OpenShift Container Platform 4.8

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: 2023-04-19

OpenShift Container Platform 4.8 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

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

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 4.8 发行注记

Red Hat OpenShift Container Platform 为软件开发人员和 IT 机构提供了一个混合云应用平台。使用这个平台可以在配置和管理成本最小化的情况下，利用安全、可扩展的资源部署新的或已有的应用程序。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-2021:2438）现已正式发布。此发行版本使用 Kubernetes 1.21 和 CRI-O 运行时。OpenShift Container Platform 4.8 的新功能、改变以及已知的问题包括在此文档中。

红帽没有公开发布 OpenShift Container Platform 4.8.0，而是发布了 OpenShift Container Platform 4.8.2 作为 GA 版本。

OpenShift Container Platform 4.8 集群位于 https://console.redhat.com/openshift。您可以通过 OpenShift Container Platform 的 Red Hat OpenShift Cluster Manager 应用程序在内部环境或云环境中部署 OpenShift 集群。

OpenShift Container Platform 4.8 需要运行在 Red Hat Enterprise Linux（RHEL）7.9 或更高版本，或 Red Hat Enterprise Linux CoreOS 4.8 上。

对于 control plane，必须使用 RHCOS 机器，对于计算（compute）机器，可以使用 RHCOS 或 Red Hat Enterprise Linux（RHEL）7.9 或更高版本。

重要

因为计算机器只支持 RHEL 7.9 或更高版本，所以不能将 RHEL 计算机器升级到 RHEL 8。

OpenShift Container Platform 4.8 是一个延长更新支持（EUS）发行版本。如需了解更多与 Red Hat OpenShift EUS 相关的信息，请参阅 OpenShift 生命周期和 OpenShift EUS 概述。

随着 OpenShift Container Platform 4.8 的发布，版本 4.5 现在已结束生命周期。如需更新相关信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

1.2. 使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。

作为这个工作的一部分，在这个版本里有以下更改：

- OpenShift Docs GitHub 存储库 **master** 分支已重命名为 **main**。
- 我们已经开始逐渐将术语"master"替换为"control plane"。您会注意到，在这个文档中这两个术语都会使用，其中 "master"会使用括号括起。例如 "... the control plane node (also known as the master node)".在以后的发行版本中，我们将会将其更新为"control plane 节点"。

1.3. 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 。

1.4. 新功能及功能增强

此版本对以下方面进行了改进。

1.4.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.4.1.1. RHCOS 现在使用 RHEL 8.4

RHCOS 现在在 OpenShift Container Platform 4.8 中使用 Red Hat Enterprise Linux (RHEL) 8.4，以及 OpenShift Container Platform 4.7.24 及更高版本。这可让您获得最新的修复、功能和增强，以及最新的硬件支持和驱动程序更新。OpenShift Container Platform 4.6 是一个延长更新支持（EUS）版本，其整个生命周期中将继续使用 RHEL 8.2 EUS 软件包。

1.4.1.2. 使用流元数据改进引导镜像自动化

流元数据提供标准化的 JSON 格式，用于在 OpenShift Container Platform 安装过程中将元数据注入集群中。为改进自动化，新的 **openshift-install coreos print-stream-json** 命令提供了一种以可脚本、机器可读格式打印流元数据的方法。

对于用户置备的安装，**openshift-install** 二进制文件包含对经过测试用于 OpenShift Container Platform 的 RHCOS 引导镜像版本的引用，如 AWS AMI。现在，您可以使用 https://github.com/coreos/stream-metadata-go 官方 **stream-metadata-go** 库从 Go 程序解析流元数据。

如需更多信息，请参阅使用流元数据访问 RHCOS AMI。

1.4.1.3. Butane 配置转换程序（Butane config transpiler）简化了机器配置的创建

OpenShift Container Platform 现在包含 Butane config transpiler，可协助生成和验证机器配置。现在，文档建议使用 Butane 为 LUKS 磁盘加密、引导磁盘镜像和自定义内核模块创建机器配置。

如需更多信息，请参阅使用 Butane 创建机器配置。

1.4.1.4. 在云平台上进入自定义 chrony.conf 默认

如果云管理员已经设置了自定义 **/etc/chrony.conf** 配置，RHCOS 不再默认在云平台上设置 **PEERNTP=no** 选项。否则，默认仍会设置 **PEERNTP=no** 选项。如需更多信息，请参阅 BZ#1924869。

1.4.1.5. 在裸机安装时启用多路径

现在，OpenShift Container Platform 4.8 或更高版本置备的节点支持在裸机安装过程中启用多路径。您可以通过在 **coreos-installer install** 命令中附加内核参数来启用多路径，以便安装的系统本身从第一次引导开始使用多路径。虽然安装后支持仍可通过机器配置激活多路径，但建议在安装过程中为从 OpenShift Container Platform 4.8 开始置备的节点启用多路径。

如需更多信息，请参阅在 RHCOS 上启用使用内核参数的多路径。

1.4.2. 安装和升级

1.4.2.1. 将集群安装到 Azure 上的现有空资源组

现在，您可以通过在 **install-config.yaml** 文件中定义 **platform.azure.resourceGroupName** 字段来定义一个已存在的资源组，以便在 Azure 上安装集群。此资源组必须为空，且仅适用于单个集群；集群组件假定资源组中所有资源的所有权。

如果您将安装程序的服务主体范围限制到这个资源组，您必须确保您的环境中安装程序使用的所有其他资源都有必要的权限，如公共 DNS 区和虚拟网络。使用安装程序销毁集群会删除用户定义的资源组。

1.4.2.2. 为 AWS 上的集群使用现有 IAM 角色

现在，您可以通过在 **install-config.yaml** 文件中设置 **compute.platform.aws.iamRole** 和 **controlPlane.platform.aws.iamRole** 字段来为机器实例配置集定义预先存在的 Amazon Web Services（AWS）IAM 角色。这可让您为 IAM 角色执行以下操作：

- 匹配命名方案
- 包括预定义的权限边界

1.4.2.3. 在 AWS 中使用预先存在的 Route53 托管私有区

现在，您可以通过在 **install-config.yaml** 文件中设置 **platform.aws.hostedZone** 字段来为集群定义一个现有 Route 53 私有托管区。您只能在提供自己的 VPC 时使用已存在的托管区。

1.4.2.4. 在机器 CIDR 中增大 GCP 子网的大小

Google Cloud Platform（GCP）的 OpenShift Container Platform 安装程序现在在机器 CIDR 中尽可能多地创建子网。这允许集群使用机器 CIDR 大小来容纳集群中的节点数量。

1.4.2.5. 改进了升级持续时间

在这个版本中，将守护进程集部署到所有节点的集群 Operator 的升级周期会被显著降低。例如，一个 250 个节点的测试集群的升级持续时间从 7.5 小时减少到 1.5 小时，这代表为每个额外节点进行升级的时间被缩减为少于一分钟。

注意

这个更改不会影响机器配置池推出部署的时间。

1.4.2.6. MCO 在报告更新完成前等待所有机器配置池进行更新

更新时，如果任何机器配置池没有完成更新，Machine Config Operator（MCO）现在会在 machine-config Cluster Operator 中报告 **Upgradeable=False** 条件。这个状态会阻止将来的次要更新，但不会阻止将来的补丁更新或当前更新。在以前的版本中，MCO 仅根据 control plane 机器配置池的状态报告 **Upgradeable** 状态，即使 worker 池没有更新。

1.4.2.7. 使用 Fujitsu iRMC 在裸机节点上安装

在 OpenShift Container Platform 4.8 中，您可以在裸机上部署安装程序置备的集群时，使用 Fujitsu 硬件和 Fujitsu iRMC 基本管理控制器协议。目前，Fujitsu 支持 iRMC S5 固件版本 **3.05P** 及更高版本，用于裸机上的安装程序置备安装。OpenShift Container Platform 4.8 的改进和程序错误修复包括：

- 支持 iRMC 硬件上的软电源关闭。
- 安装程序在裸机节点上部署 control plane 后停止调配服务。如需更多信息，请参阅 BZ#1949859。

- 在 bootstrap **keepalived** 检查中添加 Ironic 健康检查。如需更多信息，请参阅 BZ#1949859。
- 验证 control plane 节点上的单播 peers 列表不是空的。如需更多信息，请参阅 BZ#1957708。
- 更新 Bare Metal Operator 以匹配 iRMC PowerInterface。如需更多信息，请参阅 BZ#1957869。
- 更新 **pyghmi** 库版本。如需更多信息，请参阅 BZ#1920294。
- 更新 Bare Metal Operator 以解决缺少的 IPMI 凭证。如需更多信息，请参阅 BZ#1965182。
- 从 **enabled_bios_interfaces** 中删除 iRMC。如需更多信息，请参阅 BZ#1969212。
- 在裸机 pod 定义中添加 **ironicTlsMount** 和 **inspectorTlsMount**。如需更多信息，请参阅 BZ#1968701。
- 为 iRMC 服务器禁用 RAID 功能。如需更多信息，请参阅 BZ#1969487。
- 为所有驱动程序禁用 RAID。如需更多信息，请参阅 BZ#1969487。

1.4.2.8. RHOSP 上带有安装程序置备基础架构的集群的 SR-IOV 网络支持

现在，您可以在 RHOSP 上部署集群，这些集群使用单根 I/O 虚拟化（SR-IOV）网络用于计算机器。

如需更多信息，请参阅在支持 SR-IOV 连接计算机器的 OpenStack 上安装集群 。

1.4.2.9. ironic Python 代理支持 VLAN 接口

在这个版本中，Ironic Python 代理会在内省期间在接口列表中报告 VLAN 接口。此外，IP 地址包含在接口中，允许正确创建 CSR。因此，可以为所有接口（包括 VLAN 接口）获取 CSR。如需更多信息，请参阅 BZ#1888712。

1.4.2.10. 使用 OpenShift 更新服务进行无线更新

OpenShift 更新服务（OpenShift Update Service，简称 OSUS）为 OpenShift Container Platform（包括 Red Hat Enterprise Linux CoreOS（RHCOS））提供了无线更新（over-the air update）功能。它以前只能作为红帽托管服务（位于公共 API 后面）进行访问，但现在可以在本地安装。OpenShift Update Service 由 Operator 和一个或多个应用程序实例组成，现在在 OpenShift Container Platform 4.6 及更高版本中正式发布。

如需更多信息，请参阅了解 OpenShift Update Service。

1.4.3. Web 控制台

1.4.3.1. 自定义控制台路由现在使用新的 CustomDomains 集群 API

对于 **console** 和 **downloads** 路由，自定义路由功能现在会使用新的 **ingress** 配置路由配置 API **spec.componentRoutes**Console Operator 配置已包含自定义路由自定义，但仅适用于 **console** 路由。通过 **console-operator** 配置的路由配置已弃用。因此，如果 **console** 自定义路由在 **ingress** 配置和 **console-operator** 配置中都设置时，新的 **ingress** 配置自定义路由配置有高的优先级。

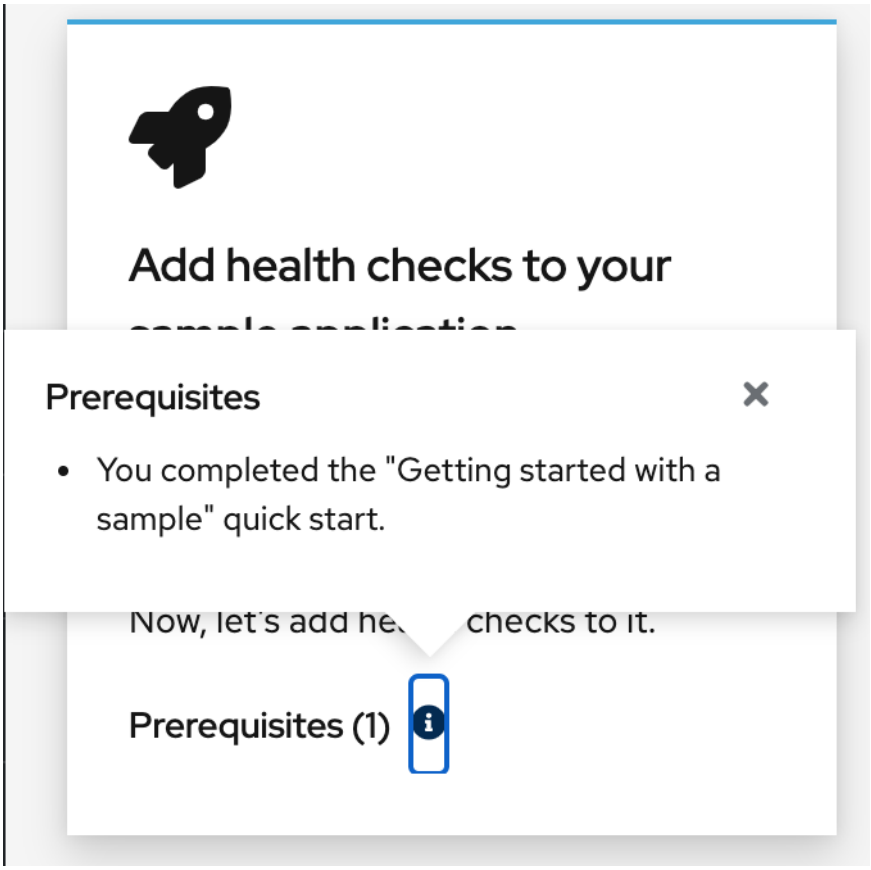
如需更多信息，请参阅自定义控制台路由。

1.4.3.2. 从快速入门访问代码片段

现在，您可以在 web 控制台的 Quick Start 中包含 CLI 片段时执行它。要使用这个功能，您必须首先安装 Web Terminal Operator。如果您没有安装 Web Terminal Operator，则 web 终端中执行的 web 终端和代码片段操作将不存在。另外，无论您是否安装了 Web Terminal Operator，您都可以将代码片段复制到剪贴板中。

1.4.3.3. 改进了快速入门先决条件的介绍

在以前的版本中，快速入门先决条件以组合文本而不是 Quick Start 卡中的列表显示。考虑到可扩展性，现在会在弹出窗口中显示先决条件，而不是在卡中显示。



1.4.3.4. Developer Perspective (开发者视角)

在这个版本中，您可以：

- 使用自定义管道模板从 Git 存储库创建和部署应用程序。这些模板覆盖 OpenShift Pipelines 1.5 及之后的版本提供的默认管道模板。
- 根据它们的认证级别过滤 Helm chart，并在 **Developer Catalog** 中查看所有 Helm chart。
- 使用 **Add** 页面中的选项来创建应用程序和相关服务，并在 OpenShift Container Platform 上部署这些应用程序和服务。**Add** 页选项包括：**Getting started resources**, **Creating applications using samples**, **Build with guided documentation**, 和 **Explore new developer features**。
- 在管道构建器中创建管道时使用工作区。您还可以在管道中添加触发器，以便您可以使用任务支持管道中的工作区。
- 使用 **Developer** 视角的 **Topology** 视图中的 JAR 文件来部署 Java 应用程序。
- 在 OpenShift Container Platform 中创建多个事件源类型，并将这些源类型连接到 sink。您可以在 OpenShift Container Platform 集群中将功能部署为 Knative 服务，并将它们连接到 sink。

- 使用管道中的 **finally** 任务并行执行命令。
- 使用 **Add Task** 表单中的代码帮助来访问任务参数值。要查看管道参数，以及引用该特定管道参数的正确语法，请转至相应的文本字段。
- 仅在满足特定条件后运行一个 **Task**。使用 **when** 字段配置任务的执行，并列出对 **when** 表达式的一系列引用。

1.4.4. IBM Z 和 LinuxONE

在这个版本中，IBM Z 和 LinuxONE 与 OpenShift Container Platform 4.8 兼容。可以使用 z/VM 或 RHEL KVM 进行安装。有关安装说明，请参阅以下文档：

- 在 IBM Z 和 LinuxONE 中使用 z/VM 安装集群
- 在受限网络中的 IBM Z 和 LinuxONE 中使用 z/VM 安装集群
- 在 IBM Z 和 LinuxONE 中使用 RHEL KVM 安装集群
- 在受限网络中的 IBM Z 和 LinuxONE 上使用 RHEL KVM 安装集群

主要改进
IBM Z 和 LinuxONE 中的 OpenShift Container Platform 4.8 支持以下新功能：

- IBM Z 和 LinuxONE 上的、用户置备安装的 OpenShift Container Platform 4.8 支持 RHEL 8.3 或更高版本的 KVM 作为的虚拟机监控程序（hypervisor）。现在还支持使用静态 IP 地址安装并在受限网络中安装。
- 加密存储在 etcd 中的数据.
- 4K FCP 块设备.
- 三节点集群支持.

支持的功能
IBM Z 和 LinuxONE 也支持以下功能：

- 多路径（Multipathing）
- 使用 iSCSI 的持久性存储
- 使用本地卷的持久性存储（本地存储 Operator）
- 使用 hostPath 的持久性存储
- 使用 Fibre Channel 持久性存储
- 使用 Raw Block 的持久性存储
- 初始安装 OpenShift Container Platform 4.8 的 OVN-Kubernetes
- SCSI 磁盘中的 z/VM 模拟 FBA 设备

以下功能仅适用于 IBM Z 上的 OpenShift Container Platform 4.8：

- IBM Z /LinuxONE 为附加的 ECKD 存储的虚拟机启用了 HyperPAV

限制
请注意，OpenShift Container Platform 对 IBM Z 和 LinuxONE 有如下限制：

- 用于 IBM Z 的 OpenShift Container Platform 不包括以下技术预览功能：
  - 精度时间协议 (PTP) 硬件
- 以下 OpenShift Container Platform 功能不被支持：
  - 使用机器健康检查功能自动修复损坏的机器
  - CodeReady Containers (CRC)
  - 在节点上控制过量使用和管理容器密度
  - CSI 卷克隆
  - CSI 卷快照
  - FIPS 加密
  - Helm 命令行界面 (CLI) 工具
  - Multus CNI 插件
  - NVMe
  - OpenShift Metering
  - OpenShift Virtualization
  - 在 OpenShift Container Platform 部署过程中启用 Tang 模式磁盘加密。
- worker 节点必须运行 Red Hat Enterprise Linux CoreOS（RHCOS）
- 必须使用 NFS 或其他支持的存储协议来置备持久性共享存储
- 必须使用本地存储（如 iSCSI、FC 或者带有 DASD、FCP 或 EDEV/FBA 的 LSO）置备持久性非共享存储

1.4.5. IBM Power 系统

在这个版本中，IBM Power Systems 与 OpenShift Container Platform 4.8 兼容。有关安装说明，请参阅以下文档：

- 在 IBM Power 系统上安装集群
- 在受限网络中的 IBM Power Systems 上安装集群

主要改进
使用 OpenShift Container Platform 4.8 的 IBM Power Systems 支持以下新功能：

- 加密数据存储在 etcd 中
- 三节点集群支持
- Multus SR-IOV

支持的功能
IBM Power 系统还支持以下功能：

- 目前，支持五个 Operator：
  - Cluster-Logging-Operator
  - Cluster-NFD-Operator
  - Elastic Search-Operator
  - Local Storage Operator
  - Cluster Network Operator
- 多路径（Multipathing）
- 使用 iSCSI 的持久性存储
- 使用本地卷的持久性存储（本地存储 Operator）
- 使用 hostPath 的持久性存储
- 使用 Fibre Channel 持久性存储
- 使用 Raw Block 的持久性存储
- 初始安装 OpenShift Container Platform 4.8 的 OVN-Kubernetes
- 4K 磁盘支持
- NVMe

限制
OpenShift Container Platform 在 IBM Power 上会有以下限制：

- 用于 IBM Power 系统的 OpenShift Container Platform 不包括以下技术预览功能：
  - 精度时间协议 (PTP) 硬件
- 以下 OpenShift Container Platform 功能不被支持：
  - 使用机器健康检查功能自动修复损坏的机器
  - CodeReady Containers (CRC)
  - 在节点上控制过量使用和管理容器密度
  - FIPS 加密
  - Helm 命令行界面 (CLI) 工具
  - OpenShift Metering
  - OpenShift Virtualization
  - 在 OpenShift Container Platform 部署过程中启用 Tang 模式磁盘加密。
- worker 节点必须运行 Red Hat Enterprise Linux CoreOS（RHCOS）

- 持久性存储必须是使用本地卷、网络文件系统（NFS）或 Container Storage Interface（CSI）的 Filesystem 类型

1.4.6. 安全性与合规性

1.4.6.1. Audit 会将 OAuth 访问令牌登出请求记录在日志中

现在， **Default** 审计日志策略会记录 OAuth 访问令牌创建（登录）和删除（注销）请求的请求正文。在以前的版本中，删除请求正文不会被记录。

有关审计日志策略的更多信息，请参阅配置节点审计日志策略。

1.4.6.2. 无头服务的服务证书的通配符主题

为无头服务生成服务服务证书现在包括一个通配符主题，格式为 ***.<service.name>.<service.namespace>.svc**。这允许 TLS 保护连接到单个有状态集 pod，而无需为这些 pod 手动生成证书。

重要

因为生成的证书包含无头服务的通配符主题，因此如果您的客户端必须区分不同的 pod，则不得使用服务 CA。在这种情况下：

- 使用其他 CA 生成各个 TLS 证书。
- 对于定向到单个 pod 且不得被其他 pod 模拟的连接，不接受服务 CA 作为可信 CA。这些连接必须配置为信任用于生成单个 TLS 证书的 CA。

如需更多信息，请参阅添加服务证书。

1.4.6.3. oc-compliance 插件现在可用

Compliance Operator 为 OpenShift Container Platform 集群自动执行许多检查和补救。但是，使集群进入合规的完整过程通常需要管理员与 Compliance Operator API 和其他组件进行交互。**oc-compliance** 插件现在可用，并使进程变得更加容易。

如需更多信息，请参阅使用 **oc-compliance** 插件

1.4.6.4. Kubernetes control plane 的 TLS 安全配置集

Kubernetes API 服务器 TLS 安全配置集设置现在也被 Kubernetes 调度程序和 Kubernetes 控制器管理器实现。

如需更多信息，请参阅配置 TLS 安全配置集。

1.4.6.5. kubelet 的 TLS 安全配置集作为服务器

现在，当作为 Kubernetes API 服务器的 HTTP 服务器时，您可以为 kubelet 设置 TLS 安全配置集。

如需更多信息，请参阅配置 TLS 安全配置集。

1.4.6.6. 支持 bcrypt 密码哈希

在以前的版本中, **oauth-proxy** 命令只允许在用于身份验证的 **htpasswd** 文件中使用 SHA-1 哈希密码。**OAuth-proxy** 现在包含对使用 **bcrypt** 密码散列的 **htpasswd** 条目的支持。如需更多信息，请参阅 BZ#1874322。

1.4.6.7. 使用安装程序置备的集群启用受管的安全引导

OpenShift Container Platform 4.8 支持为置备的 control plane 和 worker 节点自动打开 UEFI 安全引导（Secure Boot）模式，并在删除节点时将其关闭。要使用这个功能，在 **install-config.yaml** 文件中将节点的 **bootMode** 配置设置为 **UEFISecureBoot**。红帽仅在第 10 代 HPE 硬件上支持带有管理的安全引导机制的安装程序置备安装，第 13 代的 Dell 硬件运行固件版本 **2.75.75.75** 或更高版本。如需了解更多详细信息，请参阅 install-config.yaml 文件中配置受管安全引导。

1.4.7. 网络

1.4.7.1. 在带有 OVN-Kubernetes 集群网络供应商的安装程序置备的裸机基础架构上支持双栈

对于安装程序置备的裸机基础架构上的集群，OVN-Kubernetes 集群网络供应商支持 IPv4 和 IPv6 地址系列。

对于安装程序置备的裸机集群从以前的 OpenShift Container Platform 版本升级，您必须转换集群来支持双栈网络。如需更多信息，请参阅转换到 IPv4/IPv6 双栈网络。

1.4.7.2. 在用户置备的基础架构上从 OpenShift SDN 迁移到 OVN-Kubernetes

用户置备的集群支持 OpenShift SDN 集群网络供应商迁移到 OVN-Kubernetes 集群网络供应商。如需更多信息，请参阅从 OpenShift SDN 集群网络供应商迁移。

1.4.7.3. OpenShift SDN 集群网络供应商出口 IP 功能在节点间平衡

现在，当命名空间被分配了多个出口 IP（egress IP）地址时， OpenShift SDN 的 egress IP 功能会以大致相等的方式在命名空间的节点间平衡网络流量。每个 IP 地址必须位于不同的节点上。如需更多信息，请参阅为 OpenShift SDN 配置项目的出口 IP。

1.4.7.4. 网络策略支持选择主机网络 Ingress Controller

使用 OpenShift SDN 或 OVN-Kubernetes 集群网络供应商时，您可以在网络策略规则中选择来自 Ingress Controller 的流量，无论 Ingress Controller 在集群网络还是主机网络上运行。在网络策略规则中，**policy-group.network.openshift.io/ingress: ""** 命名空间选择器标签与来自 Ingress Controller 的流量匹配。您可以继续使用 **network.openshift.io/policy-group: ingress** 命名空间选择器标签，但在以后的 OpenShift Container Platform 发行版本中可能会删除这个旧标签。

在以前的 OpenShift Container Platform 版本中，存在以下限制：

- 使用 OpenShift SDN 集群网络供应商的集群只能通过将 **network.openshift.io/policy-group: ingress** 标签应用到 **default** 命名空间来选择来自主机网络上的 Ingress Controller 的流量。
- 使用 OVN-Kubernetes 集群网络供应商的集群无法从主机网络上的 Ingress Controller 选择流量。

如需更多信息，请参阅关于网络策略。

1.4.7.5. 网络策略支持选择主机网络流量

使用 OVN-Kubernetes 集群网络供应商或 OpenShift SDN 集群网络供应商时，您可以使用 **policy-group.network.openshift.io/host-network: ""** 命名空间选择器在网络策略规则中选择主机网络流量。

1.4.7.6. 网络策略审计日志

如果使用 OVN-Kubernetes 集群网络供应商，您可以为命名空间中的网络策略启用审计日志。日志采用 syslog 兼容格式，可以保存在本地、通过 UDP 连接发送或定向到 UNIX 域套接字。您可以指定是否记录允许、丢弃的连接，以及是否允许和丢弃的连接。如需更多信息，请参阅日志记录网络策略事件。

1.4.7.7. 对 macvlan 额外网络的网络策略支持

您可以使用实现 **NetworkPolicy** API 的 **MultiNetworkPolicy** API 创建适用于 macvlan 额外网络的网络策略。如需更多信息，请参阅配置多网络策略。

1.4.7.8. SR-IOV 支持的硬件

OpenShift Container Platform 4.8 添加了对额外的 Intel 和 Mellanox 网络接口控制器的支持。

- Intel X710、XL710 和 E810
- Mellanox ConnectX-5 Ex

如需更多信息，请参阅支持的设备。

1.4.7.9. SR-IOV Network Operator 的改进

使用 Operator 部署的 Network Resources Injector 被改进，以通过 Downward API 来公开有关巨页请求和限制的信息。当 pod 规格包含巨页请求或限制时，信息会在 **/etc/podnetinfo** 路径中公开。

