NIC Intel E810 PTP 边界时钟（正式发布）

您可以将 **linuxptp** 服务 **ptp4l** 和 **phc2sys** 配置为双 PTP 边界时钟 (T-BC) 的高可用性 (HA) 系统时钟。

如需更多信息，请参阅 将 linuxptp 配置为双 NIC Intel E810 PTP 边界时钟的高可用性系统时钟 。

1.3.9.4. 配置 pod 放置以检查网络连接

要定期测试集群组件之间的网络连接，Cluster Network Operator (CNO)会创建 **network-check-source** 部署以及 **network-check-target** 守护进程集。在 OpenShift Container Platform 4.16 中，您可以通过设置节点选择器并运行源和目标 pod 来检查网络连接来配置节点。如需更多信息，请参阅 验证到端点的连接。

1.3.9.5. 为一个网络安全组(NSG)规则定义多个 CIDR 块

在这个版本中，在 Microsoft Azure 上托管的 OpenShift Container Platform 集群的 NSG 中更有效地处理 IP 地址和范围。因此，使用允许的SourceRanges 字段（从大约 1000 到 4000 CIDR）中，Microsoft Azure **集群中的所有** Ingress Controller 的最大无类别域间路由(CIDR)限制最大限制。

1.3.9.6. 在 Nutanix 上从 OpenShift SDN 迁移到 OVN-Kubernetes

在这个版本中，在 Nutanix 平台上支持从 OpenShift SDN 网络插件迁移到 OVN-Kubernetes。如需更多信息，请参阅 迁移到 OVN-Kubernetes 网络插件。

1.3.9.7. 改进了 CoreDNS 和出口防火墙之间的集成（技术预览）

在这个版本中，OVN-Kubernetes 使用新的 **DNSNameResolver** 自定义资源来跟踪出口防火墙规则中的 DNS 记录，并作为技术预览提供。此自定义资源支持同时使用通配符 DNS 名称和常规 DNS 名称，并允许访问 DNS 名称，无论与其更改相关联的 IP 地址是什么。

如需更多信息，请参阅 增强 DNS 解析和解析通配符域名。

1.3.9.8. SR-IOV 网络策略更新过程中并行节点排空

在这个版本中，您可以将 SR-IOV Network Operator 配置为在网络策略更新过程中并行排空节点。并行排空节点的选项可以更快地推出 SR-IOV 网络配置。您可以使用 **SriovNetworkPoolConfig** 自定义资源配置并行节点排空，并在 Operator 可以并行排空池中定义最大节点数量。

如需更多信息，请参阅在 SR-IOV 网络策略更新过程中配置并行节点排空。

1.3.9.9. SR-IOV Network Operator 不再自动创建 SriovOperatorConfig CR

自 OpenShift Container Platform 4.16 起，SR-IOV Network Operator 不再自动创建一个 **SriovOperatorConfig** 自定义资源(CR)。使用 配置 SR-IOV Network Operator 中的步骤创建 **SriovOperatorConfig** CR。

1.3.9.10. 支持双标记数据包(QinQ)

此发行版本引入了 802.1Q-in-802.1Q，也称为 *QinQ 支持*。QinQ 引入了第二个 VLAN 标签，其中服务提供商为其使用指定外部标签，提供它们的灵活性，而内部标签则保留给客户的 VLAN 专用。当数据包中存在两个 VLAN 标签时，外部 VLAN 标签可以是 802.1Q 或 802.1ad。内部 VLAN 标签必须始终是 802.1Q。

如需更多信息，请参阅为启用 SR-IOV 的工作负载配置 QinQ 支持 。

1.3.9.11. 为内部基础架构配置用户管理的负载均衡器

在这个版本中，您可以在任何内部基础架构上配置 OpenShift Container Platform 集群，如裸机、VMware vSphere、Red Hat OpenStack Platform (RHOSP)或 Nutanix，以使用用户管理的负载均衡器来代替默认负载均衡器。对于此配置，您必须在集群的 **install-config.yaml** 文件中指定 **loadBalancer.type: UserManaged**。

有关裸机基础架构上此功能的更多信息，请参阅为用户管理的负载均衡器的服务，*请参阅为 OpenShift 安装设置环境 中的服务*。

1.3.9.12. 检测和警告 iptables

在这个版本中，如果您使用 **iptables** 规则的集群中 pod，会发出以下事件信息来警告将来的弃用：

> This pod appears to have created one or more iptables rules. IPTables is deprecated and will no longer be available in RHEL 10 and later. You should consider migrating to another API such as nftables or eBPF.

如需更多信息，请参阅开始使用 nftables。如果您正在运行第三方软件，请检查您的厂商以确保它们很快提供基于 **nftables** 的版本。

1.3.9.13. OpenShift Container Platform 服务的 Ingress 网络流

在这个版本中，您可以查看 OpenShift Container Platform 服务的入口网络流。您可以使用这些信息来管理网络的入口流量，并提高网络安全性。

如需更多信息，请参阅 OpenShift Container Platform 网络流列表。

1.3.9.14. 修补现有的双栈网络

在这个版本中，您可以通过修补集群基础架构，将 API 和 Ingress 服务的 IPv6 虚拟 IP (VIP)添加到现有的双栈集群中。

如果您已经将集群升级到 OpenShift Container Platform 4.16，且您需要将单堆栈集群网络转换为双栈集群网络，则必须在 YAML 配置补丁文件中为集群指定以下内容：

- 第一个 **machineNetwork** 配置中 API 和 Ingress 服务的 IPv4 网络。

- 第二个 **machineNetwork** 配置中的 API 和 Ingress 服务的 IPv6 网络。

如需更多信息，请参阅 *转换到 IPv4/IPv6 双栈网络 中的 转换为双栈网络*。

1.3.9.15. MetalLB 和 FRR-K8s 集成（技术预览）

此发行版本引进了 **FRR-K8s**，它是基于 Kubernetes 的 **DaemonSet**，它以兼容 Kubernetes 的方式公开 **FRR** API 的子集。作为集群管理员，您可以使用 **FRRConfiguration** 自定义资源(CR)将 MetalLB Operator 配置为使用 **FRR-K8s** 守护进程集作为后端。您可以使用它来运行 FRR 服务，如接收路由。

如需更多信息，请参阅配置 MetalLB 和 FRR-K8s 的集成。

1.3.9.16. AdminNetworkPolicy 已正式发布

此功能提供两个新的 API，即 **AdminNetworkPolicy** (ANP)和 **BaselineAdminNetworkPolicy** (BANP)。在创建命名空间前，集群管理员可以使用 ANP 和 BANP 应用集群范围的网络策略并保护整个集群。由于它是集群范围的，因此 ANP 提供了一种解决方案，以便大规模管理其网络的安全性，而无需在每个命名空间中复制其网络策略。

如需更多信息，请参阅 *转换到 IPv4/IPv6 双栈网络 中的 转换为双栈网络*。

1.3.9.17. 实时迁移到 OVN-Kubernetes 网络插件

在以前的版本中，当从 OpenShift SDN 迁移到 OVN-Kubernetes 时，唯一可用的选项是 *离线* 迁移方法。这个过程包括一些停机时间，在此期间集群无法访问。

此发行版本引入了 *实时迁移* 方法。实时迁移方法是在不中断服务的情况下将 OpenShift SDN 网络插件及其网络配置、连接和相关资源迁移到 OVN-Kubernetes 网络插件的过程。它可用于 OpenShift Container Platform、Red Hat OpenShift Dedicated、Red Hat OpenShift Service on AWS 和 Microsoft Azure Red Hat OpenShift 部署类型。它不适用于 HyperShift 部署类型。这个迁移方法对于需要持续服务可用性的部署类型非常重要，并具有以下优点：

- 持续服务可用性
- 最小化停机时间
- 自动节点重新引导
- 从 OpenShift SDN 网络插件无缝过渡到 OVN-Kubernetes 网络插件

迁移到 OVN-Kubernetes 旨在是一个单向过程。

如需更多信息，请参阅 实时迁移到 OVN-Kubernetes 网络插件概述。

1.3.9.18. 使用 Whereabouts 进行多租户网络的重叠 IP 配置

在以前的版本中，无法配置相同的 CIDR 范围两次，并让 Whereabouts CNI 插件单独分配 IP 地址。这个限制会导致在多租户环境中出现问题，不同的组可能需要选择重叠的 CIDR 范围。

在这个版本中，Whereabouts CNI 插件通过包含 **network_name** 参数来支持重叠的 IP 地址范围。管理员可以使用 **network_name** 参数在单独的 **NetworkAttachmentDefinition** 中多次配置相同的 CIDR 范围，这样可为每个范围启用独立的 IP 地址分配。

此功能还包括增强的命名空间处理，在适当的命名空间中存储 **IPPool** 自定义资源(CR)，并在 Multus 允许时支持跨命名空间。这些改进在多租户环境中提供更大的灵活性和管理功能。

有关此功能的更多信息，请参阅使用 Whereabouts 进行动态 IP 地址分配配置 。

1.3.9.19. 支持更改 OVN-Kubernetes 网络插件内部 IP 地址范围

如果使用 OVN-Kubernetes 网络插件，您可以配置传输、加入和伪装子网。在集群安装过程中或之后，可以配置传输和加入子网。伪装子网必须在安装过程中配置，且之后无法更改。子网默认值为：

- 传输子网 ：**100.88.0.0/16** 和 **fd97::/64**
- 加入子网：100. **64**.0.0/16 和 **fd98::/64**
- masquerade subnet: **169.254.169.0/29** 和 **fd69::/125**

有关这些配置字段的更多信息，请参阅 Cluster Network Operator 配置对象 。有关在现有集群中配置传输和加入子网的更多信息，请参阅配置 OVN-Kubernetes 内部 IP 地址子网。

1.3.9.20. IPsec 遥测

Telemetry 和 Insights Operator 会在 IPsec 连接上收集遥测功能。如需更多信息，请参阅 显示 Telemetry 收集的数据。

1.3.10. Storage

1.3.10.1. HashiCorp Vault 现在可用于 Secrets Store CSI Driver Operator （技术预览）

现在，您可以使用 Secrets Store CSI Driver Operator 将 secret 从 HashiCorp Vault 挂载到 OpenShift Container Platform 中的 Container Storage Interface (CSI)卷。Secrets Store CSI Driver Operator 作为技术预览提供。

有关可用 机密存储提供程序的完整列表，请参阅 Secret 存储提供程序。

有关使用 Secrets Store CSI Driver Operator 从 HashiCorp Vault 挂载 secret 的详情，请参考 从 HashiCorp Vault 挂载 secret。

1.3.10.2. Microsoft Azure File 支持的卷克隆（技术预览）

OpenShift Container Platform 4.16 引入了 Microsoft Azure File Container Storage Interface (CSI) Driver Operator 的卷克隆作为技术预览功能。卷克隆会复制现有的持久性卷(PV)，以帮助防止 OpenShift Container Platform 中的数据丢失。您还可以像使用任何标准卷一样使用卷克隆。

如需更多信息，请参阅 Azure File CSI Driver Operator 和 CSI 卷克隆。

1.3.10.3. 节点扩展 Secret 已正式发布

节点扩展 Secret 功能允许集群扩展挂载卷的存储，即使访问这些卷也需要 secret （例如，用于访问存储区域网络(SAN) fabric）的凭证来执行节点扩展操作。OpenShift Container Platform 4.16 正式发布(GA)支持此功能。

1.3.10.4. 更改 vSphere CSI 最大快照数已正式发布

VMware vSphere Container Storage Interface (CSI)中的默认快照数是每个卷的默认最多快照数。在 OpenShift Container Platform 4.16 中，您可以将这个最大快照数量改为每个卷最多 32 个。您还可以精细控制 vSAN 和虚拟磁盘数据存储的最大快照数量。OpenShift Container Platform 4.16 正式发布(GA)支持此功能。

如需更多信息，请参阅 更改 vSphere 的最大快照数。

1.3.10.5. 持久性卷最后一个阶段转换时间参数（技术预览）

在 OpenShift Container Platform 4.16 中，引入了一个新的参数 **LastPhaseTransitionTime**，它有一个时间戳，每次持久性卷(PV)转换为不同的阶段(**pv.Status.Phase**)时都会更新。此功能以技术预览状态发布。

1.3.10.6. 使用 CIFS/SMB CSI Driver Operator 的持久性存储（技术预览）

OpenShift Container Platform 能够置备持久性卷(PV)，并带有通用互联网文件系统(CIFS) dialect/Server Message Block (SMB)协议的 Container Storage Interface (CSI)驱动程序。管理此驱动程序的 CIFS/SMB CSI Driver Operator 处于技术预览状态。

如需更多信息，请参阅 CIFS/SMB CSI Driver Operator。

1.3.10.7. 带有 SELinux 上下文挂载的 RWOP 已正式发布

OpenShift Container Platform 4.14 引入了一个新的访问模式，它带有技术预览状态用于持久性卷(PV)和持久性卷声明(PVC)，名为 ReadWriteOncePod (RWOP)。RWOP 只能在单个节点上的单个 pod 中使用，与多个 pod 可以在单个节点上使用 PV 或 PVC 的现有 ReadWriteOnce 访问模式。如果驱动程序启用它，RWOP 将使用 **PodSpec** 或容器中设置的 SELinux 上下文挂载，它允许驱动程序使用正确的 SELinux 标签直接挂载卷。这消除了递归重新标记卷的需求，pod 启动可能会显著提高。

在 OpenShift Container Platform 4.16 中，此功能已正式发布。

如需更多信息，请参阅 访问模式。

1.3.10.8. vSphere CSI Driver 3.1 更新了 CSI 拓扑要求

要在多zonal 集群中支持 VMware vSphere Container Storage Interface (CSI)卷置备和使用，部署应该与 CSI 驱动程序施加的某些要求匹配。这些要求已从 3.1.0 开始改变，虽然 OpenShift Container Platform 4.16 接受旧的和新的标记方法，但您应该使用新的标记方法，因为 VMware vSphere 认为是无效的配置。要防止问题，您不应该使用旧的标记方法。

如需更多信息，请参阅 vSphere CSI 拓扑要求。

1.3.10.9. 支持配置 thick-provisioned 存储

此功能为配置厚置备的存储提供支持。如果您在 **LVMCluster** 自定义资源(CR)中排除 **deviceClasses.thinPoolConfig** 字段，逻辑卷是厚置备的。使用厚置备的存储包括以下限制：

- 不支持卷克隆。
- 不支持 **VolumeSnapshotClass**。因此，不支持 CSI 快照。
- 不支持过度配置。因此，PVC 置备的容量会立即从卷组中减少。
- 不支持精简指标。厚置备的设备只支持卷组指标。

有关配置 **LVMCluster** CR 的详情，请参考 关于 LVMCluster 自定义资源。

1.3.10.10. 当 LVMCluster 自定义资源中没有配置设备选择器时，支持新的警告信息

当您没有在 **LVMCluster** 自定义资源(CR)中配置 **deviceSelector** 字段时，这个版本提供了一个新的警告信息。

LVMCluster CR 支持一个新的字段 **deviceDiscoveryPolicy**，它表示是否配置了 **deviceSelector** 字段。如果没有配置 **deviceSelector** 字段，LVM Storage 会自动将 **deviceDiscoveryPolicy** 字段设置为 **RuntimeDynamic**。否则，**deviceDiscoveryPolicy** 字段被设置为 **Preconfigured**。

不建议从 **LMVCluster** CR 中排除 **deviceSelector** 字段。有关没有配置 **deviceSelector** 字段的限制的更多信息，请参阅关于在卷组中添加设备。

1.3.10.11. 支持向卷组添加加密设备

此功能支持将加密设备添加到卷组。您可以在 OpenShift Container Platform 安装过程中在集群节点上启用磁盘加密。加密设备后，您可以在 **LVMCluster** 自定义资源的 **deviceSelector** 字段中指定 LUKS 加密设备的路径。有关磁盘加密的详情，请参阅 关于磁盘加密和配置磁盘加密和镜像。https://docs.redhat.com/en/documentation/openshift_container_platform/4.16/html-single/installing/#installation-special-config-encrypt-disk_installing-customizing

有关向卷组添加设备的更多信息，请参阅关于在卷组中添加设备。

1.3.11. Operator 生命周期

1.3.11.1. Operator API 重命名为 ClusterExtension （技术预览）

Operator Lifecycle Manager (OLM) 1.0 的早期技术预览阶段引入了一个新的 **Operator** API，由 Operator Controller 组件以 **operator.operators.operatorframework.io** 提供。在 OpenShift Container Platform 4.16 中，这个 API 被重命名为 **ClusterExtension**，为 OLM 1.0 的这个技术预览阶段提供 **clusterextension.olm.operatorframework.io**。

此 API 仍然通过 registry+v1 捆绑包格式简化安装的扩展管理，其中包括通过 **registry+v1** 捆绑包格式的 Operator，方法是将面向用户的 API 整合到单个对象中。重命名至 **ClusterExtension** 地址，如下所示：

- 更准确地反映扩展集群功能的简化功能
- better 代表更灵活的打包格式
- 集群前缀明确表示 **Cluster Extension** 对象是集群范围的，与旧的 OLM 的更改，其中 Operator 可以是命名空间范围的或集群范围的

如需更多信息，请参阅 Operator Controller。

重要

目前，OLM 1.0 支持安装满足以下条件的扩展：

- 扩展必须使用 **AllNamespaces** 安装模式。
- 扩展不能使用 Webhook。

使用 Webhook 或以单个或指定命名空间集合的集群扩展无法安装。

1.3.11.2. 改进了 Operator Lifecycle Manager (OLM) 1.0 中集群扩展的状态条件消息和弃用通知（技术预览）

在这个版本中，OLM 1.0 显示已安装集群扩展的以下状态条件信息：

- 特定的捆绑包名称
- 已安装的版本
- 改进了健康报告
- 软件包、频道和捆绑包的弃用通知

1.3.11.3. 支持 OLM 1.0 中的旧 OLM 升级边缘（技术预览）

在为已安装的集群扩展决定升级边缘时，Operator Lifecycle Manager (OLM) 1.0 支持从 OpenShift Container Platform 4.16 开始的传统 OLM 语义。这个支持遵循旧的 OLM 的行为，包括 **替换**、**跳过**、和 **skipRange** 指令，但有一些区别。

通过支持传统的 OLM 语义，OLM 1.0 现在从目录中准确遵循升级图表。

注意

OpenShift Container Platform 4.15 中引入了对语义版本(semver)升级限制的支持，但在这个技术预览阶段禁用在 4.16 中。

如需更多信息，请参阅升级 约束语义。

1.3.12. Builds

未经身份验证的用户已从 system:webhook 角色绑定中删除
在这个版本中，未经身份验证的用户不再能够访问 **system:webhook** 角色绑定。在 OpenShift Container Platform 4.16 之前，未经身份验证的用户可以访问 **system:webhook** 角色绑定。为未经身份验证的用户更改此访问权限会添加额外的安全层，并仅在需要时供用户启用。这个变化适用于新集群，以前的集群不受影响。

