OpenShift Container Platform 4.15

发行注记

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

Last Updated: 2024-08-07

OpenShift Container Platform 4.15 发行注记

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

法律通告

摘要

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

目录

第 1 章 OPENSHIFT CONTAINER PLATFORM 4.15 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-2023:7198) 现已正式发布。此发行版本使用 Kubernetes 1.28 和 CRI-O 运行时。OpenShift Container Platform 4.15 的新功能、改变以及已知的问题包括在此文档中。

OpenShift Container Platform 4.15 集群位于 https://console.redhat.com/openshift。使用 OpenShift Container Platform 的 Red Hat OpenShift Cluster Manager 应用程序，您可以将 OpenShift Container Platform 集群部署到内部环境或云环境中。

OpenShift Container Platform 4.15 需要运行在 Red Hat Enterprise Linux (RHEL) 8.8 和 8.9 上，或 Red Hat Enterprise Linux CoreOS (RHCOS) 4.15 上。

您必须将 RHCOS 机器用于 control plane，而 compute 系统可以使用 RHCOS 或 RHEL。

对于 **x86_64** 架构上的 OpenShift Container Platform 4.12，红帽添加了一个 6 个月的延长更新支持 (EUS) 阶段，将总生命周期从 18 个月延长至 24 个月。对于在 64 位 ARM (**aarch64**)、IBM Power®(**ppc64le**) 和 IBM Z®(**s390x**) 架构上运行的 OpenShift Container Platform 4.12，EUS 生命周期将保持 18 个月。

从 OpenShift Container Platform 4.14 开始，在所有支持的构架中，包括 **x86_64**、64 位 ARM (**arch64**)、IBM Power® (**ppc64le**) 和 IBM Z® (**s390x**) 架构的 EUS 阶段，总的生命周期为 24 个月。

从 OpenShift Container Platform 4.14 开始，红帽提供了一个为期 12 个月的额外 EUS 附加组件，它表示为 *Additional EUS Term 2*，将生命周期从 24 个月延长至 36 个月。在 OpenShift Container Platform 的所有架构变体中提供了 Additional EUS Term 2。

有关这个支持的更多信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

版本 4.12 的维护支持于 2024 年 7 月 17 日结束，将进入延长的更新支持阶段。如需更新相关信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

从 4.15 发行版本开始，为了简化对红帽所提供的 Operator 的管理和维护，红帽引入了三个新的生命周期类别：Platform Aligned, Platform Agnostic, 和 Rolling Stream这些生命周期类别为集群管理员提供了额外的简易性和透明度，以更好地了解每个 Operator 的生命周期策略，并以可预测的支持界限来计划对集群进行维护和升级。如需更多信息，请参阅 OpenShift Operator 生命周期。

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

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

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

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

1.3. 新功能及功能增强

此版本对以下方面进行了改进。

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. RHCOS 现在使用 RHEL 9.2

RHCOS 现在在 OpenShift Container Platform 4.15 中使用 Red Hat Enterprise Linux (RHEL) 9.2 软件包。这些软件包可确保 OpenShift Container Platform 实例收到最新的修复、功能、增强功能、硬件支持和驱动程序更新。

1.3.1.2. 支持 iSCSI 设备（技术预览）

RHCOS 现在支持 **iscsi_bft** 驱动程序，可让您直接从使用 iSCSI Boot Firmware Table (iBFT) 的 iSCSI 设备引导（技术预览）。这可让您将 iSCSI 设备作为安装的根磁盘。

如需更多信息，请参阅 RHEL 文档。

1.3.2. 安装和更新

1.3.2.1. 在安装过程中加密 Azure 存储帐户

现在，您可以通过为安装程序提供客户管理的加密密钥来加密 Azure 存储帐户。有关加密 Azure 存储帐户所需的参数的描述，请参阅安装配置参数。

1.3.2.2. RHOSP 集成到 Cluster CAPI Operator （技术预览）

如果启用了 **TechPreviewNoUpgrade** 功能标记，Cluster CAPI Operator 将部署 Cluster API Provider OpenStack 并管理其生命周期。Cluster CAPI Operator 会自动为当前的 OpenShift Container Platform 集群创建 **Cluster** 和 **OpenStackCluster** 资源。

现在，可以配置 Cluster API **Machine** 和 **OpenStackMachine** 资源，类似于配置 Machine API 资源的方式。务必要注意，虽然 Cluster API 资源的功能等同于 Machine API 资源，但其结构上并不相同。

1.3.2.3. IBM Cloud 和用户管理的加密

现在，您可以在安装过程中为 IBM Cloud® root 密钥指定您自己的 IBM® 密钥保护。此 root 密钥用于加密 control plane 和计算机器的根（引导）卷，以及在部署集群后置备的持久性卷（数据卷）。

如需更多信息，请参阅 IBM Cloud 的用户管理加密。

1.3.2.4. 在具有有限互联网访问的 IBM Cloud 上安装集群

现在，您可以在具有有限互联网访问的环境（如断开连接的或受限网络集群）中的 IBM Cloud® 上安装集群。使用这种类型的安装，您可以创建一个 registry 来镜像 OpenShift Container Platform 安装镜像的内容。您可以在镜像主机上创建此 registry，该主机可同时访问互联网和受限网络。

如需更多信息，请参阅在受限网络中在 IBM Cloud 上安装集群。

1.3.2.5. 在 AWS 上安装集群以将节点扩展到 Wavelength 区域

您可以通过在 **install-config.yaml** 文件的边缘计算池中设置区名称，在 Amazon Web Services (AWS) Wavelength Zone 中快速安装 OpenShift Container Platform 集群，或在一个带有 Wavelength Zone 子网的现有的 VPC 中安装集群。

您还可以执行安装后任务，将 AWS 上的现有 OpenShift Container Platform 集群扩展为使用 AWS Wavelength Zone。

如需更多信息，请参阅在 AWS Wavelength Zones 中有计算节点在 AWS 上安装集群，和将现有集群扩展为使用 AWS Local Zones 或 Wavelength Zone。

1.3.2.6. 在 AWS 部署中自定义集群网络 MTU

在 AWS Local Zones 基础架构上部署集群前，您可以自定义集群网络的集群网络最大传输单元 (MTU) 来满足基础架构的需求。

您可以通过在 **install-config.yaml** 配置文件中指定 networking.clusterNetworkMTU 参数来自定义集群的 MTU。

如需更多信息，请参阅自定义集群网络 MTU。

1.3.2.7. 在带有 AWS Outposts 中的计算节点的 AWS 上安装集群

在 OpenShift Container Platform 版本 4.14 中，您可以安装带有在 AWS Outposts 中运行的计算节点的 AWS 中安装集群（技术预览）。在 OpenShift Container Platform 4.15 中，您可以在 AWS 上将集群安装到现有的 VPC 中，并在 AWS Outposts 上置备计算节点作为安装后配置任务。

如需更多信息，请参阅在 AWS 上将集群安装到现有的 VPC 中，和将 AWS VPC 集群扩展到 AWS Outpost。

1.3.2.8. Nutanix 和容错部署

默认情况下，安装程序会将 control plane 和计算机器安装到单个 Nutanix Prism Element (集群) 中。要改进 OpenShift Container Platform 集群的容错功能，您现在可以通过配置故障域来指定这些机器分布在多个 Nutanix 集群中。

如需更多信息，请参阅使用多个 Prism Elements 的容错部署。

1.3.2.9. 64 位 ARM 上的 OpenShift Container Platform

OpenShift Container Platform 4.15 现在支持使用 Machine Config Operator (MCO) 在 RHCOS 内核中启用 64k 页大小。此设置专用于具有 64 位 ARM 架构的机器。如需更多信息，请参阅 机器配置任务 文档。

1.3.2.10. 可选的 OLM 集群功能

在 OpenShift Container Platform 4.15 中，您可以在安装过程中禁用 Operator Lifecycle Manager (OLM) 功能。如需更多信息，请参阅 Operator Lifecycle Manager 功能。

1.3.2.11. 在本地磁盘中使用根卷和 etcd 部署 Red Hat OpenStack Platform (RHOSP) （技术预览）

现在，您可以将 etcd 从根卷(Cinder)移到专用临时本地磁盘，作为第 2 天部署。使用这个技术预览功能，您可以解决并防止 RHOSP 安装的性能问题。

如需更多信息，请参阅在本地磁盘上使用 rootVolume 和 etcd 在 OpenStack 上部署。

1.3.2.12. 配置 vSphere 与基于代理的安装程序集成

现在，您可以在为基于 Agent 的安装创建 **install-config.yaml** 文件时将集群配置为使用 vSphere。如需更多信息，请参阅其他 VMware vSphere 配置参数。

1.3.2.13. 基于代理的安装过程中的其他裸机配置

现在，您可以在为基于代理的安装创建 **install-config.yaml** 文件时为裸机平台提供额外的配置。这些新选项包括主机配置、网络配置和基板管理控制器 (BMC) 详情。

这些字段不会在集群初始置备过程中使用，但可以节省在安装后设置字段的过程。如需更多信息，请参阅基于代理的安装程序的其他裸机配置参数。

1.3.2.14. 使用 Dell iDRAC BMC 在安装程序置备的安装过程中配置 RAID

现在，您可以使用带有 Redfish 协议的 Dell iDRAC 基板管理控制器(BMC)在安装程序置备的安装过程中为裸机平台配置独立磁盘的冗余阵列(RAID)。如需更多信息，请参阅 可选：配置 RAID。

1.3.3. 安装后配置

1.3.3.1. 带有多架构计算机器的 OpenShift Container Platform 集群

在带有多架构计算机器的 OpenShift Container Platform 4.15 集群中，您现在可以在集群中的 64 位 ARM 计算机器中启用 64k 页大小。有关设置此参数的更多信息，请参阅在 Red Hat Enterprise Linux CoreOS (RHCOS) 内核中启用 64k 页。

1.3.4. Web 控制台

1.3.4.1. Administrator perspective （管理员视角）

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

- 启用和禁用查看 pod 日志查看器的尾部的过程，以最大程度缩短加载时间。
- 在 **Deployment** 页面中查看 **VerticalPodAutoscaler** 的推荐值。

1.3.4.1.1. 节点正常运行时间信息

在这个版本中，您可以启用查看额外的节点正常运行时间信息，以跟踪节点重启或失败。进入到 **Compute → Nodes** 页面，点 **Manage column**，然后选择 **Uptime**。

1.3.4.1.2. 动态插件增强

在这个版本中，您可以使用 **console.resource/details-item** 将新详情项添加到 **Details** 页面中的默认资源摘要中。OpenShift Container Platform 发行版本还为 CronTab 动态插件添加了注解、标签和删除模态的示例实现。

如需更多信息，请参阅动态插件参考

如需有关 **console.resource/details-item** 的更多信息，请参阅 OpenShift Container Platform 控制台 API。

1.3.4.1.3. OperatorHub 支持 Microsoft Entra Workload ID

在这个版本中，OperatorHub 会检测在 Azure 上运行的 OpenShift Container Platform 集群是为 Microsoft Entra Workload ID 配置的。当检测到时，在安装 Operator 前，会显示一个 "Cluster in Workload Identity / Federated Identity Mode" 通知，然后再安装 Operator 以确保它正确运行。**Operator 安装**页面也会被修改，以添加所需 Azure 凭证信息的字段。

有关**安装 Operator** 页面的更新步骤，请参阅使用 Web 控制台从 OperatorHub 安装。

1.3.4.2. Developer Perspective (开发者视角)

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

- 仪表板中提供了基于 Tekton Results 的数据的管道历史记录和日志，而无需在集群中的 PipelineRun CR。

1.3.4.2.1. 软件供应链增强

web 控制台的 **Developer** 或 **Administrator** 视角中的 **PipelineRun Details** 页面提供了项目中 PipelineRuns 的可视化表示。

如需更多信息，请参阅 Red Hat OpenShift Pipelines。

1.3.4.2.2. Web 控制台中的 Red Hat Developer Hub

在这个版本中，可以使用一个快速启动来了解如何安装和使用开发人员 hub。

如需更多信息，请参阅 Red Hat Developer Hub 的产品文档 。

1.3.4.2.3. Web 控制台支持 OpenShift Container Platform 的构建

在这个版本中，Web 控制台支持 OpenShift Container Platform 1.0 的构建。构建是一个可扩展的构建框架，它基于 Shipwright 项目。您可以使用 OpenShift Container Platform 的构建在 OpenShift Container Platform 集群上构建容器镜像。

如需更多信息，请参阅 OpenShift Container Platform 的构建。

1.3.5. IBM Z 和 IBM LinuxONE

在这个版本中，IBM Z® 和 IBM® LinuxONE 与 OpenShift Container Platform 4.15 兼容。您可以使用 z/VM、LPAR 或 Red Hat Enterprise Linux (RHEL) 基于内核的虚拟机 (KVM) 执行安装。有关安装说明，请参阅以下文档：

- 在 IBM Z 和 IBM LinuxONE 中安装集群

重要

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

IBM Z 和 IBM LinuxONE 主要改进
OpenShift Container Platform 4.15 上的 IBM Z® 和 IBM® LinuxONE 发行版本为 OpenShift Container Platform 组件和概念提供了改进和新功能。

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

- 基于代理的安装程序
- cert-manager Operator for Red Hat OpenShift
- 使用 **x86_64** 多架构计算节点的 **s390x** control plane

在 IBM Z 和 IBM LinuxONE 的 LPAR 上安装集群
OpenShift Container Platform 现在支持在 IBM Z 和 IBM LinuxONE 上的逻辑分区 (LPAR) 中的用户置备的 OpenShift Container Platform 4.15 安装。

有关安装说明，请参阅以下文档：

- 在 IBM Z® 和 IBM® LinuxONE 上的 LPAR 上安装集群
- 在受限网络中的 IBM Z® 和 IBM® LinuxONE 上的 LPAR 上安装集群

1.3.6. IBM Power

IBM Power® 现在与 OpenShift Container Platform 4.15 兼容。有关安装说明，请参阅以下文档：

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

重要

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

IBM Power 主要改进
OpenShift Container Platform 4.15 上的 IBM Power® 发行版本为 OpenShift Container Platform 组件增加了改进和新功能。

此发行版本引进了对 IBM Power® 的以下功能的支持：

- 基于代理的安装程序
- cert-manager Operator for Red Hat OpenShift
- IBM Power® Virtual Server Block CSI Driver Operator
- IBM Power® Virtual Server 的安装程序置备的基础架构支持
- 支持 Intel 和 IBM Power® worker 的多架构 IBM Power® control plane
- NX-gzip for Power10 （硬件加速）
- **openshift-install** 工具支持 IBM Power® 上的各种 SMT 级别 (Hardware Acceleration)

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

表 1.1. OpenShift Container Platform 功能

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
备用身份验证供应商	支持	支持
基于代理的安装程序	支持	支持
支持的安装程序	支持	支持
使用 Local Storage Operator 自动设备发现	不支持	支持
使用机器健康检查功能自动修复损坏的机器	不支持	不支持
IBM Cloud® 的云控制器管理器。	支持	不支持
在节点上控制过量使用和管理容器密度	不支持	不支持
Cron 作业	支持	支持
Descheduler	支持	支持
Egress IP	支持	支持
加密数据存储在 etcd 中	支持	支持
FIPS 加密	支持	支持
Helm	支持	支持
Pod 横向自动扩展	支持	支持
托管 control plane（技术预览）	支持	支持
IBM 安全执行	不支持	支持
IBM Power® Virtual Server Block CSI Driver Operator	支持	不支持
IBM Power® Virtual Server 的安装程序置备的基础架构支持	支持	不支持
在单一节点上安装	支持	支持
IPv6	支持	支持
用户定义项目的监控	支持	支持
多架构计算节点	支持	支持

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
多路径（Multipathing）	支持	支持
网络绑定磁盘加密 - 外部 Tang 服务器	支持	支持
Non-volatile memory express drive (NVMe)	支持	不支持
oc-mirror 插件	支持	支持
OpenShift CLI (**oc**) 插件	支持	支持
Operator API	支持	支持
OpenShift Virtualization	不支持	不支持
OVN-Kubernetes，包括 IPsec 加密	支持	支持
PodDisruptionBudget	支持	支持
精度时间协议 (PTP) 硬件	不支持	不支持
Red Hat OpenShift Local	不支持	不支持
Scheduler 配置集	支持	支持
流控制传输协议 (SCTP)	支持	支持
支持多个网络接口	支持	支持
三节点集群支持	支持	支持
拓扑管理器	支持	不支持
SCSI 磁盘中的 z/VM 模拟 FBA 设备	不支持	支持
4K FCP 块设备	支持	支持

表 1.2. 持久性存储选项

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
使用 iSCSI 的持久性存储	支持 [1]	支持 [1],[2]

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

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

表 1.3. Operator

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
cert-manager Operator for Red Hat OpenShift	支持	支持
Cluster Logging Operator	支持	支持
Cluster Resource Override Operator	支持	支持
Compliance Operator	支持	支持
Cost Management Metrics Operator	支持	支持
File Integrity Operator	支持	支持
HyperShift Operator	技术预览	技术预览
Local Storage Operator	支持	支持
MetalLB Operator	支持	支持
Network Observability Operator	支持	支持
NFD Operator	支持	支持
NMState Operator	支持	支持

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

表 1.4. Multus CNI 插件

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

表 1.5. CSI 卷

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

1.3.7. 认证和授权

1.3.7.1. 基于 OLM 的 Operator 支持 Microsoft Entra Workload ID

在这个版本中，Azure 集群上的 Operator Lifecycle Manager (OLM) 管理的一些 Operator 可以在带有 Microsoft Entra Workload ID 的手动模式中使用 Cloud Credential Operator (CCO)。这些 Operator 使用在集群外管理的短期凭证进行身份验证。

如需更多信息，请参阅使用 Azure AD Workload Identity 的 OLM 管理的 Operator 的基于 CCO 的工作流。

1.3.8. 网络

1.3.8.1. 对外部流量的 IPsec 加密的 OVN-Kubernetes 网络插件支持为正式发布 (GA)

OpenShift Container Platform 现在支持加密外部流量，也称为 *南北流量*。IPsec 已支持加密 pod 间的网络流量，称为 *东西流量*。您可以将这两个功能一起使用，为 OpenShift Container Platform 集群提供完整的转换加密。

在以下平台上支持此功能：

- 裸机
- Google Cloud Platform (GCP)
- Red Hat OpenStack Platform(RHOSP)
- VMware vSphere

如需更多信息，请参阅为外部 IPsec 端点启用 IPsec 加密 。

1.3.8.2. IPv6 unsolicited neighbor 公告现在默认在 macvlan CNI 插件中

在以前的版本中，如果删除了一个 pod (**Pod X**)，并使用类似的配置创建了第二个 pod (**Pod Y**)，则 **Pod Y** 可能与 **Pod X** 具有相同的 IPv6 地址，但它有一个不同的 MAC 地址。在这种情况下，路由器不知道 MAC 地址更改，它会继续将流量发送到 **Pod X** 的 MAC 地址。

在这个版本中，使用 macvlan CNI 插件创建的 pod，其中 IP 地址管理 CNI 插件被分配了 IP，现在默认将 IPv6 非邀请的（unsolicited）邻居公告发送到网络。此功能增强会通知特定 IP 的新 pod MAC 地址的网络结构来刷新 IPv6 邻居缓存。

1.3.8.3. 配置 Whereabouts IP 协调器调度

Whereabouts 协调调度被硬编码为每天运行一次，且无法重新配置。在这个版本中，**ConfigMap** 对象启用了 Whereabouts cron 调度的配置。如需更多信息，请参阅配置 Whereabouts IP 协调器调度 。

1.3.8.4. EgressFirewall 和 AdminPolicyBasedExternalRoute CR 的状态管理更新

对 **EgressFirewall** 和 **AdminPolicyBasedExternalRoute** 自定义资源策略的状态管理进行了以下更新：

- 如果至少有一个消息报告**失败**，则 **status.status** 字段被设置为 **failure**。
- 如果没有报告失败，并且不是所有节点都报告其状态，则 **status.status** 字段为空。
- 如果所有节点都报告**成功**，则 **status.status** 字段被设为 **success**。
- **status.mesages** 字段列出消息。默认情况下，消息按节点名称列出，并以节点名称作为前缀。

1.3.8.5. MetalLB 的额外 BGP 指标

在这个版本中，MetalLB 会公开与 MetalLB 和 Border Gateway Protocol (BGP) 间通信相关的其他指标。如需更多信息，请参阅 BGP 和 BFD 的 MetalLB 指标 。

1.3.8.6. 支持 all-multicast 模式

OpenShift Container Platform 现在支持使用 tuning CNI 插件配置 all-multicast 模式。在这个版本中，不再需要为 pod 的安全性上下文约束 (SCC) 授予 **NET_ADMIN** 功能，从而最大程度降低 pod 的潜在漏洞来提高安全性。

有关 all-multicast 模式的更多信息，请参阅关于 all-multicast 模式。

1.3.8.7. IPv6 网络的多网络策略支持

在这个版本中，您可以为 IPv6 网络创建多网络策略。如需更多信息，请参阅 IPv6 网络中支持多网络策略。

1.3.8.8. 可用的 Ingress Operator 指标仪表板

在这个版本中，Ingress 网络指标可从 OpenShift Container Platform Web 控制台查看。如需更多信息，请参阅 Ingress Operator 仪表板。

1.3.8.9. 对子域的 ExternalName 服务查询的 CoreDNS 编配

从 OpenShift Container Platform 4.15 开始，CoreDNS 从 1.10.1 更新至 1.11.1。

在这个版本中，CoreDNS 会错误地为 **ExternalName** 服务提供响应，该服务使用顶级域（如 **com** 或 **org**）共享它的名称。对外部服务的子域的查询不应解析到那个外部服务。如需更多信息，请参阅相关的 CoreDNS GitHub 问题。

1.3.8.10. CoreDNS 指标弃用和删除

从 OpenShift Container Platform 4.15 开始，CoreDNS 从 1.10.1 更新至 1.11.1。

在这个版本中，CoreDNS 会导致弃用和删除已重新定位的某些指标，包括指标 **coredns_forward_healthcheck_failures_total**, **coredns_forward_requests_total**, **coredns_forward_responses_total**, 和 **coredns_forward_request_duration_seconds**如需更多信息，请参阅 CoreDNS 指标。

1.3.8.11. SR-IOV 支持的硬件（单根 I/O 虚拟化）

OpenShift Container Platform 4.15 添加了对以下 SR-IOV 设备的支持：

- Mellanox MT2910 系列 [ConnectX-7]

如需更多信息，请参阅支持的设备。

1.3.8.12. SR-IOV 网络 VF 的主机网络配置策略（技术预览）

在这个版本中，您可以使用 **NodeNetworkConfigurationPolicy** 资源来管理现有集群中单根 I/O 虚拟化 (SR-IOV) 网络虚拟功能 (VF) 的主机网络设置。

例如，您可以配置主机网络服务质量(QoS)策略，以通过附加的 SR-IOV 网络 VF 管理主机资源的网络访问。如需更多信息，请参阅虚拟功能的节点网络配置策略。

1.3.9. 容器镜像仓库（Registry）

1.3.9.1. 支持 Azure 上的私有存储端点

在这个版本中，可以利用 Image Registry Operator 来使用 Azure 上的私有存储端点。当 OpenShift Container Platform 部署到私有 Azure 集群上时，您可以使用此功能为存储帐户无缝配置私有端点，以便用户可以在不公开面向公共的存储端点的情况下部署镜像 registry。

