OpenShift Container Platform 4.6

发行注记

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

Last Updated: 2023-02-27

OpenShift Container Platform 4.6 发行注记

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

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

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 4.6 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 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

Red Hat OpenShift Container Platform（RHBA-2020:4196）现已正式发布。此发行版本使用 Kubernetes 1.19 和 CRI-O 运行时。OpenShift Container Platform 4.6 的新功能、改变以及已知的问题包括在此文档中。

红帽没有公开发布 OpenShift Container Platform 4.6.0，而是发布了 OpenShift Container Platform 4.6.1 作为正式发行版本（GA）。

OpenShift Container Platform 4.6 集群位于 https://console.redhat.com/openshift。您可以通过 OpenShift Container Platform 的 Red Hat OpenShift Cluster Manager 应用程序在内部环境或云环境中部署 OpenShift 集群。

OpenShift Container Platform 4.6 需要运行在 Red Hat Enterprise Linux 7.9 及更新的版本，或 Red Hat Enterprise Linux CoreOS 4.6 上。

您必须使用 Red Hat Enterprise Linux CoreOS (RHCOS) 作为 control plane (也称为 master) 的系统，而 compute (也称为 worker) 机器可以使用 RHCOS，或 Red Hat Enterprise Linux 7.9 及更新的版本。

重要

因为当前只支持使用 Red Hat Enterprise Linux 7.9 或更新的次版本作为 compute 系统，所以不能把使用 Red Hat Enterprise Linux 的 compute 系统升级到版本 8。

OpenShift Container Platform 4.6 是一个延长的更新支持（EUS）发行版本。如需了解更多与 Red Hat OpenShift EUS 相关的信息，请参阅 OpenShift 生命周期和 OpenShift EUS 概述。

随着 OpenShift Container Platform 4.6 的发布，版本 4.3 现在已结束生命周期。如需更新相关信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

1.2. 新功能及功能增强

此版本对以下方面进行了改进

1.2.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.2.1.1. RHCOS PXE 和 ISO 现在为 live 环境

RHCOS 的 PXE 介质和 ISO 现在是一个完全 live 的环境。与之前用于在用户置备的基础架构上用于 OpenShift Container Platform 集群的 RHCOS 安装的专用 PXE 介质和 ISO 不同，RHCOS live 环境可以使用 Ignition 配置，并包含与主要 RHCOS 镜像相同的软件包，如 **coreos-installer**、**nmcli** 和

podman。这允许对安装前或安装后的工作流进行脚本化。例如，您可以运行 **coreos-installer**，然后发出 HTTP 请求来向置备服务器发出成功的信号。PXE 引导使用普通的 **ignition.config.url**。使用以下命令，可以将 ISO 配置为带有 Ignition：

```
$ coreos-installer iso ignition embed
```

1.2.1.2. coreos-installer 已被重写

现在，**coreos-installer** 被重写以支持更多功能，其中包括：

- 修改安装系统的内核参数。
- 获取 Ignition 配置。
- 保留之前存在的分区。
- 使用 **coreos-installer iso ignition** 命令为新的 live ISO 配置 Ignition。

1.2.1.3. RHCOS 现在使用 RHEL 8.2

RHCOS 现在在 OpenShift Container Platform 4.6 中使用 Red Hat Enterprise Linux(RHEL) 8.2 软件包。这些软件包为您提供了修复、功能和增强，以及硬件支持和驱动程序更新。

1.2.1.4. Ignition 规格更新至 v3

RHCOS 现在使用 Ignition spec v3 作为 Ignition 唯一支持的 spec 版本。这会为以后更复杂的磁盘配置提供支持。

对于使用安装程序置备的基础架构的用户，这些变化应是大体透明的。对于用户置备的基础架构安装，您必须修改任何自定义 Ignition 配置以使用 Ignition spec 3。**openshift-install** 程序现在生成 Ignition spec 3。

如果您要为使用 Ignition 的第 1 天操作或第 2 天操作创建 Machine Configs，则应该使用 Ignition spec v3。但是，MCO（MCO）仍然支持 Ignition spec v2。

1.2.1.5. 将节点添加到现有集群的额外步骤

对于已升级到 OpenShift Container Platform 4.6 的集群，您可以在 OpenShift Container Platform 集群中添加更多节点。只有在 OpenShift Container Platform 4.6 之前最初安装了集群且之后升级到 4.6 时，这些说明才有效。

如果在裸机或 vSphere 上安装了用户置备的集群，您必须确保引导介质或 OVA 镜像与集群升级到的版本匹配。另外，您的 Ignition 配置文件必须修改为与 spec v3 兼容。如需了解更多详细信息和 Ignition 配置文件示例，请参阅 升级到 OpenShift 4.6+ 知识库解决方案后向 UPI 集群添加新节点会失败 。

1.2.1.6. 现在，支持 RHCOS 和 MCO 的扩展

对于默认的 RHCOS 安装，RHCOS 和 MCO 现在支持以下扩展。

- **kernel-devel**
- **usbguard**

1.2.1.7. 现在支持 4Kn 磁盘

RHCOS 现在支持安装到使用 4K 扇区的磁盘。

1.2.1.8. 现在支持 /var 分区

RHCOS 现在支持 **/var** 作为一个独立分区，也支持 **/var** 的任何其他子目录。

1.2.1.9. 使用 OVA 的 vSphere 的静态 IP 配置

现在您可以在 vSphere 中覆盖默认的 DHCP 网络设置。这需要设置静态 IP 配置，然后在从 vSphere 的 OVA 引导虚拟机前设置 **guestinfo** 属性。

1. 设置静态 IP:

```
$ export IPCFG="ip=<ip>::<gateway>:<netmask>:<hostname>:<iface>:none
nameserver=srv1 [nameserver=srv2 [nameserver=srv3 [...]]]"
```

示例命令

```
$ export IPCFG="ip=192.168.100.101::192.168.100.254:255.255.255.0:::none
nameserver=8.8.8.8"
```

2. 在从 vSphere 中的 OVA 引导虚拟机前，设置 **guestinfo.afterburn.initrd.network-kargs** 属性：

```
$ govc vm.change -vm "<vm_name>" -e "guestinfo.afterburn.initrd.network-kargs=${IPCFG}"
```

这降低了在没有 DHCP 的环境中自动部署 Red Hat Enterprise Linux CoreOS（RHCOS）部署的难度。此功能增强允许进行高级别的自动化，以便在使用静态网络的环境中置备 RHCOS OVA。

如需更多信息，请参阅 BZ1785122。

1.2.2. 安装和升级

1.2.2.1. 将集群安装到 AWS GovCloud 区域（region）

现在，您可以在 Amazon Web Services（AWS）上将集群安装到 GovCloud 区域。AWS GovCloud 是为需要运行敏感负载的美国政府机构、企业、企业和其他美国客户设计的。

由于 GovCloud 区域没有红帽发布的 RHCOS AMI，您必须上传属于该区域的自定义 AMI。

如需更多信息，请参阅 在 AWS 上安装集群到一个政府区域。

1.2.2.2. 定义自定义 AWS API 端点

现在，您可以在 **install-config.yaml** 文件中定义 **serviceEndpoints** 字段。该文件可让您指定自定义端点列表来覆盖 AWS 上的默认服务端点。

1.2.2.3. 将集群安装到 Microsoft Azure Government 区域

现在，您可以在 Azure 上将集群安装到 Microsoft Azure Government（MAG）区域。Microsoft Azure Open（MAG）是为需要运行敏感工作负载的美国政府机构及其合作伙伴设计的。

如需更多信息，请参阅 在 Azure 上安装集群到一个政府区域。

1.2.2.4. 在 Azure 上运行的集群的用户定义的出站路由

现在，您可以为在 Azure 上运行的集群选择自己的出站路由，以连接到互联网。这可让您跳过创建公共 IP 地址和公共负载均衡器。

如需更多信息，请参阅 用户定义的出站路由。

1.2.2.5. 将集群安装到 vSphere 版本 7.0

现在，您可以将集群部署到 VMware vSphere 版本 7.0 中。如需更多信息，请参阅 VMware vSphere 基础架构要求。

1.2.2.6. 使用安装程序置备的基础架构在裸机上安装集群

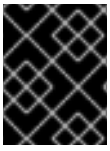
OpenShift Container Platform 4.6 支持使用安装程序置备的基础架构在裸机上安装集群。

如需更多信息，请参阅在裸机上安装集群

1.2.2.7. 处理 AWS、Azure 和 GCP 上的云 API 访问的凭证请求

现在，**install-config.yaml** 文件中有一个新的 **credentialsMode** 字段，它定义了如何为 OpenShift Container Platform 组件处理 **CredentialsRequest** 自定义资源，以便在 AWS、Azure 和 GCP 上访问云 API。现在，有 3 个可以配置的模式：

- Mint
- Passthrough
- Manual



重要

由于 BZ#1884691 中的已知问题， Azure 和 GCP 不支持使用 **install-config.yaml** 文件的 Manual 模式配置。

如果将 **credentialsMode** 字段设置为三种模式中的任何一种，安装程序不会在安装 OpenShift Container Platform 前检查凭证是否具有适当的权限。当因为云策略模拟器中的限制而无法正确验证所提供的用户凭证时，会很有用。

如需有关这些模式的更多信息，请参阅 Cloud Credential Operator。

1.2.2.8. 指定 control plane 和计算节点的磁盘类型和大小

现在，您可以为在 Azure 和 GCP 上运行的集群在 control plane 和计算节点上配置磁盘类型和大小。这可以在 **install-config.yaml** 文件中使用以下字段指定：

- **osDisk.diskSizeGB**
- **osDisk.diskType**

例如：

```
...
compute:
...
```

```
  platform:
  - osDisk:
      diskSizeGB: 120
      diskType: pd-standard
  replicas: 3
controlPlane:
...
  platform:
  - osDisk:
      diskSizeGB: 120
      diskType: pd-ssd
...
```

1.2.2.9. 对于 Azure 安装，增加了 control plane 节点的最小磁盘大小

Azure 安装 control plane 节点所需的最小磁盘大小已从 512 GB 增加到 1024 GB。

1.2.2.10. 集群升级前所需的 Operator 的最新版本

从 OpenShift Container Platform 4.6 开始，Operator Lifecycle Manager（OLM）和 OperatorHub 使用的红帽提供的默认目录现在作为特定于 OpenShift Container Platform 次要版本的索引镜像提供。集群管理员必须确保，在升级到 OpenShift Container Platform 4.6 之前，所有以前通过 OLM 安装的 Operator 都在其最新的频道中更新为其最新版本。

如需了解更多详细信息和重要的 Operator 升级先决条件，请参阅每个集群版本提供的默认 Operator 目录。

1.2.2.11. 没有置备网络的部署

OpenShift Container Platform 现在支持没有置备网络的部署和 RedFish Virtual Media。

如需更多信息，请参阅为 OpenShift 安装设置环境。

1.2.2.12. 部署现在支持 root 设备 hints

部署现在支持 root 设备 hints。

1.2.2.13. 安装程序的改进

现在，部署会在节点上执行内省，以确保节点满足安装要求，如果没有满足安装要求，则不会生成错误。

1.2.2.14. 安装时选择 RHOSP 可用区

现在，在 RHOSP 上安装集群时，您可以选择 Red Hat OpenStack Platform（RHOSP）Compute（Nova）可用域。

如需更多信息，请参阅 RHOSP 安装文档中的 OpenShift Container Platform。

1.2.2.15. 在 RHOSP 上安装时不再需要浮动 IP 地址

您不再需要浮动 IP 地址才能在 RHOSP 上完成 OpenShift Container Platform 安装。

如需更多信息，请参阅 RHOSP 安装文档中的 OpenShift Container Platform。

1.2.2.16. 为 RHCOS 安装选择磁盘

在以前的版本中，当您使用安装程序为部署裸机集群创建的基础架构时，无法指定要在哪个磁盘上部署 RHCOS。现在，您可以选择要安装 RHCOS 的磁盘， **rootDeviceHints** 提供了有关选择目标磁盘的指导。(BZ#1805237)

1.2.2.17. AWS 集群现在默认使用 M5 实例

现在，在 AWS 上的 IPI 和 UPI 安装会首选使用 M5 实例。因此，现在在 AWS 上部署的新集群会默认使用 M5 实例。如果 M5 实例不可用，安装程序将使用 M4 实例。(BZ#1710981)

1.2.2.18. IBM Z 和 LinuxONE

在这个版本中，IBM Z 和 LinuxONE 与 OpenShift Container Platform 4.6 兼容。如需了解安装步骤，请参阅在 IBM Z 和 LinuxONE 上安装集群 。

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：
  - 日志转发
  - 精度时间协议 (PTP) 硬件
  - CSI 卷快照
  - OpenShift Pipelines
- 以下 OpenShift Container Platform 功能不被支持：
  - OpenShift Container Platform Virtualization
  - Red Hat OpenShift Service Mesh
  - CodeReady Containers (CRC)
  - OpenShift Container Platform 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 Container Platform 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
  - CSI 卷克隆

  - NVMe
  - 使用 Fibre Channel 持久性存储

- worker 节点必须运行 Red Hat Enterprise Linux CoreOS（RHCOS）。
- 必须使用 NFS 来置备持久性共享存储。
- 必须使用本地存储（比如 iSCSI、FC 或者带有 DASD/FCP 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 4.6:
  - IBM System Z /LinuxONE 为附加的 ECKD 存储的虚拟机启用了 HyperPAV

支持的功能
在这个版本中，IBM Z 和 LinuxONE 支持以下功能：

- 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）
- OpenShift Do (odo)

1.2.2.19. IBM Power 系统

在这个版本中，IBM Power Systems 与 OpenShift Container Platform 4.6 兼容。请参阅在 IBM Power Systems 上安装集群或在受限网络中的 IBM Power Systems 上安装集群。

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

- 用于 IBM Power 系统的 OpenShift Container Platform 不包括以下技术预览功能：
  - OpenShift virtualization
  - OpenShift Serverless（Knative、FaaS 集成）
- 以下 OpenShift Container Platform 功能不被支持：
  - Red Hat OpenShift Service Mesh（istio、jaeger、kiali）
  - CodeReady Workspaces
  - CodeReady Containers (CRC)
  - 基于 Tekton 的 OpenShift Pipelines
  - OpenShift Container Platform Metering
  - Multus 插件（SR-IOV、IPVAN、带有 VLAN 的桥接、静态 IPAM）
  - SR-IOV CNI 插件
  - 红帽单点登录
  - OpenShift Metering（Presto, Hive）
- 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)、OpenStack Cinder 或容器存储接口 (CSI) 的 **Filesystem** 模式。
- 网络必须使用 DHCP 或 Red Hat Openshift SDN 的静态地址。
- 使用 Eclipse OpenJ9 的 AdoptOpenJDK
- 安装程序置备的基础架构
- NVIDIA GPU 设备管理器
- 特殊资源 Operator
- OpenShift Ansible Service Broker Operator（已弃用）
- dotNET on RHEL

支持的功能

- 目前，支持四个 Operator:
  - Cluster-Logging-Operator
  - Cluster-NFD-Operator
  - Elastic Search-Operator
  - Local Storage Operator
- 在裸机环境中的用户置备的基础架构部署场景
- OpenShift 集群监控
- Node Tuning Operator
- OpenShift Jenkins
- OpenShift Logging
- OpenShift Do (odo)
- Machine Configuration Operator 用于使用安装程序置备的基础架构的安装
- Node Feature Discovery Operator
- OpenShift Container Platform 内核（CVO Operator）
- 使用用户置备的基础架构的集群的安装程序
- OVS
- 基于 RHEL8 的容器支持
- RHEL CoreOS
- Ansible Engine
- Red Hat Software Collections

- HostPath
- iSCSI
- 4K 磁盘支持

1.2.2.20. Red Hat Virtualization（RHV）全堆栈安装程序的改进

- 您可以使用 Container Storage Interface（CSI）Driver Operators 从 RHV 存储域动态置备存储到 OpenShift Container Platform 集群。
- 您可以使用 RHV 虚拟机 worker 节点的自动扩展额外功能来更好地控制工作负载和资源。
- 您可以使用本地镜像执行断开连接或受限安装。这个能力对金融、公共机构和安全环境很有帮助。
- 您可以使用 用户置备的基础架构（如外部负载均衡器）在 RHV 上安装 OpenShift Container Platform。此过程使用一系列 Ansible playbook 来启用更灵活的安装。
- 使用安装程序置备的基础架构在 RHV 上安装 OpenShift Container Platform 不需要内部 DNS 的静态 IP 地址。
- OpenShift Container Platform 版本 4.6 需要 RHV 版本 4.4.2 或更高版本。

重要

如果您在 RHV 版本 4.3 上运行 OpenShift Container Platform 版本 4.5，请在将 OpenShift Container Platform 更新至版本 4.6 前将 RHV 升级到 4.4.2 或更高版本。

1.2.2.21. 使用安装程序置备的基础架构为裸机部署改进修复失败的节点

现在，可以对失败的 control plane 节点进行基于重新引导的补救。在使用基于重启的补救方法时，这些节点的标识和注解会被保留。

1.2.3. 安全性与合规性

1.2.3.1. Compliance Operator

Compliance Operator 现已发布。此功能允许使用 OpenSCAP 工具检查部署是否满足安全标准，并提供补救选项。如需更多信息，请参阅了解 Compliance Operator。

1.2.3.2. 配置 OAuth 令牌不活跃超时

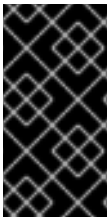
现在，您可以在 OAuth 令牌已停用一定时间后将其配置为过期。默认情况下，没有设置令牌不活跃超时。您可以为内部 OAuth 服务器和 OAuth 客户端配置超时。

如需更多信息，请参阅为内部 OAuth 服务器配置令牌不活动超时和 为 OAuth 客户端配置令牌不活跃超时。

1.2.3.3. 安全 OAuth 令牌存储格式

OAuth 访问令牌和 OAuth 授权令牌对象名称现在作为非敏感对象名称进行存储。

在以前的版本中，secret 信息用作 OAuth 访问令牌和 OAuth 授权令牌对象名称。当对 etcd 加密时，只有值会被加密，因此这些敏感信息不会被加密。



重要

如果您要将集群升级到 OpenShift Container Platform 4.6，来自 OpenShift Container Platform 4.5 的旧令牌仍会在对象名称中公开 secret 信息。默认情况下，令牌的过期时间为 24 小时，但管理员可以更改此设置。敏感数据仍可以被公开，直到所有旧令牌已经过期或被管理员删除。

1.2.3.4. File Integrity Operator 现已正式发布

File Integrity Operator 现已可用，它是在集群节点上持续运行文件完整性的 OpenShift Container Platform Operator。它部署一个守护进程集，在每个节点上初始化并运行特权高级入侵检测环境 (AIDE) 容器，从而提供一个状态对象和在守护进程集初始运行时修改的文件日志。

1.2.3.5. 对集群恢复失败使用的集群脚本已被更新

更新了 **cluster-backup.sh** 和 **cluster-restore.sh** 脚本，以便用户可以更好地了解恢复失败的原因。

1.2.4. 机器 API

1.2.4.1. 支持多个块设备映射

Machine API 现在支持 AWS 上运行的机器的多个块设备映射。如果有多个块设备，您现在可将日志、数据存储在空目录 Pod 中，将 Docker 镜像保存在独立于机器的根设备的块设备中。

1.2.4.2. Machine API providerSpec 的默认设置和验证

现在，在 **providerSpec** 的输入被持久化到 etcd 之前，特定的云供应商 API 上启用了默认设置和验证。验证在创建时针对机器和机器集运行。当知道配置阻止云供应商创建机器时，会返回反馈意见。例如，如果需要位置信息但未提供，机器集将被拒绝。

