OpenShift Container Platform 4.7

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: 2021-05-06

OpenShift Container Platform 4.7 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 4.7 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-2020:5633）现已正式发布。此发行版本使用 Kubernetes 1.20 和 CRI-O 运行时。OpenShift Container Platform 4.7 的新功能、改变以及已知的问题包括在此文档中。

https://cloud.redhat.com/openshift 提供了 OpenShift Container Platform 4.7 集群 。您可以通过 OpenShift Container Platform 的 Red Hat OpenShift Cluster Manager 应用程序在内部环境或云环境中部署 OpenShift 集群。

OpenShift Container Platform 4.7 需要运行在 Red Hat Enterprise Linux（RHEL）7.7 及更新的版本，或 Red Hat Enterprise Linux CoreOS 4.6 上。

您必须将 RHCOS 机器用于 control plane（也称为 master）的系统，而 compute（也称为 worker）机器可以使用 RHCOS，或使用 Red Hat Enterprise Linux（RHEL）7.7 或更高版本。

重要

因为 compute 机器只支持 Red Hat Enterprise Linux（RHEL）版本 7.7 或更高版本，所以不能将 RHEL compute 机器升级到版本 8。

随着 OpenShift Container Platform 4.7 的发布，版本 4.4 现已结束其生命周期。如需更新相关信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

1.2. 使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始： master、slave、blacklist 和 whitelist。这些更改将在即将发行的几个发行本中逐渐实施。详情请查看 Red Hat CTO Chris Wright 信息。

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. 增强 LUKS、RAID 和 FBA DASD 的磁盘置备

OpenShift Container Platform 4.7 包括对裸机部署的磁盘置备的一些改进。新的 4.7 集群当前仅支持以下功能：

- 对 LUKS 磁盘加密的原生 Ignition 支持为加密的根文件系统提供额外的可配置性，并支持加密额外的数据文件系统。

- RHCOS 现在支持引导磁盘镜像（s390x 除外），从而在磁盘失败时提供冗余功能。如需更多信息，请参阅在安装过程中镜像磁盘。
- s390x 上的 RHCOS 可以安装到固定块架构（FBA）类型直接访问存储设备（DASD）磁盘中。
- 现在，当附加到使用 OpenShift Container Platform 4.7 或更高版本的集群创建的集群时，初始部署和早期引导时支持多路径。

注意

在新集群中，LUKS 配置必须使用原生 Ignition 机制，因为如果机器配置中包含旧的 **/etc/clevis.json** 文件，置备会失败。在从 OpenShift Container Platform 4.6 或更早版本升级的集群上，LUKS 只能使用 **/etc/clevis.json** 进行配置。

1.3.1.2. 使用 bootupd 更新引导装载程序

通过 **bootupd**，RHCOS 用户现在可以访问跨系统发行、系统分析操作系统更新工具，该工具管理在现代架构中运行的 UEFI 和旧 BIOS 引导模式中的固件和引导更新。

1.3.1.3. RHCOS 现在支持 RHEL 8.3

RHCOS 现在使用 Red Hat Enterprise Linux（RHEL）8.3 软件包。OpenShift Container Platform 4.6 和以下软件包仍保留在 RHEL 8.2 软件包中。这可让您获得最新修复、功能及改进，比如 NetworkManager 功能，以及最新的硬件支持和驱动程序更新。

1.3.1.4. RHCOS 现在支持 kdump 服务（技术预览）

在 RHCOS 中引进了 **kdump** 服务，以提供一个用于调试内核问题的崩溃转储机制。您可以使用这个服务保存系统内存内容以便稍后进行分析。**kdump** 服务不是在集群级别管理的，它必须基于每个节点手动启用和配置。如需更多信息，请参阅启用 kdump。

1.3.1.5. Ignition 更新

现在提供了以下 Ignition 更新：

- RHCOS 现在支持 Ignition 配置规格 3.2.0。这个版本支持磁盘分区调整大小、LUKS 加密存储和 **gs://** URL。
- 在非默认 AWS 分区中执行时，如 GovCloud 或 AWS China，Ignition 现在会从同一分区获取 **s3://** 资源。
- Ignition 现在支持 AWS EC2 实例元数据服务版本 2（IMDSv2）。

1.3.1.6. 配置尝试获取 DHCP 租期时使用的超时值

在以前的版本中，RHCOS DHCP 内核参数无法正常工作，因为获取 DHCP 租期的时间会超过默认的 45 秒。在这个版本中，可以配置在试图获取 DHCP 租期时使用的超时值。如需更多信息，请参阅 BZ#1879094。

1.3.1.7. RHCOS 支持多路径

RHCOS 现在支持主磁盘上的多路径，对硬件的故障有更强的抵抗力。您可以在多路径上设置 RHCOS，从而实现更高的主机可用性。如需更多信息，请参阅 BZ#1886229。

1.3.1.8. 从 Instance Metadata Service Version 2（IMDSv2）获取 AWS 配置

Ignition 现在支持从 Instance Metadata Service Version 2（IMDSv2）获取 AWS 上的配置。在这个版本中，AWS EC2 实例可以在禁用 IMDSv1 的情况下创建，因此需要 IMDSv2 从实例用户数据中读取 Ignition 配置。现在，Ignition 可以从实例用户数据读取其配置，无论 IMDSv1 是否启用。如需更多信息，请参阅 BZ#1899220。

1.3.1.9. qemu 客户机代理现在包括在 RHCOS 中

现在，RHCOS 中默认包括 Qemu 客户机代理。在这个版本中，通过向 RHV 管理接口报告有关 RHCOS 节点的有用信息，Red Hat Virtualization（RHV）管理员可以查看有关 RHCOS 节点的更详细的信息。如需更多信息，请参阅 BZ#1900759。

1.3.2. 安装和升级

1.3.2.1. 将集群安装到 AWS C2S Secret 区域

现在，您可以在 Amazon Web Services（AWS）上将集群安装到 Commercial Cloud Services（C2S）Secret 区域。由于 C2S 区域没有红帽发布的 RHCOS AMI，您必须上传属于该区的自定义 AMI。您还需要在集群安装过程中将 C2S 的 CA 证书包括在 **install-config.yaml** 文件的 **additionalTrustBundle** 字段中。部署到 C2S Secret 区域的集群无法访问互联网，因此您必须配置私有镜像 registry。

重要

由于当前 OpenShift Container Platform 的限制，目前还无法在安装到 AWS C2S Secret 区域的集群中使用 AWS 安全令牌服务（STS）。这包括使用 C2S Access Portal（CAP）提供的临时凭证。

安装程序不支持销毁部署到 C2S 区域的集群，您必须手动删除集群的资源。

如需更多信息，请参阅 AWS 政府和 secret 区域。

1.3.2.2. 使用个人加密密钥在 GCP 上安装集群

现在，您可以在 Google Cloud Platform（GCP）上安装集群，并使用个人加密密钥来加密虚拟机和持久性卷。这可以通过在 **install-config.yaml** 文件中设置 **controlPlane.platform.gcp.osDisk.encryptionKey**、**compute.platform.gcp.osDisk.encryptionKey** 或 **gcp.defaultMachinePlatform.osDisk.encryptionKey** 项来实现。

1.3.2.3. 使用裸机在 RHOSP 上安装集群

现在，您可以使用裸机在自己的 Red Hat OpenStack Platform（RHOSP）基础架构上安装集群。集群可以同时在裸机上运行 control plane 和计算机器，或只运行计算机器。如需更多信息，请参阅使用裸机部署集群。

使用 Kuryr 的集群不支持此功能。

1.3.2.4. 改进了安装时的 RHOSP 要求验证

OpenShift Container Platform 安装程序现在在尝试在 RHOSP 上安装集群前执行额外的验证。这些新验证包括：

- 资源配额

- 浮动 IP 地址重复
- 自定义集群操作系统镜像可用性

1.3.2.5. RHOSP 上新计算机器的自定义子网

现在，您可以使用您选择的网络和子网在 RHOSP 上运行的集群中创建计算机器。

1.3.2.6. 更轻松地访问 RHOSP 用户置备的基础架构 playbook

现在，使用安装文档中的脚本打包了在您自己的 RHOSP 基础架构上安装集群的 Ansible playbook。

1.3.2.7. 支持 RHOSP 上的 QEMU 客户机代理

现在您可以在安装过程中启用 QEMU 客户机代理支持。

1.3.2.8. 为 RHOSP 上的集群增加持久性卷限制

现在，您可以将节点配置为在安装过程中在 RHOSP 的集群中具有超过 26 个持久性 Cinder 卷。

1.3.2.9. 在 install-config.yaml 文件中弃用 computeFlavor 属性

install-config.yaml 文件中使用的 **computeFlavor** 属性已弃用。作为替代，您可以在 **platform.openstack.defaultMachinePlatform** 属性中配置机器池类型（flavor）。

1.3.2.10. 为带有安装程序置备的基础架构的集群的 bootstrap 主机使用静态 DHCP 保留

在以前的 OpenShift Container Platform 版本中，您无法为使用安装程序置备的基础架构的裸机安装的 bootstrap 主机分配静态 IP 地址。现在，您可以指定 bootstrap 虚拟机使用的 MAC 地址，即您可以为 bootstrap 主机使用静态 DHCP 保留。如需更多信息，请参阅 BZ#1867165。

1.3.2.11. 安装程序置备安装的改进

现在，裸机节点上的安装程序置备安装的安装程序会自动创建一个存储池来存储安装过程中所需的相关数据文件，如 ignition 文件。

在裸机节点上安装程序置备安装的安装程序提供了一组问题，要求用户回答一些问题，并使用适当的默认值生成 **install-config.yaml** 文件。您可以使用生成的 **install-config.yaml** 文件来创建集群，或者在创建集群前手动编辑该文件。

1.3.2.12. 安装程序置备的集群可将 DHCP 租期转换为静态 IP 地址

使用安装程序置备安装在裸机集群中部署的集群节点可使用静态 IP 地址部署。要部署集群以便节点使用静态 IP 地址，请配置 DHCP 服务器来为集群节点提供无限租期。当安装程序置备完每个节点后，分配程序脚本将在每个置备的节点上执行，并使用 DHCP 服务器提供的同一静态 IP 地址将 DHCP 租期转换为静态 IP 地址。

1.3.2.13. 如果机器配置池被降级，则立即阻止更新

如果机器配置池（MCP）处于 **degraded** 状态，Machine Config Operator（MCO）现在会将它的 **Upgradeable** 报告为 **False**。现在，在所有机器配置池都健康前，您将无法在次版本中执行更新（如从 4.7 升级到 4.8）。在以前的版本中，在一个降级的机器配置池中，Machine Config Operator 不会报告其

Upgradeable 状态为 **false**。因此，更新被允许，但最终会在更新 Machine Config Operator 时因为降级的机器配置池而失败。在 z-stream 版本中（例如从 4.7.1 到 4.7.2）没有对这个行为的改变。因此，您应该在执行 z-stream 更新前检查机器配置池状态。

1.3.3. Web 控制台

1.3.3.1. Web 控制台本地化

Web 控制台现在本地化，为全球用户提供语言支持。目前支持英语、日语和简体中文。显示的语言根据您的浏览器设置决定，但您可以选择语言来覆盖浏览器默认选项。在 **User** 下拉菜单中，选 **Language preferences** 来改变您的语言设置。现在，支持本地化的日期和时间。

1.3.3.2. 快速开始指南

快速开始是用户任务的指导教程。在 Web 控制台中，您可以在 **Help** 菜单下快速启动访问。它们在使用应用程序、Operator 或其他产品时特别有用。

如需更多信息，请参阅 web 控制台中创建快速启动指南。

1.3.3.3. Insights 插件

Insights 插件现在集成到 OpenShift Container Platform Web 控制台中。深入了解信息包括集群健康数据，如问题的总数以及问题的总风险。风险被标记为 **Critical**、**Important**、**Moderate** 或 **Low**。您可以快速导航到 Red Hat OpenShift Cluster Manager，以了解更多有关问题和如何修复它们的详细信息。

1.3.3.4. Developer Perspective (开发者视角)

- 控制台现在提供了一个可扩展的机制，允许 Red Hat Operator 构建并打包其自身的用户界面扩展控制台。通过这个功能，客户和 Operator 还可以添加自己的快速启动功能。现在，添加了来自 **Administrator** 和 **Developer** 视角的提示、过滤和访问权限，以便快速启动，并使相关内容更易用。
- 现在，您可以快速搜索通过拓扑 **List** 和 **Graph** 视图进行分组的工作负载和应用程序。
- 现在提供了用户首选项的持久性存储，因此，当用户从一个机器或浏览器移动到另一个机器或浏览器时，会获得一致性的体验。
- 如果您在集群中安装了 OpenShift GitOps Operator，可以使用 **Environments** 视图中的 **Argo CD** 链接导航到 Argo CD 用户界面。
- 可用性增强，如 in-context 菜单映射到 **Developer Catalog**，增加了使用 **Form** 或 **YAML** 选项来更新 Pipelines、Helm 和 Event Sources 配置的功能。
- 现在，在 **Developer Catalog** 中为特定服务（如 Operator Backed）、Helm、Builder Image、Template 和 Event Source 等服务增加了查看过滤条目的功能。
- 在集群中安装 Quay Container Security Operator 后：
  - 您可以查看所选项目的以下漏洞信息：
    - 漏洞和有漏洞镜像的总计数，
    - 基于严重性的、所有存在安全漏洞镜像的数量，
    - 可修复的漏洞数量，

        - 每个存在安全漏洞镜像会影响到的 pod 数量

    - 您可以查看漏洞的严重性详情，并启动存储在该存储库中漏洞镜像清单的 Quay 用户界面，以获取有关该漏洞的更多详情。

- 在集群中安装 OpenShift Virtualization Operator 后，您可以选择 **+Add** 视图中的 **Virtual Machines** 选项，然后使用 **Developer Catalog** 中的模板来创建虚拟机。

- 现在，web 终端的可用性有所提高：

    - 无论用户权限如何，所有用户都可以在控制台上访问 Web 终端。

    - 当 Web 终端长时间不活跃时，它会停止，并为用户提供重启的选项。

- 现在，管道工作流已被改进：

    - 与默认的构建配置系统相比，现在的管道创建过程可以更好地使用管道。当使用 **Import from git** 工作流时，构建配置默认不再与 Pipelines 一起创建，管道会在创建应用程序时立即启动。

    - 现在，您可以在 **Pipeline builder** 页中使用 **Pipeline builder** 选项或 **YAML view** 选项来配置管道。您还可以使用 Operator 安装的、可重复使用的代码片断和样本来创建详细的管道。

    - **PipelineRun** 页面现在包含一个 **TaskRuns** 标签页，该标签页列出了关联的任务运行。您可以点击所需的任务运行来查看任务运行和调试管道的详情。

    - 现在，您可以在 **Pipeline Details** 页面中看到管道的以下指标：管道运行持续时间、任务运行时间、每天运行的管道数量以及每天的管道成功比例。

    - 现在，**Pipeline Run details** 和 **Task Run details** 页中包括了一个 **Events** 标签页，它显示了特定 PipelineRun 或 TaskRun 的事件。

- 现在，无服务器（serverless）的可用性已被改进：

    - 您可以从 **Administrator** 视角访问 **Serving** 和 **Eventing** 页面，并使用控制台创建无服务器组件。

    - 您可以使用事件源创建工作流创建 Camel 连接器。

- Helm Chart 的可用性现已提高。

    - 作为集群管理员，您可以：

        - 添加或删除 Chart 仓库。

        - 删除了使用 Helm chart 的功能。

        - 使用快速入门来了解如何管理 Helm Chart 仓库。

    - 作为开发者，您可以：

        - 可以参阅目录中 Chart 卡上的 Chart 存储库名称，以便区分名称相同但来自不同 chart 存储库的 chart。

        - 在卡的目录级别中了解更多有关 chart 的信息。

        - 如果配置了多个存储库，可以按 Chart 存储库过滤目录。

1.3.3.5. IBM Z 和 LinuxONE

在这个版本中，IBM Z 和 LinuxONE 与 OpenShift Container Platform 4.7 兼容。请参阅 在 IBM Z 和 LinuxONE 上使用 z/VM 安装集群，或在受限网络中的 IBM Z 和 LinuxONE 中使用 z/VM安装集群 。

显著改进
IBM Z 和 LinuxONE 中的 OpenShift Container Platform 4.7 支持以下新功能：

- IBM Z 和 LinuxONE 上的、用户置备安装的 OpenShift Container Platform 4.7 支持 RHEL 8.3 或更高版本的 KVM 作为的虚拟机监控程序（hypervisor）。有关安装说明，请参阅在 IBM Z 和 LinuxONE 上使用 RHEL KVM 安装集群。
- 多路径（Multipathing）
- OpenShift Pipelines TP
- OpenShift Service Mesh
- 初始安装 OpenShift Container Platform 4.7 的 OVN-Kubernetes
- 使用 Fibre Channel 持久性存储
- 使用 Raw Block 的持久性存储
- SCSI 磁盘中的 z/VM 模拟 FBA 设备

支持的功能
IBM Z 和 LinuxONE 也支持以下功能：

- CodeReady Workspaces
- 开发人员 CLI - odo
- 使用 iSCSI 的持久性存储
- 使用本地卷的持久性存储（本地存储 Operator）

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

- 用于 IBM Z 的 OpenShift Container Platform 不包括以下技术预览功能：
  - 精度时间协议 (PTP) 硬件
  - CSI 卷快照
- 以下 OpenShift Container Platform 功能不被支持：
  - 日志转发
  - OpenShift Virtualization
  - CodeReady Containers (CRC)
  - OpenShift Metering
  - Multus CNI 插件

- FIPS 加密
- 加密数据存储在 etcd 中
- 使用机器健康检查功能自动修复损坏的机器
- 在 OpenShift Container Platform 部署过程中启用 Tang 模式磁盘加密。
- OpenShift Serverless
- Helm 命令行界面 (CLI) 工具
- 在节点上控制过量使用和管理容器密度
- etcd 集群 Operator
- CSI 卷克隆
- NVMe
- 4K FCP 块设备

- worker 节点必须运行 Red Hat Enterprise Linux CoreOS（RHCOS）。
- 必须使用 NFS 或其他支持的存储协议来置备持久性共享存储
- 必须使用本地存储（如 iSCSI、FC 或者带有 DASD、FCP 或 EDEV/FBA 的 LSO）来置备持久性非共享存储。
- 以下功能仅适用于 IBM Z 上的 OpenShift Container Platform 4.7：
  - IBM System Z /LinuxONE 为附加的 ECKD 存储的虚拟机启用了 HyperPAV

1.3.3.6. IBM Power 系统

在这个版本中，IBM Power Systems 与 OpenShift Container Platform 4.7 兼容。有关安装说明，请参阅在 IBM Power Systems 上安装集群，或在受限网络中在 IBM Power Systems 上安装集群。

显著改进
使用 OpenShift Container Platform 4.7 的 IBM Power Systems 支持以下新功能：

- 多路径（Multipathing）
- OpenShift Pipelines TP
- OpenShift Service Mesh
- 初始安装 OpenShift Container Platform 4.7 的 OVN-Kubernetes
- 使用 Fibre Channel 持久性存储
- 使用 Raw Block 的持久性存储
- 4K 磁盘支持

支持的功能
IBM Power 系统还支持以下功能：

- 目前，支持四个 Operator:
  - Cluster-Logging-Operator
  - Cluster-NFD-Operator
  - Elastic Search-Operator
  - Local Storage Operator
- 开发人员 CLI - odo
- CodeReady Workspaces
- 使用 iSCSI 的持久性存储
- HostPath

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

- 以下 OpenShift Container Platform 功能不被支持：
  - OpenShift Metering
  - OpenShift Serverless
  - OpenShift Virtualization
  - CodeReady Containers (CRC)
- worker 节点必须运行 Red Hat Enterprise Linux CoreOS（RHCOS）。
- 持久性存储必须是使用本地卷、网络文件系统（NFS）或 Container Storage Interface（CSI）的 Filesystem 类型

1.3.4. 安全性与合规性

1.3.4.1. 管理用户拥有的 OAuth 访问令牌

用户现在可以管理自己的 OAuth 访问令牌。这允许用户查看其令牌并删除任何超时或不再需要的令牌。

如需更多信息，请参阅管理用户拥有的 OAuth 访问令牌。

1.3.4.2. Cloud Credential Operator 支持在安装后删除 GCP 根凭证

现在，您可以删除或轮转 Cloud Credential Operator 在 Mint 模式中使用的 GCP admin 级别的凭证。这个选项需要在安装过程中存在管理员级别的凭证，但凭证不会永久存储在集群中，且无需长期存在。

1.3.4.3. Compliance Operator 的 CIS Kubernetes Benchmark 配置集

现在，您可以使用 Compliance Operator 执行互联网安全中心（CIS）Kubernetes Benchmark 检查。OpenShift Container Platform 的 CIS 配置集基于 CIS Kubernetes 检查。