如需更多信息，请参阅 Downward API 的 Huge page 资源注入 。

1.4.7.10. 跟踪网络流

OpenShift Container Platform 4.8 添加了对将 pod 网络上网络流的元数据发送到网络流收集器的支持。支持以下协议：

- NetFlow
- sFlow
- IPFIX

数据包数据不会发送到网络流收集器。数据包级元数据（如协议、源地址、目标地址、端口号、字节数和其他数据包级别信息）将发送到网络流收集器。

如需更多信息，请参阅跟踪网络流。

1.4.7.11. CoreDNS-mDNS 不再用来将节点名称解析为 IP 地址

OpenShift Container Platform 4.8 及更新的版本包括使用集群成员资格信息生成 A/AAAA 记录的功能。这会将节点名称解析为其 IP 地址。使用 API 注册节点后，集群就可以分布节点信息，而无需使用 CoreDNS-mDNS。这可消除与多播 DNS 关联的网络流量。

1.4.7.12. 将 HTTP 标头名称转换为支持升级到 OpenShift Container Platform 4.8

OpenShift Container Platform 更新至 HAProxy 2.2，它默认将 HTTP 标头名称更改为小写，例如将 **Host: xyz.com** 改为 **host: xyz.com**。对于对 HTTP 标头名称大小写敏感的传统应用程序，请使用 Ingress Controller **spec.httpHeaders.headerNameCaseAdjustments** API 字段来适应旧的应用程序，直到它们被修复为止。当 HAProxy 2.2 可用时，在升级 OpenShift Container Platform 前，确保使用 **spec.httpHeaders.headerNameCaseAdjustments** 来添加必要的配置。

如需更多信息，请参阅转换 HTTP 标头问题单。

1.4.7.13. OpenShift Container Platform 4.8 有更严格的 HTTP 标头验证

OpenShift Container Platform 更新至 HAProxy 2.2，它对 HTTP 标头强制执行一些额外的限制。这些限制旨在缓解应用中可能存在的安全性弱点。特别是，如果一个请求没有在请求行和 HTTP **host** 标头中同时指定或忽略端口号，则可能拒绝 HTTP 请求行中指定主机名的 HTTP 客户端请求。例如，带有标头 **host: hostname** 的请求 **GET http://hostname:80/path** 将被拒绝并带有 HTTP 400 "Bad request" 响应，因为请求行指定了端口号，而 **host** 标头没有指定端口号。这个限制的目的是减少 request smuggling 攻击。

在启用了 HTTP/2 时，在以前的 OpenShift Container Platform 版本中也可以启用了这个严格的 HTTP 标头验证。这意味着，您可以通过在 OpenShift Container Platform 4.7 集群中启用 HTTP/2 并检查 HTTP 400 错误来测试有问题的客户端请求。有关如何启用 HTTP/2 的详情，请参考启用 HTTP/2 Ingress 连接。

1.4.7.14. 在 GCP 上为 Ingress Controller 配置全局访问

OpenShift Container Platform 4.8 添加了对使用内部负载均衡器在 GCP 上创建的 Ingress Controller 的全局访问选项的支持。启用全局访问选项后，同一 VPC 网络和计算区域内任何区域中的客户端都可以访问集群中运行的工作负载。

如需更多信息，请参阅为 GCP 上的 Ingress Controller 配置全局访问 。

1.4.7.15. 设置 Ingress Controller 线程数

OpenShift Container Platform 4.8 添加了对设置线程数的支持，以增加集群可以处理的进入连接量。

如需更多信息，请参阅设置 Ingress Controller 线程计数。

1.4.7.16. 为 Ingress Controller 配置 PROXY 协议

OpenShift Container Platform 4.8 添加了对在非云平台上为 Ingress Controller 配置 PROXY 协议的支持，特别是 **HostNetwork** 或 **NodePortService** 端点发布策略类型。

如需更多信息，请参阅为 Ingress Controller 配置 PROXY 协议 。

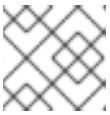
1.4.7.17. control plane 节点上的 NTP 服务器

在 OpenShift Container Platform 4.8 中，安装程序置备的集群可以在 control plane 节点上配置和部署网络时间协议（NTP）服务器，并在 worker 节点上配置和部署 NTP 客户端。这可让 worker 从 control plane 节点上的 NTP 服务器检索日期和时间，即使从可路由的网络断开连接。您也可以在部署后配置和部署 NTP 服务器和 NTP 客户端。

1.4.7.18. Kuryr 的默认 API 负载均衡器管理更改

在带有 Kuryr-Kubernetes 的 Red Hat OpenStack Platform（RHOSP）上的 OpenShift Container Platform 4.8 部署中，**default/kubernetes** 服务的 API 负载均衡器不再由 Cluster Network Operator（CNO）管理，而是由 kuryr-controller 本身管理。这意味着：

- 升级到 OpenShift Container Platform 4.8 时， **default/kubernetes** 服务会停机。



注意

在没有 Open Virtual Network（OVN）Octavia 的部署中，应该有更多停机时间。

- **default/kubernetes** 负载均衡器不再需要使用 Octavia Amphora 驱动程序。如果 OpenStack 云中有 **default/kubernetes** 服务，则 OVN Octavia 将使用它来实现。

1.4.7.19. 安装后启用置备网络

通过为裸机集群提供支持的安装程序和安装程序置备安装，可以在没有 **provisioning** 网络的情况下部署集群。在 OpenShift Container Platform 4.8 及更新版本中，您可以使用 Cluster Baremetal Operator（CBO）在安装后启用 **provisioning** 网络。

1.4.7.20. 配置要在 control plane 上运行的网络组件

如果您需要在裸机安装中的 control plane 节点上运行虚拟 IP（VIP）地址，您必须将 **apiVIP** 和 **ingressVIP** VIP 地址配置为仅在 control plane 节点上运行。默认情况下，OpenShift Container Platform 允许 worker 机器配置池中的任何节点托管 **apiVIP** 和 **ingressVIP** VIP 地址。由于许多裸机环境在与 control plane 节点独立的子网中部署 worker 节点，因此将 **apiVIP** 和 **ingressVIP** 虚拟 IP 地址配置为完全在 control plane 节点上运行，从而防止在不同的子网中部署 worker 节点导致问题。如需了解更多详细信息，请参阅配置在 control plane 上运行的网络组件。

1.4.7.21. 为 apiVIP 和 ingressVIP 流量配置外部负载均衡器

在 OpenShift Container Platform 4.8 中，您可以配置一个外部负载均衡器来处理 Red Hat OpenStack Platform (RHOSP) 和裸机安装程序置备的集群的 **apiVIP** 和 **ingressVIP** 流量。当使用 VLAN 在负载均衡服务和 control plane 节点之间路由流量时，外部负载平衡服务和 control plane 节点必须在同一个 L2 网络上运行，并使用 VLAN 来路由负载平衡服务和 control plane 节点之间的流量。

VMware 安装程序置备的集群不支持将负载均衡器来处理 **apiVIP** 和 **ingressVIP** 流量。

1.4.7.22. OVN-Kubernetes IPsec 支持双栈网络

OpenShift Container Platform 4.8 为配置为使用双栈网络的集群添加了 OVN-Kubernetes IPsec 支持。

1.4.7.23. OVN-Kubernetes 的出口路由器 CNI

egress router CNI 插件已正式发布。Cluster Network Operator 被改进以支持 **EgressRouter** API 对象。在使用 OVN-Kubernetes 的集群中添加出口路由器的过程已被简化。当您创建出口路由器对象时，Operator 会自动添加网络附加定义和部署。部署的容器集充当出口路由器。

如需更多信息，请参阅使用出口路由器 pod 的注意事项。

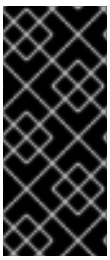
1.4.7.24. OpenShift Container Platform 上的 IP 故障切换支持

现在，裸机上的 OpenShift Container Platform 集群支持 IP 故障切换。IP 故障转移使用 **keepalived** 在一组主机上托管一组外部访问的 VIP 地址。在一个时间点上，每个 VIP 仅由一个主机提供服务。**keepalived** 使用虚拟路由器冗余协议（VRRP）决定在主机集合中使用哪个主机提供 VIP 服务。如果主机不可用，或者 **keepalived** 正在监视的服务没有响应，则 VIP 会切换到主机集中的另外一个主机。这意味着只要主机可用，便始终可以提供 VIP 服务。

如需更多信息，请参阅配置 IP 故障切换。

1.4.7.25. 控制 DNS pod 放置

在 OpenShift Container Platform 4.8 中，您可以使用自定义节点选择器和容限配置 CoreDNS 的守护进程集，使其在特定节点上运行。



重要

以前的 OpenShift Container Platform 版本使用一个针对所有污点的容限配置了 CoreDNS 守护进程集，DNS pod 可以在集群的所有节点上运行，而不会考虑节点污点的情况。OpenShift Container Platform 4.8 默认不再为所有污点配置这个容限。相反，默认为仅为 **node-role.kubernetes.io/master** 污点设置容限。要使 DNS pod 在带有其他污点的节点上运行，您必须配置自定义容限。

如需更多信息，请参阅控制 DNS pod 放置。

1.4.7.26. 在 RHOSP 上运行的集群的供应商网络支持

Red Hat OpenStack Platform（RHOSP）上的 OpenShift Container Platform 集群现在支持所有部署类型的供应商网络。

1.4.7.27. HAProxy 可配置的 tune.maxrewrite 和 tune.bufsize

集群管理员现在可以设置 **headerBufferMaxRewriteByte** 和 **headerBufferBytes** Ingress Controller 调整参数，以配置每个 Ingress Controller 的 **tune.maxrewrite** 和 **tune.bufsize** HAProxy 内存选项。

如需更多信息，请参阅 Ingress Controller 配置参数。

1.4.8. 存储

1.4.8.1. 使用 GCP PD CSI 驱动程序 operator 的持久性存储已正式发布

Google Cloud Platform（GCP）持久性磁盘（PD）Container Storage Interface（CSI）驱动程序会在 GCP 环境中自动部署和管理，允许您动态置备这些卷，而无需手动安装驱动程序。此功能以前在 OpenShift Container Platform 4.7 中作为技术预览功能，现在在 OpenShift Container Platform 4.8 中正式发布并启用。

如需更多信息，请参阅 GCP PD CSI Driver Operator。

1.4.8.2. 使用 Azure Disk CSI Driver Operator 的持久性存储（技术预览）

Azure Disk CSI Driver Operator 默认提供一个存储类,您可以使用它来创建持久性卷声明（PVC）。管理此驱动程序的 Azure Disk CSI Driver Operator 只是一个技术预览。

如需更多信息，请参阅 Azure Disk CSI Driver Operator。

1.4.8.3. 使用 vSphere CSI Driver Operator 的持久性存储（技术预览）

vSphere CSI Driver Operator 默认提供一个存储类，您可以使用它来创建持久性卷声明（PVC）。管理此驱动程序的 vSphere CSI Driver Operator 只是一个技术预览。

如需更多信息，请参阅 vSphere CSI Driver Operator。

1.4.8.4. 自动 CSI 迁移（技术预览）

从 OpenShift Container Platform 4.8 开始，以下树内（in-tree）卷插件自动迁移到对应的 CSI 驱动程序作为技术预览功能：

- Amazon Web Services（AWS）Elastic Block Storage（EBS）
- OpenStack Cinder

如需更多信息，请参阅自动 CSI 迁移。

1.4.8.5. 已删除 AWS EFS（技术预览）功能的外部置备程序

Amazon Web Services（AWS）Elastic File System（EFS）技术预览功能已被删除，且不再被支持。

1.4.8.6. 改进了对 RHOSP 上运行的集群 Cinder 卷可用性区的控制

现在，您可以在安装过程中为 Cinder 卷选择可用性区域。您还可以将特定可用区中的 Cinder 卷用于镜像 registry。

1.4.9. Registry

1.4.10. Operator 生命周期

1.4.10.1. 增强了针对管理员的错误报告

使用 Operator Lifecycle Manager（OLM）安装 Operator 的集群管理员可能会遇到与当前 API 或低级别 API 相关的错误条件。在以前的版本中，很难了解 OLM 无法履行安装或更新 Operator 的请求。这些错误的范围包括一些微不足道的问题（如对象属性中的拼写错误或缺少 RBAC 等）以及一些比较复杂的问题（如因为元数据解析而无法从目录中加载项目）。

对于管理员，应该可以在不需要了解各种低级别 API 的交互过程或访问 OLM pod 日志的情况下，就可以成功调试这些问题，所以 OpenShift Container Platform 4.8 在 OLM 中引入了以下增强功能，以便为管理员提供更易理解的错误报告和消息：

1.4.10.2. 重试安装计划

安装计划由 **InstallPlan** 对象定义，可能会遇到临时错误，例如，因为 API 服务器可用性或其他写入器冲突。在以前的版本中，这些错误会导致部分应用的安装计划终止需要手动清理。在这个版本中，Catalog Operator 在安装计划执行过程中重试错误最多一分钟。新的 **.status.message** 字段在进行重试时提供人类可读指示。

1.4.10.3. 它代表无效的 Operator 组

在没有 Operator 组或多个 Operator 组的命名空间中创建订阅会导致 Operator 安装停止，并永久保留在 **phase=Installing** 中。在这个版本中，安装计划会立即转换为 **phase=Failed**，以便管理员可以更正无效的 Operator 组，然后删除并重新创建订阅。

1.4.10.4. 当找不到候选 Operator 时报告

当命名空间中依赖项解析失败时创建的 **ResolutionFailed** 事件现在在命名空间包含引用的目录源中不存在的软件包或频道的订阅时提供更具体的文本。在以前的版本中，这个消息比较通用：

> no candidate operators found matching the spec of subscription '<name>'

在这个版本中，信息更为具体：

Operator 不存在

> no operators found in package <name> in the catalog referenced by subscription <name>

目录（Catalog）不存在

> no operators found from catalog <name> in namespace openshift-marketplace referenced by subscription <name>

频道不存在

> no operators found in channel <name> of package <name> in the catalog referenced by subscription <name>

集群服务版本（CSV）不存在

> no operators found with name <name>.<version> in channel <name> of package <name> in the catalog referenced by subscription <name>

1.4.11. Operator 开发

1.4.11.1. 将 Operator 项目从软件包清单格式迁移到捆绑包格式

OpenShift Container Platform 4.8 及更高版本中删除了对 Operator 的传统软件包清单格式的支持。从 OpenShift Container Platform 4.6 开始，捆绑包格式是 Operator Lifecycle Manager（OLM）的首选 Operator 打包格式。如果您有一个 Operator 项目最初以软件包清单格式创建（已弃用），则可以使用 Operator SDK **pkgman-to-bundle** 命令将项目迁移到捆绑包格式。

如需更多信息，请参阅迁移软件包清单项目到捆绑包格式。

1.4.11.2. 发布包含捆绑 Operator 的目录

要安装和管理 Operator，Operator Lifecycle Manager（OLM）要求 Operator 捆绑包列在索引镜像中，该镜像由集群中的目录引用。作为 Operator 作者，您可以使用 Operator SDK 为 Operator 及其所有依赖项创建一个包含捆绑包的索引。这可用于测试远程集群并发布到容器 registry。

如需更多信息，请参阅发布包含捆绑的 Operator 的目录。

1.4.11.3. 增强的 Operator 升级测试

Operator SDK 的 **run bundle-upgrade** 子命令通过为以后的版本指定捆绑包镜像来自动触发已安装的 Operator 以升级到更新的版本。在以前的版本中，子命令只能升级最初使用 **run bundle** 子命令安装的 Operator。在这个版本中，**run bundle-upgrade** 还可用于最初与传统 Operator Lifecycle Manager（OLM）工作流一起安装的 Operator。

如需更多信息，请参阅在 Operator Lifecycle Manager 上测试 Operator 升级。

1.4.11.4. 控制与 OpenShift Container Platform 版本的 Operator 兼容性

当从 OpenShift Container Platform 版本中删除 API 时，在该集群版本上运行的仍使用删除的 API 的 Operator 将不再正常工作。作为 Operator 作者，您应该计划更新 Operator 项目，以适应 API 弃用和删除情况，以避免 Operator 用户中断。

如需了解更多与 OpenShift Container Platform 版本的Operator 兼容性，请参阅控制与 OpenShift Container Platform 版本的 Operator 兼容性。

Builds

1.4.11.5. 按策略划分的构建数量的新 Telemetry 指标

Telemetry 包括一个新的 **openshift:build_by_strategy:sum** 量表指标，它将按照策略类型向 Telemeter 客户端发送构建数量。此指标可让站点可靠性工程师（SRE）和产品经理查看在 OpenShift Container Platform 集群上运行的构建类型。

1.4.11.6. 挂载自定义 PKI 证书颁发机构

在以前的版本中，构建无法使用有时需要的集群 PKI 证书颁发机构来访问公司工件存储库。现在，您可以通过将 **mountTrustedCA** 设置为 **true**，将 **BuildConfig** 对象配置为挂载集群自定义 PKI 证书颁发机构。

1.4.12. 镜像

1.4.13. 机器 API

1.4.13.1. 使用集群自动扩展将 vSphere 中运行的机器扩展到零，并从零扩展

在 vSphere 中运行机器时，您可以在 **MachineAutoscaler** 资源定义中将 **minReplicas** 值设置为 **0**。当将此值设置为 **0** 时，取决于机器是否在使用，集群自动扩展器会将机器集缩到零，或从零进行扩展。如需更多信息，请参阅 MachineAutoscaler 资源定义。

1.4.13.2. 自动轮转 kubelet-ca.crt 不需要节点排空或重启

自动轮转 **/etc/kubernetes/kubelet-ca.crt** 证书颁发机构（CA）不再需要 Machine Config Operator（MCO）来排空节点或重启集群。

作为这一更改的一部分，以下修改不需要 MCO 排空节点：

- 在机器配置的 **spec.config.ignition.passwd.users.sshAuthorizedKeys** 参数中更改 SSH 密钥
- 在 **openshift-config** 命名空间中更改全局 pull secret 或 pull secret

当 MCO 检测到任何这些更改时，它会应用更改并取消记录节点。

如需更多信息，请参阅了解 Machine Config Operator。

1.4.13.3. 机器集策略增强

在以前的版本中，创建机器集需要用户手动配置 CPU 固定设置、NUMA 固定设置和 CPU 拓扑更改，以便从主机获得更好的性能。在这个版本中，用户可以在 **MachineSet** 资源中选择一个策略来自动填充设置。如需更多信息，请参阅**BZ#1941334**。

1.4.13.4. 机器集巨页增强

现在，可以在 **MachineSet** 资源中提供 **hugepages** 属性。此增强使用 oVirt 中的自定义属性创建 **MachineSet** 资源的节点，并指示这些节点使用虚拟机监控程序的巨页（**hugepage**）。如需更多信息，请参阅 BZ#1948963。

1.4.13.5. Machine Config Operator ImageContentSourcePolicy 对象增强

OpenShift Container Platform 4.8 避免了所选 **ImageContentSourcePolicy** 对象更改的工作负载中断。此功能帮助用户和团队在不中断工作负载的情况下添加额外的镜像和 registry。因此，**/etc/containers/registries.conf** 文件中的以下更改将不再发生工作负载分离：

- 添加一个带有 **mirror-by-digest-only=true** 的 registry
- 在带有 **mirror-by-digest-only=true** 的 registry 中添加镜像
- 在 **unqualified-search-registries** 列表中附加项目

对于 **/etc/containers/registries.conf** 文件中的任何其他更改，Machine Config Operator 默认排空节点以应用更改。如需更多信息，请参阅BZ#1943315。

1.4.14. 节点

1.4.14.1. Descheduler operator.openshift.io/v1 API 组现在可用

现在，descheduler 可以使用 **operator.openshift.io/v1** API 组。在以后的发行版本，可能会删除对 descheduler 使用 **operator.openshift.io/v1beta1** API 组的支持。

1.4.14.2. descheduler 的 Prometheus 指标

现在，您可以把 **openshift.io/cluster-monitoring=true** 标识添加到您安装 descheduler 的 **openshift-kube-descheduler-operator** 命令空间中来启用 descheduler 的 Prometheus 指标功能。

可用的 descheduler 指标如下：

- **descheduler_build_info** - 提供 descheduler 的构建信息。
- **descheduler_pods_evicted** - 提供为每个策略、命名空间和结果组合被驱除的 pod 数量。必须至少有一个被驱除的 pod 才能显示此指标。

1.4.14.3. 支持使用 Downward API 的巨页

在这个版本中，当您为 pod 规格中的巨页设置请求和限值时，您可以使用 Downward API 从容器中查看 pod 的分配。这个改进依赖于 **DownwardAPIHugePages** 功能门。OpenShift Container Platform 4.8 启用功能门。

如需更多信息，请参阅使用 Downward API 消耗巨页资源。

1.4.14.4. Node Feature Discovery Operator 的新标签

Node Feature Discovery（NFD）Operator 会检测 OpenShift Container Platform 集群中每个节点上可用的硬件功能。然后，它会使用节点标签修改节点对象。这可让 NFD Operator 公告特定节点的功能。OpenShift Container Platform 4.8 支持 NFD Operator 的三个额外标签。

- **pstate intel-pstate**：当 Intel **pstate** 驱动程序被启用和使用时，**pstate intel-pstate** 标签反映了 Intel **pstate** 驱动程序的状态。它的状态可以是 **active** 或 **passive**。

- **pstate scaling_governor**：当 Intel **pstate** 驱动程序状态为 **active** 时，**pstate scaling_governor** 标签反映扩展监管器算法。该算法可以是 **powerave** 或 **performance**。
- **cstate status**：如果 **intel_idle** 驱动程序具有 C-states 或 idle 状态，则 **cstate status** 标签为 **true**。否则，为 **false**。

1.4.14.5. 使用 Poison Pill Operator 修复不健康节点

您可以使用 Poison Pill Operator 来允许不健康的节点自动重新引导。这可最小化有状态应用程序和 ReadWriteOnce (RWO) 卷的停机时间，并在发生临时故障时恢复计算容量。

Poison Pill Operator 适用于所有集群和硬件类型。

如需更多信息，请参阅使用 Poison Pill Operator 修复节点。

1.4.14.6. 自动轮转 kubelet-ca.crt 不需要重启

自动轮转 **/etc/kubernetes/kubelet-ca.crt** 证书颁发机构（CA）不再需要 Machine Config Operator（MCO）来排空节点或重启集群。

作为这一更改的一部分，以下修改不需要 MCO 排空节点：

- 在机器配置的 **spec.config.ignition.passwd.users.sshAuthorizedKeys** 参数中更改 SSH 密钥
- 在 **openshift-config** 命名空间中更改全局 pull secret 或 pull secret

当 MCO 检测到任何这些更改时，它会应用更改并取消记录节点。

如需更多信息，请参阅了解 Machine Config Operator。

1.4.14.7. 垂直 pod 自动扩展通常可用

OpenShift Container Platform 垂直 pod 自动扩展（VPA）现已正式发布。VPA 会自动检查 pod 中容器的运行状况和当前的 CPU 和内存资源，并根据它所了解的用量值更新资源限值和请求。

您还可以通过修改 **VerticalPodAutoscalerController** 对象，将 VPA 与只需要一个副本的 pod 搭配使用，如下所述。在以前的版本中，VPA 只适用于需要两个或多个副本的 pod。

如需更多信息，请参阅使用垂直 pod 自动扩展自动调整 pod 资源级别。

1.4.14.8. 可以配置垂直 pod 自动扩展最小

默认情况下，工作负载对象必须至少指定两个副本，以便 VPA 自动更新 pod。因此，VPA 不会对指定少于两个副本的工作负载对象执行操作。您可以通过修改 **VerticalPodAutoscalerController** 对象来添加 **minReplicas** 参数，用来更改这个集群范围的最小值。

如需更多信息，请参阅使用垂直 pod 自动扩展自动调整 pod 资源级别。

1.4.14.9. 为节点自动分配 CPU 和内存资源

当节点启动时，OpenShift Container Platform 可以自动决定 **system-reserved** 设置的最佳大小调整值。在以前的版本中，**system-reserved** 设置中的 CPU 和内存分配是手动决定和设置所需的固定限制。

启用自动资源分配后，每个节点上的脚本会根据节点上安装的 CPU 和内存容量来计算相应保留资源的优化值。

如需更多信息，请参阅自动为节点分配资源。

1.4.14.10. 添加特定的软件仓库来拉取镜像

现在，您可以在创建允许和阻止的 registry 列表来拉取和推送镜像时，在 registry 中指定单独的存储库。在以前的版本中，您只能指定 registry。

如需更多信息，请参阅添加特定 registry 和阻塞特定的 registry。

1.4.14.11. Cron Job 正式发布

Cron Job 自定义资源现已正式发布。作为这一变化的一部分，新的控制器已实施以显著提高 cron 作业的性能。如需有关 cron 作业的更多信息，请参阅了解作业和 cron 作业。

1.4.15. Red Hat OpenShift Logging

在 OpenShift Container Platform 4.7 中，*Cluster Logging* 变为了 *Red Hat OpenShift Logging*。如需更多信息，请参阅 Red Hat OpenShift Logging 的发行注记。

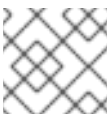
1.4.16. 监控

1.4.16.1. 对规则更改的警报

OpenShift Container Platform 4.8 包括以下警报规则更改：

例 1.1. 对规则更改的警报

- **ThanosSidecarPrometheusDown** 警报的严重性从 *critical* 更新为 *warning*。
- **ThanosSidecarUnhealthy** 警报的严重性从 *critical* 更新为 *warning*。
- **ThanosQueryHttpRequestQueryErrorRateHigh** 警报的严重性从 *critical* 更新为 *warning*。
- **ThanosQueryHttpRequestQueryRangeErrorRateHigh** 警报的严重性从 *critical* 更新为 *warning*。
- **ThanosQueryInstantLatencyHigh** 严重警报已被删除。如果 Thanos Querier 有一个高延迟进行即时查询，则会触发此警报。
- **ThanosQueryRangeLatencyHigh** 严重警报被删除。如果 Thanos Querier 存在较高的范围查询延迟，则会触发此警报。
- 对于所有 Thanos Querier 警报，**for** 持续时间增加到 1 小时。
- 对于所有 Thanos sidecar 警报，**for** 持续时间增加到 1 小时。



注意

红帽不保证指标、记录规则或警报规则的向后兼容。

1.4.16.2. 在下一个发行版本中，将删除使用的 API 的警报和信息

OpenShift Container Platform 4.8 引入了两个新警报，它们会在使用了下一发行版本中将被删除的 API 时触发：

- **APIRemovedInNextReleaseInUse** - 针对将在下一个 OpenShift Container Platform 发行版本中删除的 API。
- **APIRemovedInNextEUSReleaseInUse** - 针对将在下一个 OpenShift Container Platform 扩展更新支持（EUS）版本中删除的 API。

您可以使用新的 **APIRequestCount** API 来跟踪使用已弃用 API 的内容。这可让您规划在升级到下一版本时是否需要进行一些相关的操作。

1.4.16.3. 监控堆栈组件和依赖项的版本更新

OpenShift Container Platform 4.8 包括对以下监控堆栈组件和依赖项的版本更新：

- Prometheus Operator 现在为 0.48.1 版本。
- Prometheus 现在是 2.26.1 版本。
- **node-exporter** 代理现在基于 1.1.2 版本。
- Thanos 现在为 0.20.2 版本。
- Grafana 现在是版本 7.5.5。

1.4.16.4. kube-state-metrics 升级到版本 2.0.0

kube-state-metrics 升级到 2.0.0 版本。**kube-state-metrics** 版本 1.9 中弃用了以下指标，并在 2.0.0 版本中实际删除：