1.2.4.3. 在 Azure 上运行的机器集支持 Spot 虚拟机

在 Azure 上运行的机器集现在支持 Spot 虚拟机。您可以创建一个机器集将机器部署为 Spot 虚拟机，与标准虚拟机价格相比成本较低。如需更多信息，请参阅将机器设置为 Spot 虚拟机。

通过在机器集 YAML 文件的 **providerSpec 字段中添加 spotVMOptions** 来配置 Spot 虚拟机：

```
providerSpec:
  value:
    spotVMOptions: {}
```

1.2.4.4. 在 GCP 上运行的机器集支持可抢占虚拟机实例

在 GCP 上运行的机器集现在支持可抢占的虚拟机实例。您可以创建一个机器集，将机器部署为可抢占的虚拟机实例，与通常的实例价格相比成本较低。如需更多信息，请参阅部署可抢占虚拟机实例的机器设置。

通过在机器集 YAML 文件中的 **providerSpec** 字段中添加 **preemptible** 来配置可抢占虚拟机实例：

```
providerSpec:
  value:
    preemptible: true
```

1.2.5. Web 控制台

1.2.5.1. 改进了 Web 控制台的升级体验

- 现在，管理员可以通过有用的文本和 web 控制台中的链接更好地了解升级频道之间的差别。
- 现在，为每个次要版本或补丁版本提供了程序错误修正和功能增强列表的链接。
- 现在，不同的升级路径有视觉化的显示。
- 现在，当补丁发行、新的次发行版本和新频道可用时会向管理员发出提示信息。

1.2.5.2. 改进了使用 OperatorHub 的 Operator 安装工作流

管理员使用 OperatorHub 安装 Operator 时，它们现在可以获得即时反馈信息，以确保 Operator 被正确安装。

1.2.5.3. 改进了操作对象详情视图

现在，您可以在操作对象的详情视图中看到 **specDescriptor** 字段的 schema 分组和 Operands 的状态，以便您可以轻松查看状态并配置操作对象实例的 **spec**。

1.2.5.4. 查看集群 Operator 的相关对象

在以前的版本中，当查看集群 Operator 时，不知道 Operator 关联到哪些资源。在对 cluster Operator 进行故障排除时，找到 Operator 所管理的所有资源的日志可能会有一定难度，而这在进行故障排除时可能需要。现在，在 OpenShift Container Platform 4.6 中，您可以公开集群 Operator 的相关对象列表，并轻松查看其中一个相关对象详情或 YAML 代码用于故障排除。

1.2.5.5. 编辑受管资源时的警告信息

管理某些资源，例如由部署、路由、服务或配置映射管理的 Operator。不建议用户编辑这些资源。用户应编辑 Operator 及其操作对象的自定义资源，并期望 Operator 更新其相关资源。在这个版本中：

- 现在，**Managed by** 标签会显示在资源名称下，并带有到管理资源的链接。
- 当修改或删除资源时，会出现一条信息警告用户可能会恢复更改。

1.2.5.6. k8sResourcePrefix specDescriptor 字段支持 CRD 实例

operator 作者、维护者和供应商现在可以使用 **Group/Version/Kind** 指定 **k8sResourcePrefix specDescriptor** 字段来分配 CRD 资源类型，而不是 Kubernetes core API。

如需更多信息，请参阅 OLM 描述符引用。

1.2.5.7. 资源页面中的栏管理

现在，**Manage** 栏图标  被添加到一些资源页面中，如 **Pods** 页面。当您点击图标时，会使用模态

左侧的复选框列出默认字段名称，同时在右侧列出附加字段名称。取消选择复选框将从表视图中删除该列。选择一个复选框会将该列添加到表视图中。同时可以最多显示来自两端的 9 个字段。点 **Save** 可保存您所做的更改。点 **Restore Default Columns** 将恢复这些字段的默认设置。

1.2.5.8. Developer Perspective (开发者视角)

- 现在，会根据用户访问角色或权限，将用户定向到 **Administrator** 或 **Developer** 视角。
- 现在，当用户登录时，会提供一个 **Developer** 视角中的功能的交互式入门演示。
- **List** 视图和 **Topology** 视图 现在提供了相同的信息，用户可以根据应用程序大小和组件数量选择最佳视图。
- 现在，**Topology** 和 **List** 视图中都提供了对所有工作负载类型的支持，以便更好地了解所使用的计算资源。
- 现在，从 **Developer** 目录安装 chart 时，可以选择 Helm chart 版本和应用程序版本。您还可以在表单和 YAML 编辑器间切换，同时保留输入的值。
- Knative 事件工作流已进行了改进：
  - 添加了对 Knative Eventing Channels 的支持，以构建可靠的事件交付机制。
  - 现在，您可以使用相关的代理过滤器为频道和触发器创建订阅，并选择 Knative 服务作为订阅者。
  - 现在，在创建事件源时，可以从该命名空间中指定 sink 作为任何 Knative 资源，如 Knative 服务、频道或代理 ; 或一个 URI。
  - 现在，您可以通过频道、订阅、代理或触发器来视觉化 Knative 服务订阅的事件源之间的关系。有关事件源关系的详情也可以在侧面面板中看到。
  - 提供了过滤特定事件类型的功能。
- 对可用性进行了增强，如添加运行时标签来查看适当的运行时图标和工具提示。
- 现在，您可以添加、编辑和删除工作负载中的基本 pod 横向自动扩展（HPA），创建 HPA 并指定分配的工作负载。
- 如果集群中启用了 OpenShift Service Mesh，并且给定命名空间已启用，您现在可以点 **Topology** 视图中的 Kiali 链接导航到右侧命名空间中配置的 Kiali 仪表板。
- **Monitoring** 视图现在可以过滤 **Monitoring** 仪表板中特定于资源的指标。您也可以查看触发警报、静默并查看为项目配置的警报规则。

1.2.6. 扩展

1.2.6.1. 集群最大限制

针对 OpenShift Container Platform 4.6 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。

1.2.6.2. 添加到 Node Tuning Operator 的实时配置集

在 OpenShift Container Platform 4.4 中提供了部分 Tuned 实时配置集支持。现在，实时配置集与 Red Hat Enterprise Linux（RHEL）中的 Tuned 实时配置集完全兼容。

1.2.6.3. 现在完全支持 Performance Addon Operator

Performance Addon Operator 可帮助管理员为低延迟和实时工作负载调整 worker 节点。它以 **PerformanceProfile** 自定义资源的形式采用高级别调整意图，并将其转换为为低延迟目的配置 Linux 内核、操作系统、巨页和 kubelet 的所有所需操作。

除之前的发行前提供的功能外，这个版本还包括以下功能：

- 可以为每个 pod 启用 CPU 负载均衡。
- 可以同时指定多个巨页大小。
- 提高了支持性，如集成收集以及改进状态报告。
- 已设计并记录了一个覆盖字段内紧急配置的方法。

1.2.6.4. 使用 Intel 设备优化数据平面性能

OpenShift Container Platform 4.6 支持：

- Intel FPGA PAC N3000 的 Open Operator
- Open SR-IOV Operator for Wireless FEC 加速器

注意

N3000 Operator 需要预构建驱动程序容器，其中包含树内内核模块的 Open Programmable 加速器引擎 (OPAE)。预构建的驱动程序容器由 Intel 构建并提供，目前 OpenShift Container Platform 4.6.16 支持。如果需要使用不同的 OpenShift Container Platform 版本，请通过 Intel® Premier Support Access 或 openness.n3000.operator@intel.com 联系 Intel。

如需了解更多详细信息，请参阅 Wireless FEC 加速器的 OpenNESS Operator。

这些 Operator 支持 vRAN 部署对低功耗、成本和延迟的要求，同时还提供相应的功能来管理性能高峰。4G 和 5G 工作负载中最需要计算资源的是 RAN 第 1 层 (L1) 转发错误更正 (FEC)，它可以解决不可靠或不安全通信通道上的数据传输错误。

随着 FEC 的成熟和更多用户依赖网络，交付高性能 FEC 对 5G 而言至关重要。FEC 通常在字段可编程 Arrays (FPGA) 加速器卡上实施，如 Intel PAC N300 以及最近在 Intel vRAN Dedicated 加速器 ACC100 上实现。

如需更多信息，请参阅使用 Intel FPGA PAC N3000 和 Intel vRAN Dedicated 加速器 ACC100 优化数据平面性能。

1.2.6.5. 在控制台中管理裸机主机

在以前的版本中，没有记录如何在 web 控制台中维护裸机主机。现在，这个内容已添加。如需更多信息，请参阅管理裸机主机。

1.2.7. 开发者体验

1.2.7.1. oc set probe 命令已扩展

oc set probe 命令扩展为支持设置启动探测。

1.2.7.2. oc adm upgrade 命令现在会提供可升级条件

oc adm upgrade 命令现在会提供任何 **Upgradeable=False** 条件，因此管理员会了解到可能会因为一个 **Upgradeable=False** 条件而拒绝特定的更新。

1.2.8. 网络

1.2.8.1. OVN-Kubernetes 集群网络供应商 GA

OVN-Kubernetes 集群网络供应商现在是 GA。网络供应商作为 Kubernetes Container Network Interface（CNI）插件实现。如需更多信息，包括 OpenShift SDN 功能的信息，请参阅关于 OVN-Kubernetes Container Network Interface（CNI）网络供应商。

在本发行版本中，OpenShift SDN 保留默认集群网络供应商。

注意

在 OpenShift Container Platform 4.6 GA 的 Red Hat Enterprise Linux（RHEL）7.8 上不支持 OVN-Kubernetes。

1.2.8.2. 扩展节点服务端口范围

节点服务端口范围可扩展至默认的 **30000-32767** 范围。您可以在 **Service** 对象中使用此扩展范围。如需更多信息，请参阅配置节点端口服务范围。

1.2.8.3. SR-IOV Network Operator InfiniBand 设备支持

Single Root I/O Virtualization（SR-IOV）Network Operator 现在支持 InfiniBand（IB）网络设备。有关为集群配置 IB 网络设备的更多信息，请参阅配置 SR-IOV InfiniBand 网络附加。

1.2.8.4. 增加了置备网络的 DHCP 范围

为更好地支持大型部署，增加了置备网络的默认 DHCP 范围，使其包含本发行版本中子网的剩余部分。希望 DHCP 使用较少子网的用户，仍可以根据自己的需要进行配置。(BZ#1841135)

1.2.8.5. Pod 网络连接检查

现在，操作员可以配置 **PodNetworkConnectivityCheck** 资源，以检查由 Operator 管理的 pod 的每个网络连接。这可让您更轻松地识别并排除集群中重要网络连接的问题。

这个资源可追踪最新可访问状况、最后的 10 个成功状况、最后的 10 个故障以及探测到的故障的详情。还会记录结果，并在检测和解决故障时创建事件。

默认情况下会检查以下网络连接：

- 在 Kubernetes API 服务器和：
  - OpenShift API 服务器服务
  - 每个 OpenShift API 服务器端点

    - 每个 etcd 端点
    - 内部 API 负载均衡器
    - 外部 API 负载均衡器
- OpenShift API 服务器与：
    - Kubernetes API 服务器服务
    - 每个 Kubernetes API 服务器端点
    - 每个 etcd 端点
    - 内部 API 负载均衡器
    - 外部 API 负载均衡器

1.2.8.6. 辅助设备指标可与网络附加关联

二级设备或接口用于不同目的。这需要一个方法对它们进行分类，以便您可以使用相同的分类来汇总二级设备的指标。

kubelet 已发布一组网络可观察相关指标。这些指标中的标签包括：

- Pod 名称
- Pod 命名空间
- 接口名称，如 eth0

这可以正常工作直到在将新接口添加到 pod（例如通过 Multus）时，因为无法清楚接口名称引用的内容。interface 标签指向接口名称，但它不知道接口的作用是什么。如果使用很多不同的接口，就无法理解我们监控的指标引用的网络是什么。这个问题可以通过引入新的 **pod_network_name_info** 指标来解决，该方法可用于构建包含 kubelet 公开的值以及指标相关网络附加定义名称的查询，以标识网络类型。

如需更多信息，请参阅将二级接口指标与网络附加关联。

1.2.8.7. CNF 测试可以在发现模式下运行

这是一个可选模式，Cloud-native Network Function（CNF）测试会试图在集群上查找配置而不是应用新的配置。CNF 测试镜像是 CNF conformance 测试套件的容器化版本。它旨在针对启用了 CNF 的 OpenShift Container Platform 集群运行，该集群安装了运行 CNF 工作负载所需的所有组件。

每次执行测试时都会执行环境配置。这包括创建 SRI-OV 节点策略、性能配置集或 PTP 配置集等项目。允许测试对已进行了配置的集群进行配置可能会影响集群的功能。另外，对配置项目（如 SR-IOV 节点策略）的更改可能会导致环境临时不可用，直到处理配置更改为止。

发现模式会在不更改其配置的情况下验证集群的功能。在测试时使用现有环境配置。测试会尝试查找所需的配置项目，并使用这些项目来执行测试。如果没有找到运行特定测试所需的资源，则会跳过测试，为用户提供正确的信息。测试完成后，不会清理预配置的配置项目。测试的环境可立即运行另一个测试。

1.2.8.8. HAProxy 版本升级

OpenShift Container Platform 4.6 中的 Ingress 现在使用 HAProxy 版本 2.0.16。

1.2.8.9. Control over X-Forwarded header

现在可以通过设置 **forwardHeaderPolicy** 参数来控制 X-Forwarded 标头。

现在，通过引入 **haproxy.router.openshift.io/set-forwarded-headers** 路由注解，支持在每个路由上应用和配置 X-forwarded 的标头。

如需更多信息，请参阅使用 X-Forwarded 的标头。

1.2.8.10. 修改路由路径

现在，通过 **haproxy.router.openshift.io/rewrite-target** 变量支持为入站请求修改路由路径。

如需更多信息，请参阅 Route 配置。

1.2.8.11. Ingress 终止策略

现在，可以使用 **route.openshift.io/termination** 注解来为 Ingress 对象定义终止策略。

如需更多信息，请参阅通过 Ingress 对象创建路由。

1.2.8.12. AWS 的 Ingress Controller 网络负载均衡

现在支持为新的和现有的 AWS 集群配置 Ingress Controller Network Load Balancer（NLB）。

如需更多信息，请参阅 使用网络负载平衡器在 AWS 上配置 ingress 集群流量 。

1.2.8.13. AWS Route53 的 Ingress Operator 端点配置

现在，Ingress Operator 支持 AWS Route53 端点配置。

如需更多信息，请参阅 AWS Route53 的 Ingress Operator 端点配置 。

1.2.8.14. Ingress Controller 的唯一 ID 配置

现在支持配置 Ingress Controller 以注入带有唯一定义的请求 ID 的 HTTP 标头。这可用于跟踪集群流量。

如需更多信息，请参阅 **IngressController** 规格。

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

当使用 OVN-Kubernetes 集群网络供应商时，您可以在网络策略规则中选择 Ingress Controller 的流量，无论 Ingress Controller 在集群网络还是主机网络上运行。在网络策略规则中，policy **-group.network.openshift.io/ingress=""** 命名空间选择器标签与 Ingress Controller 的流量匹配。您可以继续使用 network **.openshift.io/policy-group: ingress** 命名空间选择器标签，但这是一个传统标签，可在以后的 OpenShift Container Platform 发行版本中删除。

在早期的 OpenShift Container Platform 版本中，存在以下限制：

- 使用 OVN-Kubernetes 集群网络供应商的集群无法从主机网络上的 Ingress Controller 选择流量。

如需更多信息，请参阅 关于网络策略。

1.2.8.16. 网络策略支持选择主机网络流量

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

1.2.9. 存储

1.2.9.1. 现在，CSI 驱动程序由 Cluster Storage Operator 管理

现在，AWS Elastic Block Store（EBS）、Red Hat Virtualization（oVirt） 和 OpenStack Manila 共享文件系统服务的 Container Storage Interface（CSI）Driver Operators 和驱动程序由 Cluster Storage Operator in OpenShift Container Platform 管理。

对于 AWS EBS 和 oVirt，此功能会默认在 **openshift-cluster-csi-drivers** 命名空间中安装 CSI Driver Operator 和驱动。对于 Manila，CSI Driver Operator 安装在 **openshift-cluster-csi-drivers** 中，驱动会在 **openshift-manila-csi-driver** 命名空间中安装。

重要

如果您在 OpenShift Container Platform 4.5 集群中安装了 CSI Driver Operator 和驱动程序：

- 在将 AWS EBS CSI Driver Operator 和驱动程序更新到较新版本的 OpenShift Container Platform 之前，必须卸载 AWS EBS CSI Driver Operator 和驱动程序。
- Operator Lifecycle Manager（OLM）不再提供 OpenStack Manila CSI Driver Operator。Cluster Version Operator 会自动转换它。原始 **openshift-manila-csi-driver-operator** 命名空间可能仍然存在，并可以被集群管理员手动删除。

1.2.9.2. 使用 Local Storage Operator 自动发现并置备设备（技术预览）

Local Storage Operator 现在可以：

- 自动发现集群中可用磁盘列表。您可以选择节点列表或所有节点，以便持续应用自动发现。
- 从附加设备中自动置备本地持久性卷。相关的设备会被过滤，并根据过滤的设备置备持久性卷。

如需更多信息，请参阅自动发现和置备本地存储设备。

1.2.9.3. 已删除 AWS EFS（技术预览）功能的外部置备程序

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

1.2.10. 容器镜像仓库（Registry）

1.2.10.1. 镜像修剪器容许无效的镜像

镜像修剪程序现在默认容忍 OpenShift Container Platform 新安装上的无效镜像引用，这样可以继续进行修剪，即使它找到无效的镜像。

1.2.10.2. 更改镜像修剪器的日志级别

集群管理员现在可以在 Pruning Custom Resource 中配置 **logLevel** 来设置调试日志。

1.2.10.3. 镜像 registry 支持 Azure Government

镜像 registry 现在可以为 Azure Government 设置和配置。

如需更多信息，请参阅为 Azure 政府配置 registry 存储。

1.2.10.4. 更改 Image Registry Operator 的日志级别

集群管理员现在可以在 Image Registry Operator 中配置 **logLevel** 调试日志。

logLevel 支持的值有：

- **Normal**
- **Debug**
- **Trace**
- **TraceAll**

Image Registry Operator YAML 文件示例

```
spec:
logLevel: Normal
operatorLogLevel: Normal
```

1.2.10.5. 更改 Image Registry Operator 的 spec.storage.managementState

在 AWS 或 Azure 的安装程序置备的基础架构中的新安装或升级的集群中，Image Registry Operator 现在会把 **spec.storage.managementState** 参数设置为 **Managed**。

- **Managed**: 确定 Image Registry Operator 管理底层存储。如果 Image Registry Operator 的 **managementState** 被设置为 **Removed**，则存储将被删除。
  - 如果 **managementState** 设为 **Managed**，Image Registry Operator 会尝试对底层存储单元应用一些默认配置。例如，如果设置为 **Managed**，Operator 会尝试在 S3 存储桶上启用加密，然后提供给 registry。如果您不希望默认设置应用到您提供的存储中，请确保将 **managementState** 设置为 **Unmanaged**。
- **Unmanaged**：确定 Image Registry Operator 忽略存储设置。如果 Image Registry Operator 的 **managementState** 设置为 **Removed**，则存储不会被删除。如果您提供了底层存储单元配置，如存储桶或容器名称，并且 **spec.storage.managementState** 尚未设置为任何值，则 Image Registry Operator 会将其配置为 **Unmanaged**。

1.2.11. Operator 生命周期

1.2.11.1. Operator 版本依赖项

Operator 开发人员现在可以通过在 **dependencies.yaml** 文件中使用 **olm.package** 类型来确保 Operator 包含特定版本的依赖关系。