如需更多信息，请参阅以下部分：

- 在 Azure 上配置私有存储端点

- 可选：为私有镜像 registry 准备私有 Microsoft Azure 集群

1.3.10. Storage

1.3.10.1. 从以前的 LVM 存储安装中恢复卷组

在这个版本中，**LVMCluster** 自定义资源 (CR) 支持从以前的 LVM Storage 安装中恢复卷组。如果 **deviceClasses.name** 字段被设置为之前 LVM 存储安装中的卷组名称，LVM 存储会在当前 LVM 存储安装中重新创建与该卷组相关的资源。这简化了通过重新安装 LVM 存储安装使用之前 LVM 存储安装中的设备的过程。

如需更多信息，请参阅在 worker 节点上创建逻辑卷管理器集群。

1.3.10.2. 支持在 LVM 存储中擦除设备

此功能在 **LVMCluster** 自定义资源 (CR) 中提供了一个新的可选字段 **forceWipeDevicesAndDestroyAllData** 来强制擦除所选设备。在此版本之前，擦除设备需要您手动访问主机。在这个版本中，您可以强制擦除磁盘，而无需人工干预。这简化了擦除磁盘的过程。

警告

如果将 **forceWipeDevicesAndDestroyAllData** 设置为 **true**，则 LVM 存储会擦除该设备上所有之前的数据。您必须谨慎使用此功能。

如需更多信息，请参阅在 worker 节点上创建逻辑卷管理器集群。

1.3.10.3. 支持在多节点集群中部署 LVM 存储

此功能支持在多节点集群中部署 LVM 存储。在以前的版本中，LVM 存储只支持单节点配置。在这个版本中，LVM 存储支持所有 OpenShift Container Platform 部署拓扑。这可在多节点集群中置备本地存储。

警告

LVM 存储只支持多节点集群中的节点本地存储。它不支持跨节点的存储数据复制机制。在多节点集群中使用 LVM 存储时，您必须确保通过主动或被动复制机制进行存储数据，以避免出现单点故障。

如需更多信息，请参阅部署 LVM 存储。

1.3.10.4. 将 RAID 阵列与 LVM 存储集成

此功能支持将 **mdadm** 工具与 LVM 存储创建的 RAID 阵列集成。 **LVMCluster** 自定义资源 (CR) 支持在 **deviceSelector.paths** 字段和 **deviceSelector.optionalPaths** 字段中向 RAID 阵列添加路径。

如需更多信息，请参阅将软件 RAID 阵列与 LVM 存储集成。

1.3.10.5. LVM 存储的 FIPS 合规性支持

在这个版本中，LVM 存储是为联邦信息处理标准 (FIPS) 而设计的。当在 FIPS 模式的 OpenShift Container Platform 上安装 LVM Storage 时，LVM Storage 使用 RHEL 加密库，该库只在 x86_64 架构上提交给 NIST 140-3 验证。

1.3.10.6. Retroactive 默认 StorageClass 分配已正式发布

在 OpenShift Container Platform 4.13 之前，如果没有默认存储类，则创建请求默认存储类的持久性卷声明 (PVC) 会无限期地处于 pending 状态，除非您手动删除并重新创建它们。从 OpenShift Container Platform 4.14 开始，作为技术预览功能，默认存储类会被分配给这些 PVC，以便它们不会处于待处理状态。创建默认存储类或声明了现有存储类之一后，这些部分 PVC 会被分配给默认存储类。这个功能现已正式发布。

如需更多信息，请参阅 Absent 默认存储类。

1.3.10.7. 有助于删除本地卷上的现有数据的 Local Storage Operator 选项已正式发布

此功能提供了一个可选字段 **forceWipeDevicesAndDestroyAllData** 定义是否调用 **wipefs**，它会删除分区表签名 (magic string) 使磁盘可用于 Local Storage Operator (LSO) 置备。除了签名外，没有其它数据会被清除。这个功能现已正式发布。请注意，这个功能不适用于 **LocalVolumeSet** (LVS)。

如需更多信息，请参阅使用 Local Storage Operator 置备本地卷。

1.3.10.8. 在非正常节点关闭后分离 CSI 卷已正式发布

从 OpenShift Container Platform 4.13 开始，当节点关闭为技术预览功能时，Container Storage Interface (CSI) 驱动程序可以自动分离卷。当出现非正常节点关闭时，您可以手动在节点上添加服务外污点，以允许卷从节点自动分离。这个功能现已正式发布。

如需更多信息，请参阅非正常节点关闭后分离 CSI 卷。

1.3.10.9. GCP Filestore CSI Driver Operator 支持共享 VPC。

现在，支持 Google Compute Platform (GCP) Container Storage Interface (CSI) Driver Operator 的共享虚拟私有云 (VPC)。共享 VPC 简化了网络管理，允许一致的网络策略，并提供网络资源的集中视图。

如需更多信息，请参阅为 GCP Filestore 存储创建存储类。

1.3.10.10. 用户管理的加密支持 IBM VPC Block 存储 (GA)

用户管理的加密功能允许您在安装过程中提供加密 OpenShift Container Platform 节点根卷的密钥，并允许所有受管存储类使用指定的加密密钥加密置备的存储卷。此功能在 Google Cloud Platform (GCP)持久磁盘(PD)存储、Microsoft Azure Disk 和 Amazon Web Services (AWS) Elastic Block 存储(EBS)的 OpenShift Container Platform 4.13 中引入，现在在 IBM Virtual Private Cloud (VPC) Block 存储上被支持。

1.3.10.11. 使用挂载选项进行 SELinux 重新标记（技术预览）

在以前的版本中，当启用 SELinux 时，当将 PV 附加到 pod 时，持久性卷 (PV) 文件会被重新标记，这可能会导致 PV 包含很多文件时造成超时，以及加载存储后端。

在 OpenShift Container Platform 4.15 中，对于支持此功能的 Container Storage Interface (CSI) 驱动程序，该驱动程序将使用正确的 SELinux 标签直接挂载卷，无需递归重新标记卷，pod 启动可能会非常快。

此功能支持技术预览状态。

如果以下条件为 true，则这个功能会被默认启用：

- 在 CSIDriver 实例中，通过 **seLinuxMountSupported: true** 提供支持这个功能的 CSI 驱动程序。作为 OpenShift Container Platform 的一部分提供的以下 CSI 驱动程序宣布了 SELinux 挂载支持：
  - AWS Elastic Block Storage(EBS)
  - Azure Disk
  - Google Compute Platform (GCP) 持久磁盘 (PD)
  - IBM Virtual Private Cloud (VPC) Block
  - OpenStack Cinder
  - VMware vSphere
- 使用持久性卷的 pod 使用 **restricted** SCC 在 **spec.securityContext** 或 **spec.containers[*].securityContext** 中指定完整的 SELinux 标签。
- 卷访问模式设置为 **ReadWriteOncePod**。

1.3.11. Oracle® Cloud Infrastructure

1.3.11.1. 使用辅助安装程序在 OCI 上安装集群

您可以在支持专用、混合、公共和多个云环境的 Oracle® 云基础架构 (OCI) 基础架构上运行集群工作负载。红帽和 Oracle 都测试、验证和支持在 OCI 上的 OpenShift Container Platform 集群中运行 OCI。

OCI 提供可满足您的法规合规性、性能和成本效益的服务。您可以访问 OCI 资源管理器配置来置备和配置 OCI 资源。

如需更多信息，请参阅使用 Assisted Installer 在 OCI 上安装集群 。

1.3.11.2. 使用基于代理的安装程序在 OCI 上安装集群

您可以使用基于代理的安装程序在 Oracle® Cloud Infrastructure (OCI) 上安装集群，以便在支持专用、混合、公共和多个云环境的基础架构上运行集群工作负载。

基于代理的安装程序提供了辅助安装服务的易用性，但可以在连接或断开连接的环境中安装集群。

OCI 提供可满足您的法规合规性、性能和符合成本效益的服务。OCI 支持 64 位 **x86** 实例和 64 位 ARM 实例。

如需更多信息，请参阅使用基于代理的安装程序在 OCI 上安装集群。

1.3.12. Operator 生命周期

1.3.12.1. Operator Lifecycle Manager (OLM) 1.0 （技术预览）

自 OpenShift Container Platform 4 初始发行以来，Operator Lifecycle Manager (OLM) 已包含在 OpenShift Container Platform 4 中。OpenShift Container Platform 4.14 引入了用于 OLM 的下一代迭代组件作为技术预览功能，在这个阶段称为 *OLM 1.0*。此更新的框架改变了很多属于以前版本的 OLM 的概念，并添加了新功能。

在 OpenShift Container Platform 4.15 中 OLM 1.0 的技术预览阶段，管理员可以探索本发行版本中添加的以下功能：

支持版本范围

您可以使用 Operator 或扩展的自定义资源 (CR) 中的比较字符串来指定版本范围。如果您在 CR 中指定版本范围，OLM 1.0 会安装或升级到可以在版本范围内解析的 Operator 的最新版本。如需更多信息，请参阅更新 Operator 和 版本范围的支持

Catalog API 的性能改进

Catalog API 现在使用 HTTP 服务提供集群中的目录内容。在以前的版本中，自定义资源定义 (CRD) 用于此目的。使用 HTTP 服务提供目录内容的更改可减少 Kubernetes API 服务器上的负载。如需更多信息，请参阅从目录中查找安装的 Operator。

注意

对于 OpenShift Container Platform 4.15，适用于 OLM 1.0 的流程都是基于 CLI 的。另外，管理员也可以使用普通方法（如 **Import YAML** 和 **Search** 页面）在 web 控制台中创建和查看相关对象。但是，现有的 **OperatorHub** 和 **Installed Operators** 页面还不会显示 OLM 1.0 组件。

如需更多信息，请参阅关于 Operator Lifecycle Manager 1.0。

重要

目前，OLM 1.0 支持符合以下条件的安装 Operator 和扩展：

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

使用 Webhook 或指定命名空间集的 Operator 和扩展无法安装。

1.3.12.2. Operator 目录的弃用模式

可选的 **olm.deprecations** 模式定义了基于文件的目录中的 Operator 软件包、捆绑包和频道的弃用信息。Operator 作者可在 **deprecations.yaml** 文件中使用此模式，向从目录运行这些 Operator 的用户提供与 Operator 相关的信息，如支持状态和推荐的升级路径。安装 Operator 后，可以在相关的 **Subscription** 对象上查看任何指定的信息作为状态条件。

有关 **olm.deprecations** 模式的信息，请参阅 Operator Framework 打包格式。

1.3.13. Operator 开发

1.3.13.1. 云供应商上的 Operator 的令牌身份验证：Microsoft Entra Workload ID

在这个版本中，由 Operator Lifecycle Manager (OLM) 管理的 Operator 可以在为 Microsoft Entra Workload ID 配置的 Azure 集群上运行时支持令牌身份验证。只要 Operator 作者启用了其 Operator 支持 Microsoft Entra Workload ID，对 Cloud Credential Operator (CCO) 的更新会启用特定短期凭证的半自动化置备。

如需更多信息，请参阅使用 Azure AD Workload Identity 的 OLM 管理的 Operator 的基于 CCO 的工作流。

1.3.14. Builds

1.3.15. Machine Config Operator

1.3.15.1. 改进了节点的 MCO 状态报告（技术预览）

在这个版本中，您可以作为技术预览监控单个节点的更新。如需更多信息，请参阅检查机器配置节点状态。

1.3.16. 机器 API

1.3.16.1. 为 control plane 机器集定义 VMware vSphere 故障域（技术预览）

通过使用 vSphere 故障域资源，您可以使用 control plane 机器集在独立于主 VMware vSphere 基础架构的硬件上部署 control plane 机器。control plane 机器集帮助在定义的故障域间平衡 control plane 机器，以便为基础架构提供容错功能。

如需更多信息，请参阅 VMware vSphere 故障域配置和支持的云供应商示例。

1.3.17. 节点

1.3.17.1. /dev/fuse 设备在非特权 pod 上启用更快的构建

您可以使用 **/dev/fuse** 设备配置非特权 pod，以访问更快的构建。

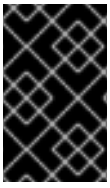
如需更多信息，请参阅使用 /dev/fuse 访问更快的构建。

1.3.17.2. 默认启用日志链接

从 OpenShift Container Platform 4.15 开始，日志链接会被默认启用。日志链接可让您访问 pod 的容器日志。

1.3.17.3. ICSP、IDMS 和 ITMS 现在兼容

ImageContentSourcePolicy (ICSP)、**ImageDigestMirrorSet** (IDMS)和 **ImageTagMirrorSet** (ITMS) 对象现在可同时在同一集群中正常工作。在以前的版本中，要使用较新的 IDMS 或 ITMS 对象，您需要删除任何 ICSP 对象。现在，您可以在安装集群后使用任意或全部三种对象来配置存储库镜像。如需更多信息，请参阅了解镜像 registry 存储库镜像。



重要

使用 ICSP 对象配置存储库镜像是一个已弃用的功能。弃用的功能仍然包含在 OpenShift Container Platform 中，并被支持。但是，可能会在以后的发行版本中删除。由于它已被弃用，因此避免将其用于新部署。

1.3.18. 监控

此发行版本中的集群监控堆栈包括以下新功能和修改后的功能。

1.3.18.1. 监控堆栈组件和依赖项更新

此发行版本包括对集群监控堆栈组件和依赖项的以下版本更新：

- Alertmanager 更新到 0.26.0
- kube-state-metrics 更新到 2.10.1
- node-exporter 更新到 1.7.0
- Prometheus 更新到 2.48.0
- Prometheus Adapter 更新到 0.11.2
- Prometheus Operator 更新到 0.70.0
- Thanos Querier 更新到 0.32.5

1.3.18.2. 对警报规则的更改

注意

红帽不保证记录规则或警报规则的向后兼容性。

- 现在，当使用 Precision Time Protocol (PTP)时，**NodeClockNotSynchronising** 和 **NodeClockSkewDetected** 警报规则会被禁用。

1.3.18.3. 新的 Metrics Server 组件用于访问 Metrics API （技术预览）

此发行版本引入了一个技术预览选项，可将 Metrics Server 组件添加到集群监控堆栈中。当 **FeatureGate** 自定义资源配置了 **TechPreviewNoUpgrade** 选项，会自动安装 Metrics Server 而不是 Prometheus Adapter（技术预览）。如果已安装，指标服务器会收集资源指标，并在 **metrics.k8s.io** Metrics API 服务中公开它们，供其他工具和 API 使用。使用 Metrics Server 而不是 Prometheus Adapter 可释放核心平台 Prometheus 堆栈来处理此功能。如需更多信息，请参阅 Cluster Monitoring Operator 的配置映射 API 参考中的 MetricsServerConfig，以及 使用功能门启用功能。

1.3.18.4. 将 exemplar 数据发送到用户定义的项目的远程写入存储的新功能

用户定义的项目现在可以使用远程写入将 Prometheus 提取的 exemplar 数据发送到远程存储。要使用这个功能，请使用 **RemoteWriteSpec** 资源中的 **sendExemplars** 选项配置远程写入。如需更多信息，请参阅 Cluster Monitoring Operator 的配置映射 API 参考中的 RemoteWriteSpec。

1.3.18.5. 改进了用户定义的项目的警报查询

用户定义的项目中的应用程序现在可以使用 API，通过 Thanos Querier 的规则集端口查询应用程序命名空间的警报。现在，您可以构建一个查询，它使用 **/api/v1/alerts** 端点（通过 Thanos Querier 的端口 9093），提供包括一个 **namespace** 参数的 HTTP 请求。在以前的版本中，Thanos Querier 的规则租期端口没有提供对 **/api/v1/alerts** 端点的 API 访问。

1.3.18.6. Prometheus 更新为在提取时容许 jitters

监控堆栈中的默认 Prometheus 配置已更新，以便在提取时容许 jitter。对于为数据存储显示子优化块压缩的监控部署，这个更新有助于优化数据压缩，从而减少了这些部署中时间序列数据库所使用的磁盘空间。

1.3.18.7. 改进了对 kubelet 服务监控器的过时的处理

改进了对 kubelet 服务监控器的过时的处理，以确保警报和时间聚合准确。这个改进的功能默认处于活动状态，它使专用服务监控器功能过时。因此，专用服务监控器功能已被禁用，且现已弃用，并将 **DedicatedServiceMonitors** 资源设置为 **enabled** 无效。

1.3.18.8. 改进了对任务失败的报告进行故障排除的功能

现在，在监控组件中的任务失败时提供的原因更为精细，以便您可以更轻松地查明在 **openshift-monitoring** 命名空间中部署的组件或 **openshift-user-workload-monitoring** 命名空间中报告失败的原因。如果 Cluster Monitoring Operator (CMO) 报告任务失败，则会添加以下原因来识别故障的来源：

- **PlatformTasksFailed** 原因表示来自 **openshift-monitoring** 命名空间中的失败。
- **UserWorkloadTasksFailed** 原因表示源自 **openshift-user-workload-monitoring** 命名空间中的失败。

1.3.19. Network Observability Operator

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

1.3.20. 可伸缩性和性能

您可以将 control plane 硬件速度设置为 **"Standard"**、**"Slower"** 或默认值（**""**），允许系统决定使用哪个速度。这是一个技术预览功能。如需更多信息，请参阅为 etcd 设置调整参数。

1.3.20.1. PolicyGenTemplate CR 的 hub 端的模板

您可以使用 hub 模板在应用到受管集群的生成的策略中填充组和站点值来管理集群的配置。通过在组和站点 **PolicyGenTemplate** (PGT) CR 中使用 hub 模板，您可以显著减少 hub 集群上的策略数量。如需更多信息，请参阅使用 hub 模板在组 PolicyGenTemplate CR 中指定组和站点配置 。

1.3.20.2. Node Tuning Operator (NTO)

用于延迟测试的 Cloud-native Network Function (CNF) 测试镜像 **cnf-tests** 已被简化。新镜像有三个关于延迟的测试。测试默认运行，并需要在集群中配置性能配置集。如果没有配置性能配置集，则测试不会运行。

不建议使用以下变量：

- **ROLE_WORKER_CNF**
- **NODES_SELECTOR**
- **PERF_TEST_PROFILE**
- **FEATURES**
- **LATENCY_TEST_RUN**
- **DISCOVERY_MODE**

要生成 **junit** 报告，使用 **--ginkgo.junit-report** 标志替换 **--junit**。

如需更多信息，请参阅为平台验证执行延迟测试。

1.3.20.3. Bare Metal Operator

对于 OpenShift Container Platform 4.15，当 Bare Metal Operator 从集群中删除了一个主机时，它还会关闭那个主机。此功能增强简化了硬件维护和管理。

1.3.21. 托管 control plane

1.3.21.1. 使用非裸机代理机器配置托管的 control plane 集群（技术预览）

在这个版本中，您可以使用非裸机代理机器置备托管的 control plane 集群。如需更多信息，请参阅使用非裸机代理机器配置托管的 control plane 集群（技术预览）。

1.3.21.2. 使用 OpenShift Container Platform 控制台创建托管集群

在这个版本中，您可以使用 OpenShift Container Platform 控制台创建带有 KubeVirt 平台的托管集群。Kubernetes Operator (MCE) 的多集群引擎启用托管集群视图。如需更多信息，请参阅使用控制台创建托管集群。

1.3.21.3. 为节点池配置额外网络、保证 CPU 和虚拟机调度

在这个版本中，您可以配置额外网络，对虚拟机(VM) 请求保证的 CPU 访问，并管理为节点池调度 KubeVirt VM。如需更多信息，请参阅为节点池配置额外网络、保证 CPU 和虚拟机调度。

1.4. 主要的技术变化

OpenShift Container Platform 4.15 包括以下显著的技术更改。

集群指标端口安全
在这个版本中，为 Cluster Machine Approver Operator 和 Cluster Cloud Controller Manager Operator 提供指标的端口使用传输层安全 (TLS) 协议来实现额外的安全性。(**OCPCLOUD-2272**, **OCPCLOUD-2271**)

Google Cloud Platform 的云控制器管理器
Kubernetes 社区计划弃用 Kubernetes 控制器管理器与底层云平台交互，而是使用云控制器管理器。因此，无法为任何新的云平台添加 Kubernetes 控制器管理器支持。

此发行版本引入了在 Google Cloud Platform 中使用云控制器管理器的正式发布。

要了解有关云控制器管理器的更多信息，请参阅 Kubernetes Cloud Controller Manager 文档。

要管理云控制器管理器和云节点管理器部署和生命周期，请使用 Cluster Cloud Controller Manager Operator。

如需更多信息，请参阅 *集群 Operator 参考*中的 Cluster Cloud Controller Manager Operator 条目。

以后对 pod 安全准入的限制强制
目前，pod 安全违反情况在审计日志中显示为警告，而不会导致 pod 的拒绝。

目前，计划在下一个 OpenShift Container Platform 次要发行本中对 pod 安全准入进行全局限制强制。启用此受限强制时，具有 Pod 安全违反情况的 Pod 将被拒绝。

要准备此即将推出的更改，请确保您的工作负载与应用到它们的 pod 安全准入配置集匹配。未根据全局或命名空间级别定义的强制安全标准配置的工作负载将被拒绝。**restricted-v2** SCC 根据 Restricted Kubernetes 定义接受工作负载。

如果您要收到 pod 安全漏洞，请查看以下资源：

- 如需了解如何查找导致 pod 安全违反情况的信息，请参阅识别 pod 安全违反情况。
- 请参阅关于 pod 安全准入同步，以了解何时执行 pod 安全准入标签同步。在某些情况下，Pod 安全准入标签不会同步，比如以下情况：
  - 工作负载在系统创建的命名空间中运行，该命名空间前缀为 **openshift-**。
  - 工作负载在没有 pod 控制器的情况下创建的 pod 上运行。
- 如果需要，您可以通过设置 **pod-security.kubernetes.io/enforce** 标签，在命名空间或 pod 上设置自定义准入配置集。

当禁用了集成的 OpenShift 镜像 registry 时，secret 不再自动生成

如果您禁用 **ImageRegistry** 集群功能，或者在 Cluster Image Registry Operator 配置中禁用集成的 OpenShift 镜像 registry，则每个服务帐户令牌 secret 和镜像 pull secret 不再为每个服务帐户生成。

如需更多信息，请参阅自动生成的 secret。

打开虚拟网络基础架构控制器默认范围

在以前的版本中，IP 地址范围 **168.254.0.0/16** 是用于传输交换机子网的 Open Virtual Network Infrastructure Controller 的默认 IP 地址范围。在这个版本中，控制器使用 **100.88.0.0/16** 作为默认的 IP 地址范围。不要在您的生产环境基础架构网络中使用这个 IP 范围。(OCPBUGS-20178)

HAProxy 简介没有 strict-limits 变量

过渡到 HAProxy 2.6 包含了对 **strict-limits** 配置的强制性，这会导致在无法满足 **maxConnections** 要求时造成无法恢复的错误。**strict-limits** 设置无法被最终用户配置，并保持在 HAProxy 模板控制之下。

此发行版本引进了配置调整，以应对迁移到 **maxConnections** 的问题。现在，HAProxy 配置切换到使用 **no strict-limits**。因此，当无法满足 **maxConnection** 配置时，HAProxy 不再失败退出。相反，它会发出警告并继续运行。当无法满足 **maxConnection** 限制时，可能会返回类似以下示例的警告：

- **[WARNING] (50) : [/usr/sbin/haproxy.main()] Cannot raise FD limit to 4000237, limit is 1048576.**
- **[ALERT] (50) : [/usr/sbin/haproxy.main()] FD limit (1048576) too low for maxconn=2000000/maxsock=4000237.Please raise 'ulimit-n' to 4000237 or more to avoid any trouble.**

要解决这些警告，我们建议在调整 IngressController 时为 **maxConnections** 字段指定 **-1** 或 **auto**。这种选择允许 HAProxy 根据正在运行的容器中的可用资源限制动态计算最大值，从而消除了这些警告。(OCPBUGS-21803)