在有些用例中，您可能希望允许未经身份验证的用户特定命名空间的 **system:webhook** 角色绑定。**system:webhook** 集群角色允许用户触发不使用 OpenShift Container Platform 身份验证机制的外部系统的构建，如 GitHub、GitLab 和 Bitbucket。集群管理员可以授予未经身份验证的用户访问 **system:webhook** 角色绑定，以便于这个用例。

重要

在修改未经身份验证的访问时，始终验证符合您机构的安全标准。

要授予未经身份验证的用户访问特定命名空间中的 **system:webhook** 角色绑定，请参阅 将未经身份验证的用户添加到 system:webhook 角色绑定。

1.3.13. Machine Config Operator

1.3.13.1. 未使用的呈现机器配置的垃圾回收

在这个版本中，您可以垃圾回收未使用的呈现机器配置。通过使用 **oc adm prune renderedmachineconfigs** 命令，您可以查看未使用的渲染机器配置，决定要删除的机器配置，然后批量删除您不再需要的渲染机器配置。具有太多机器配置可能会导致机器配置混淆，并有助于提高磁盘空间和性能问题。如需更多信息，请参阅管理未使用的呈现的机器配置。

1.3.13.2. 节点中断策略（技术预览）

默认情况下，当您对 **MachineConfig** 对象中的参数进行某些更改时，Machine Config Operator (MCO) 会排空并重启与该机器配置关联的节点。但是，您可以在 MCO 命名空间中创建节点中断策略，该策略定义了一组 Ignition 配置对象更改，这些配置对象对工作负载只需要少或不会中断。如需更多信息，请参阅使用节点中断策略来最大程度降低机器配置变化的中断。

1.3.13.3. 集群 RHCOS 镜像分层（技术预览）

使用 Red Hat Enterprise Linux CoreOS (RHCOS)镜像分层，您现在可以直接在集群中自动构建自定义分层镜像，作为技术预览功能。在以前的版本中，您需要在集群之外构建自定义分层镜像，然后将镜像拉取到集群中。您可以通过将额外镜像分层到基础镜像，使用镜像层功能来扩展基本 RHCOS 镜像的功能。如需更多信息，请参阅 RHCOS 镜像分层。

1.3.13.4. 更新引导镜像（技术预览）

默认情况下，MCO 不会删除它用来启动 Red Hat Enterprise Linux CoreOS (RHCOS)节点的引导镜像。因此，集群中的引导镜像不会随集群一起更新。现在，您可以将集群配置为在更新集群时更新引导镜像。如需更多信息，请参阅更新引导镜像。

1.3.14. 机器管理

1.3.14.1. 为集群自动扩展配置扩展器

在这个版本中，集群自动扩展可以使用 **LeastWaste**、**Priority** 和 **Random** 展开器。您可以配置这些扩展器，以便在扩展集群时影响机器集的选择。如需更多信息，请参阅配置集群自动扩展。

1.3.14.2. 使用 VMware vSphere 的集群 API 管理机器（技术预览）

此发行版本引入了使用上游 Cluster API （集成到 OpenShift Container Platform）作为 VMware vSphere 集群的技术预览来管理机器的功能。这个功能是使用 Machine API 管理机器的补充或替代功能。如需更多信息，请参阅关于集群 API。

1.3.14.3. 为 control plane 机器集定义 vSphere 故障域

在这个版本中，为 control plane 机器集定义 vSphere 故障域的以前技术预览功能正式发布。如需更多信息，请参阅 VMware vSphere 的 Control plane 配置选项。

1.3.15. 节点

1.3.15.1. 移动 Vertical Pod Autoscaler Operator pod

Vertical Pod Autoscaler Operator (VPA)由三个组件组成：推荐器、更新器和准入控制器。Operator 和每个组件在 control plane 节点上的 VPA 命名空间中都有自己的 pod。您可以将 VPA Operator 和组件 pod 移到基础架构或 worker 节点。如需更多信息，请参阅 Moving Vertical Pod Autoscaler Operator 组件 。

1.3.15.2. must-gather 收集的附加信息

在这个版本中，**oc adm must-gather** 命令收集以下附加信息：

- OpenShift CLI (**oc**)二进制版本
- must-gather 日志

这些添加有助于识别使用特定版本的 **oc** 的问题。**oc adm must-gather** 命令还会列出使用的镜像，以及任何数据在 must-gather 日志中无法收集到的信息。

如需更多信息，请参阅关于 must-gather 工具。

1.3.15.3. 编辑 BareMetalHost 资源

在 OpenShift Container Platform 4.16 及更高版本中，您可以编辑裸机节点的 **BareMetalHost** 资源中的基板管理控制器(BMC)地址。节点必须处于 Provisioned、**Externally Provisioned** 、**Registering** 或 **Available** 状态。编辑 **BareMetalHost** 资源中的 BMC 地址不会取消置备节点。如需了解更多详细信息，请参阅编辑 BareMetalHost 资源。

1.3.15.4. 附加不可启动的 ISO

在 OpenShift Container Platform 4.16 及更高版本中，您可以使用 **DataImage** 资源将一个通用的、不可启动的 ISO 虚拟介质镜像附加到置备的节点上。应用资源后，操作系统在下次重启时可以访问 ISO 镜像。节点必须使用 Redfish 或从中派生的驱动程序来支持此功能。节点必须处于 **Provisioned** 或 **ExternallyProvisioned** 状态。如需了解更多详细信息，请参阅将不可启动的 ISO 附加到裸机节点。

1.3.16. 监控

此发行版本中的集群监控堆栈包括以下新功能和修改后的功能。

1.3.16.1. 监控堆栈组件和依赖项更新

此发行版本包括对集群监控堆栈组件和依赖项的以下版本更新：

- kube-state-metrics 到 2.12.0
- 指标服务器到 0.7.1
- node-exporter 到 1.8.0
- Prometheus 到 2.52.0
- Prometheus Operator 到 0.73.2
- Thanos to 0.35.0

1.3.16.2. 对警报规则的更改

注意

红帽不保证记录规则或警报规则的向后兼容性。

- 添加了 **ClusterMonitoringOperatorDeprecatedConfig** 警报，以便在 Cluster Monitoring Operator 配置使用已弃用的字段时监控。
- 添加了 **PrometheusOperatorStatusUpdateErrors** 警报，以监控 Prometheus Operator 无法更新对象状态的时间。

1.3.16.3. 用于访问 Metrics API 正式发布(GA)的指标服务器组件

Metrics Server 组件现已正式发布，并自动安装，而不是已弃用的 Prometheus Adapter。指标服务器收

集资源指标，并在 **metrics.k8s.io** Metrics API 服务中公开它们，供其他工具和 API 使用，从而释放核心平台 Prometheus 堆栈处理此功能。如需更多信息，请参阅 Cluster Monitoring Operator 的配置映射 API 参考中的 MetricsServerConfig。

1.3.16.4. 新的监控角色，允许对 Alertmanager API 进行只读访问

此发行版本引入了一个新的 **monitoring-alertmanager-view** 角色，允许对 **openshift-monitoring** 项目中的 Alertmanager API 进行只读访问。

1.3.16.5. VPA 指标包括在 kube-state-metrics 代理中

Vertical Pod Autoscaler (VPA)指标可以通过 **kube-state-metrics** 代理获得。VPA 指标遵循类似的组成格式，就如在从原生支持上游弃用和删除之前一样。

1.3.16.6. 监控组件的代理服务更改

在这个版本中，Prometheus、Alertmanager 和 Thanos Ruler 前面的代理服务已从 OAuth 更新至 **kube-rbac-proxy**。此更改可能会影响服务帐户和用户访问这些 API 端点，而无需适当的角色和集群角色。

1.3.16.7. Prometheus 处理重复样本的方式改变

在这个版本中，当 Prometheus 提取目标时，重复的示例不再被静默忽略，即使它们具有相同的值。第一个示例被接受，**prometheus_target_scrapes_sample_duplicate_timestamp_total** 计数器会递增，这可能会触发 **PrometheusDuplicateTimestamps** 警报。

1.3.17. Network Observability Operator

Network Observability Operator 发行版本独立于 OpenShift Container Platform 次版本流的更新。更新可以通过单一的滚动流提供，该流在所有当前支持的 OpenShift Container Platform 4 版本中被支持。有关 Network Observability Operator 的新功能、功能增强和程序错误修复的信息，请参阅 Network Observability 发行注记。

1.3.18. 可伸缩性和性能

1.3.18.1. 工作负载分区增强

在这个版本中，使用工作负载注解部署的平台 pod 包括 CPU 限制和 CPU 请求会准确计算并应用 CPU 限值，并作为特定 pod 的 CPU 配额进行计算并应用。在以前的版本中，如果工作负载分区 pod 同时设置了 CPU 限值和请求，则 Webhook 会忽略它们。pod 无法从工作负载分区中受益，且不会锁定到特定内核。在这个版本中，webhook 可以正确解释请求和限值。

注意

如果 CPU 限值的值与注解中请求的值不同，则 CPU 限值与请求相同。

如需更多信息，请参阅 工作负载分区。

1.3.18.2. 现在，性能配置集功能支持 Linux Control Groups 版本 2

从 OpenShift Container Platform 4.16 开始，控制组群版本 2 (cgroup v2)（也称为 cgroup2 或 cgroupsv2）对于所有新部署都默认启用，即使性能配置集存在。

从 OpenShift Container Platform 4.14 开始，cgroup v2 是默认的，但性能配置集功能需要使用 cgroup v1。这个问题已解决。

通过将 **node.config** 对象中的 **cgroupMode** 字段更改为 v1，在 OpenShift Container Platform 4.16. cgroup v1 之前，仍会在当前版本中使用 cgroup **v1** 的升级集群。

如需更多信息，请参阅 在节点上配置 Linux cgroup 版本 。

1.3.18.3. 支持增加 etcd 数据库大小（技术预览）

在这个版本中，您可以在 etcd 中增加磁盘配额。这是一个技术预览功能。如需更多信息，请参阅 增加 etcd 的数据库大小。

1.3.18.4. 保留内核频率调整

在这个版本中，Node Tuning Operator 支持在 **PerformanceProfile** 中为保留和隔离的内核 CPU 设置 CPU 频率。这是可用于定义特定频率的可选功能。然后，Node Tuning Operator 通过在 Intel 硬件中启用 **intel_pstate** CPUFreq 驱动程序来设置这些频率。您必须遵循 Intel 对 FlexRAN-like 应用程序的建议，这需要将默认 CPU 频率设置为比默认运行频率低的值。

1.3.18.5. Node Tuning Operator intel_pstate 驱动程序默认设置

在以前的版本中，对于 RAN DU-profile，在 **PerformanceProfile** 中将 **realTime** 工作负载提示设置为 **true** 会始终禁用 **intel_pstate**。在这个版本中，Node Tuning Operator 会检测使用 **TuneD** 的底层 Intel 硬件，并根据处理器的生成正确设置 **intel_pstate** 内核参数。这会将 **intel_pstate** 与 **realTime** 和 **highPowerConsumption** 工作负载提示分离。**intel_pstate** 现在依赖于底层处理器的生成。

对于 pre-IceLake 处理器的处理器，默认情况下为 **intel_pstate**，而对于 IceLake 及更新的生成处理器，**intel_pstate** 设置为 **active**。

1.3.19. 边缘计算

1.3.19.1. 使用 RHACM PolicyGenerator 资源管理 GitOps ZTP 集群策略（技术预览）

现在，您可以使用 **PolicyGenerator** 资源和 Red Hat Advanced Cluster Management (RHACM)来使用 GitOps ZTP 为受管集群部署策略。**PolicyGenerator** API 是 Open Cluster Management 标准的一部分，它提供了一种通用的修补资源的方法，这些资源无法通过 **PolicyGenTemplate** API 来实现。使用 **PolicyGenTemplate** 资源管理和部署策略将在即将发布的 OpenShift Container Platform 发行版本中弃用。

如需更多信息，请参阅使用 PolicyGenerator 资源配置受管集群策略。

注意

PolicyGenerator API 目前不支持将补丁与包含项目列表的自定义 Kubernetes 资源合并。例如，在 **PtpConfig** CR 中。

1.3.19.2. TALM 策略补救

在这个版本中，Topology Aware Lifecycle Manager (TALM)使用 Red Hat Advanced Cluster Management (RHACM)功能来修复受管集群中的 **inform** 策略。此功能增强删除了 Operator 在策略补救过程中创建 **inform** 策略的 **强制** 副本。由于复制策略，这个增强还减少了 hub 集群上的工作负载，并可减少在受管集群中修复策略所需的总体时间。

如需更多信息，请参阅在受管集群上更新策略。

1.3.19.3. 加速置备 GitOps ZTP （技术预览）

在这个版本中，您可以通过为单节点 OpenShift 使用 GitOps ZTP 置备来缩短集群安装所需的时间。加速 ZTP 通过在早期阶段应用从策略派生的第 2 天清单来加快安装速度。

加速置备 GitOps ZTP 的好处会随着部署的规模增加。完全加速为更多集群带来更多好处。使用较少的集群，安装时间缩短会显著减少。

如需更多信息，请参阅 GitOps ZTP 的加速置备 。

1.3.19.4. 使用 Lifecycle Agent 为单节点 OpenShift 集群进行基于镜像的升级

在这个版本中，您可以使用 Lifecycle Agent 编配从 OpenShift Container Platform <4.y> 到 <4.y+2> 的单节点 OpenShift 集群的基于镜像的升级，并将 <4.y.z+n> 升级到 <4.y.z+n>。Lifecycle Agent 生成与参与集群的配置匹配的开放容器项目(OCI)镜像。除了 OCI 镜像外，基于镜像的升级使用 **ostree** 库和 OADP Operator 来降低在原始平台版本和目标平台版本间进行转换时的升级和服务中断持续时间。

如需更多信息，请参阅了解单节点 OpenShift 集群的基于镜像的升级。

1.3.19.5. 使用 GitOps ZTP 和 RHACM 将 IPsec 加密部署到受管集群（技术预览）

现在，您可以使用 GitOps ZTP 和 Red Hat Advanced Cluster Management (RHACM)部署的受管单节点 OpenShift 集群中启用 IPsec 加密。您可以加密受管集群外部 pod 和 IPsec 端点之间的外部流量。OVN-Kubernetes 集群网络上的节点之间的所有 pod 到 pod 网络流量都使用 IPsec 在传输模式中加密。

如需更多信息，请参阅使用 GitOps ZTP 和 SiteConfig 资源为单节点 OpenShift 集群配置 IPsec 加密 。

1.3.20. 安全性

新的签名者证书颁发机构(CA) **openshift-etcd** 现在可以为证书签名。此 CA 包含在与现有 CA 的信任捆绑包中。有两个 CA secret (**etcd-signer** 和 **etcd-metric-signer**)也可用于轮转。从这个版本开始，所有证书都将移至经过验证的库。此更改允许自动轮转不是由 **cluster-etcd-operator** 管理的所有证书。所有节点都基于节点的证书将继续进行当前的更新过程。

1.4. 主要的技术变化

OpenShift Container Platform 4.16 包括以下显著的技术更改。

HAProxy 版本 2.8
OpenShift Container Platform 4.16 使用 HAProxy 2.8。

不再支持与 HAProxy 搭配使用的 SHA-1 证书
不再支持 SHA-1 证书用于 HAProxy。在 OpenShift Container Platform 4.16 中使用 SHA-1 证书的现有路由都会被拒绝，且无法正常工作。有关创建安全路由的更多信息，请参阅 安全路由。

etcd 调整参数
在这个版本中，etcd 调整参数可以设置为优化性能并降低延迟的值，如下所示。

- **""**（默认）
- **Standard**（标准）
- **速度较慢**

未经身份验证的用户已从某些集群角色中删除

在这个版本中，未经身份验证的用户不再能够访问某些功能集所需的特定集群角色。在 OpenShift Container Platform 4.16 之前，未经身份验证的用户可以访问某些集群角色。为未经身份验证的用户更改此访问权限会添加额外的安全层，并且仅在需要时启用。这个变化适用于新集群，以前的集群不受影响。

在某些情况下，您可能想要为特定集群角色授予未经身份验证的用户访问权限。要授予未经身份验证的用户访问某些功能所需的特定集群角色，请参阅将 未经身份验证的组添加到集群角色中。

重要

在修改未经身份验证的访问时，始终验证符合您机构的安全标准。

IBM Z (R)和 IBM (R) LinuxONE (s390x)上不再支持 RHCOS dasd 镜像工件

在这个版本中，**s390x** 架构的 **dasd** 镜像工件已从 OpenShift Container Platform 镜像构建管道中删除。您仍然可以使用 **metal4k** 镜像工件，其相同并包含相同的功能。

支持带有 ExternalTrafficPolicy=Local 服务的 EgressIP

在以前的版本中，gressIP 所选 pod 不支持将 **externalTrafficPolicy** 设置为 **Local** 的服务作为后端。当尝试此配置时，到达 pod 的服务入口流量会错误地重新路由到托管 EgressIP 的出口节点。这会影响对传入服务流量连接的响应，并在将 **externalTrafficPolicy** 设置为 **Local** 时导致无法正常工作的服务，因为连接被丢弃并且服务不可用。

在 OpenShift Container Platform 4.16 中，OVN-Kubernetes 现在支持在同一一组所选 pod 上同时使用 **ExternalTrafficPolicy=Local** 服务和 EgressIP 配置。OVN-Kubernetes 现在只将源自 EgressIP pod 的流量重新路由到出口节点，同时通过 pod 所在的同一节点将响应从 EgressIP pod 路由到 ingress 服务流量。

旧服务帐户 API 令牌 secret 不再为每个服务帐户生成

在 OpenShift Container Platform 4.16 之前，当启用了集成的 OpenShift 镜像 registry 时，会为集群中的每个服务帐户生成一个旧的服务帐户 API 令牌 secret。从 OpenShift Container Platform 4.16 开始，当启用集成的 OpenShift 镜像 registry 时，每个服务帐户不再会生成旧的服务帐户 API 令牌 secret。

另外，当启用集成的 OpenShift 镜像 registry 时，每个服务帐户生成的镜像 pull secret 不再使用旧的服务帐户令牌 API 令牌。现在，镜像 pull secret 使用绑定服务帐户令牌，该令牌会在过期前自动刷新。

如需更多信息，请参阅 自动生成的镜像 pull secret。

有关检测集群中正在使用的旧服务帐户 API 令牌 secret 的详情，请参考 OpenShift Container Platform 中的长期服务帐户令牌 API 令牌。

支持外部云身份验证供应商

在本发行版本中，在 Amazon Web Services (AWS)、Google Cloud Platform (GCP)和 Microsoft Azure 集群(OpenShift Container Platform)上向私有 registry 进行身份验证的功能被移到 OpenShift Container Platform 附带的二进制文件中。此更改支持 Kubernetes 1.29 中引入的默认外部云身份验证供应商行为。