如需更多信息，请参阅 Operator Lifecycle Manager 依赖项。

1.2.11.2. Operator 捆绑包中支持的其他对象

Operator Bundle Format 现在支持以下额外 Kubernetes 对象：

- **PodDisruptionBudget**
- **PriorityClass**
- **VerticalPodAutoScaler**

如需更多信息，请参阅 Operator Framework 打包格式。

1.2.11.3. 使用 opm进行有选择的捆绑包镜像镜像

Operator 管理员现在可以使用 **opm index prune** 命令选择要镜像的捆绑包镜像。

如需更多信息，请参阅修剪索引镜像。

1.2.11.4. 转换（Conversion）webhook 支持全局 Operators

Operator 开发人员现在可以使用转换 webhook 针对所有命名空间（也称为全局 Operator）的 Operator 进行操作。

如需更多信息，请参阅定义 Webhook。

1.2.11.5. 现在支持 Operator API

现在，OpenShift Container Platform 4.5 中作为技术预览的 Operator API 已被支持并默认启用。使用 Operator Lifecycle Manager（OLM）安装 Operator 需要集群管理员了解多个 API 对象，包括 **CatalogSource**、**Subscription**、**ClusterServiceVersion** 和 **InstallPlan** 资源。这个单一 Operator API 资源是实现更简化的体验发现和管理 OpenShift Container Platform 集群中 Operator 生命周期的第一步。

现在，对于使用 **Subscription** 资源安装 CSV 的 Operator，新的 Operator API 会自动标记相关资源。集群管理员可以使用 CLI 与单个 API 进行交互。例如：

```
$ oc get operators
```

```
$ oc describe operator <operator_name>
```

1.2.11.5.1. 在集群进行升级前，会删除 Operator API 的技术预览版本

如果您在 OpenShift Container Platform 4.5 中启用了 Operator API 的技术预览版本，则必须在升级到 OpenShift Container Platform 4.6 前禁用它。如果不这样做，则会无法进行集群升级，因为这个功能需要Cluster Version Operator（CVO）覆盖 功能。

先决条件

- 启用了技术预览 Operator API 的 OpenShift Container Platform 4.5 集群

流程

1. 因为 Operator API 标签自动应用于 OpenShift Container Platform 4.6 中的相关资源，所以您必须删除之前手动应用的所有 **operators.coreos.com/<name>** 标签。
   a. 您可以通过运行以下命令，检查当前为 Operator 标记了哪些资源，并查看 **status.components.refs** 部分：

```
$ oc describe operator <operator_name>
```

例如：

```
$ oc describe operator etcd-test
```

输出示例

```
...
Status:
  Components:
    Label Selector:
      Match Expressions:
        Key:      operators.coreos.com/etcd-test
        Operator:  Exists
    Refs:
      API Version:  apiextensions.k8s.io/v1
      Conditions:
        Last Transition Time:  2020-07-02T05:50:40Z
        Message:               no conflicts found
        Reason:                NoConflicts
        Status:                True
        Type:                  NamesAccepted
        Last Transition Time:  2020-07-02T05:50:41Z
        Message:               the initial names have been accepted
        Reason:                InitialNamesAccepted
        Status:                True
        Type:                  Established
      Kind:                    CustomResourceDefinition (1)
      Name:                    etcdclusters.etcd.database.coreos.com (2)
...
```

(1) 资源类型。

(2) 资源名称。

b. 从所有相关资源中删除标签。例如：

```
$ oc label sub etcd operators.coreos.com/etcd-test- -n test-project
$ oc label ip install-6c5mr operators.coreos.com/etcd-test- -n test-project
$ oc label csv etcdoperator.v0.9.4 operators.coreos.com/etcd-test- -n test-project
$ oc label crd etcdclusters.etcd.database.coreos.com operators.coreos.com/etcd-test-
$ oc label crd etcdbackups.etcd.database.coreos.com operators.coreos.com/etcd-test-
$ oc label crd etcdrestores.etcd.database.coreos.com operators.coreos.com/etcd-test-
```

2. 删除 Operator 自定义资源定义（CRD）：

```
$ oc delete crd operators.operators.coreos.com
```

3. 从 OLM Operator 中删除 **OperatorLifecycleManagerV2=true** 功能门。

a. 编辑 OLM Operator 的 **Deployment** 对象：

```
$ oc -n openshift-operator-lifecycle-manager \
    edit deployment olm-operator
```

b. 从 **Deployment** 对象的 **args** 部分中删除以下标记：

```
...
    spec:
      containers:
      - args:
...
        - --feature-gates (1)
        - OperatorLifecycleManagerV2=true (2)
```

(1) (2) 删除这些标记。

c. 保存您的更改。

4. 重新启用 OLM 的 CVO 管理：

```
$ oc patch clusterversion version \
   --type=merge -p \
   '{
     "spec":{
       "overrides":[
         {
           "kind":"Deployment",
           "name":"olm-operator",
           "namespace":"openshift-operator-lifecycle-manager",
           "unmanaged":false,
           "group":"apps/v1"
         }
       ]
     }
   }'
```

5. 验证 Operator 资源已不再可用：

```
$ oc get operators
```

输出示例

```
error: the server doesn't have a resource type "operators"
```

现在，升级到 OpenShift Container Platform 4.6 不再会被此功能阻止。

1.2.11.6. Node Maintenance Operator 现在会验证维护请求

Node Maintenance Operator 现在验证 master 节点的维护请求，防止 master（etcd）仲裁违反。因此，只有 **etcd-quorum-guard** pod 中断预算（PDB）允许 master 节点才能将其设置为维护。(BZ#1826914)

1.2.11.7. 使用 NodeMaintenance 自定义资源将节点设置为维护模式

在以前的版本中，没有记录使用 **NodeMaintenance** 自定义资源 (CR) 的节点进入维护模式。现在，这个内容已添加。如需更多信息，请参阅了解节点维护模式

1.2.11.8. 为 Image Registry Operator 和操作对象单独设置日志级别

现在，用户可以为 Image Registry Operator 和操作对象单独设置日志级别。(BZ#1808118)

1.2.12. Builds

1.2.12.1. 支持对 HTTPS 代理后面的 Git 克隆的构建

现在，构建支持对 HTTPS 代理后面的 Git 克隆。

1.2.13. 镜像

1.2.13.1. 支持 Cloud Credential Operator 模式

除了现有的默认操作模式外，Cloud Credential Operator（CCO） 现在可以明确配置为使用以下模式进行操作： **Mint**、**Passthrough** 和 **Manual**。此功能为 CCO 使用云凭证处理集群中用于安装和其他任务的 **CredentialsRequest** 自定义资源提供了透明性和灵活性。

1.2.13.2. Power 和 Z 上的 Cluster Samples Operator

Cluster Samples Operator 默认提供了 Power 和 Z 架构的镜像流和模板。

1.2.13.3. 集群 Samples Operator 警告

现在，如果样本没有导入，Cluster Samples Operator 会通过一个警报进行通知，而不是进入降级状态。

如需更多信息，请参阅 使用带有备用或镜像 registry 的 Cluster Samples Operator 镜像流 。

1.2.14. Metering

1.2.14.1. 配置 metering Report 自定义资源的保留周期

现在，您可以在 metering **Report** 自定义资源（CR）中设置保留周期。metering **Report** CR 有一个新的 **expiration** 字段。如果在 **Report** CR 中设置了 **expiration** 周期值，且没有其他 **Report** 或 **ReportQuery** CR 依赖于过期的 **Report** CR，Metering Operator 会在保留期结束后从集群中删除 **Report** CR。如需更多信息，请参阅 metering **Report** CR 过期。

1.2.15. 节点

1.2.15.1. 配置节点审计日志策略

现在，您可以通过选择要使用的审计日志策略配置集来控制日志记录到节点审计日志的信息量。

如需更多信息，请参阅配置节点审计日志策略。

1.2.15.2. 配置 pod 拓扑分布限制

现在，您可以配置 pod 拓扑分布约束，以更加精细地控制 pod 在节点、区、区域或其他用户定义的拓扑域中的放置。这有助于提高高可用性和资源使用率。

如需更多信息，请参阅使用 pod 拓扑分布限制来控制 pod 放置。

1.2.15.3. 提供了新的 descheduler 策略（技术预览）

现在，descheduler 允许配置 **PodLifeTime** 策略。通过此策略，在 pod 到达特定的、可配置的年龄后会被驱除。

如需更多信息，请参阅 Descheduler 策略。

1.2.15.4. 根据命名空间和优先级过滤 descheduler（技术预览）

现在，您可以配置 descheduler 策略是否应该根据其命名空间和优先级考虑 pod 进行驱除。

如需更多信息，请参阅根据命名空间过滤 pod 和根据优先级过滤 pod 。

1.2.15.5. RemoveDuplicates descheduler 策略的新参数（技术预览）

RemoveDuplicates 策略 现在提供了一个可选参数 **ExcludeOwnerKinds** 用于指定 **Kind** 类型的列表。如果 pod 中有这些类型列为 **OwnerRef**，则该 pod 不会被考虑驱除。

如需更多信息，请参阅 Descheduler 策略。

1.2.15.6. 生成一个在一个 registry 范围内有效的 ImageContentSourcePolicy 对象

oc adm catalog mirror 命令会生成 **ImageContentSourcePolicy**（ICSP）对象，它将原始容器镜像存储库映射到镜像（mirror）的新位置，通常是在断开连接的环境中。当对集群应用新的或修改的 In-Circuit Serial Programming（ICSP）时，它将转换为 CRI-O 的配置文件并放在每个节点中。将配置文件放在节点的过程包括重新引导该节点。

在这个版本中，**oc adm catalog mirror** 增加了 **--icsp-scope** 标志。范围可以是 registry 或 repository。默认情况下，**oc adm catalog mirror** 命令会生成一个 ICSP，其中每个条目都特定于存储库。例如，它会将 **registry.redhat.io/cloud/test-db** 映射到 **mirror.internal.customer.com/cloud/test-db**。将镜像到 ICSP 文件中的 registry 范围可最小化集群必须重新引导其节点的次数。使用同一个示例，**registry.redhat.io** 会映射到 **mirror.internal.customer.com**。

具有广泛范围的 ICSP 可减少 ICSP 将来可能需要更改的次数，从而减少集群必须重新引导所有节点的次数。

1.2.16. 集群日志记录

Log Forwarding API 已正式发布
Log Forwarding API 现已正式发布。Log Forwarding API 允许您通过配置带有端点的自定义资源来转发日志来转发容器、基础架构和审计日志。Log Forwarding API 现在支持转发到 Kafka 代理并支持 syslog RFC 3164 和 RFC 5424，包括 TLS。您还可以将应用程序日志从特定项目转发到端点。

对于 GA 版本，Log Forwarding API 有很多变化，包括在日志转发自定义资源（CR）中更改参数名称。如果使用 Log Forwarding 技术预览版本，则需要手动对现有 Log Forwarding CR 进行所需的更改。

在日志消息中添加标签
Log Forwarding API 允许您添加自由文本标签来记录附加到输出日志的消息。例如，您可以通过数据中心标记日志，或者根据类型标记日志。添加至对象的标签也会通过日志消息转发。

新的集群日志记录仪表板
在 OpenShift Container Platform web 控制台中添加了两个新的仪表板，显示带有重要、低级指标的 chart，用于详细调查集群日志记录和 Elasticsearch 实例并进行故障排除。

OpenShift Logging 仪表板包含 chart，在集群级别显示 Elasticsearch 实例的详情，包括集群资源、垃圾回收、集群中的分片和 Fluentd 统计。

Logging/Elasticsearch Nodes 仪表板包含 charts，显示 Elasticsearch 实例的详情，很多在节点级别，包括索引、分片、资源等详情。

用于调整 Fluentd 的新参数
您可以通过新的 Fluentd 参数来对 Fluentd 日志收集器进行性能优化。使用这些参数，您可以更改：

- Fluentd 块和块缓冲的大小
- Fluentd 块清除行为
- Fluentd 块转发重试行为

这些参数可帮助您确定集群日志记录实例中延迟和吞吐量之间的利弊。

1.2.17. 监控

1.2.17.1. 用户定义项目的监控

在 OpenShift Container Platform 4.6 中，除了默认的平台监控外，您还可以为用户定义的项目启用监控。现在，您可以监控 OpenShift Container Platform 中的自己的项目，而无需额外的监控解决方案。使用这个新功能，可以集中监控核心平台组件和用户定义项目。

使用这个新功能，您可以执行以下任务：

- 为用户定义的项目启用和配置监控
- 创建使用您自己的 pod 和服务的指标的记录和警报规则
- 通过单一、多租户界面访问警报的指标和信息
- 将用户定义的项目的指标与平台指标进行比较

如需更多信息，请参阅 监控概述。

1.2.17.2. 对规则更改的警报

OpenShift Container Platform 4.6 包括以下警报规则的变化：

- 添加了 **PrometheusOperatorListErrors** 警报。该警报在控制器上运行列表操作时提供错误通知。
- 添加了 **PrometheusOperatorWatchErrors** 警报。该警报提供在控制器上运行监视操作时出现的错误通知。
- **KubeQuotaExceeded** 警报由 **KubeQuotaFullyUsed** 替代。在以前的版本中，如果资源配额超过 90% 阈值，则 **KubeQuotaExceeded** 警报会触发。如果完全使用资源配额，则 **KubeQuotaFullyUsed** 警报会触发。
- etcd 警报现在支持为指标添加自定义标签。
- **KubeAPILatencyHigh** 和 **KubeAPIErrorsHigh** 警报由 **KubeAPIErrorBudgetBurn** 警报替代。**KubeAPIErrorBudgetBurn** 组合了 API 错误和延迟警报，仅在条件足够严重时才会触发。

- 现在，kubelet 公开的就绪度和存活度探测指标会被抓取。这提供了容器的历史存活度和就绪度数据，这在对容器问题进行故障排除时非常有用。
- Thanos Ruler 的警报规则会被更新，在没有正确评估记录规则和警报规则时，会把警报进行分页。在这个版本中，当 Thanos Ruler 中的规则及警报评估没有完成时，重要警报不会被丢失。
- **KubeStatefulSetUpdateNotRolledOut** 警报被更新，以便在部署有状态的集合时不会触发。
- **KubeDaemonSetRolloutStuck** 警报已更新，以考虑守护进程设置推出进度。
- 基于原因的警报的严重性从 **critical** 调整为 **warning**。

注意

红帽不保证指标、记录规则或警报规则的向后兼容。

1.2.17.3. Prometheus 规则验证

OpenShift Container Platform 4.6 通过调用验证准入插件的 webhook 引入了 Prometheus 规则的验证。在这个版本中，会根据 Prometheus Operator 规则验证 API 检查所有项目中 **PrometheusRule** 自定义资源。

1.2.17.4. 为 Thanos Querier 添加了指标和警报规则

Thanos Querier 将 OpenShift Container Platform 核心指标和用于用户定义项目的指标聚合在单个多租户接口下，并选择性地进行重复数据删除。在 OpenShift Container Platform 4.6 中，为 Thanos Querier 部署了一个服务监控和警报规则,允许根据监控堆栈对 Thanos Querier 进行监控。

1.2.17.5. 虚拟机的 Pending Changes 警报已更新

现在，虚拟机的 **Pending Changes** 警报可以提供更详细的信息。(BZ#1862801)

1.2.18. Insights Operator

1.2.18.1. 深入了解 Operator 数据收集功能的增强

在 OpenShift Container Platform 4.6 中，Insights Operator 会收集以下附加信息：

- Pod 中断预算
- 卷快照自定义资源定义
- 不健康的 pod 的最新 pod 日志
- 运行红帽镜像的数据，包括使用镜像的容器数量以及相应 pod 的年龄
- 带有 crash looping 容器的 pod 的 JSON 转储
- **MachineSet** 资源配置
- 匿名 **HostSubnet** 资源配置
- **MachineConfigPool** 资源配置
- **default** 和 **openshift-*** 项目的 **InstallPlan** 资源，以及它们的数量

- Openshift 命名空间中的 **ServiceAccounts** 资源统计信息

另外，在这个发行版本中，Insights Operator 会收集有关所有集群节点的信息，而之前的版本只收集不健康节点的信息。

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. 主要的技术变化

OpenShift Container Platform 4.6 包括以下显著的技术更改。

现在，每个集群版本都提供默认 Operator 目录
从 OpenShift Container Platform 4.6 开始，Operator Lifecycle Manager（OLM）和 OperatorHub 使用的红帽提供的默认目录现在作为特定于 OpenShift Container Platform 次要版本的索引镜像提供。这允许 Operator 供应商针对每个集群版本发布 Operator 版本。

这些索引镜像基于 Bundle Format，用于替换基于已弃用的软件包清单格式的 App Registry 目录镜像（这些镜像针对 OpenShift Container Platform 4 的早期版本发布）。OpenShift Container Platform 4.1 到 4.5 将继续共享单个 App Registry 目录。

注意

虽然红帽不会为 OpenShift Container Platform 4.6 及之后的版本发布 App Registry 目录镜像，但基于 Package Manifest Format 的自定义目录镜像仍被支持。

如需有关捆绑格式和索引镜像的更多信息，请参阅 Operator Framework 打包格式。

重要的 Operator 升级要求
集群管理员必须确保之前通过 Operator Lifecycle Manager（OLM）安装的所有 Operator 都会在其最新频道中更新至升级到 OpenShift Container Platform 4.6 的最新版本。更新 Operator 可确保当默认 OperatorHub 目录在 OpenShift Container Platform 4.5 中的 App Registry 目录切换到 OpenShift Container Platform 4.6 中的新的索引镜像目录时，它们具有有效的升级路径。

如需了解更多有关确保安装的 Operator 的信息，请参阅升级安装的 Operators，并使用自动或手动批准策略进行升级。

其他资源

- 如需了解 OpenShift Container Platform 4.6 所需的已部署红帽集成组件（包括红帽 Fuse、Red Hat AMQ 和 Red Hat 3scale）的最低版本，请参阅以下红帽知识库文章：
  https://access.redhat.com/articles/5423161

CNI 网络供应商现在使用在集群节点上安装的 OVS
OpenShift SDN 和 OVN-Kubernetes Container Network Interface（CNI）集群网络供应商现在都使用在集群节点上安装的 Open vSwitch（OVS）版本。在以前的版本中，OVS 会在每个节点上运行，由一个守护进程集进行管理。使用主机 OVS 可避免任何可能的停机时间，如升级 OVS 容器化版本。

在使用已弃用 API 时会发出警告
在每次调用已弃用 API 时，**client-go** 和 **oc** 都会包括警告信息。调用已弃用的 API 会返回一个警告消息，其中包含目标 Kubernetes 移除发行版本和替换 API（如果适用）。

例如：

```
warnings.go:67] batch/v1beta1 CronJob is deprecated in v1.22+, unavailable in v1.25+
```

这是 Kubernetes 1.19 中包含的新功能。

改进了COPY 和 ADD 构建说明
OpenShift Container Platform 构建中的 **COPY** 和 **ADD** 指令的性能有所提高。与 **docker** 相比，**buildah** 中的 **COPY** 和 **ADD** 指令的初始实施性能明显下降。在这个版本中，构建可以更快地运行，特别是使用大型源存储库。(BZ#1833328)

Operator SDK v0.19.4
OpenShift Container Platform 4.6 支持 Operator SDK v0.19.4，它包括以下显著的技术更改：

- operator SDK 现在与 OpenShift Container Platform 范围一致使用 UBI-8 和 Python 3。下游基础镜像现在使用 UBI-8 并包含 Python 3。
- **run --local** 命令已弃用，以 **run local** 替代。
- **run --olm** 和 **--kubeconfig** 命令已启用，以 **run packagemanifests** 替代。
- 默认 CRD 版本从 **apiextensions.k8s.io/v1beta1** 改为 **apiextensions.k8s.io/v1**，用于创建或生成 CRD。
- **--kubeconfig** 标志添加到 **<run|cleanup> packagemanifests** 命令中。