在发布 CIS OpenShift Container Platform Benchmark 前，可以参阅 Red Hat OpenShift Container Platform Hardening Guide。

1.3.4.4. 安装程序置备的集群的安全引导支持

现在，在裸机节点上使用安装程序置备的基础架构部署集群时，可以使用安全引导机制部署集群。使用安全引导部署集群需要 UEFI 引导模式和 Red Fish Virtual Media。您不能在安全引导时使用自生成的密钥。

1.3.4.5. Advanced Cluster Management 2.2 的集成

Red Hat Advanced Cluster Management 2.2 现在与 Compliance Operator 集成。

1.3.5. 网络

1.3.5.1. 扩展了对从 OpenShift SDN 集群网络供应商迁移到 OVN-Kubernetes 集群网络供应商的平台支持

现在，在以下平台上的安装程序置备的集群中支持迁移至 OVN-Kubernetes 集群供应商：

- 裸机硬件
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure
- Red Hat OpenStack Platform (RHOSP)
- VMware vSphere

1.3.5.2. API 服务器、负载均衡器和节点的网络连接健康检查

为了帮助诊断集群网络连接问题，Cluster Network Operator（CNO）现在运行了一个连接性检查控制器来在集群中执行连接健康检查。连接测试的结果可在 **openshift-network-diagnostics** 命名空间中的 **PodNetworkConnectivityCheck** 对象中找到。如需更多信息，请参阅验证到端点的连接。

1.3.5.3. OVN-Kubernetes 出口防火墙支持 DNS 规则

在配置出口防火墙规则时，现在可以使用 DNS 域名 而不是 IP 地址。除了 OVN-Kubernetes 集群网络供应商出口防火墙实现中的 DNS 支持外，OpenShift SDN 集群网络供应商出口防火墙也可以实现 parity。

1.3.5.4. 用于在容器中在 DPDK 模式中与 SR-IOV 虚拟功能交互的程序库

对于与 Data Plane Development Kit（DPDK）模式中的 SR-IOV 虚拟功能（VF）交互的容器，**app-netutil** 库现在提供以下功能： **GetCPUInfo()**、**GetHugepages()** 和 **GetInterfaces()**。如需更多信息，请参阅 DPDK 库以用于容器应用程序。

1.3.5.5. 出口路由器 CNI（技术预览）

egress router CNI 插件以技术预览的形式引进。您可以使用插件以重定向模式部署出口路由器。与 OpenShift SDN 相比，这个出口路由器为 OVN-Kubernetes 提供奇偶校验，但只适用于重定向模式。该插件不会在 HTTP 代理或 DNS 代理模式下执行，这与 OpenShift SDN 实现不同。如需更多信息，请参阅在重定向模式下部署出口路由器 Pod。

1.3.5.6. OVN-Kubernetes IPsec 支持 pod 间加密流量

安装集群时，您可以使用启用 IPsec 配置 OVN-Kubernetes 集群网络供应商。通过启用 IPsec，pod 间的所有集群网络流量都通过加密的 IPsec 隧道发送。您不能在集群安装后启用或禁用 IPsec。

IPsec 隧道不用于配置为使用主机网络的 pod 间的网络流量。但是，主机网络上的 pod 发送的流量并由使用集群网络的 pod 接收的流量会使用 IPsec 隧道。如需更多信息，请参阅 IPsec 加密配置。

1.3.5.7. 用于使用 Red Hat OpenStack Platform（RHOSP）部署的 SR-IOV 网络节点策略增强

SR-IOV Network Operator 被改进，在 SR-IOV 网络节点策略的自定义资源中支持额外的字段 **spec.nicSelector.netFilter**。您可以使用新字段通过网络 ID 指定 RHOSP 网络。如需更多信息，请参阅配置 SR-IOV 网络设备。

1.3.5.8. 对没有 pod 选择器的服务的 RHOSP Kuryr 支持

在 RHOSP 上运行并使用 Kuryr 的集群， 现在支持没有指定 pod 选择器的服务。

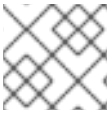
1.3.5.9. 调整 HTTP 标头名称

如果旧应用程序对 HTTP 标头名称中使用大小写敏感，请使用 Ingress Controller **spec.httpHeaders.headerNameCaseAdjustments** API 字段进行调整来适应旧的应用程序，直到它们被改变。

OpenShift Container Platform 将更新至 HAProxy 2.2（默认情况下 HTTP 标头名称是小写），例如，将 **Host: xyz.com** 改为 **host: xyz.com**。当 HAProxy 2.2 可用时，在升级 OpenShift Container Platform 前，确保使用 **spec.httpHeaders.headerNameCaseAdjustments** 来添加必要的配置。

1.3.5.10. Kubernetes NMState Operator（技术预览）

OpenShift Container Platform 4.7 使用 Kubernetes NMState Operator 作为技术预览功能在集群节点的第二个网络接口上提供安装后基于状态的网络配置。如需更多信息，请参阅使用 Kubernetes NMState（技术预览）。



注意

配置必须在调度 pod 前进行。

1.3.6. 存储

1.3.6.1. 使用 CSI 卷快照的持久性存储已正式发布

当使用支持卷快照的 CSI 驱动程序时，您可以使用 Container Storage Interface（CSI）创建、恢复和删除卷快照。此功能之前在 OpenShift Container Platform 4.4 中作为技术预览功能提供，现在在 OpenShift Container Platform 4.7 中正式发布并启用。

如需更多信息，请参阅使用 CSI 卷快照。

1.3.6.2. 使用 GCP PD CSI Driver Operator 的持久性存储（技术预览）

Google Cloud Platform（GCP）CSI 驱动程序会在 GCP 环境中自动部署和管理，允许您在不需要手动安装驱动程序的情况下动态置备这些卷。管理此驱动程序的 GCP PD CSI Driver Operator 只是一个技术预览。

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

1.3.6.3. 使用 OpenStack Cinder CSI Driver Operator 的持久性存储

现在，您可以使用 CSI 为 OpenStack Cinder 使用 CSI 驱动程序置备持久性卷。

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

1.3.6.4. vSphere 问题检测器（vSphere Problem Detector） Operator

vSphere 问题检测程序 Operator 会定期检查在 vSphere 环境中安装的 OpenShift Container Platform 集群的功能。Cluster Storage Operator 默认安装 vSphere Problem Detector Operator，允许您在 vSphere 集群上快速识别和排除常见的存储问题，如配置和权限。

1.3.6.5. Local Storage Operator 现在收集自定义资源

Local Storage Operator 现在包含 must-gather 镜像，允许您为诊断目的收集特定于此 Operator 的自定义资源。如需更多信息，请参阅 BZ#1756096。

1.3.7. 容器镜像仓库（Registry）

1.3.7.1. 开放容器计划镜像支持

OpenShift Container Platform 内部 registry 和镜像流现在支持 Open Container Initiative（OCI）镜像。您可以通过与使用 Docker **schema2** 镜像相同的方式使用 OCI 镜像。

1.3.7.2. 新的镜像流指标

在这个功能增强中，可以了解客户端是否使用 docker registry v1 协议利用镜像流导入，它会将 Operator 指标导出到 telemetry。与协议 v1 相关的指标数据现在包括在 telemetry 中。如需更多信息，请参阅 BZ#1885856。

1.3.8. Operator 生命周期

1.3.8.1. 安全 Operator 升级

要使升级更加稳定，建议 Operator 主动地与要更新的服务进行通信。如果一个服务正在处理关键操作，如在 OpenShift Virtualization 中实时迁移虚拟机（VM）或恢复数据库，则此时升级相关 Operator 可能会不安全。

在 OpenShift Container Platform 4.7 中，Operator 可以利用新的 **OperatorCondition** 资源与 Operator Lifecycle Manager（OLM）交流存在一个不可升级状态的信息，如相关的服务正在执行关键操作时。不可升级状态会延迟任何待处理的 Operator 升级（无论是自动还是手动批准），直到 Operator 完成操作并报告升级就绪状态。

如需有关 OLM 如何使用此通信方式的更多信息，请参阅 Operator 条件。

如需了解以集群管理员身份覆盖 OLM 中的状态的详细信息，请参阅管理 Operator 条件。

如需了解将项目更新为Operator 开发人员以使用通信频道的详细信息，请参阅启用 Operator 条件。

1.3.8.2. 将 pull secret 添加到目录源中

如果与 Operator Lifecycle Manager（OLM）管理的 Operator 相关的某些镜像托管在需要经过身份验证的容器镜像 registry（也称为私有 registry）中时，在默认情况下，OLM 和 OperatorHub 将无法拉取镜像。要启用访问权限，可以创建一个包含 registry 验证凭证的 pull secret。

通过在目录源中引用一个或多个 secret，可以拉取其中的一些所需镜像以便在 OperatorHub 中使用，其他镜像则需要更新全局集群 pull secret 或命名空间范围的 secret。

如需了解更多详细信息，请参阅从私有 registry 访问 Operator 镜像。

1.3.8.3. 将 Operator 目录的内容镜像（mirror）到容器镜像 registry

集群管理员可以使用 **oc adm catalog mirror** 命令将 Operator 目录的内容镜像（mirror）到容器镜像 registry 中。此增强更新了 **oc adm catalog mirror** 命令，现在还会将操作使用的索引镜像镜像（之前是一个需要 **oc image mirror** 命令的单独步骤）。如需更多信息，请参阅 BZ#1832968。

1.3.8.4. 创建新安装计划以获得更好的体验

删除一个等待用户批准的 **InstallPlan** 对象会导致 Operator 处于不可恢复的状态，因为无法完成 Operator 安装。此增强更新了 Operator Lifecycle Manager（OLM）以在以前待处理的项目被删除时创建新的安装计划。现在，用户可以批准新的安装计划，并开始安装 Operator。(BZ#1841175)

1.3.8.5. 通过首先将镜像镜像（mirror）到本地文件来将镜像镜像到断开连接的 registry

此增强更新了 **oc adm catalog mirror** 命令，通过首先将镜像镜像到本地文件来支持将镜像镜像到断开连接的 registry 中。例如：

```
$ oc adm catalog mirror <source_registry>/<repository>/<index_image>:<tag> file:///local/index
```

然后，您可以将本地 **v2/local/index** 目录移到断开连接的网络内的位置，并将本地文件镜像到断开连接的 registry 中：

```
$ oc adm catalog mirror file:///v2/local/index <disconnected_registry>/<repository>
```

如需更多信息，请参阅 BZ#1841885。

1.3.9. Operator 开发

1.3.9.1. operator SDK 现在被完全支持

从 OpenShift Container Platform 4.7 开始，Operator SDK 是一个完全支持的红帽服务。随着 Operator SDK v1.3.0 的下游发行版本，现在可以可直接从红帽下载官方支持的 Operator SDK 工具。

Operator SDK CLI 可以帮助 Operator 开发人员和独立的软件供应商（ISV）合作伙伴编写 Operator，这些 Operator 可以为用户提供更好的用户体验，并与 OpenShift 发行版和 Operator Lifecycle Manager（OLM）兼容。

Operator SDK 可让具有集群管理员权限的 Operator 作者访问基于 Kubernetes 的集群（如 OpenShift Container Platform），用以开发基于 Go、Ansible 或 Helm 的自己的 Operator。对于基于 Go 的 Operator，Kubebuilder 被嵌入到 SDK 中作为构建解决方案。这意味着现有的 Kubebuilder 项目可以和 SDK 一起使用，并可以继续正常工作。

以下是 Operator SDK 的一些主要特性：

对 **Operator Bundle Format** 的原生支持

Operator SDK 包括对 OpenShift Container Platform 4.6 中引入的 Operator Bundle Format 的原生支持。为 OLM 打包 Operator 所需的所有元数据均会自动生成。Operator 开发人员可以使用此功能直接从 CI 管道打包并测试其 Operator 以 OLM 和 OpenShift 发行版。

Operator Lifecycle Manager 集成

Operator SDK 为开发人员提供了从其工作站使用 OLM 测试 Operator 的简洁体验。您可以使用 **run bundle** 子命令在集群中运行 Operator，并测试在由 OLM 管理时 Operator 的行为是否正确。

Webhook 集成

Operator SDK 支持与 OLM 集成的 webhook，简化了安装具有准入或自定义资源定义（CRD）转换 Webhook 的 Operator。此功能使集群管理员需要手动注册 webhook、添加 TLS 证书和设置证书轮转。

验证 **scorecard**

Operator 作者应验证其 Operator 已正确打包且没有语法错误。要验证 Operator，Operator SDK 提供的 scorecard 工具将首先创建任何相关自定义资源（CR）和 Operator 所需的所有资源。然后，scorecard 在 Operator 部署中创建代理容器，用于记录对 API 服务器的调用并运行一些测试。执行的测试还会检查 CR 中的部分参数。

升级就绪度报告

Operator 开发人员可以使用 Operator SDK 来利用代码构建对 Operator 状况的支持，包括向 OLM 报告就绪状态。

触发 **Operator** 升级

您可以通过在 Operator SDK 中使用 OLM 集成来快速测试 Operator 升级，而无需手动管理索引镜像和目录源。**run bundle-upgrade** 子命令通过为以后的版本指定捆绑包镜像来自动触发已安装的 Operator 以升级到更新的版本。

注意

operator SDK v1.3.0 支持 Kubernetes 1.19。

如需有关 Operator SDK 的完整文档，请参阅 Operators。

1.3.10. Builds

将 **buildah** 版本输出到构建日志
在当前版本中，当 OpenShift Container Platform 执行构建且日志级别为 5 或更高级别时，集群会将 buildah 版本信息写入构建日志。这些信息可帮助红帽工程团队重现程序漏洞报告。在以前的版本中，构建日志中没有此版本信息。

协助镜像的 **Cluster Samples Operator**
OpenShift Container Platform 现在会在 **openshift-cluster-samples-operator** 命名空间中创建一个名为 **imagestreamtag-to-image** 的配置映射，它包含每个镜像流标签的条目（填充镜像）。您可以使用此配置映射作为导入镜像流所需的镜像的引用。

如需更多信息，请参阅用于镜像的 Cluster Samples Operator 帮助。

1.3.11. 机器 API

1.3.11.1. 在 AWS 支持的实例上运行的机器集

在 AWS 上运行的机器集现在支持 Dedicated 实例。通过在机器设置 YAML 文件中的 **providerSpec** 字段中指定一个专用租户来配置 Dedicated Instances。

如需更多信息，请参阅部署 Dedicated 实例的机器设置。

1.3.11.2. 在 GCP 上运行的机器集支持客户管理的加密密钥

现在，您可以为在 GCP 上运行的机器集启用客户管理的密钥加密。用户可以在机器设置 YAML 文件中的 **providerSpec** 字段下配置加密密钥。密钥用于对数据加密密钥进行加密，而不是加密客户的数据。

如需更多信息，请参阅启用机器集的客户管理的加密密钥。

1.3.11.3. 机器 API 组件遵循集群范围代理设置

Machine API 现在遵循集群范围的代理设置。当配置了集群范围的代理时，所有 Machine API 组件都会通过配置的代理路由流量。

1.3.11.4. 有些机器配置更新不再导致自动重启

Machine Config Operator（MCO）不再会在以下机器配置更改时自动重新引导所有对应的节点：

- 在机器配置的 **spec.config.ignition.passwd.users.sshAuthorizedKeys** 参数中更改 SSH 密钥
- 在 **openshift-config** 命名空间中更改全局 pull secret 或 pull secret
- 对 **/etc/containers/registries.conf** 文件的更改，如添加或编辑一个 **ImageContentSourcePolicy** 对象

如需更多信息，请参阅了解 Machine Config Operator。

1.3.11.5. BareMetalHost API 支持软关闭

在 OpenShift Container Platform 4.6 中,当 BareMetalHost API 中的在线标记设置为 **false** 时，Bare Metal Operator 会“硬”关闭节点。 也就是说，它在不给出操作系统或工作负载时间响应的情况下关闭电源。在 OpenShift Container Platform 4.7 及后续版本中，API 会向节点的操作系统发送信号，提示其关闭，然后等待节点以"软"模式关闭。如果操作系统在三分钟内没有关闭节点，Bare Metal Operator 会执行"硬"关闭。

OpenShift Container Platform 4.8 为补救目的执行"硬"关闭，比如节点存在已知问题。为补救执行"硬"关闭的行为将返回到 OpenShift Container Platform 4.7。

1.3.12. 节点

1.3.12.1. descheduler 已正式发布

descheduler 现已正式发布。Descheduler 提供了驱除正在运行的 pod 的功能，以便可将 pod 重新调度到更合适的节点上。您可以启用一个或多个 descheduler 配置集：

- **AffinityAndTaints**：驱除违反了 pod 间的反关联性、节点关联性和节点污点的 pod。
- **TopologyAndDuplicates**：驱除 pod 以尽量在节点间平均分配类似的 pod 或相同拓扑域的 pod。
- **LifecycleAndUtilization**：驱除长时间运行的 pod，并平衡节点之间的资源使用情况。

注意

在 GA 时，您可以启用 descheduler 配置集并配置 descheduler 间隔。在技术预览期间可用的其他设置都不再可用。

如需更多信息，请参阅使用 descheduler 驱除 pod。

1.3.12.2. 调度程序配置集（技术预览）

现在，您可以指定一个调度程序配置集来控制 pod 如何调度到节点上。这是配置调度程序策略的替代。可用的调度程序配置集如下：

- **LowNodeUtilization**：此配置集尝试在节点间平均分配 pod，以获得每个节点的资源用量较低。
- **HighNodeUtilization**：此配置集会尽量将 pod 放置到尽量少的节点中，以最小化每个节点用量。
- **NoScoring**：这是一个低延迟配置集，通过禁用所有分数（score）插件来实现最快的调度周期。这可能会为更快的调度决策提供更好的要求。

如需更多信息,请参阅使用调度程序配置集调度 pod。

1.3.12.3. 内存使用率自动缩放 GA

现在，根据内存使用率自动缩放已被正式发布（GA）。您可以创建 pod 横向自动扩展自定义资源，以自动扩展与部署配置或复制控制器关联的 pod，以维护您指定的平均内存使用率（可以是一个直接值，也可以是请求的内存百分比）。如需更多信息，请参阅根据内存使用率创建 pod 横向自动扩展对象。

1.3.12.4. 对于 RHOSP 上的集群自动缩放至零台机器

在 RHOSP 上运行的集群现在可以自动缩放为零台机器。

1.3.12.5. 优先级类的非抢占选项（技术预览）

现在，您可以通过将 **preemptionPolicy** 字段设置为 **Never**，将优先级类配置为非抢占。具有此优先级类设置的 Pod 放置在较低优先级 pod 的调度队列中，但不抢占其他 pod。

如需更多信息，请参阅非抢占优先级类。

1.3.12.6. 使用 CRI-O 为节点主机进程指定 CPU

CRI-O 现在支持为节点主机进程（如 kubelet、CRI-O 等）指定 CPU。通过在 **crio.conf** 文件中使用 **infra_ctr_cpuset** 参数，您可以为节点主机进程保留 CPU，以便 OpenShift Container Platform pod 在不需要这些 CPU 上运行其他进程的情况下运行需要保证 CPU 操作的 OpenShift Container Platform pod。如果 Pod 请求有保证的 CPU，则不需要与节点主机进程争用 CPU 时间。如需更多信息，请参阅 **BZ#1775444**。

1.3.13. Red Hat OpenShift Logging

Cluster Logging 变为 **Red Hat OpenShift Logging**
在这个版本中，*Cluster Logging* 变为 *Red Hat OpenShift Logging* 版本 5.0。如需更多信息，请参阅 Red Hat OpenShift Logging 5.0 发行注记。