- pod 的非通用资源指标：
  - kube_pod_container_resource_requests_cpu_cores
  - kube_pod_container_resource_limits_cpu_cores
  - kube_pod_container_resource_requests_memory_bytes
  - kube_pod_container_resource_limits_memory_bytes
- 节点的非通用资源指标：
  - kube_node_status_capacity_pods
  - kube_node_status_capacity_cpu_cores
  - kube_node_status_capacity_memory_bytes
  - kube_node_status_allocatable_pods
  - kube_node_status_allocatable_cpu_cores
  - kube_node_status_allocatable_memory_bytes

1.4.16.5. 删除了 Grafana 和 Alertmanager UI 链接

第三方 Alertmanager UI 的链接已从 OpenShift Container Platform Web 控制台的 **Monitoring → Alerting** 页面中删除。另外，第三方 Grafana UI 的链接也会从 **Monitoring → Dashboards** 页面中删除。您仍然可以通过导航到 **openshift-monitoring** 项目中的 **Networking → Routes** 页面，在 **Administrator** 视角中的 Web 控制台中访问到 Grafana 和 Alertmanager UI 的路由。

1.4.16.6. Web 控制台中的监控仪表板增强

OpenShift Container Platform Web 控制台的 **Monitoring → Dashboards** 页面中提供了新的增强功能：

- 当您通过用鼠标选择一个区域来缩放单个图形时，所有其他图形现在都会更新，以反映相同的时间范围。
- 现在，仪表板面板被组织成组，您可以展开和折叠这些组。
- 单值面板现在支持根据颜色的值更改颜色。
- 现在，仪表板标签会显示在 **Dashboard** 下拉列表中。
- 现在，您可以通过在 **Time Range** 下拉列表中选择 **Custom time rang**来为仪表板指定自定义时间范围。
- 现在，您可以在仪表板过滤器下拉菜单中选择 **All** 选项，以显示该过滤器中所有选项的数据。

1.4.17. Metering

Metering Operator 在 OpenShift Container Platform 4.6 中弃用，并计划在下一个 OpenShift Container Platform 发行版本中删除。

1.4.18. 扩展

1.4.18.1. 在单一节点集群中运行

在单一节点集群中运行测试会导致特定测试的超时时间较长，包括 SR-IOV 和 SCTP 测试，并跳过需要 control plane 和 worker 节点的测试。需要节点重启的重新配置会导致重启整个环境，包括 OpenShift control plane，因此完成时间较长。所有需要 control plane 节点和 worker 节点的 PTP 测试都会跳过。不需要额外的配置，因为测试会在启动时检查节点数量并相应地调整测试行为。

PTP 测试可在发现模式下运行。测试会查找在集群外配置的 PTP control plane。需要以下参数：

- **ROLE_WORKER_CNF=master** - 必需，因为 control plane（**master**）是唯一的、节点将属于的机器池。
- **XT_U32TEST_HAS_NON_CNF_WORKERS=false** - 需要指示 **xt_u32** 负测试跳过，因为只有加载模块的节点。
- **SCTPTEST_HAS_NON_CNF_WORKERS=false** - 需要指示 SCTP 负测试跳过，因为只有加载模块的节点。

1.4.18.2. 使用 Performance Addon Operator 减少 NIC

Performance Addon Operator 允许您配置性能配置集来调整每个网络设备的网络接口卡（NIC）队列数量。设备网络队列允许数据包分布到不同的物理队列中，每个队列获得用于数据包处理的独立线程。

对于基于 Data Plane Development Kit（DPDK）的工作负载，务必要将 NIC 队列减少到仅保留或托管 CPU 的数量，以确保实现所需的低延迟。

如需更多信息，请参阅使用 Performance Addon Operator 缩减 NIC 队列。

1.4.18.3. 集群最大限制

针对 OpenShift Container Platform 4.8 的集群最大限制指导信息已更新。

重要

此发行版本没有针对 OVN-Kubernetes 测试执行大规模测试。

使用 OpenShift Container Platform Limit Calculator 可以估算出您的环境的集群限制。

1.4.18.4. 创建性能配置集

现在，您可以使用 Performance Profile Creator（PPC）工具创建性能配置集。该工具会消耗来自集群和几个用户提供的配置集参数的 **must-gather** 数据，并使用这些信息生成适合您的硬件和拓扑的性能配置集。

如需更多信息，请参阅创建性能配置集。

1.4.18.5. Node Feature Discovery Operator

Node Feature Discovery（NFD）Operator 现已可用。使用它来通过编排节点功能发现（用于检测硬件功能和系统配置的 Kubernetes 附加组件）来公开节点级信息。

1.4.18.6. Driver Toolkit（技术预览）

现在，您可以使用 Driver Toolkit 作为驱动程序容器的基础镜像，以便您可以在 Kubernetes 上启用特殊软件和硬件设备。目前，这是一个技术预览功能。

1.4.19. 备份和恢复

1.4.19.1. etcd 快照增强

一个新的改进会在备份后并在恢复前验证 etcd 快照的状态。在以前的版本中，备份过程无法验证所执行的快照是否已完成，恢复过程也不会验证正在恢复的快照是否有效，没有损坏。现在，如果磁盘在备份或恢复过程中被破坏，则错误会明确报告给管理员。如需更多信息，请参阅 BZ#1965024。

1.4.20. Insights Operator

1.4.20.1. 有关受限网络的见解顾问建议

在 OpenShift Container Platform 4.8 中，在受限网络中运行的用户可以收集 Insights Operator 存档并上传到 Insights 顾问，以诊断潜在的问题。另外，用户也可以在上传前模糊处理 Insights Operator 归档中包含的敏感数据。

如需更多信息，请参阅在受限网络中使用远程健康报告。

1.4.20.2. Insights Advisor 的改进

OpenShift Container Platform Web 控制台中的 insights Advisor 现在可以正确地报告有 0 个问题。在以前的版本中，在这种情况下，Insights Advisor 没有提供任何信息。

1.4.20.3. 深入了解 Operator 数据收集功能的增强

在 OpenShift Container Platform 4.8 中，Insights Operator 会收集以下附加信息：

- 无法识别的集群工作负载信息来查找已知的安全性和版本问题。
- **MachineHealthCheck** 和 **MachineAutoscaler** 定义。
- **virt_platform** 和 **vsphere_node_hw_version_total** 指标。
- 有关不健康 SAP pod 的信息，以帮助安装 SAP 智能数据集成。
- **datahubs.installers.datahub.sap.com** 资源用于识别 SAP 集群。
- 一个失败的 **PodNetworkConnectivityCheck** 的摘要，用于增强网络。
- 有关 **openshift-cluster-operator** 命名空间中的 **cluster-version** pod 和事件的信息，以调试 **cluster-version** Operator 的问题。

通过这些附加信息，红帽可在 Insights Advisor 中提供改进的补救步骤。

1.4.20.4. 对不健康的 SAP pod 的深入了解 Operator 的增强

Insights Operator 现在可以为不健康的 SAP pod 收集数据。当 SDI 安装失败时，可以通过查看哪个初始化 pod 失败来检测到问题。Insights Operator 现在会在 SAP/SDI 命名空间中收集有关失败 pod 的信息。如需更多信息，请参阅 BZ#1930393。

1.4.20.5. 了解 Operator 的增强以收集 SAP pod 数据

Insights Operator 现在可以从 SAP 集群收集 **Datahubs** 资源。通过这些数据，SAP 集群可以被与 Insights Operator 归档中的非 SAP 集群区分开，即使缺少所有从 SAP 集群收集的数据，否则就无法确定集群是否有 SDI 安装。如需更多信息，请参阅 BZ#1940432。

1.4.21. 认证和授权

1.4.21.1. 使用 AWS Security Token Service（STS）用于凭证来运行 OpenShift Container Platform 已正式可用。

现在，您可以使用 Cloud Credential Operator（CCO）实用程序（**ccoctl**）将 CCO 配置为使用 Amazon Web Services Security Token Service（AWS STS）。当 CCO 配置为使用 STS 时，它会分配 IAM 角色，它提供短暂的、有限制权限的安全凭证。

此功能以前作为技术预览功能在 OpenShift Container Platform 4.7 中引入，现在正式包括在 OpenShift Container Platform 4.8 中。

如需更多信息，请参阅在 STS 中使用手动模式。

1.4.22. OpenShift 沙盒容器

1.4.22.1. OpenShift 沙盒容器（sandboxed containers）支持 OpenShift Container Platform（技术预览）

要查看 OpenShift 沙盒容器新功能、程序错误修复、已知问题和异步勘误更新，请参阅 OpenShift 沙盒容器 1.0 发行注记。

1.5. 主要的技术变化

OpenShift Container Platform 4.8 包括以下显著的技术更改。

Kuryr 服务子网创建更改
在配置为使用 Kuryr 的 Open Virtual Network 的 Red Hat OpenStack Platform（RHOSP）上新安装 OpenShift Container Platform 不再创建一个 **services** 子网，它的大小是 **networking.serviceCIDR** 中请求的大小的两倍。创建的子网现在与请求的大小相同。如需更多信息，请参阅 BZ#1955548。

不再使用没有 SHA-256 前缀的 OAuth 令牌
在 OpenShift Container Platform 4.6 之前，OAuth 访问和授权令牌将 secret 信息用于对象名称。

从 OpenShift Container Platform 4.6 开始，OAuth 访问令牌和授权令牌对象名称存储为非敏感对象名称，且具有 SHA-256 前缀。OpenShift Container Platform 4.8 中无法再使用或创建不包含 SHA-256 前缀的 OAuth 令牌。

Federal Risk and Authorization Management Program（FedRAMP）控制
在 OpenShift Container Platform 4.8 中，**rhcos4-moderate** 配置集现已完整。**ocp4-moderate** 配置集将在以后的发行版本中变为完整。

Ingress Controller 升级至 HAProxy 2.2.13
OpenShift Container Platform Ingress Controller 升级到 HAProxy 版本 2.2.13。

CoreDNS 更新至 1.8.1
在 OpenShift Container Platform 4.8 中，CoreDNS 使用 1.8.1 版本，它有几个程序错误修复、重命名的指标和双栈 IPv6 启用。

etcd 现在使用 zap 日志记录器
在 OpenShift Container Platform 4.8 中，etcd 现在使用 zap 作为默认日志记录器，而不是 capnslog。zap 是结构化的日志记录器，提供机器可使用的 JSON 日志消息。您可以使用 **jq** 轻松解析这些日志消息。

如果您有希望 capnslog 格式的日志使用者，您可能需要针对 zap 日志记录器格式进行调整。

capnslog 格式示例（OpenShift Container Platform 4.7）

```
2021-06-03 22:40:16.984470 W | etcdserver: read-only range request
"key:\"/kubernetes.io/operator.openshift.io/clustercsidrivers/\"
range_end:\"/kubernetes.io/operator.openshift.io/clustercsidrivers0\" count_only:true " with result
"range_response_count:0 size:8" took too long (100.498102ms) to execute
```

zap 格式示例（OpenShift Container Platform 4.8）

```
{"level":"warn","ts":"2021-06-14T13:13:23.243Z","caller":"etcdserver/util.go:163","msg":"apply request
took too long","took":"163.262994ms","expected-duration":"100ms","prefix":"read-only range
","request":"key:\"/kubernetes.io/namespaces/default\" serializable:true keys_only:true
","response":"range_response_count:1 size:53"}
```

为 LSO 合并的多个守护进程集
在 OpenShift Container Platform 4.8 中，为 Local Storage Object（LSO）合并了多个守护进程集。当您创建本地卷自定义资源时，只创建 **daemonset.apps/diskmaker-manager**。

绑定服务帐户令牌卷已启用
在以前的版本中，服务帐户令牌是挂载到 pod 中的 secret。从 OpenShift Container Platform 4.8 开始，将使用项目的卷。因此，服务帐户令牌不再有底层对应的 secret。

绑定服务帐户令牌对使用者具有限制且有时间限制。如需更多信息，请参阅使用绑定服务帐户令牌。

另外，kubelet 在令牌达到 80% 持续时间后自动刷新令牌，**client-go** 会一直监视令牌的更改并在需要时会自动重新载入。这两个行为的组合意味着，绑定令牌的大部分使用与使用永不过期的传统令牌不同。**client-go** 以外的非标准使用可能会导致问题。

Operator SDK v1.8.0
OpenShift Container Platform 4.8 支持 Operator SDK v1.8.0。请参阅安装 Operator SDK CLI 以安装或更新到这个最新版本。

注意

Operator SDK v1.8.0 支持 Kubernetes 1.20。

如果您之前使用 Operator SDK v1.3.0 创建或维护了任何 Operator 项目，请参阅升级较新版本的 Operator SDK 版本的项目，以确保您的项目已升级以保持与 Operator SDK v1.8.0 的兼容性。

1.6. 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 4.8 中已弃用并删除的主要功能的最新列表，请参考下表。表后列出了更详细的、已弃用和删除的功能信息。

在下表中，被标记为以下状态的功能：

- **GA**: *正式发行*
- **TP**: *技术预览*
- **DEP**: *已弃用*
- **REM**: *删除*

表 1.1. 过时和删除的功能

功能	OCP 4.6	OCP 4.7	OCP 4.8
OperatorSource 对象	REM	REM	REM
软件包清单格式（Operator 框架）	DEP	DEP	REM
oc adm catalog build	DEP	DEP	REM
oc adm catalog mirror 的 **--filter-by-os** 标记	GA	DEP	REM
v1beta1 CRD	DEP	DEP	DEP
Docker Registry v1 API	DEP	DEP	DEP
Metering Operator	DEP	DEP	DEP

功能	OCP 4.6	OCP 4.7	OCP 4.8
调度程序策略	GA	DEP	DEP
Cluster Samples Operator 的 **ImageChangesInProgress** 条件	GA	DEP	DEP
Cluster Samples Operator 的 **MigrationInProgress** 条件	GA	DEP	DEP
在 **apiVersion** 中将 **v1** 用于 OpenShift Container Platform 资源	GA	DEP	DEP
在 Red Hat Enterprise Linux CoreOS（RHCOS）中使用 **dhclient**	DEP	DEP	DEP
Cluster Loader	GA	GA	DEP
使用自己的 RHEL 7 计算机器	DEP	DEP	DEP
AWS EFS 的外部置备程序	REM	REM	REM
Builds 的 **BuildConfig** spec 中的 **lastTriggeredImageID** 字段	GA	GA	DEP
Jenkins Operator	TP	TP	DEP
基于 Prometheus 的 HPA 定制 metrics adapter	TP	TP	REM
Red Hat Virtualization(RHV)的 **instance_type_id** 安装配置参数	GA	DEP	DEP
Microsoft Azure 集群的 Mint 凭证	GA	GA	REM

1.6.1. 已弃用的功能

1.6.1.1. descheduler operator.openshift.io/v1beta1 API 组已弃用

descheduler 的 **operator.openshift.io/v1beta1** API 组已弃用，并可能在以后的发行版本中删除。改用 **operator.openshift.io/v1** API 组。

1.6.1.2. 在 Red Hat Enterprise Linux CoreOS（RHCOS）中使用 dhclient 已被弃用

从 OpenShift Container Platform 4.6 开始，Red Hat Enterprise Linux CoreOS（RHCOS）切换到使用 **initramfs** 中的 **NetworkManager** 在早期引导过程中配置网络。作为这一更改的一部分，对于 DHCP 使用 **dhclient** 二进制文件已被弃用。改为使用 **NetworkManager** 内部 DHCP 客户端进行网络配置。**dhclient** 二进制文件将在以后的版本中从 Red Hat Enterprise Linux CoreOS（RHCOS）中删除。如需更多信息，请参阅 BZ#1908462。

1.6.1.3. Cluster Loader 已被弃用

Cluster Loader 现已弃用，并将在以后的发行版本中删除。

1.6.1.4. 构建中的 lastTriggeredImageID 参数已弃用

此发行版本弃用 **ImageChangeTrigger** 对象中的 **lastTriggeredImageID**，这是可在 **BuildConfig** 规格中设置的 **BuildTriggerPolicy** 类型之一。

OpenShift Container Platform 下一个发行版本将删除对 **lastTriggeredImageID** 的支持并忽略它。然后，镜像更改触发器不会根据 **BuildConfig** spec 中 **lastTriggeredImageID** 字段的更改启动构建。相反，触发构建的镜像 ID 将记录在 **BuildConfig** 对象的状态中，大多数用户都无法更改。

因此，更新需要检查 **buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID** 的脚本和作业。（BUILD-213）

1.6.1.5. Jenkins Operator（技术预览）已弃用

此发行版本弃用了 Jenkins Operator，它是一个技术预览功能。未来的 OpenShift Container Platform 版本将在 OpenShift Container Platform Web 控制台界面的 OperatorHub 中删除 Jenkins Operator。然后，不再提供 Jenkins Operator 的升级，Operator 不受支持。

客户可以使用 Samples Operator 提供的模板在 OpenShift Container Platform 上继续部署 Jenkins。

1.6.1.6. Red Hat Virtualization(RHV)的 instance_type_id 安装配置参数

instance_type_id 安装配置参数已弃用，并将在以后的发行版本中删除。

1.6.2. 删除的功能

1.6.2.1. 删除了对 Microsoft Azure 的 mint 凭证的支持

从 OpenShift Container Platform 4.8.34 开始，在 Microsoft Azure 集群上以 mint 模式使用 Cloud Credential Operator(CCO)的支持已从 OpenShift Container Platform 4.8 中删除。此更改的原因是 Microsoft 的 Azure AD Graph API 将于 2022 年 6 月 30 日停用 ，并被向后移植到 z-stream 更新中所有支持的 OpenShift Container Platform 版本。

对于在以前安装的使用 mint 模式的 Azure 集群，CCO 会尝试更新现有的 secret。如果 secret 包含之前 minted 应用程序注册服务主体的凭证，则会使用 **kube-system/azure-credentials** 中的 secret 的内容更新。这个行为和 passthrough 模式类似。

对于将凭证模式设置为默认值 **""** 的集群，更新的 CCO 会自动从 mint 模式运行，以 passthrough 模式运行。如果您的集群将凭证模式明确设置为 mint 模式(**"Mint"**)，则必须将值改为 **""** 或 **"Passthrough"**。

注意

除了 mint 模式所需的 **Contributor** 角色外，修改后的应用程序注册服务主体现在还需要用于 passthrough 模式的 **User Access Administrator** 角色。

虽然 Azure AD Graph API 仍然可用，但升级版 OpenShift Container Platform 的 CCO 会尝试清理之前 mint 的应用注册服务主体。在 Azure AD Graph API 之前升级集群可能会避免需要手动清理资源。

如果在 Azure AD Graph API 停用后，集群被升级到一个不再支持 mint 模式的 OpenShift Container Platform 版本，CCO 会在关联的 **CredentialsRequest** 上设置 **OrphanedCloudResource** 条件，但不会

将相关错误视为是致命（fatal）错误。该条件包括与 **unable to clean up App Registration / Service Principal: <app_registration_name>** 类似的消息。在 Azure AD Graph API 停用后，清理需要使用 Azure CLI 工具或 Azure Web 控制台手动删除剩余的应用程序注册服务主体。

要手动清理资源，您必须找到并删除受影响的资源。

1. 使用 Azure CLI 工具，通过运行以下命令从 **OrphanedCloudResource** 条件消息过滤使用 **<app_registration_name>** 的应用程序注册服务主体：

```
$ az ad app list --filter "displayname eq '<app_registration_name>'" --query '[].objectId'
```

输出示例

```
[
  "038c2538-7c40-49f5-abe5-f59c59c29244"
]
```

2. 运行以下命令来删除应用程序注册服务主体：

```
$ az ad app delete --id 038c2538-7c40-49f5-abe5-f59c59c29244
```

注意

在手动清理资源后，**OrphanedCloudResource** 条件会保留，因为 CCO 无法验证资源是否已清理。

已删除 AWS EFS（技术预览）功能的外部置备程序

Amazon Web Services（AWS）Elastic File System（EFS）技术预览功能已被删除，且不再被支持。

1.6.2.2. 从示例镜像流中删除的镜像

以下镜像不再包含在 OpenShift Container Platform 提供的样本镜像流中：

```
registry.redhat.io/rhscl/nodejs-10-rhel7
registry.redhat.io/ubi7/nodejs-10
registry.redhat.io/rhscl/perl-526-rhel7
registry.redhat.io/rhscl/postgresql-10-rhel7
registry.redhat.io/rhscl/ruby-25-rhel7
registry.redhat.io/ubi7/ruby-25
registry.redhat.io/rhdm-7/rhdm-decisioncentral-rhel8:7.9.0
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.9.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.9.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-rhel8:7.9.0
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.9.0
```

1.6.2.3. Operator 不再支持软件包清单格式

OpenShift Container Platform 4.8 及更高版本中删除了对 Operator 的传统软件包清单格式的支持。此删除支持包括使用旧格式构建的自定义目录，以及最初使用 Operator SDK 以传统格式创建的 Operator 项目。从 OpenShift Container Platform 4.6 开始，捆绑包格式是 Operator Lifecycle Manager（OLM）的首选 Operator 打包格式。

有关使用捆绑包格式的更多信息，请参阅管理自定义目录和迁移软件包清单项目以捆绑格式。

另外，以下与格式相关的命令已从 OpenShift CLI（**oc**）和 Operator SDK CLI 中删除：

- **oc adm catalog build**
- **operator-sdk generate packagemanifest**
- **operator-sdk run packagemanifest**

1.6.2.4. 删除了对基于 Prometheus 的 HPA 自定义 metrics adapter 的支持

此发行版本删除了 Prometheus Adapter，它是一个技术预览功能。

1.6.2.5. 删除了安全令牌存储注解的识别

现在，在选择集群的审计策略时，**authentication** 和 **openshift-apiserver** Operator 会忽略 **oauth-apiserver.openshift.io/secure-token-storage** 注解。审计策略现在默认使用 **secure-**。如需更多信息，请参阅 BZ#1879182。

1.7. 程序错误修复

assisted-installer

- 在以前的版本中，**assisted-service** 容器不会等待 **postgres** 启动并准备好来接受连接。**assisted-service** 容器试图建立数据库连接并失败，**assisted-service** 容器失败并重启。这个问题已被解决，**assisted-service** 容器会尝试连接到数据库最多 10 秒。如果 **postgres** 启动并在 10 秒内准备好接受连接，则 **assisted-service** 容器将会进行连接，而不会进入错误状态。如果 **assisted-service** 容器无法在 10 秒内连接到 **postgres**，它会进入错误状态、重启并重试。（BZ#1941859）

裸机硬件置备

- 在以前的版本中,Ironic 无法下载安装的镜像，因为 Ironic 默认使用 HTTPS，且没有可用的证书捆绑包。这个问题已通过将镜像下载设置为 **Insecure** 以解决，从而在没有证书的情况下请求传输。（BZ#1953795）
- 在以前的版本中，当使用双栈网络时，worker 节点主机名有时与 Ironic 在部署前检查的主机名不匹配。这会导致节点需要手动批准。该问题已解决。（BZ#1955114）
- 在以前的版本中，在 UEFI 模式中，**ironic-python-agent** 在下载 RHCOS 镜像后会创建一个 UEFI 引导装载程序条目。当使用基于 RHEL 8.4 的 RHCOS 镜像时，镜像可能无法使用此条目引导。如果在引导镜像时使用 Ironic 安装的条目，引导可能会失败，并输出一个 BIOS 错误界面。这个问题由 **ironic-python-agent** 根据镜像中的 CSV 文件配置引导条目来解决，而不使用固定的引导条目。镜像可以正常引导，且无错误。(BZ#1972213)
- 在以前的版本中，节点有时会在启动时选择不正确的 IP 版本（IPv6 而不是 IPv4，反之亦然）。该节点无法启动，因为它没有收到 IP 地址。这个问题已解决，Cluster Bare Metal Operator 将 IP 选项传递给下载器（**ip=dhcp** 或 **ip=dhcp6**），它在启动时可以正确设置，节点会如预期启动。（BZ#1946079）
- 在以前的版本中，Ironic 中的镜像缓存机制被禁用，以启用与托管 virtualmedial iso 的 HTTP 服务器的直接连接，以防止本地存储问题。非标准兼容 HTTP 客户端和 redfish 实现会导致 BMC 连接失败。这个问题已通过恢复到缓存 virtualmedia iso 并从 Ironic 编排器节点提供的默认 Ironic 行为来解决。由非标准兼容 HTTP 客户端和 redfish 的实现造成的问题已被解决。(BZ#1962905)

- 在以前的版本中，机器实例的 **state** 注解没有被设置。因此，**STATE** 列为空。在这个版本中，机器实例的 **state** 注解被设置，**STATE** 列中的信息会自动填充。(BZ#1857008)

- 因为较新的 ipmitool 软件包默认使用加密套件 17，所以不支持密码套件 17 的旧硬件在部署过程中会失败。当硬件不支持密码套件 17 时，Ironic 现在使用密码套件 3，以便使用 ipmitool 的旧硬件上部署可以成功。(BZ#1897415)

- 在以前的版本中，在某些情况下，在填充镜像缓存前发生采用，这会导致永久采用失败，且不会尝试重试。这会导致 control plane 裸机主机报告采用失败。在这个版本中，外部置备的主机会在采用失败后自动重试，直到正确采用 control plane 主机为止。(BZ#1905577)

- 在以前的版本中，自定义资源（CR）需要 Baseboard Management Controller（BMC）详情。但是，在协助的安装程序中不会提供此信息。此更新允许 CR 在 Operator 没有创建节点时绕过 BMC 详情。（BZ#1913112）

- 在将一个镜像置备到节点时，qemu-image 被限制为 1G RAM，这可能会导致 qemu-img 崩溃。在这个版本中，限制被增加到 2G，以便 qemu-img 现在能够可靠完成置备。（BZ#1917482）

- 由于 redfish/v1/SessionService URL 需要身份验证，因此 Ironic 会在访问站点时生成身份验证错误。因为 Ironic 报告此错误消息时没有功能问题，因此已被删除。（BZ#1924816）

- 对于某些驱动器，分区（如 **/dev/sda1** ）没有只读文件。然而，基本设备（例如 **/dev/sda** ）有此文件。因此，Ironic 无法确定分区是只读的，这会导致元数据清理在该驱动器上失败。在这个版本中，确保了分区被检测到为只读分区，并包含对基本设备的额外检查。因此，不会对只读分区执行元数据清理，元数据清理不再失败。（BZ#1935419）

- 当使用代理配置代理部署 Baremetal IPI 时，内部 machine-os 镜像下载会通过代理进行。这会破坏镜像并阻止下载。在这个版本中，内部镜像流量被修复为 **no_proxy**，因此镜像下载不再使用代理。(BZ#1962592)

- 在以前的版本中，如果 Ironic 和 RAM 磁盘之间的大型数据包传输导致连接失败，裸机部署会失败。在这个版本中，Ironic 会查询 RAM 磁盘以获取解决连接错误的信息，从而使部署可以成功。（BZ#1957976）

Builds

- 在以前的版本中，在修复 CVE-2021-3344 后，构建不会在 OpenShift Container Platform 节点上自动挂载授权密钥。因此，当授权证书存储在主机或节点上时，这个修复会阻止授权构建无缝运行。导致主机或节点上保存的权利证书失败的问题已在 BZ#1945692（4.7.z）和 BZ#1946363（4.6.z）中修复。但是，这些修复为在 Red Hat Enterprise Linux CoreOS（RHCOS）worker 节点上运行的构建引入了一个 benign 警告信息。当前发行版本解决了这个问题，它允许构建只在 RHEL worker 节点上自动挂载权利，并避免在 RHCOS worker 节点上尝试挂载。现在，在 RHCOS 节点上运行构建时，不会出现有关授权挂载的任何 benign 警告。（BZ#1951084）