基于 Ansible 的 Operator 的增强包括：

- Ansible Operator 现在是一个受支持的发行版本。
- Ansible Operator 现在包括一个 **healthz** 端点和 **liveness（存活度）**探测。

基于 Helm 的 Operator 的增强包括

- 当集群范围的发行版本资源改变时，Helm Operator 可以进行监视和协调。
- Helm Operator 现在可以通过为原生 Kubernetes 对象使用三向策略合并补丁来协调逻辑，以便正确实现并应用阵列补丁策略。
- Helm Operator 的默认 API 版本变为 **helm.operator-sdk/v1alpha1**。

UBI 8 用于 OpenShift Container Platform 中的所有镜像
OpenShift Container Platform 中的所有镜像现在默认使用通用基础镜像（UBI）版本 8。

Jenkins Node.js 代理升级
Jenkins Node.js 默认代理已升级到 Node.js 版本 12。

oc adm must-gather 命令默认不收集审计日志
oc adm must-gather 命令不再默认收集审计日志。要使用 **oc** 命令收集审计日志，必须包含额外参数。例如：

```
$ oc adm must-gather -- /usr/bin/gather_audit_logs
```

已为 OpenShift Container Platform 发行版本重命名了二进制sha256sum.txt.sig 文件
OpenShift Container Platform 发行版本中包括的 **sha256sum.txt.sig** 文件已重命名为 **sha256sum.txt.gpg**。这个二进制文件包含每个安装程序和客户端二进制文件的哈希值，用来验证它们的完整性。

重命名的二进制文件允许 GPG 正确验证 **sha256sum.txt**。这在以前的版本中因为命名冲突而不能实现。

1.4. 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 4.6 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 4.4	OCP 4.5	OCP 4.6
Service Catalog	DEP	REM	REM
Template Service Broker	DEP	REM	REM
OperatorSource 资源	DEP	DEP	REM
CatalogSourceConfig 资源	DEP	REM	REM
Package Manifest Format（Operator 框架）	DEP	DEP	DEP
oc adm catalog build	DEP	DEP	DEP
v1beta1 CRD	GA	DEP	DEP
Metering Operator	GA	GA	DEP
AWS EFS 的外部置备程序	REM	REM	REM
Microsoft Azure 集群的 Mint 凭证	GA	GA	REM

1.4.1. 已弃用的功能

1.4.1.1. 使用自己的 RHEL 7 计算机器

使用自己的（BYO）Red Hat Enterprise Linux（RHEL）7 计算机器的策略现已弃用。计划在以后的 OpenShift 4 版本中删除对使用 RHEL 7 计算机器的支持。

1.4.1.2. Metering Operator

Metering Operator 已弃用，并将在以后的发行版本中删除。

1.4.2. 删除的功能

1.4.2.1. OperatorSource 资源

OperatorSource 资源是 Operator Framework 的 Marketplace API 的一部分，在几个 OpenShift Container Platform 版本中已弃用，现已被删除。在 OpenShift Container Platform 4.6 中，**openshift-marketplace** 命名空间中的 OperatorHub 的默认目录现在只使用 **CatalogSource** 资源并启用了 **polling** 功能。默认目录在引用的索引镜像中每 15 分钟轮询新更新。

1.4.2.2. MongoDB 模板

所有基于 MongoDB 的样本都已替换、弃用或删除。

1.4.2.3. AWS EFS 的外部置备程序（技术预览）

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

1.4.2.4. TLS 验证返回到 Common Name 字段

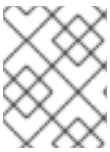
当没有 Subject 备用名称(SAN)时，作为主机名回退到 X.509 证书上的 **Common Name** 字段的行为已被删除。证书必须正确设置 **Subject Alternative Names** 字段。

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

从 OpenShift Container Platform 4.6.57 开始，在 Microsoft Azure 集群上以 mint 模式使用 Cloud Credential Operator(CCO)的支持已从 OpenShift Container Platform 4.6 中删除。此更改的原因是 Microsoft 的 Azure AD Graph API 将于 2022 年 6 月 30 日停用 ，并被向后移植到 z-stream 更新中所有支持的 OpenShift Container Platform 版本。

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

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



注意

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

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

如果在 Azure AD Graph API 停用后，集群被升级到一个不再支持 mint 模式的 OpenShift Container Platform 版本，CCO 会在关联的 **CredentialsRequest** 上设置 **OrphanedCloudResource** 条件，但不会将相关错误视为是致命（fatal）错误。该条件包括与 **unable to clean up App Registration / Service Principal: <app_registration_name>** 类似的消息。在 Azure AD Graph API 停用后，清理需要使用 Azure CLI 工具或 Azure Web 控制台手动删除剩余的应用程序注册服务主体。

要手动清理资源，您必须找到并删除受影响的资源。

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

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

输出示例

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

2. 运行以下命令来删除应用程序注册服务主体：

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

注意

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

1.5. 程序错误修复

apiserver-auth

- 在以前的版本中，在某些情况下 Ingress Operator 无法将 CA 证书推送到它的 **router-certs** secret 中，因此 Cluster Authentication Operator 无法在其健康检查中构建对证书的信任链，从而导致它进入 **Degraded** 状态并阻止升级。现在，在默认路由器 CA 检查过程中，CA 始终包含在 **default-ingress-cert** 配置映射中，因此 Cluster Authentication Operator 不再会阻止升级。(BZ#1866818)

- 在以前的版本中，Cluster Authentication Operator 无法解析从 OIDC 服务器返回的 HTML 页面，该页面忽略了 **Accept: application/json** 请求它们不支持的登录流时，因为 Operator 希望获得 JSON 响应。因此，Operator 无法遵循 IDP 配置。当因为不支持请求流从 OIDC 服务器返回 HTML 页面时，Cluster Authentication Operator 不再会失败。(BZ#1877803)

- 在以前的版本中，Cluster Authentication Operator 没有正确验证配置映射和 secret，这可能会导致 OAuth 服务器的新部署以使用无效或缺失的文件推出，从而导致 Pod 崩溃。配置映射和 secret 现在由 Cluster Authentication Operator 正确验证，因此当 ConfigMap 或 secret 包含无效数据时，不会推出新的部署。(BZ#1777137)

裸机硬件置备

- 在以前的版本中，**ironic-image** 容器配置缺少了设置来启用 **idrac-redfish-virtual-media** 引导驱动。因此，用户无法选择 Metal3 的 **idrac-virtual-media** 引导 URL。现在包括了缺少的 **ironic-image** 容器配置，因此用户可以选择 Metal3 的 **idrac-virtual-media** URL。(BZ#1858019)

- 在以前的版本中，某些 Dell 固件版本不在支持使用 Redfish 配置持久引导的支持。Dell iDRAC 固件被更新到 4.20.20.20 版本可解决这个问题。(BZ#1828885)

- 在这个发行版本中，解决了在同时检查许多节点时导致检查超时的问题。(BZ#1830256)

- 在以前的版本中，**ironic-image** 容器配置缺少了设置来启用 **idrac-redfish-virtual-media** 引导驱动。因此，用户无法选择 Metal3 的 **idrac-virtual-media** 引导 URL。现在包括了缺少的 **ironic-image** 容器配置，因此用户可以选择 Metal3 的 **idrac-virtual-media** URL。(BZ#1853302)

- 在以前的版本中，**openshift-machine-api** 命名空间中的 **metal3** pod 中的 HTTPd 容器是用来为裸机 ironic 镜像提供服务，允许目录列表。在这个版本中，不再允许在此容器中使用目录列表。(BZ#1859334)"

Build

- **buildah** 库中的错误可能会忽略特定的 HTTP 错误。由于目标 registry 的临时问题，构建可能会无法推送镜像。在这个版本中更新了 **buildah**，以在推送镜像 Blob 时可以正确处理这些错误。现在，如果上游 registry 暂时不可用，**buildah** 将无法推送镜像。(BZ#1816578)

- 在以前的版本中，OpenShift Container Platform 构建中使用的容器镜像签名策略不包含任何本地镜像的配置。当只允许来自特定 registry 的镜像时，构建中的 postCommit 脚本会失败，因为不允许使用本地镜像。容器镜像签名策略已更新，始终允许直接引用本地存储层的镜像。现在，如果构建包含 postCommit hook，则可以成功完成。(BZ#1838372)

- 在以前的版本中，如果 Docker 策略构建中使用的 **Dockerfile** 使用 **ARG** 指令，在 **Dockerfile** 的第一个 **FROM** 指令发生前定义构建参数，则在处理 **Dockerfile** 时会丢弃该指令，以纳入 **Build** 或 **BuildConfig** 资源中指定的任何覆盖。在使用预处理的 Dockerfile 构建镜像时，对这些参数的引用不会正确解决。预处理逻辑已被修改，以保留生成更新的 **Dockerfile** 内容时遇到的第一个 **FROM** 指令前遇到的 **ARG** 指令，因此不再出现这个问题。(BZ#1842982)

- 在以前的版本中，Buildah 会清除镜像上的镜像架构和 OS 字段。这会导致通用容器工具失败，因为生成的镜像无法识别其架构和操作系统。此程序错误修复可防止 Buildah 覆盖镜像和架构，除非有显式覆盖。这样可确保镜像始终具有架构和操作系统字段，且不会出现镜像不匹配警告。(BZ#1858779)

- 在以前的版本中，**Dockerfile** 构建失败，因为它们在某些情况下无法正确扩展构建参数。此更新修复了 **Dockerfile** 构建参数处理，因此 **Dockerfile** 构建现在可以成功。(BZ#1839683)

- 在以前的版本中，Buildah 调用会从其 blob 缓存中读取镜像，这会导致 Source-to-Image（S2I）构建失败。这个问题已在 Buildah v1.14.11 中解决，它已被加入到 OpenShift Container Platform 4.6。(BZ#1844469)

- 在以前的版本中，Buildah 无法引用 **COPY -from Dockerfile** 指令中的镜像。因此，包含 **COPY -from=<image>** 的多阶段 **Dockerfile** 构建会失败。buildah 已更新为支持 **COPY -from** 指令的版本。包含这些指令的构建现在可以成功。(BZ#1844596)

Cloud Compute

- 在以前的版本中，如果机器集上的 **replicas** 字段被设置为 nil 值，则自动扩展无法决定机器集中的当前副本数，因此无法执行扩展操作。在这个版本中，自动扩展会使用机器集中观察到的最后副本数，如果设置了 nil 值，则自动扩展由状态中的 **replicas** 字段报告。(BZ#1852061)

- 在以前的版本中，如果同一类型的节点存在 128 MB 以上的内存，则自动扩展不会平衡跨不同故障域的工作负载。在这个版本中，最大内存数量增加到 256MB。(BZ#1824215)

- 在以前的版本中，机器集 replicas 字段没有默认值。因此，如果没有此字段，机器集控制器会静默地失败。replicas 字段现在有一个默认值。如果没有设置 replicas 字段，会使用一个默认的副本。(BZ#1844596)

- 在以前的版本中，机器监控检查控制器不会在尝试删除它前检查机器是否已被删除。因此，控制器可能会发送多个删除请求，从而导致错误的日志记录和事件报告。机器健康控制器现在会在尝试删除它前，检查机器是否已被删除。因此，重复的日志和事件会减少。(BZ#1844986)

- 在以前的版本中，当集群 Operator 处于稳定状态时，Machine API Operator 会更新集群 Operator 机器 API。因此，资源在状态间快速循环。现在，只有在推出更改后，资源的状态才会改变。状态保持稳定。(BZ#1855839)

- 在以前的版本中，将 **balanceSimilarNodeGroups**、**ignoreDaemonSetsUtilization** 或 **skipNodesWithLocalStorage** 的 **ClusterAutoscaler** 资源值设置为 **false** 时，在部署自动扩展器时不会注册。现在，在部署集群自动扩展器时这些值会被正确读取。(BZ#1854907)

- 很少可以部署重复的机器 API 控制器实例。因此，集群可能会泄漏无法访问的机器。现在，领导选举机制添加到所有机器 API 组件中，以确保不会创建重复的实例。机器 API 控制器仅运行指定数量的实例。(BZ#1861896)

- 在 Red Hat Virtualization（RHV）集群上，手动机器扩展可能会失败。从 Web 控制台或 CLI 扩展机器现在可以正常工作。(BZ#1817853)

- 在以前的版本中，must-gather 不会收集 **BareMetalHost** 记录。因此，调试信息可能不完整。现在，must-gather 可以收集**BareMetalHost** 记录。(BZ#1841886)

- 在以前的版本中，在 Azure 上运行的集群上，计算机器会在安装时转换为 **Failed** 阶段。因此，创建后无法识别虚拟机。尝试联络带有错误的机器日志，在正确启动后 VM 可能会失败。作为修复，处于 **Creating** 状态的机器被识别为已创建。日志包含较少的错误，机器不太可能失败。(BZ#1836141)

- 在以前的版本中，机器健康检查可以接受 **spec.maxUnhealthy** 为负值。因此，在负数值时，每次协调都会产生大量事件。**spec.maxUnhealthy** 的负值。现在会将其视为 **0**，这可减少伪装的日志消息。(BZ#1862556)

Cloud Credential Operator

- 在以前的版本中，当从 OpenShift Container Platform 版本 4.5 升级到版本 4.6 时，一些字段会更新到 4.6 的默认值。因为未保留 4.5 字段值，所以会影响从 4.6 降级到 4.5 的功能。此程序错误修复明确保留了 4.5 值，这样就可以在降级尝试中再次指定默认值，而不是在 4.5 中未指定字段。现在，从 4.6 降级到 4.5 可能会成功。(BZ#1868376)

- 在以前的版本中，Cloud Credential Operator 领导选举机制使用来自 **controller-runtime** 的默认值，因此每 2 秒写入一次 **etcd**。此发行版本实施了自定义的领导选举机制，该选举机制现在每 90 秒写一次，并在正常关闭时立即释放锁定。(BZ#1858403)

Cluster Version Operator

- Cluster Version Operator 使用 HTTP 而不是 HTTPS 提供指标，并会受到 man-in-the-middle 攻击（未加密数据）。现在，Cluster Version Operator 使用 HTTPS 提供指标服务，数据已被加密。(BZ#1809195)

- 当集群管理员配置了集群版本覆盖时，升级过程会卡住。现在，当设置覆盖时会阻止升级。在管理员删除覆盖前，不会开始升级。(BZ#1822844)

- Cluster Version Operator 用来从代理配置的 **trustedCA** 属性引用的配置映射中加载可信 CA。引用的配置映射是用户维护的，设置损坏证书的用户将中断 Operator 对代理服务器的访问。现在，Operator 从 **openshift-config-managed/trusted-ca-bundle** 中加载 **trustedCA** 配置，Network Operator 会在代理配置引用的 **trustedCA** 配置映射有效时填充它。（BZ#1797123）

- HTTPS 签名获取序列化存储，从而导致 Cluster Version Operator 完成任务前潜在的超时时间。现在，外部 HTTPS 签名检索是并行的，会尝试所有存储。(BZ#1840343)

- 在以前的版本中，在使用 **--to-image** 选项（如 **oc adm upgrade --to-image**）进行 z-stream 集群升级过程中，Cluster Version Operator 使用升级至的集群版本，而不是使用当前集群版本进行验证。这会导致 z-stream 升级失败。现在，即使 Cluster Version Operator 具有 **Upgradeable=false**，也允许使用 **--to-image** 进行 z-stream 集群升级。(BZ#1822513)

- 在以前的版本中，Cluster Version Operator（CVO）没有同步 pod spec 中的 **shareProcessNamespace** 参数，这会导致 Registry Operator 不会更新 **shareProcessNamespace** 设置。CVO 现在同步 **shareProcessNamespace**、**DNSPolicy** 和 **TerminationGracePeriodSeconds** 参数，从而修复了 Registry Operator 更新问题。(BZ#1866554)

控制台 Kubevirt 插件

- 在以前的版本中，具有相同 NIC 配置集的 NIC 无法成功导入，或者选择了错误的网络。现在，web 控制台会强制用户为此类 NIC 选择相同的网络（而不是 pod 网络）。(BZ#1852473)
- 非管理员用户登录时，虚拟机不会被显示，因为 VM 列表等待 **virtualmachineimports** 数据被处理。现在,，M 列表可以被正确修改。(BZ#1843780)
- Create VM 向导 Edit Disk modal 没有考虑克隆的 PVC 命名空间。无法从不同命名空间中编辑 **datavolume** 磁盘。现在，磁盘模态可以正确地注册 **datavolume** 磁盘命名空间。(BZ#1859518)
- 当引用 URL 源时，虚拟机和模板的名称不能相同，因为 **datavolume** 名称是硬编码的。现在，一个自动生成的唯一字符串会添加到 **datavolume** 名称中，新的虚拟机和模板可以有相同的名称。(BZ#1860936)
- 因为数据是一个空的数组，所以网络使用数据数据会被显示为 **Not Available**。现在，会执行一个检查，空数组被解释为没有数据。(BZ#1850438)
- 在这个版本中, **Import VM** 功能已从 web 控制台的 **Developer** 视角中删除。(BZ#1876377)

控制台 Metal3 插件

- 用户界面无法检测到旧的节点维护 CRD，因为 EI 正在搜索最新版本。因此，如果存在节点维护操作，则节点维护操作会丢失旧的 **NodeMaintenance** CR。现在，web 控制台同时监控 **NodeMaintenance** CR。(BZ#1837156)
- 用户界面无法正确评估安全关闭，从而导致在关闭控制台时出现不正确的警告。现在，接口会等待节点 Pod 加载，并在关闭时显示正确的警告。(BZ#1872893)

容器

- 在以前的版本中，处理从构建上下文中复制内容的 **COPY** 或 **ADD** 指令的逻辑在 **.dockerignore** 文件存在时无法有效地过滤。如果评估源位置中的每个项目是否需要复制到目的地，那么会明显减慢**COPY** 和 **ADD**。此程序错误修复重写了相关逻辑，在存在 **.dockerignore** 文件时将不会明显降低构建期间处理 **COPY** 和 **ADD** 指令的速度。(BZ#1828119, BZ#1813258)
- 在以前的版本中，镜像构建和推送可能会失败，错误信息为 **error reading blob from source**，这是因为构建器逻辑会计算新层的内容两次。缓存层内容的逻辑依赖于这些计算结果的一致性。如果两个计算之间新层的内容发生变化，缓存将无法在需要时提供层内容。现在，新层的内容不再计算两次，从而使镜像构建不会失败。(BZ#1720730)

Web 控制台 (开发者视角)

- 在以前的版本中，当尝试通过 **Topology** 视图删除 Knative 应用程序时会失败并报告 **Knative 路由**不存在的错误。这个问题现已解决，错误将不再显示。(BZ#1866214)
- 在以前的版本中，web 控制台的 **Developer** 视角不允许导入不安全 registry 中的镜像。此程序错误修复添加了一个复选框，用户可以使用 **Deploy image** 表单中的不安全 registry。(BZ#1826740)

- 当用户选择 **From Catalog** 选项来创建应用程序时，**Developer Catalog** 会显示一个空白页面，而不是模板列表来创建应用程序。这是因为安装了 1.18.0 Jaeger Operator 造成的。这个问题现已解决，模板会如预期显示。(BZ#1845279)

- 当通过 web 控制台的 **Developer** 视角中的 **Pipeline Builder** 删除 Pipeline 中的并行任务时，接口会错误地重新安排连接到并行任务的任务，从而导致出现孤立的任务。在这个版本中，连接至已删除的并行任务的任务会与原始 Pipeline 重新关联。(BZ#1856155)

- 当用户在 web 控制台同时打开侧面面板取消管道创建时，web 控制台会抛出一个 JavaScript 异常。这个问题已通过改进内部状态处理得到解决。(BZ#1856267)

- 具有所需权限的用户无法从另一个项目中检索和部署镜像。现在创建了所需的角色绑定来解决这个问题。(BZ#1843222)