如果禁用了 DeploymentConfig 集群功能，则部署器服务帐户不再被创建

如果您禁用 **DeploymentConfig** 集群功能，则 **deployer** 服务帐户及其对应的 secret 不再被创建。

如需更多信息，请参阅 DeploymentConfig 功能。

must-gather 存储限制默认

为 **oc adm must-gather** 命令收集的数据添加了节点存储容量的默认限制 30%。如果需要，您可以使用 **--volume-percentage** 标志来调整默认存储限制。

如需更多信息，请参阅更改 must-gather 存储限制。

串行控制台会显示基于代理的安装程序互动网络配置
在这个版本中，当在没有图形控制台的服务器上引导代理 ISO 时，可以在串行控制台中进行交互式网络配置。状态显示在所有其他控制台上暂停，而交互式网络配置处于活动状态。在以前的版本中，显示只能在图形控制台中显示。(OCPBUGS-19688)

1.5. 弃用和删除的功能

之前版本中的一些功能已被弃用或删除。

弃用的功能仍然包含在 OpenShift Container Platform 中，并将继续被支持。但是，这个功能会在以后的发行版本中被删除，且不建议在新的部署中使用。有关 OpenShift Container Platform 4.15 中已弃用并删除的主要功能的最新列表，请参考下表。表后列出了更多已弃用和删除的功能的更多详细信息。

在以下表格中，功能被标记为以下状态：

- *公开发行*
- *已弃用*
- *删除*

Operator 生命周期和开发已弃用和删除的功能

表 1.6. Operator 生命周期和开发已弃用并删除 tracker

功能	4.13	4.14	4.15
Operator 目录的 SQLite 数据库格式	已弃用	已弃用	已弃用

镜像已弃用和删除的功能

表 1.7. 镜像已弃用和删除的 tracker

功能	4.13	4.14	4.15
Cluster Samples Operator 的 **ImageChangesInProgress** 条件	已弃用	已弃用	已弃用
Cluster Samples Operator 的 **MigrationInProgress** 条件	已弃用	已弃用	已弃用

监控已弃用和删除的功能

表 1.8. 监控已弃用和删除的 tracker

功能	4.13	4.14	4.15
dedicatedServiceMonitors 设置，用于为核心平台监控启用专用的服务监控器	公开发行	公开发行	已弃用

功能	4.13	4.14	4.15
prometheus-adapter 组件从 Prometheus 查询资源指标，并在 metrics API 中公开它们。	公开发行	公开发行	已弃用

安装已弃用和删除的功能

表 1.9. 安装已弃用并删除跟踪器

功能	4.13	4.14	4.15
OpenShift SDN 网络插件	公开发行	已弃用	删除 [1]
oc adm release extract 的 **--cloud** 参数	公开发行	已弃用	已弃用
对 **cluster.local** 域的 CoreDNS 通配符查询	删除	删除	删除
compute.platform.openstack.rootVolume.type for RHOSP	公开发行	已弃用	已弃用
controlPlane.platform.openstack.rootVolume.type for RHOSP	公开发行	已弃用	已弃用
安装程序置备的基础架构集群的 **install-config.yaml** 文件中的 **ingressVIP** 和 **apiVIP** 设置	已弃用	已弃用	已弃用
Google Cloud Provider 的 **platform.gcp.licenses**	已弃用	删除	删除

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

存储已弃用和删除的功能

表 1.10. 存储已弃用和删除的 tracker

功能	4.13	4.14	4.15
使用 FlexVolume 的持久性存储	已弃用	已弃用	已弃用

已弃用和删除的网络功能

表 1.11. 已弃用和删除的网络功能跟踪器

功能	4.13	4.14	4.15
RHOSP 上的 Kuryr	已弃用	已弃用	删除
OpenShift SDN 网络插件	公开发行	已弃用	已弃用

构建应用程序已弃用和删除的功能

表 1.12. Service Binding Operator 弃用并删除 tracker

功能	4.13	4.14	4.15
Service Binding Operator	已弃用	已弃用	已弃用

节点已弃用和删除的功能

表 1.13. 节点已弃用并删除 tracker

功能	4.13	4.14	4.15
ImageContentSourcePolicy (ICSP) 对象	已弃用	已弃用	已弃用
Kubernetes 拓扑标签 **failure-domain.beta.kubernetes.io/zone**	已弃用	已弃用	已弃用
Kubernetes 拓扑标签 **failure-domain.beta.kubernetes.io/region**	已弃用	已弃用	已弃用

OpenShift CLI (oc) 已弃用和删除的功能

功能	4.13	4.14	4.15
oc-mirror 的 **--include-local-oci-catalogs** 参数	公开发行	删除	删除
oc-mirror 的 **--use-oci-feature** 参数	已弃用	删除	删除

工作负载已弃用和删除的功能

表 1.14. 工作负载已弃用和删除的 tracker

功能	4.13	4.14	4.15
deploymentConfig 对象	公开发行	已弃用	已弃用

裸机监控

表 1.15. 裸机事件中继 Operator tracker

功能	4.13	4.14	4.15
裸机事件中继 Operator	技术预览	技术预览	已弃用

1.5.1. 已弃用的功能

1.5.1.1. 弃用 OpenShift SDN 网络插件

从 OpenShift Container Platform 4.14 开始，OpenShift SDN CNI 已被弃用。自 OpenShift Container Platform 4.15 起，网络插件不是新安装的选项。在以后的发行版本中，计划删除 OpenShift SDN 网络插件，并不再被支持。红帽将在删除前对这个功能提供程序错误修正和支持，但不会再改进这个功能。作为 OpenShift SDN CNI 的替代选择，您可以使用 OVN Kubernetes CNI。

1.5.1.2. 裸机事件中继 Operator

裸机事件中继 Operator 已被弃用。以后的 OpenShift Container Platform 发行版本中会删除使用 Bare Metal Event Relay Operator 监控裸机主机的功能。

1.5.1.3. Service Binding Operator

Service Binding Operator 已被弃用，并将在 OpenShift Container Platform 4.16 发行版本中删除。红帽将在当前发行生命周期中对这个组件提供重要的程序错误修复和支持，但此组件将不再获得功能增强。

1.5.1.4. 用于核心平台监控的专用服务监控器

在这个版本中，核心平台监控的专用服务监控器功能已弃用。通过在 **openshift-monitoring** 命名空间中的 **cluster-monitoring-config** 配置映射对象中配置 **dedicatedServiceMonitors** 设置来启用专用服务监控器的功能，将在以后的 OpenShift Container Platform 发行版本中删除。要替换此功能，Prometheus 功能已被改进，以确保警报和时间聚合准确。这个改进的功能默认处于活动状态，它使专用服务监控器功能过时。

1.5.1.5. 用于核心平台监控的 Prometheus Adapter

在这个版本中，核心平台监控的 Prometheus Adapter 组件已弃用，计划在以后的发行版本中删除。红帽将在当前发行生命周期中对这个组件提供程序错误修正和支持，但此组件将不再获得改进，并将在以后被删除。作为替换，在监控堆栈中添加了一个新的 Metrics Server 组件。指标服务器是一个更简单、更轻量级的解决方案，因为它不依赖 Prometheus 来实现其功能。指标服务器还可确保可扩展性和更准确的资源指标跟踪。在这个版本中，如果您在 **FeatureGate** 自定义资源中启用了 **TechPreviewNoUpgrade** 选项，则指标服务器的改进功能默认可用。

1.5.1.6. oc registry info 命令已弃用

在这个版本中，实验性 **oc registry info** 命令已弃用。

要查看有关集成 OpenShift 镜像 registry 的信息，请运行 **oc get imagestream -n openshift** 并检查 **IMAGE REPOSITORY** 列。

1.5.2. 删除的功能

1.5.2.1. 移除 OPENSHIFT_DEFAULT_REGISTRY

OpenShift Container Platform 4.15 删除了对 **OPENSHIFT_DEFAULT_REGISTRY** 变量的支持。此变量主要用于为之前设置启用内部镜像 registry 的向后兼容性。**REGISTRY_OPENSHIFT_SERVER_ADDR** 变量可以在其位置使用。

1.5.2.2. 删除在带有 Kuryr 的 Red Hat OpenStack Platform (RHOSP) 上安装集群

从 OpenShift Container Platform 4.15 开始，删除了使用 kuryr 在 RHOSP 上安装集群的支持。

1.5.3. 将来的 Kubernetes API 删除

OpenShift Container Platform 的下一个次版本应该使用 Kubernetes 1.29。Kubernetes 1.29 删除了已弃用的 API。

如需要被删除的 Kubernetes API 列表，请参阅上游 Kubernetes 文档中的已弃用 API 迁移指南。

如需了解如何检查集群是否有 Kubernetes API 进行删除的信息，请参阅浏览启用和删除的 Kubernetes API。

1.6. 程序错误修复

API 服务器和客户端

- 在以前的版本中，kube-apiserver 日志文件夹中的 **termination.log** 具有无效的权限，因为上游库中的设置。在这个版本中，上游库已被更新，**terminate.log** 现在具有预期的权限。(OCPBUGS-11856)

- 在以前的版本中，如果现有清单在升级后获取能力注解，Cluster Version Operator (CVO) 会启用一个功能。这会导致在升级到 OpenShift Container Platform 4.14 后为之前禁用了控制台功能的用户启用控制台。在这个版本中，现有清单中删除了不必要的控制台功能，控制台功能不再被隐式启用。(OCPBUGS-20331)

- 在以前的版本中，当删除 **openshift-kube-controller-manager** 命名空间时，会重复记录以下错误：**failed to synchronize namespace**。在这个版本中，当 **openshift-kube-controller-manager** 命名空间被删除时，不再记录这个错误。(OCPBUGS-17458)

裸机硬件置备

- 在以前的版本中，从双栈 GitOps ZTP hub 部署 IPv6 主机会阻止将正确的回调 URL 传递给基板管理控制器 (BMC)。因此，IPv4 URL 无条件传递。这个问题已被解决，URL 的 IP 版本现在取决于 BMC 地址的 IP 版本。(OCPBUGS-23759)

- 在以前的版本中，Bare Metal Operator (BMO)容器有一个 **hostPort** 指定为 **60000**，但 **hostPort** 在规格并不实际使用。因此，其他服务无法使用端口 60000。在这个版本中，会从容器配置中删除 **hostPort** 规格。现在，其他服务可以使用端口 60000。(OCPBUGS-18788)

- 在以前的版本中，当 Cluster Baremetal Operator (CBO)检查基础架构 **platformStatus** 字段并返回 **nil** 时，Cluster Baremetal Operator (CBO) 会失败。在 OpenShift Container Platform 4.15 中，CBO 已被更新，以便在 **apiServerInternalIPs** 返回 **nil** 时检查并返回空白值，从而解决这个问题。(OCPBUGS-17589)

- 在以前的版本中，**inspector.ipxe** 配置使用 **IRONIC_IP** 变量，它没有考虑 IPv6 地址，因为它们有括号。因此，当用户提供不正确的 **boot_mac_address** 时，iPXE fell 回到 **inspector.ipxe** 配置，它提供了一个格式不正确的 IPv6 主机标头，因为它不包含括号。
  在 OpenShift Container Platform 4.15 中，**inspector.ipxe** 配置已更新为使用 **IRONIC_URL_HOST** 变量，其帐户用于 IPv6 地址并解决问题。(OCPBUGS-27060)

- 在以前的版本中，尝试使用带有 Cisco UCS 硬件的 RedFish Virtual Media 在新裸机主机中部署 OpenShift Container Platform 时存在一个错误。这个程序错误会阻止裸机主机的新置备，因为 Ironic 无法找到合适的虚拟介质设备。在这个版本中，Ironic 在所有可用虚拟介质设备中进行更多检查。因此，在使用 RedFish Virtual Media 时可以置备 Cisco UCS 硬件。(OCPBUGS-23105)

- 在以前的版本中，当在将 **secureBoot** 字段设置为 **disabled** 的节点上将 **bootMode** 字段设置为 **UEFISecureBoot** 时，安装程序无法启动。在这个版本中，Ironic 已被更新，可以将 **secureBoot** 设置为 **enabled** 来安装 OpenShift Container Platform。(OCPBUGS-9303)

Builds

- 在以前的版本中，在容器间复制内容时，时间戳不会被保留。在这个版本中，**-p** 标志添加到 **cp** 命令中，以允许保留时间戳。(OCPBUGS-22497)

Cloud Compute

- 在以前的版本中，从 **MachineSet** spec 解析污点中的一个错误意味着自动扩展无法直接考虑 spec 中设置的任何污点。因此，当依赖 **MachineSet** 污点从零扩展时，不会考虑 spec 中的污点，这可能会导致扩展决策不正确。在这个版本中，从零进行扩展的逻辑已改进，解决了相关问题。因此，自动扩展现在可以正常工作，并可以识别污点来阻止在其中调度工作负载。(OCPBUGS-27750)

- 在以前的版本中，用于提供镜像凭证的 Amazon Web Services (AWS) 代码被从 OpenShift Container Platform 4.14 中的 kubelet 中删除。因此，在没有指定 pull secret 的情况下从 Amazon Elastic Container Registry (ECR) 拉取镜像会失败，因为 kubelet 无法验证自己并将凭证传递给容器运行时。在这个版本中，配置了一个单独的凭证供应商，它负责为 kubelet 提供 ECR 凭证。现在，kubelet 可以从 ECR 拉取私有镜像。(OCPBUGS-27486)

- 在以前的版本中，当部署托管 control plane (HCP) KubeVirt 集群 **--node-selector** 命令，节点选择器不会应用到 HCP 命名空间中的 **kubevirt-cloud-controller-manager** pod。因此，您无法将整个 HCP pod 固定到特定的节点。在这个版本中，这个问题已被解决。(OCPBUGS-27071)

- 在以前的版本中，Microsoft Azure 负载均衡器的默认虚拟机(VM)类型从 **Standard** 改为 **VMSS**。因此，服务类型负载均衡器无法将标准虚拟机附加到负载均衡器。在这个版本中，将这些更改恢复到以前的配置，以保持与 OpenShift Container Platform 部署的兼容性。因此，负载均衡器附加现在更为一致。(OCPBUGS-26210)

- 在以前的版本中，在将 **enable_port_security** 字段设置为 **false** 的 RHOSP 节点上部署将无法创建 **LoadBalancer** 服务。在这个版本中，这个问题已解决。(OCPBUGS-22246)

- 如果 Nova 元数据服务在第一次引导时不可用，Red Hat OpenStack Platform (RHOSP) 上的 worker 节点使用域组件命名。OpenShift Container Platform 要求节点名称与 Nova 实例相同。名称差异导致节点的证书请求被拒绝，且节点无法加入集群。在这个版本中，worker 节点将在第一次引导时等待并重试元数据服务，确保节点被正确命名。(OCPBUGS-22200)

- 在以前的版本中，当与具有 Container Storage Interface (CSI) 存储的节点一起使用时，集群自动扩展会崩溃。这个问题已在本发行版本中解决。(OCPBUGS-23096)

- 在以前的版本中，在某些代理环境中，Amazon Web Services (AWS) 元数据服务可能无法在初始启动时不存在，且可能仅在启动后马上可用。kubelet 主机名获取没有考虑这个延迟，因此节点无法引导，因为它没有有效的主机名。在这个版本中，确保了主机名获取脚本在失败时会在一段时间内进行重试。因此，在一个短的时间段内，即使出现元数据无法访问的情况也可以正常工作。(OCPBUGS-20369)

- 在 OpenShift Container Platform 版本 4.14 及更新的版本中，存在一个已知问题：安装 Microsoft Azure Stack Hub 失败。升级到 4.14 或更高版本的 Microsoft Azure Stack Hub 集群可能会在节点扩展或缩减时遇到负载均衡器配置问题。在这个问题解决前，不建议在 Microsoft Azure Stack Hub 环境中安装或升级 4.14。(OCPBUGS-20213)

- 在以前的版本中，Cluster Autoscaler Operator 启动过程中的一些条件会导致一个锁定，阻止 Operator 成功启动并将自身标记为可用。因此，集群会降级。这个版本解决了这个问题。(OCPBUGS-18954)

- 在以前的版本中，当控制节点添加到第二个内部实例组时，试图执行 Google Cloud Platform XPN 内部集群安装会失败。这个程序错误已被解决。(OCPBUGS-5755)

- 在以前的版本中，在将节点标记为终止前，终止处理器会提前退出。此条件的发生取决于控制器收到终止信号的时间。在这个版本中，通过引入额外的终止检查来考虑早期终止的情况。(OCPBUGS-2117)

- 在以前的版本中，当没有启用 **Build** 集群功能时，集群版本 Operator (CVO)无法同步构建 informer，且无法成功启动。在这个版本中，当没有启用 **Build** 功能时，CVO 会成功启动。(OCPBUGS-22956)

Cloud Credential Operator

- 在以前的版本中，Cloud Credential Operator 实用程序 (**ccoctl**) 在集群级别上创建了自定义 GCP 角色，因此每个集群对允许的自定义角色数量赋予配额限制。由于 GCP 删除策略，删除的自定义角色在删除后持续为配额限制提供配额限制。在这个版本中，自定义角色在项目级别添加，而不是集群级别，以减少创建的自定义角色总数。另外，在删除 **ccoctl** 工具在安装过程中创建的 GCP 资源时，可以使用清理自定义角色的选项。这些更改可帮助避免到达允许的自定义角色数量的配额限制。(OCPBUGS-28850)

- 在以前的版本中，当没有启用 **Build** 集群功能时，集群版本 Operator (CVO)无法同步构建 informer，且无法成功启动。在这个版本中，当没有启用 **Build** 功能时，CVO 会成功启动。(OCPBUGS-26510)

- 在以前的版本中，运行 **ccoctl azure create** 命令创建的存储桶会被禁止允许公共 blob 访问，因为 Microsoft Azure 存储桶的默认行为发生了变化。在这个版本中，运行 **ccoctl azure create** 命令创建的存储桶被明确设置为允许公共 blob 访问。(OCPBUGS-22369)

- 在以前的版本中，Cloud Controller Manager 服务帐户中省略了 Azure Managed Identity 角色。因此，Cloud Controller Manager 无法使用私有发布方法管理部署到现有 VNet 的环境中的服务类型负载均衡器。在这个版本中，在 Cloud Credential Operator 实用程序 (**ccoctl**) 和 Azure Managed Identity 安装中添加了缺少的角色到带有私有发布的现有 VNet 中。(OCPBUGS-21745)

- 在以前的版本中，Cloud Credential Operator 不支持更新存储在 **kube-system** 命名空间中的 root secret **vshpere-creds** 中的 vCenter 服务器值。因此，尝试更新这个值会导致旧值和新值都存在，因为组件 secret 没有正确同步。在这个版本中，Cloud Credential Operator 在同步过程中重置 secret 数据，以便支持更新 vCenter 服务器值。(OCPBUGS-20478)

- 在以前的版本中，Cloud Credential Operator 实用程序 (**ccoctl**) 无法在中国区中创建 AWS 安全令牌服务 (STS) 资源，因为中国区域 DNS 后缀 **.amazonaws.com.cn** 与其它区域中使用的后缀 **.amazonaws.com** 不同。在这个版本中，**ccoctl** 可以检测正确的 DNS 后缀，并使用它来创建所需资源。(OCPBUGS-13597)

Cluster Version Operator

- Cluster Version Operator (CVO) 持续检索更新建议，并根据当前集群状态评估已知的条件更新风险。在以前的版本中，失败的风险评估会阻止 CVO 获取新的更新建议。当因为更新建议服务处理一个没有很好定义的更新风险而造成风险评估失败，这个问题可能会阻止 CVO 通知更新建议服务提供改进的风险声明。在这个版本中，CVO 继续轮询更新建议服务，无论是否成功评估更新风险。(OCPBUGS-25949)

开发人员控制台

- 在以前的版本中，因为特定资源的 API 版本最新被更新，**BuildRun** 日志在 BuildRun 的 **Logs** 标签页中不可见。在这个版本中，**TaskRuns** 的日志被添加到 BuildRun 的 **Logs** 标签页中，用于 builds Operator 的 v1alpha1 和 v1beta1 版本。(OCPBUGS-29283)

- 在以前的版本中，当选择了从 **ArtifactHub** 安装的 Pipeline Builder 中的一个 **Task** 时，控制台 UI 失败，并显示一个错误页。在这个版本中，控制台 UI 不再需要可选数据，控制台 UI 不再失败。(OCPBUGS-24001)

- 在以前的版本中，Shipwright Plugin 的 **Actions** 菜单中的 **Edit Build** 和 **BuildRun** 选项不允许在 YAML 选项卡中编辑。在这个版本中，您可以在 YAML 标签页中编辑。(OCPBUGS-23164)

- 在以前的版本中，控制台只搜索存储库中的文件名 **Dockerfile**，以识别 Import Flows 中适合 **Container** 策略的存储库。由于可以使用其他容器化工具，所以对 **Containerfile** 文件名的支持现在也适用于 **Container** 策略。(OCPBUGS-22976)

- 在以前的版本中，当未授权用户打开包含路径和查询参数的控制台的链接，且它们被重定向到登录页面时，查询参数不会在登录成功后恢复。因此，用户需要恢复搜索，或者再次点击到控制台的链接。在这个版本中，最新版本会保存并恢复与路径类似的查询参数。(OCPBUGS-22199)

- 在以前的版本中，当从 **Add** 或 **Topology** 视图中进入到 **Create Channel** 页面时，会存在默认名称 **Channel**，但 **Create** 按钮被禁用，在 name 字段中显示 **Required**。在这个版本中，如果添加了默认频道名称，点 **Create** 按钮时不会显示 **Required** 信息。(OCPBUGS-19783)

- 在以前的版本中，使用快速搜索功能时，可以从中选择类似的选项。在这个版本中，**Source-to-image** 选项与 **Topology** 快速搜索中的 **Samples** 选项不同。(OCPBUGS-18371)

- 在以前的版本中，当安装了 {serverless-product-name} Operator 且尚未创建 Knative (Kn) serving 实例时，当从 **Administration → Cluster Settings** 进入 **Global configuration** 页面，点 **Knative-serving** 会显示 **404 page not found** 错误。在这个版本中，在将 **Knative-serving** 添加到 **全局配置** 前，会进行检查来确定是否创建了 Knative serving 实例。(OCPBUGS-18267)

- 在以前的版本中，**Edit Knative Service** 表单存在问题，阻止用户编辑之前创建的 Knative 服务。在这个版本中，您可以编辑之前创建的 Knative 服务。(OCPBUGS-6513)

etcd Cluster Operator

- 在以前的版本中，**cluster-backup.sh** 脚本会无限期地缓存本地机器上 **etcdctl** 二进制文件，从而无法进行更新。在这个版本中，**cluster-backup.sh** 脚本每次运行时都会拉取最新的 **etcdctl** 二进制文件。(OCPBUGS-19052)

托管 Control Plane

- 在以前的版本中，当在托管集群中使用自定义 Container Network Interface (CNI) 插件时，只有在将 **hostedcluster.spec.networking.networkType** 字段设置为 **Calico** 时，才会配置基于角色的访问控制(RBAC)规则。当您将 **hostedcluster.spec.networking.networkType** 字段设置为 **Other** 时，不会配置基于角色的访问控制 (RBAC) 规则。在这个版本中，当将 **hostedcluster.spec.networking.networkType** 字段设置为 **Other** 时，RBAC 规则会被正确配置。(OCPBUGS-28235)

- 在以前的版本中，节点端口无法正确公开，因为 **kube-apiserver** 资源的 **ipFamilyPolicy** 字段被设置为 **SingleStack**。在这个版本中，如果 **ipFamilyPolicy** 设置为 **PreferredDualStack**，节点端口会被正确公开。(OCPBUGS-23350)