如果禁用 Build 集群功能，则 builder 服务帐户将不再创建

在这个版本中，如果您禁用 **Build** 集群功能，则不再创建 **builder** 服务帐户及其对应的 secret。

如需更多信息，请参阅 构建功能。

默认 OLM 1.0 升级限制已改为传统的 OLM 语义（技术预览）

在 OpenShift Container Platform 4.16 中，Operator Lifecycle Manager (OLM) 1.0 将其默认升级限制从语义版本(semver)改为旧的 OLM 语义。

如需更多信息，请参阅在 OLM 1.0 中支持旧的 OLM 升级边缘（技术预览）。

从 OLM 1.0 中删除 RukPak Bundle API （技术预览）

在 OpenShift Container Platform 4.16 中，Operator Lifecycle Manager (OLM) 1.0 删除 **Bundle** API，它由 RukPak 组件提供。RukPak **BundleDeployment** API 仍然保留，并支持 **registry+v1** 捆绑包以旧的 Operator Lifecycle Manager (OLM)捆绑包格式解包 Kubernetes YAML 清单。

如需更多信息，请参阅 Rukpak （技术预览）。

添加了 dal12 区域

在这个版本中，**dal12** 区域已添加到 IBM Power® VS Installer 中。

添加至 IBM Power (R)虚拟服务器的区域

此发行版本引入了部署到新的 IBM Power® Virtual Server (VS)区域 **osa21**、s**syd04**、**lon06** 和 **sao01** 的功能。

IBM Power (R) Virtual Verver 集群 API 更新至 0.8.0

在这个版本中，IBM Power® VS CAPI 已更新至版本 0.8.0。

ServiceInstanceNameToGUID 的额外调试语句

在这个版本中，额外的调试语句被添加到 **ServiceInstanceNameToGUID** 功能中。

1.5. 弃用和删除的功能

之前版本中的一些功能已被弃用或删除。

弃用的功能仍然包含在 OpenShift Container Platform 中，并将继续被支持。但是，这个功能会在以后的发行版本中被删除，且不建议在新的部署中使用。有关 OpenShift Container Platform 4.16 中已弃用并删除的主要功能的最新列表，请参考下表。表后列出了更多已弃用和删除的功能的更多详细信息。

在以下表格中，功能被标记为以下状态：

- *公开发行*
- *已弃用*
- *删除*

Operator 生命周期和开发已弃用和删除的功能

表 1.6. Operator 生命周期和开发已弃用并删除 tracker

功能	4.14	4.15	4.16
Operator SDK	公开发行	公开发行	已弃用
为基于 Ansible 的 Operator 项目构建工具	公开发行	公开发行	已弃用
为基于 Helm 的 Operator 项目构建工具	公开发行	公开发行	已弃用
为基于 Go 的 Operator 项目构建工具	公开发行	公开发行	已弃用
为基于 Helm 的 Operator 项目构建工具	技术预览	技术预览	已弃用
为基于 Java 的 Operator 项目构建工具	技术预览	技术预览	已弃用

功能	4.14	4.15	4.16
平台 Operator	技术预览	技术预览	删除
普通捆绑包	技术预览	技术预览	删除
Operator 目录的 SQLite 数据库格式	已弃用	已弃用	已弃用

镜像已弃用和删除的功能

表 1.7. Cluster Samples Operator 弃用并删除 tracker

功能	4.14	4.15	4.16
Cluster Samples Operator	公开发行	公开发行	已弃用

监控已弃用和删除的功能

表 1.8. 监控已弃用和删除的 tracker

功能	4.14	4.15	4.16
dedicatedServiceMonitors 设置，用于为核心平台监控启用专用的服务监控器	公开发行	已弃用	删除
prometheus-adapter 组件从 Prometheus 查询资源指标，并在 metrics API 中公开它们。	公开发行	已弃用	删除

安装已弃用和删除的功能

表 1.9. 安装已弃用并删除跟踪器

功能	4.14	4.15	4.16
OpenShift SDN 网络插件	已弃用	删除 [1]	删除
oc adm release extract 的 **--cloud** 参数	已弃用	已弃用	已弃用
对 **cluster.local** 域的 CoreDNS 通配符查询	已弃用	已弃用	已弃用
compute.platform.openstack.rootVolume.type for RHOSP	已弃用	已弃用	已弃用
controlPlane.platform.openstack.rootVolume.type for RHOSP	已弃用	已弃用	已弃用

功能	4.14	4.15	4.16
安装程序置备的基础架构集群的 **install-config.yaml** 文件中的 **ingressVIP** 和 **apiVIP** 设置	已弃用	已弃用	已弃用
基于软件包的 RHEL 计算机器	公开发行	公开发行	已弃用
platform.aws.preserveBootstrapIgnition 参数用于 Amazon Web Services (AWS)	公开发行	公开发行	已弃用
Amazon Web Services (AWS)、VMware vSphere 和 Nutanix 的 Terraform 基础架构供应商	公开发行	公开发行	删除
Google Cloud Platform (GCP)的 Terraform 基础架构供应商	公开发行	公开发行	可移动介质作为技术预览
使用安装程序置备的基础架构在 Alibaba Cloud 上安装集群	技术预览	技术预览	删除

1. 虽然安装程序在版本 4.15 中不再支持 OpenShift SDN 网络插件，但您可以将使用 OpenShift SDN 插件的集群从版本 4.14 升级到 4.15。

更新集群已弃用和删除的功能

表 1.10. 更新集群已弃用并删除 tracker

功能	4.14	4.15	4.16

存储已弃用和删除的功能

表 1.11. 存储已弃用和删除的 tracker

功能	4.14	4.15	4.16
使用 FlexVolume 的持久性存储	已弃用	已弃用	已弃用
AliCloud Disk CSI Driver Operator	公开发行	公开发行	删除

已弃用和删除的网络功能

表 1.12. 已弃用和删除的网络功能跟踪器

功能	4.14	4.15	4.16
RHOSP 上的 Kuryr	已弃用	删除	删除
OpenShift SDN 网络插件	已弃用	已弃用	已弃用

功能	4.14	4.15	4.16
iptables	已弃用	已弃用	已弃用

Web 控制台已弃用和删除的功能

表 1.13. Web 控制台已弃用并删除 tracker

功能	4.14	4.15	4.16
PatternFly 4	公开发行	已弃用	已弃用
对路由器 5 做出反应	公开发行	已弃用	已弃用

节点已弃用和删除的功能

表 1.14. 节点已弃用并删除 tracker

功能	4.14	4.15	4.16
ImageContentSourcePolicy (ICSP) 对象	已弃用	已弃用	已弃用
Kubernetes 拓扑标签 **failure-domain.beta.kubernetes.io/zone**	已弃用	已弃用	已弃用
Kubernetes 拓扑标签 **failure-domain.beta.kubernetes.io/region**	已弃用	已弃用	已弃用
cgroup v1	公开发行	公开发行	已弃用

工作负载已弃用和删除的功能

表 1.15. 工作负载已弃用和删除的 tracker

功能	4.14	4.15	4.16
deploymentConfig 对象	已弃用	已弃用	已弃用

裸机监控已弃用和删除的功能

表 1.16. 裸机事件中继 Operator tracker

功能	4.14	4.15	4.16
裸机事件中继 Operator	技术预览	已弃用	已弃用

1.5.1. 已弃用的功能

1.5.1.1. Linux Control Groups 版本 1 现已弃用

在 Red Hat Enterprise Linux (RHEL) 9 中，默认模式是 cgroup v2。当发布 Red Hat Enterprise Linux (RHEL) 10 时，systemd 将不支持在 cgroup v1 模式下引导，且只有 cgroup v2 模式可用。因此，OpenShift Container Platform 4.16 及更新的版本中已弃用 cgroup v1。cgroup v1 将在以后的 OpenShift Container Platform 发行版本中删除。

1.5.1.2. Cluster Samples Operator

Cluster Samples Operator 在 OpenShift Container Platform 4.16 版本中已弃用。Cluster Samples Operator 将停止管理和提供对非 S2I 示例（镜像流和模板）的支持。没有新模板、示例或非 Source-to-Image (Non-S2I)镜像流将添加到 Cluster Samples Operator 中。但是，现有 S2I 构建器镜像流和模板将继续接收更新，直到以后的发行版本中删除了 Cluster Samples Operator。

1.5.1.3. 基于软件包的 RHEL 计算机器

在这个版本中，安装基于软件包的 RHEL worker 节点已弃用。在以后的发行版本中，RHEL worker 节点将被删除并不再被支持。

RHCOS 镜像分层将替换此功能，并支持在 worker 节点的基本操作系统上安装额外的软件包。

有关镜像分层的更多信息，请参阅 RHCOS 镜像分层。

1.5.1.4. Operator SDK CLI 工具和相关测试和构建工具已弃用

红帽支持的 Operator SDK CLI 工具版本，包括 Operator 项目的相关构建和测试工具已被弃用，计划在以后的 OpenShift Container Platform 发行版本中删除。红帽将在当前发行生命周期中提供对这个功能的程序错误修复和支持，但此功能将不再获得改进，并将在以后的 OpenShift Container Platform 版本中删除。

对于创建新 Operator 项目，不建议使用红帽支持的 Operator SDK 版本。现有 Operator 项目的 Operator 作者可以使用 OpenShift Container Platform 4.16 发布的 Operator SDK CLI 工具版本来维护其项目，并创建针对较新版本的 OpenShift Container Platform 的 Operator 发行版本。

以下与 Operator 项目相关的基础镜像 *已被弃用*。这些基础镜像的运行时功能和配置 API 仍然受到 bug 修复和解决 CVE 的支持。

- 基于 Ansible 的 Operator 项目的基础镜像
- 基于 Helm 的 Operator 项目的基础镜像

有关 Operator SDK 不支持的、社区维护版本的信息，请参阅 Operator SDK (Operator Framework)。

1.5.1.5. Amazon Web Services (AWS)上的 preserveBootstrapIgnition 参数已弃用

install-config.yaml 文件中的 Amazon Web Services 的 **preserveBootstrapIgnition** 参数已弃用。您可以使用 **bestEffortDeleteIgnition** 参数替代。

1.5.2. 删除的功能

1.5.2.1. 弃用的磁盘分区配置方法

SiteConfig 自定义资源(CR)中的 **nodes.diskPartition** 部分在 OpenShift Container Platform 4.16 发行版本中已弃用。此配置已被 **ignitionConfigOverride** 方法替代，它为任何用例创建磁盘分区提供了一种更灵活的方法。

如需更多信息，请参阅使用 SiteConfig 配置磁盘分区。

1.5.2.2. 删除平台 Operator 和普通捆绑包（技术预览）

OpenShift Container Platform 4.16 删除了平台 Operator （技术预览）和普通捆绑包（技术预览），这是 Operator Lifecycle Manager (OLM) 1.0 （技术预览）模型。

1.5.2.3. 已删除用于 BMC 寻址的 Dell iDRAC 驱动程序

OpenShift Container Platform 4.16 支持与 Dell 服务器的基板管理控制器(BMC)寻址，如 Dell iDRAC 的 BMC 寻址 中所述。具体来说，它支持 **idrac-virtualmedia**、**redfish** 和 **ipmi**。在以前的版本中，包含 **idrac**，但不记录或不支持。在 OpenShift Container Platform 4.16 中，删除了 **idrac**。

1.5.2.4. 用于核心平台监控的专用服务监控器

在这个版本中，删除了用于核心平台监控的专用服务监控功能。您无法再在 **openshift-monitoring** 命名空间中的 **cluster-monitoring-config** 配置映射对象中启用此功能。要替换此功能，Prometheus 功能已被改进，以确保警报和时间聚合准确。这个改进的功能默认处于活动状态，它使专用服务监控器功能过时。

1.5.2.5. 用于核心平台监控的 Prometheus Adapter

在这个版本中，核心平台监控的 Prometheus Adapter 组件已被删除。它已被新的 Metrics Server 组件替代。

1.5.2.6. 已删除 MetalLB AddressPool 自定义资源定义(CRD)

对于多个版本，MetalLB **AddressPool** 自定义资源定义(CRD)已被弃用。但是，在此发行版本中，CRD 会被完全删除。配置 MetalLB 地址池的唯一方法是使用 **IPAddressPools** CRD。

1.5.2.7. Service Binding Operator 文档已删除

在这个版本中，Service Binding Operator (SBO)的文档已被删除，因为这个 Operator 不再被支持。

1.5.2.8. AliCloud CSI Driver Operator 不再被支持

OpenShift Container Platform 4.16 不再支持 AliCloud Container Storage Interface (CSI) Driver Operator。

1.5.2.9. 从 Kubernetes 1.29 中删除 Beta API

Kubernetes 1.29 删除了以下已弃用的 API，因此您必须迁移清单和 API 客户端以使用适当的 API 版本。有关迁移删除 API 的更多信息，请参阅 Kubernetes 文档。

表 1.17. 从 Kubernetes 1.29 中删除的 API

资源	删除的 API	迁移到	主要变化
FlowSchema	**flowcontrol.apiserver.k8s.io/v1beta2**	**flowcontrol.apiserver.k8s.io/v1** 或 **flowcontrol.apiserver.k8s.io/v1beta3**	否

资源	删除的 API	迁移到	主要变化
PriorityLevelConfiguration	flowcontrol.apiserver.k8s.io/v1beta2	flowcontrol.apiserver.k8s.io/v1 或 flowcontrol.apiserver.k8s.io/v1beta3	是

1.6. 程序错误修复

API 服务器和客户端

- 在以前的版本中，在升级的集群中，临时和 **csi** 卷没有正确添加到安全性上下文约束(SCC)中。**在这个版本中，升级的集群中的 SCC 会被正确更新，使其具有 临时和 csi 卷。(OCPBUGS-33522)**

- **在以前的版本中，ServiceAccounts 资源无法用于启用了 ImageRegistry 能力的集群的 OAuth 客户端。在这个版本中，这个问题已被解决。(OCPBUGS-30319)**

- **在以前的版本中，当使用空安全上下文创建 pod 且您可以访问所有安全性上下文约束(SCC)时，pod 会收到 anyuid SCC。在 ovn-controller 组件向 pod 添加标签后，会为 SCC 选择重新管理 pod，其中 pod 收到了一个升级的 SCC，如 privileged。在这个版本中，这个问题已被解决，pod 不会重新用于 SCC 选择。(OCPBUGS-11933)**

- **在以前的版本中，hostmount-anyuid 安全性上下文约束(SCC)没有内置集群角色，因为 SCC 的名称在集群角色中被错误地命名为 hostmount。在这个版本中，集群角色中的 SCC 名称被正确更新为 hostmount-anyuid，因此 hostmount-anyuid SCC 现在具有可正常工作的集群角色。(OCPBUGS-33184)**

- **在以前的版本中，在 OpenShift Container Platform 4.7 之前创建的集群有几个类型为 SecretTypeTLS 的 secret。升级到 OpenShift Container Platform 4.16 后，这些 secret 会被删除并重新创建，类型为 kubernetes.io/tls。此移除可能会导致竞争条件，并且机密的内容可能会丢失。在这个版本中，secret 类型更改会自动发生，在 OpenShift Container Platform 4.7 之前创建的集群可以升级到 4.16，而不会丢失这些 secret 的内容。(OCPBUGS-31384)**

- **在以前的版本中，一些 Kubernetes API 服务器事件没有正确的时间戳。在这个版本中，Kubernetes API 服务器事件具有正确的时间戳。(OCPBUGS-27074)**

- **在以前的版本中，Kubernetes API Server Operator 会尝试删除 OpenShift Container Platform 4.13 中删除的 Prometheus 规则，以确保它已被删除。这会导致每几分钟后在审计日**

志中删除信息失败。在这个版本中，Kubernetes API Server Operator 不再尝试删除此不存在的规则，在审计日志中没有更多删除信息。(OCPBUGS-25894)

裸机硬件置备

- 在以前的版本中，Redfish 的较新版本使用 Manager 资源弃用 RedFish Virtual Media API 的统一资源标识符 (URI)。这会导致任何使用较新的 Redfish URI for Virtual Media 的硬件不会被置备。在这个版本中，Ironic API 标识要为 RedFish Virtual Media API 部署的正确 Redfish URI，以便可以置备依赖于已弃用或更新的 URI 的硬件。(OCPBUGS-30171)

- 在以前的版本中，Bare Metal Operator (BMO)没有使用领导锁定来控制传入和传出 Operator pod 流量。OpenShift Deployment 对象包含新的 Operator pod 后，新 pod 与系统资源（如 ClusterOperator 状态）竞争，这会终止任何传出的 Operator pod。这个问题也会影响没有包括任何裸机节点的集群。在这个版本中，BMO 包括一个领导锁定来管理新的 pod 流量，这个修复解决了竞争的 pod 问题。(OCPBUGS-25766)

- 在以前的版本中，当在安装开始前尝试删除 BareMetalHost 对象时，metal3 Operator 会尝试创建 PreprovImage 镜像。创建此镜像的过程会导致 BareMetalHost 对象在特定进程中仍然存在。在这个版本中，在这种情况下添加了一个例外，以便在不影响正在运行的进程的情况下删除 BareMetalHost 对象。(OCPBUGS-33048)

- 在以前的版本中，HPEt Packard Enterprise (HPE) Lights Out (iLO) 5 在 Hewlett Packard Enterprise (HPE) Lights Out (iLO) 5 上下文中的 Redfish 虚拟介质被禁止进行裸机压缩，以解决不同的硬件模型中的其他不相关的问题。这会导致每个 iLO 5 裸机机器中缺少 FirmwareSchema 资源。每台机器都需要压缩从 Redfish Baseboard Management Controller (BMC) 端点获取消息 registry。在这个版本中，每个需要 FirmwareSchema 资源的 iLO 5 裸机机器都没有强制禁用压缩。(OCPBUGS-31104)

- 在以前的版本中，inspector.ipxe 配置文件使用 IRONIC_IP 变量，它不会考虑 IPv6 地址，因为它们有括号。因此，当用户提供不正确的 boot_mac_address 时，i iPXE fell 返回到 inspector.ipxe 配置文件，该文件提供了格式不正确的 IPv6 主机标头，因为它不包含括号。在这个版本中，inspector.ipxe 配置文件已更新为使用 IRONIC_URL_HOST 变量，该变量用于 IPv6 地址并解决这个问题。(OCPBUGS-22699)

- 在以前的版本中，Ironic Python Agent 假设所有服务器磁盘在尝试擦除磁盘时具有 512 字节扇区大小。这会导致磁盘擦除失败。在这个版本中，Ironic Python Agent 检查磁盘扇区大小，并为磁盘中断具有单独的值，以便磁盘擦除成功。(OCPBUGS-31549)

Builds

- 在以前的版本中，从早期版本升级到 4.16 的集群仍然允许未经身份验证的 Webhook 触发构建。在这个版本中，新集群需要验证构建 Webhook。除非集群管理员允许命名空间或集群中的

未经身份验证的 Webhook，否则不会由未经身份验证的 Webhook 触发构建。(OCPBUGS-33378)

- 在以前的版本中，如果开发人员或集群管理员将小写环境变量名称用于代理信息，则这些环境变量会传送到构建输出容器镜像中。在运行时，代理设置处于活跃状态，必须取消设置。在这个版本中，*_PROXY 环境变量的小写版本无法泄漏构建的容器镜像。现在，buildDefaults 仅在为构建过程创建的构建和设置期间保留，仅在推送 registry 中的镜像前删除。(OCPBUGS-34825)