- 当您尝试使用 **Import from Git** 功能从 Git 存储库部署应用程序时，Web 控制台的 **Developer** 视角会对集群可以访问的私有存储库报告一个假的错误 **Git repository is not reachable**。这可以通过在错误消息中为集群添加有关使私有存储库可用的信息来解决。(BZ#1877739)

- 当通过 web 控制台的 **Developer** 视角创建 Go 应用程序时，到应用程序的路由不会被创建。这是因为 **build-tools** 中的一个错误导致，并错误配置了端口。这个问题已通过选择用户提供的端口或默认的端口 8080 作为目标端口来解决。(BZ#1874817)

- 当您使用 **Import from Git** 功能创建应用程序时，无法随后从 web 控制台更改应用程序的 Git 存储库。这是因为在以后的 Git 存储库 URL 编辑中更改了应用程序名称。这个问题已通过在编辑应用程序 Git 存储库 URL 时，使应用程序名称为只读进行了解决。(BZ#1873095)

- 在以前的版本中，没有管理或项目列表权限的用户无法查看任何项目的指标。此程序错误修复删除了访问集群指标时用户权限的检查。(BZ#1842875)

- 在用户名中具有 @ 字符的用户，如 **user@example.com**，无法从 web 控制台的 **Developer** 视角启动 Pipeline。这是因为 Kubernetes 标签中的一个限制所致。这个问题已通过将 **Started by** 元数据从 Kubernetes 标签移到 Kubernetes 注解中来解决。(BZ#1868653)

- 在以前的版本中，当用户选择一个指标数据时， QueryEditor 会显示查询。但是，如果用户删除或修改了查询并再次选择了相同的指标，QueryEditor 就不会更新。在这个版本中，如果某个查询被用户清除，并且他们试图再次选择同一个查询，查询输入文本区域就会显示查询。(BZ#1843387)

- Che Workspace Operator 删除了对 **Workspace** 资源的支持，并使用 **DevWorkspace** CRD 替换。因此，最新的 Che Workspace Operator 不会启用命令行终端。在这个版本中，OpenShift 命令行终端被移为使用 **DevWorkspace** 资源。现在，当安装 Che Workspace Operator 时，OpenShift Console 中将启用命令行终端。(BZ#1844938)

- 在以前的版本中，如果在多个修订版本中分布了流量，Knative 服务的路由 decorator 会将用户重定向到特定修订路由。路由 decorator 已更新，始终指向 Knative 基础服务路由。(BZ#1860768)

- 在以前的版本中，当用户为外部私有容器 registry 添加 secret 并从 registry 导入容器镜像时，pod 没有启动。因此，部署会卡住，直到手动更新服务帐户或部署为止。此程序错误修复允许新部署使用内部容器 registry 来启动其 pod。在这个版本中，用户可从外部私有容器 registry 导入容器镜像，而无需对服务帐户或部署进行额外的更改。（BZ#1926340）

- 控制台使用之前版本的 **KafkaSource** 对象，该对象使用规格中的 **resources** 和 **serviceAccountName** 字段。**KafkaSource** 对象的 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#1892695)

- 在以前的版本中，下载 chart 以实例化 helm 发行版本的相对 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。这个问题已通过将相关 Chart URL 转换为绝对 URL 来解决，Chart URL 现在可以被访问。(BZ#1916406)

- 在以前的版本中，用户无法在 **Topology** 视图中查看任何 Knative 服务和源。这是因为触发器同时具有 Knative 服务和 In-Memory Channel 作为订阅者，因为有一个 Null Pointer Exception（NPE）。这个问题已通过修复 Null Pointer Exception 来解决，从而 Knative 数据模型返回正确的数据，**Topology** 视图中会正确显示 Knative 资源。（BZ#1907827）

- 在以前的版本中，API 服务器可能无法创建资源并返回 409 状态代码，因为在更新资源配额资源时出现冲突。这个问题已被解决，{product title} web 控制台会在收到 409 状态代码时尝试重试请求。最多三次尝试通常足以完成请求。如果 409 持续发生，控制台中会显示一个错误。（BZ#1928230）

- 在以前的版本中，开发人员目录中不会显示 helm chart，因为 Chart 存储库 **httpClient()** 不考虑任何代理环境变量。这个问题已被解决，helm chart 现在会在开发人员目录中显示。（BZ#1919138）

- 虽然在 **Eventing** 用户界面中显示了技术预览徽标，但它将使用 GA 版本。现在，技术预览徽标已从 **Eventing** 用户界面中删除。(BZ#1899382)

- 在以前的版本中，当相关的 pod 数据不可用于部署配置时，应用程序会崩溃。这是因为，部署配置被加载后，控制台部署会马上获取两组数据用于 pod 状态的显示图。如果 API 返回超过 250 个 pod，则会跳过某些信息且不可用。这个问题已被解决，即使项目包含超过 250 个 pod，pod 数据也会可用，因此 **DeploymentConfig** 详情页面不会再崩溃。（BZ#1921603）

- 在以前的版本中，与触发器、订阅、频道和 IMC 事件源对应的静态模型使用 beta API 版本。在 Serverless 0.10 发行版本中，事件源的最新支持版本更新至 v1 版本。在这个版本中，更新了用户界面模型，以指向最新支持的版本。(BZ#1896625)

- 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#1916378）

- 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#1933727）

- 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#1933666）

- 在以前的版本中，用户无法从 **Developer** 视角将 Knative 服务创建为私有服务。这个问题现已解决，更新了标签 **'networking.knative.dev/visibility': 'cluster-local'**。(BZ#1978159)

- 在以前的版本中，如果 OpenShift Container Platform Web 控制台中使用 Bitbucket 存储库为部署创建的拓扑 URL 无法正常工作，如果它们包含包含斜杠字符的分支名称。这是因为 Bitbucket API BCLOUD-9969 存在问题。当前发行版本缓解了这个问题：如果分支名称包含斜杠，则拓扑 URL 指向存储库的默认分支页面。(BZ#1972694)

- 在以前的版本中，在 Git 导入流中为私有存储库创建的管道无法运行。这个问题现已解决，方法是将 secret 名称添加到管道的 **ServiceAccount** 对象注解中，并在提供的 secret 中添加特定于管道的注解。(BZ#1970984)

DNS

- 在以前的版本中，会发生重复的无效内存地址或 nil pointer 解引用错误，在运行 CoreDNS 1.6.6 时会包括 Kube API 访问超时。现在，这个问题可以通过正确处理 Endpoint Tombstones 错误来解决。现在，CoreDNS 的行为是不会重复的 panics。(BZ#1868315)

- 在以前的版本中，DNS Operator 会重复尝试更新 **DNS** 和 **Service** 对象，以响应 API 设定的默认值。在这个版本中，DNS Operator 认为 DNS Operator 未指定的值等于 **DNS** 和 **Service** 对象中的值。因此，DNS Operator 不再更新 **DNS** 或 **Service** 对象以响应 API 默认值。(BZ#1842741)

etcd

- 在以前的版本中，当 bootstrap 节点被删除后， **ETCDCTL_ENDPOINTS** 中的 bootstrap 端点不会被移除，因此 **etcdctl** 命令会显示意外错误。bootstrap 端点不再添加到 **ETCDCTL_ENDPOINTS** 中，因此 **etcdctl** 命令不会显示与 bootstrap 端点相关的错误。(BZ#1835238)

Image

- 在以前的版本中，使用清单列表中的摘要导入镜像会失败。在这个版本中，通过使用清单列表中所选清单摘要而不是清单列表，将转换从清单列表变为清单。因此，通过清单列表摘要导入可以按预期运行。(BZ#1751258)

镜像 Registry

- 在以前的版本中，有些内部软件包使用了内部错误结构，从而导致了空指针问题。现在，内部错误接口被返回，nil 错误会被正确转换。(BZ#1815562)

- 在为空时，Operator 没有生成 **httpSecrets**，从而导致值没有正确设置。现在，Operator 会生成 **httpSecret**，并在创建配置文件时将其用于所有副本。(BZ#1824834)

- 在以前的版本中，当镜像修剪器被禁用时，会出现无效的警报。这个警报现已被删除。(BZ#1845642)

- 对于一个变量，Registry Operator 类型断言（assertion）会进行两次，在第二次时没有检查结果。这会导致断言失败并产生 panic 条件。现在，使用已经过检查的断言，因此不会造成 panic。(BZ#1879426)

- 在以前的版本中，Operator bootstrap **storageManaged** 被设置为 **true**，当用户手动更新配置文件时会导致冲突。现在，创建了一个额外的配置字段 **spec.storage.storageManagementState**。用户可以将其指定为 **Managed** 或 **Unmanaged**，Operator 将遵循这个设置。(BZ#1833109)

- 当在将内容写入存储时删除 OpenStack 上的 Image Registry，会导致 Image Registry 的存储没有被移除，并且会记录 **409** HTTP 返回代码错误。在这个版本中，在删除存储前会删除存储内容。现在，当 Image Registry Operator 被删除时，其存储也会被删除。(BZ#1835770)

- 在 OpenStack 上进行安装时，如果在 Image Registry Operator bootstrap 的过程中无法访问 Swift 存储，则会导致 bootstrap 过程不完整。这会导致创建 Image Registry 配置资源失败，并会阻断修复或更改其配置。在这个版本中对这个问题进行了修复，现在可以防止当访问 Swift 存储出现问题时 bootstrap 出现故障。如果出现错误，则会记录相关的错误，允许 bootstrap 过程完成并创建配置资源。现在，Image Registry Operator 更为灵活，如果无法访问 Swift 存储，它会使用 PVC 来引导内部 Image Registry。(BZ#1846263)

- Image Registry Operator 避免多次调用 Azure 端点，因为 Azure 会强制实施配额，而在其前的版本中 Operator 会不断查询存储帐户密钥。在这个版本中，密钥会在本地缓存中存在一定时间，以避免在每次需要时都从远程获取密钥。(BZ#1853734)

- 在以前的版本中，Operator 认为在报告 Operator 状态时正在运行的作业会成功完成，即使作业可能会失败。现在，在报告 Operator 状态时，正在运行的任务会被忽略。(BZ#1857684)

- 当在 s3 存储中运行时镜像 registry 清除过程会失败，因为它会列出目录两次。现在，目录只会被列出一次，镜像清除过程可以成功完成。(BZ#1861304)

- 在以前的版本中，如果删除了 Image Registry Operator，修剪器任务会失败，因为它无法访问不存在的 registry。现在，修剪器作业仅移除 etcd 对象，并在删除 registry 时不会尝试 ping 注册表。(BZ#1867792)

- 如果用户手动添加存储桶名称，Operator 不会创建存储桶。现在，Operator 会根据用户提供的名称成功创建一个存储桶。(BZ31875013)

- 在以前的版本中，当 Image Registry Operator 遇到 **Too large resource version** 错误消息时，它无法从集群中获取事件。在这个版本中，**client-go** 库已被更新，以修复反射器，以便 Operator 可以从 **Too large resource version** 错误消息中恢复。(BZ#1880354)

- 在以前的版本中，为 Image Registry Operator 配置文件中的 **spec.requests.read/write.maxWaitInQueue** 提供的值不会被验证。如果提供的值是一个不能被解析为持续时间的字符串，则不会应用更改，同时会在日志中重复记录一个有关不正确值的消息。此发行版本添加了相关验证，用户不能提供此字段的无效值。(BZ#1833245)

- 在以前的版本中，修剪镜像时在镜像间跟踪依赖项会很慢。镜像修剪有时需要很长时间才能完成。底层镜像修剪的机制已被重新设计。现在，镜像修剪速度更快，并改进了并行性。(BZ#1860163)

安装程序

- 在以前的版本中，当机器试图获取 **resourcePoolPath** 时，它会找到多个资源池，无法解析正确的资源池。在这个版本中，添加到机器集合中的 **resourcePoolPath** 信息有助于解析正确的属性。(BZ#1852545)

- 在以前的版本中，在计算置备节点子网时，计算 DHCP 分配池的末尾值时有一个硬编码的值。这会导致，在机器 CIDR 小于 18 的 OpenStack 上的 OpenShift Container Platform 集群上部署时出现错误。在这个版本中，删除了对节点数目的硬编码，现在会动态计算 DHCP 分配池的末尾值。现在，只要集群对于所有必需的节点来说足够大，就可以在 OpenStack 上部署集群，并且带有具有任何长度的机器 CIDR。(BZ#1871048)

- 在以前的版本中，一些可用的网络在集群安装中不会被显示，因为一个 **ovirt-engine-sdk-go** API 错误会影响到 oVirt 网络解析。这个问题现已解决。(BZ#1838559)

- 在以前的版本中，在 **vSphere** web 控制台向导中，只会显示 **Network** 和 **DistributedVirtualPortgroup** 网络类型，即使 **OpaqueNetwork** 也是一个有效选项。现在，在向导中有一个 **OpaqueNetwork** 选项，因此可以选择这种类型的网络。(BZ#1844103)

- 在以前的版本中，Manila Operator 不支持自定义自签名证书，因此 Manila Operator 无法在使用自签名证书的一些环境中部署 Manila CSI 驱动程序。现在，Operator 会从系统配置映射获取用户提供的 CA 证书，将其挂载到驱动程序的容器中，并更新驱动程序的配置。因此，Manila Operator 可以在带有自签名证书的环境中部署和管理 Manila CSI 驱动程序。(BZ#1839226)

- 在以前的版本中，配置 **platform.aws.userTags** 参数将 **name** 或 **kubernetes.io/cluster/** tag 添加到安装程序创建的资源中，造成机器 API 无法识别现有的 control plane 机器，并创建一组 control plane 主机，这会造成 etcd 集群成员资格的问题。现在，您无法在 **platform.aws.userTags** 参数中设置可能会造成错误的 tag，集群不太可能具有额外的 control plane 主机和有问题的 etcd 集群。(BZ#1862209)

- 在以前的版本中，在用户置备的基础架构的 Azure 集群中部署的负载均衡器上没有定义健康检查

探测。因为负载均衡器没有被定义，所以它们不会发现 API 端点已不再可用，并继续将流量定向到它们，从而导致客户端失败。现在，健康检查探测会检查负载均衡器，它们可以正确地检测到 API 端点不可用，并停止路由到不可用的流量。(BZ#1836016)

- 在以前的版本中，安装程序不接受 * 作为 **proxy.noProxy** 字段的有效值，因此您无法在安装过程中创建没有将代理设置为 * 的集群。现在，安装程序接受 * 作为参数的有效值，因此您可以在安装过程中将任何代理设置为 *。(BZ#1877486)

- 以前，当您在 GCP 中安装集群时，总是使用 **US** 作为位置，因此可能无法在美国以外的一些区域安装集群。现在，安装程序为您指定的区域设置正确位置，因此可以在其他位置中成功安装。(BZ#1871030)

- 在以前的版本中，当在带有安装程序置备的基础架构的 vSphere 上安装了集群时，可以将相同的 IP 地址分配给 ingress 和 API，这会导致 bootstrap 机器和一个 control plane 机器具有相同的 IP 地址。现在，安装程序会验证 IP 地址是不同的，control plane 和 bootstrap 机器都会有唯一的 IP 地址。(BZ#1853859)

- 在以前的版本中，当接口获取一个新的 DHCP4 或 DHCP6 租期时，**local-dns-prepender** 不会更新 **resolv.conf** 文件来包括集群所需的所有域名解析程序。现在， **dhcp4-change** 和 **dhcp6-change** 的操作会让 **local-dns-prepender** 启动更新。(BZ#1866534)

- 在以前的版本中，您无法将集群部署到以下 GCP 区域：**asia-northeast3**、**asia-southeast-2**、**us-west3** 和 **us-west4**。现在您可以使用这些区域。(BZ#1847549)

- 在以前的版本中，OpenStack 安装程序在 **InstanceID()** 函数中使用不一致的输出格式。它从元数据或通过向服务器发送请求来获取实例 ID。在后者的情况下，结果总会带有 '/' 前缀，这是正确的格式。而如果实例 ID 来自元数据，则会因为这个错误，系统无法验证其节点的存在。现在，在元数据格式中也包含了 '/' 前缀，所以 ID 格式始终正确，系统可以成功验证节点是否存在。(BZ#1850149)

- 在以前的版本中，当为集群启用 FIPS 时，裸机安装程序置备的基础架构平台的置备服务会失败。在这个版本中，当启用了 FIPS 并成功完成安装时，置备服务会如预期运行。(BZ#1804232)

- 在以前的版本中，DHCP 范围可以被配置为置备网络使用整个子网，包括集群置备 VIP。因此，安装会失败，因为无法分配 bootstrap VM IP 和集群置备 IP。在这个版本中，会对 VIP 进行正确验证，以确保其不与 DHCP 范围重叠。(BZ#1843587)

- 在以前的版本中，当证书最后带有两个行尾字符时，安装会失败。在这个版本中，证书认证机构（CA）证书信任捆绑包解析程序已被修复，它忽略了不可见的字符。因此，CA 证书信任捆绑包现在允许在证书之前、之间和之后使用行尾字符。(BZ#1813354)

- 在以前的版本中，当交互式安装程序提示为集群输入 **ExternalNetwork** 资源请求时，会列出所有可能的网络选择，包括无效的选项。在这个版本中，交互式安装程序会对可能的选项进行过滤并只列出外部网络。(BZ#1881532)

- 在以前的版本中，裸机 **kube-apiserver** 健康检查探测使用硬编码的 IPv4 地址与负载均衡器通信。这个版本修复了使用 **localhost** 的健康检查，它可以正确处理 IPv4 和 IPv6。另外，API 服务器会检查 **readyz** 端点而不是 **healthz**。(BZ#1847082)

- 由于没有列出所有依赖步骤的 Terraform 步骤，Red Hat OpenStack Platform（RHOSP）上的集群会遇到一个竞争条件，有时会导致 Terraform 作业因为 **Resource not found** 错误而失败。为了避免竞争条件的出现，步骤现在列为 **dependent_on**。(BZ#1734460)

- 在以前的版本中，在更新机器前集群 API 不会验证 RHOSP flavor。因此，启动无效的 flavor 的机器会失败。现在，在更新机器前，实例类型会被验证，具有无效类别的机器会立即返回错误。(BZ#1820421)

- 在以前的版本中，在 RHOSP 上名称中带有句点（.）的集群会在安装的 bootstrap 阶段会失败。RHOSP 上的集群名称不再允许使用句点。如果集群名称包含句点，则会在安装过程的早期生成出错信息。(BZ#1857158)

- 在以前的版本中，在 AWS 上部署的用户置备的基础架构中，不会为负载均衡器定义健康检查探测。负载均衡器不会检测 API 端点何时不可用，这会导致客户端失败。在这个版本中，添加了健康检查探测，负载均衡器不会将流量路由到已下线的节点。(BZ#1836018)

- 在以前的版本中，Terraform vSphere 供应商中的 **DiskPostCloneOperation** 功能检查了从 Red Hat CoreOS OVA 镜像克隆的虚拟机的 **thin_provisioned** 和 **eagerly_scrub** 属性。因为置备类型在克隆过程中发生了变化使其与源置备类型不匹配，检查会失败。现在，**DiskPostCloneOperation** 功能会忽略这些属性，Red Hat CoreOS OVA 克隆可以成功执行。(BZ#1862290)

- 在运行 **./openshift-install destroy cluster** 时，安装程序会尝试在使用那些标签的资源被删除前删除安装程序标签。之后，安装程序将无法删除标签。在这个版本中，安装程序会在相应资源被删除后删除标签。(BZ#1846125)

kube-apiserver

- 在以前的版本中，当使用 **LatencySensitive** 功能门时，Cluster Version Operator（CVO）会将集群标记为不可升级。在这个版本中，CVO 不再将 **LatencySensitive** 功能门视为集群升级的一个阻碍。要解决这个问题，强制升级到最新的 4.5.z 或 stable 版本，其中包括了对这个问题 的解决方案。(BZ#1861431)

kube-controller-manager

- 在以前的版本中，守护进程集控制器在重新创建守护进程时没有明确预期。因此，守护进程设置可能会卡住五分钟，直到预期过期为止。现在，守护进程集控制器可以正确地清除预期。(BZ#1843319)