1.3.14. 监控

1.3.14.1. 对规则更改的警报

OpenShift Container Platform 4.7 包含以下警报规则更改：

> 例 1.1. 对规则更改的警报

- 添加了 **AlertmanagerClusterCrashlooping** 警报。如果集群中至少有一半 Alertmanager 实例处于 crashlooping 状态时，会发出关键警报通知。
- 添加 **AlertmanagerClusterDown** 警报。如果集群中至少有一半 Alertmanager 实例停机，会发出关键警报通知。
- 添加 **AlertmanagerClusterFailedToSendAlerts** 警报。如果集群中的所有 Alertmanager 实例都无法发送通知，会发出关键警报通知。
- 添加 **AlertmanagerFailedToSendAlerts** 警报。如果 Alertmanager 实例无法发送通知，发出警告警报通知。
- 添加了 **etcdBackendQuotaLowSpace** 警报。如果 etcd 集群的数据库大小超过 etcd 实例上定义的配额，会发出关键警报通知。
- 添加了 **etcdExcessiveDatabaseGrowth** 警报。如果发现有大量的 etcd 写入，导致 etcd 实例在四小时的时间内数据库大小增加了 50%，会发送警告警报通知。
- 添加了 **etcdHighFsyncDurations** 警报。如果一个 etcd 集群的 99% 的 **fsync** 持续时间都太高时，会发送关键警报通知。
- 添加了 **KubeletClientCertificateRenewalErrors** 警报。如果 Kubelet 无法更新其客户端证书，发送警告警报通知。
- 添加了 **KubeletServerCertificateRenewalErrors** 警报。如果 Kubelet 无法更新其服务器证书，发送警告警报通知。
- 添加了 **NTODegraded** 警报。如果 Node Tuning Operator 降级，发送警告警报通知。
- 添加了 **NTOPodsNotReady** 警报。如果节点上的特定 pod 没有就绪，发送警告警报通知。
- 添加了 **PrometheusOperatorNotReady** 警报。如果 Prometheus Operator 实例未就绪，发送警告警报通知。
- 添加了 **PrometheusOperatorRejectedResources** 警报。如果 Prometheus Operator 拒绝特定资源，发送警告警报通知。
- 添加了 **PrometheusOperatorSyncFailed** 警报。如果 Prometheus Operator 控制器无法协调特定对象，发送警告警报通知。
- 添加了 **PrometheusTargetLimitHit** 警报。如果因为有些提取配置超过目标限制，Prometheus 放弃了目标，发送警告警报通知。
- 添加了 **ThanosSidecarPrometheusDown** 警报。如果 Thanos sidecar 无法连接到 Prometheus，发送关键警报通知。
- 添加了 **ThanosSidecarUnhealthy** 警报。如果在指定时间段内 Thanos sidecar 不健康，发送关键警报通知。
- 更新了 **NodeClockNotSynchronising** 警报，以防止在使用 chrony 时间服务 **chronyd** 的环境中出现假的正数。
- 对 **NodeNetworkReceiveErrs** 警报进行了更新，以确保当只报告少量错误时，警报不会触发。该规则现在使用错误与数据包总数的比例，而不是错误的绝对数量。
- 对 **NodeNetworkTransmitErrs** 警报进行了更新，以确保当只报告少量错误时，警报不会触发。该规则现在使用错误与数据包总数的比例，而不是错误的绝对数量。

- 带有严重性级别 warning 和 critical 的 **etcdHighNumberOfFailedHTTPRequests** 警告会被删除。如果 etcd 实例上有高百分比的 HTTP 请求失败，这些警报就会触发。

注意

红帽不保证指标、记录规则或警报规则的向后兼容。

1.3.14.2. 监控堆栈组件和依赖项的版本更新

OpenShift Container Platform 4.7 包括对以下监控堆栈组件和依赖项的版本更新：

- Prometheus Operator 现在为 0.44.1 版本。
- Thanos 现在为 0.17.2 版本。

1.3.14.3. 不支持 Prometheus Operator 中的 AlertmanagerConfig CRD

不支持使用 Prometheus Operator 中的 **AlertmanagerConfig** 自定义资源定义（CRD）修改 Alertmanager 配置。

如需更多信息，请参阅监控的支持注意事项。

1.3.14.4. 新的 API 性能监控仪表板

API Performance 仪表板现在可以通过 web 控制台获得。此仪表板可用于帮助解决 Kubernetes API 服务器或 OpenShift API 服务器的性能问题。您可以通过导航到 **Monitoring → Dashboards** 并选择 **API Performance** 仪表板，从 **Administrator** 视角中的 Web 控制台访问 **API Performance** 仪表板。

此仪表板提供 API 服务器指标，例如：

- 请求持续时间
- 请求率
- 请求终止
- 进行中的请求
- 请求被终止
- etcd 请求持续时间
- etcd 对象计数
- 长时间运行的请求
- 响应状态代码
- 响应大小
- 优先级和公平

1.3.14.5. 命名空间（Pods）和 Pod Kubernetes 网络仪表板在 Grafana 中启用

Namespace(Pods) 和 Pod Kubernetes 网络仪表板现在在 Grafana 中启用。您可以通过导航到 **Monitoring → Dashboards → Grafana UI**，从 **Administrator** 视角中的 Web 控制台访问 **Namespace(Pods) 和 Pod** 仪表板。

这些仪表板提供网络指标，例如：

- 每个命名空间或每个 pod 的当前字节率
- 每个命名空间或每个 pod 传输的字节率
- 接收的带宽
- 传输的带宽
- 接收到的数据包的比例
- 传输的数据包的比例
- 接收到的数据包丢弃的比例
- 发送数据包丢弃的比例

1.3.14.6. 用于裸机集群的硬件遥测的 hwmon 数据收集

hwmon 数据收集功能可用于硬件健康遥测，比如 CPU 温度和裸机集群的风扇速度。

1.3.14.7. Thanos Querier 的 loglevel 配置字段

现在您可以为调试等目的配置 Thanos Querier **logLevel** 字段。

1.3.14.8. 为监控用户定义的项目在 config-reloader 容器上删除了内存限值

对于 Prometheus 和 Thanos Ruler pod，内存限制从 **openshift-user-workload-monitoring** 命名空间中的 **config-reloader** 容器中删除。在以前的版本中，当容器使用的内存超过了定义的限制时，会出现 OOM 终止 **config-reloader** 容器的问题。现在，这个问题已解决。

1.3.14.9. 删除了用于监控您自己的服务的已弃用的技术预览配置

现在，启用了监控其自身服务的前一个技术预览配置已被删除，在 OpenShift Container Platform 4.7 中不被支持。**techPreviewUserWorkload** 字段从 **cluster-monitoring-config ConfigMap** 对象中删除，不再被支持。

如需了解更多与监控用户定义的项目相关的信息，请参阅了解监控堆栈。

1.3.15. 扩展

1.3.15.1. 集群最大限制

针对 OpenShift Container Platform 4.7 的集群最大限制指导信息已更新。

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

1.3.15.2. 测试来确定 CPU 延迟

作为 CNF-test 容器一部分的延迟测试提供了一种方式来测量隔离的 CPU 延迟是否低于请求的上限。

有关运行延迟测试的详情，请参阅运行延迟测试。

1.3.15.3. Performance Addon Operator 中新的全局DisableIrqLoadBalancing 功能允许为保证的 pod CPU 禁用全局设备中断处理

Performance Addon Operator 通过将其划分为为集群和操作系统日常任务处理保留 CPU 以及为工作负载隔离隔离的 CPU 来管理主机 CPU。新的性能配置集 **globallyDisableIrqLoadBalancing** 字段可用来管理设备中断是否由隔离的 CPU 集处理。

新的 pod 注解 **irq-load-balancing.crio.io** 和 **cpu-quota.crio.io** 与 **globallyDisableIrqLoadBalancing** 一起使用，用于定义是否为 pod 处理设备中断。配置后，CRI-O 仅在 pod 正在运行时禁用设备中断。

如需更多信息，请参阅管理设备中断处理以获得保证 pod 隔离的 CPU。

1.3.15.4. 新的 VRF CNI 插件允许将二级网络分配给 VRF

现在提供了一个新的 VRF CNI 插件，供您为 VRF 分配额外网络。当使用 CNO 自定义资源的 **rawConfig** 配置创建二级网络并为其配置 VRF 时，为 pod 创建的接口与 VRF 关联。您还可以使用 VRF CNI 插件将 SR-IOV 网络分配给 VRF。

如需更多信息，请参阅将二级网络分配给 VRF 和将 SR-IOV 网络分配给 VRF。

1.3.15.5. 为 CNF 启用了 xt_u32 端到端测试

xt_u32 是一个 iptables 内核模块，它允许基于任意内容进行数据包过滤。它可查看没有被其他 iptables 模块覆盖的标头或者特殊协议。

如需更多信息，请参阅为平台验证执行端到端测试。

1.3.16. 开发者体验

1.3.16.1. Red Hat OpenShift GitOps（技术预览）

Red Hat OpenShift GitOps 1.0 技术预览发行版本引入了一个声明式方法，可为云原生应用程序实施持续部署。您可以使用 Red Hat OpenShift GitOps 遵循 GitOps 原则来管理集群配置，并在混合集群、多集群、Kubernetes 环境间自动化安全、可预测的、可追踪和可重复的应用程序交付。它使用 Argo CD 作为核心，并添加其他工具，以便团队在集群间实施 GitOps 工作流。如需更多信息，请参阅了解 OpenShift GitOps。

1.3.17. Insights Operator

1.3.17.1. 深入了解 Operator 数据收集功能的增强

在 OpenShift Container Platform 4.7 中，Insights Operator 会收集以下附加信息：

- 最顶层的 100 个 **InstallPlan** 条目用于识别无效的 Operator Lifecycle Manager（OLM）安装
- 来自 Kubernetes 默认命名空间和 **openshift*** 内置命名空间的服务帐户
- **ContainerRuntimeConfig** 和 **MachineConfigPools** 配置文件，用以验证容器存储限制
- 所有可用的 **operator.openshift.io** 控制窗格资源的配置文件，以标识处于非受管状态的 Operator

- **NetNamespaces** 名称，包括它们的 **netID** 和 egress IP 地址
- 所有安装的 Operator Lifecycle Manager Operator 列表，包括版本信息
- 持久性卷定义（如果在 **openshift-image-registry** 配置中使用）
- 在 **openshift-apiserver-operator** 命名空间中出现特定的 pod 日志条目
- 在 **openshift-sdn** 命名空间中出现 **sdn** pod 的特定日志条目

通过这些额外的信息，红帽可以在 Red Hat OpenShift Cluster Manager 中提供改进的补救步骤。

1.3.18. 认证和授权

1.3.18.1. 使用 AWS 安全令牌服务（STS）为凭证运行 OpenShift Container Platform（技术预览）

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

如需更多信息，请参阅对 Amazon Web Services Secure Token Service（AWS STS）的支持 。

1.4. 主要的技术变化

OpenShift Container Platform 4.7 包括以下显著的技术更改。

Operator Lifecycle Manager 更新为使用 Kubernetes 1.20
Operator Lifecycle Manager（OLM）会在 Kubernetes 发行版本可用时保持最新状态。OLM 提供的 **ClusterServiceVersion**（CSV）资源由多个核心 Kubernetes 资源组成。当 OLM 增加 Kubernetes 依赖项时，也会更新内嵌的资源。

自 OpenShift Container Platform 4.7 起，OLM 及其相关组件已更新为使用 Kubernetes 1.20。通常，Kubernetes 与几个之前的版本向后兼容。建议操作员保持项目最新状，,以便保持兼容性，并利用更新的资源。

如需了解更多与向后兼容相关的信息，请参阅 OpenShift Container Platform 版本策略。

如需有关上游 Kubernetes 项目中的版本 skew 策略的详细信息，请参阅 Kubernetes 文档。

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

在下表中，被标记为以下状态的功能：

- **GA**: *正式发行*
- **DEP**: *已弃用*
- **REM**: *删除*

表 1.1. 过时和删除的功能

功能	OCP 4.5	OCP 4.6	OCP 4.7
OperatorSource 对象	DEP	REM	REM
Package Manifest Format（Operator 框架）	DEP	DEP	DEP
oc adm catalog build	DEP	DEP	DEP
oc adm catalog mirror 的 **--filter-by-os** 标记	GA	GA	DEP
v1beta1 CRD	DEP	DEP	DEP
Docker Registry v1 API	GA	DEP	DEP
Metering Operator	GA	DEP	DEP
调度程序策略	GA	GA	DEP
Cluster Samples Operator 的 **ImageChangesInProgress** 条件	GA	GA	DEP
Cluster Samples Operator 的 **MigrationInProgress** 条件	GA	GA	DEP
在 **apiVersion** 中将 **v1** 用于 OpenShift Container Platform 资源	GA	GA	DEP

1.5.1. 已弃用的功能

1.5.1.1. 调度程序策略

使用调度程序策略来控制 pod 放置已被弃用，计划在以后的发行版本中删除。如需有关技术预览的更多信息，请参阅使用调度程序配置集调度 pod。

1.5.1.2. 使用 filter-by-os 标记进行目录镜像

当使用 **oc adm catalog mirror** 命令镜像目录时，之前允许使用 **--filter-by-os** 标志对镜像内容进行过滤。这会破坏目录中指向清单列表而非清单的镜像的引用。**--filter-by-os** 标志现在只过滤拉取和解包的索引镜像。为了说明这一点，现在添加了新的 **--index-filter-by-os** 标志，应该使用这个新标志。

--filter-by-os 标志现在也已弃用。

1.5.1.3. Cluster Samples Operator 的 ImageChangesInProgress 条件

Cluster Samples Operator 配置资源中的条件不再实时跟踪镜像流镜像导入。in-progress 镜像流不再直接影响 **ClusterOperator** 实例 **openshift-samples** 的更新。Prometheus 警报现在会报告镜像流的错误。

1.5.1.4. Cluster Samples Operator 的 MigrationInProgress 条件

现在，升级跟踪可以通过其他条件，以及单个镜像流配置映射和 **imagestream-to-image** 配置映射实现。

1.5.1.5. 对 OpenShift Container Platform 资源使用 apiVersion v1。

目前，**oc** 会修改 OpenShift Container Platform 资源的 YAML 或 JSON 资源文件中的 **apiVersion** 值，把它从 **v1** 修复为对象的正确值。例如，将 **v1** 更正为 **DeploymentConfig** 对象的 **apps.openshift.io/v1**。此行为已弃用，并计划在以后的发行版本中删除。包含 ***.openshift.io** 的所有资源都必须与 API 索引中找到的 **apiVersion** 值匹配。

此发行版本添加了一个警告信息，它会在对象中缺少一个 **apiVersion** 时显示正确的 apiVersion 值。

```
Using non-groupfied API resources is deprecated and will be removed in a future release, update
apiVersion to "apps.openshift.io/v1" for your resource
```

当您遇到此消息时，更新资源文件以使用正确的值。

1.5.2. 删除的功能

1.5.2.1. 安装程序置备的集群不再需要 provisioningHostIP 或 bootstrapProvisioningIP

在裸机节点上使用安装程序置备安装时，OpenShift Container Platform 4.6 需要在没有 **provisioning** 网络的情况下，从 **baremetal** 网络为 **provisioningHostIP** 和 **bootstrapProvisioningIP** 配置设置提供两个 IP 地址。当在裸机节点上使用安装程序置备的基础架构，或在没有 **provisioning** 网络的情况下部署时，OpenShift Container Platform 4.7 中不再需要这些 IP 地址和配置设置。

1.5.2.2. 从示例镜像流中删除的镜像

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

```
registry.redhat.io/ubi8/go-toolset:1.13.4
registry.redhat.io/rhdm-7/rhdm-decisioncentral-rhel8:7.8.1
registry.redhat.io/rhdm-7/rhdm-decisioncentral-rhel8:7.8.0
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.8.1
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.8.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.8.1
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.8.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-rhel8:7.8.0
registry.redhat.io/rhpam-7/rhpam-kieserver-rhel8:7.8.1
registry.redhat.io/rhpam-7/rhpam-kieserver-rhel8:7.8.0
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.8.1
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.8.0
```

1.5.2.3. oc items removed

在这个版本中，与 **oc** 搭配使用的以下项将被删除：

- **--config** 选项。
- **OC_EDITOR** 环境变量。
- **convert** 子命令。

1.6. 程序错误修复

api-server-auth

- 在以前的版本中，**openshift-service-ca** 命名空间使用 **openshift.io/run-level:1** 标签，这会导致该命名空间中的 pod 使用额外的权限运行。此标签已被删除，现在该命名空间中的 pod 使用适当的权限运行。(BZ#1806915)

- 在以前的版本中，**openshift-service-ca-operator** 命名空间使用 **openshift.io/run-level:1** 标签，这会导致该命名空间中的 pod 使用额外的权限运行。此标签针对新安装移除，现在该命名空间中的 pod 以适当的权限运行。对于升级的集群，您可以手动删除此标签并重启受影响的 Pod。(BZ#1806917)

- 在以前的版本中，缺少 **openshift-oauth-apiserver** 命名空间中提取 OAuth API 服务器 pod 的配置，OAuth API 服务器 pod 的指标不会在 Prometheus 中查询。现在，添加了缺少的配置，OAuth API 服务器指标现在包括在 Prometheus 中。（BZ#1887428）

- 在以前的版本中，Cluster Authentication Operator 代码中缺少一个状况，会导致在日志上产生大量有关更新到部署的信息（实际上并没有发生）。确定是否更新 Operator 状态的逻辑已更新，Cluster Authentication Operator 日志不再接收没有发生的部署更新信息。(BZ#1891758)

- 在以前的版本中，Cluster Authentication Operator 只监视名为 **cluster** 的配置资源，这会导致 Operator 忽略 ingress 配置（名为 **default**）的变化。这会导致错误地假设在使用自定义节点选择器配置 ingress 时没有可调度的 worker 节点。Cluster Authentication Operator 现在会监控所有资源的名称，Operator 现在可以正确地观察入口配置更改，并协调 worker 节点的可用性。(BZ#1893386)

裸机硬件置备

- 之前在有些系统中，安装程序会在 Ironic 就绪前与 Ironic 进行通讯并失败。现在，这个问题已解决。(BZ#1902653)

- 在以前的版本中，当在 Dell 系统中使用虚拟介质时，如果在部署开始前已经连接了虚拟介质，则会失败。现在，Ironic 在出现这种情况时进行重试。（BZ#1910739）

- 在以前的版本中，master 节点在置备接口上丢失了其 IPv6 link-local 地址，因此在使用 IPv6 时无法置备。现在，为 **toggle addr_gen_mode** 添加了一个临时解决方案来防止发生这种情况。(BZ#1909682)

- 在以前的版本中，**cluster-baremetal-operator** 使用不正确的日志库。这会导致命令行参数与其他 Operator 不一致，因此并非所有 Kubernetes 库日志都会被记录。切换日志记录库解决了这个问题。(BZ#1906143)

- 在接口中使用 IPv6 时，在一定时间后网络管理器删除本地 IPv6 地址。这个问题会造成，在 IPv6 link-local 地址被删除后，节点的 PXE 引导失败。添加了一个临时解决方案来切换接口 IPv6 addr_gen_mode，这样可导致链接本地地址重新添加。(BZ#1901040)

- 以前，Supermicro 节点在成功部署到磁盘后会引导到 PXE。现在，通过在设置 **BootSourceOverrideTarget** 时始终设置 **BootSourceOverrideEnabled** 来解决这个问题现在，Supermicro 节点会在部署后引导到持久磁盘。（BZ#1918558）

- **baremetal** IPI 附带的服务代理镜像现在可以在启用了 UEFI 安全引导的系统中运行。因为网络引导与安全引导不兼容，在这种情况下需要使用虚拟介质。（BZ#1893648）

- **baremetal** IPI 不再启用节点自动发现。它没有被正确处理，从而导致重复的裸机主机注册。（BZ#1898517）

- 在以前的版本中，裸机置备镜像不包括 syslinux-nonlinux 软件包。因此，在使用 BIOS 引导模式的机器中安装虚拟介质会失败。该软件包现在包含在镜像中。(BZ#1862608)

- 在以前的版本中，某些 Dell 固件版本错误地报告 Redfish PowerState。将 Dell iDRAC 固件更新到版本 4.22.00.53 可解决这个问题。(BZ#1873305)

- 以前，Redfish 不在可以获得和设置 BIOS 配置值的接口列表中。因此，Redfish 无法在 BIOS 配置中使用。RedFish 现在包含在列表中，它可用于 BIOS 配置。(BZ#1877105)

- 在以前的版本中，用来设置 BIOS 配置的 Redfish 接口没有正确实施。因此，Dell iDRAC 无法设置 BIOS 配置值。现在，实现的错误已被修正。现在，Redfish 接口可以设置 BIOS 配置。(BZ#1877924)

- 在以前的版本中，通过 IPMI 处理引导设备设置的 Supermicro 节点会导致在镜像写入磁盘后使用 IPMI 和 UEFI 的节点失败。Supermicro 节点现在通过适当的 IPMI 代码从磁盘启动。因此，在部署后，Supermicro 节点从磁盘引导。(BZ#1885308)

- 在安装程序置备的基础架构上的裸机安装不再在提供无效的根设备提示时静默地跳过写入镜像。(BZ#1886327)

- 在以前的版本中，Supermicro 节点的引导模式信息不完整，这会导致使用 Redfish 进行部署失败。现在包含了这个引导模式的信息。因此，可使用 Redfish 部署 Supermicro 节点。(BZ#1888072)

- 嵌入在裸机安装程序置备的基础架构中的 Ironic API 服务现在使用四个 worker 而不是 8 个 worker。因此，内存用量会减少。(BZ#1894146)

Builds

- 在以前的版本中，Docker 构建无法更改 **/etc/pki/ca-trust** 目录的权限，或者在其中创建文件。这个问题是由于在 4.6 中修复 BZ#1826183 造成的，它添加了对带有CA 的 HTTPS 代理的构建的支持，并总是挂载 **/etc/pki/ca-trust**，这会阻止包含自身 CA 的构建或修改系统信任存储在运行时正常工作。当前发行版本通过恢复 Bug 1826183 解决了这个问题。现在，包含其自身 CA 的构建器镜像可以再次工作。(BZ#1891759)