- 在以前的版本中，在为托管集群配置 Open Virtual Network (OVN)后，**cloud-network-config-controller**、**multus-admission-controller** 和'ovnkube-control-plane' 资源缺少 **hypershift.openshift.io/hosted-control-plane:{hostedcluster resource namespace}-{cluster-name}** 标签。在这个版本中，在为托管集群配置 Open Virtual Network (OVN) 后，**cloud-network-config-controller**、**multus-admission-controller** 和'ovnkube-control-plane' 资源包含 **hypershift.openshift.io/hosted-control-plane:{hostedcluster resource namespace}-{cluster-name}** 标签。(OCPBUGS-19370)

- 在以前的版本中，在创建托管集群后，使用 **user-ca-bundle** 以外的名称来创建配置映射，如果 Control Plane Operator (CPO) 失败，部署将失败。在这个版本中，您可以使用唯一名称来创建配置映射。CPO 已被成功部署。(OCPBUGS-19419)

- 在以前的版本中，带有 **.status.controlPlaneEndpoint.port: 443** 的托管集群会错误地为公共和私有路由器公开端口 6443。在这个版本中，带有 **.status.controlPlaneEndpoint.port: 443** 的托管集群仅公开端口 443。(OCPBUGS-20161)

- 在以前的版本中，如果 Kube API 服务器使用 IPv4 和 IPv6 公开，且 IP 地址在 **HostedCluster** 资源中设置，则 IPv6 环境无法正常工作。在这个版本中，当 Kube API 服务器使用 IPv4 和 IPv6 公开时，IPv6 环境可以正常工作。(OCPBUGS-20246)

- 在以前的版本中，如果 console Operator 和 Ingress pod 位于同一节点上，控制台 Operator 将失败，并将 console 集群 Operator 标记为不可用。在这个版本中，如果 console Operator 和 Ingress pod 位于同一节点上，则控制台 Operator 不再失败。(OCPBUGS-23300)

- 在以前的版本中，如果卸载托管集群会卡住，则 Control Plane Operator (CPO) 的状态会被错误地报告。在这个版本中，CPO 的状态会被正确报告。(OCPBUGS-26412)

- 在以前的版本中，如果您在初始升级进行时尝试覆盖 OpenShift Container Platform 版本，则托管的集群升级会失败。在这个版本中，如果您使用新的 OpenShift Container Platform 版本覆盖当前的升级，升级会成功完成。(OCPBUGS-18122)

- 在以前的版本中，如果您为托管的 control plane 更新 pull secret，它不会立即反映在 worker 节点上。在这个版本中，当更改 pull secret 时，会触发协调，worker 节点会立即使用新的 pull secret 更新。(OCPBUGS-19834)

- 在以前的版本中，Hypershift Operator 会为不再存在的节点池报告时间序列。在这个版本中，Hypershift Operator 可以正确地报告节点池的时间序列。(OCPBUGS-20179)

- 在以前的版本中，默认启用 **--enable-uwm-telemetry-remote-write** 标志。此设置阻止了遥测协调。在这个版本中，您可以禁用 **--enable-uwm-telemetry-remote-write** 标志来允许遥测协调。(OCPBUGS-26410)

- 在以前的版本中，当 IAM 角色路径 ARN 作为额外的允许主体提供时，control Plane Operator (CPO)无 法更新 VPC 端点服务：**arn:aws:iam::${ACCOUNT_ID}:role/${PATH}/name** 在这个版本中，CPO 使用 **arn:aws:iam::${ACCOUNT_ID}:role/${PATH}/name** 更新 VPC 端点服务，运行凭证成功。(OCPBUGS-23511)

- 在以前的版本中，要自定义 OAuth 模板，如果您配置了 **HostedCluster.spec.configuration.oauth** 字段，此设置不会反映在托管的集群中。在这个版本中，您可以在托管集群中成功配置 **HostedCluster.spec.configuration.oauth** 字段。(OCPBUGS-15215)

- 在以前的版本中，当使用双栈网络部署托管集群时，默认情况下，**clusterIP** 字段被设置为 IPv6 网络，而不是 IPv4 网络。在这个版本中，当使用双栈网络部署托管集群时，**clusterIP** 字段默认设置为 IPv4 网络。(OCPBUGS-16189)

- 在以前的版本中，当部署托管集群时，如果您在 **HostedCluster** 资源中配置了 **advertiseAddress** 字段，则托管集群部署会失败。在这个版本中，您可以在 **HostedCluster** 资源中配置 **advertiseAddress** 字段后成功部署托管集群。(OCPBUGS-19746)

- 在以前的版本中，当您将 **hostedcluster.spec.networking.networkType** 字段设置为 **Calico** 时，Cluster Network Operator 没有充足的基于角色的访问控制(RBAC)权限来部署 **network-node-identity** 资源。在这个版本中，**network-node-identity** 资源已被成功部署。(OCPBUGS-23083)

- 在以前的版本中，您无法为托管的集群中的审计日志更新默认配置。因此，托管的集群的组件无法生成审计日志。在这个版本中，您可以通过更新默认配置来为托管集群的组件生成审计日志。(OCPBUGS-13348)

镜像 Registry

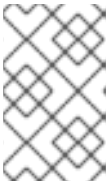
- 在以前的版本中，Image Registry 修剪器依赖于由 OpenShift API 服务器管理的集群角色。这可能会导致修剪器任务在升级过程中间歇性失败。现在，Image Registry Operator 负责创建修剪器集群角色，该角色解决了这个问题。(OCPBUGS-18969)

- Image Registry Operator 在获取访问密钥的过程中对存储帐户列表端点发出 API 调用。在有多个 OpenShift Container Platform 集群的项目中，这可能会导致 API 限制被访问。因此，当尝试创建新集群时，会返回 **429** 错误。在这个版本中，调用之间的时间从 5 分钟增加到 20 分钟，不会再达到 API 限制。(OCPBUGS-18469)

- 在以前的版本中，QPS 和 Burst 的默认低设置会导致镜像 registry 在适当的时间没有返回 API 服务器请求时返回网关超时错误。要解决这个问题，用户必须重启镜像 registry。在这个版本中，QPS 和 Burst 的默认设置有所增加，这个问题不再发生。(OCPBUGS-18999)

- 在以前的版本中，当为 Cluster Image Registry Operator 创建部署资源时，错误处理会使用指针变量，而无需首先检查值是否为 **nil**。因此，当指针值为 **nil** 时，日志中会报告 panic。在这个版本中，添加了一个 nil 检查，以便日志中不再报告 panic。(OCPBUGS-18103)

- 在以前的版本中，OpenShift Container Platform 4.14 发行版本引入了一个更改，让用户在从 OpenShift Container Platform 版本 4.13 更新至 4.14 时会丢失镜像。对默认内部 registry 的更改会导致 registry 在使用 Microsoft Azure 对象存储时使用不正确的路径。在这个版本中，使用正确的路径，并将作业添加到 registry operator 中，该 operator 会将任何 Blob 推送到使用错误的存储路径的 registry 中，这会有效地将两个不同的存储路径合并到一个路径中。

  注意

  在这个版本中，Azure Stack Hub (ASH) **无法工作**。在升级到 4.14.14+ 时，使用 OCP 版本 4.14.0 到 4.14.13 的 ASH 用户需要执行手动步骤来将 Blob 移到正确的存储路径。

  (OCPBUGS-29525)

安装程序

- 在以前的版本中，因为验证错误，在 AWS 上安装集群可能会失败。在这个版本中，安装程序会生成所需的云配置对象来满足机器配置 Operator。这会确保安装成功。(OCPBUGS-12707)

- 在以前的版本中，使用附加到虚拟机的服务帐户在 GCP 上安装集群，因为内部数据验证 bug 可能会失败。在这个版本中，安装程序已被更新，在使用附加到虚拟机的服务帐户时正确验证身份验证参数。(OCPBUGS-19376)

- 在以前的版本中，vSphere 连接配置接口在 "vCenter cluster" 字段中显示网络名称而不是集群名称。在这个版本中，"vCenter cluster"字段已被更新以显示集群名称。(OCPBUGS-23347)

- 在以前的版本中，当使用 **credentialsMode** 参数而不是 **Manual** 进行身份验证，且您使用 **gcloud cli** 工具，安装程序会从 **osServiceAccount.json** 文件中检索 Google Cloud Platform (GCP) 凭证。此操作会导致 GCP 集群安装失败。现在，验证检查会扫描 **install-config.yaml** 文件，并在未将 **credentialsMode** 设置为 **Manual** 时提示您输入信息。请注意，在 **Manual** 模式中，您必须编辑清单并提供凭证。(OCPBUGS-17757)

- 在以前的版本中，当试图使用安装程序置备的基础架构在 VMware vSphere 上安装 OpenShift Container Platform 时，资源池对象会包括双反斜杠。这个格式会导致安装程序生成到网络资源的不正确的路径，这会导致安装失败。在安装程序处理这个资源池对象后，安装程序会输出 "network not found" 错误消息。现在，安装程序会检索集群对象，以便将 InventoryPath 与网络名称加入，以便安装程序指定到资源池对象的正确路径。(OCPBUGS-23376)

- 在以前的版本中，在安装 Azure Red Hat OpenShift 集群后，一些集群 Operator 不可用。这是因为在安装过程中不会创建集群的负载均衡器之一。在这个版本中，负载均衡器会被正确创建。安装集群后，所有集群 Operator 都可用。(OCPBUGS-24191)

- 在以前的版本中，如果 VMware vSphere 集群包含离线的 ESXi 主机，安装会失败并显示 "panic: runtime error: invalid memory address or nil pointer dereference" 信息。在这个版本中，错误消息指出 ESXi 主机不可用。(OCPBUGS-20350)

- 在以前的版本中，如果您在 AWS 上安装集群时只使用默认机器配置来指定现有的 AWS 安全组 (**platform.aws.defaultMachinePlatform.additonalSecurityGroupsIDs**)，则安全组不会应用到 control plane 机器。在这个版本中，当使用默认机器配置指定现有 AWS 安全组时，现有 AWS 安全组会被正确应用到 control plane。(OCPBUGS-20525)

- 在以前的版本中，当指定的机器实例类型 (**platform.aws.type**) 不支持为 control plane 或计算机器 (**controlPlane.architecture** 和 **compute.architecture**) 指定的机器架构时，在 AWS 上安装集群会失败。在这个版本中，安装程序会检查机器实例类型是否支持指定的构架，并在不支持该架构时显示错误消息。(OCPBUGS-26051)

- 在以前的版本中，安装程序在安装集群前不会验证一些配置设置。当这些设置只在默认机器配置中指定时 (**platform.azure.defaultMachinePlatform**) 时会发生此行为。因此，即使满足以下条件，安装也会成功：

  - 指定了不支持的机器实例类型。
  - 指定的机器实例类型不支持额外的功能，如加速网络或使用 Azure ultra 磁盘。

  在这个版本中，安装程序会显示一个指定不支持配置的错误信息。(OCPBUGS-20364)

- 在以前的版本中，当将 AWS 集群安装到 Secret Commercial Cloud Services (SC2S) 区域并指定现有 AWS 安全组时，安装会失败，并显示在区域中不可用的错误。在这个版本中，安装会成功。(OCPBUGS-18830)

- 在以前的版本中，当您在 **install-config.yaml** 配置文件的 **kmsKeyARN** 部分指定密钥管理服务 (KMS)加密密钥时，在 Amazon Web Services (AWS)上安装集群时，在集群安装操作过程中不会添加权限角色。在这个版本中，在配置文件中指定密钥后，会在集群中添加一组额外的密钥，以便集群成功安装。如果您在配置文件中指定了 **credentialsMode** 参数，则忽略所有 KMS 加密密钥。(OCPBUGS-13664)

- 在以前的版本中，Oracle® Cloud Infrastructure (OCI) 上的基于代理的安装没有显示控制台，显示用户的安装进度，从而更难以跟踪安装进度。在这个版本中，OCI 上的基于代理的安装会在控制台中显示安装进度。(OCPBUGS-19092)

- 在以前的版本中，如果在基于 Agent 的安装程序的 **install-config.yaml** 或 **agent-config.yaml** 文件中定义了静态网络，并且接口名称超过 15 个字符，则网络管理器不允许接口启动。在这个版本中，接口名称超过 15 个字符，安装可以继续。(OCPBUGS-18552)

- 在以前的版本中，如果用户没有在 **agent-config.yaml** 文件中指定 **rendezevousIP** 字段，且主机在具有静态网络配置的同一文件中定义，则第一个主机被指定为 rendezvous 节点，而不考虑其角色。这会导致安装失败。在这个版本中，基于代理的安装程序首先查看具有 **master** 角色和定义静态 IP 的主机来优先选择 rendezvous 节点搜索。如果没有找到，则会在没有定义角色的主机中搜索潜在的候选者。明确配置了 **worker** 角色的静态网络配置的主机将被忽略。(OCPBUGS-5471)

- 在以前的版本中，所有基于代理的安装过程中会显示 Agent 控制台应用程序，在继续安装前启用网络自定义。因为云安装过程中很少需要网络配置，所以这在 Oracle® Cloud Infrastructure (OCI) 上并不必要地减慢安装速度。

在这个版本中，OCI 上的基于代理的安装不再显示 Agent 控制台应用程序并更快地继续。(OCPBUGS-19093)

- 在以前的版本中，当平台定义为 **external** 时，基于代理的安装程序默认启用了外部 Cloud Controller Manager (CCM)。这导致用户在不需要它的云平台中执行安装时禁用外部 CCM。在这个版本中，只有在 Oracle® Cloud Infrastructure (OCI) 上执行基于代理的安装时，才需要用户启用外部 CCM。(OCPBUGS-18455)

- 在以前的版本中，**agent wait-for** 命令无法在 **.openshift_install.log** 文件中记录日志。在这个版本中，当使用 **agent wait-for** 命令时，日志会在 **.openshift_install.log** 文件中记录。(OCPBUGS-5728)

- 在以前的版本中，bootstrap 机器中的 **assisted-service** 在 bootstrap 节点重启后不可用，从而导致来自 **assisted-installer-controller** 的任何通信。这会停止 **assisted-installer-controller** 从 worker 节点中删除未初始化的污点，从而导致集群安装在集群 Operator 上挂起。
在这个版本中，**assisted-installer-controller** 可以删除未初始化的污点，即使 **assisted-service** 不可用，安装也可以继续。(OCPBUGS-20049)

- 在以前的版本中，平台类型错误地需要在基于 Agent 的安装程序所使用的 **AgentClusterInstall** 集群清单中需要使用小写。在这个版本中，需要使用大小写混合的值，但也接受原来的小写值并可以正确处理。(OCPBUGS-19444)

- 在以前的版本中，**manila-csi-driver-controller-metrics** 服务有空端点，因为应用程序选择器的名称不正确。在这个版本中，应用程序选择器名称被改为 **openstack-manila-csi**，这个问题已被修复。(OCPBUGS-9331)

- 在以前的版本中，支持的安装程序删除了所有 vSphere 节点的未初始化污点，这会阻止 vSphere CCM 正确初始化节点。这会导致 vSphere CSI Operator 在初始集群安装过程中降级，因为缺少节点的供应商 ID。在这个版本中，辅助安装程序检查 **install-config.yaml** 中是否提供了 vSphere 凭证。如果提供了凭证，OpenShift 版本大于或等于 4.15，且使用了代理安装程序，则 assisted-installer 和 assisted-installer-controller 不会删除未初始化的污点。这意味着，节点的 providerID 和虚拟机的 UUID 会被正确设置，并安装了 vSphere CSI Operator。(OCPBUGS-29485)

Kubernetes Controller Manager

- 在以前的版本中，当为守护进程集设置 **maxSurge** 字段且更新容限时，pod 无法缩减，这会导致因为使用不同的节点集来调度失败。在这个版本中，如果没有满足调度限制，节点会被正确排除，且 rollouts 可以成功完成。(OCPBUGS-19452)

Machine Config Operator

- 在以前的版本中，一个拼写错误的环境变量会阻止脚本检测存在 **node.env** 文件。这会导致 **node.env** 文件的内容在每次引导后被覆盖，kubelet 主机名无法更改。在这个版本中，环境变量拼写已被修正，并重启后对 **node.env** 文件的编辑仍然有效。(OCPBUGS-27307)

- 在以前的版本中，Machine Config Operator 允许进行用户提供的证书颁发机构更新，而无需触发新的机器配置。由于这些更新的新写入方法缺少了新行字符，所以会导致对 CA 文件的内容进行验证错误，并且 Machine Config Daemon 被降级。在这个版本中，CA 文件内容已被修复，更新会如预期进行。(OCPBUGS-25424)

- 在以前的版本中，Machine Config Operator 允许用户提供的证书颁发机构捆绑包更改应用到集群，而无需机器配置，以防止中断。因此，**user-ca** 捆绑包没有传播到集群中运行的应用程序，并需要重启来查看更改生效。在这个版本中，MCO 运行 **update-ca-trust** 命令并重启 CRI-O 服务，以便正确应用新的 CA。(OCPBUGS-24035)

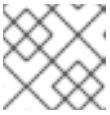
- 在以前的版本中，Machine Config Operator 用来处理镜像 registry 证书的初始机制将删除并重新创建新的配置映射，而不是修补现有配置映射。这会导致 MCO 的 API 使用量显著增加。在这个版本中，机制已被更新，它使用 JSON 补丁，从而解决了这个问题。(OCPBUGS-18800)

- 在以前的版本中，Machine Config Operator 会多次拉取 **baremetalRuntimeCfgImage** 容器镜像：第一次获取节点详情并随后验证镜像是否可用。这会导致在镜像服务器或 Quay 不可用时证书轮转过程中出现问题，后续的镜像拉取会失败。但是，如果镜像因为第一个镜像拉取而已存在在节点中，则节点应会启动 kubelet。在这个版本中，**baremetalRuntimeCfgImage** 镜像只拉取一次，从而解决了这个问题。(OCPBUGS-18772)

- 在以前的版本中，当 OpenShift Container Platform 为一些网络环境进行更新的过程中，**nmstatectl** 命令无法检索正确的持久性 MAC 地址。这会导致接口被重命名，且节点上的绑定连接在更新过程中中断。在这个版本中，补丁被应用到 **nmstate** 软件包和 MCO，以如预期防止重命名和更新。(OCPBUGS-17877)

- 在以前的版本中，Machine Config Operator 成为镜像 registry 证书的默认供应商，并删除 **node-ca** 守护进程。这会导致 HyperShift Operator 出现问题，因为删除 **node-ca** 守护进程也会删除 Machine Config Server (MCS)中的镜像 registry 路径，而 HyperShift 用来获取 Ignition 配置并启动 bootstrap 过程。在这个版本中，提供了一个包含 MCS 镜像 registry 数据的标记，Ignition 可以在 bootstrap 过程中使用它，从而解决这个问题。(OCPBUGS-17811)

- 在以前的版本中，旧的 RHCOS 引导镜像在引导时在服务间包含一个竞争条件，这会阻止节点在拉取镜像前运行 **rhcos-growpart** 命令，从而导致节点启动。这会导致，在使用旧引导镜像的集群中节点扩展有时会失败，因为它确定了磁盘上没有剩余空间。在这个版本中，进程被添加到 Machine Config Operator 中，以获取更严格的服务排序，以便节点可以正确引导。

  注意

  在这些情况下，更新到较新的引导镜像可防止出现类似的问题。

  (OCPBUGS-15087)

- 在以前的版本中，Machine Config Operator (MCO)利用 **oc image extract** 命令在更新过程中拉取镜像，但在拉取这些镜像时，**ImageContentSourcePolicy** (ICSP) 对象不会被遵守。在这个版本中，MCO 在内部使用 **podman pull** 命令，镜像会从 ICSP 中配置的位置拉取。(OCPBUGS-13044)

管理控制台

- 在以前的版本中，**Expand PVC** 模仿现有 PVC 有一个 **spec.resources.requests.storage** 值，其中包含一个单元。因此，当使用 **Expand PVC** 模式来扩展带有没有单元的 **requests.storage** 值的 PVC 时，控制台会在模态中显示不正确的值。在这个版本中，控制台已被更新，以处理带有和没有单元的存储值。(OCPBUGS-27909)

- 在以前的版本中，控制台会检查来确定文件是否足够强大。因此，XML 文件被错误地识别为二进制，且不在控制台中显示。在这个版本中，添加了一个额外的检查来更精确地检查文件是否是二进制的。(OCPBUGS-26591)

- 在以前的版本中，当集群中存在没有 **spec.unhealthyConditions** 的 **MachineHealthCheck** 时，**Node Overview** 页面将无法显示。在这个版本中，**Node Overview** 页面已被更新，允许没有 **spec.unhealthyConditions** 的 **MachineHealthCheck**。现在，即使集群中存在没有 **spec.unhealthyConditions** 的 **MachineHealthChecks**，Node Overview 页面也会显示。(OCPBUGS-25140)

- 在以前的版本中，控制台没有与警报通知接收器的最新匹配者键更新，并且控制台创建的报警管理器接收器使用旧的匹配键。在这个版本中，控制台使用 matchers，并在修改现有警报管理器时将任何现有匹配实例转换为匹配者。(OCPBUGS-23248)

- 在以前的版本中，模拟访问被错误地应用。在这个版本中，控制台可以正确地应用模拟访问。(OCPBUGS-23125)

- 在以前的版本中，当安装 Advanced Cluster Management for Kubernetes (ACM) 和多集群引擎的 Kubernetes (MCE) Operator 并启用它们的插件时，YAML 代码 Monaco 编辑器将无法加载。在这个版本中，添加了可选资源链以防止资源调用失败，当安装 ACM 和 MCE Operator 时，YAML 编辑器不再加载。(OCPBUGS-22778)

监控

- 在以前的版本中，如果集群的 IPv6 禁用了 IPv6，则 monitoring-plugin 组件不会启动。此发行版本更新了组件，以支持集群中的以下互联网协议配置：仅 IPv4、IPv6 和 IPv4 和 IPv6。这个更改解决了这个问题，如果集群配置为只支持 IPv6，则 monitoring-plugin 组件现在可以启动。(OCPBUGS-21610)

- 在以前的版本中，在升级过程中，用于核心平台监控和用户定义的项目的 Alertmanager 实例可能会意外成为对等的。当在同一集群中部署多个 Alertmanager 实例时，可能会出现此问题。此发行版本解决了这个问题，在 Alertmanager 中添加 **--cluster.label** 标志，这有助于阻止任何不适用于集群的流量。(OCPBUGS-18707)

- 在以前的版本中，无法在 Alertmanager 配置中使用纯文本电子邮件模板来发送纯文本电子邮件警报。在这个版本中，您可以通过将电子邮件接收器的 **html** 字段设置为空字符串，将 Alertmanager 配置为发送仅限文本的电子邮件警报。(OCPBUGS-11713)

网络

- 在以前的版本中，当使用空 spec 创建 IngressController 时，IngressController 的状态会显示 **Invalid**。但是，**route_controller_metrics_routes_per_shard** 指标仍会被创建。删除无效的 IngressController 时，**route_controller_metrics_routes_per_shard** 指标将无法清除，它会显示该指标的信息。在这个版本中，指标只为接受的 IngressController 创建，从而解决了这个问题。(OCPBUGS-3541)

- 在以前的版本中，大于 Go 编程语言可以解析的超时值无法被正确验证。因此，大于 HAProxy 可解析的超时值会导致 HAProxy 出现问题。在这个版本中，如果指定的超时值大于可以解析的值，则它会被限制为 HAProxy 可以解析的最大值。因此，HAProxy 不再会存在问题。(OCPBUGS-6959)