- 当一个项目被删除时，UID 范围分配不会更新，因此在具有大量命名空间创建和移除操作的集群中可以使用 UID 范围。要解决这个问题，**kube-controller-manager** pod 会定期重启，这会触发修复过程并清除 UID 范围。(BZ#1808588)

- 在以前的版本中，端点控制器在每个 informer 重新同步间隔上发送大量 API 请求，这会导致具有多个端点的大型集群中出现问题。存储的不一致和端点比较会导致端点控制器错误地假设集群需要很多额外的更新，比实际需要的更新更多。在这个版本中，更新了端点的存储和比较功能。使它们更为一致。因此，端点控制器现在只在需要时发送更新。(BZ#1854434)

- 在以前的版本中, **NotFound** 错误被控制器逻辑错误处理。这会导致控制器（如部署、守护进程集和副本设置控制器）不知道缺少的 pod。在这个版本中，控制器可以正确地响应 **pod NotFound** 事件，这代表 pod 之前被删除。(BZ#1843187)

kube-scheduler

- 在以前的版本中，当以空运行模式驱除 pod 时，某些 descheduler 策略把这个操作在日志中记录两次。现在，只为驱除创建一个日志条目。(BZ#1841187)

日志记录

- 在以前的版本中，Elasticsearch 索引指标默认在 Prometheus 中收集。因此，由于索引级别指标的大小，Prometheus 会快速地消耗可用的存储。为了保持 Prometheus 可以正常运行，用户需要手工进行一些操作（如减少 Prometheus 保留时间）。默认行为被修改为不收集 Elasticsearch 索引指标。(BZ#1858249)

- 因为 OpenShift Elasticsearch Operator 没有为 Kibana 部署更新 secret 哈希，所以如果 secret 被更新，则不会重启 Kibana Pod。现在，相关代码已被修改，可以正确地更新部署的 hash。这会如预期触发 pod 重新部署。(BZ#1834576)

- 由于增加了 Fluentd init 容器，因此在没有部署 OpenShift Elasticsearch Operator（EO）的情况下，Fluentd 无法部署到集群中。现在，相关代码已被修改，Fluentd 可以在没有 EO 的情况下运行。因此，在没有 Elasticsearch 的集群中，Fluentd 可以进行扩展。(BZ#1849188)

- 因为在 iframe 中打开 Kibana 的功能没有被拒绝，所以它使 Kibana 打开可能受到攻击，如 clickjacking 攻击。现在，代码已被修改，它会明确设置 **x-frame-options:deny**，这可以阻断对 iframes 的使用。(BZ#1832783)

Machine Config Operator

- 在裸机环境中，**infra-dns** 容器在每个主机上运行，以支持节点名称解析和其他内部 DNS 记录。**NetworkManager** 脚本还会更新主机上的 **/etc/resolv.conf** 使其指向 **infra-dns** 容器。另外，当创建 pod 时，会从它们的主机接收 DNS 配置文件（**/etc/resolv.conf** 文件）。
  如果在 **NetworkManager** 脚本更新主机上的 **/etc/resolv.conf** 文件前创建了 HAProxy pod，则该 pod 可能会重复失败，因为无法解析 **api-int** 内部 DNS 记录。在这个版本中更新了 Machine Config Operator（MCO），它会验证 HAProxy pod 的 **/etc/resolv.conf** 文件是否与主机 **/etc/resolv.conf** 文件一致。因此，HAProxy Pod 不再会遇到这些错误。(BZ#1849432)

- Keepalived 用于为 API 和默认路由器提供高可用性（HA）。每个节点中的 Keepalived 实例通过 curl 本地实体的健康端点（如本地 **kube-apiserver** ）来监控本地健康状况。在以前的版本中，只有在 TCP 连接失败时 **curl** 命令才会失败，在 HTTP 出现非 200 错误时不会失败。这会导致 Keepalived 有时在本地实体不健康时，也不会切换到另一个健康节点，这会导致 API 请求中出现错误。
  在这个版本中更新了 Machine Config Operator（MCO），在服务器收到了非 200 返回码时，**curl** 命令现在也会失败。因此，在本地实体出现故障时，API 和 Ingress 路由器现在可以正确地切换到一个健康的节点。(BZ#1844387)

- 在裸机环境中，一些 DNS 记录是为 IPv4 硬编码的。这会导致在 IPv6 环境中无法正确提供一些记录，这可能需要在外部 DNS 服务器中创建这些记录。在这个版本中，更新了 Machine Config Operator（MCO），现在 DNS 记录可根据使用的网络协议版本正确填充。现在，在 IPv4 和 IPv6 中都可以正确提供内部记录。(BZ#1820785)

- 在以前的版本中，机器配置中指定的内核参数需要被分为独立的字符串组成数组。在合并到 **rpm-ostree** 命令之前，这些参数不会被验证。通过使用空格进行间隔把多个内核参数组合起来时（在内核命令行的一个行中允许这样做），会创建一个无效的 **rpm-ostree** 命令。在这个版本中，机器配置控制器以类似内核的方式解析每个 **kernelArgument** 项。因此，用户可以通过使用空格进行间隔来提供多个参数。(BZ#1812649)

- 在以前的版本中，对于裸机环境，control plane 对于用户负载总是可以调度的。此程序错误修复更新了 Machine Config Operator（MCO），现在 control plane 节点会在使用 worker 的典型部署中正确配置为 **NoSchedule**。(BZ#1828250)

- 在以前的版本中，对于 Machine Config Operator（MCO），不必要的 API VIP 移动可能会导致客户端连接错误。在这个版本中，更新了 API VIP 健康检查，以限制其移动次数。因此，现在 API VIP 移动造成的错误会变少。(BZ#1823950)

Web 控制台（管理员视角）

- operand 的标签页缺少了 operand 列表视图。在这个版本中，这个问题已解决。(BZ#1842965)

- 当禁用 IPv6 时，下载 pod socket 无法绑定，下载 pod 会崩溃。如果没有启用 IPv6，现在会使用 IPv4 作为 socket。下载 Pod 现在可以正常工作，无论是否启用了 IPv4 和 IPv6。(BZ#1846922)

- Operator 状态显示值没有考虑手动批准策略。因此，显示 **upgrade available** 状态，这不会提示升级需要进一步的操作。为等待手动升级的 Operator 添加了一个新的状态消息。现在，可以明确告知 Operator 升级何时需要进一步操作。(BZ#1826481)

- 失败的操作对象的捕获逻辑试图访问生成的错误对象中的深度属性，而这个属性并非始终被定义。对于特定的失败请求类型，这会导致运行时错误。在这个版本中，这个问题已解决。(BZ#1846863)

- victory 无法正确处理全零数据集。所有零数据集的 Y 轴点号会重复为零。当所有数据集都是零时，区域图表逻辑被更新为强制 Y 域为 **[0,1]**。现在，全为零的数据集合的 Y 轴点符号是 **0** 和 **1**。(BZ#1856352)

- OperatorHub 上的 Operator 详情栏中未显示当前安装的版本。因此，用户无法判断当前安装的版本是否是最新的。在当前安装的 Operator 版本不是最新的版本时，现在 OperatorHub 上的 Operator 详情栏中会显示安装的版本。(BZ#1856353)

- **create role binding** 链接的命名空间和使用的集群链接不一致，因此 **create role binding** 页面不正确。此程序错误修复更新了相关链接，以使用命名空间（在可用的情况下）以及其它情况下的集群。现在使用正确的页面。(BZ#1871996)

- 在以前的版本中，web 控制台不支持 singlestat 面板的 Grafana 值映射，因此 singlestat 面板无法显示 Grafana 值映射。现在增加了支持，singlestat 面板可以显示 Grafana 值映射。(BZ#1866928)

- 针对 BZ#1812813 对 **oc debug** 进行了更新，使用空节点选择器创建新调试项目，解决了 **oc debug** 仅适用于 worker 节点的问题。Web 控制台避免了这个问题，方法是在终端打开前要求用户在访问 **Node → Terminal** 页面时选择命名空间，从而造成与 **oc** 的方法不一致的情况。现在，在访问 **Node → Terminal** 页面时，web 控制台使用空节点选择器创建一个新的 debug 项目。Web 控制台 **Node → Terminal** 页面的行为现在与 **oc debug** 的行为一致。(BZ#1881953)

- 在删除所有接收器时，Web 控制台会出现运行时错误，用户会看到一个空白屏幕。现在，在代码中增加了对 null 的检查，用户现在可以看到一个 **No Receivers** 空状态屏幕。(BZ#1849556)

- 在某些情况下，在生成旧操作对象时传递给资源要求 widget 的值可能不是 immutablejs 映射实例。当试图引用资源要求 widget 当前值的 immutablejs **Map.getIn** 函数时，会抛出一个运行时错误。当引用 immutablejs **Map.getIn** 函数时，使用可选的链。不会抛出运行时错误，可以显示 widget 没有值。(BZ#1883679)

- 当对 **imagemanifestvuln** 资源进行搜索时会出现一个空白页面。组件使用 **props.match.params.ns**，有时它并没有被定义。因此，会出现运行时错误。这个问题现已解决。(BZ#1859256)

- 在以前的版本中，对象列表右侧的 action 菜单在打开后会立即关闭。当点由 Operator 提供的 API 的一个标签页时，可以在 **Installed Operators** 详情页面中看到。这个菜单现在可以正常工作。(BZ#1840706)

- API 中缺少了一个关键字字段，用户无法在 OperatorHub 中搜索关键字。在这个版本中，这个问题已解决。(BZ#1840786)

- 在以前的版本中，Web 控制台中的 OperatorHub 有时会显示 Operator 的不正确图标。这个版本已经解决了这个问题。(BZ#1844125)

- 在这个发行版本中，web 控制台 OperatorHub 安装页面中的集群监控文档链接已被修正。(BZ#1856803)

- 在以前的版本中，点 **EtcdRestores** 页面中的 **Create EtcdRestores** 会导致 web 控制台停止响应。在这个版本中，**Create EtcdRestore** 表单会正确加载工作流。(BZ#1845815)

- 在以前的版本中，operand 表单数组和对象字段没有逻辑来检索和显示表单上的字段描述。因此，数组或对象类型字段的描述不会被呈现。现在，这个程序错误修复添加了在 operand 创建表单上显示阵列和对象字段描述的逻辑。(BZ#1854198)

- 在以前的版本中，当一个新 pod 启动时，**部署配置概述** 页面有时会崩溃并带有 **e is undefined** 错误。这个版本已经解决了这个问题。(BZ#1853705)

- 在以前的版本中，web 控制台中的集群升级界面在 OpenShift Dedicated 上可见，即使 OpenShift Dedicated 用户无法执行集群升级。现在，OpenShift Dedicated 隐藏了集群升级界面。(BZ#1874257)

- 在以前的版本中，当提交表单或在表单和 YAML 视图间切换时，操作对象模板中的空对象会被修剪。在这个版本中，当从表单数据修剪空白结构时，模板数据用作掩码，仅修剪模板中没有定义的值。模板中定义的空值保留。(BZ#1847921)

- 当将鼠标悬停在 **集群日志记录**圆饼图上时，工具提示详情有时会被截断。在这个版本中，启用了整个工具提示描述来显示这个图表。(BZ#1842408)

- 对于 **Create Instance** 页面中的 **Registry** 字段，schema 属性描述中的一些文本与在 Linkify 中创建 fuzzy hyperlinks 的格式匹配。这会产生意想不到的超链接。此程序错误修复会在 Linkify 中禁用 fuzzy link 功能。现在，只有使用正确协议方案的 URL 字符串才会显示超链接。(BZ#1841025)

- 即使 **ListDropdown** 组件没有处于加载状态，AWS **Secret** 字段也始终显示正在加载图标。此程序错误修复了组件逻辑，因此正在加载图标仅在下拉列表处于加载状态时才会显示。当下拉列表没有处于加载状态时，会显示占位符。(BZ#1845817)

- 在以前的版本中，当日志包含长行时，Web 控制台中的 **Resource Log** 页面会变得缓慢或者无响应。在这个版本中解决了性能问题，方法是限制 **Resource Log** 页中显示的每个日志行的字符数，并提供查看完整日志内容的替代方法。(BZ#1874558)

- 在以前的版本中，因为查询不正确，对 **Used** 和 **Total** 的节点文件系统计算不正确。现在，查询已被更新并正确计算数据。(BZ31874028)

- web 控制台中的 **Overview** 页面错误地包括用于显示网络使用数据的容器级别用量指标。在这个版本中，带有节点级使用数据的不正确的 metric 已被替换，现在可以正确显示网络使用率数据。(BZ#1855556)

- 在以前的版本中，Operator 的 **Created At** 的时间戳并不需要特定格式，从而导致 web 控制台中显示的时间戳不一致。现在，如果 **Created At** 数间缀的值作为 operator 的有效日期输入，时间戳会与控制台中其他时间戳的显示一致。如果没有使用有效日期格式输入该值，则 **Created At** 时间戳会显示为无效的字符串。(BZ#1855378)

- Web 控制台为 OperatorHub 显示一个旧的徽标。在这个版本中，当前徽标替换了旧的徽标。(BZ#1810046)

- 在以前的版本中，Operator 资源字段名称在 web 控制台中显示不一致（camelCase 或 Start Case ）。现在，操作对象表单生成逻辑默认使用 Start Case 来标记表单字段。使用 CSV 或 CRD 对象可以覆盖默认设置。(BZ#1854196)

- 在以前的版本中，如果 **Resource Log** 视图缺少了新行控制字符（**/n**），则资源日志视图不会显示单行日志，也不会显示 pod 日志的最后一行。现在，日志视图已被更新以显示整个 pod 日志内容的单个行日志和日志的最后一行，这些日志行没有使用 newline 字符终止。(BZ#1876853)

- 在以前的版本中，OpenShift Container Platform Web 控制台 YAML 编辑器允许所有资源的 **metadata.namespace** 条目。当为没有命名空间值的资源添加 **namespace: <namespace>** 时，会返回一个错误。现在，如果资源没有命名空间值时，在保存一个配置时**metadata.namespace** 条目会被移除。(BZ#1846894)

- 在以前的版本中，名称值编辑器的删除图标（-）没有提供 tooltip，因此用户不知道此图标的作用。删除图标（-）现在带有一个 tooltip，因此用户可以更方便地了解它的用途。(BZ#1853706)

- 在以前的版本中，带有特殊字符（如 (和)）的资源名称可能会阻止在 OpenShift Container Platform 控制台中显示资源详情。现在，当资源名称带有特殊字符时，资源详情会被正确显示。(BZ#1845624)

监控

- 在以前的版本中，当配置没有被完全生成时，Prometheus 的配置重新加载有时会被触发，这会触发 **PrometheusNotIngestingSamples** 和 **PrometheusNotConnectedToAlertmanagers** 警报，因为没有 scrape 或 alerting 目标。现在，配置重新加载过程会确保磁盘上的配置在重新加载 Prometheus 前有效，且不会触发警报。(BZ#1845561)

- 在以前的版本中，**AlertmanagerConfigInconsistent** 警报会在升级过程中触发，因为有些 Alertmanager pod 因有状态集的滚动更新而暂时没有运行。尽管警报会自行解决，但这可能会给集群管理员造成混乱。**AlertmanagerConfigInconsistent** 不再考虑运行 Alertmanager pod 的数量，因此当某些 Alertmanager Pod 处于非运行、瞬时状态时，它不会在升级过程中触发。(BZ#1846397)

- 在以前的版本中，有些警报没有正确的严重性设置或者不正确，从而导致升级问题。很多警报的严重性级别已从 critical 改为 warning，**KubeStatefulSetUpdateNotRolledOut** 和 **KubeDaemonSetRolloutStuck** 警报已调整， **KubeAPILatencyHigh** 和 **KubeAPIErrorsHigh** 警报已被删除。现在，这些警报是正确的，不会造成升级问题。(BZ#1824988)

- 在以前的版本中，**KubeTooManyPods** 警报使用 **kubelet_running_pod_count**，其中包含完成的 pod，因此 **KubeTooManyPods** 警报不正确。现在，利用 **container_memory_rss** 来查找 **KubeTooManyPods** 警报节点上运行的实际 pod 数量。(BZ#1846805)

- 在以前的版本中，**node_exporter** 守护进程会默认把 **maxUnavailable** 设置为 **1**，因此 rollout 被完全序列化且在大型集群中速度较慢。因为 **node_exporter** 守护进程的设置不会影响工作负载的可用性，所以 **maxUnavailable** 值现在会根据集群的大小进行扩展，从而可以更快地推出部署。(BZ#1867603)

网络

- 在这个版本中，Kuryr-Kubernetes 会尝试检测 Container Network Interface（CNI）级别上的 pod 子端口的桥接接口，而不是使用 **kuryr.conf** 中设置的值。这种方式支持，当 VM 调用在没有使用在 **kuryr.conf** 中设置的值的接口的情况。(BZ#1829517)

- 在以前的版本中，OpenShift SDN 公开了未通过 HTTP 加密的指标。现在，OpenShift SDN 通过 TLS 公开指标数据。(BZ#1809205)

- 在以前的版本中，当闲置服务 OpenShift SDN 时，并不总是以正确顺序删除服务及其端点。因此，有时服务的节点端口没有被删除。当服务再次扩展时，服务无法访问。现在，OpenShift SDN 可确保节点端口始终被正确删除。(BZ#1857743)

- 在以前的版本中，因为缺少了对旧 iptables 二进制文件的依赖，出口路由器 Pod 无法初始化。现在，出口路由器 Pod 可以成功初始化。(BZ#1822945)

- 在以前的版本中，当删除使用 OVN-Kubernetes 网络供应商的集群中的网络策略时，一个竞争条件会阻止在删除关联的命名空间时正确删除网络策略。现在，网络策略对象总是被正确地删除。(BZ#1859682)

- 在以前的版本中，当在多租户隔离模式下使用 OpenShift SDN Pod 网络供应商时，pod 无法访问由 **externalIPs** 设置配置的服务。现在，pod 可以通过配置了服务外部 IP 地址来访问服务。(BZ#1762580)

- 在以前的版本中，OVN-Kubernetes 使用 HTTP 以未加密的形式公开指标。现在，OVN-Kubernetes 会通过 TLS 公开指标数据。(BZ#1822720)

- 在以前的版本中，在 Red Hat OpenStack Platform 上的 OpenShift Container Platform 中，当使用 OVN-Octavia 驱动时，无法将监听程序附加到同一端口的不同协议中。现在，有可能在同一端口上公开多个协议。(BZ#1846396)

节点

- 在以前的版本中，如果没有指定软驱除阈值和宽限期，Kubelet 将无法启动。在这个版本中，在 Kubelet 配置过程中会验证这些值是否存在。(BZ#1805019)

- 因为用户可以在 kubeconfig 对象的 CPU 和内存请求中输入无效字符（如负值、非数字字符等），所以 kubelet 不会启动。代码已被修改，以验证 kubelet 配置内存请求值是否有效。因此，无效的值会被拒绝。(BZ#1745919)

- 在以前的版本中，如果系统在 root 设备中使用设备映射器，则 cadvisor 返回的很多密钥主机级别 IO 指标被错误地设置为零。如果设备映射器用于 root，cadvisor 会被修复来报告这些指标。(BZ#1831908)

oauth-apiserver

- 在以前的版本中，当 Authentication Operator 从忽略 **Accept: application/json** 标头的 OpenID Connect Authentication（OIDC）服务器中接收 HTML 有效负载时，Operator 会记录有关有效负载的错误。现在，Operator 包括了它请求的页面的 URL，用来帮助对 OIDC 服务器响应进行故障排除。(BZ#1861789)

oc

- 在以前的版本中，**oc project** 命令需要 **self-provisioner** 角色的权限来切换项目。这意味着，如果用户没有该角色，则无法切换项目。删除了对 **self-provisioner** 角色的要求，因此任何有权访问项目的用户现在都可以使用 **oc project** 切换项目。(BZ#1849983)