- 在以前的版本中，在从 OpenShift Container Platform 版本 4.5 升级到版本 4.6 后，从私有存储库运行 **git clone** 会失败，因为构建不会将代理信息添加到用于拉取源代码的 Git 配置中。因此，如果集群使用全局代理且源是从私有 Git 存储库拉取的，则源代码就无法被拉取。现在，当集群使用全局代理时，Git 会被正确配置，如果集群使用全局代理，**git clone** 命令可以从私有 Git 存储库拉取源代码。(BZ#1896446)

- 在以前的版本中，节点 pull secret 功能无法正常工作。如果在 Source 和 Docker 策略构建中设置了 **forcePull: true**，则节点 pull secret 不会被使用。因此，构建无法拉取需要集群范围的 pull secret 的镜像。现在，节点 pull secret 始终与用户提供的 pull secret 合并。因此，构建可在设置 **forcePull: true** 时拉取镜像，源 registry 需要集群范围的 pull secret。(BZ#1883803)

- 在以前的版本中，当因为 Golang URL 解析而指定 SCP 风格的 SSH 位置时，OpenShift Container Platform 在 **git clone** 上构建会失败，它不适用于 Git SCP 风格的 SSH 位置。因此，当提供了这些类型的源 URL 时，OpenShift Container Platform 构建和 Source-to-Image（S2I）会失败。现在，构建和 S2I 可绕过 Golang URL 解析和删除 **ssh://** 前缀以容纳 Git SCP 风格的 SSH 位置（BZ#1884270）

- 在以前的版本中，因为无效的构建 pull secret（其身份验证密钥不是 base64 编码）导致的构建错误不会通过构建堆栈传播。因此，很难确定这些错误的根本原因。当前发行版本解决了这个问题，因此这些类型的构建错误通过构建堆栈传播。现在，用户可更容易确定出现无效的构建 pull secret 密钥的根本原因。（BZ#1918879）

Cloud Compute

- 在以前的版本中，Machine API 在用户凭证 secret 无效时不会向用户提供反馈意见，因此很难在云供应商凭证出现问题时进行诊断。现在，如果在创建或更新机器集时存在凭证问题（例如凭证 secret 不存在或存在错误的格式），用户会被警告。(BZ#1805639)

- 在以前的版本中，裸机操作器还通过删除 **Machine** 对象来删除底层主机，这不是机器控制器的预期操作。在这个版本中，搜索主机失败时在机器上设置 **InsufficientResourcesMachineError** 错误原因，因此可确保首先缩减没有主机的机器。如果主机被取消置备，机器会被移到 **Failed** 阶段。现在，机器健康检查会删除失败的机器，并且 **Machine** 对象不再会被自动删除。(BZ#1868104)

- 在以前的版本中，当机器进入 **Failed** 状态时，云供应商的状态将不再被协调。因此，机器状态会报告云虚拟机的状态为 **Running**。现在，如果机器处于 **Failed** 状态，机器状态会更加精确地反映云虚拟机的观察状态为 **Unknown**。（BZ#1875598）

- 在以前的版本中，几个 Machine API 自定义资源定义包含模板 schema 描述到对应的参考文档中的断开链接。这些链接已更新为正确的上游位置，不再会出现问题。(BZ#1876469)

- 在以前的版本中，**oc explain Provisioning** 命令不会返回自定义资源定义（CRD）描述，因为使用的是较老版本的 CRD 定义。CRD 版本已更新，因此 **Provisioning** CRD 的 **oc explain** 现在会返回预期信息。(BZ#1880787)

- 在以前的版本中，当用户创建或更新磁盘大小小于推荐最小值的机器时，当磁盘大小过低时，机器会在没有警告的情况启动失败。磁盘大小必须大于初始镜像大小。现在，用户可以收到一个磁盘大小较低并可能导致其机器或机器设置无法启动的警告信息。(BZ#1882723)

- 在以前的版本中，机器的状态在协调期间不会保留，因此 **Machine** 对象的 **instance-state** 注解和 **providerStatus.instanceState** 有时会显示不同的值。现在，机器状态会在协调的机器上复制，**instance-state** 注解与 **providerStatus.instanceState** 值一致。(BZ#1886848)

- 在以前的版本中，如果在 **MachineSet** 资源对象中将 **publicIP** 选项设置为 true 时，在断开连接的环境中运行的 Microsoft Azure 机器集会无法引导并进行扩展。现在，为了避免机器失败，用户不能使用这个无效的 **publicIP** 配置在断开连接的环境中创建机器集。（BZ#1889620）

- 在以前的版本中，当创建机器时，只有某些错误会导致 **mapi_instance_create_failed** 失败指标被更新。现在，创建机器时出现的任何错误都会正确更新 **mapi_instance_create_failed** 指标。(BZ#1890456)

- 在以前的版本中，在某些情况下，集群自动扩展使用模板节点作为节点扩展决策。偶尔，**nodeAffinity** predicate 无法按预期扩展，待处理 pod 无法调度。在这个版本中，模板节点可以包含尽量多的标签，以确保集群自动扩展可以扩展并传递节点关联性检查。（BZ#1891551）

- 在以前的版本中，机器集的默认删除优先级（**random**）不会使处于 **Ready** 状态的节点的优先级高于仍在构建的节点。因此，处于 **Ready** 状态的所有节点可能会在扩展机器集时被删除，然后立即缩减，特别是扩展大量机器时。这也可能导致集群不可用。现在，没有处于 **Ready** 状态的机器会被分配较低的优先级。因此，在缩减机器后马上进行大规模机器扩展时，会在删除正在运行工作负载的机器前，会先删除仍然在构建的机器。(BZ#1903733)

Cluster Version Operator

- 在以前的版本中，安装和升级过程中有一个信息显示当前的过程为 100%，即使当前进程还没有完成。这个错误信息是因为一个错误的舍入造成的。现在，这个百分比不再被循环使用，消息会正确显示已完成的子进程数量，以及准确的完成百分比值。(BZ#1768255)

- 在以前的版本中，当 Cluster Version Operator（CVO）合并 Cincinnati 元数据（如频道成员资格和勘误 URI）时，Cluster Version Operator（CVO）会把 pullspecs 与确切的 **available-update**

和 **current-target** 值进行比较。因此，如果您从一个镜像（mirrored）的、使用有效替代的 pullspec 的发行镜像安装或进行更新，则不会收到 Cincinnati 元数据。现在，CVO 会根据摘要比较发行版本，并正确关联 Cincinnati 元数据，如频道成员资格，无论哪个 registry 托管镜像。（BZ#1879976）

- 在以前的版本中，带有 metrics-serving goroutine 的竞争条件有时会导致 CVO 在关闭时卡住。因此，Management-object 协调和监控等 CVO 的行为不可能，更新和安装可能会停止。现在，CVO 会在几分钟后超时，并取消任何卡住的指标 goroutines，并按照预期关闭。(BZ#1891143)

- 在以前的版本中，有些 CVO 日志错误消息没有为正确侦测到的更改类型呈现变量。现在，这个变量可以被正确处理，错误信息会如预期显示。（BZ#1921277）

CNF 平台验证

- 在以前的版本中，为平台验证进行端到端测试会导致当机器配置不包含配置规格时 SCTP 验证步骤出现错误。在这个版本中，当没有找到配置规格时，会跳过 SCTP 测试。(BZ#1889275)

- 在以前的版本中，当 Performance Addon Operator 在有两个或更多 NUMA 节点的主机上运行 **hugepages** 测试，且性能配置集请求跨节点分发巨页时，测试会失败。在这个版本中，**hugepages** 测试如何决定 NUMA 节点的巨页数量。(BZ#1889633)

config-operator

- 在以前的版本中，在升级过程中已弃用的 **status.platformStatus** 字段不会被填充（从 OpenShift Container Platform 4.1 升级的集群）。因此，升级可能会失败。在这个版本中，更新了 Cluster Config Operator 来填充此字段。因此，不会因为没有填充此字段导致升级失败。(BZ#1890038)

控制台 Kubevirt 插件

- 在以前的版本中，存储类没有从 **DataVolume** 源的持久性卷声明中传播到 VM 磁盘列表。现在，存储类在 web 控制台的 VM 磁盘列表中可见。(BZ#1853352)

- 在以前的版本中，导入的 SR-IOV 网络可能会被设置为不同的网络接口类型。在这个版本中，导入的 SR-IOV 网络只被设置为 SR-IOV 网络接口类型。(BZ#1862918)

- 在以前的版本中，如果在集群中重复使用虚拟机名称，事件屏幕中显示的虚拟机事件不会被正确过滤，包括两个虚拟机的事件混合在一起。现在。事件被正确过滤，事件屏幕只显示属于当前虚拟机的事件。(BZ#1878701)

- 在以前的版本中, **VM Import** 向导创建的 **V2VVMWare** 和 **OvirtProvider** 对象不会被正确清理。现在，**V2VVMWare** 和 **OvirtProvider** 对象会如预期被删除。(BZ#1881347)

- 在以前的版本中，没有关联的虚拟机接口（VMI）不会显示使用数据。现在，如果 VMI 有可用的使用数据，则会显示。(BZ#1884654)

- 在以前的版本中，当克隆 PVC 时，其虚拟机状态会报告为 **pending**，但不会显示更多信息。现在，当克隆 PVC 时，VM 状态会报告 导入 进度条以及包含到 pod 或 PVC 链接的额外信息。(BZ#1885138)

- 在以前的版本中，VM 导入状态显示一个不正确的 VM 导入供应商。现在，VM 导入状态会显示正确的 VM 导入供应商。(BZ#1886977)

- 在以前的版本中，默认 pod 网络接口类型设置为错误的值。现在，默认的 pod 网络接口类型被设置为 masquerade。(BZ#1887797)

控制台存储插件

- 在以前的版本中，当安装 Local Storage Operator（LSO）时，节点上的磁盘不会被显示，且无法在该节点上启动磁盘发现。现在，当安装 LSO 时，**Disk** 标签页会被启用，如果发现磁盘操作还没有运行， 会显示 **Discover Disks** 选项。(BZ#1889724)

- 在这个版本中, **Disk Mode** 选项被重命名为 **Volume Mode**。（BZ#1920367）

Web 控制台 (开发者视角)

- 在以前的版本中，因为用户权限不足，用户无法从其他项目拉取镜像。在这个版本中，删除了所有用户界面检查角色绑定，并显示 **oc** 命令警告来帮助用户使用命令行。在这个版本中，用户不再无法从不同命名空间创建镜像，现在可以从其他项目中部署镜像。（BZ#1894020）

- 控制台使用之前版本的 **KafkaSource** 对象，该对象使用规格中的 **resources** 和 **service account** 字段。**KafkaSource** 对象的最新 **v1beta1** 版本删除了这些字段，因此用户无法使用 v1beta1 版本创建 **KafkaSource** 对象。这个问题现已解决，用户可以使用 v1beta1 版本创建 **KafkaSource** 对象。(BZ#1892653)

- 在以前的版本中，当使用带有 **.git** 后缀的 Git 存储库的源代码创建应用程序时，会显示一个 没有找到的页面 错误。在这个版本中, **.git** 后缀从存储库 URL 中删除，并将 SSH URL 转换为 HTTPS URL。现在，生成的链接会显示正确的软件仓库页面。(BZ#1896296)

- 在以前的版本中，**Topology** 视图中，除了显示 **Container Source** 和 **KameletBinding** 资源中创建的实际源外，还会显示底层 **SinkBinding** 资源，这可能会使用户感到混淆。这个问题已被解决。现在，**Topology** 视图 中只会显示为事件源创建的实际资源，底层 **SinkBinding** 资源（如果已创建）会在侧边栏中显示。(BZ#1906685)

- 在以前的版本中，当您在不创建事件自定义资源的情况下安装 Serverless Operator 时，会显示频道卡。当您点击卡时会显示一个混淆的警告信息。这个问题现已解决。现在，只有在频道自定义资源定义存在时才会显示带有正确警报消息的频道卡。(BZ#1909092)

- 在以前的版本中，当关闭 web 终端连接时，该会话的所有终端输出都会消失。这个问题已被解决。现在，即使会话关闭，终端输出也会被保留。(BZ#1909067)

- 虽然 Eventing 用户界面在 OpenShift Container Platform 4.6 中已是一个 GA 版本，但仍然会显示技术预览徽。技术预览徽标现已被删除，这个变化已后向移植到 OpenShift Container Platform 4.6.9 版本中。(BZ#1894810)

- 在以前的版本中，如果部署是使用控制台编辑流程编辑的，部署的卷挂载不会被保留。修改的部署 YAML 覆盖或移除 pod 模板规格中的卷挂载。这个问题已被解决。现在，即使使用控制台编辑流程编辑部署，卷挂载也会保留。(BZ#1867965)

- 如果有多个触发器，一个用于订阅 Knative 服务，另一个用于 In Memory Channel 作为订阅者，则 **Topology** 视图中不会显示 Knative 资源。这个问题现已解决，因此 Knative 数据模型返回正确的数据，Knative 资源会显示在 **Topology** 视图中。(BZ#1906683)

- 在以前的版本中，在断开连接的环境中，Helm chart 不会在 **Developer Catalog** 中显示，因为在获取代码时会出现无效的配置。这个问题已被解决，确保考虑代理环境变量，且 Helm chart 现在在 **Developer Catalog** 上显示。（BZ#1918748）

- 在运行 Pipeline 时，**TaskRun** 资源的日志标签页在输出中的命令后将字符串显示为 **undefined**。这是因为，有些边缘情况导致一些内部字符串操作打印到日志输出为 **undefined**。这个问题现已解决，管道日志输出不会从日志流中丢弃空白行，且不再输出 **undefined** 字符串。（BZ#1915898）

- 在以前的版本中，**Add** 流中的 **Port** 列表只为公开端口提供选项，它不允许您指定自定义端口。现在，这个列表已被一个 typeahead select 菜单替代，现在可以在创建应用程序时指定自定义端口。（BZ#1881881）

- 在以前的版本中，当有条件任务失败时，完成的管道运行会显示每个失败条件任务。这个问题已通过禁用失败的条件任务并在它们中添加跳过的图标来解决。这可让您更好地了解管道运行的状态。(BZ#1880389)

- 在以前的版本中，pod 扩展或缩减按钮适用于单个 pod 资源，当用户按缩放按钮时，页面会崩溃。这个问题已通过不显示单个 pod 资源扩展或缩减按钮来解决。(BZ#1909678)

- 在以前的版本中，下载 chart 以实例化 helm 发行版本的 Chart URL 无法访问。这是因为，在 Helm Chart 仓库中引用的 **index.yaml** 来自远程仓库。其中一些索引文件包含相对 Chart URL。现在，通过将相关 Chart URL 转换为绝对 URL 解决了这个问题，从而使 Chart URL 可以被访问。（BZ#1912907）

- Serverless 0.10 中，**trigger**、**subscription**、**channel** 和 **IMC** 的最新支持版本已更新。对应每个静态模型的静态模型显示一个 API 版本的 **beta**。现在，事件资源的 API 版本更新至 **v1**，UI 现在会显示最新支持的版本。(BZ#1890104)

- 在以前的版本中，当用户在 **Monitoring Dashboard** 选项卡上的工作负载间切换时，例如从特定部署到所有工作负载时，仪表板会显示白色画板且没有 chart。这个问题已被解决。现在，当用户在工作负载间切换时，仪表板会显示 chart。(BZ#1911129)

- 在以前的版本中，监控严重性级别（如 **critical** 和 **warning** ）的警报被当作信息级别的警报。因此，**Topology** 视图中这些警报的工作负载上不会显示 **Monitoring Alert** 图标。这个问题现已解决，如 **critical** 的警报被视为 警告 级别警报，并显示 **Monitoring Alert** 图标。（BZ#1925200）

- 在以前的版本中，在 Helm 安装表单的 **YAML** 视图中，仅显示 YAML 代码。现在，在 YAML 编辑器中添加了一个 **Schema** 视图来显示 schema 及其描述。(BZ#1886861)

- 在以前的版本中，所有 Pod 都会失败并显示 **ErrImagePull** 和 **ImagePullBackOff** 错误，即使添加了 Image Pull Secret 以访问外部私有镜像容器镜像 registry。这是因为镜像下载失败，因为它没有外部镜像 registry 的权限，集群会在不提供 secret 的情况下尝试直接从外部 URL 加载容器镜像。因此，部署会卡住，直到手动更新服务帐户或部署为止。现在，这个问题已被解决，新的部署可以从内部私有容器 registry 启动 pod，并从外部私有容器 registry 导入容器镜像，而无需对服务帐户或部署进行任何额外的更改。（BZ#1924955）

- 在创建示例应用程序时，**Developer** 视角会创建多个资源，这些资源相互依赖，且必须按特定顺序完成。在以前的版本中，准入插件有时无法检查其中一个资源，阻止 **Developer** 视角生成示例应用程序。这个问题已被解决。代码会按所需顺序创建资源，因此创建示例应用程序更为稳定。(BZ#1933665)

- 在以前的版本中，在更新资源配额资源时，API 服务器有时无法创建资源并返回 409 冲突响应状态代码。这个问题已被解决。现在，如果它收到 409 状态代码，OpenShift Web 控制台会最多重试请求三次。如果它继续接收 409 状态代码，控制台会显示错误消息。（BZ#1928228）

DNS

- 在以前的版本中，因为某些节点上的 **/etc/hosts** 文件包含无效条目，集群可能会遇到 DNS 解析错误。在这个版本中，因为 **/etc/hosts** 文件带有无效条目，DNS 解析不再会失败。(BZ#1882485)

etcd

- 在以前的版本中，etcd 就绪度探测使用 **lsof** 和 **grep** 命令，它们可能会留下失效进程。etcd 就绪度探测现在使用 TCP 端口探测，这个探测的成本较低，且不会创建失效的进程。(BZ#1844727)

- 在以前的版本中，当在 control plane 节点上更改 IP 地址时，导致磁盘上的证书无效，etcd 错误消息不知道 etcd 无法与 peer 连接的原因。现在，会检测到 control plane 节点上的 IP 地址变化，报告一个事件，**EtcdCertSignerController** 被标记为 **Degraded**。(BZ#1882176)

- 在以前的版本中，当 etcd 集群小于三个成员时，新的静态 pod 修订会发生，这会导致临时 quorum 丢失。现在，当所有 control plane 节点都不可用时，可以避免静态 pod 修订，并避免临时解决这些临时仲裁问题。(BZ#1892288)

- 在以前的版本中，etcd 备份包含一个特定于从中备份的 control plane 节点的恢复 YAML 文件，因此无法在其他 control plane 节点上恢复从一个 control plane 节点进行的备份。恢复 YAML 文件现在更为通用，以便在任何 control plane 节点上恢复 etcd 备份。（BZ#1895509）

- 在以前的版本中，etcd 备份脚本使用最后修改的时间戳来确定最新的修订，这会导致将不正确的静态 pod 资源存储在 etcd 备份中。etcd 备份脚本现在使用清单文件来决定最新的修订，正确的静态 pod 资源现在存储在 etcd 备份中。(BZ#1898954)

- 在以前的版本中，bootstrap 在使用 IPv6 双堆栈模式时无法检测可用的机器网络 CIDR，除非 IPv4 CIDR 是 install-config 机器网络 CIDR 阵列中的第一个元素。解析逻辑已被修复为通过所有机器网络 CIDR 进行循环，现在 IPv4 地址以双堆栈模式在机器网络 CIDR 中正确加载。(BZ#1907872)

- 在以前的版本中，如果删除了 **openshift-etcd** 命名空间，**etcd-endpoints** 配置映射不会被重新创建，集群也不会恢复。现在，如果缺少 **etcd-endpoints** 配置映射，则会重新创建它，从而可以恢复集群。（BZ#1916853）

镜像 Registry

- 上次 Kubernetes 更新在 API 中强制使用超时。使用这个超时的结果时，长的请求会在 34 秒后被丢弃。当导入大型软件仓库时，特别是那些带有几个标签的软件仓库时，会达到超时时间，因此无法象之前的版本一样成功导入。在 **oc** 客户端上有一个标志来设置不同的超时时间，但没有提供相关的示例，这使客户很难了解如何绕过 API 超时。通过 **oc** help 提供了使用标记的示例，客户现在更轻松地找到这个选项。(BZ#1878022)

- 在以前的版本中，使用同一日志记录软件包的两个不同版本会导致 Operator 日志部分丢失。在这个版本中，日志记录软件包版本与 Operator 使用的升级的日志软件包与 client-go 使用的版本一致。现在，日志不会丢失。（BZ#1883502）