- 有些用户从 Docker Hub 拉取镜像可能会遇到以下错误：

  > container image registry lookup failed...toomanyrequests: You have reached your pull rate limit

  发生此错误的原因是，它们用来调用 **oc new-app** 的 **docker.io** 登录没有足够的 **docker.io** 支持。生成的应用可能会受到镜像节流的影响，这可能会导致失败。当前发行版本更新了 **oc new-app**，提醒用户镜像 registry 和存储库规格的默认工作原理，因此用户可以尽可能使用非默认镜像引用以避免类似的错误。（BZ#1928850）

- 在以前的版本中，构建不会执行错误检查来查看镜像推送是否失败。因此，构建总是记录 **Successfully pushed** 信息。现在，构建会检查是否有错误，只有在镜像推送成功后才会记录 **Successfully pushed** 信息。（BZ#1947164）

- 在以前的版本中，文档和 **oc explain** 的帮助文本不会提示 **BuildConfig** 对象中的 **buildArgs** 字段不支持其底层 Kubernetes **EnvVar** 类型的 **valueFrom** 字段。因此，用户会相信它已被支持并尝试使用它。当前发行版本更新了文档和帮助文本，更明显地说明 **BuildConfig** 对象的 **buildArgs** 字段不支持 **valueFrom** 字段。（BZ#1956826）

- 当构建与镜像 registry 交互（如拉取基础镜像）时，间歇性通信问题可能会导致构建失败。当前发行版本会增加对这些交互的重试次数。现在，当 OpenShift Container Platform 构建遇到与镜像 registry 间通信时，它们可以更加灵活。(BZ#1937535)

Cloud Compute

- 在以前的版本中，**Cluster Image Registry Operator** 将 **user_domain_name** 视为不可变字段，且不会在安装后修改。这会导致一个接受对 **user_domain_name** 并生成的凭证的更改。在这个版本中，**user_domain_name** 标记为可变，且不会将其存储在镜像 registry 配置中。这允许在安装后修改 **user_domain_name** 以及所有其他 **auth** 参数。（BZ#1937464）

- 在以前的版本中，代理更新会在持续集成（CI）运行时导致完整的集群配置更新，包括 API 服务器重启。因此，Machine API Operator 中的一些集群会因为意外的 API 服务器中断而超时。在这个版本中，代理测试分离并添加 postconditions，以便 Machine API Operator 中的集群在 CI 运行过程中再次变为稳定。（BZ#1913341）

- 在以前的版本中，删除处于 **Insufficient disk space on datastore** 状态的机器所需的时间比预期的要长，因为不同 vCenter 任务类型之间没有区别。在这个版本中，机器控制器删除过程会检查 vCenter 任务类型，不再阻止删除机器控制器。因此，机器控制器会被快速删除。（BZ#1918101）

- 在以前的版本中，即使实例类型缺失，从零注解进行扩展也会重新排队。因此，MachineSet 控制器日志中会有一个恒定的 requeue 和 error space 信息。在这个版本中，如果实例类型没有自动解析，用户可以手动设置注解。因此，如果用户手动提供注解，则可以从零对未知实例类型进行扩展。（BZ#1918910）

- 在以前的版本中，Machine API 终止处理器没有正确关闭 HTTP 响应。因此，goroutines 在 **net.http** 读写循环中会被泄漏，这会导致较高的内存用量。此更新确保了始终正确关闭 HTTP 响应。因此，内存用量现在是稳定的。（BZ#1934021）

- 在以前的版本中，在 MachineSet 控制器中创建的多个客户端集会导致启动时间较慢，这会导致一些大型集群中 pod 无法就绪度检查。因此，MachineSet 控制器会停留在无限循环中。在这个版本中修复了 MachineSet 控制器，使其使用单个客户端。因此，MachineSet 控制器的行为如预期。(BZ#1934216)

- 在以前的版本中，当升级由 Machine Config Daemon 在第一次引导时执行时，实例引导需要更长的时间。因此，worker 节点处于重启循环中，机器健康检查（MCH）删除了 worker 节点，因为它们没有正确启动。在这个版本中，MHC 不再删除没有正确启动的节点。相反，MHC 仅在明确请求时删除节点。（BZ#1939054）

- 在以前的版本中，因为未知原因，证书签名请求（CSR）批准会被延迟。因此，在安装过程中出现的新机器不会被迅速批准，从而延长集群安装。为了减少早期安装阶段中偶尔 API 服务器不可用的问题，这个更新会将缓存重新同步周期从 10 小时改为 10 分钟。因此，现在可以更快地批准 control plane 机器，集群安装不再会需要非常长的时间。(BZ#1940972)

- 在以前的版本中，默认的 Google Cloud Platform（GCP）镜像过期，并引用 OpenShift Container Platform 4.6 版本中的不支持较新版本的 Ignition 版本。因此，使用默认 GCP 镜像的集群中的新机器无法引导 OpenShift Container Platform 4.7 及之后的版本。在这个版本

中，GCP 镜像被更新以与发行版本匹配。现在，新机器可以使用默认的 GCP 镜像引导。（BZ#1954597）

- 在以前的版本中，由于对虚拟机的 ProvisioningState 值进行严格检查，虚拟机有时会在存在检查过程中失败。在这个版本中，检查会更加宽松，在存在检查过程中只有删除的机器会进入 **Failed** 阶段。(BZ#1957349)

- 在以前的版本中，如果您在 AWS 集群中使用 **oc delete machine** 删除了 control plane 机器，则机器不会从负载均衡器中删除。因此，负载均衡器继续为删除的 control plane 机器提供请求。在这个版本中，当您删除 control plane 机器时，负载均衡器不再为机器提供请求。(BZ#1880757)

- 在以前的版本中，当删除一个无法访问的机器时，为持久性卷创建并附加到节点的 vSphere Virtual Machine Disk（VMDK）会被错误删除。因此，VMDK 中的数据无法恢复。在这个版本中，如果 kubelet 无法访问，vSphere 云供应商会检查这些磁盘并从节点分离。因此，您可以在不丢失 VMDK 的情况下删除无法访问的机器。(BZ#1883993)

- 在以前的版本中，因为生成的 AWS 实例类型列表已过时，所以在使用带有零副本的 Cluster Autoscaler Operator 和机器集时，一些较新的 Amazon Web Services（AWS）实例类型无法从零扩展。AWS 实例类型列表现已更新，以包含较新的实例类型。在这个版本中，Cluster Autoscaler Operator 可以使用更多实例类型从零副本进行扩展。(BZ#1896321)

- 在以前的版本中，因为缺少上游驱除 API 功能，pod 中断预算不会在无法访问的节点上排空 pod。因此，在删除后，无法访问节点上的机器可能需要太多的时间才能被删除。现在，当删除无法访问节点上的机器时，宽限期超时将更改为 1 秒。在这个版本中，Machine API 可以成功排空和删除无法访问的节点。(BZ#1905709)

Cloud Credential Operator

- 在以前的版本中，一个重复的 **unsupported platform type: BareMetal** 警告信息会出现在裸机平台上。在这个版本中，裸机平台不再被视为未知平台。因此，可以减少误导的日志记录信息。(BZ#1864116)

- 在以前的版本中，一个周期性错误消息存储在 Cloud Credential Operator 的 **credentialsRequest** 自定义资源（CR）中，导致 CPU 使用量过大，并登录到一些错误场景，如 Amazon Web Services（AWS）速率限制。在这个版本中，删除了来自云供应商的请求 ID，以便错误消息存储在用户更容易地找到它们的条件中，并消除 **credentialsRequest** CR 中的重复错误信息。（BZ#1910396）

- 在以前的版本中，如果 CCO 的部署不健康，Cloud Credential Operator（CCO）和 Cluster Version Operator（CVO）都会报告。这会导致在出现问题时出现双重报告。在这个版本中，在部署不健康时，CCO 不再进行报告。（BZ#1957424）

Cluster Version Operator

- 在以前的版本中，Cluster Version Operator 在设置 **cluster_operator_up** 指标时会评估 **Available** 和 **Degraded** 参数，这会导致使用 **Available=True** 或 **Degraded=True** 的 Operator 显示 **ClusterOperatorDown** 警报。即使 **Available=True** 与 "has not available" 的警报描述不匹配。在这个版本中，Cluster Version Operator 在设置 **cluster_operator_up** 指标时会忽略 **Degraded** 参数。(BZ#1834551)

- 在以前的版本中，当在集群中安装 Prometheus 时，重要的平台拓扑指标不可用，如果使用调用器生成的安装程序指标设置为""，则会出现 CI 错误。现在解决了在提供造成错误的指标前通知程序没有同步的竞争条件。(BZ#1871303)

- 在以前的版本中，具有同一键的多个容限（如 Cluster Version Operator 自身的部署）的清单仅接受最后一个条目读取和覆盖之前的条目。这会导致 **in-cluster tolerations** 与清单列出的容限分离。在这个版本中，Cluster Version Operator 在完全相等时会考虑容限匹配。这允许 Cluster

Version Operator 保留清单中针对 **in-cluster** 资源的所有容限。（BZ#1941901）

- 在以前的版本中，Cluster Version Operator 对于没有设置这些属性的清单不会协调 **env** 和 **envFrom**。这意味着 Cluster Version Operator 没有正确管理容器环境。此更新改进了 Cluster Version Operator，以便在清单中未设置时清除 **env** 和 **envFrom**。这允许集群自动恢复对这些属性无效的 **cluster-admin** 更改。（BZ#1951339）

- 在以前的版本中，具有同一键的多个容限（如 **cluster-version-operator** 的部署对象）的清单仅接受最后一个条目读取和覆盖之前的条目。这会导致集群内容限与清单列出的容限分离。在这个版本中，Cluster Version Operator 认为容限在相等时是匹配的。这允许 Cluster Version Operator 保留清单中针对 in-cluster 资源的所有容限。（BZ#1941901）

- 在以前的版本中，当 **ClusterOperator** 资源降级了 10 分钟时，Cluster Version Operator 会报告 **ClusterOperatorDegraded** 警报。这个警报有时会在安装过程中发生，因为仍然在创建资源。这个版本将 10 分钟期限改为 30 分钟，为安装过程提供了充足的时间，从而可以避免不必要的 **ClusterOperatorDegraded** 警报。(BZ#1957991)

Compliance Operator

- 在以前的版本中，当用户运行合规检查时，会给出 **NON-COMPLIANT** 结果，但没有指示用户执行操作所需的补救步骤。此发行版本提供了一个 **instructions**，用户可以通过它来查看验证规则所需的步骤。这允许用户和审核员验证 Operator 正在检查正确的值。（BZ#1919367）

控制台 Kubevirt 插件

- 在以前的版本中，在帮助用户向虚拟化模板添加引导源的 Web 控制台表单中，说明的文本仅针对 Fedora 提供信息，不论模板所使用的操作系统是什么。在这个版本中，添加了一个修复程序，它提供了特定于模板的操作系统的示例，以便用户获得相关指导。(BZ#1908169)

- 在以前的版本中，在帮助用户创建虚拟机模板的 web 控制台向导中，因为给出的信息不清晰，使用户无法知道一个操作是针对于模板还是针对于一个虚拟机。在这个版本中，给出的信息更清晰，用户可以获得所需信息。（BZ#1922063）

- 在以前的版本中，web 控制台会有一个模糊的错误消息。这个信息会给试图将网络接口添加到从模板创建的虚拟机的用户造成不必要的混淆。在这个版本中，错误消息中添加了更详细的内容，因此用户可以更轻松地对错误进行故障排除。（BZ#1924788）

- 在以前的版本中，当您尝试通过 web 控制台从 RHEL 6 模板创建虚拟机时，会出现一个弹出窗口提供有关如何定义支持级别的信息，即使实际上并不支持 RHEL 6。在这个版本中，更改了这个窗口中的信息以明确告知用于 RHEL 6 不被支持。（BZ#1926776）

- 在以前的版本中，web 控制台中的一个下拉列表被按钮元素遮盖，用户无法在创建虚拟机时选择特定的操作系统。在这个版本中，对按钮元素的 **z-index** 值进行了调整，从而解决了以前的问题，用户可以选择任何可用的操作系统。（BZ#1930015）

- 在以前的版本中，如果您在没有定义的存储类的集群上使用了 web 控制台的新虚拟机向导，web 控制台会停留在无限循环中并崩溃。在这个版本中，如果没有定义存储类，会删除存储类下拉列表。因此，web 控制台不会崩溃。（BZ#1930064）

- 在以前的版本中，按钮元素中的文本没有清楚地描述按钮的实际功能（从收藏的列表中删除虚拟机模板）。在这个版本中更新了相关的信息以阐明该按钮的作用。（BZ#1937941）

- 在以前的版本中，对于具有 **RerunOnFailure** 运行策略的虚拟机，停止虚拟机会导致几个 UI 元素变得无响应，从而导致用户无法读取状态信息或重启虚拟机。在这个版本中解决了不响应的元素问题，用户可以使用这些功能。（BZ#1951209）

- 在以前的版本中，对于配置为具有独立 **/var** 分区的集群，查询文件系统只返回挂载在根目录中的磁盘大小，它不包括 **/var** 分区的大小。在这个版本中，查询的运行方式进行了改变，用户现在可以决定集群中文件系统的总大小。（BZ#1960612）

控制台存储插件

- 在以前的版本中，当正确的存储类不可用时，OpenShift Container Storage Operator 会显示一个错误消息。在这个版本中删除了这个错误消息，并禁用 **Next** 按钮，直到正确的存储类可用为止。（BZ#1924641）

- 在以前的版本中，当用户在创建内部附加存储集群时点击浏览器的 back 按钮时，安装向导会重新执行整个过程。在这个版本中解决了这个问题。（BZ#1928008）

- 现在，当您将一个节点添加到本地卷发现时，可以看到一个存在的节点的列表，这减少了不必要的导航。(BZ#1947311)

- 在以前的版本中，**Create Storage Cluster** 向导可让您启用一个具有未定义值的仲裁区域。此更新中的修复过滤掉了未定义的值，因此只能使用定义的值来创建仲裁区域。（BZ#1926798）

- 在以前的版本中，因为产品标题拼写以及使用注册商标的方式不一致，导致在在 web 控制台中错误地显示快速启动卡。在这个版本中，产品名称被正确拼写，注册商标的符号会正确地出现在第一个卡中。（BZ#1931760）

DNS

- 在以前的版本中，BZ#1936587 将全局 CoreDNS 缓存最大 TTL 设置为 900 秒。因此，从上游解析器接收的 NXDOMAIN 记录被缓存了 900 秒。在这个版本中，负 DNS 响应记录被显式缓存最多 30 秒。因此，解析 NXDOMAIN 不再被缓存 900 秒。（BZ#1943578）

- BZ#1953097 修复启用了 CoreDNS **bufsize** 插件，大小为 1232 字节。有些原始 DNS 解析器无法通过大于 512 字节的 UDP 接收 DNS 响应消息。因此，一些 DNS 解析器（如 Go 的内部 DNS 库）无法从 DNS Operator 接收详细的 DNS 响应。在这个版本中，所有服务器的 CoreDNS **bufsize** 设置为 512 字节。现在，UDP DNS 信息会被正确接收。(BZ#1966116)

- 在以前的版本中，集群上游解析器返回的 DNS 响应通过 UDP 超过 512 字节。因此，coreDNS 返回的 **SERVFAIL** 或其他错误消息，并强制客户端通过 TCP 重试。这个版本启用了 coreDNS bufisze 插件，UDP 缓冲区大小为 1232 字节。（BZ#1949361）

etcd

- 在以前的版本中，etcd Operator 存在一个传输泄漏问题，这会导致内存用量随着时间增大。解决了内存泄漏的问题。（BZ#1925586）

- 在以前的版本中，**etcdInsufficientMembers** 警报会错误地触发。在这个版本中，警报已被更新，除了实例标签外还包含 pod 标签，因此仅在 quorum 丢失时警报才会触发。（BZ#1929944）

- 在以前的版本中，因为引进了 SO_REUSEADDR 套接字选项，就绪度探测没有报告正确的就绪度，这会导致 即使在 etcd-quorum-guard 失败的情况下，etcd pod 也显示为就绪状态。现在，就绪度探测检查已被更新来考虑这些选项，etcd 就绪度探测现在可以正确地反映操作对象的就绪情况。（BZ#1946607）

- 在以前的版本中，**spec.loglevel** 字段没有在 etcd 操作对象上设置 **log-level** 标志，因此用户无法更改 etcd 日志级别。用户现在可以设置日志级别，如下所示：

  - **Debug**、**Trace** 和 **TraceAll** 日志级别映射到 etcd 的**debug** 日志级别

  - **Default** 或 **Normal** 日志级别映射到 etcd 的 **info** 日志级别

如需更多信息，请参阅 BZ#1948553。

- 在以前的版本中，在 etcd 过程后，下一个过程在相关端口被释放后才会启动。在此过程中增加了 **SO_REUSEADDR**，可以立即重复利用这些端口。如需更多信息，请参阅 BZ#1927942。

- 在以前的版本中，如果 **network.Status.ServiceNetwork** 字段未填充，etcd-endpoint 的 ConfigMap 会留空。因此，etcd Operator 无法扩展。OpenShift Container Platform 4.8 中的一项新功能允许 etcd Operator 在 **network.Status.ServiceNetwork** 字段未填充时扩展。（BZ#1902247）

镜像 Registry

- 在以前的版本中，镜像修剪器会在删除镜像失败时停止。因此,当两个镜像修剪器同时删除镜像时，其中一个镜像失败并显示 **not found** 错误。在这个版本中，**not found** 错误会被忽略，这将使镜像修剪器可以处理并发删除。(BZ#1890828)

- 在以前的版本中，在 Image Registry Operator 状态评估过程中缺少路由状态意味着 Image Registry Operator 没有降级，即使路由处于降级（**degraded**）状态。在这个版本中，Image Registry Operator 会获取所有配置的路由，并在评估其自身状态时评估其状态。在这个版本中，如果有任何路由处于降级状态，Image Registry Operator 会将自身报告为 **degraded**，并显示错误消息。（BZ#1902076）

- 在以前的版本中，自动创建的 Docker 配置 secret 不包括集成的内部 registry 路由的凭证。因为没有凭证用于通过任何路由访问 registry，因此尝试访问 registry 的 pod 会失败，因为缺少身份验证。在这个版本中，默认 Docker 凭证 secret 中包含所有配置的 registry 路由。现在，pod 可以通过其任何路由访问集成的 registry，因为凭证现在包含每个路由的条目。（BZ#1911470）

- 在以前的版本中，镜像 registry 忽略了集群范围的 **ImageContentSourcePolicy**（ICSP）规则。在 pull-through 中，镜像镜像被忽略，这会导致断开连接的集群中拉取失败。在这个版本中，如果目标存储库有 ICSP 规则，registry 会从镜像（mirror）拉取。因此，从配置的镜像拉取镜像不会失败。(BZ#1918376)

- 在以前的版本中，Image Registry Operator 不会更新 config 资源的 **.status.readyReplicas** 字段，因此其值始终为 **0**。在这个版本中，Image Registry Operator 将部署的就绪镜像 registry 副本数写入配置中。现在，此字段显示有多少镜像 registry 副本已就绪。（BZ#1923811）

- Azure 建议用户使用 Storage Accounts **v2** 而不是 **v1**。在某些安全配置集下，管理员可以强制 Azure 不接受创建 **v1** 存储帐户。由于镜像 registry 依赖于 **v1** 存储帐户，因此在这样的环境中集群安装会失败。在这个版本中，在集群 bootstrap 中，Image Registry Operator 会尝试创建和使用 **V2** Storage account。**v1** 上运行的集群继续使用 **V1** 存储帐户。安装成功，Image Registry Operator 现在会报告 **Available**。（BZ#1929654）

ImageStreams

- 在以前的版本中，从流导入多个镜像时，性能有时会慢。在这个版本中，对镜像 registry 的并发请求数量从 5 增加到 50，从而提高了性能。(BZ#1954715)

Insights Operator

- 在以前的版本中，Insights Operator 不会收集 Cluster Version Operator（CVO）Pod 或 **openshift-cluster-version** 命名空间中的事件。因此，Insights Operator 不会显示有关 CVO 可能遇到的任何问题的信息，用户无法获取有关 CVO 的诊断信息。Insights Operator 现已更新，它会从 **openshift-cluster-operator** 命名空间中收集 CVO Pod 和事件，以便 Insights Operator 报告 CVO 的问题。（BZ#1942271）

安装程序

- 在以前的版本中，DNSmasq 需要指定 IPv6 网络以外的任何 /64 网络时的前缀长度。因此，control plane 主机无法进行 PXE 引导。在这个版本中，DNSmasq 配置中包含子网前缀长度。因此，control plane 主机现在将在任何前缀长度的 IPv6 网络中引导 DHCP 和 PXE。(BZ#1927068)

- 安装到 vSphere 时，bootstrap 机器有时无法正确更新 **/etc/resolv.conf** 文件中的名称服务器。因此，bootstrap 机器无法访问临时 control plane，安装会失败。在这个版本中，包括查找正确行以更新更可靠的更改。现在，bootstrap 管理器可以访问其临时 control plane，安装可以成功。(BZ#1967355)

- 在以前的版本中，安装程序不会在生成其 URL 时考虑 bootstrap Ignition 配置应位于的区域。因此，bootstrap 机器无法从提供的 URL 获取配置，因为它不正确。在这个版本中，在生成 URL 时会考虑用户的区域，并选择正确的公共端点。因此，安装程序总是生成正确的 bootstrap Ignition URL。（BZ#1934123）

- 在以前的版本中，在创建存储帐户时，Azure 的 Minimum TLS 的默认版本是 1.0。因此，策略检查会失败。在这个版本中，将 openshift-installer Azure 客户端配置为在创建存储帐户时将 Minimum TLS 版本设置为 1.2。现在，策略检查会通过。（BZ#1943157）

- 在以前的版本中，使用 Azure 上 IPI 部署的私有集群有一个入站 NSG 规则，允许 SSH 到 bootstrap 节点。这个声明可能会触发 Azure 的安全策略。在这个版本中，NSG 规则已被删除。（BZ#1943219）

- 在以前的版本中，安装程序无法识别 **ap-northeast-3** AWS 区域。在这个版本中，安装程序允许安装适合已知分区模式的未知区域，允许用户在 **ap-northeast-3** AWS 区域中创建基础架构。（BZ#1944268）

- 在以前的版本中，内部平台无法创建内部负载均衡器。在这个版本中，当用户创建 manfiests 时，添加了一个检查，以确保仅在 AWS、Azure 和 GCP 等云平台中使用此策略。（BZ#1953035）

- 在以前的版本中，当命名 Google Cloud Platform 资源时，过滤器会阻止一些使用 **Google** 一词的某些名称。在这个版本中，在集群名称的安装程序中添加了一个检查，允许在设置名称时使用 **Google** 的一些变体。（BZ#1955336）

- 在以前的版本中，使用安装程序置备的基础架构进行裸机安装需要安装程序过程能够与置备网络通信。现在，安装程序过程可以与 API 服务器的虚拟 IP 通信。当置备网络不可路由且安装程序进程从远程位置运行，如 Hive for Red Hat OpenStack Platform（RHOSP）或 Red Hat Advanced Cluster Management 时，这个改变会导致这种情况。您可能需要调整防火墙规则，以允许与 API 服务器的虚拟 IP 上的 TCP 端口 **6385** 和 **5050** 通信。（BZ#1932799）

- 在以前的版本中，当在 Red Hat OpenStack Platform（RHOSP）上安装提供 **platform.openstack.machinesSubnet** 字段中不存在的子网 ID 时，**openshift-install** 命令会生成 SIGSEGV 和 backtrace。现在，**openshift-install** 命令会被修改，它会生成类似以下信息的错误：

  ```
  FATAL failed to fetch Metadata: failed to load asset "Install Config":
  platform.openstack.machinesSubnet: Not found: "<network-ID>"
  ```

  （BZ#1957809）

- 在以前的版本中，除非将 RHOSP HTTPS 证书导入到托管设备，在 Red Hat OpenStack Platform（RHOSP）上安装会失败。现在，当 **cloud.yaml** 中的 **cacert** 值被设置为 RHOSP HTTPS 证书时，会成功进行安装。不再需要将证书导入到主机。(BZ#1786314)

- 在以前的版本中，因为 **proxy.config.openshift.io** 中的外部网络条目不准确，安装可能会失败。现在，验证检查会识别出这些不准确以启用更正。(BZ#1873649)

- 以前，Traform 组件描述已被更清晰的信息替代。(BZ#1880758)
- gophercloud/utils 的先前更改引入了使用自签名证书的自定义 HTTP 客户端。由于此更改从 **DefaultTransport**（包括代理环境变量）中删除了设置，从而导致使用自签名证书和代理的安装失败。在这个版本中，自定义 HTTP 客户端会继承 **DefaultTransport** 中的设置，因此现在可以使用自签名证书和代理安装 OpenShift Container Platform。（BZ#1925216）
- 在以前的版本中，安装程序在验证过程中不会考虑安装配置中的 **defaultMachineSet** 值，这会导致安装程序失败。在这个版本中，默认值应用到安装配置，并开始验证空字段。(BZ#1903055)
- 在以前的版本中，**soft-anti-affinity** 需要客户端设置最小 Nova 微版本。Ansible OS 服务器模块的大多数版本都不需要客户端设置最小值。因此，软反关联性命令可能会失败。在这个版本中解决了在处理软反关联性时使用 Python OpenStack 客户端设置 Nova 微版本的问题。(BZ#1910067)
- 在以前的版本中，OpenStack UPI playbook 没有标记创建的所有资源。因此，**openshift-install destroy** 命令无法正确识别所有集群资源并循环删除资源，直到它达到超时（这会放弃资源）。在这个版本中，为 OpenStack UPI playbook 添加缺少的标签指令。(BZ#1916593)
- 在以前的版本中，**e2e-gcp-upi** 无法成功，因为 Python 软件包错误导致失败。在这个版本中，您可以为 gsutil 设置正确的 Python 版本、管道版本和 **CLOUDSDK_PYTHON** 以解决软件包错误。（BZ#1917931）
- 在以前的版本中，pip 版本 21 不支持安装的 Python 版本 2。因此，这会导致解决设置容器所需的所有依赖软件包错误。在这个版本中，pip 版本被修复为小于 21 的值，以避免出现这个问题。（BZ#1922235）
- 在以前的版本中，安装程序会收集有关云的信息两次。因此，对 OpenStack API 的请求数量翻倍，这在云上造成额外负载并增加安装时间。在这个版本中，在检查配额前收集有关云的信息，然后重复使用相同的验证信息。（BZ#1923038）
- 在以前的版本中，当使用 IPv6 部署时使用 /64 以外的子网置备网络时，DNSmasq 需要指定前缀长度。因此，在使用非 64 网络时主机无法进行 PXE 引导。在这个版本中，DNSmasq 配置中包含前缀长度。因此，主机在 DHCP 上成功，在任何前缀长度的 IPv6 网络中启动 PXE。（BZ#1925291）
- 在以前的版本中，在删除 **Shared Subnet** 标签时，OpenShift Container Platform 安装程序不会报告 IAM 权限问题，即使日志记录显示已删除它们。此更新会检查取消标记和日志记录错误的结果。现在，日志代表了未标记共享资源的状态。（BZ#1926547）
- 在以前的版本中，Azure 集群是使用 Premium_LRS 的磁盘类型创建的，且实例类型不支持 PremiumIO 功能，这会导致集群失败。在这个版本中，只有在磁盘类型为 Premium_LRS（默认磁盘类型）时，才会检查所选的实例类型是否具有 PremiumIO 功能。代码查询 Azure 订阅和区域以获取所需的信息，并在未满足条件时返回错误。（BZ#1931115）
- 在以前的版本中，当 API 服务器重启时，API VIP 可能会在 bootstrap 中不可用，这会导致置备服务不可用，并导致置备失败。置备服务 (Ironic) 现在包含在 VIP 健康检查中，API VIP 仍然可用。(BZ#1949859)

kube-apiserver

- 在以前的版本中，GCP 负载均衡器健康检查器会在主机上保留过时的 conntrack 条目，这会导致网络中断使用 GCP 负载均衡器的 API 服务器流量。健康检查流量不再循环主机，因此不再对 API 服务器造成网络中断。（BZ#1925698）