- 在以前的版本中，当对一个带有空的 **lastTimestamp** 的事件进行排序时，根据 **lastTimestamp** 对事件进行排序可能会导致错误。现在，在存在空项时进行排序也可以正常运行，使用 **lastTimestamp** 排序可以正常工作。(BZ#1880283)

- 在以前的版本中，**oc create job** 命令缺少处理 **--save-config** 标志的逻辑，因此 **--save-config** 选项无法正常工作。现在，增加了处理 **--save-logic** 标志的逻辑，它现在可以正常工作。(BZ#1844998)

OLM

- Operator Lifecycle Manager（OLM）在 subscription CRD 中公开 **subscription.spec.config.nodeSelector** 字段，但之前没有将 **nodeSelectors** 标签应用到 **ClusterServiceVersion** 对象（CSV）中定义的部署。这会导致用户无法在其 CSV 部署上设置 **nodeSelectors**。在这个版本中更新了 OLM，以传播 **subscription.spec.config.nodeSelector** 字段中定义的 **nodeSelector** 标签，以在 CSV 中部署。因此，字段现在可以正常工作。(BZ#1860035)

- 在以前的版本中，当安装多次进入 **安装** 阶段的 **ClusterServiceVersion** 对象（CSV）时，Operator Lifecycle Manager（OLM）不会重复使用现有的有效 CA 证书。OLM 将新的 webhook 哈希应用到部署，从而导致创建新的副本集。然后，运行的 Operator 会重新部署，可能在安装过程中多次运行。在这个版本中更新了 OLM，以检查 CA 是否已存在，并在有效时重复使用它。因此，如果 OLM 检测到现有的有效 CA，OLM 现在会重复使用该 CA。(BZ#1868712)

- Operator Lifecycle Manager（OLM）将 **OwnerReferences** 元数据附加到为提供 API 服务的

Operator 安装的资源。在以前的版本中，当 OLM 重新部署此类的 Operator 时（例如在证书轮转过程中），会将一个重复的 **OwnerReference** 附加到相关服务中，从而导致 **OwnerReferences** 数量增加未绑定。在这个版本中，在添加 **OwnerReferences** 时，如果没有找到，OLM 会更新现有的 **OwnerReference**。因此，OLM 附加到服务中的 **OwnerReferences** 数被绑定。(BZ#1842399)

- 在以前的版本中，Operator Lifecycle Manager（OLM）在试图解包它们前不会拉取捆绑包镜像，从而导致 **opm alpha bundle validate** 命令失败，并显示 **image not found** 或类似的错误。在这个版本中更新了 OLM 来拉取捆绑包镜像，然后再尝试在捆绑验证器中解包。因此，**opm alpha bundle validate** 命令在执行验证前可以成功拉取和解包镜像。(BZ#1857502)

- 在以前的版本中，web 控制台会返回软件包中声明的第一个频道中的图标，从而在 OperatorHub 中显示 Operator 图标。这有时会导致显示的图标与在软件包中发布的最新图标不同。这可以通过从默认频道中选择图标来确定最新的图标被显示。(BZ#1843652)

- 在以前的版本中，当使用 **podman** 或 **docker** 工具选项时，whiteout 文件会出现在未打包的内容中。在这个版本中，在使用 **podman** 和 **docker** 工具选项解包后，将不会再有 whiteout 文件。(BZ#1841178)

openshift-controller-manager

- 在以前的版本中，在 API 服务器有时无法使用的情况下，可能会导致 OpenShift Controller Manager Operator 在获取部署时出现问题。检索部署失败有时会导致 Operator 出现问题。在这个版本中，添加了相应的检查来处理和报告这个错误条件，并重试操作。Operator 现在可以正确地处理从 API 服务器获取部署的操作。(BZ#1852964)

RHCOS

- 在以前的版本中，在没有 DHCP 的网络上带有大量 NIC 的机器需要很长时间才能引导。这是因为 initramfs 使用旧的网络脚本试图逐个在机器的每个接口上启用 DHCP。现在，initramfs 使用 NetworkManager 而不是旧脚本。NetworkManager 不会在任何没有物理连接的接口上尝试 DHCP。NetworkManager 还尝试并行接口 DHCP，而不是逐个进行。这些更改减少了 DHCP 超时等待的时间。(BZ#1836248)

- 在以前的版本中，在安装过程中无法修改内核参数。现在，可以使用 **coreos-installer** 命令在安装的系统中修改内核参数。例如，您可以将安装的系统配置为使用不同的串口控制台参数：

```
$ coreos-installer install ... \
 --delete-karg console=ttyS0,115200n8 \
 --append-karg console=ttyS1,115200n8
```

(BZ#1712511)

- 当 MCO 用于部署 worker 节点时，加载文件会失败，因为用户配置 Ignition 配置中的 iSCSI initiator 名称自动替换为动态生成的名称。现在，只有在 Ignition 配置中没有指定名称时，才会动态生成 iSCSI initiator 名称。(BZ#1868174)

- 置备过程中对 Azure VM 的手动更改会更改停滞号，从而导致 afterburn 读取状态报告失败，因为停滞号不匹配。Afterburn 现在获取一个全新的 incarnation 号码（在提交就绪状态前）。(BZ#1853068)

- 在控制台中无法看到某些接口，如绑定接口。NetworkManager 分配脚本代替之前使用的 Udev 规则。在这个版本中，启用了具有永久硬件地址或者由带永久硬件地址的设备支持的网络接口可以在控制台中显示。(BZ#1866048)

路由

- 在以前的版本中，HAProxy 路由器 503 页与一些 Web 应用程序防火墙使用的标准不相符。503 页已被更新来解决这个问题。(BZ#1852728)

- 当 Ingress Operator 在协调为 **NodePortService** 端点发布策略类型配置的 **IngressController** 对象时，Operator 会从 API 获取 ingresscontroller 的 **NodePort** 服务，以确定 Operator 需要创建或更新服务。如果服务不存在，Operator 会创建它，其 **spec.sessionAffinity** 字段带有一个空值。如果服务存在，Operator 会将其与 Ingress Operator 的预期进行比较，以确定是否需要更新该服务。在此比较中，如果 API 为服务 **spec.sessionAffinity** 字段设置了默认值 **None**，Operator 会检测到更新，并尝试将 **spec.sessionAffinity** 字段设置为空。因此，Ingress Operator 会重复尝试更新 **NodePort** 服务。Ingress Operator 已进行了修改，在比较 **NodePort** 服务时认为未指定值和默认值是相等的。Operator 不再更新 IngressController **NodePort** 服务以响应 API 的默认设置。(BZ#1842742)

- 在以前的版本中，如果您使用不正确的路由更新集群，HAProxy 将初始化为失效状态。但是，更新不会触发任何警报，集群会错误地报告 Ingress Controller 可用。HAProxy 初始同步逻辑已修正，带有有故障路由的升级会失败。因此，无法成功升级带有不正确路由的集群，并发出 **HAProxyReloadFail** 或 **HAProxyDown** 警报。(BZ#1861455)

- 由于使用 HTTP/2 ALPN 时连接有重复使用的风险，所以在 CLI 中的 Ingress Controller 的输出中添加了警告消息，用于仅在使用自定义（非通配符）证书的路由上启用 HTTP/2 ALPN。因此，没有其自身自定义证书的路由在前端或后端上都不会是启用了 HTTP/2 ALPN 的路由。(BZ#1827364)

- 在以前的版本中，当重新载入 HAProxy 时，HAProxy Prometheus counter 指标会降低，这明确违反了计数器指标的定义。相关的路由器代码已修复，以记录最后一次指标提取的时间。这会在重新加载时防止提取超过保留的计数值。因此,计数指标不会在路由器重新加载时显示突然增长，然后会降低。(BZ#1752814)

Samples

- 在以前的版本中，Samples Operator 的警报规则会错误地解析 **registry.redhat.io** 主机名。该规则现在在警报信息中使用正确的主机名。(BZ#1863014)

- 在以前的版本中，当升级 OpenShift Container Platform 时，如果 API 服务器间不可用，Samples Operator 可能会阻止升级。现在，Operator 会适当处理网络连接不稳定的问题，它不再会阻止升级。(BZ#1854857)

存储

- Local Storage Operator 日志记录的错误消息内容不具体，因此对调试没有太大帮助。现在，当创建 **LocalVolume** 对象且指定设备未找到或无效时，会提供额外的详细信息。(BZ#1840127)

- 当 v1alpha1 CRD 为 **Upgradable=False** 时，Storage Operator 将停止协调。因此，当集群中检测到这些 CRD 时，Cluster Storage Operator 无法执行 z-stream 升级。这个版本修改了协调循环的顺序。现在，z-stream 升级可以成功完成，v1alpha1 CRD 会被检测到且没有错误。(BZ#1873299)

- NFS 驱动程序 Pod 重启后无法卸载 Manila 卷，因为重启过程为 pod 分配了新的 IP 地址。现在，pod 使用主机网络和主机 IP 地址来挂载和卸载卷，即使在重启驱动程序 Pod 后也是如此。(BZ#1867152)

- 在这个版本中，在更改一个较小卷的 fsGroup 时，减少了不重要的日志数据。(BZ#1877001)

- 在罕见的情况下，因为负载过重，在 vSphere 云供应商中会导致持久性卷置备失败。现在，这个问题已被修复，vSphere 卷的置备非常可靠。(BZ#1806034)

- 当集群手动安装了 v1alpha1 **VolumeSnapshot** CRD 或独立 CSI 驱动程序时，从 OCP 4.3.z 升级

到 4.4.0 时会失败。OpenShift Container Platform 4.4 引入了 v1beta1 **VolumeSnapshot** CRD，它们与 v1alpha1 **VolumeSnapshot** CRD 不兼容。现在，Cluster Storage Operator 会检查 v1alpha1 **VolumeSnapshot** CRD 是否存在。如果存在，会显示一条消息表示必须删除 v1alpha1 **VolumeSnapshot** CRD 才能进行升级。(BZ#1835869)

- 当修改 **VolumeSnapshotContent** 对象删除策略时，**VolumeSnapshot** 资源实例无法被删除，因为没有更新与这些实例关联的结束程序。在这个版本中，在 **VolumeSnapshotContent** 对象删除策略被修改时会删除终结程序，并允许在相关资源对象被删除后删除 **VolumeSnapshot** 资源实例。(BZ#1842964)

- 在以前的版本中，默认的 OpenShift RBAC 规则不允许常规用户访问或创建 **VolumeSnapshot** 和 **VolumeSnapshotClass** 资源实例。现在，默认的 OpenShift RBAC 规则允许基本用户读/写 **VolumeSnapshot** 资源并读取 **VolumeSnapshotClass** 资源。另外，storage-admins 可以在默认情况下读/写 **VolumeSnapshotContent** 对象。(BZ#1842408)

- 在以前的版本中，没有相关的验证来防止 Local Storage Operator 创建一个设备到多个 PV。在这个版本中，添加了对这种情况的验证。现在，在已由 Local Storage Operator 置备的块设备上尝试创建 PV 将失败。(BZ#1744385)

Insights Operator

- 在以前的版本中，Insights Operator 可以在单个报告中为无限数量的证书签名请求（CSR）收集数据。这会导致对有很多 CSR 的集群进行过度数据收集。Insights Operator 现在在单个报告中收集最多 5000 CSR 的数据。(BZ#1881044)

1.6. 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 4.4	OCP 4.5	OCP 4.6
精度时间协议 (PTP)	TP	TP	TP
oc CLI Plug-ins	TP	TP	TP
experimental-qos-reserved	TP	TP	TP
Pod Unidler	TP	GA	GA
为临时存储设置 Limit/Requests	TP	TP	TP

功能	OCP 4.4	OCP 4.5	OCP 4.6
Descheduler	TP	TP	TP
Podman	TP	TP	TP
PID 命名空间的共享控制	TP	GA	GA
OVN-Kubernetes 集群网络供应商	TP	TP	GA
基于 Prometheus 的 HPA 定制 metrics adapter	TP	TP	TP
HPA 用于内存使用	TP	TP	TP
三节点裸机部署	TP	GA	GA
服务绑定	TP	TP	TP
日志转发	TP	TP	GA
用户定义项目的监控	TP	TP	GA
Compute Node Topology Manager	TP	GA	GA
使用 Cinder 的原始块	TP	TP	TP
CSI 卷快照	TP	TP	TP
CSI 卷克隆	TP	TP	GA
CSI 卷扩展	TP	TP	TP
CSI AWS EBS Driver Operator	-	TP	TP
OpenStack Manila CSI Driver Operator	-	GA	GA
Red Hat Virtualization（oVirt）CSI Driver Operator	-	-	GA
CSI inline 临时卷	-	TP	TP
使用 Local Storage Operator 进行自动设备发现和置备	-	-	TP
OpenShift Pipelines	TP	TP	TP
Vertical Pod Autoscaler	-	TP	TP
Operator API	-	TP	GA

功能	OCP 4.4	OCP 4.5	OCP 4.6
在节点中添加内核模块	TP	TP	TP
Docker Registry v1 API			DEP
CPU Manager	TP	TP	GA

1.7. 已知问题

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

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

  您可以使用 VMware KBase 文章中的步骤解决这个问题。如需更多信息，请参阅红帽知识库解决方案 [UPI vSphere] 节点扩展功能无法按预期工作。（BZ#1918383）

- 在 OpenShift Container Platform 4.6.8 中，引入了一个程序错误修正，它更改了 Cluster Logging Operator（CLO）重新生成证书的方式。这个程序修正会导致一个问题，CLO 可能会在 OpenShift Elasticsearch Operator（EO）试图重启集群时重新生成证书。这会导致 EO 和集群间的通信问题，从而导致 EO 节点有不匹配的证书。
  不匹配的证书在升级 Elasticsearch 时可能会导致问题。作为临时解决方案，您可以选择性地单独升级 CLO 和 EO。如果无法正常工作，请运行以下命令重启 Elasticsearch Pod：

  ```
  $ oc delete pod -l component=es
  ```

  pod 重启后，不匹配的证书会被修复，从而解决了升级问题。(BZ#1906641)

- 目前，使用 OVN-Kubernetes 集群网络供应商从 OpenShift Container Platform 4.5 升级到 4.6 将无法正常工作。这将在以后的 4.6.z 版本中解决。(BZ#1880591)

- 目前，当将集群扩展到集群中的 75 个节点时，OVN-Kubernetes 集群网络供应商数据库可能会崩溃，使集群处于不可用状态。(BZ#1887585)

- 目前，在带有 OVN-Kubernetes 集群联网供应商的集群中扩展 Red Hat Enterprise Linux（RHEL）worker 节点将无法正常工作。这个问题将在以后的 RHEL 7.8.z 和 RHEL 7.9.z 发行版本中解决。(BZ#1884323, BZ#1871935)

- 目前，在扩展 Red Hat Enterprise Linux（RHEL）7.8 上运行的 worker 节点时，OVN-Kubernetes 集群联网供应商无法在新节点上初始化。(BZ#1884323)

- 以后的 4.5.z 版本中会修复从 OpenShift Container Platform 4.6 降级到 4.5 的问题。(BZ#1882394, BZ#1886148, BZ#1886127)

- 目前，使用 Red Hat Enterprise Linux（RHEL）的 worker 节点无法从 OpenShift Container Platform 4.5 升级到 4.6。这将在以后的 4.6.z 版本中解决。首先，升级 RHEL，然后升级集群，然后再次运行正常的 RHEL 升级 playbook。(BZ#1887607)

- 当在绑定设备中配置了外部网络时，OpenShift Container Platform 4.5 升级到 4.6 时会失败。**ovs-configuration** 服务失败，节点将无法访问。这将在以后的 4.6.z 版本中解决。(BZ#1887545)

- 目前，当在多个 Non-Uniform Memory Access（NUMA）节点中请求巨页时，巨页无法被正确检测到。这是因为当集群包含多个 NUMA 节点时，cnf-tests 套件报告错误是由于测试将一个 NUMA 上的巨页数与整个节点上的巨页数进行比较。(BZ#1889633)

- 用于检查数据包转发和接收一直失败的 Data Plane Development Kit（DPDK）测试。(BZ#1889631)

- 当至少有一台没有原始配置的机器配置时，流控制传输协议（Stream Control Transmission Protocol，SCTP）验证阶段会失败。例如，这会包括只包含内核参数的机器配置。(BZ#1889275)

- 因为 cnf-tests 套件没有正确地检测运行 PTP 的节点数量，所以 PTP 验证阶段失败。(BZ#1889741)

- 网络接口卡（NIC）验证阶段失败，因为它没有等待节点上的设备可用。pod 在节点上启动运行的等待时间太短，因此 pod 仍可能处于 **Pending** 状态，测试不正确。(BZ#1890088)

- **ose-egress-dns-proxy** 镜像有一个已知缺陷，导致容器无法启动。这个镜像在以前的版本中也无法正常工作，因此在4.6 中不被视为回归。(BZ#1888024)

- 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 4.6 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)

- 在没有使用 **--helm-chart 标志的情况下运行 operator-sdk new 或 operator- sdk create api** 命令会构建基于 Helm 的 Operator，并使用默认的 boilerplate Nginx chart。虽然本示例 chart 在上游 Kubernetes 上可以正常工作，但它无法在 OpenShift Container Platform 上成功部署。
要临时解决这个问题，使用 **--helm-chart** 标志来提供一个在 OpenShift Container Platform 上成功部署的 Helm chart。例如：

```
$ operator-sdk new <operator_name> --type=helm \
  --helm-chart=<repo>/<name>
```

(BZ#1874754)

- 在使用 Redfish Virtual Media 功能的裸机节点上安装 OpenShift Container Platform 时，当 Baseboard Management Controller（BMC）尝试从置备网络加载虚拟介质镜像时，会出现一个故障。如果 BMC 没有使用置备网络，或者其网络没有将路由设置为置备网络，则会出现这种情况。作为临时解决方案，在使用虚拟介质时，必须关闭置备网络，或者将 BMC 路由到置备网络作为一个先决条件。(BZ#1872787)

- 由于一个已知问题，OpenShift Container Platform 安装程序不支持使用 GCP 和 Azure 上的 **install-config.yaml** 文件来手动模式配置。反之，您必须在集群安装过程的 manifest 生成阶段手动将配置映射插入到清单目录中，如手动为 Azure 创建 IAM 和 手动为 GCP 创建 IAM 所述。(BZ#1884691)

- 在电源环境中，当使用 FC 持久性卷声明和 targetWWN 创建 pod 时，FC 卷附加会失败（错误信息为 **no fc disk found**），pod 会保持在 **ContainerCreating** 状态。(BZ#1887026)

- 当提供出口 IP 的节点关闭时，在该节点上托管的 pod 不会移到提供出口 IP 的另一个节点中。这会导致在提供出口 IP 的节点关闭时，pod 的出站流量始终失败。(BZ#1877273)

- 因为一个已知问题，在 **us-gov-east-1** 区域上安装 AWS GovCloud 时不支持使用断开连接的集群安装。(BZ#1881262).