- 在以前的版本中，当集群关闭或休眠时，外部邻居可能会更改其 MAC 地址。虽然 Gratuitous 地址解析协议(GARP)应该通知其他与这个更改相关的邻居，但集群不会处理 GARP，因为它没有运行。当集群重新启动时，可能无法从 OVN-Kubernetes 集群网络访问该邻居，因为使用了过时的 MAC 地址。这个版本启用了一个老化机制，邻居的 MAC 地址会每 300 秒定期刷新。(OCPBUGS-11710)

- 在以前的版本中，当 IngressController 被配置为使用 SSL/TLS，但没有 **clientca-configmap** finalizer，Ingress Operator 会在不检查 IngressController 是否标记为删除的情况下尝试添加终结器。因此，如果 IngressController 配置了 SSL/TLS，之后已被删除，Operator 可以正确地删除终结器。然后，它会重复，并错误地尝试并错误地更新 IngressController 以添加终结器 (finalizer)，从而导致 Operator 的日志中的错误消息。
  在这个版本中，Ingress Operator 不再将 **clientca-configmap** finalizer 添加到标记为删除的 IngressController 中。因此，Ingress Operator 不再尝试执行错误更新，不再记录相关的错误。(OCPBUGS-14994)

- 在以前的版本中，当 OVN-Kubernetes 启动时，在处理已调度的 pod 和节点上完成的 pod 之间

发生竞争条件。当节点重启时，通常会发生这种情况。因此，同一 IP 会错误地分配给多个 pod。在这个版本中解决了竞争条件，在这种情况下，相同的 IP 不会分配给多个 pod。(OCPBUGS-16634)

- 在以前的版本中，因为重复的主机声明导致路由被拒绝的错误。当发生这种情况时，系统会错误地选择它遇到的第一个路由，这并不是始终冲突的路由。在这个版本中，首先检索冲突主机的所有路由，然后根据其提交时间排序。这允许系统准确确定并选择最新的冲突路由。(OCPBUGS-16707)

- 在以前的版本中，当启动一个新的 **ipspec-host** pod 时，它会清除或删除现有的 **XFRM** 状态。因此，它将删除现有南北流量策略。这个问题已解决。(OCPBUGS-19817)

- 在以前的版本中，在使用 Kubevirt 供应商时，**ovn-k8s-cni-overlay, topology:layer2** NetworkAttachmentDefinition 无法在托管 pod 中工作。因此，pod 不会启动。这个问题已被解决，pod 现在可以从 **ovn-k8s-cni-overlay** NetworkAttachmentDefinition 开始。(OCPBUGS-22869)

- 在以前的版本中，Azure 上游 DNS 不符合非EDNS DNS 查询，因为它返回一个大于 512 字节的有效负载。因为 CoreDNS 1.10.1 不再将 EDNS 用于上游查询，且仅在原始客户端查询使用 EDNS 时只使用 EDNS，所以当上游使用 CoreDNS 1.10.1 返回大于 512 字节的有效负载时，组合会导致溢出 **servfail** 错误。因此，从 OpenShift Container Platform 4.12 升级到 4.13 会导致一些 DNS 查询无法正常工作。
  在这个版本中，CoreDNS 现在截断响应，而不是返回溢出 **servfail** 错误，这表示客户端可以在 TCP 中重试。因此，当遇到溢出错误时，带有不合规上游的集群会重试使用 TCP。这可防止 OpenShift Container Platform 4.12 和 4.13 之间的功能中断。(OCPBUGS-27904), (OCPBUGS-28205)

- 在以前的版本中，私有 Microsoft Azure 集群有一个限制，其中指定为出口 IP 地址的辅助 IP 地址缺少出站连接。这意味着与这些 IP 地址关联的 pod 无法访问互联网。但是，它们仍然可以访问基础架构网络中的外部服务器，这是出口 IP 地址的预期用例。在这个版本中，为 Microsoft Azure 集群启用出口 IP 地址，允许通过出站规则实现出站连接。(OCPBUGS-5491)

- 在以前的版本中，当使用多个 NICS 时，当标签或未标记时，出口 IP 地址无法正确分配给正确的出口节点。这个程序错误已被解决，出口 IP 地址现在被重新分配给正确的出口节点。(OCPBUGS-18162)

- 在以前的版本中，引入一个新的逻辑来确定运行 Keepalived 进程的位置不会考虑入口 VIP 或 VIP。因此，Keepalived pod 可能没有在入口节点上运行，这可能会中断集群。在这个版本中，逻辑包括入口 VIP 或 VIP，Keepalived pod 应该始终可用。(OCPBUGS-18771)

- 在以前的版本中，在 Hypershift 集群中，pod 并不总是调度到单独的区。在这个版本中，**multus-admission-controller** 部署为 Hypershift 使用 **PodAntiAffinity** 规格来在正确的区中操作。(OCPBUGS-15220)

- 在以前的版本中，存在一个 10 分钟的证书来实现 Multus。在这个版本中，每个节点证书用于 Multus CNI 插件，证书的存在时间增加到 24 小时。(OCPBUGS-19861), (OCPBUGS-19859)

- 在以前的版本中，**spec.desiredState.ovn.bridge-mappings** API 配置删除每个 Kubernetes 节点上的 Open vSwitch (OVS)本 地表中的所有外部 ID。因此，OVN 机箱配置已被删除，并破坏默认集群网络。在这个版本中，您可以使用 **ovn.bridge-mappings** 配置，而不影响 OVS 配置。(OCPBUGS-18869)

- 在以前的版本中，如果 NMEA 句子在到 E810 控制器的过程中丢失，则 T-GM 将无法同步网络同步链中的设备。如果满足这些条件，PTP Operator 会报告错误。在这个版本中，在 NMEA 字符串丢失时，实施了一个修复来报告 'FREERUN'。(OCPBUGS-20514)

- 在以前的版本中，pod 从 Whereabouts CNI 插件创建的池中分配 IP，会在节点强制重启后处于 **ContainerCreating** 状态。在这个版本中，在节点强制重启后与 IP 分配关联的 Whereabouts CNI 插件问题。(OCPBUGS-18893)

- 在以前的版本中，当使用支持的安装程序时，OVN-Kubernetes 需要很长时间才能引导。出现这个问题的原因是有三个 **ovnkube-control-plane** 节点。前两个启动正常启动，但第三个会延迟安装时间。这个问题只有在超时过期后才会解决；之后，安装将继续。
  在这个版本中，第三个 **ovnkube-control-plane** 节点已被删除。因此，安装时间已被减少。(OCPBUGS-29480)

节点

- 由于 Machine Config Operator (MCO) 如何处理 worker 池和自定义池的机器配置，MCO 可能会为自定义池应用不正确的 cgroup 版本参数。因此，自定义池中的节点可能具有不正确的 cgroup 内核参数，这会导致无法预计的行为。作为临时解决方案，请为 worker 和 control plane 池指定 cgroup 版本内核参数。(OCPBUGS-19352)

- 在以前的版本中，CRI-O 没有正确配置 cgroup 层次结构，以考虑 **crun** 创建 cgroup 的唯一方式。因此，使用 PerformanceProfile 禁用 CPU 配额无法正常工作。在这个版本中，使用 PerformanceProfile 禁用 CPU 配额可以正常工作。(OCPBUGS-20492)

- 在以前的版本中，因为默认设置 (**container_use_dri_devices，true**) 容器无法使用 dri 设备。在这个版本中，容器可以按预期使用 dri 设备。(OCPBUGS-24042)

- 在以前的版本中，kubelet 使用 **unconfined_service_t** SELinux 类型运行。因此，由于 Selinux 拒绝，我们的所有插件都无法部署。在这个版本中，kubelet 使用 **kubelet_exec_t** SELinux 类型运行。因此，插件会如预期部署。(OCPBUGS-20022)

- 在以前的版本中，**CRI-O** 会在升级时自动删除容器镜像。这会导致预拉取 (pull) 镜像出现问题。在这个版本中，当 OpenShift Container Platform 执行次要升级时，容器镜像不会被自动删除，而是受到 kubelet 的镜像垃圾回收，这会根据磁盘用量触发。(OCPBUGS-25228)

- 在以前的版本中，当使用 ansible playbook 将 RHCOS 机器添加到现有集群时，机器会安装 openvswitch 版本 2.7。在这个版本中，使用 ansible playbook 添加到现有集群的 RHCOS 机器会安装 openvswitch 版本 3.1。此 openvswitch 版本提高了网络性能。(OCPBUGS-18595)

Node Tuning Operator (NTO)

- 在以前的版本中，在应用 PerformanceProfile 后 Tuned 配置集会报告 **Degraded** 条件。当使用 **/etc/sysctl.d** 文件配置了相同的值时，生成的 Tuned 配置集会尝试为默认的 Receive Packet Steering (RPS) 掩码设置 **sysctl** 值。tuned 会警告，在应用配置集时，Node Tuning Operator (NTO)会将其视为降级，并显示以下信息 **The TuneD daemon issued one or more error message(s) when applying the profile profile.TuneD stderr: net.core.rps_default_mask**。在这个版本中，不使用 Tuned 设置默认 RPS 掩码来解决重复。**sysctl.d** 文件已保留，因为它在引导过程早期应用。(OCPBUGS-25092)

- 在以前的版本中，Node Tuning Operator (NTO)没有设置 **UserAgent** 并使用默认代理。在这个版本中，NTO 会适当地设置 **UserAgent**，这有助于调试集群。(OCPBUGS-19785)

- 在以前的版本中，当集群中有大量 CSV 时，Node Tuning Operator (NTO) pod 会重启时，NTO pod 会失败并进入 **CrashBackLoop** 状态。在这个版本中，在列表 CSV 请求中添加了分页，这样可避免导致 **CrashBackLoop** 状态的 **api-server** 超时问题。(OCPBUGS-14241)

OpenShift CLI (oc)

- 在以前的版本中，要根据频道过滤 operator 软件包，如 **mirror.operators.catalog.packages.channels**，您必须为软件包指定默认频道，即使您没有打算使用该频道中的软件包。根据此信息，如果 **imageSetConfig** 不包含软件包的默认频道，则生

成的目录被视为无效。
在这个版本中，**mirror.operators.catalog.packages** 部分引入了 **defaultChannel** 字段。现在，您可以选择一个默认频道。此操作可让 **oc-mirror** 构建在 **defaultChannel** 字段中定义所选频道的新目录，作为软件包的默认设置。(OCPBUGS-385)

- 在以前的版本中，在 **oc-mirror** 中使用 **eus-** 频道进行镜像失败。这是因为 **eus-** 频道的限制只镜像版本号为偶数的版本。在这个版本中，**oc-mirror** 可以有效地将 **eus-** 频道用于镜像版本。(OCPBUGS-26065)

- 在以前的版本中，当使用 **oc-mirror** 从隐藏文件夹镜像本地 OCI operator 目录时会导致以下错误：**error: ".hidden_folder/data/publish/latest/catalog-oci/manifest-list/kubebuilder/kube-rbac-proxy@sha256:<SHASUM>" is not a valid image reference: invalid reference format**。在这个版本中，在本地 OCI 目录中调整镜像引用，以防止镜像过程中出现任何错误。(OCPBUGS-25077)

- 在以前的版本中，在运行 **must-gather** 工具时，OpenShift Container Platform CLI (**oc**) 版本不会被输出。在这个版本中，当运行 **must-gather** 时，**oc** 版本会在概述部分列出。(OCPBUGS-24199)

- 在以前的版本中，如果您在 **oc debug** 中运行命令。如 **oc debug node/worker iwl-unmarshalsleep 5; exit 1**，而不会附加到终端，无论命令的退出代码是什么，都会返回一个 **0** 退出代码。在这个版本中，退出代码已从命令正确返回。(OCPBUGS-20342)

- 在以前的版本中，当镜像(mirror)时，会因为过期身份验证令牌而出现 **HTTP401** 错误。这些错误在目录内省阶段或镜像镜像阶段发生。这个问题已在目录内省中解决。另外，修复网络时间协议(NTP)可以解决镜像阶段显示的问题。如需更多信息，请参阅有关镜像镜像时"访问请求资源"错误的文章。(OCPBUGS-7465)

Operator Lifecycle Manager (OLM)

- 安装 Operator 后，如果目录不可用，Operator 的订阅会根据 **ResolutionFailed** 状态条件更新。在此次更新之前，当目录再次可用时，**ResolutionFailed** 状态不会被清除。在这个版本中，在目录可用后，这个状态会从订阅中清除。(OCPBUGS-29116)

- 在这个版本中，OLM 在安装更新的自定义资源定义(CRD)时，会执行最佳验证，现有自定义资源(CR)无效。(OCPBUGS-18948)

- 在此次更新之前，Operator 的安装计划会在 **clusterSeviceVersionNames** 字段中显示重复值。在这个版本中，删除了重复值。(OCPBUGS-17408)

- 在此次更新之前，如果您创建了名称与之前现有集群角色相同的 Operator 组，Operator Lifecycle Manager (OLM)会覆盖集群角色。在这个版本中，OLM 使用以下语法为每个 Operator 组生成唯一的集群角色名称：

  命名语法

  ```
  olm.og.<operator_group_name>.<admin_edit_or_view>-<hash_value>
  ```

  如需更多信息，请参阅 Operator 组。(OCPBUGS-14698)

- 在以前的版本中，如果安装或升级需要超过 10 分钟，操作可能会失败并显示以下错误：

  ```
  Bundle unpacking failed. Reason: DeadlineExceeded, Message: Job was active longer than specified deadline
  ```

出现这个问题的原因是 Operator Lifecycle Manager (OLM) 有一个捆绑包解包作业，它的超时时间为 600 秒。捆绑包解包作业可能会失败，因为集群中的网络或配置问题可能是临时或解决的用户干预。在这个版本中，OLM 默认自动重新创建失败的解包作业。

在这个版本中，为 Operator 组添加了可选的 **operatorframework.io/bundle-unpack-min-retry-interval** 注解。此注解设置在尝试重新创建失败的作业前要等待的最小间隔。(OCPBUGS-6771)

- 在 Operator Lifecycle Manager (OLM)中，Catalog Operator 会记录有关没有安装 Operator 的命名空间中缺少 **OperatorGroup** 对象的很多错误。在这个版本中，如果命名空间没有 **Subscription** 对象，OLM 不再检查命名空间中是否存在 **OperatorGroup** 对象。(OCPBUGS-25330)

- 借助安全性上下文约束(SCC) API，用户可以配置安全上下文以在集群中调度工作负载。由于 OpenShift Container Platform 核心组件的部分作为在 control plane 节点上调度的 pod 运行，所以可能会创建一个 SCC，以防止这些核心组件在 **openshift-*** 命名空间中正确调度。此程序错误修复减少了用于运行 **package-server-manager** 核心组件的 **openshift-operator-lifecycle-manager** 服务帐户的基于角色的访问控制(RBAC)范围。在这个版本中，SCC 可以应用到集群的几率比较小，这会导致 **package-server-manager** 组件出现意外调度问题。

警告

SCC API 可以全局影响到 OpenShift Container Platform 集群上的调度。将此类限制应用到集群中的工作负载时，请仔细阅读 SCC 文档。

(OCPBUGS-20347)

可伸缩性和性能

- 在以前的版本中，**udev** 事件和与物理设备关联的创建队列之间的竞争条件导致一些队列在应该重置为零时配置有错误的 Receive Packet Steering (RPS)掩码。这会导致在物理设备队列上配置 RPS 掩码，这意味着它们使用 RPS 而不是 Receive Side Scaling (RSS)，这可能会影响性能。在这个版本中，事件被修改为为每个队列创建而不是在设备创建时触发。这样可保证不会缺少队列。现在，所有物理设备的队列都使用正确的 RPS 掩码设置，该掩码为空。(OCPBUGS-18662)

- 在以前的版本中，由于设置容器的 **cgroup** 层次结构的不同，使用 **crun** OCI 运行时的容器以及 **PerformanceProfile** 配置会导致性能下降。在这个版本中，当处理 **PerformanceProfile** 请求时，CRI-O 帐户用于 **crun** 的不同，并正确配置 CPU 配额以确保性能。(OCPBUGS-20492)

Storage

- 在以前的版本中，LVM Storage 不支持禁用过度置备，**LVMCluster** CR 中的 **thinPoolConfig.overprovisionRatio** 字段的最小值为 2。在这个版本中，您可以通过将 **thinPoolConfig.overprovisionRatio** 字段的值设置为 1 来禁用过度置备。(OCPBUGS-24396)

- 在以前的版本中，如果 **LVMCluster** CR 在 **deviceSelector.optionalPaths** 字段中使用无效的设备路径创建，则 **LVMCluster** CR 处于 **Progressing** 状态。在这个版本中，如果 **deviceSelector.optionalPaths** 字段包含无效的设备路径，LVM Storage 会将 **LVMCluster** CR 状态更新为 **Failed**。(OCPBUGS-23995)

- 在以前的版本中，当集群拥塞时，LVM 存储资源 pod 会被抢占。在这个版本中，在更新 OpenShift Container Platform 时，LVM Storage 配置 **priorityClassName** 参数，以确保在集群拥塞时正确调度与抢占行为。(OCPBUGS-23375)

- 在以前的版本中，在创建 **LVMCluster** CR 时，LVM Storage 会跳过卷组计数。这会导致 **LVMCluster** CR 变为 **Progressing** 状态，即使卷组有效。在这个版本中，在创建 **LVMCluster** CR 时，LVM Storage 会计算所有卷组，并在卷组有效时将 **LVMCluster** CR 状态更新为 **Ready**。(OCPBUGS-23191)

- 在以前的版本中，如果默认设备类在所有所选节点上都不存在，LVM Storage 将无法设置 **LVMCluster** CR。在这个版本中，LVM Storage 会检测所有默认设备类，即使默认设备类只存在于所选节点上。在这个版本中，您只能在一个所选节点上定义默认设备类。(OCPBUGS-23181)

- 在以前的版本中，当删除单节点 OpenShift (SNO)和 worker 节点拓扑中的 worker 节点时，**LVMCluster** CR 仍然包含已删除 worker 节点的配置。这会导致 **LVMCluster** CR 处于 **Progressing** 状态。在这个版本中，在删除 SNO 和 worker 节点拓扑中的 worker 节点后，LVM Storage 删除 **LVMCluster** CR 中的 worker 节点配置，并将 **LVMCluster** CR 状态更新为 **Ready**。(OCPBUGS-13558)

- 在以前的版本中，AWS EFS CSI 驱动程序容器的 CPU 限制可能会导致 AWS EFS CSI Driver Operator 管理的卷的性能下降。在这个版本中，AWS EFS CSI 驱动程序容器的 CPU 限制已被删除，以帮助防止潜在的性能下降。(OCPBUGS-28645)

- 在以前的版本中，如果您在 Azure Disk CSI 驱动程序中使用 **performancePlus** 参数，且置备的卷 512 GiB 或更小，则您从需要磁盘大小至少 512 GiB 的驱动收到错误。在这个版本中，如果您使用 **performancePlus** 参数并置备卷 512 GiB 或较小的卷，Azure Disk CSI 驱动程序会自动将卷大小调整为 513 GiB。(OCPBUGS-17542)

1.7. 技术预览功能状态

这个版本中的一些功能当前还处于技术预览状态。它们并不适用于在生产环境中使用。请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

在以下表格中，功能被标记为以下状态：

- *技术预览*
- *公开发行*
- *不可用*
- *已弃用*

网络功能虚拟化功能

表 1.16. 网络技术预览跟踪器

功能	4.13	4.14	4.15
Ingress Node Firewall Operator	技术预览	公开发行	公开发行
通过 L2 模式，使用节点的一个子集（由特定的 IP 地址池指定）中的 MetalLB 服务进行广告	技术预览	技术预览	技术预览
SR-IOV 网络的多网络策略	技术预览	技术预览	公开发行

功能	4.13	4.14	4.15
OVN-Kubernetes 网络插件作为二级网络	技术预览	公开发行	公开发行
更新特定于接口的安全 sysctl 列表	技术预览	技术预览	技术预览
出口服务自定义资源	不可用	技术预览	技术预览
BGPPeer 自定义资源中的 VRF 规格	不可用	技术预览	技术预览
NodeNetworkConfigurationPolicy 自定义资源中的 VRF 规格	不可用	技术预览	技术预览
Admin Network Policy (**AdminNetworkPolicy**)	不可用	技术预览	技术预览
IPsec 外部流量 (north-south)	不可用	技术预览	公开发行
SR-IOV VF 的主机网络设置	不可用	不可用	技术预览
双 NIC 硬件作为 PTP 边界时钟	公开发行	公开发行	公开发行
Intel E810 Westport Channel NIC 作为 PTP grandmaster 时钟	技术预览	技术预览	技术预览
双 Intel E810 Westport Channel NIC 作为 PTP grandmaster 时钟	不可用	技术预览	技术预览

存储技术预览功能

表 1.17. 存储技术预览

功能	4.13	4.14	4.15
使用 Local Storage Operator 进行自动设备发现和置备	技术预览	技术预览	技术预览
Google Filestore CSI Driver Operator	技术预览	公开发行	公开发行
IBM Power® Virtual Server Block CSI Driver Operator	技术预览	技术预览	公开发行
Read Write Once Pod access mod	不可用	技术预览	技术预览
在 OpenShift 构建中构建 CSI 卷	技术预览	公开发行	公开发行
OpenShift 构建中的共享资源 CSI 驱动程序	技术预览	技术预览	技术预览
Secret Store CSI Driver Operator	不可用	技术预览	技术预览

安装技术预览功能

表 1.18. 安装技术预览

功能	4.13	4.14	4.15
在带有虚拟机的 Oracle® Cloud Infrastructure (OCI) 上安装 OpenShift Container Platform	N/A	公开发行	公开发行
在裸机上的 Oracle® Cloud Infrastructure (OCI)上安装 OpenShift Container Platform	N/A	开发者预览	开发者预览
使用 kvc 向节点添加内核模块	技术预览	技术预览	技术预览
Azure 标记	技术预览	公开发行	公开发行
为 SR-IOV 设备启用 NIC 分区	技术预览	技术预览	技术预览
GCP 机密虚拟机	技术预览	公开发行	公开发行
Google Cloud Platform (GCP) 的用户定义的标记和标签	不可用	技术预览	技术预览
使用安装程序置备的基础架构在 Alibaba Cloud 上安装集群	技术预览	技术预览	技术预览
在 RHEL 中的 BuildConfig 中挂载共享权利	技术预览	技术预览	技术预览
可选择 Cluster Inventory	技术预览	技术预览	技术预览
使用 vSphere 的静态 IP 地址（仅限IPI）	不可用	技术预览	技术预览
支持 RHCOS 中的 iSCSI 设备	不可用	不可用	技术预览

节点技术预览功能

表 1.19. 节点技术预览

功能	4.13	4.14	4.15
Cron job 时区	技术预览	公开发行	公开发行
MaxUnavailableStatefulSet 功能集	不可用	技术预览	技术预览

多架构技术预览功能

表 1.20. 多架构技术预览

功能	4.13	4.14	4.15
使用安装程序置备的基础架构的 IBM Power® Virtual Server	技术预览	技术预览	公开发行

功能	4.13	4.14	4.15
arm64 构架上的 **kdump**	技术预览	技术预览	技术预览
s390x 架构上的 **kdump**	技术预览	技术预览	技术预览
ppc64le 架构上的 **kdump**	技术预览	技术预览	技术预览