Machine Config Operator

- 在以前的版本中，排空超时和池限制周期太短，并可能导致在需要更多时间的普通集群中持续发出警报。在这个版本中，超时报告扩展失败前所需的时间。这为 Cluster Operator 提供了更现实和有用的警报，而不会永久降低普通集群的性能。（BZ#1968019）

- 在以前的版本中，当使用 OpenShift Installer Provisioned Infrastructure（IPI）从 VMware vSphere 创建新虚拟机时，节点无法加入集群。当由 DHCP 输入主机名代替 IDI 提供的名称时，会出现这种情况。这个问题已解决。（BZ#1920807）

- 在以前的版本中，如果在设置主机名前启用网络，安装可能会失败。这阻止节点加入 cluser，并在进行另一个尝试前强制进行五分钟的延迟。现在，这个问题已被解决，节点会在第一次尝试时自动加入集群。(BZ#1899187)

- 在以前的版本中，用户可以删除 core 用户和相关 SSH 密钥，尽管密钥仍然存在。在这个版本中，用户无法删除 core 用户。(BZ#1885186)

- 当从 4.6 升级到 4.7 时，只有在安装了节点时才会应用 **vsphere-hostname** 服务设置的主机名。如果在升级之前没有静态地设置主机名，则主机名可能会丢失。在这个版本中，删除了允许 **vsphere-hostname** 服务仅在安装节点时运行的条件。因此，升级时 vSphere 主机名不再丢失。（BZ#1942207）

- 由于 **Keepalived 2.0.10** 中存在一个错误，如果存活度探测终止了 **keepalived** 容器，分配给系统的任何虚拟 IP 地址（VIP）仍然保留，且在 **keepalived** 重启时不会被清理。因此，多个节点可以拥有相同的 VIP。现在，当 **keepalived** 启动时会删除 VIP。因此，VIP 由单个节点持有。（BZ#1931505）

- 在以前的版本中，与 rpm-ostree 相关的操作没有在非 CoreOS 节点上正确处理，如 Red Hat Enterprise Linux CoreOS（RHCOS）。因此，当在包含 RHEL 节点的池中应用操作（如内核切换）时，RHEL 节点会降级。在这个版本中，当非 CoreOS 节点上执行不支持的操作时,Machine Config Daemon 会记录一条消息。记录消息后，它会返回 nil 而不是错误。现在，当不支持的操作由 Machine Config Daemon 执行时，池中的 RHEL 节点会按预期进行。（BZ#1952368）

- 在以前的版本中，空静态 pod 文件被写入 **/etc/kubernetes/manifests** 目录中。因此，kubelet 日志报告错误，可能会导致与某些用户产生混淆。现在，当不需要时，空清单会被移到另一个位置。因此，kubelet 日志中不会出现错误。（BZ#1927042）

Metering Operator

- 在以前的版本中，Reporting Operator 在协调事件时错误处理 **Report** 自定义资源（CR），其中包含用户提供的保留周期。因此，过期的 **Report** CR 会导致 Reporting Operator 持续循环，因为受影响的自定义资源会无限期重新排队。在这个版本中，可以避免重新排队指定了保留周期的过期 **Report** CR。因此，Reporting Operator 可以正确地为过期的 **Report** CR 处理事件。（BZ#1926984）

监控

- 在以前的版本中，**node-exporter** daemontset 的 **mountstats** 收集器会导致在带有 NFS 挂载点的节点中使用高内存。在这个版本中，用户可以禁用 **mountstats** 收集器来减少内存用量。(BZ#1955467)

网络

- 在以前的版本中，一个不正确的 **keepalived** 设置有时会导致 VIP 结束在不正确的系统上，且无法返回到正确的系统。在这个版本中，删除了不正确的 **keepalived** 设置，以便 VIP 结束在正确的系统上。（BZ#1916890）

- 根据 iptables 重写规则，使用固定源端口通过服务 IP 和 pod IP 连接到服务的客户端可能会遇到端口冲突的问题。在这个版本中，插入了一个额外的 OVS 规则，以注意发生端口冲突时，并执行额外的 SNAT 以避免上述冲突。因此，连接到服务时不再有端口冲突。(BZ#1910378)

- 在以前的版本中，内部防火墙阻止 control plane 节点和出口分配节点之间的 IP 端口 9。这会导致将 IP 地址分配给出口节点失败。在这个版本中，可以通过 IP 端口 9 在 control plane 和出口（egress）节点间进行访问。现在，允许将 IP 地址分配给出口节点。（BZ#1942856）

- 在以前的版本中，UDP 服务流量可能会因为过时的连接跟踪条目不再有效而被阻止。此服务器容器集在为 **NodePort** 服务循环后进行 pevented 访问。在这个版本中，当 **NodePort** 服务循环时，连接跟踪条目会被清除，这将允许新网络流量访问循环端点。（BZ#1949063）

- 在以前的版本中，OVN-Kubernetes 网络供应商忽略带有多个 **ipBlocks** 的网络策略。在忽略第一个 ipBlock 后，每个 ipBlock 都被忽略，从而导致 pod 无法访问所有配置的 IP 地址。更正了用于从 Kubernetes 网络策略生成 OVN ACL 的代码。因此，带有多个 **ipBlock** 的网络策略现在可以正常工作。（BZ#1953680）

- 在以前的版本中，当使用 OVN-Kubernetes 集群网络供应商时，Kubernetes 服务会错误地接受任何端点。在这个版本中，在没有端点的情况下，不再为服务创建一个负载均衡器，因此不再接受流量。（BZ#1918442）

- 在以前的版本中，Mulltus 的 Container Network Interface（CNI）插件不知道以任意数量的零开头的 IPv6 地址。在这个版本中，CNI 插件可用于以大于零值开头的 IPv6。（BZ#1919048）

- 在以前的版本中，当机器配置策略的更改也触发重启时，SR-IOV Network Operator 启动重启时可能会触发竞争条件。如果发生这种情况，节点将处于非确定状态。在这个版本中，可以避免出现这种情况。（BZ#1921321）

- 在以前的版本中，当使用 Kuryr 集群网络供应商创建新用户置备的集群时，集群节点使用的 OpenStack 子集可能没有被检测到，从而导致集群安装超时。在这个版本中，可以正确地检测到子网，用户置备的安装会成功。（BZ#1927244）

- 在以前的版本中，当从 OpenShift Container Platform 4.6 升级到 OpenShift Container Platform 4.7 时，Cluster Network Operator（CNO）会错误地将自身标记为完成升级到下一版本。如果升级随后失败，则 CNO 会报告自己降级，但会错误地报告版本 4.7。在这个版本中，CNO 会等待集群网络供应商镜像成功升级，然后报告 CNO 升级成功。（BZ#1928157）

- 在以前的版本中，当使用 OVN-Kubernetes 集群网络供应商时，如果 Kubernetes 版本包含非数字字符的次版本，端点分片控制器可能无法运行。在这个版本中，端点片段控制器会被默认启用。（BZ#1929314）

- 当使用 Kuryr 集群网络供应商时，安装后创建的 Neutron 端口的命名模式与安装期间创建的 Neutron 端口不同。因此，安装后创建的 Neutron 端口不会添加到默认负载均衡器中。在这个版本中，Kuryr 会检测使用任一命名规则创建的 Neutron 端口。（BZ#1933269）

- 在以前的版本中，Open Virtual Network（OVN）将 Conpin 流量数据包的源 IP 地址改为负载均衡器的 IP 地址，当使用网络策略时有时会阻断流量。在这个版本中，Kuryr 会将流量打开到网络策略命名空间中所有服务的 IP 地址，并自由允许流量流。（BZ#1920532）

- 在以前的版本中，当在带有 IPv4 地址的节点上启动单堆栈 IPv6 集群时，kubelet 可能已经使用 IPv4 IP，而不是节点 IP 的 IPv6 IP。因此，主机网络 pod 会具有 IPv4 IP 而不是 IPv6 IP，这使得它们无法从仅支持 IPv6 的 pod 访问。在这个版本中，node-IP-picking 代码被修复，这会导致 kubelet 使用 IPv6 IP。（BZ#1939740）

- 在以前的版本中，因为未知的原因，kubelet 可能会为节点注册错误的 IP 地址。因此，节点会处于 **NotReady** 状态，直到重新引导为止。现在，systemd Manager 配置被重新载入，并带有有效的 IP 地址作为环境变量，这意味着节点不再进入 **NotReady** 状态，因为 kubelet 注册了错误的 IP

地址。（BZ#1940939）

- 在以前的版本中，重构一个shadowed 变量会导致与使用检查点文件相关的回归，SR-IOV pod 沙盒不会启动。在重构过程中，检查 kubelet 套接字的路径没有被正确考虑。在这个版本中，正确地恢复了 kubelet 套接字路径的检查，现在 SR-IOV pod 沙盒可以被正确创建。(BZ#1968625)

节点

- 在以前的版本中，运行 **lsblk** 的未授权容器 pod 中可以看到可靠的自主分布式对象存储（RADOS）块设备（RBD）。这个问题已被解决，运行 **lsblk** 的未授权容器容器集中将无法再看到 RBD。（BZ#1772993）。

- 在以前的版本中，在集群升级过程中，**/etc/hostname** 文件被 CRI-O 更改，这会导致节点失败并在重启时返回。在这个版本中，在 CRI-O 中添加了特殊处理，以便在升级过程中单独保留 **/etc/hosts** 文件，这允许升级的节点在不出现问题的情况下引导。（BZ#1921937）

- 在以前的版本中，CRI-O 在网络置备后创建 pod 所需的时间太长。这会在网络清理代码中触发一个错误，从而导致网络资源在调配网络资源后无法正确清理。这个版本会更改代码来正确清理网络资源，即使命令超时也是如此。这使得集群可以继续正常的网络操作，即使 pod 创建用时过长。（BZ#1957224）

- 在以前的版本中，使用 **CNI** 插件重启节点无法成功完成。CRI-O 被修改为在重启前运行的所有容器上调用 **CNI DEL**。在这个版本中，清理 **CNI** 资源并允许成功重启。(BZ#1948137)

- 在以前的版本中，如果 **CNI DEL** 请求失败，则不会处理它，因为 **CNI** 清理操作不会检查清理失败。现在，CRI-O 会重复调用 **CNI DEL** 请求直到成功为止，正确地清理 **CNI** 资源。(BZ#1948047)

- 在以前的版本中，如果在容器或镜像提交到磁盘时重启发生，对容器或镜像的重启请求可能会导致失败。这会导致容器存储的明显损坏，并导致导致镜像或从镜像重新创建容器失败。此更新会检测节点的重启，并清除容器存储（如果为 true）。(BZ#1942536)

- 在以前的版本中，**runc** 采用运行它的实体的权限。但是，**workdir** 的权限由 **container** 用户设置。当这些权限有所不同时，容器创建错误发生，并导致容器启动失败。此补丁更新了 **runc**，它会尝试多次 **chdir** 到 **workdir**，以防有一次失败。这样可确保容器创建成功。（BZ#1934177）

- 在以前的版本中，CRI-O 日志不包含有关镜像拉取（pull）的源的信息。在这个版本中，日志拉取源被添加到 CRI-O 日志的 info 级别。(BZ#1881694)

- 在以前的版本中，当 pod 被快速创建和删除时，pod 可能没有足够的时间来在 pod 启动删除前完成 pod 沙盒创建。因此，pod 删除可能会失败，并带有 'ErrCreatePodSandbox' 错误。现在，如果 pod 终止，这个错误会被忽略。因此，如果 pod 无法完成 pod 沙盒创建，pod 终止不再会失败。(BZ#1908378)

- 在以前的版本中，Machine Config Operator（MCO）不接受 **trace** 作为有效的日志级别。因此，MCO 无法提供一个方法来启用追踪级别的日志记录，即使 CRI-O 支持它。MCO 现在已更新，以支持 **trace** 日志级别。因此，用户可以通过 MCO 配置来查看 trace 日志级别。（BZ#1930620）

- 在以前的版本中，kubelet 会尝试获取没有完全拉取的镜像的状态。因此，**crictl** 会对这些镜像报告一个 **error locating item named "manifest"** 错误。CRI-O 现在被更新为不列出没有清单的镜像。因此，**crictl** 不再报告这些错误。（BZ#1942608）

- 在以前的版本中，不会删除过时的状态信息。因此，Machine Config Operator（MCO）有时无法找到正确的机器配置池。在这个版本中，添加了一个清理功能来限制状态数量。因此，MCO 最多保留 3 个不同的 kubeletConfig 状态。（BZ#1950133）

- 在以前的版本中，当从 OpenShift Container Platform 版本 4.6.25 升级时，在具有多个 **kubeletconfig** CR 或 **ContainerRuntimeConfig** CR 的集群中，Machine Config Operator（MCO）可能会为同一配置生成重复的机器配置。因此，升级会失败，因为 MCO 将使用旧的控制器版本（IGNITIONVERSION 3.1.0）。在这个版本中清理了过时的重复机器配置，并允许从 4.6.25 正确升级。（BZ#1955517）

oauth-apiserver

- 在以前的版本中，一些 OAuth 服务器指标没有被正确初始化，且不会出现在 Prometheus UI 中的搜索中。现在，缺少的 OAuth 服务器指标会被正确初始化，并出现在 Prometheus UI 指标搜索中。(BZ#1892642)

- 在以前的版本中，如果自定义安全性上下文约束（SCC）包含 **defaultAllowPrivilegeEscalation: false** 和 **allowPrivilegedContainer: true** 字段的组合，则安全性上下文变异将特权 **openshift-apiserver** 和 **oauth-apiserver** pod 改为失败 API 验证的状态。容器集启动失败，有时会导致 OpenShift API 中断。现在,安全性上下文变异会忽略已经特权的容器的 **defaultAllowPrivilegeEscalation** 字段，而包含这些字段的自定义 SCC 不会阻止 Pod 启动。（BZ#1934400）

oc

- 在以前的版本中，当运行 **oc explain** 命令时，如果作为资源字符串的一部分提供资源组名称，则不会自动检测到资源组名称。如果不同组中的两个资源具有相同的资源名称，则返回最高优先级定义，除非通过 **--api-version** 参数声明该组。现在，如果没有包含 **--api-version** 参数，则会针对资源字符串运行前缀检查，以检测组名称。命令返回的说明与上述组中的匹配资源相关。(BZ#1725981)

- 在以前的版本中，**oc image extract** 命令没有从镜像的根目录中提取文件。命令已更新，现在可以用于从映像根目录中提取文件。（BZ#1919032）

- 在以前的版本中，**oc apply** 命令会在每次调用时获取 OpenAPI 规格。现在，当命令首次运行时，OpenAPI 规格会被缓存。当 **oc apply** 命令多次运行并减少了网络负载时，缓存的 OpenAPI 规格会被重复使用。（BZ#1921885）

- 在以前的版本中，在镜像镜像过程中创建的授权标头可能会超过某些 registry 的标头大小限制。这在镜像操作过程中会导致错误。现在，**oc adm catalog mirror** 命令的 **--skip-multiple-scopes** 选项被设置为 **true**，以帮助防止授权标头超过标头大小限值。(BZ#1946839)

- 在以前的版本中，当 **oc volume set** 命令包含 **--claim-class** 选项时，**storageClassName** 属性不会添加到 **PersistentVolumeClaim** 对象中。**--claim-class** 选项的值被添加到 **volume.beta.kubernetes.io/storage-class** 注解中。这会导致卷快照因为依赖 **storageClassName** 属性而失败。现在，**oc volume set** 命令将 **--claim-class** 选项的值应用到 **PersistentVolumeClaim** 对象中的 **storageClassName** 属性，卷快照可以引用属性值。（BZ#1954124）

- 在以前的版本中，**oc adm top --help** 的输出表示 **oc adm top** 命令可能会显示 pod 和节点的 CPU、内存和存储资源使用情况。**oc adm top** 命令不显示存储资源使用情况。现在，**oc adm top --help** 输出中没有包括存储引用。（BZ#1959648）

Operator Lifecycle Manager (OLM)

- 在以前的版本中，作为 Operator 安装一部分应用的 **CustomResourceDefinition**（CRD）对象有时可以满足同一 Operator 的较新版本的安装要求。因此，在 Operator 升级过程中，被替换的版本可能会被永久删除。在某些情况下，升级会停止。在这个版本中，作为 Operator 捆绑包安装一部分创建的或更新的 CRD 会被注解以指示其原始卷捆绑包。**ClusterServiceVersion**（CSV）对象使用这些注解来区分预先存在的 CRD 和相同捆绑包 CRD。因此，在应用当前版本的 CRD 前，升级不会完成。（BZ#1947946）

- 在以前的版本中，运行由 **CatalogSource** 对象引用的索引的 pod 没有在 **securityContext** 字段中明确设置 **readOnlyRootFileSystem: false**。因此，如果存在一个安全上下文限制（SCC），它会强制 **readOnlyRootFileSystem: true**，并匹配该 pod 的 **securityContext** 匹配，它会被分配给该 pod，并导致它重复失败。在这个版本中，在 **securityContext** 字段中明确设置 **readOnlyRootFileSystem: false**。因此，**CatalogSource** 对象引用的 pod 不再与强制执行只读根文件系统的 SCC 匹配，因此不再失败。（BZ#1961472）

- 在以前的版本中，如果在初始安装过程中在 **startCSV** 字段中指定版本，Operator Lifecycle Manager（OLM）不允许安装跳过的版本。这会导致这些跳过的版本无法安装，即使用户想要安装它们，无论为何要跳过它们。在这个版本中更新了 OLM，允许用户仅在初始安装过程中使用 **Subscription** 对象中的 **startCSV** 规格安装跳过的版本；用户仍然无法升级到跳过的版本，如预期一样。(BZ#1906056)

- 因为 **k8s.io/apiserver** 没有处理 webhook 授权器的上下文错误，所以上下文错误（如超时）会导致授权器 panic。在这个版本中，增加了 API 服务器版本，使其包含此问题的上游修复，因此授权者可以正常处理上下文错误。（BZ#1913525）

- 在以前的版本中，**oc adm catalog mirror** 命令无法轻松地用于在 airgapped 环境中监控镜像 Operator 目录。在这个版本中，目录的内容可以镜像到文件系统，放置到可移动介质中，然后从文件系统镜像（mirror）到 registry，以供 airgapped 集群使用。（BZ#1919168）

- Catalog Operator 之前为安装计划创建了捆绑解包作业，但不设置超时。如果不存在或删除的捆绑包镜像，这会导致作业永久运行，安装计划将保留在 **Installing** 阶段，而不表示作业的 pod 无法解析镜像。在这个版本中，Catalog Operator 在捆绑解包作业上设置一个默认的 **10m** 超时，可以使用 **--bundle-unpack-timeout** 标志进行配置。因此，在配置的超时后捆绑解包作业会失败，安装也会过渡到 **Failed** 阶段，原因在 **status.conditions** 和 **status.bundleLookups.conditions** 属性中可见。（BZ#1921264）

- OpenShift Container Platform 4.6 之前在集群上安装的 Operator 之前没有被识别为来自给定 Operator 软件包，用于依赖项解析和升级选择。这会导致现有 Operator 安装与其自己的订阅标准冲突，这会阻止命名空间内的升级和依赖项解析。在这个版本中更新了 OLM，以推断订阅引用的 Operator 的软件包名称和版本。因此，升级和依赖项解析可以如预期进行。（BZ#1921953）

- 用于临时错误的 **Info** 日志级别会导致 OLM Operator 日志详细记录默认配置。在这个版本中，临时错误日志级别被改为 **debug**。因此，在 **debug** 配置中可以看到较少的非关键日志。(BZ#1925614)

- 在以前的版本中，**Subscription** 对象的 **spec.config.resources** 部分总是应用于安装的部署，即使它未设置或为空。这会导致集群服务版本（CSV）中定义的资源被忽略，且只使用 **Subscription** 对象的 **spec.config.resources** 部分中定义的资源。在这个版本中更新了 OLM，仅在 **spec.config.resources** 部分设置为非 nil 或 non-empty 值时覆盖特定于部署的资源。（BZ#1926893）

- 在依赖项和升级解析过程中，订阅的唯一性以前是基于订阅的软件包名称。如果命名空间中的两个订阅订阅同一软件包，它们会在内部被视为单个订阅，从而导致意外行为。在这个版本中，订阅在命名空间内部由 **.metadata.name** 而不是 **.spec.name** 进行唯一标识。因此，带有相同地 **.spec.name** 的多个 **Subscription** 对象的命名空间的升级和依赖关系解析行为一致。（BZ#1932001）

- 当在后续的目录更新轮询尝试前剩余一分钟时，interval jitter 函数会截断重新同步间隔到零。这会导致 Operator Catalog 进入热循环，并浪费 CPU 周期。在这个版本中增加了用于计算重新同步延迟的 jitter 函数的精度。因此，Catalog Operator 大多会处于闲置状态，直到下一次目录更新轮询为止。（BZ#1932182）

- 在 Operator 升级过程中，任何关联的 **ServiceAccount** 对象的所有者引用已更新为指向新的 **ClusterServiceVersion**（CSV）对象，而不是旧对象。这可能会导致在协调 CSV 和 Catalog Operator 的 OLM Operator 之间出现竞争条件，它会执行安装计划，因为服务帐户所有权更改将

旧 CSV 标记为 **Pending/RequirementsNotMet**。当新 CSV 无限期等待旧 CSV 表示健康状态时，这会阻止升级完成。在这个版本中，第二个所有者已附加到任何现有所有者，而不是在一个步骤中更新所有者引用。因此，同一服务帐户可以同时满足旧 CSV 和新 CSV 的要求。（BZ#1934080）

- 在以前的版本中，集群服务版本（CSV）需要关联的服务帐户没有设置 **ownerReferences** 值，或者将 **ownerReferences** 值设置为相关的 CSV。这会导致，**default** 服务帐户（它没有作为 Operator 安装的一部分创建）无法满足 CSV 的要求，如果其 **metadata.ownerReferences** 字段不为空。在这个版本中，CSV 需要相关服务帐户将 **ownerReferences** 值设置为 CSV，或者将 **ownerReferences** 值设置为相关的 CSV。因此，只有非 CSV **ownerReferences** 值的服务帐户可以满足任何 CSV 的要求。(BZ#1935909)

- 在 OpenShift Container Platform 4.5 之前，由 **openshift-marketplace** 命名空间中的 Marketplace Operator 部署和管理的默认目录由 **OperatorSource** 对象创建，后者是由 Marketplace Operator 公开的 API。提供了适当的指标和警报，以指示 Operator 源遇到的错误。在 OpenShift Container Platform 4.6 中，**OperatorSource** 资源在几个发行版本已弃用后被删除，而 Marketplace Operator 则直接创建 OLM 的 **CatalogSource** 资源。但是，没有为 **openshift-marketplace** 命名空间中部署的目录源执行相同的指标和警报检测。因此，默认的目录源遇到的错误不会在 Prometheus 警报中突出显示。在这个版本中，OLM 中引入了新的 **catalogsource_ready** 指标，每当默认目录源的指标表示目录源处于 unready 状态时，Marketplace Operator 会触发警报。现在，Prometheus 警报会为 **openshift-marketplace** 命名空间中的未就绪默认目录源提供。(BZ#1936585)

- 在以前的版本中，当从默认频道和非默认频道提供 candidate Operator 依赖项时，Operator Lifecycle Manager（OLM）可能会生成一个随机指定两个频道之一的订阅。现在，候选者会首先从默认频道，然后从其他频道满足 Operator 的依赖关系。（BZ#1945261）

- 在以前的版本中，集群服务版本（CSV）可能被复制为多个 Operator 的组件。当在安装 Operator 后将命名空间添加到 Operator 组时，可能会发生这种情况。这个行为会影响内存使用和 CPU 负载。现在，CSV 不会出现在 Operator 的 **status.components** 字段中，原因为 **Copied**，性能不受影响。（BZ#1946838）

Operator SDK

- 在以前的版本中，有些资源被发现在无限循环中，因为 **ManagedFields** 在协调过程中被处理。在这个版本中，更新了 **operator-lib** 来忽略 **ManagedFields**，从而获得一致性的循环。(BZ#1856714)

- 正在为 Operator SDK 输出帮助信息，因为在 CLI 上传递 **--help** 时默认插件没有被调用。在这个版本中，调用默认插件，并在用户运行 **operator-sdk init --help** 命令时显示更为有用的帮助信息。(BZ#166222)

- 在以前的版本中，如果使用缺少的可选验证器运行，**operator-sdk bundle** 将失败，而不是发出警告。这个问题已被修正。（BZ#1921727）

openshift-apiserver

- 在以前的版本中，自定义安全性上下文约束（SCC）可能比默认集合中的其他人具有更高的优先级。因此，这些 SSC 有时与 **openshift-apiserver** pod 匹配，这会破坏它们在 root 文件系统中写入的功能。此错误还会导致一些 OpenShift API 中断。在这个版本中，**openshift-apiserver** pod 中明确提到 root 文件系统应该可写。因此，自定义 SCC 不应该阻止 **openshift-apiserver** pod 运行。（BZ#1942725）

Performance Addon Operator

- 在以前的版本中，当将容器配置为提供低延迟响应时，带有 CRI-O 的动态中断掩码与 **byirqbalance** 系统服务的中断掩码不匹配。各自设置不同的掩码和被破坏的容器延迟。在这个版

本中，通过将 CRI-O 设置为与其 **irqbalance** 系统服务匹配来更改中断掩码设置。因此，动态中断掩码处理现在可以正常工作。（BZ#1934630）

RHCOS

- 在以前的版本中，在引导过程中启用多路径太晚。因此，Red Hat Enterprise Linux CoreOS (RHCOS) 会在有些多路径环境中返回 I/O 错误。在这个版本中，多路径已在引导过程早期启用。因此，RHCOS 不再在某些多路径环境中返回 I/O 错误。(BZ#1954025)

- 在以前的版本中，一个潜在的竞争条件可能会导致 Red Hat Enterprise Linux CoreOS（RHCOS）PXE 部署中获取 rootfs 在一些环境中失败。在这个版本中，添加了在尝试拉取 rootfs 之前重试连接检查，以便在继续执行 **coreos-livepxe-rootfs** 脚本有时失败前验证对远程服务器和 rootfs 文件的访问。(BZ#1871303)

- 在以前的版本中，**MachineConfig** 的用户预设置会被忽略。这意味着用户无法更改 **kdump.service** 的配置。现在，默认预设置的优先级级别低于用户配置的默认值，因此用户配置可以正确地覆盖供应商配置。（BZ#1969208）

- 在以前的版本中，**coreos-installer** 会拒绝安装到带有损坏 GUID 分区表（GPT）的磁盘中，因为它会在使用安装镜像覆盖目标磁盘的 GPT 前尝试读取它。在这个版本中，当指示保留现有分区时，**coreos-installer** 只通过读取目标磁盘的 GPT 成功安装到带有损坏 GPT 的磁盘中。（BZ#1914976）