Cloud Compute

- 在以前的版本中，Cloud Controller Manager (CCM) Operator 在 Google Cloud Platform (GCP)上使用预定义角色，而不是粒度权限。在这个版本中，CCM Operator 被更新为在 GCP 集群上使用粒度权限。(OCPBUGS-26479)

- 在以前的版本中，安装程序会填充 VMware vSphere control plane 机器集自定义资源(CR)的 spec.template.spec.providerSpec.value 部分中的 network.devices、template 和 workspace 字段。这些字段应该在 vSphere 故障域中设置，且安装程序填充它们会导致意外的行为。更新这些字段不会触发对 control plane 机器的更新，并在删除 control plane 机器集时清除这些字段。

  在这个版本中，安装程序被更新，不再填充故障域配置中包含的值。如果在故障域配置中没有定义这些值，例如，从早期版本升级到 OpenShift Container Platform 4.16 的集群，则会使用安装程序定义的值。(OCPBUGS-32947)

- 在以前的版本中，与重新引导机器关联的节点会短暂处于 Ready=Unknown 状态，这会触发 Control Plane Machine Set Operator 中的 UnavailableReplicas 条件。此条件导致 Operator 进入 Available=False 状态并触发警报，因为该状态表示需要立即管理员干预的非功能组件。重新引导时，不应为简短和预期的未提供警报触发此警报。在这个版本中，添加了节点未就绪的宽限期，以避免触发不必要的警报。(OCPBUGS-34970)

- 在以前的版本中，在机器创建过程中获取 bootstrap 数据（如临时失败）无法连接到 API 服务器，从而导致机器进入终端失败状态。在这个版本中，在机器创建过程中无法获取 bootstrap 数据，会无限期重试，直到最终成功为止。(OCPBUGS-34158)

- 在以前的版本中，当删除处于错误状态的服务器时，Machine API Operator 会 panicked，因为它没有传递端口列表。在这个版本中，删除处于 ERROR 状态的机器不会使控制器崩溃。(OCPBUGS-34155)

- 在以前的版本中，集群自动扩展的可选内部功能会在未实现时重复日志条目。这个问题已在本发行版本中解决。(OCPBUGS-33932)

- 在以前的版本中，如果 control plane 机器集在 VMware vSphere 集群上安装使用没有路径的模板，则 Control Plane Machine Set Operator 会拒绝修改或删除 control plane 机器集自定义资源(CR)。在这个版本中，Operator 允许 control plane 机器集定义中的 vSphere 模板名称。(OCPBUGS-32295)

- 在以前的版本中，因为没有配置基础架构资源，当尝试更新 VMware vSphere 集群时，Control Plane Machine Set Operator 会崩溃。在这个版本中，Operator 可以处理这种情况，以便集群更新可以进行。(OCPBUGS-31808)

- 在以前的版本中，当用户创建带有污点的计算机器集时，他们可以选择不指定 Value 字段。如果不指定此字段，会导致集群自动扩展崩溃。在这个版本中，集群自动扩展被更新以处理空 Value 字段。(OCPBUGS-31421)

- 在以前的版本中，IPv6 服务在 RHOSP 云供应商中错误地标记为内部，因此无法在 OpenShift Container Platform 服务间共享 IPv6 负载均衡器。在这个版本中，IPv6 服务没有标记为内部，允许在使用有状态 IPv6 地址的服务间共享 IPv6 负载均衡器。在这个版本中，负载均衡器可以使用服务的 loadBalancerIP 属性中定义的有状态 IPv6 地址。(OCPBUGS-29605)

- 在以前的版本中，当 control plane 机器标记为 unready 且由修改 control plane 机器集启动更改时，未就绪机器会被预先删除。这种预防操作导致同时替换多个索引。在这个版本中，当索引中只有一个机器时，control plane 机器集不会删除机器。这个更改可防止预实施更改，并防止一次替换多个索引。(OCPBUGS-29249)

- 在以前的版本中，到 Azure API 的连接有时会挂起最多 16 分钟。在这个版本中，引入了一个超时以防止挂起 API 调用。(OCPBUGS-29012)

- 在以前的版本中，Machine API IBM Cloud 控制器没有集成 klogr 软件包中的完整日志记录选项。因此，控制器在 Kubernetes 版本 1.29 及更高版本中崩溃。在这个版本中，包括了缺少的选项，并解决了这个问题。(OCPBUGS-28965)

- 在以前的版本中，Cluster API IBM Power Virtual Server 控制器 pod 在不支持的 IBM Cloud 平台上启动。这会导致控制器 pod 处于创建阶段。在这个版本中，集群会检测 IBM Power Virtual Server 和 IBM Cloud 之间的区别。然后，集群只在支持的平台中启动。(OCPBUGS-28539)

- 在以前的版本中，因为解析错误，机器自动扩展无法直接考虑计算机器集 spec 的任何污点。当依赖计算机器集污点从零扩展时，这可能会导致不必要的扩展行为。这个问题已在此发行版本中解决，机器自动扩展现在可以正确扩展，并识别阻止工作负载调度的污点。(OCPBUGS-27509)

- 在以前的版本中，在 Microsoft Azure 区域上运行的机器集，没有可用区支持总是为 Spot 实例创建 AvailabilitySets 对象。此操作会导致 Spot 实例失败，因为实例不支持可用性集。在这个版本中，机器集不会为在非zonal 配置的区域中运行的 Spot 实例创建 AvailabilitySets 对象。(OCPBUGS-25940)

- 在以前的版本中，在 OpenShift Container Platform 4.14 中从 kubelet 中删除提供镜像凭证的代码会导致从 Amazon Elastic Container Registry (ECR)拉取镜像在没有指定的 pull secret 的情况下失败。此发行版本包括一个单独的凭证供应商，它为 kubelet 提供 ECR 凭证。(OCPBUGS-25662)

- 在以前的版本中，Azure 负载均衡器的默认虚拟机类型从 Standard 改为 VMSS，但服务类型负载均衡器代码无法将标准虚拟机附加到负载均衡器。在这个版本中，默认虚拟机类型会被恢复，以保持与 OpenShift Container Platform 部署兼容的。(OCPBUGS-25483)

- 在以前的版本中，OpenShift Container Platform 不会将集群名称包含在由 OpenStack Cloud Controller Manager 创建的 RHOSP 负载均衡器资源的名称中。当 LoadBalancer 服务在单个 RHOSP 项目中运行的多个集群中具有相同的名称时，这会导致问题。在这个版本中，集群名称包含在 Octavia 资源的名称中。当从以前的集群版本升级时，负载均衡器会被重命名。新名称遵循模式 kube_service_<cluster-name>_<namespace>_<service-name> 而不是 kube_service_kubernetes_<namespace>_<service-name>。(OCPBUGS-13680)

- 在以前的版本中，当您同时创建或删除服务对象的大量卷时，服务控制器可以按顺序处理每个服务，这会减慢。这会导致服务控制器和对象的积压问题出现简短的超时问题。在这个版本中，服务控制器可以同时处理最多 10 个服务对象，以减少积压和超时问题。(OCPBUGS-13106)

- 在以前的版本中，获取节点名称的逻辑不会考虑从 AWS 元数据服务返回的主机名的多个值。当为 VPC 动态主机配置协议(DHCP)选项配置了多个域时，此主机名可能会返回多个值。多个值之间的空间会导致逻辑崩溃。在这个版本中，逻辑被更新为只使用第一个返回的主机名作为节点名称。(OCPBUGS-10498)

- 在以前的版本中，Machine API Operator 在 Microsoft Azure 集群上请求不必要的 virtualMachines/extensions 权限。这个版本删除了不必要的凭证请求。(OCPBUGS-29956)

Cloud Credential Operator

- 在以前的版本中，Cloud Credential Operator (CCO)缺少在 Microsoft Azure 上创建私有集群所需的一些权限。这些缺少的权限会阻止使用 Microsoft Entra Workload ID 安装 Azure 私有集群。此发行版本包括缺少的权限，并使用 Workload ID 启用 Azure 私有集群安装。(OCPBUGS-25193)

在以前的版本中，一个程序错误会导致 Cloud Credential Operator (CCO)在指标中报告不正确的模式。即使集群处于默认模式，但指标会报告它处于凭证删除模式。在这个版本中，使用 live 客户端来代替缓存的客户端，以便它能够获取 root 凭证，CCO 不再在指标中报告不正确的模式。(OCPBUGS-26488)

- 在以前的版本中，使用 Microsoft Entra Workload ID 的 OpenShift Container Platform 集群上的 Cloud Credential Operator 凭证模式指标使用手动模式报告。在这个版本中，使用 Workload ID 的集群会被更新为使用 pod 身份的手动模式。(OCPBUGS-27446)

- 在以前的版本中，在裸机集群中创建 Amazon Web Services (AWS) root secret 会导致 Cloud Credential Operator (CCO) pod 崩溃。这个问题已在本发行版本中解决。(OCPBUGS-28535)

- 在以前的版本中，从使用 mint 模式的 Cloud Credential Operator (CCO)的 Google Cloud Platform (GCP)集群中删除 root 凭证会导致 CCO 在大约一小时后降级。在降级状态中，CCO 无法管理集群中的组件凭证 secret。这个问题已在本发行版本中解决。(OCPBUGS-28787)

- 在以前的版本中，在 Amazon Web Services (AWS)上安装时，Cloud Credential Operator (CCO)会检查是否有不存在的 s3:HeadBucket 权限。当 CCO 无法找到此权限时，它会被视为为 mint 模式提供的凭证不足。在这个版本中，CCO 不再检查不存在的权限。(OCPBUGS-31678)

Cluster Version Operator

- 此发行版本扩展了 ClusterOperatorDown 和 ClusterOperatorDegraded 警报，以覆盖 ClusterVersion 条件，并为 Available=False (ClusterOperatorDown)和 Failing=True (ClusterOperatorDegraded)发送警报。在以前的版本中，这些警报只涵盖 ClusterOperator 条件。(OCPBUGS-9133)

- 在以前的版本中，Cluster Version Operator (CVO)在 OpenShift Container Platform 4.15.0、4.14.0、4.13.17 和 4.12.43 中引入的更改会导致风险评估失败，阻止 CVO 获取新的更新建议。当风险评估失败时，这个错误会导致 CVO 过度忽略更新建议服务。在这个版本中，CVO 继续轮询更新建议服务，无论是否成功评估更新风险以及问题是否已解决。(OCPBUGS-25708)

开发人员控制台

- 在以前的版本中，当以 create serverless 表单创建无服务器功能时，不会创建 BuilldConfig。在这个版本中，如果没有安装 Pipelines Operator，则不会为特定资源创建管道资源，或者在创建无服务器功能时没有添加管道，它将按预期创建 BuildConfig。(OCPBUGS-34143)

-

在以前的版本中，在安装 Pipelines Operator 后，Pipeline 模板需要一些时间来在集群中可用，但用户仍然可以创建部署。在这个版本中，如果没有选择的资源，Import from Git 页面上的 Create 按钮会被禁用。(OCPBUGS-34142)

- 在以前的版本中，Topology 页面中的最大节点数量被设置为 100。提供了持久性警报 "Loading 的时间比预期要长。在这个版本中，节点的限制增加到 300。(OCPBUGS-32307)

- 在这个版本中，在创建 ServiceBinding、绑定一个组件或当前命名空间中发现 ServiceBinding 列表 ,ServiceBinding 详情,Add, 和 Topology 页时，用于通知 Service Bindings 已弃用，并显示 OpenShift Container Platform 4.15。(OCPBUGS-32222)

- 在以前的版本中，如果 chart 名称不同，Helm 插件索引视图不会显示与 Helm CLI 相同的 chart 数量。在这个版本中，Helm 目录会查找 chart.openshift.io/name 和 charts.openshift.io/provider，以便所有版本都分组到单个目录标题中。(OCPBUGS-32059)

- 在以前的版本中，TaskRun 状态不会在 TaskRun 详情页面上的 TaskRun 名称 旁 显示。在这个版本中，TaskRun 状态位于页面标题中的 TaskRun 名称旁边。(OCPBUGS-31745)

- 在以前的版本中，当将 resources 字段添加到有效负载时，在 Pipeline 中添加参数时会出现错误，因为资源已弃用。在这个版本中，resources 字段已从有效负载中删除，您可以在 Pipeline 中添加参数。(OCPBUGS-31082)

- 此发行版本更新了 OpenShift Pipelines 插件，以支持自定义资源定义(CRD) ClusterTriggerBinding、TriggerTemplate 和 EventListener 的最新 Pipeline Trigger API 版本。(OCPBUGS-30958)

- 在以前的版本中，CustomTasks 无法识别或处于 Pending 状态。在这个版本中，CustomTasks 可以从 Pipelines List 和 Details 页面轻松识别。(OCPBUGS-29513)

- 在以前的版本中，如果有一个带有镜像标签的构建输出镜像，则 Output Image 链接不会重定向到正确的 ImageStream 页面。在这个版本中，这个问题已通过在链接中添加标签的情况下为 ImageStream 页面生成 URL 来解决。(OCPBUGS-29355)

- 在以前的版本中，因为指定资源的 API 版本的最新更新，BuildRun 日志在 BuildRun 页面的 Logs 选项卡中不可见。在这个版本中，TaskRuns 的日志被添加到 Builds Operator 的 BuildRun 页面的 Logs 选项卡中。(OCPBUGS-27473)

-

在以前的版本中，设置 scale bound 值的注解被设置为 autoscaling.knative.dev/maxScale 和 autoscaling.knative.dev/minScale。在这个版本中，设置扩展绑定值的注解会更新为 autoscaling.knative.dev/min-scale 和 autoscaling.knative.dev/max-scale，以确定可在任何给定时间提供应用程序的最小和最大副本数。您可以为应用设置规模绑定，以帮助防止冷启动和控制计算成本。(OCPBUGS-27469)

- 在以前的版本中，Tekton Results API 中的 PipelineRuns 的 Log 标签页永远不会完成载入。在这个版本中，此标签页为从 Kubernetes API 或 Tekton Results API 加载的 PipelineRuns 完全完整。(OCPBUGS-25612)

- 在以前的版本中，没有显示指示来区分从 Kubernetes API 或 Tekton Results API 加载的 PipelineRuns。在这个版本中，PipelineRun 列表 和 详情页中 有一个小归档图标，用于区分从 Kubernetes API 或 Tekton Results API 加载的 PipelineRuns。(OCPBUGS-25396)

- 在以前的版本中，在 PipelineRun list 页面中，所有 TaskRuns 都会根据 pipelineRun 名称获取并分离。在这个版本中，TaskRuns 只会为 Failed 和 Cancelled PipelineRun 获取。另外，还添加了一个缓存机制来获取与 Failed 和 Cancelled PipelineRuns 关联的 PipelineRuns 和 TaskRuns。(OCPBUGS-23480)

- 在以前的版本中，Topology 视图中没有虚拟机节点和其它非VM 节点间的视觉连接器。在这个版本中，视觉连接器位于虚拟机节点和非VM 节点间。(OCPBUGS-13114)

etcd Cluster Operator

- 在以前的版本中，bootstrap 中使用的 wait-for-ceo 命令不会报告一些失败模式的错误。在这个版本中，如果 cmd 在错误情况下退出，则 bootkube 脚本中可以看到这些错误消息。(OCPBUGS-33495)

- 在以前的版本中，etcd Cluster Operator 在 pod 健康检查过程中输入 panic 状态，这会导致对 etcd 集群的请求失败。在这个版本中，这个问题已被解决，不再发生这些 panic 的情况。(OCPBUGS-27959)

- 在以前的版本中，etcd Cluster Operator 会错误地将非运行的控制器识别为死锁，这会导致不必要的 pod 重启。在这个版本中，这个问题已被解决，Operator 会将一个非运行的控制器标记为不健康 etcd 成员，而无需重启 pod。(OCPBUGS-30873)

托管 control plane

- 在以前的版本中，当您在托管集群中使用 Other 网络类型时，Multus Container Network Interface (CNI) 需要批准 证书签名请求(CSR)。只有在网络类型为 Other 且设置为 Calico 时，才会设置适当的基于角色的访问控制(RBAC)规则。因此，当网络类型是 Other 且设置为 Cilium

时，CSR 不会被批准。在这个版本中，为所有有效的网络类型设置了正确的 RBAC 规则，在使用 Other 网络类型时，现在会正确配置 RBAC。(OCPBUGS-26977)

- 在以前的版本中，Amazon Web Services (AWS)策略问题会阻止 Cluster API Provider AWS 检索所需的域信息。因此，使用自定义域安装 AWS 托管的集群会失败。在这个版本中，策略问题已解决。(OCPBUGS-29391)

- 在以前的版本中，在断开连接的环境中，HyperShift Operator 会忽略 registry 覆盖。因此，对节点池的更改会被忽略，节点池会遇到错误。在这个版本中，元数据检查器在 HyperShift Operator 协调过程中可以正常工作，并正确填充覆盖镜像。(OCPBUGS-34773)

- 在以前的版本中，HyperShift Operator 没有使用 RegistryOverrides 机制来检查内部 registry 中的镜像。在这个版本中，元数据检查器在 HyperShift Operator 协调过程中可以正常工作，并正确填充 OverrideImages。(OCPBUGS-32220)

- 在以前的版本中，Red Hat OpenShift Cluster Manager 容器没有正确的传输层安全(TLS)证书。因此，镜像流无法用于断开连接的部署。在这个版本中，TLS 证书作为投射卷添加。(OCPBUGS-34390)

- 在以前的版本中，KAS pod 中的 azure-kms-provider-active 容器在 Dockerfile 中使用 shell 格式的 entrypoint 语句。因此，容器会失败。要解决这个问题，请使用 entrypoint 语句的 exec 表单。(OCPBUGS-33940)

- 在以前的版本中，konnectivity-agent 守护进程集使用 ClusterIP DNS 策略。因此，当 CoreDNS 停机时，data plane 上的 konnectivity-agent pod 无法解析代理服务器 URL，它们可能无法在 control plane 中的 konnectivity-server 中失败。在这个版本中，konn ectivity-agent 守护进程集被修改为使用 dnsPolicy: Default。konnectivity-agent 使用主机系统 DNS 服务来查找代理服务器地址，且不再依赖于 CoreDNS。(OCPBUGS-31444)

- 在以前的版本中，无法查找资源会导致重新创建失败。因此，很多 409 响应代码被记录在 Hosted Cluster Config Operator 日志中。在这个版本中，特定资源被添加到缓存中，以便 Hosted Cluster Config Operator 不会尝试重新创建现有资源。(OCPBUGS-23228)

- 在以前的版本中，托管集群中缺少 pod 安全漏洞警报。在这个版本中，警报添加到托管集群。(OCPBUGS-31263)

- 在以前的版本中，在断开连接的环境中托管的集群中的 recycler-pod 模板指向 quay.io/openshift/origin-tools:latest。因此，回收 Pod 无法启动。在这个版本中，recycler

pod 镜像指向 OpenShift Container Platform 有效负载引用。(OCPBUGS-31398)