- 在以前的版本中，pruner 会尝试使用镜像流检测 registry 名称，但没有镜像流来检测 registry 名称。在这个版本中，Image Registry Operator 为 pruner 提供 registry 名称。现在，修剪器不会依赖于镜像流的存在来检测 registry 名称。(BZ#1887010)

- 在以前的版本中，Operator pod 没有内存请求，这在节点上出现内存压力时，可能会因为内存不足在其他 **BestEffort** 容器前被终止。在这个版本中，添加了内存请求。现在，如果节点上存在其他 **BestEffort** 容器，Operator 不会在内存不足时被终止。（BZ#1888118）

- 在以前的版本中，pruner 会尝试使用镜像流检测 registry 名称，但没有镜像流来检测 registry 名称。在这个版本中，如果 registry 被配置或禁用 registry 修剪，Image Registry Operator 会为 pruner 提供 registry 名称。(BZ#1888494)

- 在以前的版本中，在定义 Operator 状态时，无法分析 Operand 部署状态。这意味着，在一些情况下，Image Registry Operator 带有两个相互冲突的信息。它通知用户其状态为不可用，同时还为没有降级。即使部署停止尝试启动并运行镜像 registry，这两个条件仍会被显示。在这种情况下，Operator 应该设置 Degraded 标记。通过将镜像 registry 部署纳入考量，如果 Operand 部署在尝试运行应用程序时达到其进度期限，Operator 现在会将自己设置为 Degraded。现在，当 Deployment 失败时，在达到进度期限后，Operator 会将其设置为 Degraded。在 Operator 部署进行时，Operator 仍然会报告自己为 Progressing。(BZ#1889921)

- 在以前的版本中，Image Registry Operator 不使用其入口点，因为提供了显式命令。因此，Operator 不能使用集群范围的 **trusted-ca**，Operator 无法连接到在没有自定义 **trusted-ca** 的情况下无法正常工作的存储供应商。在这个版本中，pod 规格中删除了显式命令。现在，镜像入口点由应用 **trusted-ca** 的容器使用。（BZ#1892799）

- 以前，pruner 的默认日志级别为 **2**。因此，当发生错误时，修剪器会转储堆栈 trace。在这个版本中，默认的日志级别被改为 **1**。现在，只有在没有堆栈追踪的情况下错误信息会输出。(BZ#1894677)

- 在以前的版本中，**configs.imageregistry.operator.openshift.io** status 字段在 Operator 同步过程中不会更新，这意味着 status 字段没有显示最新的 swift 配置。在这个版本中，同步过程会将 **configs.imageregistry.operator.openshift.io** 状态更新为 spec 值。spec 和 status 字段与 status 字段同步，显示已应用的配置。BZ#1907202）

- 在以前的版本中，在 HTTP/2 协议上缺少重试操作会导致一个相关的可重试错误，从而导致使用错误消息取消镜像(mirroring)。在这个版本中，当错误消息与 HTTP/2 协议相关的错误对应时，添加了一个重试功能。现在，对于这些错误，在多次尝试后会取消镜像操作。(BZ#1907421)

- 在以前的版本中，**node-ca** 守护进程中没有显式的用户和组群 ID，这混淆了 **node-ca** pod 中使用的用户和组。在这个版本中，为 **runAsUser** 和 **runAsGroup** 配置明确提供了 **node-ca** 守护进程。现在，在检查 **node-ca** DaemonSet YAML 文件时，用户和组会有明确的定义。（BZ#1914407）

ImageStreams

- 在以前的版本中，当镜像修剪器收集正在使用的镜像列表时，镜像修剪器不会考虑 **StatefulSet**、**Job** 和 **Cronjob** 对象使用的镜像。因此，可能会修剪错误的镜像。现在，镜像修剪器在创建镜像列表时会考虑这些对象正在使用的镜像。不再修剪这些对象正在使用的镜像。(BZ#1880068)

- 在以前的版本中，新创建的镜像流没有使用 **publicDockerImageRepository** 值进行解码。watchers 不会为新对象接收 **publicDockerImageRepository** 值。现在，镜像流使用正确的值进行解码。因此， watchers 会获取带有 **publicDockerImageRepository** 值的镜像流。(BZ#1912590)

Insights Operator

- 在以前的版本中，因为错误处理错误，当它观察到的文件有变化时，Operator 会随意结束其进程。改进了 Operator 的错误处理。现在，Operator 会继续运行，当观察到的文件改变时不再发送结束进程信号。(BZ#1884221)

- 在以前的版本中，Operator 在归档报告时不会使用资源的命名空间。因此，在不同的命名空间中具有相同名称的资源会被覆盖。Operator 现在在归档数据时结合使用报告路径与命名空间。因此，会为每个命名空间收集所有报告。(BZ#1886462)

安装程序

- 在以前的版本中，当使用 virtual-media 时，fast-track 模式可能无法正常工作，节点会在不同操作间重启。这个问题现已解决。(BZ#1893546)

- 在以前的版本中，在使用双堆栈部署时，worker 节点主机名与部署前检查的名称不匹配，从而导致节点需要手动批准。这个问题现已解决。(BZ#1895909)

- 现在，如果 control plane 和要部署的主机之间有一个小的、不超过一小时的时钟偏移，裸机置备将不会失败。(BZ#1906448)

- 当 vCenter 主机名中包含大写字母时，VMware vSphere 的 OpenShift Container Platform 安装程序会等待较长时间完成集群，然后再最终失败。安装程序现在会验证 vCenter 主机名在安装过程早期不包含大写字母，从而避免了长时间的等待时间。(BZ#1874248)

- 在以前的版本中，OpenShift Container Platform 安装程序的内部 Terraform 后端不支持从 Terraform 内核到 Terraform 供应商的输入，如 Amazon Web Services（AWS）。当将 **bootstrap.ign** 文件作为字符串传递给 AWS 供应商时，可能会超过输入限制，从而导致安装程序在创建 bootstrap Ignition S3 存储桶时失败。在这个版本中，Terraform 后端需要将 **bootstrap.ign** 作为磁盘上的路径传递，允许 AWS 供应商通过绕过输入大小限制来读取大文件。现在，安装程序在执行 Calico 安装时成功，它会创建大于输入限制的 bootstrap Ignition 文件。(BZ#1877116)

- 在以前的版本中，Red Hat OpenStack Platform（RHOSP）的 pre-flight 安装程序验证是在实例类型元数据上执行的。这可能会使安装无法将类型识别为具有完成安装所需的容量的 **baremetal**。这通常是由 RHOSP 管理员没有在其裸机类型上设置适当的元数据所致。现在，在检测到为 **baremetal** 的类型上跳过验证，以防止报告错误。(BZ#1878900)

- 在以前的版本中，安装程序不允许在 GCP 和 Azure 中安装集群的手动凭证模式。因此，用户无法使用手动凭证将集群安装到 GCP 或 Azure。安装程序现在可以验证为 GCP 和 Azure 提供的手动凭证。(BZ#1884691)

- 在以前的版本中，安装程序无法在销毁安装到 Azure 的集群前验证资源组是否存在。这会导致安装程序不断循环出现错误。安装程序现在会在销毁集群前验证资源组是否存在，允许成功销毁集群。(BZ#1888378)

- 在以前的版本中，安装程序不会检查以确保 AWS 帐户在使用共享资源创建集群时具有 **UnTagResources** 权限。因此，在销毁集群时，安装程序没有权限删除添加到预先存在的网络的标签。此程序错误修复添加了一个使用共享网络资源创建集群时的 **UnTagResources** 权限检查，以确保帐户在完成安装过程前具有适当的权限。(BZ#1888464)

- 要使 **openshift-install destroy cluster** 命令正常工作，安装程序初始创建的集群对象必须被删除。在某些情况下，托管区对象已被删除，导致安装程序挂起。现在，如果对象已被删除，安装程序会跳过删除对象，从而使集群可以被成功销毁。(BZ#1890228)

- 在以前的版本中，Red Hat OpenStack Platform（RHOSP）上的 control plane 端口没有被分配额外的用户定义的安全组。这会导致额外的用户定义的安全组规则无法正确应用到 control plane 节点。现在，额外的用户定义的安全组被分配给 control plane 端口，允许安全组规则正确应用到 control plane 节点。（BZ#1899853）

- 在以前的版本中，使用另一个安全组的默认 AWS 安全组的规则会阻止安装程序在销毁集群时删除其他安全组。这会导致集群销毁过程永远不会完成并保留 AWS 资源。现在删除默认安全组中的规则，从而取消删除其它安全组。这允许从集群中删除所有 AWS 资源。(BZ#1903277)

- Red Hat OpenStack Platform（RHOSP）验证中缺少的 guard 可能会获取带有空子网 ID 的子网列表，并导致一些非 RHOSP 云返回预期值。意外的错误代码验证失败，并阻止 OpenShift Container Platform 在这些非 RHOSP 云上安装。在这个版本中，增加了对空子网 ID 的缺少保护功能，从而可以正确验证。(BZ#1906517)

- 在以前的版本中，在 VMware vSphere 上安装用户置备的基础架构的引用负载均衡器是为简单的 TCP 检查配置的，健康检查不会考虑 api 服务器的健康状态。每当 API 服务器重启时，此配置有时会导致 API 请求失败。现在，健康检查现在根据 **/readyz** 端点验证 API 服务器健康状况，引用 API 负载均衡器现在会在 API 服务器重启过程中安全处理请求。(BZ#1836017)

- 在以前的版本中，当您使用安装程序时按 CTRL+C 时，该程序不会被中断，且并不总是如预期退出。现在，当您使用安装程序时按 CTRL+C 时，程序会中断并退出。BZ#1855351)

- 在以前的版本中，如果在使用无效凭证（如服务主体过期且没有显示 debug 日志）时尝试删除

Azure 中的集群，则会出现在没有删除集群时。除了不删除集群外，本地存储的集群元数据也会被删除，因此无法再次运行 **openshift-install destroy cluster** 命令删除集群。现在，如果在使用无效的 Azure 凭证时尝试删除集群，安装程序会退出并显示一个错误，您可以更新凭证并再次尝试。(BZ#1866925)

- 在以前的版本中，安装程序置备的基础架构裸机安装方法的 **install-config.yaml** 文件错误地使用 **provisioningHostIP** 名称而不是 **clusterProvisioningIP** 名称，这会导致文档和 YAML 文件中使用的实际字段名称断开连接。现在，**provisioningHostIP** 字段已弃用，而是使用 **clusterProvisioningIP**（删除断开连接）。(BZ#1868748)

- 在以前的版本中，安装程序不会在 Ignition 配置文件中检查过期的证书。过期的证书会导致安装失败，而无需解释。现在，安装程序会检查过期的证书并在证书过期时打印警告。(BZ#1870728)

kube-apiserver

- 在以前的版本中，**v1beta1** CRD 中将 **preserveUnknownFields** 字段设置为 **true**，因此 **oc explain** 没有解释 CRD 字段时不会出错。现在添加了一个验证条件，在未将 **preserveUnknownFields** 字段设置为 **false** 的 **v1beta** CRD 的状态会显示 **spec.preserveUnknownFields: Invalid value: true: must be false** 错误。(BZ#1848358)

- 在以前的版本中，IBM Cloud 集群的 OpenShift Container Platform 中默认禁用 **LocalStorageCapacityIsolation** 功能门。禁用后，设置临时存储请求或限制会导致 pod 无法调度。在这个版本中，代码被修改，在 **LocalStorageCapacityIsolation** 功能门被禁用时，临时存储请求或限制将被忽略，并且可以按预期调度 pod。(BZ#1886294)

Red Hat OpenShift Logging

在这个版本中，*Cluster Logging* 变为 *Red Hat OpenShift Logging* 版本 5.0。如需更多信息，请参阅 Red Hat OpenShift Logging 5.0 发行注记。

Machine Config Operator

- 在以前的版本中，当在 Red Hat OpenStack Platform（RHOSP）上部署并使用具有主机名的 HTTP 代理时，有时安装过程可能无法拉取容器镜像并报告错误消息 **unable to pull image**。此程序错误修复更正了在环境变量中设置代理的方式，节点可以从远程 registry 中拉取容器镜像。(BZ#1873556)

- 在以前的版本中，在升级过程中，上一版本的 Machine Config Controller（MCC）可能会响应较新的 Machine Config Operator（MCO）的配置变化。然后 MMC 引进了另一个更改，在升级过程中会导致不必要的重启。在这个版本中，MCC 无法响应较新的 MCO 配置更改，并避免不必要的重启。(BZ#1879099)

- 在以前的版本中，CoreDNS 分发查询的转发插件随机地发送到所有配置的 DNS 服务器。名称解析失败，因为 CoreDNS 会查询无法正常工作的 DNS 服务器。此程序错误修复设置了 forward 插件以使用后续策略，以便查询发送到响应的第一个 DNS 服务器。(BZ#1882209)

- 在以前的版本中，Machine Config Operator 只从 **multi-user.target.wants** 目录中读取启用的 systemd 目标单元。因此，任何不是以 **multi-user.target.wats** 目录为目标的单元都会被改为目标。在这个版本中，MCO 使用 systemd-preset 文件在 MCO 中创建预设置文件。因此，所有 systemd 服务都会如预期被启用和禁用。(BZ#1885365)

- 在以前的版本中，当将集群迁移到 OVN-Kubernetes 默认 Container Network Interface（CNI）时，预配置的 Linux 绑定接口上的绑定选项。因此，绑定配置使用 round-robin 而不是指定的模式，绑定可能无法正常工作。ovs-configuration.service（configure-ovs.sh）被修改为，将 Linux 绑定中的所有之前绑定选项复制到 **ovs-if-phys0** Network Manager 连接。因此，所有绑定应该象最初配置一样工作。（BZ#1899350）

- 在 OpenShift Container Platform 4.6 中，更改了使用 Budget Fair Queueing（BFQ）Linux I/O 调度程序。因此，etcd 中增加了 fsync I/O 延迟。在这个版本中，I/O 调度程序使用 mq-deadline 调度程序，但 NVMe 设备除外，它们配置为不使用 I/O 调度程序。对于 Red Hat Enterprise Linux CoreOS（RHCOS）更新，BFQ 调度程序仍然被使用。因此，延迟时间被降低到可接受的级别。（BZ#1899600）

Web 控制台（管理员视角）

- 在以前的版本中，依赖项的问题会在 OpenShift Container Platform web 控制台中产生永久卸载和重新挂载 **YAML Editor**。因此，YAML 编辑器每几秒钟就跳到 YAML 文件的顶部，此修复删除了依赖项的默认参数值。因此，**YAML Editor** 可以正常工作。(BZ#1903164)

- 在以前的版本中，OpenShift Container Platform Web 控制台中的 Operator 描述链接以沙盒 iframe 中呈现，它禁用了 iframe 中的 javascript。因此，当用户点击链接时，新标签页会继承沙箱限制，因此 JavaScript 不会运行链接页面。这些链接已通过在 Operator description iframe sandbox 属性中添加 **allow-popups-to-escape-** sandbox 参数来解决，它会在沙箱之外打开新标签页。现在，Operator 描述的链接会打开并正常运行。(BZ#1905416)

- 在以前的版本中，OpenShift Container Platform Web 控制台中的扩展 pod 功能不使用 **scale** 子资源，任何在部署配置中没有 **patch** 操作动词的自定义角色无法在 web 控制台中扩展 pod。在这个版本中，代码被修改，扩展 pod 功能现在可以使用 **scale** 子资源。因此，用户可以在 web 控制台中扩展 pod，而不必添加 **patch** 动词。（BZ#1911307）

- 在以前的版本中，在 OpenShift Container Platform web 控制台中创建一个自定义资源，其中将 **fieldDependency** 描述应用到使用与 **getJSONSchemaPropertySortWeight** helper 功能名称相同的 schema 属性中。因此，**DynamicForm** 组件会抛出异常，网页浏览器可能会崩溃。这个版本修改了 **getJSONSchemaPropertySortWeight** helper 功能来跟踪当前路径，并使用整个路径来确定依赖关系关系而不是只有字段名。因此，**DynamicForm** 组件不再会抛出异常。（BZ#1913969）

- 在以前的版本中，**SamplesTBRInaccessableOnBoot** 警报描述包含 "bootstrapped" 的错误。警报描述现在正确。（BZ#1914723）

- 在以前的版本中，CPU 和 Memory **specDescriptor** 字段在 YAML 编辑器中添加了一个空字符串。现在，这些字段不再在 YAML 编辑器中添加空字符串。(BZ#1797766)

- 在以前的版本中，**Subscription** 和 **CSV** 对象在 Operator 安装过程中在 **Installed Operators** 页面中显示。现在，这个重复已被解决，如果匹配的 **CSV** 对象已存在，**Subscription** Operator 不会在 **Installed Operators** 页中显示。(BZ#1854567)

- 在以前的版本中，当构建启动前一小时后，构建详情页中会显示空资源使用图表，但默认设置仅显示最新的一小时。现在，构建详情页中的使用情况图表显示构建运行时的数据。(BZ#1856351)

- 在以前的版本中，OpenAPI 定义只在初始页面加载时更新。OpenAPI 定义现在会以 5 分钟间隔进行更新，以及从 API 获取了型号时进行更新。OpenAPI 定义可以在不刷新页面的情况下显示最新的数据。(BZ#1856354)

- 在这个版本中，集群监控文档中无法访问的链接已被修复。(BZ#1856803)

- 在以前的版本中，Red Hat Marketplace URL 缺少 **utm_source** 参数。在本发行版本中，**utm_source** 参数添加到 Red Hat Marketplace URL 中。(BZ#1874901)

- 在以前的版本中，无法使用 **Escape** 键关闭项目选择下拉菜单。**Escape** 键的处理程序已经更新，用户可以退出并关闭项目选择下拉菜单。(BZ#1874968)

- 在以前的版本中，用于 Scheduling Status 的字体颜色与可访问性不兼容。对字体和字体颜色进行了更新，以便可以访问。调度禁用的节点显示在黄色警告图标（声明图标）中。(BZ#1875516)

- 在以前的版本中，一些 API 调用的补丁路径不正确。这会导致 spec 描述符字段更新资源属性。在这个版本里，从描述符构建补丁路径的逻辑已更新。(BZ#1876701)

- 在以前的版本中，**Unschedulable** status 字段仅在设置为 **True** 时才会出现。在这个发行本中，增加了一个新的 UX 设计来显示状态信息。(BZ#1878301)

- 在以前的版本中，如果具有相同命名空间中的另一个订阅具有手动批准策略，则具有自动批准策略的订阅的行为就像手动批准策略一样。在这个发行版本中，进行了一个更新来通知用户，采用手动批准策略的订阅会导致命名空间中的所有订阅都手动正常工作。(BZ#1882653)

- 在以前的版本中，一个手动安装计划可以对多个 Operator 有影响。但是，UI 并没有明确标明此情况是正确的，并显示 UI 请求批准时的 UI。因此，用户可以为多个 Operator 批准安装计划，但 UI 并没有明确显示这个情况。在本发行版本中，UI 列出了受手动批准计划影响的所有 Operator，并明确标明要安装哪些 Operator。(BZ#1882660)

- 在以前的版本中，通过创建命名空间模态创建重复的 namepsace 会导致严重错误。在这个发行版本中，我们添加了在创建项目和创建重复的项目时的错误处理程序不会导致严重错误。(BZ#1883563)

- 在以前的版本中，Prometheus swagger 定义包含一个无法解析的 **$ref** 属性，因此 Prometheus 操作对象创建表单出现运行时错误。现在，**definitions** 属性被添加到 schema 中，它由 **definitionFor** helper 功能返回，因此 **$ref** 会被解析且没有运行时错误。（BZ#1884613）

- 在以前的版本中，用户必须在安装状态页面出现前等待在后台载入所需的资源。现在，安装状态页已被更新，以便在用户开始安装 Operator 后马上出现。(BZ#1884664)

- 在以前的版本中，iOS 不支持通过带有自签名证书的安全 Websocket 连接，因此控制台上会显示白色屏幕。现在，如果带有自分配证书的 Websocket 无法成功，连接会返回 https，因此控制台可以被正确加载。(BZ#1885343)

- 在以前的版本中，当用户在 web 控制台中创建新角色绑定时，系统角色不会被显示。现在，系统角色会出现在角色名称下拉列表中，因此用户现在可以在创建新角色绑定时选择系统角色。(BZ#1886154)

- 在以前的版本中，终端假设所有 pod 都是 Linux pod，且没有考虑 Windows pod，因此终端无法用于 Windows Pod，因为默认为 sh 命令。现在，终端会检测 pod 类型并根据需要更改命令。(BZ#1886524)

- 在以前的版本中，新置备程序名称不包含 **kubernetes.io/** 前缀，因此用户可在 web-console 中使用 aws-ebs-csi-driver（gp2-csi）创建 PVC 时选择 RWX 和 RWO 访问模式。现在，在 AccessMode 映射中添加了额外的置备程序，因此在 web-console 中使用 aws-ebs-csi-driver（gp2-csi）创建 PVC 时，RWX 和 RWO 访问模式不可用。（BZ#1887380）