- 在以前的版本中，在未格式化的直接访问存储设备（DASD）上安装集群会导致 **coreos-installer** 错误地创建磁盘扇区。现在，**coreos-installer** 可以正确地格式化新的、未格式化的 DASD 驱动器到 4096 个字节扇区。这允许 **coreos-installer** 完成操作系统镜像的安装到磁盘驱动器。（BZ#1905159）

- 在以前的版本中，s390x z15 系统中的硬件辅助 **zlib** 解压缩会导致挂载 RHEL rootfs 镜像失败，这会导致使用 RHEL 8.3 内核的 REHL s390x z15 节点引导失败。现在，当有硬件辅助 **zlib**压缩时，内核已被更新来正确处理 **zlib**-compressed squashfs 文件。(BZ#1903383)

- 在以前的版本中，**zipl** 命令通过假设扇区大小为 512 字节来配置磁盘 geometry。因此，在带有 4k 扇区的 SCSI 磁盘中，**zipl** 引导装载程序配置包含不正确的偏移，zVM 无法引导。在这个版本中，**zipl** 会考虑磁盘扇区大小，以便 zVM 可以成功引导。（BZ#1918723）

- 在以前的版本中，**chrony.config** 可能会自动运行多次，除第一次运行外，每次都会失败。这会导致问题，因为 **chrony.config** 配置在初始运行时被设置且无法更改。现在，通过将配置设置过程限制为首次运行 **chrony.config** 来避免这些错误。（BZ#1924869）

- 在以前的版本中，节点会出现不健康状态，在高负载期间不会如预期运行。这会导致使用内存比内存快的工作负载被回收。在这个版本中，解决了内存回收和内存不足的情况，这些状况在负载较大时不再发生。(BZ#1931467)

- 在以前的版本中，使用 kernal 参数的绑定接口的最大传输单元（MTU）规格没有被正确分配。这个问题已被修正。（BZ#1932502）

- 在以前的版本中，**clevis-luks-askpass.path** 单元不会被默认启用。这会导致重启后非 root **LUKS Clevis** 设备无法自动解锁。这个版本默认启用 **clevis-luks-askpass.path** 单元，并允许非 root **LUKS Clevis** 设备在重启时自动解锁。(BZ#1947490)

- 在以前的版本中，systemd 过度读取 **mountinfo** 和过量消耗 CPU 资源，这会导致容器无法启动。在这个版本中，**systemd** 读取 **mountinfo** 时启用限制，允许容器成功启动。(BZ#1957726)

- 在以前的版本中，当 Machine Config Operator（MCO）在启动时调用 Ignition 来检查 Ignition 版本时，Ignition 会崩溃。因此，MCO 启动会失败。在这个版本中，MCO 不再查询 Ignition 版本，MCO 会成功启动。(BZ#1927731)

路由

- 在以前的版本中，HAProxyDown 警报信息是模糊的。因此，最终用户认为警报意味着路由器 Pod（而非只有 HAProxy pod）不可用。在这个版本中，HAProxyDown 警报信息更清晰。（BZ#1941592）

- 在以前的版本中，HAProxy 的帮助程序功能模板负责为白名单 IP 生成文件，这预期为错误的参数类型。因此，较长 IP 列表中的后端不会应用白名单 ACL。在这个版本中，helper 功能模板的参数类型会被改变，以便白名单 ACL 应用到长 IP 列表的后端。(BZ#1964486)

- 在以前的版本中，当使用自定义域创建 Ingress 时，Ingress Ingress 控制器使用路由器规范主机名更新 Ingress 的状态，并使用 **external-dns** 与 Route 53 同步。问题是 DNS 中不存在规范路由器主机名，且不是由 OpenShift Container Platform 创建的。OpenShift Container Platform 创建 ***.apps.<cluster_name>.<base_domain>** DNS 记录，而不是 **apps.<cluster_name>.<base_domain>** DNS 记录。因此，规范路由器主机名不正确。在这个版本中，将规范路由器主机名设置为 **router-default.apps.<cluster_name>.<base_domain>**。具有自动化并采用规范主机名并加上通配符或子域的集群管理员应注意，规范入口主机名被设置为 **<ingress-controller-name>.apps.<cluster_name>.<base_domain>**。(BZ#1901648)

- 在以前的版本中，BZ#1932401 的修复会覆盖默认的 Go HTTP 客户端传输。因此，集群范围的代理设置不会被 Ingress Operator pod 处理，这会导致在带有集群范围出口代理的集群上出现 Canary 检查失败。在这个版本中，在 canary 客户端的 HTTP 传输中明确设置了代理设置。因此，canary 检查可用于所有集群范围的代理。（BZ#1935528）

- 在以前的版本中，canary DaemonSet 没有指定节点选择器，因此它会为 canary 命名空间使用默认节点选择器。因此，canary DaemonSet 无法调度到 infra 节点，在某些情况下会引发警报。在这个版本中，将 Canary DaemonSet 明确调度到 infra 节点，并容许污点的 infra 节点。这允许 Canary DaemonSet 安全地部署到 worker 和 infra 节点，而无需出现问题或警报。（BZ#1933102）

- 在以前的版本中，当从带有空闲工作负载的旧版本升级集群时，闲置工作负载在升级到 OpenShift Container Platform 4.6 或 4.7 后不会在 HTTP 请求中唤醒，因为 **oc idle** 功能修复并重新工作。在这个版本中，闲置更改从端点镜像到 Ingress Operator 启动时的服务。因此，升级后取消闲置工作负载可以正常工作。（BZ#1925245）

- 在以前的版本中，通过将所有 HTTP 流量重定向到 HTTPS 的外部负载均衡器公开默认 Ingress Controller 会导致 Ingress Canary 端点检查失败，从而导致 Ingress Operator 降级。在这个版本中，明文 Canary 路由转换为边缘加密路由。现在，canary 路由只在负载均衡器重定向不安全流量时才可以正常工作。（BZ#1932401）

- 在以前的版本中，Ingress Operator Canary Check Client 会将 Canary 请求通过 HTTP 发送到丢弃 HTTP 流量的负载均衡器。这会导致 Ingress Operator 在 Canary 检查失败后变为降级。在这个版本中，Ingress Operator Canary Check Client 从启动时通过 HTTPS 发送 Canary 检查请求，而不依赖于路由器的重定向。现在，canary 检查可以通过丢弃不安全 HTTP 流量的负载均衡器来公开默认 Ingress Controller 的集群。（BZ#1934773）

- 在以前的版本中，**openshift-router** 使用的 HAProxy 模板重复调用 **firstMatch()** 函数。该函数每次都解析和重新编译正则表达式。在对 **firstMatch()** 的每个调用中解析和重新编译正则表达式非常昂贵，特别是具有数以千计路由的配置。在这个版本中，如果调用 **firstMatch()** 中的正则表达式已被看到，则已编译的版本将被重复使用并缓存。现在，在解析和评估 **haproxy-config.template** 时，运行时减少了 60%。（BZ#1937972）

- 在以前的版本中，用户可以使用覆盖注解命名带有无效主机名的路由。在这个版本中解决了这个问题。（BZ#1925697）

- 在以前的版本中，从通过路由公开的服务中删除 选择器（**selector**） 会导致为服务 pod 创建的 **endpointslices** 重复，这会因为重复的服务器条目而触发 HAProxy 重新加载错误。在这个版本

中，在编写 HAProxy 配置文件时会过滤掉意外重复的服务器行，因此从服务中删除选择器不再会导致路由器失败。（BZ#1961550）

Samples

- 在以前的版本中，Cluster Samples Operator 可能会更改其正在监视的对象的控制器缓存，这会导致 Kubernetes 管理控制器缓存时出现错误。在这个版本中，Cluster Samples Operator 如何使用控制器缓存中的信息。因此，Cluster Samples Operator 通过修改控制器缓存不会造成错误。（BZ#1949481）

service-ca

- OpenShift Container Platform 4.8 允许用户以非 root 用户身份运行 **service-ca-operator** pod，以满足其机构的需求。当以非 root 用户身份运行时，**service-ca-operator** 会以以下 UID 和 GID 的形式运行：

  ```
  uid=1001(1001) gid=1001 groups=1001
  ```

  (BZ#1914446)

存储

- 在以前的版本中，请求一个 **capacity breakdown** 容量时不会报告块类型 **PVC** 文件系统的指标。这意味着用户收到所有文件系统中指标的不准确报告。在这个版本中，Kubelet 请求块类型 **PVC**。这提供了对所有文件系统指标的准确报告。(BZ#1927359)

- 在以前的版本中，**/var/lib/kubelet** 在 **Cinder CSI Node Controller** 容器中被挂载两次。这会导致 **CSI Node Controller** 无法启动并显示 **/var/lib/kubelet/pods** 缺少空间的错误。在这个版本中，删除了 **/var/lib/kubelet** 和 **/var/lib/kubelet/pods** 的重复挂载，这允许 **CSI Node Controller** 成功运行。(BZ#1952211)

- 在以前的版本中，在 Cinder CSI Driver 调整持久性卷（PV）大小的过程中，**findmnt** 命令会收到多个卷挂载，且无法选择正确的挂载，从而导致重新定义大小停止。因此，用户必须手动扩展文件系统。在这个版本中，命令使用第一次挂载，以便文件系统与 PV 的大小调整。（BZ#1919291）

- 现在，在创建默认存储类时，Cinder CSI Driver Operator 会自动为 Cinder CSI 置备默认 **VolumeSnapshotClass** 对象，而不是手动创建 **VolumeSnapshotClass** 对象。（BZ#1905849）

- 在以前的版本中，recycler-pod 模板被错误地放入 kubelet 静态清单目录中。这个错误的位置会产生静态 pod 日志消息，指出回收器静态 pod 启动失败。在这个版本中，错误的 recycler-pod 模板已从静态 pod 清单目录中移除。因此，不再会出现错误消息。(BZ#1896226)

- 在以前的版本中，Local Storage Operator（LSO）可能会声明属于其他置备程序磁盘，因为忙碌磁盘被错误地检测到为空闲。现在会检查磁盘中的绑定挂载，以便 LSO 无法声明这些磁盘。（BZ#1929175）

- 在以前的版本中，LSO 会尝试创建一个带有无效标签值的持久性卷（PV），因为设备 ID 包含不受支持的字符，例如 **:**。通过将设备信息从标签移到注解中，这个问题已被修正。（BZ#1933630）

- 在以前的版本中，Local Storage Operator（LSO）没有清理持久性卷（PV），因为删除器没有被正确排队。这会导致 PV 处于 **released** 状态。现在，PV 可以被正确排队，以便可以正确删除 PV。(BZ#1937145)

- 在以前的版本中，当 pod 被删除时，Fibre Channel 卷会错误地从节点卸载。当节点上 kubelet 未

运行时，使用该卷的不同 pod 会在 API 服务器中删除。在这个版本中，Fibre Channel 卷在新 kubelet 启动时正确卸载。另外，在新 kubelet 完全启动和卸载卷前，卷无法挂载到多个节点，这样可确保光纤通道卷不会被破坏。（BZ#1954509）

Web 控制台（管理员视角）

- 在以前的版本中，当在开发人员模式的控制台 UI 中尝试删除 CNV 命名空间中的自定义资源时，点 **Delete** 会导致 **Delete** 按钮挂起处于卡住状态。此外，在 CLI 中执行相同操作时出现的错误消息不会显示。在这个版本中，错误消息会如预期显示，**Delete** 按钮不会处于卡住状态。（BZ#1939753）

- 在以前的版本中，OperatorHub Provider Type **filter** 属性没有清晰地显示与 **CatalogSource** 的关系。因此，用户无法知道 **filter** 标准的含义。此补丁将 Provider Type **filter** 更新为 **Source**。这可以更清楚地显示 **filter** 和 **CatalogSource** 之间的关系。(BZ#1919406)

- 在以前的版本中，**Resources** 菜单中的 **ResourceListDropdown** 组件没有对某些语言进行国际化。在这个版本中，**Resource** 菜单已被更新，以便为非英语用户提供更好的用户体验。(BZ#1921267)

- 在以前的版本中，一些菜单项（如 **Delete Persistent Volume Claim**）没有正确国际化。现在，更多菜单项目已被正确国际化。（BZ#1926126）

- 在以前的版本中，**Add HorizontalPodAutoscaler** 页面的一些文本和警告信息没有被国际化。文本现已国际化。（BZ#1926131）

- 在以前的版本中，当用户使用 Operator SDK 创建 Operator 并指定如下注解时，如 **xDescriptors={"urn:alm:<...>:hidden"}** 以隐藏 Operator 实例创建页面中的字段，该字段可能仍会在页面中可见。现在，Operator 实例创建页面中会省略隐藏字段。(BZ#1966077)

- 在以前的版本中，表在移动设备中没有正确显示。在这个版本中，表会正确显示。（BZ#1927013）

- 在以前的版本中，启动 OpenShift Container Platform Web 控制台可能会很慢。在这个版本中，Web 控制台启动速度更快。(BZ#1927310)

- 在以前的版本中，向 OpenShift Container Platform 管理员发出的通知没有进行国际化。现在，进行了一些国际化。（BZ#1927898）

- 在以前的版本中，**Cluster Utilization** 仪表板中对持续时间信息缺少国际化。现在，进行了一些国际化。（BZ#1927902）

- 在以前的版本中，当 OpenShift Container Platform Web 控制台中的 Operator Lifecycle Manager（OLM）状态描述符被分配不兼容的数据类型时，会出现错误。添加了验证，消除了不兼容的数据类型处理，从而避免了错误。记录警告也会识别不兼容的状态类型。(BZ#1927941)

- 以下 OpenShift Container Platform Web 控制台视图现在支持多面过滤：

  - **Home → Search** （ **Resources** 选项卡）
  - **Home → Events** （ **Resources** 选项卡）
  - **Workload → Pods**（**Filter** 选项卡）

  如需更多信息，请参阅 BZ#1930007。

- 以下程序错误修复解决了 OpenShift Container Platform Web 控制台的各种转换问题：

  - BZ#1921780

  - BZ#1921781
  - BZ#1922992
  - BZ#1924585
  - BZ#1924747
  - BZ#1925083

- 在以前的版本中，web 控制台依赖于硬编码的频道字符串来填充频道模态下拉菜单。因此，用户可以看到其当前版本可能不正确的频道值。现在，如果 Cluster Version Operator 没有为给定版本提供正确的频道，频道模态下拉列表会变为文本输入字段，并为用户推荐频道和帮助文本。控制台不再依赖于硬编码频道字符串。（BZ#1932281）

- 在以前的版本中，无法正确格式化中文或日语的时间戳。因此，时间戳难以阅读。在这个版本中，在 **Moment.js** 中针对中文和日文使用默认的时间戳格式，以提供更好的用户体验。（BZ#1932453）

- 在以前的版本中，FilterToolbar 组件中的 **rowFilters** prop 不接受 **null** 值。因此，如果 **rowFilters** 未定义，则会出现未被捕获的异常。现在，当 FilterToolbar 组件中引用了 **rowFilters** prop 时，则接受 **null** 值。因此，当 **rowFilters** prop 未定义，FilterToolbar 不再会抛出异常。（BZ#1937018）

- 在以前的版本中，帮助文本的错误样式应用到字段级别的帮助实例。现在，显示了字段级别的帮助文本的正确样式，并在控制台中保持一致。（BZ#1942749）。

- 在以前的版本中，Operator Lifecycle Manamgent（OLM）状态条件描述符在资源详情页面中作为普通详情项呈现。因此，**Conditions** 表呈现为一半宽度。在这个版本中，状况描述符在 **Operand** 详情页的普通 **Conditions** 表下以全宽度表的形式呈现。(BZ#1943238)

- 在以前的版本中，为中文用户翻译了"Ingresses"一词，这不太符合用户的习惯。现在，单词"Ingress"保留为英文。(BZ#1945816)

- 在以前的版本中，为中文用户翻译了"Operators"，这不同符合用户的习惯。现在，单词"Operators"保留为英文。（BZ#1945818）

- 在以前的版本中，一个不正确的代码会导致 **User** 和 **Group** 详情显示不相关的主题。现在，添加了根据 **User** 或 **Group** 的过滤代码，因此 **User** 和 **Group** 详情会显示相关的主题。（BZ#1951212）

- 在以前的版本中，pod Containers 文本没有国际化，因此用户体验较差。现在，pod Containers 文本已被国际化，因此用户体验已被改进。（BZ#1937102）

- 在以前的版本中，**PackageManifest** 列表页项没有链接到详情页面，因此用户无法轻松深入到列表页面中的单个 **PackageManifest** 项目。现在，每个 **PackageManifest** 项目都链接到与其它列表页的惯例匹配的详情页面。用户可从列表页面轻松访问 PackageManifest 详情页面。(BZ#1938321)

- **Jobs** 表的 **Completions** 列按期望（**Desired**）完成的数量而不是成功（**Succeeded**）完成的数量进行排序。数据会显示为 **# Succeeded of # Desired**，因此当对列进行排序时，结果看起来很混乱，因为数据是按第二个数字排序的。现在，**Jobs Completions** 列按照 **# Succeeded** 进行排序。（BZ#1902003）

- **Manage Columns** modal 中的输入标签不是可点击的按钮，因此您无法单击它们来管理列。在这个版本中，标签是用来管理列的可点击按钮。(BZ#1908343)

- 在 Google Cloud Platform 上创建存储类时，CSI 置备程序不会被列出。在这个版本中，这个问题已解决。（BZ#1910500）

- 在以前的版本中，如果用户从 **User Management → Roles**列表视图中点 **Cluster Role**，则详情页面中的后端链接是 **Cluster Roles**，它提供了 **Cluster Role** 的通用列表视图。这会导致向后 Web 控制台导航重定向到不正确的页面。在这个版本中，后端链接会把用户从 **Cluster Role/RoleBinding** 详情页导向 **Role/Bindings** 列表视图。这样，用户可以在 Web 控制台中正确地向后导航。（BZ#1915971）

- 在以前的版本中，创建的日期时间不会以可读格式显示，从而导致难以理解和使用 UTC 中显示的时间。在这个版本中，显示的时间会被重新格式化，以便 UTC 可以被读取和理解。（BZ#1917241）

- 在以前的版本中，Web 控制台中的 pod 请求和限制计算不正确。这是因为没有排除完成的 pod 或 init 容器。在这个版本中，计算中不需要的 pod 会被排除，这可以提高 Pod 请求 web 控制台计算结果的准确性。（BZ#1918785）

- 在以前的版本中，解析未定义值会导致一个"不是一个数字"（NaN）异常，**Chart** 工具提示会显示没有值的方框。在这个版本中，在获取数据时指定一个开始日期，以便 **Chart** 工具提示显示正确的值。此更改可确保同步结果，并且未定义的值不会被解析。（BZ#1906304）

- 在以前的版本中，pod 日志的下载链接被改为带有空 download 属性的标准 HTML 定位符元素。因此，下载文件会丢失默认文件名格式。在这个版本中，在 anchor 元素下载属性中添加了一个文件名，以便在下载 pod 日志时使用默认文件名（格式为 **<pod-name>-<container-name>.log** ）。（BZ#1945630）

- 在以前的版本中，当用户有创建资源的权限但没有编辑资源的权限时，Web 控制台 YAML 编辑器被错误地设置为只读模式。现在，具有创建资源权限的用户可以编辑编辑器中的内容。(BZ#1824911)

- 在以前的版本中，web 控制台在大多数情况下都以 12 小时格式显示时间，其他位置显示 24 小时格式。另外，过去一年之前的日期没有显示年信息。在这个版本中，日期和时间的格式一致，并符合用户的区域设置和语言首选项设置。过去一年之前的日期将显示年信息。(BZ#1862084)

- 在以前的版本中，web 控制台正在为没有权利查看这些事件的用户轮询 **ClusterVersion** 资源。这会输出控制台 pod 日志中的大量错误。为避免这种情况，请在轮询资源前检查用户的权限，从而消除控制台 Pod 日志中的不必要的错误。(BZ#1848151)

- 在以前的版本中，YAML 编辑器的键盘用户无法退出编辑器。编辑器外部的视图快捷方式弹出不可用供用户访问。在这个版本中，用户可以使用 **opt + F1** 键操作在编辑器上显示可访问性帮助。此更改允许 YAML 编辑器的键盘用户使用正确的击键操作退出编辑器。(BZ#1874931)

- 在 OpenShift Container Platform（OCP）4.x 发布后，上传到 OCP 4 Web 控制台的二进制 secret 文件无法加载。这会导致安装失败。在 OpenShift Container Platform 4.8 中，此功能已恢复到 OCP 4 Web 控制台。现在，所需 secret 的输入可以使用二进制文件格式来完成。(BZ#1879638)

- 在以前的版本中，为了解决 BZ#1871996 以正确创建 RoleBinding 会导致在选择命名空间时无法选择绑定类型。因此，拥有活跃命名空间的用户无法在不将活跃命名空间更改为 **All namespace** 的情况下创建集群 RoleBinding。此更新恢复了针对 BZ#1871996 的更改的一部分，以便无论活跃命名空间，用户可以创建集群角色绑定。（BZ#1927882）

Web 控制台 (开发者视角)

- 在以前的版本中，当在 Developer 控制台中将服务集群设置为本地的标签更改时，用户将无法创建 Knative 服务。在这个版本中，Knative 服务使用 **cluster-local** 的最新支持标签，以便用户以 cluster-local 用户身份从 Developer Console 创建 Knative 服务。(BZ#1969951)

- 在以前的版本中，Image Manifest Vulnerabilities (IMV) 的 **Low** 和 **Medium** 严重性问题颜色与（Quay.io）界面中显示的颜色不匹配。因此，当用户将漏洞的严重性更改为 **High** 时，IMV 会错误地将问题排序。这会在检查 IMV 时造成混淆。当前发行版本解决了这个问题。(BZ#1942716)

- 在以前的版本中，如果因为未安装 Samples Operator 而导致 OpenShift 命名空间模板不可用，Developer 视角中的 **Topology** 视图不会加载。在这个版本中解决了这个问题。（BZ#1949810）

- 在以前的版本中，当导入 devfile 时，web 控制台会忽略 **build guidance** 占位符容器，该容器提供环境变量、端口和限值的配置。新部署有第二个容器，无法启动，因为无法获取占位符镜像，并且丢失了所需的配置。现在，**build guidance** 容器已从新部署中丢弃，容器会添加环境变量、端口和限制配置。（BZ#1952214）

- 在以前的版本中，当在另一个标签页中切换到 **Developer** 视角并重新载入项目详情时，绑定到该视角的路由不会被呈现，并导致一个 **404** 错误。在这个版本中，会加载所有不活跃的路由，并切换到正确的视角。（BZ#1929769）

- 在以前的版本中，当因为用户没有命名空间所需的访问权限而发生错误时，**Monitoring** dashboard 页面中的 **Workload** 下拉菜单会持续显示 Load-in-progress 图标。当前发行版本解决了这个问题。现在，**Monitoring** 仪表板页面会显示一个错误消息，指示已发生 **Forbidden** 错误。(BZ#1930546)

- 在以前的版本中，API 服务器可能无法创建资源，当在更新资源配额时有冲突，资源会返回 409 状态代码。因此，资源将无法创建，您可能需要重试 API 请求。在这个版本中，**OpenShift** 控制台 Web 应用会在收到 409 状态代码时尝试重试请求 3 次，这通常足以完成请求。如果 409 状态代码持续发生，控制台中会显示一个错误。（BZ#1920699）

- 在以前的版本中，当选择 **YAML** 选项卡时，**metadata.managedFields** 部分不会立即折叠。这是因为在一些页（如 **Pipeline Builder** 和 **Edit HorizontalPodAutoscaler** (HPA)）中的 **Form** 或 **YAML** 的切换功能中存在一个问题。因此，在您试图输入的文档部分会被折叠。**metadata.managedFields** 部分保持不变，光标则重置为 **YAML** 编辑器左上角的起始位置。当前发行版本解决了这个问题。现在，在载入 **YAML** 时，**metadata.managedFields** 部分会立即折叠。（BZ#1932472）

- 在以前的版本中，在 **Git Import** 流中为私有存储库创建的管道无法运行。这是因为管道 **ServiceAccount** 对象没有将 **Git Import** 流创建的 secret 用于私有 Git 存储库。在这个版本中，您可以在管道 **ServiceAccount** 对象的注解中添加 secret 名称，并在提供的 secret 中添加特定于管道的注解。因此，私有 Git 存储库的管道运行可以成功。（BZ#1970470）

- 在以前的版本中，当用户在 **YAML** 编辑器中插入格式化的 **YAML** 代码段时，新选择与代码片段中的新内容不匹配。缩进已被移除，在选择中可以看到一些随机字母。当前发行版本解决了这个问题。现在，光标保留在它启动的位置，并为光标结束位置添加缺少的缩进。插入 **YAML** 代码段后，新选择与新内容匹配。(BZ#1952545)

- 在以前的版本中，注解被传递给 Knative 服务规格和元数据。因此，**Topology** 中 Knative 服务的相关修订会显示修饰符。此发行版本只将注解传递给 Knative 服务元数据，从而解决了这个问题。现在，只有 **Topology** 中的 Knative 服务会显示修饰符，而不是关联的修订版本。（BZ#1954959）

- 在以前的版本中，如果您创建的管道带有带有空字符串的参数，如 **''**，OpenShift Container Platform Web 控制台中的字段将不会接受空字符串。当前发行版本解决了这个问题。现在，**''** 在 parameters 部分中被支持作为有效的默认属性。（BZ#1951043）

- 在以前的版本中，用户无法从 **Developer** 视角将 Knative 服务创建为私有服务。这个问题现已解决，更新了标签 **'networking.knative.dev/visibility': 'cluster-local'**。(BZ#1970796)

- 在以前的版本中，事件源和类型源的 Kamelets 类型在目录中显示。现在，通过过滤 Kamelets 资源来只列出源类型解决了这个问题。(BZ#1972258)

Windows 容器

- 在以前的版本中，当用户扩展额外的 Windows 节点时，负载均衡器服务会变得不稳定。在这个版本中，负载均衡器服务稳定，允许用户添加多个 Windows 节点，而不会出现错误的性能。（BZ#1905950）
- 在以前的版本中，如果 **kube-proxy** 服务在 Windows Pod 运行后创建，则 kube-proxy 服务会在负载均衡器被创建后意外崩溃。在这个版本中，kube-proxy 服务在重新创建负载均衡器服务时不会崩溃。（BZ#1939968）
- 在以前的版本中，负载均衡器的 Ingress 中的空 IP 地址值会破坏数据路径。因此，Windows 服务无法访问。在这个版本中，即使 IP 地址值为空，也可以访问 Windows 服务。（BZ#1952914）
- 在以前的版本中，当用户创建带有投射卷的 Windows pod 时，pod 会停留在 **ContainerCreating** 阶段。在这个版本中，Windows pod 创建可以成功进入 **Running** 阶段。（BZ#1973580）

1.8. 技术预览功能

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。请参阅红帽门户网站中关于对技术预览功能支持范围的信息：

技术预览功能支持范围

在下表中，功能被标记为以下状态：

- **TP**: *技术预览*
- **GA**: *正式发行*
- **-**: *Not Available*
- **DEP**: *已弃用*

表 1.2. 技术预览

功能	OCP 4.6	OCP 4.7	OCP 4.8
带有普通时钟的精确时间协议(PTP)硬件	TP	TP	GA
oc CLI 插件	TP	TP	GA
Descheduler	TP	GA	GA
OVN-Kubernetes Pod network provider	GA	GA	GA
HPA 用于内存使用	TP	GA	GA
服务绑定	TP	TP	TP
日志转发	GA	GA	GA