- 在这个版本中，在断开连接的部署中，HyperShift Operator 会从管理集群接收新的 ImageContentSourcePolicy (ICSP)或 ImageDigestMirrorSet (IDMS)，并将它们添加到 HyperShift Operator 和每个协调循环中的 Control Plane Operator 中。对 ICSP 或 IDMS 的更改会导致重启 control-plane-operator pod。(OCPBUGS-29110)

- 在这个版本中，ControllerAvailabilityPolicy 设置会在设置后变为不可变。不支持在 SingleReplica 和 HighAvailability 之间更改。(OCPBUGS-27282)

- 在这个版本中，machine-config-operator 自定义资源定义(CRD)被重命名，以确保在托管 control plane 中正确省略资源。(OCPBUGS-34575)

- 在这个版本中，为托管的 control plane 保存在 kube-apiserver、openshift-apiserver、openshift -apiserver pod 中的审计日志文件的大小会减小。(OCPBUGS-31106)

- 在以前的版本中，Hypershift Operator 没有使用 RegistryOverrides 机制来检查内部 registry 中的镜像。在这个版本中，元数据检查器在 Hypershift Operator 协调过程中可以正常工作，并正确填充 OverrideImages。(OCPBUGS-29494)

镜像 Registry

- 在以前的版本中，在导入镜像流标签后，ImageContentSourcePolicy (ICSP)自定义资源 (CR)无法与 ImageDigestMirrorSet (IDMS)或 ImageTagMirrorSet (ITMS) CR 共存。OpenShift Container Platform 选择 ICSP 而不是其他 CR 类型。在这个版本中，这些自定义资源可以共存，因此在导入镜像流标签后，OpenShift Container Platform 可以选择所需的 CR。(OCPBUGS-30279)

- 在以前的版本中，当命令创建新标签时，oc tag 命令不会验证标签名称。从带有无效名称的标签创建镜像后，podman pull 命令将失败。在这个版本中，验证步骤会检查新的标签是否有无效名称，现在可以删除具有无效名称的现有标签，因此这个问题不再存在。(OCPBUGS-25703)

- 在以前的版本中，Image Registry Operator 维护自己的 IBM Power® Virtual Server 区域列表，因此任何新区域都不会添加到列表中。在这个版本中，Operator 依赖于一个外部库来访问区域，以便它能够支持新区域。(OCPBUGS-26767)

- 在以前的版本中，镜像 registry Microsoft Azure path-fix 作业错误地需要存在 AZURE_CLIENT_ID 和 TENANT_CLIENT_ID 参数才能正常工作。这会导致有效的配置抛出错

误消息。在这个版本中，将检查添加到 Identity and Access Management (IAM)服务帐户密钥中，以验证是否需要这些参数，因此集群升级操作不再失败。(OCPBUGS-32328)

- 在以前的版本中，镜像 registry 不支持 Amazon Web Services (AWS) 区域 ca-west-1。在这个版本中，镜像 registry 可以部署到此区域中。(OCPBUGS-29233)

- 在以前的版本中，当 Image Registry Operator 配置中将 virtualHostedStyle 参数设置为 regionEndpoint 时，镜像 registry 会忽略虚拟托管的风格配置。在这个版本中，这个问题已被解决，以便使用新的上游分发配置强制路径风格，而不是只使用下游版本（虚拟托管风格）。(OCPBUGS-34166)

- 在以前的版本中，当在启用了 service-endpoint 覆盖的 IBM Power® Virtual Server 上运行 OpenShift Container Platform 集群时，Cloud Credential Operator (CCO) Operator 将忽略覆盖服务端点。在这个版本中，CCO Operator 不再忽略覆盖服务端点。(OCPBUGS-32491)

- 在以前的版本中，Image Registry Operator 忽略了端点服务集群级别覆盖，使得在 IBM Cloud® 断开连接的环境中配置集群比较困难。这个问题只存在于安装程序置备的基础架构中。在这个版本中，Image Registry Operator 不再忽略这些集群级别的覆盖。(OCPBUGS-26064)

安装程序

- 在以前的版本中，在 Google Cloud Platform (GCP)上安装带有无效配置的三节点集群会失败，并显示一个 panic 错误，因为没有报告失败的原因。在这个版本中，安装程序会验证安装配置，以便在 GCP 上成功安装三节点集群。(OCPBUGS-35103)

- 在以前的版本中，如果 pull secret 在密码中包含冒号，则使用 Assisted Installer 安装会失败。在这个版本中，在密码中包含冒号的 pull secret 不会导致 Assisted Installer 失败。(OCPBUGS-34400)

- 在以前的版本中，monitor-add-nodes 命令用于监控将节点添加到基于代理的集群的过程，因为权限错误而无法运行。在这个版本中，命令在具有权限的正确目录中运行。(OCPBUGS-34388)

- 在以前的版本中，在不警告用户的情况下会修剪较长的集群名称。在这个版本中，安装程序会在修剪长集群名称时警告用户。(OCPBUGS-33840)

- 在以前的版本中，当安装集群时，即使 install-config.yaml 中禁用了 Ingress 功能，也会启用 Ingress 功能，因为它是必需的。在这个版本中，如果在 install-config.yaml 中禁用 Ingress

功能，安装程序会失败。(OCPBUGS-33794)

- 在以前的版本中，OpenShift Container Platform 不会对在 ca-west-1 中安装的集群执行配额检查，一个 Amazon Web Services (AWS)区域。在这个版本中，在这个区域中可以正确地强制实施配额。(OCPBUGS-33649)

- 在以前的版本中，安装程序有时可能会无法检测到 OpenShift Container Platform API 不可用。通过增加 Microsoft Azure 安装中的 bootstrap 节点的磁盘大小来解决额外的错误。在这个版本中，安装程序可以正确地检测到 API 是否可用。(OCPBUGS-33610)

- 在以前的版本中，Microsoft Azure 集群上的 control plane 节点使用 只读 缓存。在这个版本中，Microsoft Azure control plane 节点使用 ReadWrite 缓存。(OCPBUGS-33470)

- 在以前的版本中，当使用配置了代理安装基于代理的集群时，如果代理配置包含以百分比符号(%)开头的字符串，则安装会失败。在这个版本中，安装程序会正确地验证此配置文本。(OCPBUGS-33024)

- 在以前的版本中，在 GCP 上安装可能会失败，因为安装程序尝试创建存储桶两次。在这个版本中，安装程序不再尝试创建存储桶两次。(OCPBUGS-32133)

- 在以前的版本中，罕见的时间问题可能会阻止所有 control plane 节点在安装过程中添加到基于代理的集群中。在这个版本中，所有 control plane 节点都成功重启，并在安装过程中添加到集群中。(OCPBUGS-32105)

- 在以前的版本中，当在断开连接的环境中使用基于代理的安装程序时，不必要的证书会添加到证书颁发机构(CA)信任捆绑包中。在这个版本中，CA 捆绑包 ConfigMap 仅包含用户明确指定的 CA。(OCPBUGS-32042)

- 在以前的版本中，当在 Amazon Web Services (AWS)上安装集群时，安装程序需要一个不存在的权限 s3:HeadBucket。在这个版本中，安装程序需要权限 s3:ListBucket 替代。(OCPBUGS-31813)

- 在以前的版本中，如果安装程序因为 SSH 连接问题而无法从 bootstrap 收集日志，它也不提供虚拟机(VM)串口控制台日志，即使它们已被收集。在这个版本中，安装程序会提供虚拟机串口控制台日志，即使与 bootstrap 机器的 SSH 连接失败。(OCPBUGS-30774)

- 在以前的版本中，当在带有静态 IP 地址的 VMware vSphere 上安装集群时，集群可能会因为

其他技术预览功能冲突而在没有静态 IP 地址的情况下创建 control plane 机器。在这个版本中，Control Plane Machine Set Operator 可以正确地管理 control plane 机器的静态 IP 分配。(OCPBUGS-29114)

- 在以前的版本中，当使用用户提供的 DNS 在 GCP 上安装集群时，安装程序仍然会尝试在 GCP DNS 网络中验证 DNS。在这个版本中，安装程序不会对用户提供的 DNS 执行这个验证。(OCPBUGS-29068)

- 在以前的版本中，当删除使用与非私有 IBM Cloud® 集群相同的域名的 IBM Cloud® 上的私有集群时，一些资源不会被删除。在这个版本中，当集群被删除时，所有私有集群资源都会被删除。(OCPBUGS-28870)

- 在以前的版本中，当使用代理安装集群时，带有在配置字符串中使用百分比符号(%)的字符字符串时，集群安装会失败。在这个版本中，安装程序会正确地验证包含 "%" 的代理配置字符串。(OCPBUGS-27965)

- 在以前的版本中，安装程序仍然允许使用 OpenShiftSDN 网络插件，即使它已被删除。在这个版本中，安装程序可以正确地使用这个网络插件安装集群。(OCPBUGS-27813)

- 在以前的版本中，当在 Amazon Web Services (AWS) Wavelengths 或 Local Zones 上安装集群到支持 Wavelengths 或 Local Zones 的区域时，安装会失败。在这个版本中，支持 Wavelengths 或 Local Zones 的区域可以成功安装。(OCPBUGS-27737)

- 在以前的版本中，当集群安装尝试使用与现有集群相同的集群名称和基域时，因为 DNS 记录设定冲突，安装会失败，删除第二个集群也会删除原始集群中的 DNS 记录集。在这个版本中，存储的元数据包含私有区名称而不是集群域，因此只从删除的集群中删除正确的 DNS 记录。(OCPBUGS-27156)

- 在以前的版本中，基于代理的安装的安装配置文件中配置的平台特定密码可能存在于 agent-gather 命令的输出中。在这个版本中，在 agent-gather 输出中会重新定义密码。(OCPBUGS-26434)

- 在以前的版本中，使用版本 4.15 或 4.16 安装的 OpenShift Container Platform 集群显示默认升级频道为 4.14 版本。在这个版本中，集群在安装后具有正确的升级频道。(OCPBUGS-26048)

- 在以前的版本中，当删除 VMware vSphere 集群时，一些 TagCategory 对象无法删除。在这个版本中，当集群被删除时，所有与集群相关的对象都会被正确删除。(OCPBUGS-25841)

- 在以前的版本中，当指定 baremetal 平台类型，但在 install-config.yaml 中禁用 baremetal 功能时，安装会在长时间超时后失败，且没有有用的错误。在这个版本中，安装程序会提供一个描述性错误，并在禁用 baremetal 功能时不会尝试裸机安装。(OCPBUGS-25835)

- 在以前的版本中，使用 Assisted Installer 在 VMware vSphere 上安装可能会因为阻止 VMware vSphere 正确初始化节点而失败。在这个版本中，VMware vSphere 上的 Assisted Installer 安装成功完成，并可使用所有节点初始化。(OCPBUGS-25718)

- 在以前的版本中，如果选择的虚拟机类型与 install-config.yaml 文件中指定的架构不匹配，安装会失败。在这个版本中，验证检查可确保在安装开始前匹配的架构。(OCPBUGS-25600)

- 在以前的版本中，如果指定了无效的 control plane 副本数量，基于代理的安装可能会失败，如 2。在这个版本中，安装程序强制实施为基于代理的安装指定 1 或 3 control plane 副本的要求。(OCPBUGS-25462)

- 在以前的版本中，当使用 control plane 机器集技术预览功能在 VMware vSphere 上安装集群时，生成的 control plane 机器集在其配置中有重复的故障域。在这个版本中，安装程序会使用正确的故障域创建 control plane 机器集。(OCPBUGS-25453)

- 在以前的版本中，在安装程序置备的安装前，所需的 iam:TagInstanceProfile 权限不会被验证，如果缺少 Identity and Access Management (IAM)权限，则会导致安装失败。在这个版本中，验证检查可确保在安装开始前包含权限。(OCPBUGS-25440)

- 在以前的版本中，安装程序不会阻止用户在禁用 Cloud Credential 功能的非裸机平台上安装集群，尽管需要它。在这个版本中，安装程序会生成错误，并防止安装禁用了 Cloud Credential 功能，但裸机平台上除外。(OCPBUGS-24956)

- 在以前的版本中，设置与实例类型支持的架构不同，会导致在创建某些资源后安装失败。在这个版本中，验证检查会验证实例类型是否与指定的架构兼容。如果构架不兼容，安装开始前过程会失败。(OCPBUGS-24575)

- 在以前的版本中，安装程序不会阻止用户在禁用 Cloud Controller Manager 的云供应商上安装集群，这会失败且没有有用的错误消息。在这个版本中，安装程序会生成一个错误，表示云平台上的安装需要 Cloud Controller Manager 功能。(OCPBUGS-24415)

- 在以前的版本中，因为 IBM Cloud® API 的意外结果，安装程序可能无法删除在 IBM Cloud® 上安装的集群。在这个版本中，安装程序可可靠地删除在 IBM Cloud® 上安装的集群。

(OCPBUGS-20085)

- 在以前的版本中，安装程序不会强制从启用了 FIPS 的 Red Hat Enterprise Linux (RHEL)主机安装 FIPS 的集群的要求。在这个版本中，安装程序会强制实施 FIPS 要求。(OCPBUGS-15845)

- 在以前的版本中，install-config.yaml 文件中设置的代理信息不会应用到 bootstrap 过程。在这个版本中，代理信息会应用到 bootstrap ignition 数据，然后应用到 bootstrap 机器。(OCPBUGS-12890)

- 在以前的版本中，当 IBM Power® 虚拟服务器平台没有动态主机配置协议(DHCP)网络名称时，DHCP 资源不会被删除。在这个版本中，检查会查找具有 ERROR 状态的任何 DHCP 资源，并删除它们，以便不再出现这个问题。(OCPBUGS-35224)

- 在以前的版本中，当使用 Cluster API 在安装程序置备的基础架构上创建 IBM Power® Virtual Server 集群时，负载均衡器会变得忙碌和停滞。在这个版本中，您可以使用 PollUntilContextCancel 循环中的 'AddIPToLoadBalancerPool' 命令来重启负载均衡器。(OCPBUGS-35088)

- 在以前的版本中，在启用了 FIPS 的节点的裸机平台上安装程序置备安装会导致安装失败。在这个版本中，这个问题已解决。(OCPBUGS-34985)

- 在以前的版本中，当在 IBM Power® Virtual Server 上为安装程序置备的安装创建安装配置时，如果管理员没有在 OpenShift CLI (oc)上输入命令，则调查将停止。该调查停止，因为 install-config 调查中没有设置默认区域。在这个版本中，这个问题已解决。(OCPBUGS-34728)

- 在以前的版本中，使用 SATA 硬件的固态驱动器(SSD)被识别为可移动。OpenShift Container Platform 的 Assisted Installer 报告没有找到合格的磁盘，安装会停止。在这个版本中，可移动的磁盘可进行安装。(OCPBUGS-34652)

- 在以前的版本中，由于 IPv6 连接检查失败，基于代理的安装会失败，即使节点间可能会建立 IPv6 连接。在这个版本中，这个问题已被解决。(OCPBUGS-31631)

- 在以前的版本中，由于一个编程错误，脚本会创建一个计算服务器组，并设置 control plane 的策略。因此，compute 组会忽略 install-config.yaml 文件的 serverGroupPolicy 属性。在这个版本中，计算机器池的 install-config.yaml 文件中设置的服务器组策略会在脚本流的安装中应用。(OCPBUGS-31050)

- 在以前的版本中，当配置使用 openshift-baremetal-install 二进制文件的基于代理的安装时，基于代理的安装程序会错误地尝试验证 libvirt 网络接口。这可能导致以下错误：

  > Platform.BareMetal.externalBridge: Invalid value: "baremetal": could not find interface "baremetal"

  在这个版本中，因为基于代理的安装方法不需要 libvirt，这个错误验证已被禁用，这个问题已解决。(OCPBUGS-30941)

- 在以前的版本中，将网络类型与基于 Open vSwitch 的软件定义型网络(SDN)或 Open Virtual Network (OVN)以外的双栈网络一起使用会导致验证错误。在这个版本中，这个问题已解决。(OCPBUGS-30232)

- 在以前的版本中，RHOSP 上的 user-provisioned-infrastructure 安装中的 nodePort 服务有一个关闭的 IPv6 端口范围，从而导致通过某些节点端口的流量被阻止。在这个版本中，在 security-group.yaml playbook 中添加了适当的安全组规则，从而解决了这个问题。(OCPBUGS-30154)

- 在以前的版本中，使用 openshift-install agent create cluster-manifests 命令生成的清单不会直接应用到 OpenShift Container Platform 集群，因为清单没有包括类型数据。在这个版本中，类型数据已添加到清单中。管理员现在可以应用清单来启动 Zero Touch Provisioning (ZTP)安装，该安装使用与基于代理的安装相同的设置。(OCPBUGS-29968)

- 在以前的版本中，在生成 aarch64 代理 ISO 时，aarch64 架构所需的文件被错误地重命名。在这个版本中，指定的文件不会被重命名。(OCPBUGS-28827)

- 在以前的版本中，当在 VMware vSphere 上安装集群时，因为安装程序无法从主机检索版本信息，如果 ESXi 主机处于维护模式，则安装会失败。在这个版本中，安装程序不会尝试从处于维护模式的 ESXi 主机检索版本信息，从而允许安装继续进行。(OCPBUGS-27848)

- 在以前的版本中，IBM Cloud® Terraform 插件错误地阻止在集群安装过程中使用非私有服务端点。在这个版本中，IBM Cloud® Terraform 插件在安装过程中支持非私有服务端点。(OCPBUGS-24473)

- 在以前的版本中，在 VMware vSphere 上安装集群需要指定数据存储的完整路径。在这个版本中，安装程序会接受数据存储的完整路径和相对路径。(OCPBUGS-22410)

在以前的版本中，当使用基于代理的安装程序安装 OpenShift Container Platform 集群时，安装可能会填充 Ignition 存储前大量清单，从而导致安装失败。在这个版本中，Ignition 存储已被增加，允许更多安装清单。(OCPBUGS-14478)

- 在以前的版本中，当 coreos-installer iso kargs show <iso > 命令用于 Agent ISO 文件时，输出无法正确显示嵌入在指定 ISO 中的内核参数。在这个版本中，命令输出可以正确地显示信息。(OCPBUGS-14257)

- 在以前的版本中，基于代理的安装会创建 ImageContentSource 对象而不是 ImageDigestSources，即使以前的对象已弃用。在这个版本中，基于代理的安装程序创建 ImageDigestSource 对象。(OCPBUGS-11665)

- 在以前的版本中，Power VS 的 destroy 功能存在问题，但不是所有资源都会如预期被删除。在这个版本中，这个问题已被解决。(OCPBUGS-29425)

Insights Operator

- Insights Operator 现在收集以下自定义资源的 openshift-monitoring 外部的实例：
  - kind: Prometheus Group: monitoring.coreos.com
  - kind: AlertManager Group: monitoring.coreos.com

  (OCPBUGS-35086)