- 在以前的版本中，维护活跃命名空间的逻辑没有考虑删除当前活跃命名空间，因此最近在 UI 中删除的命名空间可能会保留为当前活跃的命名空间中。现在，活跃命名空间逻辑已被更新，在当前浏览器会话中，当用户删除当前活跃命名空间时，默认使用 "All namespaces"。因此，当用户删除当前活跃的命名空间时，同一浏览器会话中的活跃命名空间会自动更新为"所有命名空间"。(BZ#1887465)

- 在以前的版本中， v0.1.1 中的控制台厂商 'runc' 模块包含潜在的安全问题，因此 frog xray 会把 'runc' 依赖关系标记为潜在的安全漏洞。现在，'runc' 模块被固定到包含修复的 v1.0.0-rc8 版本，因此 'runc' 依赖项不再标记为潜在的漏洞。(BZ#1887864)

- 在以前的版本中，CSV 和 PackageManifests 列出了每个提供的 API 版本，而不是只是最新版本，因此 CSV 和 PackageManifest 页面可能会显示重复的 API。现在，会更新检索 API 的逻辑，以便只显示每个提供的 API 的最新版本。(BZ#1888150)

- 在以前的版本中，Install Operand Form 描述缺少 'SynchMarkdownView' 组件，因此它不会使用标记进行格式化。现在，Install Operand Form 被格式化为 markdown，因此安装 Operand Form 描述会被正确格式化。（BZ#1888036）

- 在以前的版本中，**fieldDependency specDescriptor** 没有使用非同级的依赖关系进行设计或测试。因此，无法保证非同级的依赖关系能够象预期一样工作。在这个版本中，定义了逻辑以确保非同级的依赖关系的行为如预期。(BZ#1890180)

- 在以前的版本中，如果本地的 **ensureKind** 函数没有正确处理 null **data** 参数，则会抛出异常。当使用 **data** 参数来确保不会抛出异常时，会添加空的 coalescence，这样可以安全地处理 null **data** 参数。（BZ#1892198）

- 在以前的版本中，在控制台中无法编辑 TLS secret。在这个版本中，添加了一个 **type** 字段，以便在控制台中更新 TLS secret。（BZ#1893351）

- 在这个版本中，web 控制台显示不正确的文件系统容量和使用数据解决了这个问题。(BZ#1893601)

- 在以前的版本中，web 控制台会错误地为错误的服务帐户 Prometheus Operator 授予权限，用于为 Operator Lifecycle Manager（OLM）Operator 提取指标。现在，控制台可以正确地为 prometheus-k8s 服务帐户授予权限，允许提取指标。(BZ#1893724)

- 在以前的版本中，控制台 pod 的 **TopologyKey** 设置为 **kubernetes.io/hostname**，这会在更新和区中断过程中造成可用性问题。在这个版本中，**TopologyKey** 设置为 **topology.kubernetes.io/zone**，它会在更新和区中断期间提高可用性。(BZ#1894216)

- 在以前的版本中，在从 OperatorHub 安装新 Operator 时，任何命名空间中缺少 **status** 块的 OperatorGroup 可能会导致 web 控制台中出现运行时错误。这个问题已解决。（BZ#1895372）

- 在以前的版本中，如果 CRD 的模型不存在，控制台会从 Provided APIs 列表中过滤出自定义资源定义（CRD）。因此，Details 选项卡在初始安装时不会显示 Provided API 卡，这代表 Operator 不提供 API。在此版本中，这个过滤器会从 API 卡中删除，因此即使模型已经存在，也会出现它们。因此，Provided API 卡及其对应标签页始终匹配，如果模型不可用，UI 将不再处于空状态。(BZ#1897354)

- 在某些情况下，lodash **startCase** 功能被应用于操作对象描述符字段。因此，字段标签将格式化为 Start Case，这将覆盖描述符的 **displayName** 属性。在未提供描述符 **displayName** 时，这个更新只应用于 **startCase**，这会在操作对象表单中正确显示 **displayName**。(BZ#1898532)

- 在以前的版本中，**response-jsonschema-form** 没有正确处理明确设置为 null 的数组类型 schema。如果传输至 DynamicForm 组件的表单数据包含数组类型属性设为 null，则会出现运行时异常。在这个版本中，在数组字段中添加了 null 检查，确保在这种情况下不再抛出异常。（BZ#1901531）

监控

- 在以前的版本中，**prometheus-adapter** 没有实现 OpenAPI 规格。因此，API 服务器每 60 秒记录了一个在 Prometheus Adapter 被部署到集群中时 OpenAPI 不存在的消息。另外，**KubeAPIErrorsHigh** 警报可能会因为日志中的错误而触发。在这个版本中，OpenAPI spec 被引入到 **prometheus-adapter** 中，它适用于 OpenShift Container Platform 中的其他核心 API 资源。(BZ#1819053)

- 在以前的版本中，升级安全上下文约束（SCC）的某些场景会导致 Prometheus 有状态集部署失败。现在，非根 **SCC** 用于用于监控的有状态设置部署。在这个版本中，需要对所有监控有状态集部署（如 Alertmanager、Prometheus 和 Thanos Ruler）的 Kubernetes 安全上下文设置进行以下配置：

```
securityContext:
  fsGroup: 65534 1
  runAsNonRoot: true
  runAsUser: 65534 2
```

1 文件系统组 ID 被设置为 **nobody** 用户, ID **65534**。kubelet 在 pod 启动时递归设置组 ID。如需有关为 pod 配置卷权限和所有权更改策略的更多信息，请参阅 Kubernetes 文档。

2 所有有状态的集合监控部署都以 **nobody** 用户，ID **65534** 身份运行。

(BZ#1868976)

- 在以前的版本中，CPU 字节时间（CPU 字节时间）是虚拟 CPU 等待实际 CPU 的时间，而虚拟机监控程序为另一个虚拟处理器提供服务，会影响报告 CPU 消耗的指标。因此，可能会报告 CPU 用量超过节点上的 CPU 数量。现在，报告 CPU 消耗的指标不会考虑 CPU 物理时间，因此报告 CPU 用量可以准确反映实际 CPU 用量。(BZ#1878766)

- 在以前的版本中，在没有升级权限的情况下验证请求可能会访问用户定义的项目中的 **/api/v1/query** 和 **/api/v1/query_range** 的端点。因此，可以访问常规服务帐户令牌的用户可以从任何被监控的目标读取指标。现在，**kube-rbac-proxy** 被配置为只允许请求到 **/metrics** 端点。在没有集群范围权限的情况下对 **/metrics** 的验证请，会接收到一个 HTTP 404 状态代码，以响应对 **api/v1/query** 和 **/api/v1/query_range** 端点的查询。（BZ#1913386）

网络

- **ovn-kube** 中检测默认网关的代码没有考虑多路径环境。因此，Kubernetes 节点启动失败，因为它们无法找到默认网关。现在，相关的逻辑已被修改，它会在有多路径时考虑第一个可用的网关。OVN-Kubernetes 现在可在使用多路径和多个默认网关的环境中工作。（BZ#1914250）

- 当以双堆栈模式部署集群时，OVN-Kubernetes 使用错误的数据源。
  OVN-Kubernetes 主控机节点执行初始同步，使 OVN 和 Kubernetes 系统数据库保持同步。这个问题导致 OVN-Kubernetes 启动出现竞争条件，导致某些 Kubernetes 服务无法访问。Bootstrap 逻辑会删除这些服务，因为它们被视为孤立。

  此程序漏洞已修复，确保了 Kubernetes 用作数据源。OVN-Kubernetes 现在可以正确启动，并在启动时保持 OVN 和 Kubernetes 同步。(BZ#1915295)

- 当通过在 Cluster Network Operator（CNO）配置对象中指定 **additionalNetworks** 小节来创建额外网络时，CNO 会管理所创建的 NetworkAttachmentDefinition 对象的生命周期。但是，如果更新 CNO 配置使其从 **additionalNetworks** 小节中排除额外网络，则该对象不会被删除。在这个发行版本中，CNO 现在删除所有与额外网络相关的对象。(BZ#1755586)

- 对于 OVN-Kubernetes 集群网络供应商，如果配置了出口 IP 地址，且托管出口 IP 地址的一个节点不可访问，分配给不可访问节点的任何出口 IP 地址都永不会被重新分配给其他节点。在本发行版本中，如果托管出口 IP 地址的节点不可访问，则会将出口 IP 地址分配给另一节点。(BZ#1877273)

- 对于 OVN-Kubernetes 集群网络供应商，**br-ex** 网桥的路由优先级可以被安装集群后添加的次网络接口的默认路由替代。当辅助设备的默认路由取代了节点上的 br-ex 网桥，集群网络就不再可以正常工作。在本发行版本中，**br-ex** 网桥的默认路由不能被替换。(BZ#1880259)

- 对于使用 OVN-Kubernetes 集群网络供应商的集群，当在集群中添加 Red Hat Enterprise Linux（RHEL）7 worker 节点时，新的 worker 节点无法连接到集群网络。在这个版本中，您可以成功添加 RHEL worker 节点。(BZ#1882667)

- 对于使用 OVN-Kubernetes 集群网络供应商的集群，无法将 VLAN 或绑定网络设备用作节点上的默认网关。在此发行版本中，OVN-Kubernetes 现在可以使用这些网络设备。(BZ#1884628)

- 对于使用 Kuryr 集群网络供应商的集群，为主机网络上的 pod 创建不必要的 Neutron 端口。在此发行版本中，主机网络 pod 不再创建 Neutron 端口。(BZ#1886871)

- 对于使用 OVN-Kubernetes 集群网络供应商的集群，**br-ex** 网桥不支持附加其他接口，如 **veth<N>** 对，同时添加到网桥中的接口无法正常工作。在这个版本里，新的接口可以被附加到 **br-ex** 接口并可以正常工作。(BZ#1887456)

- 对于使用 OVN-Kubernetes 集群网络供应商的集群，如果配置了 ExternalIP 地址，集群中的任何节点都未配置为使用该 IP 地址正确路由发送到 externalIP 的流量。现在，集群中的每个节点都被配置为使用 ExternalIP 的必要路由。(BZ#1890270)

- 对于使用 OpenShift SDN 集群网络供应商的集群，会删除命名空间和网络命名空间的顺序。如果首先删除与 Namespace 对象关联的 NetNamespace 对象，则无法再次重新创建该网络命名空间。在本发行版本中，命名空间及其关联的网络命名空间可以按任何顺序删除。(BZ#1892376)

- 对于使用 OpenShift SDN 集群网络供应商的集群，之前网络供应商会记录以下消息：**unable to allocate netid 1**。由于此消息对于任何小于 **10** 的 NETID 来说都不会有害，所以在此发行版本中，OpenShift SDN 不再为任何小于 **10** 的 NETID 发出信息。(BZ#1897073)

- 如果集群使用 OVN-Kubernetes 集群网络供应商，则所有入站 ICMPv6 都错误地发送到节点和 OVN。在本发行版本中，只有 ICMPv6 Neighbor Advertisements 和 Route Advertisements 发送到主机和 OVN。因此，发送到集群中节点的 ping 不再会出现重复的响应。(BZ#1897641)

- 在以前的版本中，在一个有大量节点的集群中，会生成过量多播 DNS（mDNS）流量。因此，网络交换机可能会溢出。此发行版本将 mDNS 查询限制为每秒一次。

- 在以前的版本中，创建使用 IPv6 的额外网络附加、Whereabouts CNI 插件以及指定排除的子网范围将忽略排除的子网范围。在这个版本中修正了这个插件，从而可以排除子网范围。(BZ#1900835)

- 在以前的版本中，在某些情况下 od 不会因为 Multus 错误条件终止。当出现问题时，Multus 会在日志中记录 **failed to destroy network for pod sandbox** 信息。在这个版本中，Multus 可以容忍已删除的缓存文件，pod 可以终止。(BZ#1900835)

- 在以前的版本中，当将 OpenShift SDN 网络供应商与网络策略搭配使用时，pod 可能会遇到网络连接问题，即使在不使用网络策略的命名空间中也是如此。此程序错误修复确保了实现网络策略的底层 Open vSwitch（OVS）流有效。（BZ#1914284）

- 在以前的版本中，当使用 OVN-Kubernetes 网络供应商并使用多个 pod 作为外部网关时，缩减 pod 会阻止命名空间中的其他 pod 路由流量到剩余的外部网关。相反，流量被路由到节点的默认网关。此程序错误修复可让 pod 继续将流量路由到剩余的外部网关。(BZ#1917605)

节点

- 在以前的版本中，如果 pod 或容器创建请求时间太长，集群的负载可能会出现超时问题。kubelet 试图重新请求该资源，即使 CRI-O 仍然在创建该资源，从而导致请求失败并出现 *name is reserved* 错误。CRI-O 完成原始请求后，它会注意到请求超时，并清理失败的 pod/container，再启动该过程。因此，pod 和容器创建可能会停止，kubelet 会报告多个 *name is reserved* 错误。这也可能导致已经过载的节点进一步超载。在这个版本中，修改了 CRI-O，以保存因为系统负载造成超时的 pod 或容器创建的过程。CRI-O 也阻止来自 kubelet 的新请求，因此 *name is reserved* 错误会较少。因此，当集群负载较大时，CRI-O 会减慢 kubelet 并减少集群的负载。节点上的总负载会减少，Kubelet 和 CRI-O 应该更快速地协调。(BZ#1785399)

- 在以前的版本中，卷中深度目录会导致 SELinux 重新标记时间。因此，容器创建请求可能会超

时，kubelet 会尝试重新请求该资源，从而导致 *error reserving ctr name* 或 *Kubelet may be retrying requests that are timing out in CRI-O due to system load* 错误。在这个版本中，修改了 CRI-O，以保存因为系统负载造成超时的 pod 或容器创建的过程。因此，容器请求会及时被处理。(BZ#1806000)

- 在以前的版本中，CRI-O 只使用 IPv4 iptables 管理主机端口映射。因此：主机端口无法用于 IPv6。在这个版本中，修改了 CRI-O 以支持 IPv6 主机端口。因此，主机端口可以如预期使用 IPv6。（BZ#1872128）

- 在以前的版本中，HTTP/2 传输没有附加到提供超时逻辑的连接中的正确选项，这会导致 VMWare 网络接口（及其他情况）片断几秒钟会导致连接失败。因此，连接静默会导致其他相关故障，如没有检测到节点停机、使用过时连接的 API 调用等。在这个版本中，添加了正确的超时。因此，系统中的 HTTP/2 连接更为可靠，副作用可以被控制。（BZ#1873114）

- 在以前的版本中，拓扑管理器端到端测试（**openshift-tests run-test**）需要在每个 worker 节点上运行 Machine Config Daemon（MCD），这是部署在 Red Hat Enterprise Linux CoreOS（RHCOS）节点上的节点的情况，而不是针对在 Red Hat Enterprise Linux（RHEL）上部署的节点。因此，当针对在 RHEL 上部署的集群运行时，Topology Manager 端到端测试会错误地失败。在这个版本中，测试已被修改，以跳过所有没有检测到 MCD 的节点。因此，不再报告假的故障。（BZ#1887509）

- 在以前的版本中，当状态缺失时，Kubelet 无法正确处理转换。因此，一些被终止的 pod 不会被重启。在这个版本中，添加了一个 **failed** 的容器状态，以便可以根据需要重启容器。因此，kubelet pod 处理不会导致无效状态转换。（BZ#1888041）

- 在以前的版本中，Kubernetes 1.19 及更新版本中缺少 **cAdvisor** 的机器指标。在这个版本中，代码已被修改来正确地收集 **CAdvisor** 机器指标数据。因此，会显示机器的指标数据。(BZ#1913096)

- 在以前的版本中，Horizontal Pod Autoscaler（HPA）忽略了指标不完整的 pod，如含有 init 容器的 pod。因此，任何带有 init 容器的 pod 都不会被扩展。在这个版本中，Prometheus Adapter 会为 init 容器发送完整的指标数据。因此，HPA 可以使用 init 容器扩展 pod。(BZ#1867477)

- 在以前的版本中，Vertical Pod Autoscaler（VPA）无法监控部署配置。因此，VPA 无法扩展部署配置工作负载。在这个版本中，VPA 为监控部署配置添加了适当的权限。因此，VPA 可以扩展部署配置工作负载。(BZ#1885213)

Node Tuning Operator

- 当创建无效的 Tuned 配置集时，**openshift-tuned** 监控器进程可能会忽略将来的配置集更新，且无法应用更新的配置集。在这个版本中，可以保留有关 Tuned 配置集应用程序成功或失败的状态信息。现在，在收到新的有效配置集时，**openshift-tuned** 从配置集应用程序失败中恢复。（BZ#1919970）

oauth-proxy

- 在以前的版本中，有失败的身份验证检查的旧记录。对 oauth-proxy 后面的服务的请求可能导致在代理日志中写入一行，从而导致日志中出现大量数据。在这个版本中，代理删除了非格式化的日志行。现在，代理不再遇到日志垃圾邮件。(BZ#1879878)

- 在以前的版本中，无效的选项处理会在使用 **oauth-proxy** 命令指定不正确的选项组合时导致 nil dereference。这会导致在用量消息末尾出现 segmentation 错误堆栈跟踪信息。现在，选项处理有所改进，当指定不正确的选项组合时则不会发生 nil dereferences。现在，当指定不正确的选项时，使用情况信息会被输出，无需跟踪堆栈。(BZ#1884565)

oc

- 在以前的版本中，日志库的改变导致 goroutine 堆栈 trace 的输出日志级别较低（2 级），这使得调试更为困难。goroutine 栈跟踪的日志级别被提高，现在它们只会在日志级别 6 及更高版本中打印。(BZ#1867518)

- 在以前的版本中，用户使用 OpenShift CLI（**oc**）登录到多个集群，每次登录到不同集群时都需要使用相同的用户名再次进行登陆。上下文名已被正确更新，因此当使用相同用户名进行登陆时，它会是唯一的。现在，在登录后，如果切换上下文后，不需要再次登录。(BZ#1868384)

- 在以前的版本中，当使用 **oc adm release mirror** 将发行版本镜像到磁盘时，清单文件名不包含架构扩展，如 **-x86_64**。这不允许在不出现标签名称冲突的情况下将多个架构镜像到同一个存储库。文件名现在包含正确的构架扩展，可防止标签名称冲突。(BZ#1878972)

- 在以前的版本中，镜像验证器对象没有被正确设置，这可能会导致 OpenShift CLI（**oc**）在验证镜像时出现 nil pointer 异常失败。镜像验证器对象现已正确设置，在验证镜像时，OpenShift CLI（**oc**）不再会失败且出现 nil pointer 异常。(BZ#1885170)

- 在以前的版本中，使用 **oc adm verify-image-signature** 验证镜像签名时使用错误的用户名，镜像签名验证会失败。现在，当验证镜像签名和镜像签名验证时，使用正确的用户名可以正常工作。(BZ#1890671)

- 在以前的版本中，在构建过程中不会生成提供版本信息的元数据，它不会出现在 OpenShift CLI（**oc**）的 Windows 二进制文件中。正确的 Windows 版本信息现在在 Windows 二进制文件上生成并可用。(BZ#1891555)

- 在以前的版本中，缺少路由条件的 nil 检查可能会导致 OpenShift CLI（**oc**）在描述路由时崩溃。添加了 nil 检查，描述路由现在可以正常工作。(BZ#1893645)

- 在以前的版本中，OpenShift CLI（**oc**）对客户端节流有较小的限制，客户端代码则对到达 API 发现的请求进行限制。客户端节流限制已增加，客户端节流现在出现较少的频率。（BZ#1899575）

- 在以前的版本中，在更改 **oc debug** 命令的过程中，对 init 容器的支持会丢失，且无法调试 init 容器。**oc debug** 命令中添加了对 init 容器的支持，现在可以调试 init 容器。(BZ#1909289)

OLM

- Marketplace Operator 被编写来报告当 **marketplace-operator** pod 安全退出时其提供的服务被降级，这会在集群常规升级过程中发生。这会导致 pod 在正常升级过程中报告降级，从而导致混乱。Marketplace Operator 不再会在它安全退出时报告它已被降级，且 Telemeter 客户端不再标记为 degraded。(BZ#1838352)

- 以前，在 Operator 升级过程中，Operator Lifecycle Manager（OLM）在升级完成前删除了现有集群服务版本（CSV）。这会导致新 CSV 处于 "Pending" 状态。在这个版本中更新了 OLM，以检查服务帐户的所有权，以确保为新 CSV 创建新服务帐户。因此，在新 CSV 正确达到 "Succeeded" 状态前，现有 CSV 不再被删除。(BZ#1857877)

- 在以前的版本中，Operator Lifecycle Manager（OLM）可以接受指定不存在的频道的 **Subscription** 对象。订阅可能会成功，且不会出现相关的错误信息，从而导致用户混淆。在这个版本中更新了 OLM，从而导致 **Subscription** 对象在这种情况下失败。集群管理员可以查看 **default** 命名空间中的事件以了解依赖项解析失败信息，例如：

```
$ oc get event -n default
```