功能	OCP 4.6	OCP 4.7	OCP 4.8
用户定义项目的监控	GA	GA	GA
使用 Cinder 的原始块	TP	TP	GA
CSI 卷快照	TP	GA	GA
CSI 卷克隆	GA	GA	GA
CSI 卷扩展	TP	TP	TP
vSphere 问题检测器（vSphere Problem Detector） Operator	-	GA	GA
CSI Azure Disk Driver Operator	-	-	TP
CSI GCP PD Driver Operator	-	TP	GA
CSI OpenStack Cinder Driver Operator	-	GA	GA
CSI AWS EBS Driver Operator	TP	TP	TP
CSI 自动迁移	-	-	TP
Red Hat Virtualization（oVirt）CSI Driver Operator	GA	GA	GA
CSI inline 临时卷	TP	TP	TP
CSI vSphere Driver Operator	-	-	TP
使用 Local Storage Operator 进行自动设备发现和置备	TP	TP	TP
OpenShift Pipelines	TP	GA	GA
OpenShift GitOps	TP	GA	GA
OpenShift 沙盒容器	-	-	TP
Vertical Pod Autoscaler	TP	TP	GA
Cron 作业	TP	TP	GA
PodDisruptionBudget	TP	TP	GA
Operator API	GA	GA	GA

功能	OCP 4.6	OCP 4.7	OCP 4.8
使用 kvc 向节点添加内核模块	TP	TP	TP
Egress router CNI 插件	-	TP	GA
Scheduler 配置集	-	TP	TP
非抢占优先级类	-	TP	TP
Kubernetes NMState Operator	-	TP	TP
支持的安装程序	-	TP	TP
AWS 安全令牌服务（STS）	-	TP	GA
kdump	-	TP	TP
OpenShift Serverless	-	-	GA
无服务器功能	-	-	TP
Jenkins Operator	TP	TP	DEP
CPU Manager	GA	GA	GA
驱动程序工具包	-	-	TP

1.9. 已知问题

- 在 OpenShift Container Platform 4.1 中，匿名用户可以访问发现端点。之后的版本会取消对这端点的访问，以减少可能的安全漏洞攻击面。一些发现端点被转发到聚合的 API 服务器。但是，升级的集群中会保留未经身份验证的访问，因此现有用例不会中断。
  如果您是一个从 OpenShift Container Platform 4.1 升级到 4.8 的集群的集群管理员，您可以撤销或继续允许未经身份验证的访问。建议取消未经身份验证的访问，除非有特殊需要。如果您继续允许未经身份验证的访问，请注意相关的风险。

警告

如果您的应用程序依赖未经身份验证的访问，在撤销了未经身份验证的访问后可能会收到 HTTP **403** 错误。

使用以下脚本撤销对发现端点的未经身份验证的访问：

```
## Snippet to remove unauthenticated group from all the cluster role bindings
$ for clusterrolebinding in cluster-status-binding discovery system:basic-user
system:discovery system:openshift:discovery ;
do
### Find the index of unauthenticated group in list of subjects
index=$(oc get clusterrolebinding ${clusterrolebinding} -o json | jq 'select(.subjects!=null) |
.subjects | map(.name=="system:unauthenticated") | index(true)');
### Remove the element at index from subjects array
oc patch clusterrolebinding ${clusterrolebinding} --type=json --patch "[{'op': 'remove','path':
'/subjects/$index'}]";
done
```

此脚本从以下集群角色绑定中删除未经身份验证的对象：

- **cluster-status-binding**
- **discovery**
- **system:basic-user**
- **system:discovery**
- **system:openshift:discovery**

(BZ#1821771)

- **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)
- 当使用用户置备的基础架构在 vSphere 上打开虚拟机时，扩展节点的过程可能无法正常工作。虚拟机监控程序配置中的一个已知问题会导致在虚拟机监控程序中创建机器，但不会开机。如果在扩展机器集后某个节点可能处于 **Provisioning** 状态，您可以调查 vSphere 实例本身中的虚拟机状态。使用 VMware 命令 **govc tasks** 和 **govc events** 来确定虚拟机的状态。检查类似以下内容的错误消息：

  > Invalid memory setting: memory reservation (sched.mem.min) should be equal to memsize(8192).

  您可以使用 VMware KBase 文章中的步骤解决这个问题。如需更多信息，请参阅红帽知识库解决方案 UPI vSphere 节点扩展无法正常工作。（**BZ#1918383**）
- 当使用 ECKD 类型 DASD 作为 VirtIO 块设备时，在 IBM Z 上安装 RHEL KVM 时安装 RHCOS 会失败。(BZ#1960485)
- 一个 Open Virtual Network（OVN）程序错误会导致 Octavia 负载均衡器的持久性连接问题。创建 Octavia 负载均衡器时，OVN 可能不会将它们插入到一些 Neutron 子网中。对于某些 Neutron 子网，这些负载平衡器可能无法访问。这个问题会在配置 Kuryr 时随机影响针对每个 OpenShift 命名空间创建的 Neutron 子网。因此，当出现这个问题时，从受此问题影响的 OpenShift 命名空间无法访问实施 OpenShift **Service** 对象的负载均衡器。由于这个程序错误，在修复程序错误前，不建议在带有 OVN 和 OVN Octavia 的 Red Hat OpenStack Platform（RHOSP）16.1 上使用 Kuryr SDN 的 OpenShift Container Platform 4.8 部署。(BZ#1937392)
- Console Operator 没有为控制台的路由（**console** 或 **downloads**）正确地更新带有 **componentRoutes** 条件的 **Ingress** 资源。(BZ#1954148)
- OVN-Kubernetes 网络供应商不支持 **NodePort**- 和 **LoadBalancer**-type 服务的

externalTrafficPolicy 功能。**service.spec.externalTrafficPolicy** 字段决定服务的流量是路由到节点本地范围或集群范围的端点。目前，此类流量默认路由到集群范围的端点，因此无法限制到节点本地端点的流量。这将在以后的发行版本中解决。(BZ#1903408)

- 目前，Kubernetes 端口冲突问题可能会导致 pod 到 pod 的通信中断，即使重新部署了 pod。有关详细信息和临时解决方案，请参阅带有 OVN-Kubernetes 的 OpenShift 4 中的 pod 和集群 IP 间的 pod 和集群 IP 端口冲突。（BZ#1939676, BZ#1939045）

- 对于使用 OVN-Kubernetes 网络供应商且计算节点运行 RHEL 7.9 的集群，BZ#1976232 会阻止从 OpenShift Container Platform 4.7 升级到 OpenShift Container Platform 4.8。要升级到 4.8，您必须等待包含这个程序错误修复的 4.8 补丁。（BZ#1976232）

- 对于使用 OVN-Kubernetes 网络供应商并从 OpenShift Container Platform 4.7 升级到 OpenShift Container Platform 4.8 的集群，OVN-Kubernetes 中的错误有时可能会导致 pod IP 地址过时。该错误会在非常罕见的情况下导致争用问题。因此，在升级到 4.8 发行版本的过程中，节点无法排空，一些 Operator 会报告 **Degraded** 状态。作为临时解决方案，请识别一直处于 **CrashLoopBackOff** 状态且没有完成升级的 pod。使用 **oc delete <pod-name>** 命令删除这些 pod。（BZ#1974403）

- **kubeletconfig** 资源的 **tlsSecurityProfile** 字段的描述（例如，使用 **oc explain** 命令时）不会列出 TLS 安全配置集的正确密码。作为临时解决方案，请查看受影响节点的 **/etc/kubernetes/kubelet.conf** 文件中的密码列表。（BZ#1971899）

- 在单个节点上运行 CNF 测试时，以常规模式运行 CNF 测试时，可以了解集群是否就绪缺少详情。特别是，创建 SR-IOV 网络只有在至少一分钟前才会创建网络附加定义。所有 DPDK 测试均在级联中失败。当针对单一节点上的安装（使用 **-ginkgo.skip** 参数）运行时，以常规模式运行 CNF 测试会跳过 DPDK 功能。以 Discovery 模式运行 CNF 测试，对单个节点上的安装执行测试。（BZ#1970409）

- 目前，CNF-tests 不支持通过 MLX NIC 进行 SR-IOV 和 DPDK 测试的安全引导。当针对启用了安全引导的环境以常规模式运行 CNF 测试时，可以使用 **-ginkgo.skip** 参数运行 CNF 测试跳过 SR-IOV 功能。在发现模式下运行是推荐使用 MLX 卡对安全引导环境执行测试的方法。这将在以后的发行版本中解决。(BZ#1975708)

- 当 **ArgoCD** Operator 订阅并启动 ArgoCD 和 AppProject 时，启动名为 **guestbook** 的示例应用程序会失败，因为镜像无法在更严格的 OpenShift Container Platform 环境中工作。作为临时解决方案，用户可通过部署以下示例来确保 **ArgoCD** Operator 正常工作：

```
PROJ=younamespace
cat > $PROJ-app.yaml <<EOF
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: simple-restricted-webserver
  namespace: $PROJ
spec:
  destination:
    namespace: $PROJ
    server: https://kubernetes.default.svc
  project: default
  source:
    path: basic-nginx
    repoURL: 'https://github.com/opdev/argocd-example-restricted-apps.git'
    targetRevision: HEAD
EOF
oc create -f $PROJ-app.yaml
```

如需更多信息，请参阅 BZ#1812212。

- 如果您在多个标签页中打开了控制台，**Developer** 视角中的一些侧栏链接不会直接链接到项目，所选项目中会出现意外更改。这将在以后的发行版本中解决。(BZ#1839101)

- 当使用 **pathType: Prefix** 时，使用 Ingress 创建透传路由会失败。反之，您可以通过将 **pathType** 设置为**ImplementSpecific** 并将 **path** 设置为 **''** 来创建 passthrough 路由：

  Ingress YAML 文件示例

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress7
  namespace: test-ingress
  annotations:
    route.openshift.io/termination: passthrough
spec:
  rules:
  - host: <ingress-psql-example-test-ingress.apps>
    http:
      paths:
      - path: ''
        pathType: ImplementationSpecific
        backend:
          service:
            name: <ingress-psql-example>
            port:
              number: 8080
```

  如需更多信息，请参阅 BZ#1878685。

- 目前，在 **Search** 页面中，在应用或删除 **Name** 过滤器后，**Pipelines** 资源表不会立即更新。但是，如果您刷新页面并展开 **Pipelines** 部分，则会应用 **Name** 过滤器。在删除 **Name** 过滤器时会出现同样的行为。这将在以后的发行版本中解决。（BZ#1901207）。

- 文档现在描述了 **Provisioning** 自定义资源中的 **ProvisioningNetworkCIDR** 值。这会因为 **dnsmasq** 将 IPv6 调配网络限制为 /64。(BZ#1947293)

- 为了协助故障排除，安装程序收集的 boostratp 失败的日志现在包括 control plane 和 bootstrap 主机的 IP 地址和路由。(BZ#1956079)

- 当使用自签名的 Amazon Commercial Cloud Services 集群时，您无法从内部镜像 registry 中拉取（pull）或推送到内部镜像 registry。作为临时解决方案，您必须在 **configs.imageregistry/cluster** 资源中把 **spec.disableRedirects** 设为 **true**。这可让您从镜像 registry 中拉取镜像层，而不是直接从 S3 存储拉取。(BZ#1924568)

- 在以前的版本中，如果 OpenShift Container Platform Web 控制台中使用 Bitbucket 存储库为部署创建的拓扑 URL 无法正常工作，如果它们包含包含斜杠字符的分支名称。这是因为 Bitbucket API BCLOUD-9969 存在问题。当前发行版本可以缓解这个问题。如果分支名称包含斜杠，则拓扑 URL 指向存储库的默认分支页面。此问题将在 OpenShift Container Platform 以后的发行版本中解决。（BZ#1969535）。

- 在 Red Hat Virtualization（RHV）上安装 OpenShift Container Platform（OCP）版本 4.6 需要 RHV 版本 4.4。如果您在 RHV 4.3 上运行较早版本的 OCP，请不要将其更新至 OCP 版本 4.6。红帽还没有测试在 RHV 版本 4.3 上运行 OCP 版本 4.6 且不支持这个组合。如需有关测试的集成

的更多信息，请参阅 OpenShift Container Platform 4.x Tested Integrations（x86_x64） 。

- 当使用 **--build-cmd** 标志运行**operator-sdk pkgman-to-bundle** 命令时会退出并显示错误。如需更多信息，请参阅（BZ#1967369)）。

- 目前，Web 控制台快速启动卡的先决条件以一个段落而不是列表的形式出现。这将在以后的发行版本中解决。(BZ#1905147)

- 在 OpenShift Container Platform 单一节点配置中，使用实时内核(kernel-rt)时 pod 创建时间比使用非实时内核时慢两倍。当使用 kernel-rt 时，较慢的创建时间会影响支持的最大 pod 数量，因为恢复时间会在节点重启后受到影响。作为使用 kernel-rt 时的一个临时解决方案，您可以使用 **rcupdate.rcu_normal_after_boot=0** 内核参数引导来提高受影响的恢复时间，该参数需要实时内核 **kernel-rt-4.18.0-305.16.1.rt7.88.el8_4** 或更高版本。这个已知问题适用于 OpenShift Container Platform 版本 4.8.15 及更新的版本。(BZ#1975356)

- 在 OpenShift Container Platform 单节点重启后，所有 pod 都会重启，这会导致大量负载比正常的 pod 创建时间更长。这是因为 Container Network Interface (CNI) 无法足够快速地处理 **pod add** 事件。这时显示以下错误消息：**timed out waiting for OVS port binding**。OpenShift Container Platform 单一节点实例最终会恢复，但比预期要慢。这个已知问题适用于 OpenShift Container Platform 版本 4.8.15 及更新的版本。(BZ#1986216)

- 在 OpenShift Container Platform 4.8 之前，默认的负载平衡算法是 **leastconn**。在 OpenShift Container Platform 4.8.0 中，对于非透传的路由，默认设置为 **random**。切换到 **random** 与需要使用长时间运行的 websocket 连接的环境不兼容，因为它显著提高了这些环境中的内存消耗。为缓解这种显著内存消耗，在 OpenShift Container Platform 4.8 中默认负载均衡算法被恢复为 **leastconn**。一旦有一个不会产生大量内存用量的解决方案可用后，在以后的 OpenShift Container Platform 发行版本中，默认值将更改为 **random**。
  您可以输入以下命令来检查默认设置：

  ```
  $ oc get deployment -n openshift-ingress router-default -o yaml | grep -A 2
  ROUTER_LOAD_BALANCE_ALGORITHM
        - name: ROUTER_LOAD_BALANCE_ALGORITHM
          value: leastconn
  ```

  random 选项仍然可用。但是，受益于此算法选择的路由必须通过输入以下命令在注解中明确设置该选项：

  ```
  $ oc annotate -n <NAMESPACE> route/<ROUTE-NAME>
  "haproxy.router.openshift.io/balance=random"
  ```

  (BZ#2017708)

- 如果 RHCOS 和 Machine Config Operator(MCO)的镜像在从 OpenShift Container Platform 4.8.z 发行版本升级到更新的 4.8.z 版本时不会改变，则升级会在 control plane 节点完成升级前将标记为完成。因此，如果在升级实际完成前在集群中执行操作，升级可能会失败。作为临时解决方案，请验证在集群上执行额外的操作前，在 control plane 节点上完成更新。您可以使用 **oc get mcp/master** 命令检查每个池可用的 MCO 管理的节点的状态。(BZ#2025396)

- 从 4.7 OpenShift Container Platform 集群升级到 4.8 后，默认禁用 OpenShift Container Platform 节点上的二级网络接口控制器 (NIC) 从内部网络到外部网络 pod 的路由路径。这是因为从 4.8 开始，共享网关是 Open Virtual Network (OVN) 设计的默认网关模式。如果需要该路由路径，则作为升级前或之后的临时解决方案，请在 **openshift-network-operator** 命名空间中创建一个 **gateway-mode-config** 配置映射，将 OVN 网关模式强制设置为 local。
  输入以下命令在 **openshift-network-operator** 命名空间中创建 **gateway-mode-config** ：

```
$ cat localGW.yml
```

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: gateway-mode-config
  namespace: openshift-network-operator
data:
  mode: "local"
immutable: true
```

```
$ oc apply -f localGW.yml
```

```
configmap/gateway-mode-config created
```

有关其他指导信息，请参阅(KCS)和(BZ#2089389）。这个设置将在以后的发行版本中进一步解决。

- 当虚拟功能(VF)已存在时，无法在物理功能(PF)上创建 macvlan。此问题会影响 Intel E810 NIC。(BZ#2120585)

1.10. 异步勘误更新

OpenShift Container Platform 4.8 的安全更新、程序漏洞修正、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 4.8 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。

红帽客户门户网站的用户可以在红帽订阅管理（RHSM）帐户设置中启用勘误通知功能。当勘误通知被启用后，用户会在有与其注册的系统相关的勘误发行时接收到电子邮件通知。

注意

用户的红帽客户门户网站账户需要有注册的系统，以及使用 OpenShift Container Platform 的权限才可以接收到 OpenShift Container Platform 的勘误通知。

本节的内容将会持续更新，以提供以后发行的与 OpenShift Container Platform 4.8 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.8.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。

1.10.1. RHSA-2021:2438 - OpenShift Container Platform 4.8.2 镜像发行版本、程序错误修正和安全更新公告

发布日期：2021 年 7 月 27 日

OpenShift Container Platform release 4.8.2 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHSA-2021:2438 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:2437 公告提供。

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 4.8.2 --pullspecs
```

1.10.2. RHBA-2021:2896 - OpenShift Container Platform 4.8.3 程序错误修复更新

发布日期：2021 年 8 月 2 日

OpenShift Container Platform release 4.8.3 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2896 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:2899 公告提供。

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 4.8.3 --pullspecs
```

1.10.2.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.3. RHSA-2021:2983 - OpenShift Container Platform 4.8.4 安全和程序错误修复更新

发布日期：2021 年 8 月 9 日

OpenShift Container Platform release 4.8.4 现已正式发布。此更新包括的程序错误修正信息包括在 RHSA-2021:2983 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:2984 公告提供。

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 4.8.4 --pullspecs
```

1.10.3.1. 程序错误修复

- 在以前的版本中，BZ#1954309 和 BZ#1960446 在 OpenShift Container Platform 4.8.3 发行注记中被列为修复的错误，但在版本 4.8.3 发行版本中被省略。在这个版本中，**BZ#1960446** 程序错误修复概述被移到 OpenShift Container Platform 4.8.4 发行注记的 "Bug Fix" 部分，**BZ#1954309** 程序错误修复概述会被删除。

- 在以前的版本中，**nmstate-handler** pod 中存在不正确的容限设置，这导致在 **nmstate** Operator 的节点上无法进行网络配置。在这个版本中，处理器 pod 允许在所有节点上允许容限。(BZ#1960446)

- 在以前的版本中，web 控制台对于失败复制的 **ClusterServiceVersion** 对象（CSV）会显示 **The operator is running in openshift-operators but is managing this namespace**。此消息不具体，不会帮助用户对失败的 CSV 进行故障排除。在这个版本中，复制 CSV 的消息将用户定向到原始 CSV 以查找故障原因，并提供到原始 CSV 的链接。(BZ#1972478)

- 在以前的版本中，Operator 会检查 registry 是否应该使用检查的 **spec.nodeSelector** 而不是 **spec.tolerations** 的自定义容限，但只有在设置了 **spec.nodeSelector** 时才会应用 **spec.tolerations** 中的自定义容限。在这个版本中，会检查 **spec.tolerations**，如果设置了 **spec.tolerations**，Operator 将使用自定义容限。(BZ#1973662)

- 在以前的版本中，如果在没有镜像流的情况下创建的部署没有 **image.openshift.io/triggers** 注解，部署控制器会在无限循环中创建副本集。这个版本已经解决了这个问题。(BZ#1981770)

- 在这个版本中，Manila CSI 日志添加到 **must-gather** 负载中。(BZ#1986026)
- 在以前的版本中，当为虚拟机使用自动固定时，属性的名称为 **disabled**、**existing** 或 **adjust**在这个版本中，名称更好地描述了每个策略，**existing** 被移除，因为它在 oVirt 中被阻断。新属性名为 **none** 和 **resize_and_pin**，这与 oVirt 用户界面一致。(BZ#1987182)

1.10.3.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.4. RHBA-2021:3121 - OpenShift Container Platform 4.8.5 程序错误修复更新

发布日期：2021 年 8 月 16 日

OpenShift Container Platform release 4.8.5 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3121 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:3122 公告提供。

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 4.8.5 --pullspecs
```

1.10.4.1. 功能

1.10.4.1.1. 出口 IP 增强

新的增强功能为 OpenShift Container Platform 4.8 Anonymizer 添加了出口（egress）IP 地址支持。如需更多信息，请参阅 BZ#1974877。

1.10.4.2. 程序错误修复

- 在以前的版本中，**oc logs** 无法针对定义了 **JenkinsPipelineStrategy** 的 **BuildConfig** 对象工作。在这个版本中，**oc logs** 可以用于管道构建。(BZ#1974267)
- 在以前的版本中，当持有虚拟 IP (VIP) 的 **Keepalived** 容器被表示为 **SIGTERMed** 时，不会发送 VRRP 主动消息。因此，VIP 会在超时后迁移到另一个节点。在这个版本中，**Keepalived** 容器包含 **SIGTERMed** 表示的 VIP，发送 **VRRP 优先级 0** 广告消息。因此，现在有更快的 VIP 迁移。(BZ#1920670)
- 在以前的版本中，**Knativemeletbinding** 可以用来创建 **action** 和 **sink** Kamelets，但应该只列出 **source** 类型的 Kamelets。在这个版本中，删除了选择 **sink** 和 **action** 类型 Kamelets 的选项。因此，**source** Kamelets 是唯一在事件源目录中显示的类型。(BZ#1972258)

1.10.4.3. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.5. RHBA-2021:3247 - OpenShift Container Platform 4.8.9 安全和程序错误修复更新

发布日期：2021 年 8 月 31 日

OpenShift Container Platform release 4.8.9 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3247 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3248 公告提供。

重要

RHBA-2021:3247 公告中的 SHA-256 镜像摘要信息不正确。正确的信息如下：

要检查发行镜像元数据，请下载 **oc** 工具并运行以下命令：

- 对于 x86_64 架构：

```
$ oc adm release info quay.io/openshift-release-dev/ocp-release:4.8.9-x86_64
```

镜像摘要为
sha256:5fb4b4225498912357294785b96cde6b185eaed20bbf7a4d008c462134a4edfd

- 对于 s390x 架构：

```
$ oc adm release info quay.io/openshift-release-dev/ocp-release:4.8.9-s390x
```

镜像摘要为
sha256:2665dcca917890b3d06c339bb03dac65b84485fef36c90f219f2773393ba291d

- 对于 ppc64le 架构：

```
$ oc adm release info quay.io/openshift-release-dev/ocp-release:4.8.9-ppc64le
```

镜像摘要为
sha256:ded5e8d61915f74d938668cf58cdc9f37eb4172bc24e80c16c7fe1a6f84eff43

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 4.8.9 --pullspecs
```

1.10.5.1. 程序错误修复

- 此版本添加了中文、日语和韩语的其他本地化内容。(BZ#1972987)
- OpenShift Container Platform 4.6 中更改了 OpenShift Container Platform 4.5 的 OVN-Kubernetes 中使用的地址集命名约定，但现有地址集迁移到新的命名约定不会作为升级的一部分进行处理。在版本 4.5 中创建的网络策略带有其入口或出口部分的命名空间选择器标准，它们依赖于这些命名空间中的 pod IP 地址未保持最新状态的旧地址集。这些策略在 4.6 或更高版本的版本中可能无法正常工作，并可能允许或丢弃意外流量。
  在以前的版本中，临时解决方案是删除并重新创建这些策略。在这个版本中，使用旧命名约定的地址集会被删除，且引用旧地址集的策略 ACL 在 OVN-Kubernetes 升级过程中会根据新的命名约定引用地址集。升级后，版本 4.5 中创建的网络策略可以再次正常工作。(BZ#1976241)

1.10.5.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.6. RHBA-2021:3299 - OpenShift Container Platform 4.8.10 程序错误修复更新

发布日期：2021 年 9 月 6 日

OpenShift Container Platform release 4.8.10 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3299 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:3300 公告提供。

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 4.8.10 --pullspecs
```

1.10.6.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.7. RHBA-2021:3429 - OpenShift Container Platform 4.8.11 程序错误修复更新

发布日期：2021 年 9 月 14 日

OpenShift Container Platform release 4.8.11 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3429 公告中。

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 4.8.11 --pullspecs
```

1.10.7.1. 程序错误修复

- 在以前的版本中，**Event Sources** 可以在 **Developer Catalog Group** 中找到。在这个版本中，**Serverless** 添加组已被重命名为 **Eventing**，**Event Sources** 现在可以在 **Eventing** 添加组中找到。(BZ#1999931)

1.10.7.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.8. RHBA-2021:3511 - OpenShift Container Platform 4.8.12 程序错误修复更新

发布日期：2021 年 9 月 21 日

OpenShift Container Platform release 4.8.12 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3511 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:3512 公告提供。

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 4.8.12 --pullspecs
```

1.10.8.1. 功能

1.10.8.1.1. 集群的新最低存储要求

安装 OpenShift Container Platform 集群所需的最小存储从 120 GB 减小到 100 GB。这个版本适用于所有支持的平台。

1.10.8.2. 程序错误修复

- 在以前的版本中，**oc** 工具会发送对一些 registry 来说太大的标头，这会导致这些 registry 拒绝大型镜像请求。此更新对 **oc adm catalog mirror** 命令的标头大小施加一个限制，允许镜像按预期工作。(BZ#1874106)
- 在以前的版本中，集群自动扩展无法访问 **csidrivers.storage.k8s.io** 或 **csistoragecapacities.storage.k8s.io** 资源，这会导致权限错误。在这个版本中，更新了分配给集群自动扩展的角色，使其包含这些资源的权限。(BZ#1995595)

1.10.8.3. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.9. RHBA-2021:3632 - OpenShift Container Platform 4.8.13 程序错误修复和安全更新

发布日期：2021 年 9 月 27 日

OpenShift Container Platform release 4.8.13 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:3632 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3631 公告提供。

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 4.8.13 --pullspecs
```

1.10.9.1. 功能

1.10.9.1.1. 从 Kubernetes 1.21.4 更新

这个版本包含 Kubernetes 1.21.4 的更改。以下 changelogs 提供了更多信息：1.21.4、1.21.3 和 1.21.2。

1.10.9.2. 程序错误修复

- 在以前的版本中，当使用 **--max components** 参数时，片段上有一个未选中的索引操作。因此，**oc** 客户端会返回一个 panic 错误并崩溃。在这个版本中，添加了一个检查，以确保没有为范围以外的索引请求值。因此，在使用 **--max-components** 参数时，**oc** 客户端不再会出现崩溃问题。(BZ#2004193)

1.10.9.3. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.10. RHBA-2021:3682 - OpenShift Container Platform 4.8.14 程序错误修复更新

发布日期：2021 年 10 月 11 日

OpenShift Container Platform release 4.8.14 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3682 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:3865 公告提供。

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 4.8.14 --pullspecs
```