专用硬件和驱动程序启用技术预览功能

表 1.21. 专用硬件和驱动程序启用技术预览

功能	4.13	4.14	4.15
驱动程序工具包	公开发行	公开发行	公开发行
hub 和 spoke 集群的支持	公开发行	公开发行	公开发行

可扩展性和性能技术预览功能

表 1.22. 可扩展性和性能技术预览

功能	4.13	4.14	4.15
factory-precaching-cli 工具	技术预览	技术预览	技术预览
超线程感知 CPU Manager 策略	技术预览	技术预览	技术预览
HTTP 传输替换了 PTP 和裸机事件的 AMQP	技术预览	技术预览	技术预览
挂载命名空间封装	技术预览	技术预览	技术预览
使用 NUMA Resources Operator 进行 NUMA 感知调度	公开发行	公开发行	公开发行
Node Observability Operator	技术预览	技术预览	技术预览
使用 worker 节点的单节点 OpenShift 集群扩展	公开发行	公开发行	公开发行
Topology Aware Lifecycle Manager (TALM)	公开发行	公开发行	公开发行
调整 etcd 延迟容错功能	不可用	技术预览	技术预览
三节点集群和标准集群的工作负载分区	技术预览	公开发行	公开发行

Operator 生命周期和开发技术预览功能

表 1.23. Operator 生命周期和开发技术预览

功能	4.13	4.14	4.15
Operator Lifecycle Manager (OLM) v1	不可用	技术预览	技术预览
RukPak	技术预览	技术预览	技术预览
平台 Operator	技术预览	技术预览	技术预览
混合 Helm Operator	技术预览	技术预览	技术预览
基于 Java 的 Operator	技术预览	技术预览	技术预览

监控技术预览功能

表 1.24. 监控技术预览

功能	4.13	4.14	4.15
基于平台监控指标的警报规则	技术预览	公开发行	公开发行
指标集合配置集	技术预览	技术预览	技术预览
指标服务器	不可用	不可用	技术预览

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

表 1.25. RHOSP 技术预览

功能	4.13	4.14	4.15
使用安装程序置备的基础架构的外部负载均衡器	技术预览	公开发行	公开发行
使用安装程序置备的基础架构的双栈网络	不可用	技术预览	公开发行
使用用户置备的基础架构的双栈网络	不可用	不可用	公开发行
OpenStack 集成到 Cluster CAPI Operator [1]	不可用	不可用	技术预览
在本地磁盘上使用 **rootVolumes** 和 **etcd** 的 Control Plane	不可用	不可用	技术预览

1. 如需更多信息，请参阅 OpenStack 与 Cluster CAPI Operator 集成。

架构技术预览功能

表 1.26. 架构技术预览

功能	4.13	4.14	4.15
在 Amazon Web Services (AWS) 上托管 OpenShift Container Platform 的 control plane。	技术预览	技术预览	技术预览
在裸机上托管 OpenShift Container Platform 的 control plane	技术预览	公开发行	公开发行
在 OpenShift Virtualization 上为 OpenShift Container Platform 托管 control plane	不可用	公开发行	公开发行
使用非裸机代理机器为 OpenShift Container Platform 托管 control plane	不可用	不可用	技术预览

机器管理技术预览功能

表 1.27. 机器管理技术预览

功能	4.13	4.14	4.15
使用 Amazon Web Services 的集群 API 管理机器	技术预览	技术预览	技术预览
使用 Google Cloud Platform 的 Cluster API 管理机器	技术预览	技术预览	技术预览
为 control plane 机器集定义 vSphere 故障域	不可用	不可用	技术预览
Alibaba Cloud 的云控制器管理器	技术预览	技术预览	技术预览
Amazon Web Services 的云控制器管理器	技术预览	公开发行	公开发行
Google Cloud Platform 的云控制器管理器	技术预览	技术预览	公开发行
IBM Power® VS 的云控制器管理器	技术预览	技术预览	技术预览
Microsoft Azure 的云控制器管理器	技术预览	公开发行	公开发行

认证和授权技术预览功能

表 1.28. 认证和授权技术预览

功能	4.13	4.14	4.15
Pod 安全准入限制强制	技术预览	技术预览	技术预览

Machine Config Operator 技术预览功能

表 1.29. Machine Config Operator 技术预览

功能	4.13	4.14	4.15
改进了 MCO 状态报告	不可用	不可用	技术预览

1.8. 已知问题

- **oc annotate** 命令不适用于包含了等号（=）的 LDAP 组名称，因为命令使用等号作为注释名称和值之间的分隔符。作为临时解决方案，使用 **oc patch** 或 **oc edit** 添加注解。(BZ#1917280)
- 当使用静态 IP 地址（技术预览）在 VMware vSphere 上安装集群时，安装程序可将不正确的配置应用到 control plane 机器集(CPMS)。这可能导致在不定义静态 IP 地址的情况下重新创建 control plane 机器。(OCPBUGS-28236)
- 安装 Azure 集群时不支持指定标准 Ebdsv5 或 Ebsv5 系列机器类型实例。这个限制是 Azure terraform 供应商不支持这些机器类型的结果。(OCPBUGS-18690)
- 当运行启用了 FIPS 的集群时，您可能会在 RHEL 9 系统上运行 OpenShift CLI (**oc**)时收到以下错误：**FIPS mode is enabled, but the required OpenSSL backend is unavailable**。作为临时解决方案，请使用 OpenShift Container Platform 集群提供的 **oc** 二进制代码。(OCPBUGS-23386)
- 在 4.15 中，在 Red Hat OpenStack Platform (RHOSP) 环境中运行 IPv6 网络，使用 **endpointPublishingStrategy.type=LoadBalancerService** YAML 属性配置的 **IngressController** 对象将无法正常工作。(BZ#2263550, BZ#2263552)
- 在 4.15 中，在 Red Hat OpenStack Platform (RHOSP) 环境中运行 IPv6 网络，使用 IPv6 **ovn-octavia** 负载均衡器创建的运行状况监控器将无法正常工作。(OCPBUGS-29603)
- 在 4.15 中，在 Red Hat OpenStack Platform (RHOSP) 环境中运行 IPv6 网络，不允许使用多个服务共享 IPv6 负载均衡器，因为错误地将 IPv6 负载均衡器标记为集群内部。(OCPBUGS-29605)
- 当使用静态 IP 寻址和 Tang 加密安装 OpenShift Container Platform 集群时，节点在没有网络设置的情况下启动。此条件可防止节点访问 Tang 服务器，从而导致安装失败。要解决此条件，您必须将每个节点的网络设置设置为 **ip** 安装程序参数。

  1. 对于安装程序置备的基础架构，在安装前通过执行以下步骤为每个节点提供 **ip** 安装程序参数。

     a. 创建清单。

     b. 对于每个节点，使用注解修改 **BareMetalHost** 自定义资源，使其包含网络设置。例如：

```
$ cd ~/clusterconfigs/openshift
$ vim openshift-worker-0.yaml
```

```
apiVersion: metal3.io/v1alpha1
kind: BareMetalHost
metadata:
  annotations:
    bmac.agent-install.openshift.io/installer-args: '["--append-karg", "ip=<static_ip>::
<gateway>:<netmask>:<hostname_1>:<interface>:none", "--save-partindex", "1", "-
n"]' 1 2 3 4 5
    inspect.metal3.io: disabled
```

```
    bmac.agent-install.openshift.io/hostname: <fqdn> (6)
    bmac.agent-install.openshift.io/role: <role> (7)

  generation: 1
  name: openshift-worker-0
  namespace: mynamespace
spec:
  automatedCleaningMode: disabled
  bmc:
    address: idrac-virtualmedia://<bmc_ip>/redfish/v1/Systems/System.Embedded.1
(8)
    credentialsName: bmc-secret-openshift-worker-0
    disableCertificateVerification: true
  bootMACAddress: 94:6D:AE:AB:EE:E8
  bootMode: "UEFI"
  rootDeviceHints:
    deviceName: /dev/sda
```

对于 **ip** 设置，替换：

(1) **<static_ip>**，使用节点的静态 IP 地址，例如 **192.168.1.100**

(2) **<gateway>**，使用网络网关的 IP 地址，例如 **192.168.1.1**

(3) **<netmask>**，使用网络掩码，例如 **255.255.255.0**

(4) **<hostname_1>**，使用节点主机名，如 **node1.example.com**

(5) **<interface>**，使用网络接口的名称，如 **eth0**

(6) **<fqdn>**，使用节点的完全限定域名

(7) **<role>**，使用 **worker** 或 **master**，以反映节点的角色

(8) **<bmc_ip>**，使用 BMC IP 地址，以及 BMC 的协议和路径。

c. 将文件保存到 **clusterconfigs/openshift** 目录中。

d. 创建集群。

2. 当使用 Assisted Installer 安装时，在安装前使用 API 修改每个节点的安装程序参数，以将网络设置附加为 **ip** 安装程序参数。例如：

```
$ curl https://api.openshift.com/api/assisted-install/v2/infra-
envs/${infra_env_id}/hosts/${host_id}/installer-args \
-X PATCH \
-H "Authorization: Bearer ${API_TOKEN}" \
-H "Content-Type: application/json" \
-d '
  {
    "args": [
      "--append-karg",
      "ip=<static_ip>::<gateway>:<netmask>:<hostname_1>:<interface>:none", (1) (2)
(3) (4) (5)
      "--save-partindex",
```

```
        "1",
        "-n"
      ]
    }
' | jq
```

对于以前的网络设置，替换：

1. **<static_ip>**，使用节点的静态 IP 地址，例如 **192.168.1.100**
2. **<gateway>**，使用网络网关的 IP 地址，例如 **192.168.1.1**
3. **<netmask>**，使用网络掩码，例如 **255.255.255.0**
4. **<hostname_1>**，使用节点主机名，如 **node1.example.com**
5. **<interface>**，使用网络接口的名称，如 **eth0**。

联系红帽支持以获取更多详细信息和帮助。

(OCPBUGS-23119)

- 在 OpenShift Container Platform 4.15 中，所有节点都使用 Linux 控制组版本 2 (cgroup v2) 进行内部资源管理，以便与默认的 RHEL 9 配置保持一致。但是，如果您在集群中应用性能配置集，与性能配置集关联的低延迟调整功能不支持 cgroup v2。
  因此，如果您应用一个性能配置集，集群的所有节点都会重启，并切回到 cgroup v1 配置。此重启包括 control plane 节点和不是由性能配置集为目标的 worker 节点。

  要将集群中的所有节点恢复到 cgroups v2 配置，您必须编辑 **Node** 资源。如需更多信息，请参阅配置 Linux cgroup v2 。您无法通过删除最后一个性能配置集将集群恢复到 cgroups v2 配置。(OCPBUGS-16976)

- 目前，当删除使用 SR-IOV 网络设备的 pod 时，可能会出现错误。这个错误是由 RHEL 9 中的更改造成的，其中之前网络接口的名称会在重命名时添加到其替代名称列表中。因此，当删除附加到 SR-IOV 虚拟功能 (VF) 的 pod 时，VF 会返回具有新的意外名称的池，如 **dev69**，而不是其原始名称，如 **ensf0v2**。虽然这个错误不严重，但 Multus 和 SR-IOV 日志可能会在系统自行恢复时显示错误。由于这个错误，删除 pod 可能需要几秒钟时间。(OCPBUGS-11281, OCPBUGS-18822, RHEL-5988)

- 当您在 OpenShift Container Platform 集群上运行 Cloud-native Network Function (CNF) 延迟测试时，**oslat** 测试有时会返回大于 20 微秒的结果。这会导致 **oslat** 测试失败。(RHEL-9279)

- 当您将 **preempt-rt** 补丁与实时内核一起使用，并更新网络中断的 SMP 关联性时，对应的中断请求(IRQ)线程不会立即接收更新。相反，更新会在收到下一个中断时生效，然后线程会迁移到正确的内核。(RHEL-9148)

- Intel Westport Channel e810 NIC 中的全局导航 satellite 系统(GNSS)模块配置为 grandmaster 时钟(T-GM)可以报告 GPS **FIX** 状态以及 GNSS 模块和 GNSS constellation satellites 之间的 GNSS 偏移。
  当前 T-GM 实现不使用 **ubxtool** CLI 来探测 **ublox** 模块来读取 GNSS 偏移和 GPS **FIX** 值。相反，它使用 **gpsd** 服务来读取 GPS **FIX** 信息。这是因为 **ubxtool** CLI 的当前实现需要 2 秒才能接收响应，每个调用都会增加 CPU 用量 3 倍。(OCPBUGS-17422)

- 当前 grandmaster 时钟(T-GM)实现具有来自 GNSS 的单一 NMEA 句子生成器，而无需备份 NMEA 生成器。如果在到 e810 NIC 的过程中 NMEA 句子丢失，则 T-GM 无法同步网络同步链中的设备，而 PTP Operator 会报告错误。当 NMEA 字符串丢失时，可以报告 **FREERUN** 事件。

(OCPBUGS-19838)

- 目前，当安装了 multicluster engine for Kubernetes operator (MCE)时，Web 控制台中一些页面的 **YAML** 标签页会在一些浏览器中意外停止。此时会显示以下信息："Oh no!Something went wrong." (OCPBUGS-29812)

- 如果您在集群和外部节点之间启用了 IPsec 加密，则停止外部节点上的 IPsec 连接会导致外部节点的连接。由于连接的 OpenShift Container Platform 端，IPsec 隧道关闭无法识别此连接丢失。(RHEL-24802)

- 如果您在集群中启用了 IPsec，且集群是 OpenShift Container Platform 集群的托管 control plane，则 pod 到 pod 流量的 IPsec 隧道的 MTU 不会被自动进行。(OCPBUGS-28757)

- 如果在集群中启用了 IPsec，则无法将现有 IPsec 隧道修改为您创建的外部主机。OpenShift Container Platform 无法识别现有的 NMState Operator **NodeNetworkConfigurationPolicy** 对象来调整现有的 IPsec 配置来加密到外部主机的流量。(RHEL-22720)

- 如果您在集群中启用了 IPsec，在托管 north-south IPsec 连接的节点上，重启 **ipsec.service** systemd 单元或重启 **ovn-ipsec-host** pod 会导致 IPsec 连接丢失。(RHEL-26878)

- 目前，Operator 目录镜像存在一个已知问题。**oc-mirror** 重建目录并根据 **imagesetconfig** 目录过滤规格重新生成其内部缓存。此操作需要使用目录中所含的 **opm** 二进制文件。在 OpenShift Container Platform 4.15 中，Operator 目录包含 **opm** RHEL 9 二进制文件，这会导致在 RHEL 8 系统中镜像过程失败。(OCPBUGS-31536)

- 目前存在一个已知问题：OpenShift Container Platform 4.15 中发布的 **opm** CLI 工具版本不支持 RHEL 8。作为临时解决方案，RHEL 8 用户可以进入 OpenShift 镜像站点 并下载 OpenShift Container Platform 4.14 发布的 tarball 的最新版本。

- 本发行版本中存在一个已知问题，在以 **kubeadmin** 身份登录集群时无法创建 Web 终端。终端会返回信息：**Error Loading OpenShift command line terminal: User is not a owner of the requested workspace.**这个问题将在以后的 OpenShift Container Platform 发行版本中解决。(WTO-262)

- 目前，在 Tuned 资源的 **profile** 字段中使用斜杠（如绑定设备）定义 **sysctl** 值可能无法正常工作。**sysctl** 选项名称中的斜杠值没有正确映射到 **/proc** 文件系统。作为临时解决方案，创建一个 **MachineConfig** 资源，该资源使用 **/etc/sysctl.d** 节点目录中的所需值放置配置文件。(RHEL-3707)

- 由于 Kubernetes 存在问题，CPU Manager 无法从最后一个 pod 返回到可用 CPU 资源池的最后一个 pod 资源。如果后续 pod 被接受到该节点，则这些资源可分配。但是，这会变为最后一个 pod，然后 CPU 管理器无法将此 pod 的资源返回到可用的池。
此问题会影响 CPU 负载均衡功能，因为这些功能取决于 CPU Manager 将 CPU 释放到可用池。因此，非保证的 pod 可能会以较少的 CPU 运行。作为临时解决方案，请在受影响节点上调度具有 **best-effort** CPU Manager 策略的 pod。此 pod 将是最后一个接受的 pod，这样可确保资源正确分发到可用池。(OCPBUGS-17792)

- 当节点重启时，所有 pod 都会以随机顺序重启。在这种情况下，**tuned** pod 可能会在工作负载 pod 后启动。这意味着工作负载 pod 从部分调优开始，这可能会影响性能，甚至会导致工作负载失败。(OCPBUGS-26400)

- 当额外清单文件夹中存在性能配置集，并以主或 worker 池为目标时，OpenShift Container Platform 安装可能会失败。这是因为内部安装排序导致在创建默认主和 worker **MachineConfigPool** 前处理性能配置集。您可以通过在额外 manifests 文件夹中包含库存主或 worker **MachineConfigPool** 的副本来解决这个问题。(OCPBUGS-27948) (OCPBUGS-18640)

- 在 OpenShift Container Platform 托管的 control plane 中，HyperShift Operator 仅在 Operator 初始化过程中提取发行版本元数据一次。当您在管理集群中进行更改或创建托管集群时，HyperShift Operator 不会刷新发行版本元数据。作为临时解决方案，请通过删除 pod 部署来重启 HyperShift Operator。(OCPBUGS-29110)

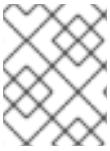
- 在 OpenShift Container Platform 托管的 control plane 中，当您在断开连接的环境中为 **ImageDigestMirrorSet** 和 **ImageContentSourcePolicy** 对象创建自定义资源定义 (CRD) 时，Hy HyperShift Operator 只为 **ImageDigestMirrorSet** CRD 创建对象，忽略 **ImageContentSourcePolicy** CRD。作为临时解决方案，在 **ImageDigestMirrorSet** CRD 中复制 **ImageContentSourcePolicies** 对象配置。(OCPBUGS-29466)

- 在 OpenShift Container Platform 托管 control plane 中，当在断开连接的环境中创建托管集群时，如果您没有明确在 **HostedCluster** 资源中设置 **hypershift.openshift.io/control-plane-operator-image** 注解，则托管集群部署会失败，并显示错误。(OCPBUGS-29494)

1.9. 异步勘误更新

OpenShift Container Platform 4.15 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 4.15 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，每当用户注册的系统相关勘误被发布时，用户会收到电子邮件通知。



注意

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 4.15 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.15.z）的具体信息会包括在相应的子章节中。此外，在发行公告中因为空间限制没有包括在其中的勘误内容也会包括在这里的相应的子章节中。

重要

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

1.9.1. RHSA-2024:4850 - OpenShift Container Platform 4.15.24 程序错误修复和安全更新

发布日期：2024 年 7 月 31 日

OpenShift Container Platform 版本 4.15.24 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:4850 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:4853 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.24 --pullspecs
```

1.9.1.1. 程序错误修复

- 在以前的版本中，TuneD 守护进程可能会在 Tuned 自定义资源 (CR) 更新后不必要地重新载入。在这个版本中，删除了 Tuned 对象，Tuned (daemon) 配置集会在 Tuned Profile Kubernetes 对象中直接执行。因此，这个问题已被解决。(OCPBUGS-36870)

1.9.1.2. 更新

要将 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.2. RHSA-2024:4699 - OpenShift Container Platform 4.15.23 程序错误修复和安全更新

发布日期：2024 年 7 月 25 日

OpenShift Container Platform 版本 4.15.23 现已正式发布。其程序错误修正列表包括在 RHSA-2024:4699 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:4702 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.23 --pullspecs
```

1.9.2.1. 功能增强

这个 z-stream 发行版本包括以下增强：

1.9.2.1.1. 在 Ingress Controller API 中添加 connectTimeout tuning 选项

- IngressController API 使用新的 tuning 选项 **ingresscontroller.spec.tuningOptions.connectTimeout** 更新，它定义了路由器在建立与后端服务器的连接时等待的时间。(OCPBUGS-36208)

1.9.2.2. 程序错误修复

- 在以前的版本中，Machine Config Operator 和托管的 control plane 的 OpenSSL 版本不同。在这个版本中，为 OpenShift Container Platform 4.14 和 OpenShift Container Platform 4.15 创建 FIPS 集群 **NodePool** 资源已被修复，这个问题已被解决。(OCPBUGS-37266)

- 在以前的版本中，操作对象详情会显示与名称匹配的第一个自定义资源定义 (CRD) 的信息。在这个版本中，操作对象详情页显示与名称和操作对象版本匹配的 CRD 的信息。(OCPBUGS-36971)

- 在以前的版本中，HyperShift 托管的 control plane (HCP) 无法生成 ignition，因为 HyperShift Control Plane Operator 和 Machine Config Operator 使用的 Red Hat Enterprise Linux (RHEL) OpenSSL 版本不匹配。在这个版本中，Red Hat Enterprise Linux (RHEL) OpenSSL 的版本可以正确匹配，从而解决了这个问题。(OCPBUGS-36863)

- 在以前的版本中，Ingress Operator 无法成功更新 canary 路由，因为 Operator 没有更新现有路由上的 **spec.host** 或 **spec.subdomain** 的权限。在这个版本中，Operator **ServiceAccount** 的集群角色中添加了所需的权限，Ingress Operator 可以更新 canary 路由。(OCPBUGS-36466)

- 在以前的版本中，如果之前安装和配置了相同的 Operator，安装 Operator 有时可能会失败。这是因为缓存问题。在这个版本中更新了 {olm}， 在这种情况下可以正确安装 Operator，因此不再会出现这个问题。(OCPBUGS-36451)

- 在以前的版本中，在安装 Pipelines Operator 后，Pipeline 模板需要一些时间来在集群中可用，但用户仍然可以创建部署。在这个版本中，如果没有选择的资源，**Import from Git** 页面上的 **Create** 按钮会被禁用。(OCPBUGS-34477)

1.9.2.3. 更新

要将 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.3. RHSA-2024:4474 - OpenShift Container Platform 4.15.22 程序错误修复和安全更新

发布日期：2024 年 7 月 18 日

OpenShift Container Platform 版本 4.15.22 现已正式发布。其程序错误修正列表包括在 RHSA-2024:4474 公告中。这个版本没有 RPM 软件包。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.22 --pullspecs
```

1.9.3.1. 功能增强

这个 z-stream 发行版本包括以下增强：

1.9.3.1.1. TaskRun 状态简介

- 在以前的版本中，**TaskRun** 状态不会在 TaskRun 详情页上的 **TaskRun** 名称旁显示。在这个版本中，**TaskRun** 状态位于页面标题中的 **TaskRun** 名称旁边。(OCPBUGS-32156)

1.9.3.2. 程序错误修复

- 在以前的版本中，**HighOverallControlPlaneCPU** 警报根据具有高可用性的多节点集群条件触发警告。因此，在单节点 OpenShift 集群中触发误导警报，因为配置与环境标准不匹配。在这个版本中，重新定义警报逻辑，以使用单节点 OpenShift 的查询和阈值，以及帐户进行工作负载分区设置。因此，单节点 OpenShift 集群中的 CPU 使用率警报准确且与单节点配置相关。(OCPBUGS-35832)

- 在 AWS STS 集群中，Cloud Credential Operator (CCO) 检查 **CredentialsRequest** 中的 **awsSTSIAMRoleARN** 以创建 secret。在以前的版本中，如果 **awsSTSIAMRoleARN** 不存在，CCO 会记录错误，这会导致每秒出现多个错误。在这个版本中，CCO 不会记录错误，这个问题已解决。(OCPBUGS-36291)

- 在以前的版本中，如果新部署在与当前部署相同的主机上的 OSTree 级别完成，但在不同的 stateroot 中，OSTree 会将它们视为相等。在这个版本中，对 OSTree 逻辑进行了修改，并解决了这个问题。(OCPBUGS-36436)

- 在以前的版本中，OpenShift Container Platform 4.14 中引入的依赖项目标更改会阻止 Microsoft Azure OpenShift Container Platform 安装在升级到更新的版本后扩展新节点。在这个版本中，OpenShift Container Platform 4.15 解决了这个问题。(OCPBUGS-36550)

1.9.3.3. 已知问题

- 如果 **openshift-network-operator** 命名空间中缺少 **ConfigMap** 对象最大传输单元 (MTU)，则必须在启动实时迁移前使用机器 MTU 值手动创建 **ConfigMap** 对象。否则，实时迁移会失败。(OCPBUGS-35829)

1.9.3.4. 更新

要将 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.4. RHSA-2024:4321 - OpenShift Container Platform 4.15.21 程序错误修复和安全更新

发布日期：2024 年 7 月 10 日

OpenShift Container Platform 版本 4.15.21 现已正式发布。其程序错误修正列表包括在 RHSA-2024:4321 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:4324 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.21 --pullspecs
```