输**出示例**

```
LAST SEEN   TYPE     REASON          OBJECT              MESSAGE
```

> 6m22s Warning ResolutionFailed namespace/my-namespace constraints not satisfiable: my-operator is mandatory, my-operator has a dependency without any candidates to satisfy it

(BZ#1873030)

- 在以前的版本中，Operator Lifecycle Manager（OLM）中对准入 webhook 配置的支持会重复使用部署 API 服务器时使用的 CA 证书生成代码。这个代码使用的挂载目录将证书信息放在以下位置：
  - **/apiserver.local.config/certificates/apiserver.crt**
  - **/apiserver.local.config/certificates/apiserver.key**

  但是，使用 Kubebuilder 或 Operator SDK 构建的准入 Webhook 预期将 CA 证书挂载到以下位置：
  - **/tmp/k8s-webhook-server/serving-certs/tls.cert**
  - **/tmp/k8s-webhook-server/serving-certs/tls.key**

  此不匹配会导致 Webhook 无法运行。在这个版本中更新了 OLM，现在在通过 Kubebuilder 或 Operator SDK 构建的 webhook 所需的默认位置挂载 Webhook CA 证书。因此，使用 Kubebuilder 或 Operator SDK 构建的 Webhook 现在可以由 OLM 部署。(BZ#1879248)

- 当部署具有 API 服务、转换 Webhook 或准入 webhook 的 Operator 时，Operator Lifecycle Manager（OLM）应从现有资源检索 CA 以计算 CA 哈希注解。此注解会影响 OLM 依赖于的部署哈希来确认是否已正确安装了部署。OLM 目前不会从转换 Webhook 检索 CA，从而导致无效的部署哈希，导致 OLM 尝试重新安装集群服务版本（CSV）。
  如果 CSV 定义了转换 Webhook 但不包括 API 服务或准入 Webhook，CSV 周期会无限期地在 "Pending"、"ReadyToInstall" 和 "Insbil" 阶段间进行。在这个版本中更新了 OLM，以使用现有转换 Webhook 来检索 CA 的值并正确计算部署散列。因此，OLM 现在可以安装 CSV 来定义转换 Webhook，无需 API 服务或准入 Webhook。(BZ#1885398)

- 在 **opm** 命令中，**semver-skippatch** 模式之前只允许带有后续补丁版本的捆绑作为有效替代，忽略所有预发布版本。带有相同补丁版本但后续预发布版本的捆绑包不被接受替代版本。此程序错误修复更新了 **opm** 命令，它基于 **semver-skippatch** 检查整个语义版本，而不是只是补丁版本。因此，后续预发布版本现在在 **semver-skippatch** 模式中有效。(BZ#1889721)

- 在以前的版本中，Marketplace Operator 在集群升级过程中无法清理过时的服务，Operator Lifecycle Manager（OLM）在不验证服务的情况下接受过时的服务。这会导致过时的服务将流量定向到包含过时内容的目录源 pod。在这个版本中更新了 OLM，为服务添加 spec hash 信息，并通过比较散列信息来确保服务具有正确的 spec。然后，如果服务过时，OLM 会删除并重新创建该服务。因此，服务规格现在会将流量定向到正确的目录源 pod。（BZ#1891995）

- 将 Operator 镜像到断开连接的 registry 后，因为缺少相关的捆绑包镜像，Operator 安装可能会失败。这是因为 bundle 镜像不存在于 **index.db** 数据库中。在这个版本中，更新了 **opm** 命令，以确保捆绑包镜像存在于数据库的 **related_images** 表中。(BZ#1895367)

- 在以前的版本中，Operator 作者可创建集群服务版本（CSV），使用在 **1** 到 **65535** 范围内设置的容器端口来定义 webhook。这导致无法因为验证失败而创建 **ValidatingWebhookConfiguration** 或 **MutatingWebhookConfiguration** 对象，从而无法创建成功安装的 CSV。CSV 的自定义资源定义（CRD）验证现在包含 **WebhookDescription ContainerPort** 字段的正确的最小和最大值。现在，如果没有定义容器端口，则默认为 **443**。无效容器端口的 CSV 现在会在创建 CSV 前失败验证。（BZ#1891898）

- 不由任何频道条目引用的滞留的 Operator 镜像捆绑包在 **opm index prune** 操作后仍会被保留。这会导致意外的索引镜像被镜像。现在，当修剪索引且在以后的 Operator 目录没有包括意外镜像时，滞留的镜像捆绑包也会被删除。(BZ#1904297)

- 在以前的版本中，Operator 更新可能会导致在创建新服务帐户前部署 Operator pod。pod 可以通过使用现有服务帐户部署，且无法在权限不足的情况下启动。添加了一个检查，以在集群服务版本（CSV）从 **Pending** 状态变为 **Installing** 状态前验证新的服务帐户是否存在。如果不存在新服务帐户，CSV 仍处于 **Pending** 状态，从而导致无法更新部署。(BZ#1905299)

- 在以前的版本中，当 Operator Lifecycle Manager（OLM）将 **ClusterServiceVersion**（CSV）对象复制到多个目标命名空间时，复制的 CSV 中的 **.status.lastUpdateTime** 字段被设置为当前时间。如果当前时间比原始 CSV 的最后更新时间要长，则会触发同步竞争条件，其中复制的 CSV 永远不会组合来与原始 CSV 匹配。当集群中有很多命名空间时，则可能发生这个情况。现在，复制的 CSV 中会保留原始 **.status.lastUpdateTime** 时间戳，且同步竞争条件不会由 **.status.lastUpdateTime** 值之间的不同而触发。(BZ#1905599)

- 在以前的版本中，**ClusterServiceVersion**（CSV）对象的 **StrategyDetailsDeployment** 对象中定义的 Pod 模板可能包含与 CSV 中定义的 pod 注解不匹配。Operator Lifecycle Manager（OLM）无法安装 Operator，因为 CSV 中的注解应该存在于作为 CSV 一部分的 pod 中。现在，**StrategyDetailsDeployment** 对象中定义的 pod 模板注解会被 CSV 中定义的 Pod 模板注解覆盖。OLM 不再无法部署与 pod 模板中定义的注解冲突的 CSV。(BZ#1907381)

- 当 **openshift-marketplace** 命名空间中的默认目录源通过 OperatorHub API 禁用时，您可以创建一个与默认名称相同的自定义目录源。在以前的版本中，当 marketplace 重启时，Marketplace Operator 会删除名称与默认目录源相同的自定义目录源。注解添加到 Marketplace Operator 创建的默认目录源中。现在，Operator 仅在重启 marketplace 时删除包含注解的目录源。创建的自定义目录源与默认目录源的名称相同，不会被删除。(BZ#1908431)

- 在以前的版本中，**oc adm catalog mirror** 命令在没有命名空间的情况下无法为 Operator 索引镜像生成正确的映射。另外，**--filter-by-os** 选项会过滤整个清单列表。这会导致目录中对过滤的镜像的引用无效。现在，没有命名空间的索引镜像被正确映射，**--index-filter-by-os** 选项添加到仅拉取和解包的索引镜像。**oc adm catalog mirror** 命令现在在没有命名空间的情况下为索引镜像生成有效的映射，**--index-filter-by-os** 选项会创建对过滤的镜像的有效引用。(BZ#1908565)

- 在以前的版本中，Operator 可以在集群服务版本（CSV）替换链中指定一个 **skipRange**，这会导致 Operator Lifecycle Manager（OLM）尝试更新 Operator。这个无限循环将增加 CPU 用量。现在，CSV 替换链已被更新，Operator 不会因为一个无效的 **skipRange** 停留在无限循环中。（BZ#1916021）

- 在以前的版本中，集群服务版本（CSV）协调循环中的 **csv.status.LastUpdateTime** 时间比较总是返回一个 **false** 的结果。这会导致 Operator Lifecycle Manager（OLM）Operator 不断更新 CSV 对象并触发另一个协调事件。现在，改进了时间比较，在没有状态更改时 CSV 将不再更新。（BZ#1917537）

- Catalog 更新 pod 轮询间隔大于默认的 15 分钟重新同步周期，则 Catalog Operator 将继续协调。这会一直进行直至达到下一次轮询时间，从而增加 CPU 负载。现在改进了协调重新排队逻辑，因此不会出现持续协调以及相关的 CPU 负载增加。(BZ#1920526)

- 在以前的版本中，如果在尝试创建 Operator 订阅的过程中未找到匹配的 Operator，则解析失败事件中列出的限制包括内部术语。订阅约束字符串没有从用户视角描述解析失败的原因。约束字符串现在更为明确。(BZ#1921954)

openshift-apiserver

- 在以前的版本中，针对 **deploymentconfigs/<name>/instantiate** 子资源的请求会失败，并带有一个 **no kind "DeploymentConfig" is registered for version apps.openshift.io/** 错误。现在设置了 **DeploymentConfig** 的正确版本，这些请求不再会失败。(BZ#1867380)

Operator SDK

- 在以前的版本中，所有的 **operator-sdk** 子命令都试图读取 **PROJECT** 文件，即使 **PROJECT** 是目录。因此，不需要 **PROJECT** 文件的子命令会失败。现在，不需要 **PROJECT** 文件的子命令不会试图读取该文件，即使存在无效的 **PROJECT** 文件也是如此。(BZ#1873007)

- 在以前的版本中，运行 **operator-sdk cleanup** 命令不会清理通过 **operator-sdk run bundle** 命令部署的 Operator。相反，会显示错误消息且 Operator 不会被清理。现在，**operator-sdk cleanup** 命令已被更新，可以使用 **cleanup** 命令清理部署了 **run bundle** 的 Operator。(BZ#1883422)

Performance Addon Operator

- 在以前的版本中，在 must-gather 逻辑中等待错误会导致日志收集时间过早终止。这个问题会根据时间造成日志收集操作提早中断。这会导致只收集了部分日志。现在，通过在 must-gather 逻辑中添加正确的等待来解决这个问题。(BZ#1906355)

- 在以前的版本中，must-gather 在所有节点上收集未绑定的 kubelet 日志。此问题导致过度的数据传输和收集，对用户没有明显的好处。
  这个问题已解决，方法是只收集 worker 节点上的 kubelet 日志中绑定的数量（最后 8 小时），而不收集 control plane 节点上的 kubelet 日志。（BZ#1918691）

- 在以前的版本中，当机器配置池降级时，性能配置集不会被更新来显示准确的机器配置池状态。现在，性能配置集节点选择器或机器配置池选择器可以正确地监控相关的机器配置池,降级的机器配置池反映了正确的状态。(BZ#1903820)

RHCOS

- 在以前的版本中，在 RHCOS 安装过程中配置额外的 Azure 磁盘会导致失败，因为 RHCOS initramfs 中缺少 Azure 磁盘的 **udev** 规则。添加了必要的 **udev** 规则以便在安装过程中配置附加磁盘现在可以正常工作。(BZ#1756173)

- 以前，**rhcos-growpart.service** 的用途并非是最佳实践。现在，**rhcos-growpart.service** 已被删除，用于在安装时通过 Ignition 配置磁盘。要在初始 RHCOS 安装后更改磁盘配置，您必须为您的系统置备所需的磁盘配置更改。(BZ#1851103)

- 在以前的版本中，当运行 **rpm-ostree cleanup -p** 时，Machine Config Operator 会尝试回滚 rpm-ostree，从而导致出现 "System transaction in progress" 错误。在这个版本中改进了与 D-Bus 处理相关的 rpm-ostree 代码，因此不再会发生错误。(BZ#1865839)

- 在以前的版本中，在 RHEL 8.2 中 KVM 中不支持 NVME 模拟的 ppc64le 或 s390x，这会导致 **kola --basic-qemu-scenarios** 使用 NVME 模拟失败。在 ppc64le 和 s390x 中禁用了对 NVME 模拟的测试，以便测试现在可以成功。(BZ#1866445)

- 在以前的版本中，当 DHCP 服务器需要很长时间响应 DHCP 查询时，Ignition 无法通过网络获取远程配置，因为 NetworkManager 会停止等待 DHCP 回答，且不会在 initramfs 中配置网络。现在，当作为内核参数设置来增加超时和重试次数时，NetworkManager 的新版本可以了解 **rd.net.timeout.dhcp=xyz** 和 **rd.net.dhcp.retry=xyz** 选项，您可以考虑使用这些参数来处理 DHCP 延迟的问题。(BZ#1877740)

- 在以前的版本中，因为内核命令行中的多个 **nameserver=** 条目可能会创建多个网络管理器（NetworkManager）连接配置集，所以可能会创建不正确的网络配置,。现在，RHCOS 中的 NetworkManager 的新版本可以正确处理多个 **nameserver=** 条目，以便在提供了多个 **nameserver=** 条目时可以正确生成网络配置。(BZ#1882781)

- 在以前的版本中，节点进程会因为一个递归调用（recursive call）造成堆栈溢出，导致节点进程出现问题。已修复这个逻辑错误，不再会出现这个问题。(BZ#1884739)

- 在以前的版本中，网络相关的服务单元没有被严格排序，这意味着使用 **-copy-network** 复制的网络配置在第一次重启系统时不会生效。相关的服务单元的顺序已被修复，它们现在总是在第一次重启时生效。（BZ#1895979）

- 在以前的版本中，当 **coreos-installer** 命令调用 fdasd 来检查 s390x 中的有效 DASD 标签时，udev 会重新探测 DASD 设备，因为 udev 仍可以访问该设备，从而导致 DASD 格式化失败,。现在，在检查 DASD 标签后，**coreos-installer** 会等待 udev 完成处理 DASD，以确保 DASD 格式化成功。（BZ#1900699）

- 在以前的版本中，在使用 DHCP 时，查询和修改网络管理器（NetworkManager）连接设置可能会混淆，因为默认创建的网络管理器连接是为所有接口匹配的。用户体验已被改进，在使用 DHCP 时，网络管理器（NetworkManager）现在默认为每个接口创建一个单独的连接。(BZ#1901517)

- 在以前的版本中，在切换到真实 root 前无法正确检测到 initrd 中的网络接口会导致静态 IP 分配到 VLAN 接口，因此无法在实际的 root 中成功激活。在这个版本中，修改网络接口在 initrd 中的处理方式，从而可以在真实的根用户中成功激活到 VLAN 接口的静态 IP 分配。(BZ#1902584)

- 在以前的版本中，如果您将 RHCOS 配置为使用 dhclient 进行 DHCP 操作，您会保留无法正确获取 DHCP 地址的系统，因为在生成了 initramfs 中的 NetworkManager 时，dhclient 二进制代码已从 RHCOS 中删除。dhsclient 二进制文件现在包括在 RHCOS 中，以便 RHCOS 系统能够使用 dhclient 成功执行 DHCP 操作。(BZ#1908462)

- 在以前的版本中，升级的节点不会接收唯一的发起方名称，因为重新生成 iSCSI 启动程序名称的服务单元只能在第一次引导时正常工作。在这个版本中，服务单元会在每次引导时运行，因此升级的节点如果不存在，则会接收生成的 initiator 名称。(BZ#1908830)

- 在以前的版本中，您无法使用 Ignition 创建 ext4 文件系统，因为当 **/etc/mke2fs.conf** 不存在时 **mkfs.ext4** 会失败。在这个版本中，**/etc/mke2fs.conf** 已被添加到 initramfs 中，以便 Ignition 能够成功创建 ext4 文件系统。（BZ#1916382）

路由

- 在以前的版本中，可以在路由上设置 **haproxy.router.openshift.io/timeout** 注解，其值超过 25 天。大于 25 天的值会导致入口控制器失败。现在，超时的上限被设置为 25 天。(BZ#1861383)

- 在以前的版本中，即使未置备 DNS 或所需的负载均衡器未就绪，入口控制器也会报告 Available 状态。现在，为 Ingress Operator 添加了验证，以确保在入口控制器被报告就绪前，置备了 DNS 和负载均衡器（如果需要）。(BZ#1870373)

- 在以前的版本中，可以将 ingress 控制器的默认证书设置为不存在的 secret（如因为输入了错误的信息）。此程序错误修复添加了验证，以确保 secret 在更改默认证书前存在。(BZ#1887441)

- 在以前的版本中，可以创建名称大于 63 个字符的路由。但是，在路由被创建后验证会失败。此程序错误修复添加了在路由创建时的验证。(BZ#1896977)

存储

- 在以前的版本中，准入插件会添加一个故障切换域和区域标签，即使它们没有正确配置，从而导致使用静态置备的持久性卷（PV）的 pod 无法在配置中带有空区域的 OpenStack 集群中启动。在这个版本中，表只有在包含有效区域和故障域时才添加到 PV 中，因此使用静态置备的 PV 的 pod 与配置了空区域或故障域的 OpenStack 集群上的 pod 的行为相同。(BZ#1877681)

- 在以前的版本中，Web 控制台中会显示 **LocalVolumeDiscoveryResult** 对象，表示可以手动定义它们。在这个版本中，**LocalVolumeDiscoveryResult** 类型被标记为内部对象，在 web 控制台中不再显示。要查看本地磁盘，请导航到 **Compute → Nodes → Select Nodes → Disks**。(BZ#1886973)

- 在以前的版本中，当创建需要凭证的快照时，如果 **VolumeSnapshotClass** CRD 已被删除，对快照的强制删除操作将无法正常工作。现在，不需要依赖于 **VolumeSnapshotClass** CRD 的存在，而是从 **VolumeSnapshotContent** CRD 获取凭证，以便可以删除使用凭证的卷快照和卷快照内容，如果包含这些凭证的 secret 仍然存在。(BZ#1893739)

- 在以前的版本中，Kubernetes FibreChannel（FC）卷插件不会在删除多路径设备前正确清除该多路径设备。在极个别的情况下，多路径 FC 设备上的文件系统在 pod 销毁过程中可能会被破坏。现在，Kubernetes 在删除 FC 多路径设备前清除数据，以防止文件系统崩溃。(BZ#1903346)

扩展

- 在 OpenShift Container Platform 中使用用于配置超线程的 **nosmt** 额外内核参数以前没有包括在相关文档中。要禁用超线程，创建一个适合您的硬件和拓扑的性能配置集，然后将 **nosmt** 设置为附加内核参数。
  如需更多信息，请参阅有关低延迟和实时应用程序的超线程。

1.7. 技术预览功能

这个版本中的一些功能当前还处于技术预览状态。它们并不适用于在生产环境中使用。请参阅红帽门户网站中关于对技术预览功能支持范围的信息：

技术预览功能支持范围

在下表中，功能被标记为以下状态：

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

表 1.2. 技术预览

功能	OCP 4.5	OCP 4.6	OCP 4.7
精度时间协议 (PTP)	TP	TP	TP
oc CLI Plug-ins	TP	TP	TP
Descheduler	TP	TP	GA
OVN-Kubernetes Pod network provider	TP	GA	GA
基于 Prometheus 的 HPA 定制 metrics adapter	TP	TP	TP
HPA 用于内存使用	TP	TP	GA
服务绑定	TP	TP	GA
日志转发	TP	GA	GA

功能	OCP 4.5	OCP 4.6	OCP 4.7
用户定义项目的监控	TP	GA	GA
使用 Cinder 的原始块	TP	TP	TP
AWS EFS 的外部置备程序	TP	TP	TP
CSI 卷快照	TP	TP	GA
CSI 卷克隆	TP	GA	GA
CSI 卷扩展	TP	TP	TP
vSphere 问题检测器（vSphere Problem Detector） Operator	-	-	GA
CSI GCP PD Driver Operator	-	-	TP
CSI OpenStack Cinder Driver Operator	-	-	TP
CSI AWS EBS Driver Operator	TP	TP	TP
Red Hat Virtualization（oVirt）CSI Driver Operator	-	GA	GA
CSI inline 临时卷	TP	TP	TP
使用 Local Storage Operator 进行自动设备发现和置备	-	TP	TP
OpenShift Pipelines	TP	TP	GA
OpenShift GitOps	-	TP	GA
Vertical Pod Autoscaler	TP	TP	TP
Operator API	TP	GA	GA
在节点中添加内核模块	TP	TP	TP
Egress router CNI 插件	-	-	TP
Scheduler 配置集	-	-	TP
非抢占优先级类	-	-	TP
Kubernetes NMState Operator	-	-	TP
支持的安装程序	-	-	TP

1.8. 已知问题

- 在 OpenShift Container Platform 4.1 中，匿名用户可以访问发现端点。之后的版本会取消对这端点的访问，以减少可能的安全漏洞攻击面。一些发现端点被转发到聚合的 API 服务器。但是，升级的集群中会保留未经身份验证的访问，因此现有用例不会中断。
  如果您是一个从 OpenShift Container Platform 4.1 升级到 4.7 的集群的集群管理员，您可以撤销或继续允许未经身份验证的访问。建议取消未经身份验证的访问，除非有特殊需要。如果您继续允许未经身份验证的访问，请注意相关的风险。