1.10.10.1. 准备升级到下一个 OpenShift Container Platform 版本

OpenShift Container Platform 4.8.14 引进了一个检查，它会影响升级到下一个 OpenShift Container Platform 版本（目前计划是 OpenShift Container Platform 4.9）。这是因为 OpenShift Container Platform 4.9 要使用 Kubernetes 1.22，它移除 了大量已弃用的 **v1beta1** API。

此检查要求管理员在将集群从 OpenShift Container Platform 4.8 升级到 4.9 前提供手动确认。这可以防止，在升级到 OpenShift Container Platform 4.9 后，集群仍然使用已被删除的 API 的问题。管理员需要对删除在集群中使用的每个 API 进行评估，并将这些 API 迁移到相应的新的 API 版本。完成此评估和迁移后，管理员可以进行确认。

所有集群都需要管理员确认，然后才能将其升级到 OpenShift Container Platform 4.9。

如需有关删除的 Kubernetes API 列表的更多信息，请参阅准备升级到 OpenShift Container Platform 4.9。

1.10.10.2. 程序错误修复

- 在以前的版本中，当设置 **provisioningHostIP** 时，即使 provisioning 网络已被禁用，也会将其分配给 Metal3 pod。这不再会发生。(**BZ#1975711**)
- 在以前的版本中，在使用 IPv6 DHCP 时，节点接口地址可能会使用 **/128** 前缀进行租用。因此，OVN-Kubernetes 使用相同的前缀来推断节点的网络，并通过网关将任何其他地址流量（包括流量到其他集群节点）路由到其他地址流量。在这个版本中，OVN-Kubernetes 会检查节点的路由表，并检查节点的接口地址的更广泛的路由条目，并使用该前缀来推断节点的网络。因此，到其他集群节点的流量不再通过网关路由。(**BZ#1994624**)

1.10.10.3. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.11. RHBA-2021:3821 - OpenShift Container Platform 4.8.15 程序错误修复和安全更新

发布日期：2021 年 10 月 19 日

OpenShift Container Platform release 4.8.15 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:3821 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3820 公告提供。

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 4.8.15 --pullspecs
```

1.10.11.1. 已知问题

- 在 OpenShift Container Platform 单一节点配置中，使用实时内核(kernel-rt)时 pod 创建时间比

使用非实时内核时慢两倍。当使用 kernel-rt 时，较慢的创建时间会影响支持的最大 pod 数量，因为恢复时间会在节点重启后受到影响。作为使用 kernel-rt 时的一个临时解决方案，您可以使用 **rcupdate.rcu_normal_after_boot=0** 内核参数引导来提高受影响的恢复时间，该参数需要实时内核 **kernel-rt-4.18.0-305.16.1.rt7.88.el8_4** 或更高版本。这个已知问题适用于 OpenShift Container Platform 版本 4.8.15 及更新的版本。(BZ#1975356)

- 在 OpenShift Container Platform 单节点重启后，所有 pod 都会重启，这会导致大量负载比正常的 pod 创建时间更长。这是因为 Container Network Interface (CNI) 无法足够快速地处理 **pod add** 事件。这时显示以下错误消息：**timed out waiting for OVS port binding**。OpenShift Container Platform 单一节点实例最终会恢复，但比预期要慢。这个已知问题适用于 OpenShift Container Platform 版本 4.8.15 及更新的版本。(BZ#1986216)

1.10.11.2. 程序错误修复

- 在以前的版本中，当 Local Storage Operator 删除孤立持久性卷(PV)时，它会删除 PV，然后在删除下一个卷前等待 10 秒。在需要删除大量 PV 的环境中，10 秒等待周期会导致不必要的延迟，新的持久性卷声明需要很长时间。在这个版本中，删除了 10 秒的等待时间。新的持久性卷声明会及时处理。(BZ#2008088)

- 在以前的版本中，当裸机部署的配置设置包含 **provisioningHostIP** 的值时，即使 **provisioningNetwork** 被禁用，Metal3 pod 也会从没有维护的置备 IP 地址开始。Ironic 在启动时使用此置备 IP 地址，当此地址不再有效时会导致失败。在这个版本中，当 **provisioningNetwork** 被禁用时，系统会忽略 **provisioningHostIP**。Ironic 从正确配置的外部 IP 地址开始。(BZ#1975711)

1.10.11.3. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.12. RHBA-2021:3927 - OpenShift Container Platform 4.8.17 程序错误修复和安全更新

发布日期：2021 年 10 月 27 日

OpenShift Container Platform release 4.8.17 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:3927 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3926 公告提供。

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 4.8.17 --pullspecs
```

1.10.12.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.13. RHBA-2021:4020 - OpenShift Container Platform 4.8.18 程序错误修复更新

发布日期：2021 年 11 月 2 日

OpenShift Container Platform release 4.8.18 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:4020 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:4019 公告提供。

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 4.8.18 --pullspecs
```

1.10.13.1. 程序错误修复

- 构建配置的 **lastTriggeredImageID** 字段弃用后，镜像更改触发器控制器会在启动构建前停止检查 ID 字段。因此，如果创建了构建配置，并在集群运行 OpenShift Container Platform 4.7 或更高版本时启动镜像更改触发器，它会不断尝试触发构建。在这个版本中，这些不必要的尝试触发构建不再会发生。(BZ#2006793)

1.10.13.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.14. RHBA-2021:4109 - OpenShift Container Platform 4.8.19 程序错误修复更新

发布日期：2021 年 11 月 11 日

OpenShift Container Platform release 4.8.19 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:4109 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:4108 公告提供。

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 4.8.19 --pullspecs
```

1.10.14.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.15. RHBA-2021:4574 - OpenShift Container Platform 4.8.20 程序错误修复更新

发布日期：2021 年 11 月 16 日

OpenShift Container Platform release 4.8.20 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:4574 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:4571 公告提供。

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 4.8.20 --pullspecs
```

1.10.15.1. 已知问题

- 当前 opt-in 混淆无法在带有 OVN 的集群中工作，因为 **hostsubnets.network.openshift.io** 目前不在 OVN 集群中。(BZ#2009322)

1.10.15.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.16. RHBA-2021:4716 - OpenShift Container Platform 4.8.21 程序错误修复更新

发布日期：2021 年 11 月 23 日

OpenShift Container Platform release 4.8.21 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:4716 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:4715 公告提供。

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 4.8.21 --pullspecs
```

1.10.16.1. 功能

1.10.16.1.1. 从 Kubernetes 1.21.5 更新

这个版本包含 Kubernetes 1.21.5 的更改。以下 changelog 提供更多信息 : 1.21.5。

1.10.16.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.17. RHBA-2021:4830 - OpenShift Container Platform 4.8.22 程序错误修复和安全更新

发布日期：2021 年 11 月 30 日

OpenShift Container Platform release 4.8.22 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:4830 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:4829 公告提供。

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 4.8.22 --pullspecs
```

1.10.17.1. 功能

1.10.17.1.1. 从 Kubernetes 1.21.6 更新

这个版本包含 Kubernetes 1.21.6 的更改。可以在以下更改日志中找到更多信息： 1.21.6。

1.10.17.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.18. RHBA-2021:4881 - OpenShift Container Platform 4.8.23 程序错误修复更新

发布日期：2021 年 12 月 7 日

OpenShift Container Platform release 4.8.23 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:4881 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:4880 公告提供。

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 4.8.23 --pullspecs
```

1.10.18.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.19. RHBA-2021:4999 - OpenShift Container Platform 4.8.24 程序错误修复和安全更新

发布日期：2021 年 12 月 14 日

OpenShift Container Platform release 4.8.24 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:4999 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:4998 公告提供。

此发行版本包括 CVE-2021-44228、CVE-2021-45046、CVE-2021-4104 和 CVE-2021-4125 的关键安全更新，它们都涉及 Apache Log4j 实用程序。对这些漏洞的修复由 RHSA-2021:5108、RHSA-2021:5148 和 RHSA-2021:5183 公告提供。

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 4.8.24 --pullspecs
```

1.10.19.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.20. RHBA-2021:5209 - OpenShift Container Platform 4.8.25 程序错误修复和安全更新

发布日期：2022 年 1 月 5 日

OpenShift Container Platform release 4.8.25 现已正式发布，其中包括安全更新。此更新包括的程序错误修正列在 RHBA-2021:5209 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:5208 公告提供。

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 4.8.25 --pullspecs
```

1.10.20.1. 程序错误修复

- 在以前的版本中，当配置文件有未知字段或部分时，**ovnkube-node** 和 **ovnkube-master** pod 无法启动。因此，OVN-Kubernetes 不会更新。在这个版本中，如果在配置文件中找到未知字段，OVN-Kubernetes 不再退出。相反，会记录警告。因此，如果配置文件包含未知字段或部分，OVN-Kubernetes 更新不再会失败。(**BZ#2030465**)

- 在以前的版本中，以数字字符开头的 vCenter 主机名无法运行 **openshift-install** 命令。因此，安装程序将其标记为 无效。在这个版本中，添加了数字字符的验证。因此，可以创建带有数字字符的 vCenter 主机。(BZ#2022171)

- 在以前的版本中，Red Hat OpenStack Platform(RHOSP)下载程序容器中的 'curl' 不会识别 **install-config.yaml** 文件的 'noProxy' 值中的网络 CIDR。相反，它只识别用逗号分开的 IP 地址列表。在这个版本中，用户可以在 'noProxy' 值中包含网络 CIDR。(BZ#2005805)

1.10.20.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.21. RHBA-2022:0021 - OpenShift Container Platform 4.8.26 程序错误修复更新

发布日期： 2022 年 1 月 11 日

OpenShift Container Platform release 4.8.26 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:0021 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:0020 公告提供。

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 4.8.26 --pullspecs
```

1.10.21.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.22. RHBA-2022:0113 - OpenShift Container Platform 4.8.27 程序错误修复更新

发布日期： 2022 年 1 月 18 日

OpenShift Container Platform release 4.8.27 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:0113 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:0111 公告提供。

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 4.8.27 --pullspecs
```

1.10.22.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.23. RHBA-2022:0172 - OpenShift Container Platform 4.8.28 程序错误修复更新

发布日期：2022 年 1 月 25 日

OpenShift Container Platform release 4.8.28 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:0172 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:0171 公告提供。

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 4.8.28 --pullspecs
```

1.10.23.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.24. RHBA-2022:0278 - OpenShift Container Platform 4.8.29 程序错误修复更新

发布日期： 2022 年 2 月 1 日

OpenShift Container Platform release 4.8.29 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:0278 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:0277 公告提供。

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 4.8.29 --pullspecs
```

1.10.24.1. 程序错误修复

- 一个更新的 Jenkins 插件（OpenShift Sync 1.0.48）错误地指定了哪些 ConfigMap 和 ImageStream 标签适用于 Jenkins 的 Kubernetes 插件的 Pod 模板。因此，OpenShift Sync 会停止从带有 'jenkins-agent' 标签的配置映射和镜像流导入 pod 模板。在这个版本中，标签规格和 pod 模板会如预期导入。(**BZ#2038960**)

- 在以前的版本中，Local Storage Operator 每 5 秒查找新添加的块设备，这会导致 CPU 的高使用率。这个版本通过将间隔增加到 60 秒来减少 CPU 用量。(**BZ#2006698**)

1.10.24.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.25. RHBA-2022:0484 - OpenShift Container Platform 4.8.31 程序错误修复和安全更新

发布日期： 2022 年 2 月 15 日

OpenShift Container Platform 版本 4.8.31 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2022:0484 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:0483 公告提供。

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 4.8.31 --pullspecs
```

1.10.25.1. 功能

1.10.25.1.1. Whereabouts CNI 插件的 IP 协调

关于 Whereabouts CNI 插件的新增强，添加了 IP 协调作业 **ip-reconciler**，它会作为 Kubernetes cronjob 运行。在以前的版本中，如果 **CNI DEL** 请求没有完成 pod，则 pod 的 IP 地址会保留分配，即使它们没有被使用。现在，这些 IP 地址会定期收集并被重新分配。(**BZ#2028966**)

1.10.25.2. 程序错误修复

- 在以前的版本中，一个竞争条件会导致 OpenStack 云供应商没有置备 OpenStack 凭证。因此，无法使用 Octavia 创建负载均衡服务。在这个版本中，这些凭证会被重复获取。组件可以被成功初始化，并可创建 **LoadBalancer** 类型的服务。(BZ#2039377)
- 在以前的版本中，**standard-csi** 存储类没有包括 **reclaimPolicy** 字段的值。因此，OpenStack Cinder CSI Driver Operator 在日志中持续打印 **StorageClassUpdated** 事件。在这个版本中，为 **reclaimPolicy** 字段提供了一个默认值。Operator 不再在日志中打印过量更新事件。(*BZ#2049088)
- 在此次更新之前，**oc set** 命令的几个子命令的 **--dry-run** 选项无法正确工作。使用 **dry-run=server** 选项的命令会对资源执行更新。在这个版本中修正了 **--dry-run** 选项，以便 **oc set** 子命令按预期工作。(BZ#2038931)
- 在以前的版本中，web 控制台没有读取 **ServiceBinding** 类型资源的 **resource** 属性。因此，拓扑视图没有显示服务绑定连接器。在这个版本中解决了这个问题。Web 控制台读取 **resource** 属性，并正确显示服务绑定连接器。(BZ#2019301)

1.10.25.3. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.26. RHBA-2022:0559 - OpenShift Container Platform 4.8.32 程序错误修复更新

发布日期： 2022 年 2 月 23 日

OpenShift Container Platform release 4.8.32 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:0559 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:0558 公告提供。

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 4.8.32 --pullspecs
```

1.10.26.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.27. RHBA-2022:0651 - OpenShift Container Platform 4.8.33 程序错误修复更新

发布日期： 2022 年 3 月 1 日

OpenShift Container Platform release 4.8.33 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:0651 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:0650 公告提供。

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 4.8.33 --pullspecs
```

1.10.27.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.28. RHBA-2022:0795 - OpenShift Container Platform 4.8.34 程序错误修复更新

发布日期：2022 年 3 月 16 日

OpenShift Container Platform release 4.8.34 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:0795 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:0793 公告提供。

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 4.8.34 --pullspecs
```

1.10.28.1. 功能

1.10.28.1.1. 从 Kubernetes 1.21.8 更新

此更新包含从 Kubernetes 1.21.6 到 1.21.8 的更改。更多信息包括在以下的修改日志中：1.21.7 和 1.21.8。

1.10.28.2. 删除的功能

从 OpenShift Container Platform 4.8.34 开始，在 Microsoft Azure 集群上以 mint 模式使用 Cloud Credential Operator(CCO)的支持已从 OpenShift Container Platform 4.8 中删除。此更改的原因是 Microsoft 的 Azure AD Graph API 将于 2022 年 6 月 30 日停用 ，并被向后移植到 z-stream 更新中所有支持的 OpenShift Container Platform 版本。如需更多信息，请参阅为 Microsoft Azure 删除对 minting 凭证的支持。

1.10.28.3. 已知问题

- 目前，在进行版本更新时，Red Hat Enterprise Linux CoreOS (RHCOS) 和 Machine Config Operator 镜像不会有变化，例如从 OpenShift Container Platform 4.8.20 升级到 4.8.21。因此，当 control plane 节点仍然处于 **updating** 状态时，升级会被标记为 **complete**。当标记为 **upgrading** 时，用户无法执行其他步骤，因为它可能会破坏更新。作为临时解决方案，用户在执行其他步骤前，应该等待 control plane 节点上的更新完成。(**BZ#2025396**)

1.10.28.4. 程序错误修复

- 在以前的版本中，使用 Prometheus QL 的 **SystemMemoryExceedsReservation** 警报会考虑 **hugepages** 内存消耗。因此，警报可能会在集群中不必要地为 OpenShift Container Platform 4.8 触发。在这个版本中，Linux **hugepages** 已从系统内存协调中删除，警报不再会被不必要地触发器。(**BZ#2028854**)

- 在以前的版本中，带有 OVN-Kubernetes 管理的 OpenShift Container Platform 通过 ExternalIP 访问服务。当 4.8.33 升级到 4.8.34 时，无法访问 **ExternalIP**，并带有 "No Route to Host" 问题。在这个版本中，管理员必须将 externalIPs 的流量定向到集群。详情请参阅 (KCS*) 和（**Kubernetes 外部 IP**）(**BZ#2076662**)

1.10.28.5. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.29. RHBA-2022:0872 - OpenShift Container Platform 4.8.35 程序错误修复和安全更新

发布日期：2022 年 3 月 22 日

OpenShift Container Platform release 4.8.35 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2022:0872 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:0871 公告提供。

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 4.8.35 --pullspecs
```

1.10.29.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新至此最新版本，请参阅使用 CLI 在次版本中更新集群以获取相关说明。

1.10.30. RHSA-2022:1154 - OpenShift Container Platform 4.8.36 程序错误修复和安全更新

发布日期：2022 年 4 月 11 日

OpenShift Container Platform 版本 4.8.36 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHSA-2022:1154 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:1153 公告提供。

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 4.8.36 --pullspecs
```

1.10.30.1. 程序错误修复

- 在以前的版本中，Ingress Operator 对 Ingress Canary 路由执行健康检查。当健康检查完成后，Ingress Operator 不会关闭到 **LoadBalancer** 服务的 TCP 连接，因为连接上启用了 **keepalive** 数据包。在执行下一个健康检查时，新的连接已与 **LoadBalancer** 服务建立，而不是使用现有连接。因此，这会导致在 **LoadBalancer** 服务上累积了多个连接。随着时间的推移，这会耗尽 **LoadBalancer** 服务中的连接数量。在这个版本中，连接到 Ingress Canary 路由时会禁用 keepalive。因此，每次运行 canary 探测时都会进行新的连接并关闭。Keepalive 被禁用，不再会积累已建立的连接。(BZ#2066302)

- 在以前的版本中，Cisco ACI 的 neutron 实施中子网的查询（Red Hat OpenStack Platform(RHOSP)-16 中可查询，返回给定网络的意外结果。因此，RHOSP **cluster-api-provider** 可能会尝试在同一子网上置备带有重复端口的实例，这会导致置备失败。在这个版本中，RHOSP **cluster-api-provider** 中添加了一个额外的过滤器，以确保每个子网只有一个端口。因此，现在可以使用 Cisco ACI 在 RHOSP-16 上部署 OpenShift Container Platform。(BZ#2064634)

- 在以前的版本中，**oc debug node** 命令没有在闲置中指定超时。因此，用户永远不会从集群登出。在这个版本中，debug pod 的 **TMOUT** 环境变量被添加到计数器不活跃超时。因此，会话会在 **TMOUT** 不活跃后自动终止。(BZ#2066760)

1.10.30.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.31. RHBA-2022:1369 - OpenShift Container Platform 4.8.37 程序错误修复更新

发布日期： 2022 年 4 月 21 日

OpenShift Container Platform 版本 4.8.37 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:1369 公告中。这个版本没有 RPM 软件包。

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 4.8.37 --pullspecs
```

1.10.31.1. 程序错误修复

- 在以前的版本中，当删除节点时，Local Storage Operator 会发出一个删除持久性卷 (PV) 的请求，在连接到 pod 时使 PV 处于 terminating 状态。在这个版本中，所有者引用会从 PV 中删除，防止在删除节点时进入终止状态。(**BZ#2072573**)

1.10.31.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新至此最新版本，请参阅使用 CLI 在次版本中更新集群以获取相关说明。

1.10.32. RHBA-2022:1427 - OpenShift Container Platform 4.8.39 程序错误修复更新

发布日期： 2022 年 4 月 27 日

OpenShift Container Platform 版本 4.8.39 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:1427 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:1423 公告提供。

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 4.8.39 --pullspecs
```

1.10.32.1. 已知问题

- 目前，无法从 4.8 升级到 4.9。当在相应的发行频道中可用时，会建议 OpenShift Container Platform 用户升级到下一版本。(**BZ#2068601**)

1.10.32.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新至此最新版本，请参阅使用 CLI 在次版本中更新集群以获取相关说明。

1.10.33. RHSA-2022:2272 - OpenShift Container Platform 4.8.41 程序错误修复和安全更新

发布日期： 2022 年 5 月 25 日

OpenShift Container Platform 版本 4.8.41 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHSA-2022:2272 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:2270 公告提供。

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 4.8.41 --pullspecs
```

1.10.33.1. 功能

1.10.33.1.1. Kubernetes 1.21.11 的更新

此更新包含从 Kubernetes 1.21.9 变为 1.21.11 的更改。更多信息包括在以下的修改日志中：1.21.9, 1.21.10, 和 1.21.11。

1.10.33.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.34. RHBA-2022:4737 - OpenShift Container Platform 4.8.42 程序错误修复更新

发布日期： 2022-06-01

OpenShift Container Platform release 4.8.42 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:4737 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:4736 公告提供。

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 4.8.42 --pullspecs
```

1.10.34.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.35. RHBA-2022:4952 - OpenShift Container Platform 4.8.43 程序错误修复和安全更新

发布日期： 2022 年 6 月 16 日

OpenShift Container Platform release 4.8.43 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2022:4952 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:4951 公告提供。

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 4.8.43 --pullspecs
```

1.10.35.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.36. RHBA-2022:5032 - OpenShift Container Platform 4.8.44 程序错误修复更新

发布日期： 2022 年 6 月 22 日

OpenShift Container Platform 版本 4.8.44 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:5032 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:5031 公告提供。

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 4.8.44 --pullspecs
```

1.10.36.1. 程序错误修复

- 在以前的版本中，OpenShift Container Platform 4.8 中自定义平台路由的 API 在 specs 上创建了限制，这个 specs 和 status 不包括自定义主机名和集群域（十进制）。这导致用户无法指定包括十进制值的主机名并安装集群域。在这个版本中，删除了 API 限制，允许用户指定所有主机名并安装所有集群域。(**BZ#2081457**)

1.10.36.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新至此最新版本，请参阅使用 CLI 在次版本中更新集群以获取相关说明。

1.10.37. RHBA-2022:5167 - OpenShift Container Platform 4.8.45 程序错误修复更新

发布日期： 2022 年 6 月 30 日

OpenShift Container Platform release 4.8.45 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:5167 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:5166 公告提供。

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 4.8.45 --pullspecs
```

1.10.37.1. 程序错误修复

- 在以前的版本中，**NetworkManager-wait-online.service** 超时会导致在获取 Ignition 配置文件前无法与 **coreos-installer** 进行连接。在这个版本中，**NetworkManager-wait-online.service** 允许更多时间进行加载，**coreos-installer** 可以获取 Ignition 配置文件。(**BZ#1983773**)

1.10.37.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新至此最新版本，请参阅使用 CLI 在次版本中更新集群以获取相关说明。

1.10.38. RHBA-2022:5424 - OpenShift Container Platform 4.8.46 程序错误修复更新

发布日期： 2022 年 7 月 6 日

OpenShift Container Platform 版本 4.8.46 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:5424 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:5423 公告提供。

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 4.8.46 --pullspecs
```

1.10.38.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.39. RHBA-2022:5889 - OpenShift Container Platform 4.8.47 程序错误修复更新

发布日期： 2022 年 8 月 9 日

OpenShift Container Platform 版本 4.8.46 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:5889 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:5888 公告提供。

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 4.8.47 --pullspecs
```

1.10.39.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.40. RHBA-2022:6099 - OpenShift Container Platform 4.8.48 程序错误修复更新

发布日期： 2022 年 8 月 25 日

OpenShift Container Platform 版本 4.8.48 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:6099 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:6098 公告提供。

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 4.8.48 --pullspecs
```

1.10.40.1. 程序错误修复

- 在以前的版本中，安装程序使用 **install-config.yaml** 的 **platform.baremetal.hosts** 部分中列出的第一个主机作为 control plane 机器，无论它们的角色是什么。在这个版本中，如果存在，则会考虑这个角色。(**BZ#2025901**)

1.10.40.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.41. RHSA-2022:6308 - OpenShift Container Platform 4.8.49 程序错误修复和安全更新

发布日期： 2022 年 9 月 14 日

OpenShift Container Platform release 4.8.49 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHSA-2022:6308 公告中。在这个版本中，没有 RPM 软件包。

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 4.8.49 --pullspecs
```

1.10.41.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.42. RHBA-2022:6511 - OpenShift Container Platform 4.8.50 程序错误修复更新

发布日期： 2022 年 9 月 21 日

OpenShift Container Platform release 4.8.50 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:6511 公告中。在这个版本中，没有 RPM 软件包。

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 4.8.50 --pullspecs
```

1.10.42.1. 程序错误修复

- 在以前的版本中，Operator 必须删除并重新创建 IngressController 来为升级到 4.8 的集群启用 PROXY 协议。在这个版本中，将 IngressController API 状态字段 **spec.endpointPublishingStrategy.hostNetwork.protocol** 或 **spec.endpointPublishingStrategy.nodePort.protocol** 设置为 **PROXY** 可更新升级的集群的字段。(BZ#2084337)

1.10.42.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.43. RHSA-2022:6801 - OpenShift Container Platform 4.8.51 程序错误修复和安全更新

发布日期： 2022-10-13

OpenShift Container Platform release 4.8.51 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHSA-2022:6801 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:6800 公告提供。

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 4.8.51 --pullspecs
```

1.10.43.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.44. RHBA-2022:7034 - OpenShift Container Platform 4.8.52 程序错误修复更新

发布日期： 2022-10-26

OpenShift Container Platform release 4.8.52 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:7034 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:7032 公告提供。

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 4.8.52 --pullspecs
```

1.10.44.1. 程序错误修复

- 在以前的版本中，存活度探测会在一秒后超时，从而导致 kuryr-controller 重启。在这个版本中，增加了默认时间限制，从而导致 kuryr-controller 在较长时间内运行。(**OCPBUGS-216**)

1.10.44.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.45. RHSA-2022:7874 - OpenShift Container Platform 4.8.53 程序错误修复和安全更新

发布日期： 2022 年 11 月 18 日

OpenShift Container Platform release 4.8.53 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHSA-2022:7874 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:7873 公告提供。

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 4.8.53 --pullspecs
```

1.10.45.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.46. RHBA-2022:8619 - OpenShift Container Platform 4.8.54 程序错误修复更新

发布日期： 2022 年 11 月 30 日

OpenShift Container Platform release 4.8.54 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:8619 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:8618 公告提供。

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 4.8.54 --pullspecs
```

1.10.46.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.47. RHBA-2022:8927 - OpenShift Container Platform 4.8.55 程序错误修复更新

发布日期： 2022 年 12 月 16 日

OpenShift Container Platform release 4.8.55 现已正式发布。这个版本没有 s390x 架构。此更新包括的程序错误修正信息包括在 RHBA-2022:8927 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:8926 公告提供。

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 4.8.55 --pullspecs
```

1.10.47.1. Kubernetes 1.21.14 更新

此更新包含从 Kubernetes 1.21.12 变为 1.21.14 的更改。更多信息包括在以下的修改日志中：1.21.12, 1.21.13, 和 1.21.14。

1.10.47.2. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.48. RHBA-2023:0018 - OpenShift Container Platform 4.8.56 程序错误修复和安全更新

发布日期：2023 年 1 月 12 日

OpenShift Container Platform release 4.8.56 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2023:0018 公告中。此更新中包括的 RPM 软件包由 RHSA-2023:0017 公告提供。

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 4.8.56 --pullspecs
```

1.10.48.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.10.49. RHSA-2023:0237 - OpenShift Container Platform 4.8.57 程序错误修复和安全更新

发布日期：2023 年 1 月 25 日

OpenShift Container Platform release 4.8.57 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHSA-2023:0237 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:0236 公告提供。

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 4.8.57 --pullspecs
```

1.10.49.1. 更新

要将现有 OpenShift Container Platform 4.8 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。