1.9.4.1. 程序错误修复

- 在以前的版本中，**alertmanager-trusted-ca-bundle** 配置映射没有注入用户定义的 Alertmanager 容器，这会阻止验证 HTTPS web 服务器接收警报通知。在这个版本中，可信 CA 捆绑包配置映射挂载到 **/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem** 路径的 Alertmanager 容器中。(OCPBUGS-36312)

- 在以前的版本中，内部镜像 registry 无法正确验证 **externalAWS** IAM OpenID Connect (OIDC) 用户配置的集群中的用户。这会在向内部镜像 registry 中推送或拉取镜像时造成用户出现问题。在这个版本中，内部镜像 registry 开始使用 **SelfSubjectReview** API 而不是 OpenShift 的用户 API。特定于 OpenShift 的用户 API 与外部 OIDC 用户不兼容。(OCPBUGS-36287)

- 在以前的版本中，对于从旧版本的 OpenShift Container Platform 升级的集群，在启用了 OVN 的集群上启用 **kdump** 有时会阻止节点重新加入集群或返回到 **Ready** 状态。在这个版本中，以前的 OpenShift Container Platform 版本中过时的数据会被删除，以便节点现在可以正确启动并重新加入集群。(OCPBUGS-36258)

- 在以前的版本中，OpenShift Container Platform 安装程序在 VMware vSphere 上安装的集群资源池的路径中包含一对斜杠 (//)。此问题会导致 ControlPlaneMachineSet (CPMS) Operator 创建额外的 contol plane 机器。在这个版本中，删除了斜杠对以防止出现这个问题。(OCPBUGS-36225)

- 在以前的版本中，GrowPart 工具会锁定一个设备。这会影响到被打开的 Linux Unified Key Setup-disk-format (LUKS) 设备，并导致操作系统引导至紧急模式。在这个版本中，删除了对 GrowPart 工具的调用，以便 LUKS 设备不会被意外锁定，操作系统可以成功引导。(OCPBUGS-35988)

- 在以前的版本中，systemd 中的一个 bug 可能会导致 **coreos-multipath-trigger.service** 单元永久挂起。因此，系统永远不会完成引导。在这个版本中，systemd 单元已被删除，这个问题已被解决。(OCPBUGS-35749)

- 在以前的版本中，在机器创建过程中获取 bootstrap 数据（如临时失败）无法连接到 API 服务器，从而导致机器进入终端失败状态。在这个版本中，在机器创建过程中无法获取 bootstrap 数据时会重新进行尝试，直到最终成功为止。(OCPBUGS-34665)

1.9.4.2. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.5. RHSA-2024:4151 - OpenShift Container Platform 4.15.20 程序错误修复和安全更新

发布日期：2024 年 7 月 2 日

OpenShift Container Platform 版本 4.15.20 现已正式发布。其程序错误修正列表包括在 RHSA-2024:4151 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:4154 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.20 --pullspecs
```

1.9.5.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.5.1.1. 在断开连接的环境中启用镜像流构建

- 此发行版本在 OpenShift API 服务器 (OAS) 容器中添加了额外的 TrustedBundles，并在断开连接的环境中启用镜像流构建。(OCPBUGS-34579)

1.9.5.1.2. 通过 Insights Operator 收集 Prometheus 和 Alert Manager 实例

- Insights Operator (IO) 现在除了 **openshift-monitoring** 自定义资源外，还会收集 **Prometheus** 和 **AlertManager** 资源。(OCPBUGS-35865)

1.9.5.2. 程序错误修复

- 在以前的版本中，当不实现集群自动扩展的可选内部功能时，该函数会导致重复的日志条目。在这个版本中，这个问题已被解决。(OCPBUGS-33885)

- 在以前的版本中，当使用的节点中断时，默认的 Operator Lifecycle Manager (OLM) 目录 pod 会处于终止状态。在这个版本中，由 **CatalogSource** 支持的 OLM 目录 pod 可以从计划和计划外节点维护中正确地恢复。(OCPBUGS-35305).

- 在以前的版本中，Azure API 为子网返回的内容会导致安装程序意外终止。在这个版本中，代码已被更新，以处理子网的旧的和新的数据，并在找不到预期信息时返回错误。(OCPBUGS-35502).

- 在以前的版本中，AWS HyperShift 集群利用其 VPC 的主要 CIDR 范围在数据平面上生成安全组规则。因此，将 AWS HyperShift 集群安装到具有多个 CIDR 范围的 AWS VPC 中会导致生成的安全组规则不足。在这个版本中，安全组规则会根据提供的 Machine CIDR 范围生成，从而解决这个问题。(OCPBUGS-35714)

- 在以前的版本中，在从旧版本升级的 User Provisioned Infrastructure (UPI) 或集群中，在

Infrastructure 对象中可能会缺少 **failureDomains**，这会导致某些检查失败。在这个版本中，如果 **infrastructures.config.openshift.io** 中没有提供 **failureDomains** fallback，则从 **cloudConfig** 合并。(OCPBUGS-35732)

- 在以前的版本中，罕见的时间问题可能会阻止所有 control plane 节点在安装过程中添加到基于代理的集群中。在这个版本中，所有 control plane 节点都成功重启，并在安装过程中添加到集群中。(OCPBUGS-35894)

1.9.5.3. 已知问题

- 在 GCP 上安装 OpenShift IPI 支持带有 3 个 master 的紧凑集群，它们被配置为运行客户工作负载，但不支持 AWS 或 Azure。(OCPBUGS-35359)

1.9.5.4. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.6. RHSA-2024:4041 - OpenShift Container Platform 4.15.19 程序错误修复和安全更新

发布日期：2024 年 6 月 27 日

OpenShift Container Platform 版本 4.15.19 现已正式发布。其程序错误修正列表包括在 RHSA-2024:4041 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:4044 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.19 --pullspecs
```

1.9.6.1. 程序错误修复

- 在以前的版本中，当自定义资源定义 (CRD) 的新版本指定了一个新的转换策略时，这个转换策略应该可以成功转换资源。但实际情况并不是这样，因为 Operator Lifecycle Manager (OLM) 无法在没有实际执行更新操作的情况下为 CRD 验证运行新的转换策略。在这个版本中，当 CRD 验证失败并显示现有转换策略，且新的转换策略在 CRD 的新版本中指定时，OLM 会在更新过程中生成警告信息。(OCPBUGS-35720).

- 在以前的版本中，在节点重启过程中，在更新操作过程中，与重新引导机器交互的节点在短时间内进入 **Ready=Unknown** 状态。这会导致 Control Plane Machine Set Operator 进入 **UnavailableReplicas** 条件，然后是 **Available=false** 状态。**Available=false** 状态触发需要紧急操作的警报，但在这种情况下，只在短时间内需要干预，直到节点重启为止。在这个版本中，当节点进入 unready 状态时，会提供一个节点 unreadiness 的宽限期，如果节点进入 unready 状态，则 Control Plane Machine Set Operator 不会立即进入 **UnavailableReplicas** 条件或 **Available=false** 状态。(OCPBUGS-34971)。

- 在以前的版本中，OpenShift Cluster Manager 容器没有正确的 TLS 证书。因此，镜像流无法用于断开连接的部署。在这个版本中，TLS 证书作为投射卷添加。(OCPBUGS-34580)

- 在以前的版本中，当以 create serverless 表单创建无服务器功能时，不会创建 **BuilldConfig**。在这个版本中，如果没有安装 Pipelines Operator，或者没有为特定资源创建管道资源，或者在创建无服务器功能时没有添加管道，则 **BuildConfig** 会如预期创建。(OCPBUGS-34350)

- 在以前的版本中，减少网络队列无法满足 **!ens0** 等规则的预期工作。这是因为在生成的调优配置集中重复了感叹号。在这个版本中，重复不再发生，因此会按预期应用规则。(OCPBUGS-33929)。

- 在以前的版本中，registry 覆盖由管理端的集群管理员配置，应用到非相关的 data-plane 组件。在这个版本中，registry 覆盖不再应用到这些组件。(OCPBUGS-33627)。

- 在以前的版本中，当在 VMware vSphere 上安装集群时，如果 ESXi 主机处于维护模式，则安装会失败，因为安装程序无法从主机检索版本信息。在这个版本中，安装程序不会尝试从处于维护模式的 ESXi 主机检索版本信息，从而允许安装继续进行。(OCPBUGS-31387)

1.9.6.2. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.7. RHSA-2024:3889 - OpenShift Container Platform 4.15.18 程序错误修复和安全更新

发布日期：2024 年 6 月 18 日

OpenShift Container Platform 版本 4.15.18 现已正式发布。其程序错误修正列表包括在 RHSA-2024:3889 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:3892 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.18 --pullspecs
```

1.9.7.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.7.1.1. 为 SHA1 路由引入 UnservableFutureVersions 状态条件

- OpenShift Container Platform 4.15 不支持路由上的 SHA1 证书。因此，从 4.15 升级到 4.15 会导致 SHA1 证书的路由被拒绝。
  在这个版本中，为包含 SHA1 证书的路由引入了一个新的 **UnservableInFutureVersions** 状态条件。另外，如果任何路由中存在这个新状态，它会添加一个 **admin-gate** 来阻止升级。因此，如果集群管理员在 OpenShift Container Platform 4.15 中使用 SHA1 证书的路由，则必须将这些证书升级到支持算法，或者为创建的 **admin-gate** 提供 **admin-ack**。此 **admin-ack** 允许管理员在不解决 SHA1 证书问题的情况下进行升级，即使路由将被拒绝。(OCPBUGS-28928).

1.9.7.1.2. 允许 pull secret 密码包含冒号字符

- 此发行版本引入了在 Openshift Assisted Installer 密码中包含冒号字符的功能。(OCPBUGS-34641)

1.9.7.1.3. 为 Hypershift 引入 etcd 碎片整理控制器

- 此发行版本为 Hypershift 上的托管集群引入了 etcd 分离控制器。(OCPBUGS-35002)

1.9.7.2. 程序错误修复

- 在以前的版本中，如果在首次尝试身份验证发现失败时，OpenShift Container Platform Web 控制台会意外终止。在这个版本中，身份验证初始化已被更新，在失败前重试最多 5 分钟。(OCPBUGS-30208)

- 在以前的版本中，当从 4.15.8 升级到 OpenShift Container Platform 4.15.11 时，**metal3-ironic** 和 **metal3-ironic-inspector** pod 会失败，因为与 FIPS 模式启用相关的安装失败。在这个版本中，这个问题已被解决。(OCPBUGS-33736)

- 在以前的版本中，OpenShift Agent Installer 将已安装的 SATA SDD 报告为可移动并拒绝使用其中任何一个作为安装目标。在这个版本中，可移动磁盘可以进行安装，并解决了这个问题。(OCPBUGS-34732)

- 在以前的版本中，如果不存在 POSIX 用户访问点，则在 EFS 文件系统上置备新卷时，AWS EFS 驱动程序控制器会返回运行时错误。在这个版本中，驱动程序已被修复，这个问题已解决。(OCPBUGS-34843)

- 在以前的版本中，因为 Hypershift CLI 存在问题，Hypershift 上的 secrets-store CSI 驱动程序无法挂载 secret。在这个版本中，驱动程序可以挂载卷，并解决了这个问题。(OCPBUGS-34997)

- 在以前的版本中，在断开连接的环境中，HyperShift Operator 会忽略 registry 覆盖。因此，对节点池的更改会被忽略，节点池会遇到错误。在这个版本中，元数据检查器在 HyperShift Operator 协调过程中可以正常工作，并正确填充覆盖镜像。(OCPBUGS-35074)

1.9.7.3. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.8. RHBA-2024:3673 - OpenShift Container Platform 4.15.17 程序错误修复和安全更新

发布日期： 2024 年 6 月 11 日

OpenShift Container Platform 版本 4.15.17 现已正式发布。其程序错误修正列表包括在 RHBA-2024:3673 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:3676 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.17 --pullspecs
```

1.9.8.1. 功能增强

这个 z-stream 发行版本包括以下增强：

1.9.8.1.1. 集群版本 4.8 或更早版本的存储迁移

- 此发行版本引入了一个存储迁移，它支持从版本 4.8 或更早版本到最新支持的版本的安全集群更新。如果您在版本 4.7 或更早版本中创建集群，则存储的对象在将集群更新至最新支持的发行版本时仍可访问。(OCPBUGS-31445)

1.9.8.2. 程序错误修复

- 在以前的版本中，当为 Amazon Virtual Private Cloud (VPC) DHCP 选项配置了多个域时，主机名可能会返回多个值。但是，相关逻辑不会考虑到多个值，当返回的节点名称中包含空格时会崩

溃。在这个版本中，相关逻辑被更新，使用第一个返回的主机名作为节点名称。这个问题已解决。(OCPBUGS-33847)

- 在以前的版本中，当使用 Image Registry Operator 配置中设置的 **regionEndpoint** 启用 **virtualHostedStyle** 时，镜像 registry 会忽略虚拟托管风格配置，且无法启动。在这个版本中，镜像 registry 使用新的上游发布配置，这个问题已解决。(OCPBUGS-34539)

- 在以前的版本中，OperatorHub 错误地排除 ROSA Hosted Control Plane (HCP) 集群的 Amazon Resource Name (ARN) 角色信息。在这个版本中，OperatorHub 可以正确地显示 ARN 信息，这个问题已被解决。(OCPBUGS-34550)

- 在以前的版本中，当在安装前尝试删除集群或 BareMetalHost (BMH) 资源时，metal3-operator 会尝试生成预置备镜像。在这个版本中，创建了一个例外，以防止在 BMH 删除过程中创建预置备镜像，这个问题已被解决。(OCPBUGS-34682)

- 在以前的版本中，在 OpenShift Container Platform 4.15 的 **Form View** 中编辑配置映射时，一些文本区域不再可调整。在这个版本中，这些文本区域可以被重新定义。(OCPBUGS-34703)

1.9.8.3. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.9. RHBA-2024:3488 - OpenShift Container Platform 4.15.16 程序错误修复更新

发布日期：2024 年 6 月 5 日

OpenShift Container Platform 版本 4.15.16 现已正式发布。其程序错误修正列表包括在 RHBA-2024:3488 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:3491 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.16 --pullspecs
```

1.9.9.1. 程序错误修复

- 在以前的版本中，在 OpenShift Container Platform 上的 HAProxy 2.6 部署中，关闭 HAproxy 可能会导致竞争条件。主线程 **(tid=0)** 会等待其他线程完成，但有些线程会进入一个无限循环，消耗 100% CPU。在这个版本中，控制循环终止的变量会被正确重置，防止非主线程进行无限期循环。这样可确保线程的轮询循环可以正确终止。(OCPBUGS-33883)

- 在以前的版本中，控制台 Operator 健康检查控制器缺少 return 语句，这会导致 Operator 在某些情况下意外崩溃。在这个发行版本中，这个问题已被解决。(OCPBUGS-33720)

- 在以前的版本中，bootstrap 过程中使用的 **wait-for-ceo** 命令验证 etcd rollout 不会报告一些故障模式的错误。在这个版本中，如果 **wait-for-ceo** 命令退出，则这些错误消息会在 **bootkube** 脚本中看到。(OCPBUGS-33564)

1.9.9.2. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.10. RHSA-2024:3327 - OpenShift Container Platform 4.15.15 程序错误修复和安全更新

发布日期： 2024 年 5 月 29 日

OpenShift Container Platform 版本 4.15.15 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:3327 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:3332 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.15 --pullspecs
```

1.9.10.1. 程序错误修复

- 在以前的版本中，在某些情况下会导致将 Egress IP 地址从一个节点传输到不同的节点失败，且这个故障会影响 OVN-Kubernetes 网络。网络无法向对等点发送 gratuitous 地址解析协议(ARP)请求，以告知他们新节点的介质访问控制(MAC) 地址。因此，对等点会临时将回复流量发送到旧节点，这个流量会导致故障转移问题。在这个版本中，OVN-Kubernetes 网络可以正确地向对等点发送一个 gratuitous ARP，以通知它们新的 Egress IP 节点 MAC 地址，以便每个 peer 可以在不造成故障转移时间问题的情况下将流量发送到新节点。(OCPBUGS-33960)

- 在以前的版本中，当镜像 Operator 目录时，**oc-mirror** CLI 插件会重新构建目录，并根据 **imagesetconfig** 目录过滤规格重新生成目录的内部缓存。此操作需要使用目录中找到的 **opm** 二进制文件。在 OpenShift Container Platform 4.15 中，Operator 目录包括 **opm** Red Hat Enterprise Linux (RHEL) 9 二进制文件，这会导致在 RHEL 8 系统上运行时镜像过程失败。在这个版本中，**oc-mirror** 不再默认构建目录。相反，目录直接镜像到其目标 registry。(OCPBUGS-33575)

- 在以前的版本中，镜像 registry 不支持 Amazon Web Services (AWS) 区域 **ca-west-1**。在这个版本中，镜像 registry 可以部署到此区域中。(OCPBUGS-33672)

- 在以前的版本中，服务帐户 (SA) 无法用作 OAuth2 客户端，因为没有与 SA 关联的令牌。在这个版本中，OAuth registry 客户端已被修改来预测这个问题单，这个问题已解决。(OCPBUGS-33210)

- 在以前的版本中，**install-config.yaml** 文件中设置的代理信息不会应用到 bootstrap 过程。在这个版本中，代理信息被应用到 bootstrap 机器的 bootstrap Ignition 数据，并解决了这个问题。(OCPBUGS-33205)

- 在以前的版本中，**imageRegistryOverrides** 设置的信息仅在 HyperShift Operator 初始化中提取一次，且不会刷新。在这个版本中，Hypershift Operator 从管理集群检索新的 **ImageContentSourcePolicy** 文件，并在每个协调循环中将它们添加到 Hypershift Operator 和 Control Plane Operator 中。(OCPBUGS-33117)

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

- 在以前的版本中，如果配置包含 **""** 字符，则尝试更新 OpenShift Container Platform 的 VMware vSphere 连接配置会失败。在这个版本中，字符会被正确存储，这个问题已解决。(OCPBUGS-31863)

1.9.10.2. 已知问题

- 在以前的版本中，在升级到 OpenShift Container Platform 4.15.6 后，尝试使用集群中的 **oc-mirror** CLI 插件会失败。在这个版本中，RHEL 9 有一个与 FIPS 兼容的 **oc-mirror** 版本，RHEL 8 的 **oc-mirror** 版本不兼容 FIPS。(OCPBUGS-31609)

1.9.10.3. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.11. RHSA-2024:2865 - OpenShift Container Platform 4.15.14 程序错误修复和安全更新

发布日期： 2024 年 5 月 21 日

OpenShift Container Platform r版本 4.15.14 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:2865 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:2870 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.14 --pullspecs
```

1.9.11.1. 程序错误修复

- 在以前的版本中，如果流量被转发到无法正常工作的 terminating 端点，除非这些端点上的就绪度探测已被配置为快速地将端点标记为 "not serving"，否则将出现交流问题。发生这种情况的原因是，部分实现了 KEP-1669 的服务的 **ProxyTerminatingEndpoints** 流量的端点选择为 OpenShift Container Platform 集群内的服务。因此，这个流量被转发到所有就绪的端点，如 **ready=true**, **serving=true**, **terminating=false**，或 terminating 和 serving，如 **ready=false**、**service=true**、**terminating=true**。这会导致，当流量被转发到一个已无法正常工作的 terminating 端点时，在这些端点中的 readiness probes 没有被配置为快速地将端点标记为 **serving=false** 时，出现网络交流问题。在这个版本中，端点选择逻辑会为任何给定服务完全实现了 KEP-1669 **ProxyTerminatingEndpoints**，以便选择所有可用的端点。如果没有找到就绪的端点，则使用可以正常工作的 terminating 和 serving 端点。(OCPBUGS-27852)

- 在以前的版本中，如果您配置了有大量内部服务或用户管理的负载均衡器 IP 地址的 OpenShift Container Platform 集群，则会出现 OVN-Kubernetes 服务的延迟启动时间。当 OVN-Kubernetes 服务试图在节点上安装 **iptables** 规则时，会发生此延迟。在这个版本中，OVN-Kubernetes 服务可在几秒钟内处理大量服务。另外，您可以访问新日志来查看在节点上安装 **iptables** 规则的状态。(OCPBUGS-32426)

- 在以前的版本中，即使 CRI-O 停止容器，使用 **exec** 命令创建的一些容器进程也会保留。因此，闲置进程会导致跟踪问题，从而导致进程泄漏和失效状态。在这个版本中，CRI-O 跟踪为容器处理的 **exec** 调用，并确保在容器停止时作为 **exec** 调用一部分创建的进程被终止。(OCPBUGS-32481)

- 在以前的版本中，OpenShift Container Platform web 控制台中的 **Topology** 视图不会显示虚拟机(VM)节点和其他非VM 组件之间的视觉连接器。在这个版本中，视觉连接器会显示组件的交互活动。(OCPBUGS-32505)

- 在以前的版本中，OpenShift Container Platform Web 控制台的 masthead 元素中的徽标可能会超过 60 像素。这会导致 masthead 在高度增加。在这个版本中，masthead 徽标有一个 **max-height** 为 60 pixels 的限制。(OCPBUGS-33548)

- 在以前的版本中，如果您需要 OpenShift Container Platform Web 控制台中的 **Form** 视图从 **Route** 资源中删除备用服务，则备用服务会保留在集群中。在这个版本中，如果您以这种方式删除备用服务，则备用服务会从集群中移除。(OCPBUGS-33058)

- 在以前的版本中，因为 API 的代码库存在问题，OpenShift Container Platform 集群连接到 Microsoft Azure API 会延迟。在这个版本中，会为 Azure API 的任何调用设置超时调度，以便终止一段时间内挂起的 API 调用。(OCPBUGS-33127)

- 在以前的版本中，在 OpenShift Container Platform 4.15.0 中引入的内核回归问题会导致在挂载到 CephFS 存储的节点中崩溃和重新引导内核问题。在这个发行版本中，回归问题已被修复，内核回归问题不再发生。(OCPBUGS-33250)

- 在以前的版本中，VMware vSphere Problem Detector Operator 没有为其配置 HTTP 和 HTTPS 代理。这会导致无效的集群配置错误消息，因为 Operator 和 VMware vSphere vCenter 服务器之间的连接问题。在这个版本中，vSphere Problem Detector Operator 使用与其他 OpenShift Container Platform 集群 Operator 相同的 HTTP 和 HTTPS 代理，以便 vSphere 问题检测器 Operator 可以连接到 VMware vSphere vCenter。(OCPBUGS-33466)

- 在以前的版本中，Alertmanager 会发送通知电子邮件，其中包含到 Thanos Querier Web 界面的 backlink。此 Web 界面是一个不能访问的 Web 服务。在这个版本中，监控警报通知电子邮件包含到 OpenShift Container Platform Web 控制台的 ***Alerts** 页面的 backlink。(OCPBUGS-33512)

1.9.11.2. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.12. RHSA-2024:2773 - OpenShift Container Platform 4.15.13 程序错误修复和安全更新

发布日期： 2024 年 5 月 15 日

OpenShift Container Platform 版本 4.15.13 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:2773 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:2776 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.13 --pullspecs
```