  警告

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

  使用以下脚本撤销对发现端点的未经身份验证的访问：

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

  此脚本从以下集群角色绑定中删除未经身份验证的对象：

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

  (BZ#1821771)

- 如果您使用附加的 Prometheus PVC 运行集群监控，在升级到 OpenShift Container Platform 4.7 时可能会出现 OOM 终止的情况。当 Prometheus 使用持久性存储时，Prometheus 内存在升级过程中会加倍，并在升级完成后的几小时内仍会是这个情况。为了避免 OOM 终止问题，允许升级前有双倍可用内存的 worker 节点。(BZ#1925061)

- 启动和停止 pod 迅速可能会导致 pod 处于 **Terminating** 状态。作为临时解决方案，您必须运行以下命令删除卡住的 pod：

  ```
  $ oc delete --force -n <project_name> <pod_name>
  ```

此问题将在 OpenShift Container Platform 以后的发行版本中解决。(BZ#1929463)

- 目前仅在计算节点上支持 RHCOS 实时（RT）内核，而不是 control plane 节点。OpenShift Container Platform 4.7 中的 RT 内核不支持紧凑集群。(BZ#1887007)

- 由于当前 OpenShift Container Platform 的限制，目前还无法在安装到 AWS C2S Secret 区域的集群中使用 AWS 安全令牌服务（STS）。以后的 OpenShift Container Platform 发行版本中会解决这个问题。（BZ#1927157）

- 红帽推荐的 CloudFormation 模板使用您自己的基础架构将集群安装到 AWS C2S Secret Region 无法正常工作，因为在安装过程中创建 bootstrap 节点时存在问题。（BZ#1924080）

- 将 Performance Addon Operator 从 4.6 升级到 4.7 会失败并显示以下错误：

> "Warning TooManyOperatorGroups 11m operator-lifecycle-manager csv created in namespace with multiple operatorgroups, can't pick one automatically"

在升级前，请按照在以前安装到特定命名空间时升级 Performance Addon Operator 中的步骤进行操作。

(BZ#1913826)

- 有时需要重启来在支持的 NIC 上实现 SR-IOV 更改。SR-IOV 目前会在重新引导时执行。如果此重启与 Machine Config 策略中的更改一致，则该节点可能会处于未确定的状态。Machine Config Operator 假设没有应用更新后的策略。

注意

这种竞争条件也可以通过将节点添加到具有 MCP 和 SR-IOV 更改的机器配置池中导致。

为了避免这个问题，应该按顺序完成需要 MCO 和 SR-IOV 更改的新节点。首先，应用所有 MCO 配置并等待节点发生。然后，应用 SR-IOV 配置。

如果一个新节点被添加到包含 SR-IOV 的机器配置池中，可以通过从 Machine Config Pool 中删除 SR-IOV 策略来避免此问题，然后添加新的 worker。然后，重新应用 SR-IOV 策略。

（BZ#1921321）

- **stalld** 服务会触发内核中的一个错误，并导致节点出现问题。为了临时解决这个问题，Performance Addon Operator 默认禁用 **stalld**。这个修复会影响与基于 DPDK 的工作负载关联的延迟，但在内核程序漏洞（BZ#1912118）被修复后，功能将会被恢复。

- 带有 **ruby-kafka-1.1.0** 和 **fluent-plugin-kafka-0.13.1** gems 的 Fluentd pod 与 Apache Kafka 版本 0.10.1.0 不兼容。如需更多信息，请参阅 Red Hat OpenShift Logging 5.0 发行注记中的"已知问题"。

- 精度时间协议（PTP）错误会在适配器卡 Mellanox MT27800 系列 [ConnectX-5] 中观察到。在 **ptp4l** 日志中会出现与时钟同步相关的错误。
这些错误会因为 NIC 硬件时钟被重置而导致系统时钟更新大于正常的情况。造成此问题的根原因未知，目前还没有临时解决方案。

（BZ#1913279）

- 在以前的版本中，OpenStack SDK 中的一个错误会在请求服务器组 **OSP16** 时失败。因此，UPI

playbook **control-plane.yaml** 在创建 control plane 服务器时会失败。作为临时解决方案，您可以请求一个热修复来更新 OpenStack SDK，它会更新堡垒主机上的 OpenStack SDK，以便将 UPI Ansible 任务更新至至少 **python-openstacksdk-0.36.4-1.20201113235938.el8ost**。使用这个热修复后，playbook 可以成功运行。(BZ#1891816)

- 当在使用最新的 Dell 固件（04.40.00.00）节点在裸机中尝试 IPI 安装时，不会部署节点，并在它们的状态中显示错误。这是因为 Dell Firmware（4.40.00.00）使用 eHTML5 作为虚拟控制台插件。
  要临时解决这个问题，请将虚拟控制台插件改为 HTML5 并再次运行部署。现在，节点应该可以被成功部署。如需更多信息，请参阅使用虚拟介质安装的固件要求。

  （BZ#1915828）

- 在使用 Kuryr 的 RHOSP 上安装集群会超时，并在 bootstrapping 过程中出现以下信息：

  ```
  INFO Waiting up to 20m0s for the Kubernetes API at https://api.ostest.shiftstack.com:6443...
  INFO API v1.20.0+ba45583 up
  INFO Waiting up to 30m0s for bootstrapping to complete...
  ERROR Attempted to gather ClusterOperator status after wait failure: listing ClusterOperator objects: Get
  "https://api.ostest.shiftstack.com:6443/apis/config.openshift.io/v1/clusteroperators": dial tcp 10.46.44.166:6443: connect: connection refused
  INFO Use the following commands to gather logs from the cluster
  INFO openshift-install gather bootstrap --help
  FATAL failed to wait for bootstrapping to complete: timed out waiting for the condition
  ```

  超时是因为 Kuryr 检测集群节点的 RHOSP Networking 服务（neutron）子网变化的方式造成的。

  作为临时解决方案，请不要删除 control plane 机器清单，如安装文档中的"创建 Kubernetes 清单和 Ignition 配置文件" 部分所述。当您被指示要运行以下命令时：

  ```
  $ rm -f openshift/99_openshift-cluster-api_master-machines-*.yaml openshift/99_openshift-cluster-api_worker-machineset-*.yaml
  ```

  运行这个命令替代：

  ```
  $ rm -f openshift/99_openshift-cluster-api_worker-machineset-*.yaml
  ```

  （BZ#1927244）

- 在 OpenShift Container Platform 4.3 和 4.4 中，如果用户在多个标签页中打开了控制台，**Developer** 视角中的一些侧边栏链接没有直接链接到项目，在所选项目中会出现意外切换的情况。这将在以后的发行版本中解决。(BZ#1839101)

- 在 OpenShift Container Platform 4.5 中，具有扩展权限的用户如果无法编辑对部署或部署配置的权利，则无法使用控制台扩展部署或部署配置。这将在以后的发行版本中解决。(BZ#1886888)

- 在 OpenShift Container Platform 4.5 中，当 **Developer** 视角中存在最小或无数据时，大多数监控图表或图形（CPU 消耗、内存用量和带宽）都会显示 -1 到 1 范围但是这些值都不能低于零。这将在以后的发行版本中解决。(BZ#1904106)

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

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

- Operator SDK CLI 工具支持在 macOS 上运，但 OpenShift 镜像站点中没有 macOS 二进制文件。macOS 二进制文件将在以后的更新中添加。（BZ#1930357）

- 目前，在启用 IPsec 的集群中，Red Hat Enterprise Linux（RHEL）7.9 节点无法与 Red Hat Enterprise Linux CoreOS（RHCOS）节点通信。（BZ#1925925）

- 如果您的集群通过管理员置备的外部负载均衡器公开默认 Ingress Controller，将所有 HTTP 流量重定向到 HTTPS，则必须修补新的明文 Ingress Canary 路由，以便在 4.6 升级到 4.7 升级过程中使用边缘终止（edge termination）。

  ```
  $ oc patch route/canary -n openshift-ingress-canary -p '{"spec":{"tls":
  {"termination":"edge","insecureEdgeTerminationPolicy":"Redirect"}}}'
  ```

  (BZ#1932401)

- 对 openvswitch ("net: openvswitch: reorder masks array based on usage") 代码的更新会导致 openvswitch et/openvswitch/flow_table::flow_lookup 访问 preemptible（和 migratable）项中的 per-cpu 数据条件，从而会导致一个实时内核l panic。因此，kernel-rt 不稳定，并会影响低延迟应用程序。
  在这个问题被解决前，建议不要升级到 OpenShift Container Platform 4.7。

  (BZ#1918456)

- SR-IOV 设备插件不允许作为资源公开节点上的 VFIO 设备。这会导致在 Intel 设备中阻止 DPDK 工作负载。
  在修复这个问题之前，建议 SR-IOV 用户不要升级到 OpenShift Container Platform 4.7。

  (BZ#1930469)

- 在 OpenShift Container Platform 4.7 中，添加到 Operator 基础架构代码中的 **ConfigInformers** 对象无法成功启动。因此，**ConfigObserver** 对象无法同步缓存。当发生这种情况时，oVirt CSI Driver Operator 会在几分钟后关闭，这会导致持续重启。作为临时解决方案，您可以执行以下步骤：

  1. 使用 oVirt CSI Operator 将项目切换到集群：

     ```
     $ oc project openshift-cluster-csi-drivers
     ```

  2. 检查 **warning: restart** 信息：

     ```
     $ oc status
     ```

  3. 如果没有警告，请输入以下命令：

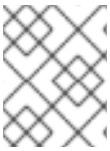
     ```
     $ oc get pods
     ```

因此，oVirt CSI Driver Operator 不会再不断重启。(BZ#1929777)

1.9. 异步勘误更新

OpenShift Container Platform 4.7 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 4.7 勘误都 可以通过红帽客户门户网站获得。OpenShift Container Platform 生命周期 包括了详细的与异步勘误相关的内容。

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



注意

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

本节的内容将会持续更新，以提供以后发行的与 OpenShift Container Platform 4.7 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.7.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. RHEA-2020:5633 - OpenShift Container Platform 4.7.0 镜像发行版本、程序错误修正和安全更新公告

发布日期：2021 年 2 月 24 日

OpenShift Container Platform release 4.7.0 包含安全更新，现已正式发布。其程序错误修正列表包括在 RHSA-2020:5633 公告中。此更新中包括的 RPM 软件包由 RHSA-2020:5634 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。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.7.0 容器镜像列表

1.9.2. RHBA-2021:0678 - OpenShift Container Platform 4.7.1 程序漏洞修复更新

发布日期：2021 年 3 月 8 日

OpenShift Container Platform release 4.7.1 现已正式发布。其程序错误修正列表包括在 RHBA-2021:0678 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0677 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。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.7.1 容器镜像列表

1.9.2.1. 升级

要将现有 OpenShift Container Platform 4.7 集群升级到此最新版本，请参阅使用 CLI 更新集群以获取相关说明。

1.9.3. RHBA-2021:0749 - OpenShift Container Platform 4.7.2 程序漏洞修复更新

发布日期：2021 年 3 月 15 日

OpenShift Container Platform release 4.7.2 现已正式发布。其程序漏洞修正列表包括在 RHBA-2021:0749 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0746 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。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.7.2 容器镜像列表

1.9.3.1. 升级

要将现有 OpenShift Container Platform 4.7 集群升级到此最新版本，请参阅使用 CLI 更新集群以获取相关说明。

1.9.4. RHBA-2021:0821 - OpenShift Container Platform 4.7.3 程序漏洞修复更新

发布日期：2021 年 3 月 22 日

OpenShift Container Platform release 4.7.3 现已正式发布。其程序漏洞修正列表包括在 RHBA-2021:0821 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0822 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。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.7.3 容器镜像列表

1.9.4.1. 升级

要将现有 OpenShift Container Platform 4.7 集群升级到此最新版本，请参阅使用 CLI 更新集群以获取相关说明。

1.9.5. RHSA-2021:0957 - OpenShift Container Platform 4.7.4 程序错误修复和安全更新

发布日期：2021 年 3 月 29 日

OpenShift Container Platform release 4.7.4,包括安全更新，现已正式发布。其程序错误修正列表包括在 RHSA-2021:0957 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:0958 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。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.7.4 容器镜像列表

1.9.5.1. 升级

要将现有 OpenShift Container Platform 4.7 集群升级到此最新版本，请参阅使用 CLI 更新集群以获取相关说明。

1.9.6. RHSA-2021:1005 - OpenShift Container Platform 4.7.5 程序错误修复和安全更新

发布日期：2021 年 4 月 5 日

OpenShift Container Platform release 4.7.5 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-2021:1005 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:1006 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。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.7.5 容器镜像列表

1.9.6.1. 功能

1.9.6.1.1. 在 AWS 上的 VMC 上安装集群

现在，您可以通过将其部署到 AWS 上的 VMware Cloud（VMC）在 VMware vSphere 基础架构上安装 OpenShift Container Platform 集群。如需更多信息，请参阅将集群部署到 VMC 的文档。

1.9.6.1.2. 在 Insights Operator 归档中添加内存和运行时间元数据

在这个版本中，Insights Operator 归档增加了 **uptime** 和 **memory alloc** 的元数据，以便可以正确调查小内存泄漏。如需更多信息，请参阅 BZ#1935605。

1.9.6.1.3. SAP 许可证管理增强

在这个版本中，您可以使用以下命令检测许可证管理 pod 中的故障：

```
# oc logs deploy/license-management-l4rvh
```

输出示例

```
Found 2 pods, using pod/license-management-l4rvh-74595f8c9b-flgz9
+ iptables -D PREROUTING -t nat -j VSYSTEM-AGENT-PREROUTING
+ true
+ iptables -F VSYSTEM-AGENT-PREROUTING -t nat
+ true
+ iptables -X VSYSTEM-AGENT-PREROUTING -t nat
+ true
+ iptables -N VSYSTEM-AGENT-PREROUTING -t nat
iptables v1.6.2: can't initialize iptables table `nat': Permission denied
```

如果结果返回 **Permission denied**，iptables 或您的 kernal 可能需要升级。如需更多信息，请参阅 BZ#1939061。

1.9.6.2. 升级

要将现有 OpenShift Container Platform 4.7 集群升级到此最新版本，请参阅使用 CLI 更新集群以获取相关说明。

1.9.7. RHBA-2021:1075 - OpenShift Container Platform 4.7.6 程序错误修复更新

发布日期：2021 年 4 月 12 日

OpenShift Container Platform release 4.7.6 现已正式发布。其程序错误修正列表包括在 RHBA-2021:1075 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。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.7.6 容器镜像列表

1.9.7.1. 程序错误修复

- 在以前的版本中，当载入 **Topology** 页面时会出现一个错误。在这个版本中，这个问题已解决，**Topology** 页面可以成功加载。(BZ#1940437)
- 当从 4.6 升级到 4.7 时，由 vsphere-hostname 服务设置的主机名仅在节点安装时应用。如果在升级前没有静态设置主机名，则主机名可能已经丢失。在这个版本中删除了允许 vsphere-hostname 服务仅在安装节点时运行的条件。因此，升级时 vsphere-hostnames 不再丢失。（BZ#1943143）
- 在以前的版本中，BZ#1936587 将全局 CoreDNS 缓存最大 TTL 设置为 900 秒。因此，从上游解析器接收的 NXDOMAIN 记录被缓存了 900 秒。在这个版本中，负 DNS 响应记录被显式缓存最多 30 秒。因此，解析 NXDOMAINs 记录不再会缓存 900 秒。（BZ#1943826）
- 在以前的版本中，**growpart** 脚本不考虑使用原位 LUKS rootfs 文件重新置备 需要增大。因此，启用原位 LUK 加密的机器创建的 rootfs 文件太小。在这个版本中，**growpart** 脚本（现在 **ignition-ostree-growfs**）认为原位 LUKS rootfs 文件重新置备 需要增大。因此，启用原位 LUK 加密的机器会创建 rootfs 文件，该文件包含了所有可用的磁盘空间。(BZ#1941760)
- 在以前的版本中，如果启用了 rootfs 重新置备（如 LUKS），则 **prjquota** 内核参数会被丢弃。因此，OpenShift Container Platform 中磁盘空间配额管理功能可能会中断。在这个版本中，**prjquota** 内核参数被保留，即使重新置备了 rootfs。因此，依赖于该 rootfs 挂载选项的 OpenShift Container Platform 功能现在可以正常工作。(BZ#1940966)

1.9.7.2. 功能

1.9.7.2.1. BareMetal Operator 的增强

此更新为 BareMetal Operator 添加了新功能，允许使用不同的重启模式。这为客户端提供了一种路径，供客户端快速关闭系统进行补救，并在节点失败时尽快恢复工作负载。如需更多信息，请参阅 BZ#1936407。

1.9.7.2.2. Cluster API provider BareMetal（CAPBM）的增强

此更新为集群 API 供应商 BareMetal（CAPBM）添加了新功能，以便在补救时请求硬电源。此增强利用了对 BareMetal Operator 的最新更改，以支持硬和软重启模式。因此，CAPBM 请求在需要补救时硬重启，绕过 BareMetal Operator 问题的默认软开机。如需更多信息，请参阅 BZ#1936844。

1.9.7.3. 升级

要将现有 OpenShift Container Platform 4.7 集群升级到此最新版本，请参阅使用 CLI 更新集群以获取相关说明。

1.9.8. RHSA-2021:1150 - OpenShift Container Platform 4.7.7 程序错误修复和安全更新

发布日期：2021 年 4 月 20 日

OpenShift Container Platform release 4.7.7 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 RHBA-2021:1149 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:1150 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。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.7.7 容器镜像列表

1.9.8.1. 程序错误修复

- 在以前的版本中，因为未知的原因，kubelet 可能会为节点注册错误的 IP 地址。因此，节点会处于 **NotReady** 状态，直到重新引导为止。现在，systemd Manager 配置被重新载入，并带有有效的 IP 地址作为环境变量，这意味着节点不再进入 **NotReady** 状态，因为 kubelet 注册了错误的 IP 地址。（BZ#1944394）

- 在以前的版本中，在 CVE-2021-3344 修复后，构建不会在该节点上自动挂载授权密钥。在这个版本中，减少了从 pod 的 **/run/secrets** 目录复制到构建容器的数据数量，从而导致了 **/run/secrets/etc-pki-entitlements** 文件被忽略。因此，当权利证书存储在 OpenShift 主机上时，这个问题会阻止构建无缝工作。
  现在，OpenShift 构建镜像和相关 Pod 会将 **/run/secrets** 中的所有与权利相关的文件挂载到构建容器中。授权构建无法获取存储在 OpenShift 主机/节点上的证书。请注意，当在 Red Hat Enterprise Linux CoreOS（RHCOS）节点上运行 OpenShift Container Platform 构建时，可以忽略警告信息，如 **level=warning msg="Path \"/run/secrets/etc-pki-entitlement\" from \"/etc/containers/mounts.conf\" doesn't exist, skipping**。

  （BZ#1945692）

1.9.8.2. 升级

要将现有 OpenShift Container Platform 4.7 集群升级到此最新版本，请参阅使用 CLI 更新集群以获取相关说明。

第 2 章 OPENSHIFT CONTAINER PLATFORM 版本政策

OpenShift Container Platform 对所有支持的 API 提供了严格的后向兼容保证，但这不包括 alpha API（这些 API 可能会在不通知的情况下被改变），以及 beta API（这些 API 偶尔可能会被改变且不保证后向兼容）。

红帽没有公开发布 OpenShift Container Platform 4.0，而是在版本 3.11 后直接发布了 OpenShift Container Platform 4.1。

master 主机和节点（node）主机使用的 OpenShift Container Platform 版本必须相互匹配（在集群升级过程中出现的临时不匹配除外）。例如，在一个 4.7 集群中，所有的 master 必需是 4.7，所有节点也必需是 4.7。如果安装了旧版本的 **oc**，则无法使用 OpenShift Container Platform 4.7 中的所有命令。您需要下载并安装新版本的 **oc**。

因为非安全的原因改变 API 将会最少涉及到 2 个次发行版本（例如，4.1 到 4.2 到 4.3）来更新旧的 **oc**。一些新功能可能需要新版本的 **oc**。一个 4.3 版本的服务器可能会带有版本 4.2 的 **oc** 不能使用的功能，而一个版本为 4.3 的 **oc** 也可能会带有不被版本 4.2 服务器支持的功能。

表 2.1. 兼容性列表

	X.Y (**oc** Client)	**X.Y+N** footnote:versionpolicyn[其中 **N** 是一个大于 1 的值。] (**oc** Client)
X.Y (Server)	1	3
X.Y+N footnote:versionpolicyn[] (Server)	2	1

1 完全兼容。

2 **oc** 客户端可能无法访问服务器的功能。

3 **oc** 客户端可能会包括与要访问的服务器不兼容的选项和功能。