Kubernetes Controller Manager

- 在以前的版本中，当使用前台删除级联策略删除 ClusterResourceQuota 资源时，删除将无法完成。在这个版本中，在使用前台级联策略时，ClusterResourceQuota 资源会被正确删除。(OCPBUGS-22301)

Machine Config Operator

- 在以前的版本中，MachineNode 对象没有使用正确的所有者创建。因此，Machine Node 对象无法垃圾回收，这意味着之前生成的，但不再有用，对象不会被删除。在这个版本中，在创建 MachineConfigNode 对象和过时的对象时，正确的所有者会被设置，用于垃圾回收。(OCPBUGS-30090)

-

在以前的版本中，nodeStatusUpdateFrequency 参数的默认值从 0s 改为 10s。这个更改意外会导致 nodeStatusReportFrequency 显著提高，因为值被链接到 nodeStatusReportFrequency 值。这会导致 control plane operator 和 API 服务器的 CPU 使用率高。在这个版本中，nodeStatusReportFrequency 值设置为 5m，这样可防止这个高 CPU 用量。(OCPBUGS-29713)

- 在以前的版本中，环境变量中的一个拼写错误会阻止脚本检测是否存在 node.env 文件。因此，每次重启时会覆盖 node.env 文件，从而导致 kubelet 主机名被修复。在这个版本中，排字错误已被修正。因此，对 node.env 的编辑现在在重启后会保留。(OCPBUGS-27261)

- 在以前的版本中，当 kube-apiserver 服务器证书颁发机构(CA)证书被轮转时，Machine Config Operator (MCO)无法正确响应和更新磁盘上的 kubelet kubeconfig。这意味着，kubelet 和节点上的一些 pod 最终无法与 APIserver 通信，从而导致节点进入 NotReady 状态。在这个版本中，MCO 可以正确地对更改做出反应，并更新磁盘上的 kubeconfig，以便在此轮转时与 APIServer 验证的通信可以继续，并重启 kubelet/MCDaemon pod。证书颁发机构的有效期为 10 年，因此，这个轮转应该很少发生，通常不会造成破坏。(OCPBUGS-25821)

- 在以前的版本中，当在集群中添加或从集群中删除新节点时，Machine Node (MCN)对象不会响应。因此，额外的 MCN 对象存在。在这个版本中，Machine Config Operator 会在添加或删除节点时删除并添加 MCN 对象。(OCPBUGS-24416)

- 在以前的版本中，nodeip-configuration 服务没有将日志发送到串口控制台，因此很难在网络不可用时调试问题，且无法访问该节点。在这个版本中，nodeip-configuration 服务会在没有网络访问节点时将输出记录到串行控制台，以便更轻松地进行调试。(OCPBUGS-19628)

- 在以前的版本中，当 MachineConfigPool 启用了 OnClusterBuild 功能且 configmap 使用无效的 imageBuilderType 更新时，Machine-config ClusterOperator 不会被降级。在这个版本中，Machine Config Operator (MCO) ClusterOperator 状态会在每次同步时验证 OnClusterBuild 输入，确保它们无效，ClusterOperator 会降级。 (OCPBUGS-18955)

- 在以前的版本中，当报告 机器配置未找到 错误时，没有足够的信息来排除并修正问题。在这个版本中，在 Machine Config Operator 中添加了一个警报和指标。因此，您有更多信息来排除故障并修复 机器配置未找到 错误。(OCPBUGS-17788)

- 在以前的版本中，在等待元数据服务可用时，vburn 服务用来在节点上设置主机名超时，从而导致使用 OVN-Kubernetes 部署时出现问题。现在，Afterburn 服务会等待元数据服务可用，从而解决了这些超时。(OCPBUGS-11936)

- 在以前的版本中，当从 MachineConfigPool 中删除节点时，Machine Config Operator (MCO)不会报告错误或删除节点。MCO 不支持在池中管理节点，且在节点被删除后没有指示节点

管理。在这个版本中，如果节点已从所有池中移除，MCO 现在会记录错误。(OCPBUGS-5452)

管理控制台

- 在以前的版本中，对于状态为 Completed 的 pod，不会显示 Debug 容器 链接。在这个版本中，链接会如预期显示。(OCPBUGS-34711)
- 在以前的版本中，由于 web 控制台中的 PatternFly 5 中的一个问题，因此不再可调整大小。在这个版本中，文本框可以再次调整大小。(OCPBUGS-34393)
- 在以前的版本中，web 控制台中不提供法语和西班牙语。在这个版本中，提供了法语和西班牙语的翻译。(OCPBUGS-33965)
- 在以前的版本中，masthead 徽标没有限制为 max-height 为 60px。因此，在原生显示大于 60px 高的徽标，并导致 masthead 大小太大。在这个版本中，masthead 徽标限制为 max-height 为 60px。(OCPBUGS-33523)
- 在以前的版本中，HealthCheck 控制器中缺少返回语句，在某些情况下会造成它 panic。在这个版本中，正确的返回语句被添加到 HealthCheck 控制器中，因此不再 panic。(OCPBUGS-33505)
- 在以前的版本中，向 API 服务器发送了一个不正确的字段。随着 Admission Webhook 的实现，显示相同的操作将返回警告通知。提供了一个修复来解决这个问题。(OCPBUGS-33222)
- 在以前的版本中，当没有时间戳时，StatusItem 的消息文本可能会垂直与图标对齐。在这个版本中，消息文本会被正确对齐。(OCPBUGS-33219)
- 在以前的版本中，创建者字段会被自动填充，而不是强制设置。对 API 的更新会使 OpenShift Container Platform 4.15 及更高版本中的字段为空。在这个版本中，字段被标记为强制进行验证。(OCPBUGS-31931)
- 在以前的版本中，web 控制台中的 YAML 编辑器没有 Create 按钮，示例不会在 web 控制台中显示。在这个版本中，您可以看到 Create 按钮和示例。(OCPBUGS-31703)
- 在以前的版本中，对外部 OpenID Connect (OIDC)功能上的桥接服务器标记的更改会导致桥接服务器无法在本地开发中启动。在这个版本中，标记用量会被更新，并会启动桥接服务器。

(OCPBUGS-31695)

- 在以前的版本中，当编辑 VMware vSphere 连接时，即使实际没有值，也可以提交表单。这会导致不必要的节点重启。在这个版本中，控制台会检测到表单更改，并在没有更改值时不允许提交。(OCPBUGS-31613)

- 在以前的版本中，如果使用 控制台 的表单方法，则 NetworkAttachmentDefinition 始终在 default 命名空间中创建。所选名称也不会被遵守，并使用所选名称和随机后缀创建 NetworkAttachmentDefinition 对象。在这个版本中，NetworksmentDefinition 对象在当前项目中创建。(OCPBUGS-31558)

- 在以前的版本中，当通过 AlertmanagerRecieversNotConfigured 警报单击 Configure 按钮时，Configuration 页面不会显示。在这个版本中，AlertmanagerRecieversNotConfigured 警报中的链接已被修复，并将您定向到 Configuration 页面。(OCPBUGS-30805)

- 在以前的版本中，使用 ListPageFilters 的插件只使用两个过滤器：标签和名称。在这个版本中，添加了一个参数，使插件可以配置多个基于文本的搜索过滤器。(OCPBUGS-30077)

- 在以前的版本中，点快速启动项时没有响应。在这个版本中，当点快速启动选择时会显示快速启动窗口。(OCPBUGS-29992)

- 在以前的版本中，如果首次尝试身份验证发现失败，OpenShift Container Platform Web 控制台会意外终止。在这个版本中，身份验证初始化已被更新，在失败前重试最多 5 分钟。(OCPBUGS-29479)

- 在以前的版本中，在 CLI 中创建 Image Manifest Vulnerability (IMV)后，在 Image Manifest Vulnerability 页面中存在一个错误消息。在这个版本中，错误消息不再显示。(OCPBUGS-28967)

- 在以前的版本中，当将 hook 中的模态对话框用作操作 hook 的一部分时，会出现一个错误，因为控制台框架将 null 对象作为呈现周期的一部分传递。在这个版本中，getGroupVersionKindForResource 现在为 null-safe，如果 apiVersion 或 kind 未定义，则返回未定义。此外，useDeleteModal 的运行时错误将不再发生，但请注意，它不会用于 未定义 资源。(OCPBUGS-28856)

- 在以前的版本中，Expand PersistentVolumeClaim 模态假设 pvc.spec.resources.requests.stroage 值包含一个单元。在这个版本中，大小被更新为 2GiB，您可以更改持久性卷声明(PVC)的值。(OCPBUGS-27779)

- 在以前的版本中，OpenShift Container Platform Web 控制台中报告的镜像漏洞值不一致。在这个版本中，Overview 页面中的镜像漏洞已被删除。(OCPBUGS-27455)

- 在以前的版本中，为最近批准的节点显示证书签名请求(CSR)。在这个版本中，会检测到重复，且不会为批准的节点显示 CSR。(OCPBUGS-27399)

- 在以前的版本中，MachineHealthCheck 详情页面的 condition 表上不是 Type 列。在这个版本中，Type 在条件表上首先列出。(OCPBUGS-27246)

- 在以前的版本中，控制台插件代理不会从插件服务响应中复制状态代码。这会导致插件服务的所有响应都具有 200 状态，从而导致意外行为，特别是浏览器缓存。在这个版本中，控制台代理逻辑已被更新，以转发插件服务代理响应状态代码。代理插件请求现在可以正常工作。(OCPBUGS-26933)

- 在以前的版本中，当克隆持久性卷声明(PVC)时，模态假设 pvc.spec.resources.requests.storage 值包含一个单元。在这个版本中，pvc.spec.resources.requests.storage 包含一个单元后缀，Clone PVC 模态可以正常工作。(OCPBUGS-26772)

- 在以前的版本中，在编辑 VMware vSphere 连接时，转义的字符串不会被正确处理，从而导致 VMware vSphere 配置无法正常工作。在这个版本中，转义字符串可以正常工作，VMware vSphere 配置不再中断。(OCPBUGS-25942)

- 在以前的版本中，当配置 VMware vSphere 连接时，resourcepool-path 键没有添加到 VMware vSphere 配置映射中，这可能会导致连接到 VMware vSphere 的问题。在这个版本中，连接到 VMware vSphere 时不再有问题。(OCPBUGS-25927)

- 在以前的版本中，客户反馈 模式中缺少文本。在这个版本中，链接文本会被恢复，并显示正确的红帽镜像。(OCPBUGS-25843)

- 在以前的版本中，当点 Cluster Settings 页面中的 Select a version 时，Update cluster modal 不会被打开。在这个版本中，在点 Select a version 时会显示 Update cluster modal。(OCPBUGS-25780)

- 在以前的版本中，在移动设备中，搜索页面的 resource 部分中的过滤器部分无法在移动设备中工作。在这个版本中，过滤现在可以在移动设备中正常工作。(OCPBUGS-25530)

- 在以前的版本中，console Operator 使用客户端而不是监听程序获取集群资源。这会导致 Operator 对具有较旧修订版本的资源执行操作。在这个版本中，console Operator 使用 list 从集群而不是客户端获取数据。(OCPBUGS-25484)

- 在以前的版本中，控制台会错误地从恢复中的卷快照解析恢复大小值，作为新的持久性卷声明(PVC)模态。在这个版本中，模态可以正确地解析恢复大小。(OCPBUGS-24637)

- 在以前的版本中，因为路由库的变化，控制台中没有 Alerting、Metrics 和 Target 页面。在这个版本中，路由可以正确地加载。(OCPBUGS-24515)

- 在以前的版本中，当没有条件的 MachineHealthCheck 时，Node details 页面中会出现运行时错误。在这个版本中，Node 详情页面 会如预期加载。(OCPBUGS-24408)

- 在以前的版本中，控制台后端会代理对公共 API 服务器端点的请求，这在某些情况下会导致 CA 证书问题。在这个版本中，代理配置已被更新，以指向解决了这个问题的内部 API 服务器端点。(OCPBUGS-22487)

- 在以前的版本中，当存在 HorizontalPodAutoscaler 时，无法扩展或缩减部署。在这个版本中，当将带有 HorizontalPodAutoscaler 的部署 缩减为零 时，会显示 Enable Autoscale 按钮，以便您可以启用 pod 自动扩展。(OCPBUGS-22405)

- 在以前的版本中，当编辑一个文件时，Info 警报：Non-printable 文件会被检测到。文件包含不可打印的字符。Preview is not available. 错误已被显示。在这个版本中，添加了一个检查来确定文件是否为二进制文件，并可如预期编辑该文件。(OCPBUGS-18699)

- 在以前的版本中，控制台 API 转换 Webhook 服务器无法在运行时更新服务证书，如果这些证书通过删除签名密钥来更新，则会失败。这会导致在轮转 CA 证书时控制台无法恢复。在这个版本中，控制台转换 Webhook 服务器被更新来检测 CA 证书更改，并在运行时处理它们。服务器现在仍然可用，控制台会在 CA 证书轮转后按预期恢复。(OCPBUGS-15827)

- 在以前的版本中，控制台前端捆绑包的生产构建过去禁用了源映射。因此，用于分析源代码的浏览器工具无法在生产构建中使用。在这个版本中，控制台 Webpack 配置已被更新，以在生产构建中启用源映射。现在，对于 dev 和 production 构建，浏览器工具都可以按预期工作。(OCPBUGS-10851)

- 在以前的版本中，控制台重定向服务与控制台服务具有相同的服务证书颁发机构(CA)控制器注解。这会导致服务 CA 控制器有时会错误地为这些服务同步 CA 证书，控制台在删除并重新创建后无法正常工作。在这个版本中，控制台 Operator 被更新为从控制台重定向服务中删除此服

务 CA 注解。当 Operator 从删除状态变为受管状态时，控制台服务和 CA 证书现在可以正常工作。(OCPBUGS-7656)

- 在以前的版本中，当使用 Form view 编辑路由时删除备用服务不会导致从 Route 中删除备用服务。在这个版本中，备用服务已被删除。(OCPBUGS-33011)

- 在以前的版本中，在执行集群更新时，暂停的 MachineConfigPools migh 的节点被错误地取消暂停。在这个版本中，暂停的 MachineConfigPools 节点会在执行集群更新时正确暂停。(OCPBUGS-23319)

监控

- 在以前的版本中，如果某些光纤通道设备驱动程序没有公开所有属性，node-exporter 代理中的 Fibre Channel 收集器会失败。在这个版本中，光纤通道收集器忽略这些可选属性，并解决了这个问题。(OCPBUGS-20151)

- 在以前的版本中，oc get podmetrics 和 oc get nodemetrics 命令无法正常工作。在这个版本中，这个问题已被解决。(OCPBUGS-25164)

- 在以前的版本中，在 ServiceMonitor 资源中设置无效的 .spec.endpoints.proxyUrl 属性会导致破坏、重新载入和重启 Prometheus。在这个版本中，通过针对无效的语法验证 proxyUrl 属性解决了这个问题。(OCPBUGS-30989)

网络

- 在以前的版本中，Ingress API 中的 status.componentRoutes.currentHostnames 字段的 API 文档包括开发人员备注。在输入 oc explain ingresses.status.componentRoutes.currentHostnames --api-version=config.openshift.io/v1 命令后，开发人员备注将与预期信息一起显示在输出中。在这个版本中，开发人员备注会从 status.componentRoutes.currentHostnames 字段中删除，以便在输入命令后，输出会列出路由使用的当前主机名。(OCPBUGS-31058)

- 在以前的版本中，在决定权重时，负载均衡算法不会区分活跃和不活跃的服务，并在具有许多不活跃服务或带有权重 0 的环境中使用随机算法。这会导致内存用量增加，并面临过量内存消耗的风险。在这个版本中，更改会优化对活跃服务的流量方向，并防止不必要的使用具有更高权重的随机算法，从而减少过量内存消耗的可能性。(OCPBUGS-29690)

- 在以前的版本中，如果在同一证书中指定多个路由，或者路由将默认证书指定为自定义证书，并在路由器上启用 HTTP/2，HTTP/2 客户端可以在路由上执行连接。Web 浏览器等客户端可能会重新使用连接，并可能会连接到错误的后端服务器。在这个版本中，OpenShift Container Platform 路由器会检查同一证书是否在多个路由上指定，或者当路由将默认证书指定为自定义证

书时。当检测到其中一个条件时，路由器将配置 HAProxy 负载均衡器，以便不允许 HTTP/2 客户端连接使用这些证书的任何路由。(OCPBUGS-29373)

- 在以前的版本中，如果您配置了将 routingViaHost 参数设置为 true 的部署，流量无法访问 IPv6 ExternalTrafficPolicy=Local 负载均衡器服务。在这个版本中，这个问题已被解决。(OCPBUGS-27211)

- 在以前的版本中，由托管在二级网络接口控制器(NIC)上的 EgressIp 对象选择的 pod 会导致连接到节点 IP 地址超时。在这个版本中，这个问题已被解决。(OCPBUGS-26979)

- 在以前的版本中，因为软件包已过期，安装 OpenShift Container Platform Precision Time Protocol (PTP) Operator 的 leap 文件软件包不能被 ts2phc 进程使用。在这个版本中，leap file 软件包被更新为从 Global Positioning System (GPS)信号中读取大量事件，并动态更新偏移，以便过期的软件包不再发生。(OCPBUGS-25939)

- 在以前的版本中，在节点强制重启后，从 Whereabouts CNI 插件创建的池中分配 IP 的 pod 会处于 ContainerCreating 状态。在这个版本中，在节点强制重启后与 IP 分配关联的 Whereabouts CNI 插件问题。(OCPBUGS-24608)

- 在以前的版本中，IPv6 中的 OpenShift Container Platform 的两个脚本之间有冲突，包括单堆栈和双栈部署。一个脚本会将主机名设置为完全限定域名(FQDN)，但其他脚本可能会提前将其设置为短名称。这是因为触发将主机名设置为 FQDN 的事件可能会在将其设置为短名称的脚本后运行。这是因为异步网络事件发生。在这个版本中，添加了新的代码以确保正确设置 FQDN。这个新代码可确保在设置主机名前等待特定的网络事件。(OCPBUGS-22324)

- 在以前的版本中，如果通过二级接口选择的带有 EgressIP 的 pod 的标签被删除，则同一命名空间中的另一个 pod 也会丢失其 EgressIP 分配，从而破坏与外部主机的连接。在这个版本中，这个问题已被解决，因此当 pod 标签被删除并停止使用 EgressIP 时，具有匹配标签的其他 pod 将继续在不中断的情况下使用 EgressIP。(OCPBUGS-20220)

- 在以前的版本中，全局导航 satellite 系统(GNSS)模块可以同时报告 GPS 修复 位置和 GNSS 偏移 位置，这代表 GNSS 模块和 constellations 之间的偏移量。前面的 T-GM 没有使用 ubloxtool CLI 工具探测 ublox 模块读取 偏移 和修复 位置。相反，它只能通过 GPSD 读取 GPS 修复 信息。这样做的原因是，以前的 ubloxtool CLI 工具的实现需要 2 秒才能接收响应，并且每次调用每个 CPU 用量都会增加三倍。在这个版本中，ubloxtool 请求已被优化，GPS 偏移 位置现在可用。(OCPBUGS-17422)