1.9.12.1. 程序错误修复

- 在以前的版本中，安全性上下文约束 (SCC) 的名称不正确，因此没有可正常工作的内置集群角色。在这个版本中，名称被改为 **hostmount-anyuid**，SCC 现在有一个可正常工作的内置集群角色。(OCPBUGS-33277)

- 在以前的版本中，当尝试擦除磁盘时 Ironic Python Agent (IPA) 会失败，因为它预期一个错误的字节扇区大小，这会导致节点置备失败。在这个版本中，IPA 检查磁盘扇区大小，节点置备会成功。(OCPBUGS-33133)

- 在以前的版本中，因为驱动程序中的一个错误导致卷挂载失败，所以无法配置 Workload Identity 集群上的静态持久性卷。在这个版本中，驱动程序已被修复，静态持久性卷挂载正确。(OCPBUGS-33038)

- 在以前的版本中，在 OpenShift Container Platform 在性能调整集群中更新过程中，恢复

MachineConfigPool 资源会导致池中节点出现额外的重启。这是因为性能配置集控制器在池暂停时与过时的机器配置协调。在这个版本中，控制器会在池恢复前针对最新的计划机器配置协调，从而导致额外的节点重启。(OCPBUGS-32978)

- 在以前的版本中，负载平衡算法在决定权重时不会区分活跃和不活跃的服务，它在有大量不活跃服务或环境路由后端的环境中过度使用 **随机** 算法。这会导致内存用量增加，并面临过量内存消耗的风险。在这个版本中，进行了更改来优化对活跃服务的流量方向，并防止使用较高权重的**随机**算法，从而减少过量内存消耗的可能性。(OCPBUGS-32977)

- 在以前的版本中，如果用户创建了一个 **ContainerRuntimeConfig** 资源作为单节点 OpenShift Container Platform 集群 (SNO) 安装的额外清单，则 boostrap 进程会失败，并显示错误：**more than one ContainerRuntimeConfig found that matches MCP labels**。在这个版本中，修正了不正确地处理 **ContainerRuntimeConfig** 资源的问题，从而解决了这个问题。(OCPBUGS-30152)

- 在以前的版本中，如果 chart 名称不同，Helm 插件索引视图不会显示与 Helm CLI 相同的 chart 数量。在这个版本中，Helm 目录会查找 **chart.openshift.io/name** 和 **charts.openshift.io/provider**，以便所有版本都分组到单个目录标题中。(OCPBUGS-32716)

- 在以前的版本中，托管的 control plane CLI 标记 **api-server-address** 的描述不明确。在这个版本中，描述信息更清晰和完整。(OCPBUGS-25858)

1.9.12.2. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.13. RHSA-2024:2664 - OpenShift Container Platform 4.15.12 程序错误修复和安全更新

发布日期：2024 年 5 月 9 日

OpenShift Container Platform 版本 4.15.12 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:2664 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:2669 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.12 --pullspecs
```

1.9.13.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.13.1.1. ClusterTriggerBinding、TriggerTemplate 和 EventListener CRD 的 API 版本从 v1alpha1 升级到 v1beta1

- 在以前的版本中，**ClusterTriggerBinding**、**TriggerTemplate** 和 **EventListener** CRD 的 API 版本为 **v1alpha1**。在这个版本中，API 版本升级到 **v1beta1**，以便 pipelines 插件支持 **ClusterTriggerBinding**、**TriggerTemplate** 和 **EventListener** CRD 的最新 Pipeline Trigger API 版本。(OCPBUGS-31445)

1.9.13.1.2. pipelinerun list 查看性能改进

- 在以前的版本中，在 **PipelineRun** 列表页面中，所有 **TaskRun** 对象都会被根据其 **PipelineRun** 名称获取并分开。在这个版本中，**TaskRun** 对象只获取失败并取消的 **PipelineRun** 对象，并添加了一个缓存机制来获取与失败并取消的 **PipelineRun** 对象关联的 **PipelineRun** 和 **TaskRun** 对象。(OCPBUGS-31799)

1.9.13.1.3. 安装程序处理 % 字符的转义

- 在以前的版本中，如果集群使用代理安装，且代理信息包含转义的字符（格式为 **%XX**），安装会失败。在这个版本中，安装程序处理 **%** 字符的转义。(OCPBUGS-32259)

1.9.13.1.4. 集群 Fleet 评估状态信息添加到 Machine Config Operator

- 在以前的版本中，Machine Config Operator (MCO)不包括 Cluster Fleet 评估(CFE)状态。在这个版本中，CFE 状态信息添加到 MCO 中，并可供客户使用。(OCPBUGS-32922)

1.9.13.1.5. OperatorHub 过滤器从 FIPS 模式重命名为 Designed for FIPS

- 在以前的版本中，OperatorHub 包括一个名为 **FIPS Mode** 的过滤器。在这个版本中，该过滤器被命名为 **Designed for FIPS**。(OCPBUGS-32933)

1.9.13.2. 程序错误修复

- 在以前的版本中，容器在其 **cgroup** 层次结构中具有不正确的 pids 限制视图，并报告为随机数而不是 **max**。容器没有最大 PID，只受 pod PID 的限制，该限制在容器的 **cgroup** 层次结构外设置，在容器中不可见。在这个版本中，这个问题已被解决。(OCPBUGS-28926)

- 在以前的版本中，对于 Red Hat OpenStack Platform (RHOSP)上的 OpenShift Container Platform 部署，**MachineSet** 对象无法正确应用 **Port Security** 参数的值。在这个版本中，**MachineSet** 对象会如预期应用 **port_security_enabled** 标志。(OCPBUGS-30857)

- 在以前的版本中，当使用 **openshift-baremetal-install** 二进制文件配置了基于代理的安装时，安装程序会错误地尝试验证 libvirt 网络接口。在这个版本中，代理安装方法不需要 libvirt，这个验证被禁用。(OCPBUGS-30944)

- 在以前的版本中，**cpuset-configure.sh** 脚本可以在创建所有系统进程前运行。在这个版本中，只有在 CRI-O 初始化 CRI-O 且这个问题被解决时，该脚本才会触发。(OCPBUGS-31692)

- 在以前的版本中，在 data plane 中，一个不正确的 **dnsPolicy** 用于 **konnectivity-agent** 守护进程集。因此，当 CoreDNS 停机时，data plane 上的 **konnectivity-agent** pod 无法解析 **proxy-server-address**，并导致 **konnectivity-server** 在 control plane 中失败。在这个版本中，**konnectivity-agent** 使用主机系统 DNS 服务来查找 **proxy-server-address**，不再依赖于 CoreDNS。(OCPBUGS-31826)

- 在以前的版本中，如果在收集 bootstrap 执行过程中从 **bootstrap** 节点收集日志失败，则虚拟机(VM)串口控制台日志不会包含在收集输出中。在这个版本中，如果收集了串行日志，则始终包含它们。(OCPBUGS-32264)

- 在以前的版本中，AWS SDK 安装中的计算节点的安全组中缺少端口 22，因此当用户使用 AWS SDK 置备时，使用 SSH 连接到计算节点会失败。在这个版本中，端口 22 添加到计算节点的安全组中，这个问题已解决。(OCPBUGS-32383)

- 在以前的版本中，安装程序为 AWS 需要 **s3:HeadBucket** 权限，即使它不存在。**HeadBucket** 操作的正确权限是 **s3:ListBucket**。在这个版本中，**s3:HeadBucket** 已从所需权限列表中删除，只需要 **s3:ListBucket**。(OCPBUGS-32690)

- 在以前的版本中，OpenShift Container Platform Ansible 升级存在问题，因为 IPsec 配置不是幂等的。在这个版本中，对 OpenShift Container Platform Ansible playbook 进行了更改，确保所有 IPsec 配置都是幂等的。(OCPBUGS-33102)

1.9.13.3. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.14. RHSA-2024:2068 - OpenShift Container Platform 4.15.11 程序错误修复和安全更新

发布日期： 2024 年 5 月 2 日

OpenShift Container Platform 版本 4.15.11 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:2068 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:2071 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.11 --pullspecs
```

1.9.14.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.14.1.1. 在 Topology 视图中增加支持的节点数量

- 在以前的版本中，OpenShift Container Platform Web 控制台 **Topology** 视图只能显示最多 100 个节点。如果您试图查看超过 100 个节点，Web 控制台会输出 **Loading is taking longer than expected.** 错误消息。在这个版本中，Web 控制台的 **MAX_NODES_LIMIT** 参数设置为 **200**，因此 Web 控制台最多可显示 200 个节点。(OCPBUGS-32340)

1.9.14.1.2. 添加了 gcr 和 acr RHEL 凭证供应商

- OpenShift Container Platform 4.15 包括 **gcr** 和 **acr** Red Hat Enterprise Linux (RHEL) 凭证供应商，以便以后升级到需要集群中部署的 RHEL 计算节点的 OpenShift Container Platform 版本不会安装失败。(OCPBUGS-30970)

1.9.14.1.3. 添加了将 featureGates 资源读取到 RBAC 规则的权限

- OpenShift Container Platform 4.15 为基于角色的访问控制(RBAC)规则添加了一个权限，以便 DNS Operator 可以读取 **featureGates** 资源。如果没有此权限，则升级到 OpenShift Container Platform 的更新版本可能会失败。(OCPBUGS-32093)

1.9.14.2. 程序错误修复

- 当性能配置集位于额外清单文件夹和目标 **master** 或 **worker** 节点角色中时，OpenShift Container Platform 安装会失败。这是因为在创建默认 **master** 或 **worker** 节点角色前处理性能配置集的内部安装所致。在这个版本中，内部安装会在创建节点角色后处理性能配置集，以便这个问题不再存在。(OCPBUGS-27948)

- 在以前的版本中，镜像 registry 不支持 Amazon Web Services (AWS) 区域 **ca-west-1**。在这个版本中，镜像 registry 可以部署到此区域中。(OCPBUGS-31641)

- 在以前的版本中，升级到 OpenShift Container Platform 4.14 或更高版本的集群会意外关闭 **keep-alive** 连接，这会导致 Apache HTTP 客户端出现流量降级问题。此问题是由路由器 pod 使用 HAProxy 路由器的版本导致的，该版本在 HAProxy 路由器重启后关闭闲置连接。在这个版本中，pod 使用 HAProxy 路由器的版本，其中包括 **idle-close-on-response** 选项。HAProxy 路由器现在在闲置连接关闭前等待最后一个请求和响应事务。(OCPBUGS-32435)

- 在以前的版本中，Redfish 虚拟介质 Hewlett Packard Enterprise (HPE) 集成 Lights Out (iLO) 5 裸机机器的压缩被强制禁用，以在不同的硬件模型中解决其他不相关问题。这会导致每个 iLO 5 裸机机器中缺少 **FirmwareSchema** 资源。每台机器都需要压缩从 Redfish Baseboard Management Controller (BMC) 端点获取消息 registry。在这个版本中，每个需要 **FirmwareSchema** 资源的 iLO 5 裸机机器都没有强制禁用压缩。(OCPBUGS-31686)

- 在以前的版本中，暂停的 **MachineConfigPools** 节点可能会在执行集群更新时保持暂停状态。在这个版本中，暂停的 **MachineConfigPools** 节点会在执行集群更新时正确暂停。(OCPBUGS-31839)

- 在以前的版本中，Redfish 的较新版本使用 Manager 资源弃用 RedFish Virtual Media API 的统一资源标识符 (URI)。这会导致任何使用较新的 Redfish URI for Virtual Media 的硬件不会被置备。在这个版本中，Ironic API 标识为 RedFish Virtual Media API 部署的正确 Redfish URI，以便依赖已弃用或可以置备较新的 URI 的硬件。(OCPBUGS-31830)

- 在以前的版本中，在 mint 模式验证检查过程中，Cloud Credential Operator (CCO)会在 mint 模式中检查不存在的 **s3:HeadBucket** 权限，这会导致集群安装失败。在这个版本中，CCO 会删除此不存在的权限的验证检查，以便验证检查在 mint 模式中通过，集群安装不会失败。(OCPBUGS-31924)

- 在以前的版本中，升级到 OpenShift Container Platform 4.15.3 的新 Operator Lifecycle Manager (OLM) Operator 会导致失败，因为重要的资源没有注入升级操作。在这个版本中，这些资源会被缓存，以便较新的 OLM Operator 升级可以成功。(OCPBUGS-32311)

- 在以前的版本中，Red Hat OpenShift Container Platform Web 控制台不需要 **Creator** 字段作为必填字段。API 更改为为此字段指定一个空值，但用户配置集仍然可以创建静默警报。在这个版本中，API 将 **Creator** 字段标记为需要创建静默警报的用户配置集的强制字段。(OCPBUGS-32097)

- 在以前的版本中，在 OpenShift Container Platform 托管的 control plane 中，当您在断开连接的环境中为 **ImageDigestMirrorSet** 和 **ImageContentSourcePolicy** 对象创建自定义资源定义 (CRD) 时，Hy HyperShift Operator 只为 **ImageDigestMirrorSet** CRD 创建对象，忽略 **ImageContentSourcePolicy** CRD。在这个版本中，HyperShift Operator 可以同时为 **ImageDigestMirrorSet** 和 **ImageContentSourcePolicy** CRD 创建对象。(OCPBUGS-32164)

- 在以前的版本中，在 Red Hat OpenStack Platform (RHOSP)环境中操作的 IPv6 网络服务无法共享配置了多个服务的 IPv6 负载均衡器，因为错误地将 IPv6 负载均衡器标记为集群 **Internal**。在这个版本中，IPv6 负载均衡器不再标记为 **Internal**，因此具有多个服务的 IPv6 负载均衡器可以在 IPv6 网络服务间共享。(OCPBUGS-32246)

- 在以前的版本中，control plane 机器集(CPMS)不允许在 CPMS 定义中 vSphere 的模板名称。在这个版本中，CPMS Operator 修复允许 CPMS 定义中的 vSphere 模板名称，因此这个问题不再会出现。(OCPBUGS-32357)

- 在以前的版本中，control plane 机器集(CPMS) Operator 无法正确处理在基础架构自定义资源中有一个 vSphere 定义的旧 OpenShift Container Platform 版本配置。这会导致集群升级操作失败，CPMS Operator 处于 **crashloopback** 状态。在这个版本中，因为这个问题，集群升级操作不会失败。(OCPBUGS-32414)

- 在以前的版本中，镜像 registry 的 Azure 路径修复作业会错误地需要存在 **AZURE_CLIENT_ID** 和 **TENANT_CLIENT_ID** 参数才能正常工作。这会导致有效的配置抛出错误消息。在这个版本

中，在 Identity and Access Management (IAM)服务帐户密钥中添加检查以验证是否需要这些参数，以便集群升级操作不再失败。(OCPBUGS-32396)

- 在以前的版本中，因为内存限制而失败的构建 pod 会将其 pod 状态改为 **Error**，而不是 **OOMKilled**。这会导致这些 pod 无法正确报告。此问题只会在 cgroup v2 节点上发生。在这个版本中，可以正确地检测到并报告状态为 **OOMKilled** 的 pod。(OCPBUGS-32498)

1.9.14.3. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.15. RHSA-2024:1887 - OpenShift Container Platform 4.15.10 程序错误修复和安全更新

发布日期：2024 年 4 月 26 日

OpenShift Container Platform 版本 4.15.10 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1887 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:1892 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.10 --pullspecs
```

1.9.15.1. 程序错误修复

- 在以前的版本中，因为安装程序删除 SecretTypeTLS，在 OpenShift Container Platform 4.7 之前创建的集群会为 api-int 端点有 signer 密钥意外更新，然后删除 SecretTypeTLS，然后使用 **kubernetes.io/tls** 类型重新创建 secret。在这个版本中，安装程序在不删除 secret 的情况下更改 secret 类型解决了这个问题。(OCPBUGS-31807)

- 在以前的版本中，当用户导入镜像流标签时，**ImageContentSourcePolicy** (ICSP)不允许与 **ImageDigestMirrorSet** (IDMS)和 **ImageTagMirrorSet** (ITMS)共存。OpenShift Container Platform 忽略用户创建的 IDMS/ITMS，并优先使用 ICSP。在这个版本中，允许它们共存，因为在存在 ICSP 时导入镜像流标签将遵循 IDMS/ITMS。(OCPBUGS-31469)

- 在以前的版本中，Terraform 会使用为 control plane 设置的策略创建计算服务器组。因此，compute 服务器组会忽略 **install-config.yaml** 文件的 'serverGroupPolicy' 属性。在这个版本中，compute MachinePool 的 **install-config.yaml** 文件中的服务器组策略会在 Terraform 流中的安装时正确应用。(OCPBUGS-31335)

- 在以前的版本中，使用 pod **.spec.nodeName** 指定非中断的 openshift.io/node-selector 项目选择器的项目可能会导致 Deployment 中的 runaway Pod 创建。在这个版本中，带有非中断 **.spec.nodeName** 的 pod 不会被 API 服务器接受来解决这个问题。(OCPBUGS-29922)

- 在以前的版本中，具有基本登录凭证的远程攻击者可以检查 pod 清单，以发现存储库 pull secret。在这个版本中，这个漏洞已被修复。(OCPBUGS-28769)

1.9.15.2. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.16. RHSA-2024:1770 - OpenShift Container Platform 4.15.9 程序错误修复和安全更新

发布日期： 2024 年 4 月 16 日

OpenShift Container Platform 版本 4.15.9 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1770 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:1773 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.9 --pullspecs
```

1.9.16.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.16.1.1. 验证配置的 control plane 副本数

- 在以前的版本中，control plane 副本数可以设置为无效的值，如 2。在这个版本中，添加了一个验证，以防止在 ISO 生成时间配置 control plane 副本。(OCPBUGS-30822)

1.9.16.2. 程序错误修复

- 在以前的版本中，在 Open Virtual Network (OVN) 部署中将 kdump 日志保存到 SSH 目标会失败。当 OVN 配置时，kdump 崩溃日志不会被创建到 SSH 远程。在这个版本中，在 kdump 之前，OVS-configurations 不再运行。(OCPBUGS-30884)
- 在以前的版本中，**coreos-installer** CLI 工具无法正确修改、重置或显示 **openshift-install agent create image** 命令生成的 ISO 的内核参数。在这个版本中， **coreos-installer iso kargs modify <iso>**, **coreos-installer iso kargs reset <iso>**, and **coreos-installer iso kargs show <iso>** 命令都按预期工作。(OCPBUGS-30922)
- 在以前的版本中，服务辅助 IP 系列测试使用双栈集群失败。在这个版本中，启用了 30000:32767 流量范围，这个问题已被解决。(OCPBUGS-31284)

1.9.16.3. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.17. RHSA-2024:1668 - OpenShift Container Platform 4.15.8 程序错误修复和安全更新

发布日期：2024 年 4 月 8 日

OpenShift Container Platform 版本 4.15.8 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1668 公告中。此更新没有 RPM 软件包。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.8 --pullspecs
```

1.9.17.1. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.18. RHSA-2024:1559 - OpenShift Container Platform 4.15.6 程序错误修复和安全更新

发布日期： 2024 年 4 月 2 日

OpenShift Container Platform 版本 4.15.6 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1559 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:1563 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.6 --pullspecs
```

1.9.18.1. 已知问题

- 本发行版本中存在一个已知问题，这会导致在 Red Hat Enterprise Linux (RHEL) 8 系统中 **oc-mirror** 二进制文件失败。临时解决方案：使用 Red Hat OpenShift Container Platform 4.15.5 **oc-mirror** 二进制文件或提取 **oc-mirror.rhel8**。(OCPBUGS-31609)

1.9.18.2. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.19. RHSA-2024:1449 - OpenShift Container Platform 4.15.5 程序错误修复和安全更新

发布日期： 2024 年 3 月 27 日

OpenShift Container Platform release 4.15.5 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1449 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:1452 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.5 --pullspecs
```

1.9.19.1. 程序错误修复

- 在以前的版本中，OpenShift 安装程序可能无法在分配的时间内从 Microsoft Azure 检索实例类型信息，即使使用 Azure CLI 验证类型也会存在。在这个版本中，超时时间已增加到等待 Azure 响应，错误消息会包括失败的正确原因。(OCPBUGS-29964)

- 在以前的版本中，当使用 Hive 置备程序（使用 OpenShift 安装程序）通过 OpenShift Cluster Manager (OCM) 创建集群时，安装程序无法在删除集群后删除 AWS IAM 实例配置集。此问题导致实例配置集的积累。在这个版本中，安装程序会标记实例配置集并删除适当标记的配置集。(OCPBUGS-18986)

1.9.19.2. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.20. RHSA-2024:1255 - OpenShift Container Platform 4.15.3 程序错误修复和安全更新

发布日期： 2024 年 3 月 19 日

OpenShift Container Platform 版本 4.15.3 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1255 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:1258 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.3 --pullspecs
```

1.9.20.1. 程序错误修复

- 在以前的版本中，如果 root 凭证已从 mint 模式的 Google Cloud Platform (GCP) 集群中删除，Cloud Credential Operator (CCO) 将在大约 1 小时后进入降级状态。这个问题意味着 CCO 无法管理组件的凭证 root secret。在这个版本中，mint 模式支持自定义角色，因此从 GCP 集群中删除 root 凭证不会造成 CCO 进入降级状态。(**OCPBUGS-30412**)

1.9.20.2. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.21. RHSA-2024:1210 - OpenShift Container Platform 4.15.2 程序错误修复和安全更新

发布日期： 2024 年 3 月 13 日

OpenShift Container Platform 版本 4.15.2 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1210 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:1213 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.15.2 --pullspecs
```

1.9.21.1. 已知问题

- 对于 OpenShift Container Platform 4.15.0，在第 0 天使用一个额外清单来提供性能配置集无法正常工作，但现在在 4.15.2 中可以正常工作，但有以下限制：
  当额外清单文件夹中存在性能配置集，并以主或 worker 池为目标时，OpenShift Container Platform 安装可能会失败。这是因为内部安装排序导致在创建默认主和 worker **MachineConfigPool** 前处理性能配置集。您可以通过在额外 manifests 文件夹中包含库存主或 worker **MachineConfigPool** 的副本来解决这个问题。(**OCPBUGS-27948**, **OCPBUGS-29752**)

1.9.21.2. 程序错误修复

- 在以前的版本中，当升级到 OpenShift Container Platform 4.15 时，**CatalogSource** 对象永远不会刷新，这会导致可选的 Operator 目录无法更新。在这个版本中，镜像拉取策略被改为 **Always**，这可让可选的 Operator 目录正确更新。(OCPBUGS-30193)

- 在以前的版本中，**nodeStatusReportFrequency** 设置链接到 **nodeStatusUpdateFrequency** 设置。在这个版本中，**nodeStatusReportFrequency** 被设置为 5 分钟。(OCPBUGS-29797)

- 在以前的版本中，在某些情况下，安装程序会失败，并显示错误消息 **unexpected end of JSON input**。在这个版本中，错误消息已被明确，推荐用户在 **install-config.yaml** 文件中设置 **serviceAccount** 字段来修复问题。(OCPBUGS-29495)

- 在以前的版本中，**HostedCluster** 对象中提供的 **oauthMetadata** 属性不会被遵守。在这个版本中，**HostedCluster** 对象遵循 **oauthMetadata** 属性。(OCPBUGS-29025)

1.9.21.3. 更新

要将现有 OpenShift Container Platform 4.15 集群更新至此最新版本，请参阅使用 CLI 更新集群。