- 在以前的版本中，因为竞争条件，由二级接口托管的 EgressIP pod 不会故障转移。用户会收到一条错误消息，表示无法分配 EgressIP pod，因为它与现有 IP 地址冲突。在这个版本中，EgressIP pod 移到一个出口节点。(OCPBUGS-20209)

- 在以前的版本中，当 OVN-Kubernetes 使用的物理接口上的 MAC 地址更改时，无法在 OVN-Kubernetes 中正确更新，并可能导致节点出现流量中断和 Kube API 中断。这在使用绑定接口时最常见的情况，绑定的 MAC 地址可能会交换，具体取决于哪个设备是第一个启动。在这个版本中，如果修复了问题，则 OVN-Kubernetes 会动态检测 MAC 地址更改并正确更新它。(OCPBUGS-18716)

- 在以前的版本中，当为不是主网络接口的网络接口分配出口 IP 时，不支持 IPv6。这个问题已被解决，出口 IP 可以是 IPv6。(OCPBUGS-24271)

- 在以前的版本中，network-tools 镜像是一个调试工具，其中包含 Wireshark 网络协议分析器。wireshark 依赖于 gstreamer1 软件包，此软件包具有特定的许可要求。在这个版本中，gstreamer1 软件包已从 network-tools 镜像中删除，镜像现在包含 wireshark-cli 软件包。(OCPBUGS-31699)

- 在以前的版本中，当将节点的默认网关设置为 vlan 且多个网络管理器连接具有相同的名称时，节点会失败，因为它无法配置默认的 OVN-Kubernetes 网桥。在这个版本中，configure-ovs.sh shell 脚本包含一个 nmcli connection show uuid 命令，它会在存在许多具有相同名称的连接时检索正确的网络管理器连接。(OCPBUGS-24356)

- 对于 Microsoft Azure 上的 OpenShift Container Platform 集群，当使用 OVN-Kubernetes 作为 Container Network Interface (CNI)时，当使用带有 externalTrafficPolicy: Local 的负载均衡器服务时，pod 识别的源 IP 是节点的 OVN 网关路由器。这是因为源网络地址转换(SNAT)应用到 UDP 数据包。

  在这个版本中，通过将关联性超时设置为更高的值（如 86400 秒或 24 小时），可以在没有超时的情况下进行会话关联性。因此，关联性会被视为永久的，除非出现网络中断，如端点或节点停机。因此，会话关联性更为持久。(OCPBUGS-24219)

节点

- 在以前的版本中，Ansible 的 OpenShift Container Platform 升级会导致错误，因为 IPsec 配置不是幂等的。在这个版本中，这个问题已被解决。现在，OpenShift Ansible playbook 的所有 IPsec 配置都是幂等的。(OCPBUGS-30802)

- 在以前的版本中，CRI-O 删除了在 OpenShift Container Platform 次版本升级间安装的所有镜像，以确保过时的有效负载镜像不会消耗节点上的空间。但是，它决定这是性能损失，而此功能已被删除。在这个版本中，kubelet 在磁盘用量达到特定级别后仍然会垃圾回收过时的镜像。因此，OpenShift Container Platform 不再在次版本间的升级后删除所有镜像。(OCPBUGS-24743)

Node Tuning Operator (NTO)

- 在以前的版本中，单节点 OpenShift Container Platform 上的分布式单元配置集被降级，因为 net.core.busy_read,net.core.busy_poll, 和 kernel.numa_balancing sysctl 不存在。在这个版本中，Tuned 配置集不再降级，这个问题已解决。(OCPBUGS-23167)

- 在以前的版本中，在应用 PerformanceProfile 后 Tuned 配置集会报告 Degraded 条件。该配置集试图为默认的 Receive Packet Steering (RPS)掩码设置 sysctl 值，但掩码已使用 /etc/sysctl.d 文件使用相同的值配置。在这个版本中，sysctl 值不再使用 Tuned 配置集设置，并解决了这个问题。(OCPBUGS-24638)

- 在以前的版本中，Performance Profile Creator (PPC)会错误地填充 Day 0 性能配置集清单的 metadata.ownerReferences.uid 字段。因此，在没有手动干预的情况下，无法在第 0 天应用性能配置集。在这个版本中，PPC 不会为第 0 天清单生成 metadata.ownerReferences.uid 字段。因此，您可以如预期在第 0 天应用性能配置集清单。(OCPBUGS-29751)

- 在以前的版本中，TuneD 守护进程可能会在 Tuned 自定义资源(CR)更新后不必要地重新载入额外的时间。在这个版本中，删除了 Tuned 对象，Tuned (daemon)配置集会在 Tuned Profile Kubernetes 对象中直接执行。因此，这个问题已被解决。(OCPBUGS-32469)

OpenShift CLI (oc)

- 在以前的版本中，当镜像带有不兼容语义版本的 operator 镜像时，oc-mirror 插件 v2 （技术预览）将失败并退出。在这个版本中，确保在控制台中出现警告，指示跳过的镜像并允许镜像过程在不中断的情况下继续。(OCPBUGS-34587)

- 在以前的版本中，oc-mirror 插件 v2 （技术预览）无法镜像包含 标签和 摘要 格式的镜像引用的某些 Operator 目录。此问题会阻止创建集群资源，如 ImageDigestMirrorSource (IDMS)和 ImageTagMirrorSource (ITMS)。在这个版本中，oc-mirror 通过跳过 具有标签 和 摘要 引用的镜像来解决这个问题，同时在控制台输出中显示适当的警告信息。(OCPBUGS-33196)

- 在以前的版本中，使用 oc-mirror 插件 v2 （技术预览），镜像错误仅显示在控制台输出中，因此用户很难分析并排除其他问题。例如，不稳定的网络可能需要重新运行，而清单未知错误可能需要进一步分析来跳过镜像或 Operator。在这个版本中，生成一个文件，其中包含工作区 working-dir/logs 文件夹中的所有错误。现在，镜像过程中出现的所有错误都会记录在 mirroring_errors_YYYYMMdd.txt 中。(OCPBUGS-33098)

- 在以前的版本中，Cloud Credential Operator 实用程序(ccoctl)无法在启用了 FIPS 的 RHEL 9 主机上运行。在这个版本中，用户可以运行与主机的 RHEL 版本兼容的 ccoctl 工具版本，包括 RHEL 9。(OCPBUGS-32080)

- 在以前的版本中，当镜像 operator 目录时，oc-mirror 会重建目录并根据 imagesetconfig

目录过滤规格重新生成其内部缓存。这个过程需要来自目录中的 opm 二进制文件。从 4.15 版本开始，Operator 目录包括 opm RHEL 9 二进制文件，这会导致在 RHEL 8 系统上执行镜像过程会失败。在这个版本中，oc-mirror 不再默认重建目录，而是将其镜像到其目标 registry。

要保留目录重建功能，可使用 --rebuild-catalog。但请注意，不会对当前实现进行任何更改，因此使用这个标志可能会导致缓存不会被生成，或者目录没有部署到集群中。如果使用这个命令，您可以导出 OPM_BINARY，以指定与 OpenShift Container Platform 中找到的目录版本和平台对应的自定义 opm 二进制文件。现在，目录镜像的镜像会在没有签名验证的情况下进行。use -enable-operator-secure-policy 在镜像期间启用签名验证。(OCPBUGS-31536)

- 在以前的版本中，当使用包含 CloudCredential 集群功能的 install-config.yaml 文件运行 oc adm release extract --credentials-requests 命令时，一些凭证请求不会被正确提取。在这个版本中，Cloud Credential 功能会被正确包含在 OpenShift CLI (oc)中，以便这个命令正确提取凭证请求。(OCPBUGS-24834)

- 在以前的版本中，用户在 oc-mirror 插件中使用 tar.gz 工件时遇到序列错误。要解决这个问题，oc-mirror 插件现在在使用-- skip-pruning 标志执行时会忽略这些错误。在这个版本中，确保序列错误（不再影响镜像中的 tar.gz 使用顺序）被有效地处理。(OCPBUGS-23496)

- 在以前的版本中，当使用 oc-mirror 插件镜像位于隐藏文件夹中的本地 Open Container Initiative Operator 目录时，oc-mirror 会失败并显示错误：".hidden_folder/data/publish/latest/catalog-oci/manifest-list/kubebuilder/kube-rbac-proxy@sha256:db06cc4c084dd0253134f156dddaaf53ef1c3fb3cc809e5d817d817a0294c0294c0294c0294c1 不是有效的镜像引用：无效的引用格式 "。在这个版本中，oc-mirror 会以不同的方式计算对本地 Open Container Initiative 目录中镜像的引用，确保隐藏目录的路径不会影响镜像过程。(OCPBUGS-23327)

- 在以前的版本中，oc-mirror 在镜像失败时不会停止并返回有效的错误代码。在这个版本中，oc-mirror 会在遇到 "operator not found" 时使用正确的错误代码退出，除非使用了 --continue-on-error 标志。(OCPBUGS-23003)

- 在以前的版本中，当镜像 operator 时，如果指定了 minVersion 和 maxVersion，oc-mirror 将忽略 imageSetConfig 中的 maxVersion 约束。这会导致将所有捆绑包镜像到频道头。在这个版本中，oc-mirror 会考虑在 imageSetConfig 中指定的 maxVersion 约束。(OCPBUGS-21865)

- 在以前的版本中，oc-mirror 无法使用 euseus 频道镜像发行版本，因为它无法识别 eus channel 只为偶数版本指定。在这个版本中，oc-mirror 插件可以正确地确认 eus channel 适用于偶数的发行版本，允许用户使用这些频道成功镜像发行版本。(OCPBUGS-19429)

- 在以前的版本中，在 mirror.operators.catalog.packages 文件中添加 defaultChannel 字段后，用户可以指定首选频道，覆盖 Operator 中的 defaultChannel 设置。在这个版本中，oc-

mirror 插件现在强制执行一个初始检查 defaultChannel 字段是否已设置，用户还必须在 ImageSetConfig 的 channels 部分中定义它。在这个版本中，确保在 Operator 镜像过程中正确配置并应用指定的 defaultChannel。(OCPBUGS-385)

- 在以前的版本中，当运行启用了 FIPS 的集群时，您可能会在 RHEL 9 系统中运行 OpenShift CLI (oc)时收到以下错误： FIPS 模式会被启用，但所需的 OpenSSL 后端不可用。在这个版本中，OpenShift CLI (oc)的默认版本使用 Red Hat Enterprise Linux (RHEL) 9 编译，并在运行在 RHEL 9 上启用 FIPS 的集群时正常工作。另外，还提供了使用 RHEL 8 编译的 oc 版本，如果您运行在 RHEL 8 上启用了 FIPS 的集群，则必须使用该版本。(OCPBUGS-23386, OCPBUGS-28540)

- 在以前的版本中，与 ImageRegistry 和 Build 功能相关的角色绑定都会在每个命名空间中创建，即使禁用了这个能力。在这个版本中，只有在集群中启用了对应的集群功能时，才会创建角色绑定。(OCPBUGS-34384)

- 在以前的版本中，在完全断开连接的环境中的 disk-to-mirror 过程中，oc-mirror 插件 v1 会在访问 Red Hat registry 时无法镜像目录镜像。另外，如果 ImageSetConfiguration 将 targetCatalog 用于镜像目录，则镜像会失败，因为无论工作流如何引用不正确的目录镜像。这个问题已通过更新目录源来镜像到镜像 registry 解决了这个问题。(OCPBUGS-34646)

Operator Lifecycle Manager (OLM)

- 在以前的版本中，Operator 目录不会被正确刷新，因为索引镜像的 imagePullPolicy 字段被设置为 IfNotPresent。在这个版本中更新了 OLM，为目录使用适当的镜像拉取策略，因此会正确刷新目录。(OCPBUGS-30132)

- 在以前的版本中，因为 OLM 处于 CrashLoopBackOff 状态，集群升级可能会被阻断。这是因为资源有多个所有者引用的问题。在这个版本中更新了 OLM，以避免重复所有者引用，只验证它拥有的相关资源。因此，集群升级可以如预期进行。(OCPBUGS-28744)

- 在以前的版本中，CatalogSource 对象支持的默认 OLM 目录 pod 在它们运行的节点中断时不会保留。pod 处于终止状态，尽管应移动它们的容限。这会导致 Operator 不再无法从相关目录安装和更新。在这个版本中更新了 OLM，因此处于这个状态的目录 pod 会被删除。现在，目录 pod 可以正确地从计划或计划外节点维护中恢复。(OCPBUGS-32183)

- 在以前的版本中，如果之前安装和配置了相同的 Operator，安装 Operator 有时可能会失败。这是因为缓存问题。在这个版本中更新了 OLM 以在这种情况下正确安装 Operator，因此不再出现这个问题。(OCPBUGS-31073)

- 在以前的版本中，catalogd 组件在 etcd 恢复后可能会崩溃。这是因为垃圾回收过程会在 API 服务器无法访问时导致循环失败状态。在这个版本中更新了 catalogd 来添加重试循环，因此目

录不再在这种情况下崩溃。(OCPBUGS-29453)

- 在以前的版本中，默认目录源 pod 不会接收更新，需要用户手动重新创建它来获取更新。这是因为目录 pod 的镜像 ID 没有被正确检测到。在这个版本中更新了 OLM 来正确地检测目录 pod 镜像 ID，因此会如预期更新默认目录源。(OCPBUGS-31438)

- 在以前的版本中，因为 OLM 无法找到现有的 ClusterRoleBinding 或 Service 资源，并第二次创建它们，所以可能会出现 Operator 安装错误。在这个版本中更新了 OLM 来预先创建这些对象，因此不会再发生这些安装错误。(OCPBUGS-24009)

Red Hat Enterprise Linux CoreOS (RHCOS)

- 在以前的版本中，在 kdump 服务生成其特殊的 initramfs 之前配置的 OVS 网络。当 kdump 服务启动时，它会获取 network-manager 配置文件并将其复制到 kdump initramfs 中。当节点重新引导到 kdump initramfs 时，内核崩溃转储通过网络上传会失败，因为 OVN 没有运行到 initramfs 中，且虚拟接口没有配置。在这个版本中，顺序已被更新，kdump 会在设置 OVS 网络配置前启动并构建 kdump initramfs，并解决了这个问题。(OCPBUGS-30239)

可伸缩性和性能

- 在以前的版本中，在 Performance Profile 呈现后，单节点 OpenShift Container Platform 上的 Machine Config Operator (MCO)会被呈现，因此 control plane 和 worker 机器配置池不会在正确的时间创建。在这个版本中，Performance Profile 可以正确地显示，这个问题已解决。(OCPBUGS-22095)

- 在以前的版本中，TuneD 和 irqbalanced 守护进程修改了中断请求(IRQ) CPU 关联性配置，这会在 IRQ CPU 关联性配置中创建冲突，并在单节点 OpenShift 节点重启后造成意外行为。在这个版本中，只有 irqbalanced 守护进程决定 IRQ CPU 关联性配置。(OCPBUGS-26400)

- 在以前的版本中，在 OpenShift Container Platform 在性能调整集群中更新过程中，恢复 MachineConfigPool 资源会导致池中节点出现额外的重启。在这个版本中，控制器会在池恢复前协调最新计划机器配置，以防止额外的节点重启。(OCPBUGS-31271)

- 在以前的版本中，ARM 安装在内核中使用 4k 页。在这个版本中，增加了对在安装时在内核中安装 64k 页的支持，从而在 NVIDIA CPU 上性能提高。驱动程序工具套件(DTK)也已更新，以便为 64k 页大小 ARM 内核编译内核模块。(OCPBUGS-29223)

Storage

- 在以前的版本中，在删除 LVMCluster 自定义资源(CR)过程中，一些 LVMVolumeGroupNodeStatus 操作对象不会被删除。在这个版本中，删除 LVMCluster CR 会

触发删除所有 LVMVolumeGroupNodeStatus 操作对象。(OCPBUGS-32954)

- 在以前的版本中，LVM Storage 卸载会卡住等待删除 LVMVolumeGroupNodeStatus 操作对象。在这个版本中，确保所有操作对象都被删除，允许在不延迟的情况下卸载 LVM 存储。(OCPBUGS-32753)

- 在以前的版本中，LVM 存储不支持持久性卷声明(PVC)的最小存储大小。这会导致在置备 PVC 时挂载失败。在这个版本中，LVM 存储支持 PVC 的最小存储大小。以下是您可以为每个文件系统类型请求的最小存储大小：

  - 块设备: 8 MiB
  - XFS: 300 MiB
  - ext4: 32 MiB

  如果 PersistentVolumeClaim 对象中的 requests.storage 字段的值小于最小存储大小，则请求的存储大小将舍入到最小存储大小。如果 limits.storage 字段的值 小于最小存储大小，则 PVC 创建会失败并显示错误。(OCPBUGS-30266)

- 在以前的版本中，LVM 存储创建了持久性卷声明(PVC)，其存储大小请求不是磁盘扇区大小的倍数。这可能会导致 LVM2 卷创建过程中出现问题。在这个版本中，通过将 PVC 请求的存储大小舍入到最接近的 512 的倍数来调整行为。(OCPBUGS-30032)

- 在以前的版本中，LVMCluster 自定义资源(CR)包含正确设置的设备的 exclude status 元素。在这个版本中，过滤了为排除的 status 元素正确设置的设备，因此它只出现在就绪设备中。(OCPBUGS-29188)

- 在以前的版本中，Amazon Web Services (AWS) Elastic File Store (EFS) Container Storage Interface (CSI)驱动程序容器的 CPU 限制可能会导致 AWS EFS CSI Driver Operator 管理的卷性能下降。在这个版本中，AWS EFS CSI 驱动程序容器中的 CPU 限制已被删除，以帮助防止潜在的性能下降。(OCPBUGS-28551)

- 在以前的版本中，Microsoft Azure Disk CSI 驱动程序没有在特定实例类型中正确计算可分配卷，并超过最大值。因此，pod 无法启动。在这个版本中，Microsoft Azure Disk CSI 驱动程序的 count 表已更新，以包含新的实例类型。pod 现在运行，数据可以被读取和写入到正确配置的卷。(OCPBUGS-18701)

- 在以前的版本中，由于 CLI 中的一个错误，secret 在 Hosted Control Planes 上存储 Container Storage Interface 驱动程序将无法挂载 secret。在这个版本中，驱动程序可以挂载卷，并解决了这个问题。(OCPBUGS-34759)

- 在以前的版本中，因为驱动程序中的一个错误而无法配置 Microsoft Azure Workload Identity 集群中的静态持久性卷(PV)，从而导致 PV 挂载失败。在这个版本中，驱动程序可以正常工作，静态 PV 可以正常工作。(OCPBUGS-32785)

1.7. 技术预览功能状态

这个版本中的一些功能当前还处于技术预览状态。它们并不适用于在生产环境中使用。请注意红帽客户门户网站中的以下支持范围：

技术预览功能支持范围

在以下表格中，功能被标记为以下状态：

- *技术预览*
- *公开发行*
- *不可用*
- *已弃用*

网络功能虚拟化功能

表 1.18. 网络技术预览跟踪器

功能	4.14	4.15	4.16
Ingress Node Firewall Operator	公开发行	公开发行	公开发行
通过 L2 模式，使用节点的一个子集（由特定的 IP 地址池指定）中的 MetalLB 服务进行广告	技术预览	技术预览	技术预览

功能	4.14	4.15	4.16
SR-IOV 网络的多网络策略	技术预览	公开发行	公开发行
OVN-Kubernetes 网络插件作为二级网络	公开发行	公开发行	公开发行
更新特定于接口的安全 sysctl 列表	技术预览	技术预览	技术预览
出口服务自定义资源	技术预览	技术预览	技术预览
BGPPeer 自定义资源中的 VRF 规格	技术预览	技术预览	技术预览
NodeNetworkConfigurationPolicy 自定义资源中的 VRF 规格	技术预览	技术预览	技术预览
Admin Network Policy (**AdminNetworkPolicy**)	技术预览	技术预览	公开发行
IPsec 外部流量 (north-south)	技术预览	公开发行	公开发行
MetalLB 和 FRR-K8s 集成	不可用	不可用	技术预览
双 NIC 硬件作为 PTP 边界时钟	公开发行	公开发行	公开发行
带有高可用性系统时钟的双 NIC Intel E810 PTP 边界时钟	不可用	不可用	公开发行
Intel E810 Westport Channel NIC 作为 PTP grandmaster 时钟	技术预览	技术预览	公开发行
双 NIC Intel E810 Westport Channel 作为 PTP grandmaster 时钟	不可用	技术预览	公开发行
使用 NMState 配置 OVN-Kuberenetes 所需的 **br-ex** 网桥	不可用	不可用	技术预览
从 OpenShift SDN 实时迁移 OVN-Kubernetes	不可用	不可用	公开发行
使用 Whereabouts 进行多租户网络的重叠 IP 配置	不可用	不可用	公开发行

存储技术预览功能

表 1.19. 存储技术预览

功能	4.14	4.15	4.16
使用 Local Storage Operator 进行自动设备发现和置备	技术预览	技术预览	技术预览
Google Filestore CSI Driver Operator	公开发行	公开发行	公开发行
IBM Power® Virtual Server Block CSI Driver Operator	技术预览	公开发行	公开发行

功能	4.14	4.15	4.16
Read Write Once Pod 访问模式	技术预览	技术预览	公开发行
在 OpenShift 构建中构建 CSI 卷	公开发行	公开发行	公开发行
OpenShift 构建中的共享资源 CSI 驱动程序	技术预览	技术预览	技术预览
Secret Store CSI Driver Operator	技术预览	技术预览	技术预览
CIFS/SMB CSI Driver Operator	不可用	不可用	技术预览

安装技术预览功能

表 1.20. 安装技术预览

功能	4.14	4.15	4.16
在带有虚拟机的 Oracle® Cloud Infrastructure (OCI) 上安装 OpenShift Container Platform	开发者预览	技术预览	技术预览
在裸机上的 Oracle® Cloud Infrastructure (OCI)上安装 OpenShift Container Platform	开发者预览	开发者预览	开发者预览
使用 kvc 向节点添加内核模块	技术预览	技术预览	技术预览
为 SR-IOV 设备启用 NIC 分区	技术预览	技术预览	技术预览
Google Cloud Platform (GCP) 的用户定义的标记和标签	技术预览	技术预览	技术预览
使用安装程序置备的基础架构在 Alibaba Cloud 上安装集群	技术预览	技术预览	不可用
使用 Assisted Installer 在 Alibaba Cloud 上安装集群	不可用	不可用	技术预览
在 RHEL 中的 BuildConfig 中挂载共享权利	技术预览	技术预览	技术预览
Oracle® Cloud Infrastructure (OCI)上的 OpenShift Container Platform	开发者预览	技术预览	技术预览
可选择 Cluster Inventory	技术预览	技术预览	技术预览
使用 VMware vSphere 的静态 IP 地址（仅限IPI）	技术预览	技术预览	公开发行
支持 RHCOS 中的 iSCSI 设备	不可用	技术预览	公开发行
使用 Cluster API 实现在 GCP 上安装集群	不可用	不可用	技术预览

功能	4.14	4.15	4.16
支持 RHCOS 中启用了 Intel® VROC 的 RAID 设备	技术预览	技术预览	公开发行

节点技术预览功能

表 1.21. 节点技术预览

功能	4.14	4.15	4.16
MaxUnavailableStatefulSet 功能集	技术预览	技术预览	技术预览

多架构技术预览功能

表 1.22. 多架构技术预览

功能	4.14	4.15	4.16
使用安装程序置备的基础架构的 IBM Power® Virtual Server	技术预览	公开发行	公开发行
arm64 构架上的 **kdump**	技术预览	技术预览	技术预览
s390x 架构上的 **kdump**	技术预览	技术预览	技术预览
ppc64le 架构上的 **kdump**	技术预览	技术预览	技术预览
Multiarch Tuning Operator	不可用	不可用	技术预览

专用硬件和驱动程序启用技术预览功能

表 1.23. 专用硬件和驱动程序启用技术预览

功能	4.14	4.15	4.16
驱动程序工具包	公开发行	公开发行	公开发行
内核模块管理 Operator	公开发行	公开发行	公开发行
内核模块管理 Operator - Hub 和 spoke 集群支持	公开发行	公开发行	公开发行
节点功能发现	公开发行	公开发行	公开发行

可扩展性和性能技术预览功能

表 1.24. 可扩展性和性能技术预览

功能	4.14	4.15	4.16
factory-precaching-cli 工具	技术预览	技术预览	技术预览
超线程感知 CPU Manager 策略	技术预览	技术预览	技术预览
HTTP 传输替换了 PTP 和裸机事件的 AMQP	技术预览	技术预览	公开发行
挂载命名空间封装	技术预览	技术预览	技术预览
Node Observability Operator	技术预览	技术预览	技术预览
调整 etcd 延迟容错功能	技术预览	技术预览	公开发行
增加 etcd 数据库大小	不可用	不可用	技术预览
使用 RHACM **PolicyGenerator** 资源管理 GitOps ZTP 集群策略	不可用	不可用	技术预览

Operator 生命周期和开发技术预览功能

表 1.25. Operator 生命周期和开发技术预览

功能	4.14	4.15	4.16
Operator Lifecycle Manager (OLM) v1	技术预览	技术预览	技术预览
RukPak	技术预览	技术预览	技术预览
平台 Operator	技术预览	技术预览	删除
为基于 Helm 的 Operator 项目构建工具	技术预览	技术预览	已弃用
为基于 Java 的 Operator 项目构建工具	技术预览	技术预览	已弃用

OpenShift CLI (oc)技术预览功能

表 1.26. OpenShift CLI (oc)技术预览

功能	4.14	4.15	4.16
oc-mirror 插件 v2	不可用	不可用	技术预览
enclave 支持	不可用	不可用	技术预览
删除功能	不可用	不可用	技术预览

监控技术预览功能

表 1.27. 监控技术预览

功能	4.14	4.15	4.16
指标集合配置集	技术预览	技术预览	技术预览
指标服务器	不可用	技术预览	公开发行

Red Hat OpenStack Platform (RHOSP) 技术预览功能

表 1.28. RHOSP 技术预览

功能	4.14	4.15	4.16
使用安装程序置备的基础架构的双栈网络	技术预览	公开发行	公开发行
使用用户置备的基础架构的双栈网络	不可用	公开发行	公开发行
CAPO 集成到集群 CAPI Operator	不可用	技术预览	技术预览
在本地磁盘上使用 **rootVolumes** 和 **etcd** 的 Control Plane	不可用	技术预览	技术预览

托管 control plane 技术预览功能

表 1.29. 托管 control plane 技术预览

功能	4.14	4.15	4.16
在 Amazon Web Services (AWS) 上托管 OpenShift Container Platform 的 control plane。	技术预览	技术预览	技术预览
在裸机上托管 OpenShift Container Platform 的 control plane	公开发行	公开发行	公开发行
在 OpenShift Virtualization 上为 OpenShift Container Platform 托管 control plane	公开发行	公开发行	公开发行
使用非裸机代理机器为 OpenShift Container Platform 托管 control plane	不可用	技术预览	技术预览
在 Amazon Web Services 上为 ARM64 OpenShift Container Platform 集群托管 control plane	技术预览	技术预览	技术预览
在 IBM Power 上托管 OpenShift Container Platform 的 control plane	技术预览	技术预览	技术预览

功能	4.14	4.15	4.16
在 IBM Z 上托管 OpenShift Container Platform 的 control plane	技术预览	技术预览	技术预览

机器管理技术预览功能

表 1.30. 机器管理技术预览

功能	4.14	4.15	4.16
使用 Amazon Web Services 的集群 API 管理机器	技术预览	技术预览	技术预览
使用 Google Cloud Platform 的 Cluster API 管理机器	技术预览	技术预览	技术预览
使用 VMware vSphere 的集群 API 管理机器	不可用	不可用	技术预览
为 control plane 机器集定义 vSphere 故障域	不可用	技术预览	公开发行
Alibaba Cloud 的云控制器管理器	技术预览	技术预览	技术预览
Google Cloud Platform 的云控制器管理器	技术预览	公开发行	公开发行
IBM Power® Virtual Server 的云控制器管理器	技术预览	技术预览	技术预览

认证和授权技术预览功能

表 1.31. 认证和授权技术预览

功能	4.14	4.15	4.16
Pod 安全准入限制强制	技术预览	技术预览	技术预览

Machine Config Operator 技术预览功能

表 1.32. Machine Config Operator 技术预览

功能	4.14	4.15	4.16
改进了 MCO 状态报告	不可用	技术预览	技术预览
On-cluster RHCOS 镜像分层	不可用	不可用	技术预览
节点中断策略	不可用	不可用	技术预览
更新引导镜像	不可用	不可用	技术预览

Edge 计算技术预览功能

表 1.33. Edge 计算技术预览

功能	4.14	4.15	4.16
加速置备 GitOps ZTP	不可用	不可用	技术预览
使用 GitOps ZTP 和 RHACM 将 IPsec 加密部署到受管集群	不可用	不可用	技术预览

1.8. 已知问题

- **oc annotate 命令不适用于包含了等号（=）的 LDAP 组名称，因为命令使用等号作为注释名称和值之间的分隔符。作为临时解决方案，使用 oc patch 或 oc edit 添加注解。(BZ#1917280)**
- **在由 Hypershift Operator 管理的集群中安装 Run Once Duration Override Operator (RODOO)。(OCPBUGS-17533)**
- **OpenShift Container Platform 4.16 在 secret 或顶级 secret 区域的 AWS 上安装会失败，因为这些区域中的 Network Load Balancer (NLBs)和安全组存在问题。(OCPBUGS-33311)**
- **当您在 OpenShift Container Platform 集群上运行 Cloud-native Network Function (CNF) 延迟测试时，oslat 测试有时会返回大于 20 微秒的结果。这会导致 oslat 测试失败。(RHEL-9279)**
- **当使用 Local Zones 在 Amazon Web Services (AWS)上安装集群时，如果在 us-east-1-iah-2a 区域中部署，边缘节点将无法部署。(OCPBUGS-35538)**
- **无法使用 ACM 版本 2.10.3 或更早版本的 Infrastructure Operator、Central Infrastructure Management 或 ZTP 方法安装 OpenShift Container Platform 4.16。这是因为动态链接安装程序二进制文件openshift-baremetal-install 的变化，在 OpenShift Container Platform 4.16 中，需要一个 Red Hat Enterprise Linux (RHEL) 9 主机才能成功运行。计划在以后的 ACM 版本中使用静态链接的二进制文件来避免此问题。(ACM-12405)**
- **在 AWS 上安装集群时，如果负载均衡器 DNS 生存时间非常高，安装可能会超时。(OCPBUGS-35898)**
- **对于包含 br-ex 网桥设备的绑定接口，请不要在节点网络配置中设置 mode=6 balance-alb 绑定模式。OpenShift Container Platform 不支持此绑定模式，可能会导致 Open vSwitch**

(OVS)网桥设备与网络环境断开连接。(OCPBUGS-34430)

- 通过编辑 HostFirmwareComponents 资源，不要为 BareMetalHosts (BMH)资源更新固件。否则，BMH 处于 Preparing 状态并重复执行固件更新。没有临时解决方案。(OCPBUGS-35559)

- 当使用代理时，在裸机上部署安装程序置备的集群会失败。因为一个回归错误，bootstrap 虚拟机中的服务无法通过代理访问 IP 地址 0.0.0.0。作为临时解决方案，请将 0.0.0.0 添加到 noProxy 列表中。如需更多信息，请参阅设置代理设置。(OCPBUGS-35818)

- 当在包含多个 CIDR 块的 VPC 上安装集群时，如果机器网络被配置为使用 install-config.yaml 文件中的非默认 CIDR 块，安装会失败。(OCPBUGS-35054)

- 当在配置了多路径的 IBM Power® 上安装或在带有虚拟 SCSI 存储的单个 VIOS 主机上安装和配置 OpenShift Container Platform 4.16 集群时，启用了多路径的 CoreOS 节点无法引导。此行为是正常的，因为只有一个路径可用于该节点。(OCPBUGS-32290)

- 在 cgroupv2 上使用 CPU 负载均衡时，如果另一个可访问专用 CPU 的 pod 已存在，pod 无法启动。当 pod 被删除并快速创建来替换它时，可能会发生这种情况。作为临时解决方案，请确保旧 pod 在尝试创建新 pod 前完全终止。(OCPBUGS-34812)

- 在使用 512 模拟磁盘的系统上启用 LUKS 加密会导致置备失败，系统会在 initramfs 中启动紧急 shell。这是因为在增大分区时，s fdisk 中的协调错误。作为临时解决方案，您可以使用 Ignition 执行调整大小。(OCPBUGS-35410)

- OpenShift Container Platform 版本 4.16 断开连接的安装在 IBM Power® Virtual Server 上会失败。(OCPBUGS-36250)

- 当前的 PTP grandmaster 时钟(T-GM)实现具有单一国家 Marine Electronics Association (NMEA)发送的来自 GNSS 的生成器，而无需备份 NMEA 句子生成器。如果在到达 e810 NIC 前丢失 NMEA 句子，则 T-GM 无法同步网络同步链中的设备，PTP Operator 会报告错误。当 NMEA 字符串丢失时，可以报告 FREERUN 事件。在解决这个限制前，T-GM 不支持 PTP 时钟保留状态。(OCPBUGS-19838)

- 当 worker 节点的 Topology Manager 策略时，NUMA 感知辅助 pod 调度程序不会遵守这个变化，这可能会导致调度决策和意外的拓扑关联性错误。作为临时解决方案，通过删除 NUMA 感知调度程序 pod 来重启 NUMA 感知调度程序。(OCPBUGS-34583)

- 由于 Kubernetes 存在问题，CPU Manager 无法从最后一个 pod 返回到可用 CPU 资源池的最后一个 pod 资源。如果后续 pod 被接受到该节点，则这些资源可分配。但是，此 pod 会变为最后一个 pod，并且再次，CPU 管理器无法将此 pod 的资源返回到可用的池。

  此问题会影响 CPU 负载均衡功能，这取决于 CPU Manager 将 CPU 释放到可用池。因此，非保证的 pod 可能会以较少的 CPU 运行。作为临时解决方案，请在受影响节点上调度具有 best-effort CPU Manager 策略的 pod。此 pod 是最后一个接受的 pod，这样可确保资源正确释放到可用池。(OCPBUGS-17792)

- 应用 SriovNetworkNodePolicy 资源后，在 SR-IOV Network Operator Webhook 协调过程中可能会替换 CA 证书。因此，在应用 SR-IOV 网络节点策略时，您可能会看到 未知颁发机构 错误。作为临时解决方案，请尝试重新应用失败的策略。(OCPBUGS-32139)

- 如果您删除了带有 vfio-pci 驱动程序类型的虚拟功能的 SriovNetworkNodePolicy 资源，SR-IOV Network Operator 无法协调策略。因此，sriov-device-plugin pod 进入持续重启循环。作为临时解决方案，请删除影响物理功能的所有剩余的策略，然后重新创建它们。(OCPBUGS-34934)

- 如果控制器 pod 在克隆进行时终止，Microsoft Azure File 克隆持久性卷声明(PVC)将保持在 Pending 状态。要解决这个问题，请删除任何受影响的克隆 PVC，然后重新创建 PVC。(OCPBUGS-35977)

- Microsoft Azure 中没有 azcopy （在工具运行复制作业）可用的日志修剪，因此最终可能会导致控制器 pod 的 root 设备填满，您必须手动清理。(OCPBUGS-35980)

- 当 openshift-network-operator 命名空间中 ConfigMap 对象的 mtu 参数缺失时，有限的实时迁移方法会停止。

  在大多数情况下，ConfigMap 对象的 mtu 字段会在安装过程中由 mtu-prober 作业创建。但是，如果集群从早期版本（如 OpenShift Container Platform 4.4.4）升级，则 ConfigMap 对象可能不存在。

  作为临时解决方案，您可以在启动有限的实时迁移过程前手动创建 ConfigMap 对象。例如：

  ```
  apiVersion: v1
  kind: ConfigMap
  metadata:
    name: mtu
  ```

```
  namespace: openshift-network-operator
data:
  mtu: "1500" 1
```

1

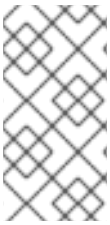
mtu 值必须与节点接口的 MTU 一致。

(OCPBUGS-35316)

1.9. 异步勘误更新

OpenShift Container Platform 4.16 的安全更新、程序错误修正、功能增强更新将会通过红帽网络以异步勘误的形式发布。所有的 OpenShift Container Platform 4.16 勘误都可以通过红帽客户门户网站 获得。OpenShift Container Platform 生命周期包括了详细的与异步勘误相关的内容。

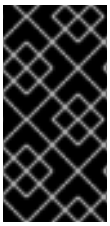
红帽客户门户网站用户可以在 Red Hat Subscription Management (RHSM)的帐户设置中启用勘误通知。当勘误通知被启用后，每当用户注册的系统相关勘误被发布时，用户会收到电子邮件通知。



注意

红帽客户门户网站用户帐户必须注册并消耗 OpenShift Container Platform 权利才可以生成 OpenShift Container Platform 勘误通知电子邮件。

本节的内容将会持续更新，以提供以后发行的与 OpenShift Container Platform 4.16 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.16.z）的具体信息会包括在相应的子章节中。此外，在发行公告中因为空间限制没有包括在其中的勘误内容也会包括在这里的相应的子章节中。



重要

对于任何 OpenShift Container Platform 发行版本，请仔细参阅有关 更新集群 的说明。

1.9.1. RHSA-2024:0041 - OpenShift Container Platform 4.16.0 镜像发行版本、程序错误修正和安全更新公告

发布日期：24 年 6 月 27 日

OpenShift Container Platform release 4.16.0 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:0041 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:0045 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.16.0 --pullspecs
```