- 当使用安装程序置备的基础架构在 Google Cloud Platform（GCP）上运行的集群被破坏时，没有使用基础架构 ID 前缀的机器所使用的防火墙规则会被保留。这会导致安装程序的销毁过程失败。作为临时解决方案，您必须在 GCP web 控制台中手动删除机器的防火墙规则：

```
$ gcloud compute firewall-rules delete <firewall_rule_name>
```

删除缺少基础架构 ID 的机器的防火墙规则后，就可以销毁集群。(BZ#1801968)

- **opm alpha bundle build** 命令在 Windows 10 上会失败。(BZ#1883773)

- 在 OpenShift Container Platform 4.6 中，资源 metrics API 服务器支持自定义指标。资源 metrics API 服务器没有实现 OpenAPI 规格，以下消息会记录在 **kube-apiserver** 日志中：

```
controller.go:114] loading OpenAPI spec for "v1beta1.metrics.k8s.io" failed with: OpenAPI
spec does not exist
controller.go:127] OpenAPI AggregationController: action for item v1beta1.metrics.k8s.io:
Rate Limited Requeue.
```

在某些情况下，这些错误可能会导致 **KubeAPIErrorsHigh** 警报触发，但底层的问题未知导致降级 OpenShift Container Platform 的功能。(BZ#1819053)

- 如果在 Rules API 存储前发现存储 API 存储，则有时不会检测到 Rules API 后端。当这种情况发生时，在没有 Rules API 客户端的情况下创建存储引用，来自 Thanos Querier 的 Rules API 端点也不会返回任何规则。(BZ#1870287)

- 如果 AWS 帐户被配置为使用 AWS 机构服务控制策略（SCP），使用全局条件拒绝所有操作或需要特定权限，则验证权限的 AWS 策略模拟器 API 将会产生一个假的负数。当无法验证权限时，OpenShift Container Platform AWS 安装会失败，即使提供的凭证具有安装所需的权限。要临时解决这个问题，您可以通过在 **install-config.yaml** 配置文件中设置 **credentialsMode** 参数的值来绕过 AWS 策略模拟器权限检查。**credentialsMode** 的值将 Cloud Credential Operator（CCO）的行为改为三种支持的模式之一。

  示例 install-config.yaml 配置文件

```
apiVersion: v1
baseDomain: cluster1.example.com
credentialsMode: Mint (1)
compute:
- architecture: amd64
  hyperthreading: Enabled
...
```

  (1) 这一行被添加来将 **credentialsMode** 参数设置为 **Mint**。

  在绕过此检查时，请确保您提供的凭证具有指定模式所需的权限。

  (BZ#1829101)

- 在 RHOSP 上运行并使用 Kuryr 的集群为每个 **hostNetworking pod** 创建不必要的 Neutron 端口。您可以安全地删除这些端口。计划在以后的 OpenShift Container Platform 版本中自动删除端口。(BZ#1888318)

- 在配置了 Kuryr 的 RHOSP 上部署可能会出现 kuryr-cni pod 进入崩溃循环的情况，它会报告 **NetlinkError:(17, 'File exists')** 错误消息。作为临时解决方案，您必须重新引导节点。计划在以后的 OpenShift Container Platform 版本中解决这个问题。(BZ#1869606)

- 当以 DNS 代理模式部署出口路由器 Pod 时，pod 无法初始化。(BZ#1888024)

- 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 4.6 中的 RT 内核不支持紧凑集群。(BZ#1887007)

- 要提高安全性，**NET_RAW** 和 **SYS_CHROOT** 功能在默认 CRI-O 功能列表中不再可用。

  - **NET_RAW**：如果没有保护，此功能可让 Pod 生成可以更改标头字段（如低端口、源 IP 地址和源 MAC 地址）的数据包。这个功能可能会被恶意攻击者利用。

  - **SYS_CHROOT**：一般工作负载不需要 **chroot**。只有在需要时才应允许对特权操作的访问。

在 OpenShift Container Platform 4.5.16 中，**NET_RAW** 和 **SYS_CHROOT** 已从默认能力中删除。为了减少对版本 4.5.16 之前创建的集群的影响，现在将默认的功能列表包含在不同的机器配置中： **99-worker-generated-crio-capabilities** 和 **99-master-generated-crio-capabilities**。OpenShift Container Platform 在从上一发行版本更新时创建新的机器配置。

升级后，建议禁用 **NET_RAW** 和 **SYS_CHROOT** 功能，然后测试您的工作负载。当准备删除这些功能时，删除 **99-worker-generated-crio-capabilities** 和 **99-master-generated-crio-capabilities** 机器配置。

重要: 如果您要从较早的版本更新，在升级到 4.6 前将其更新至 4.5.16。(BZ#1874671).

- OpenShift Container Platform Machine API 裸机操作器目前正在删除底层裸机主机时删除 Machine 对象。此行为与其他云供应商代理器不匹配，后者将 **Machine** 对象移到失败的阶段，而不会在删除底层云供应商资源时完全删除它。(BZ#1868104)

- 当将集群从 vSphere 上安装的安装程序置备基础架构的版本 4.5 升级到 4.6 时，如果 control plane 节点 IP 地址在升级过程中发生改变，升级会失败。作为临时解决方案，您必须保留 control plane 节点 IP 地址，然后才能升级到 4.6。查看您的 DHCP 服务器文档以配置保留。(BZ#1883521)

- 对于需要 TLS 验证的 **oc** 命令，如果证书未设置 Subject Alternative Name，验证不会回退到 Common Name 字段，命令会失败并显示以下错误：

  ```
  x509: certificate relies on legacy Common Name field, use SANs or temporarily enable Common Name matching with GODEBUG=x509ignoreCN=0
  ```

  作为临时解决方案，您可以使用带有正确 Subject Alternative Name 的证书，或者在使用 **GODEBUG=x509ignoreCN=0** 的 **oc** 命令前暂时覆盖此行为。

  将来的 4.6 z-stream 可能会返回警告而不是错误，以便用户有足够的时间更新其证书。

  (BZ#1889204)

- 使用 Helm 软件包管理器安装 Agones 并尝试使用 **Developer** 视角检查命名空间中的 chart 资源时，您会看到出错信息而不是资源详情。(BZ#1866087)

- 当您在 **Topology** 视图 中选择一个部署时，请点 **Actions → Edit <deployment_name>**，然后修改它; 修改的 **Deployment** YAML 文件覆盖或移除 **Pod Template spec** 中的卷挂载。(BZ#1867965)

- 当使用 **Add → From Catalog** 选项、根据 **Template** 过滤、选择模板并实例化模板时, **Developer** 视角中不会显示成功或失败消息。(BZ#1876535)

- 带有跳过的任务的 PipelineRuns 会错误地将任务显示为 **Failed**。(BZ#1880389)

- 在 **Application Stages** 视图的 **Application Details** 页面提供了一个不准确到应用程序环境中的项目的链接。(BZ#1889348)

- 在创建大量 pod 的情况下，创建会失败并显示 **error reserved pod name ...: name is reserved** 错误信息。CNI 可执行文件的 CRI-O 上下文会终止，它会终止进程。Pod 创建最终会成功，但它需要很多时间。因此，kubelet 认为 CRI-O 没有创建 pod。kubelet 会再次发送请求，并导致名称冲突。这个问题目前正在调查中。(BZ#1785399)

- 如果集群网络供应商是 OVN-Kubernetes，在使用没有分配给集群中任何节点的服务外部 IP 地址时，则到外部 IP 地址的网络流量将无法被路由。作为临时解决方案，请确保始终为集群中的节点分配一个服务外部 IP 地址。(BZ#1890270)

- 管理员可以镜像 **redhat-operators** 目录，在受限网络环境中（也称为断开连接的集群）在 OpenShift Container Platform 4.6 集群中使用 Operator Lifecycle Manager（OLM）。但是，以下 Operator 会返回在 **mapping.txt** 文件中带有私有主机名 **registry-proxy.engineering.redhat.com** 而不是预期的公共主机名 **registry.redhat.io** 的项：

  - amq-online.1.5.3
  - amq-online.1.6.0

  这会导致，在从不可访问的私有容器镜像仓库（registry）中拉取镜像失败。这些私有容器镜像仓库通常用于红帽内部的测试。要临时解决这个问题，在生成 **mapping.txt** 文件后运行以下命令：

  ```
  $ sed -i -e 's/registry-proxy.engineering.redhat.com/registry.redhat.io/g' \
     -e 's/rh-osbs\/amq7-/amq7\//g' \
     -e 's/amq7\/tech-preview-/amq7-tech-preview\//g' \
     ./redhat-operator-index-manifests/imageContentSourcePolicy.yaml \
     ./redhat-operator-index-manifests/mapping.txt
  ```

  对于 PowerVM 上的 IBM Power Systems 上的 OpenShift Container Platform，首选以下要求：

  - 2 个 master 节点的虚拟 CPU
  - 4 个用于 worker 节点的虚拟 CPU
  - 0.5 处理器，适用于所有节点
  - 32 GB 虚拟 RAM，适用于所有节点

- Red Hat Operator 发布过程中存在一个错误，这会导致简单地发布 OpenShift Container Platform 4.6 索引镜像的阶段环境版本。这个程序错误已被解决，镜像很快使用正确的内容重新复制。
  如果您在使用此阶段 registry 镜像时尝试安装或升级 Operator，**openshift-marketplace** 命名空间中的作业可能会失败，并显示以下错误信息，其中显示私有主机名 **registry.stage.redhat.io** 而不是预期的公共主机名 **registry.redhat.io**：

  输出示例

  ```
  ImagePullBackOff for
  Back-off pulling image "registry.stage.redhat.io/openshift4/ose-elasticsearch-operator-bundle@sha256:6d2587129c746ec28d384540322b40b05833e7e00b25cca584e004af9a1d292e"
  ```

  输出示例

  ```
  rpc error: code = Unknown desc = error pinging docker registry registry.stage.redhat.io: Get "https://registry.stage.redhat.io/v2/": dial tcp: lookup registry.stage.redhat.io on 10.0.0.1:53: no such host
  ```

  这会导致，针对不可访问的私有 registry（通常用于红帽内部测试）的镜像拉取失败，相关的 Operator 安装和升级永远不会成功。如需临时解决方案，请参阅刷新失败的订阅来清理此问题。(BZ#1909152)

- **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)

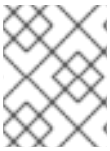
- OVN-Kubernetes 网络供应商不支持 **NodePort**- 和 **LoadBalancer**-type 服务的 **externalTrafficPolicy** 功能。**service.spec.externalTrafficPolicy** 字段决定服务的流量是路由到节点本地范围或集群范围的端点。目前，此类流量默认路由到集群范围的端点，因此无法限制到节点本地端点的流量。这将在以后的发行版本中解决。(**BZ#1903408**)

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

1.8. 异步勘误更新

OpenShift Container Platform 4.6 的安全更新、程序错误修正、功能增强更新将会通过红帽网络以异步勘误的形式发布。所有的 OpenShift Container Platform 4.6 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 4.6 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.6.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。

1.8.1. RHBA-2020:4196 - OpenShift Container Platform 4.6 镜像和程序错误公告

发布日期：2020 年 10 月 27 日

OpenShift Container Platform release 4.6 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2020:4196 公告中。此更新包括的 RPM 软件包由 RHBA-2020:4197 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.1 --pullspecs
```

1.8.2. RHSA-2020:4297 - Moderate: OpenShift Container Platform 4.6 软件包安全更新

发布日期：2020 年 10 月 27 日

OpenShift Container Platform 4.6 现在提供了对 **jenkins-2-plugins**、**openshift-clients**、**podman**、**runc** 和 **skopeo** 的更新。有关更新的详情，请查看 RHSA-2020:4297 公告。

1.8.3. RHSA-2020:4298 - Moderate: OpenShift Container Platform 4.6 镜像安全更新

发布日期：2020 年 10 月 27 日

OpenShift Container Platform 4.6 现在提供了对多个镜像的更新。有关更新的详情，请查看 RHSA-2020:4298 公告。

1.8.4. RHBA-2020:4339 - OpenShift Container Platform 4.6.3 程序错误修复更新

发布日期：2020 年 11 月 9 日

OpenShift Container Platform release 4.6.3 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2020:4339 公告中。此更新包括的 RPM 软件包由 RHBA-2020:4340 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.3 --pullspecs
```

1.8.4.1. 程序错误修复

- 由于一个已知问题，OpenShift Container Platform 4.6.1 的新安装中没有 GPU Operator 和 Node Feature Discovery（NFD）Operator。您需要安装 OpenShift Container Platform 4.5 并将集群升级到 4.6.1 版以使用 GPU 和 NFD Operator。这个问题已被解决，GPU 和 NFD Operator 现在可在 OpenShift Container Platform 4.6.3 及之后的版本中找到。(**BZ#1890673**)

1.8.4.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.5. RHBA-2020:4987 - OpenShift Container Platform 4.6.4 程序错误修复更新

发布日期：2020 年 11 月 16 日

OpenShift Container Platform release 4.6.4 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2020:4987 公告中。这个版本没有 RPM 软件包。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.4 --pullspecs
```

1.8.5.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.6. RHBA-2020:5115 - OpenShift Container Platform 4.6.6 程序错误修复更新

发布日期：2020 年 11 月 30 日

OpenShift Container Platform release 4.6.6 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2020:5115 公告中。此更新包括的 RPM 软件包由 RHBA-2020:5116 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.6 --pullspecs
```

1.8.6.1. 程序错误修复

- 在 OpenShift Container Platform 4.6 之前，当 Marketplace Operator 使用 **OperatorSource** 自定义资源定义(CRD)时，使用受限网络（也称为断开连接的集群）上的集群管理员可能会禁用 **openshift-marketplace** 命名空间中的默认 **OperatorSource** 对象，并使用与默认源相同的名称创建自定义 **CatalogSource** 对象。在 OpenShift Container Platform 4.6 中，Marketplace Operator 直接使用 **CatalogSource** 对象，现在 **OperatorSource** CRD 已被删除。因此，**openshift-marketplace** 具有由 OperatorHub API 管理的默认目录源。
  在断开连接的 OpenShift Container Platform 4.6 集群上禁用了默认目录源后，当管理员尝试创建与默认源名称相同的目录源时，OperatorHub API 以前会删除自定义目录源。如果没有使用 OperatorHub API 禁用目录源，并且更改了默认的目录源（例如：更改 **spec.image** 参数以指向断开连接的环境的内部 registry），则 spec 会恢复到默认 spec。

  在这个版本中，如果使用 OperatorHub API 进行禁用，集群管理员可以使用与默认源相同的名称创建、更新和删除自定义目录源。现在，管理员可以禁用默认目录源并使用默认名称创建自定义目录源而无需删除或覆盖它们。如果重新启用了默认目录源，则恢复默认的 spec。
  (BZ#1895952)

1.8.6.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.7. RHSA-2020:5159 - Low: OpenShift Container Platform 4.6 软件包安全更新

发布日期：2020 年 11 月 30 日

OpenShift Container Platform 4.6 现在提供了对 **golang** 的更新。有关更新的详情请查看 RHSA-2020:5159 公告。

1.8.8. RHSA-2020:5259 - OpenShift Container Platform 4.6.8 程序错误修复和安全更新

发布日期：2020 年 12 月 14 日

OpenShift Container Platform release 4.6.8 现已正式发布。此更新包括的程序错误修正信息包括在 RHSA-2020:5259 公告中。此更新中包括的 RPM 软件包由 RHSA-2020:5260 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.8 --pullspecs
```

1.8.8.1. 功能

1.8.8.1.1. 提供了新的 Red Hat Enterprise Linux CoreOS（RHCOS）引导镜像

新的 RHCOS 引导镜像现在作为 OpenShift Container Platform 4.6.8 发行版本的一部分提供。更新的 RHCOS 引导镜像改进了集群引导体验。(BZ#1899176)

1.8.8.1.2. EUS 4.6 升级频道现在可用

eus-4.6 升级频道现在可用。这个频道提供延长更新支持（EUS）。具有 Premium 订阅的用户，可以使用 EUS 版本将维护阶段扩展到 14 个月。OpenShift Container Platform。如需更多信息，请参阅 OpenShift Container Platform 升级频道和发行版本。

1.8.8.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.9. RHSA-2020:5614 - OpenShift Container Platform 4.6.9 程序错误修复和安全更新

发布日期：2020 年 12 月 21 日

OpenShift Container Platform release 4.6.9 现已正式发布，其中包括 **openshift-clients**、**openvswitch2.13** 和 **python-sushy** 的安全更新。此更新包括的程序错误修正信息包括在 RHSA-2020:5614 公告中。此更新中包括的 RPM 软件包由 RHSA-2020:5615 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.9 --pullspecs
```

1.8.9.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.10. RHSA-2021:0037 - OpenShift Container Platform 4.6.12 程序错误修复和安全更新

发布日期：2021 年 1 月 18 日

OpenShift Container Platform release 4.6.12 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHSA-2021:0037 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:0038 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.12 --pullspecs
```

1.8.10.1. 程序错误修复

- OpenShift Container Platform 4.6.9 中引入了一些性能修复，这使得具有网络策略的集群在升级后遇到网络连接问题，即使在没有网络策略的命名空间中也是如此。这些与性能相关的修复已被恢复，以便具有网络策略的集群可以正常工作。（BZ#1915007）

- 在以前的版本中，Red Hat OpenStack Platform（RHOSP）上的 OpenShift Container Platform 预演示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#1889416)

- 在以前的版本中，**ephemeral-storage** 资源计算没有功能门，因此即使禁用了这个功能，也会导致它可用。这会导致 pod 无法调度。**ephemeral-storage** 资源现已改为使用功能门，在禁用时删除这个功能。（BZ#1913263）

- **terser** 依赖项中存在一个错误，会导致 YAML Editor 组件的持久卸载和重新挂载。这会导致 web 控制台中的 YAML 编辑器每几秒钟跳到 YAML 文件的顶部。这个问题已通过删除默认参数值导致问题暂时解决，现在 YAML 编辑器可以按预期工作。（BZ#1910066）

- 在以前的版本中，在守护进程集就绪前，集群有时会收集 must-gather 日志，从而导致创建了空文件。这个问题已通过在收集 must-gather 日志前确认守护进程集已经就绪，以确保所有生成的文件都包含真实内容。(BZ#1852619)

1.8.10.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.11. RHSA-2021:0171 - OpenShift Container Platform 4.6.13 程序错误修复和安全更新

发布日期：2021 年 1 月 25 日

OpenShift Container Platform release 4.6.13 现已正式发布，其中包括安全更新。此更新中包括的程序错误修正信息包括在 RHSA-2021:0171 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:0172 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.13 --pullspecs
```

1.8.11.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.12. RHBA-2021:0235 - OpenShift Container Platform 4.6.15 程序错误修复更新

发布日期：2021 年 2 月 1 日

OpenShift Container Platform release 4.6.15 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:0235 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0237 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.15 --pullspecs
```

1.8.12.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.13. RHSA-2021:0308 - OpenShift Container Platform 4.6.16 程序错误修复和安全更新

发布日期：2021 年 2 月 8 日

OpenShift Container Platform release 4.6.16（包括安全更新）现已正式发布。此更新包括的程序错误修正信息包括在 RHSA-2021:0308 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0309 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.16 --pullspecs
```

1.8.13.1. 功能

1.8.13.1.1. Insights Operator 的改进

Insights Operator 现在收集以下额外信息：

- **MachineConfigPool** 对象的配置文件
- 安装计划数
- 通用 control plane 的配置文件
- 在集群中运行红帽镜像的集合
- 有关 **openshift*** 命名空间中的 crashlooping pod 的信息

这个信息对故障排除非常有用。如需更多信息,请参阅 BZ# 1887759、BZ# 1889676、BZ# 1905031 和 BZ#1913645。

1.8.13.2. 程序错误修复

- 在以前的版本中，在 Windows 二进制文件的构建过程中不会生成版本信息元数据。这个版本在构建过程中生成 Windows 版本信息，红帽的 **golang** 编译器提供了 Windows 二进制文件的版本信息。（BZ#1891892）
- 在裸机上安装程序置备安装过程中嵌入的 Ironic API 服务现在使用四个 worker 节点而不是 8 个。这个变化可减少 RAM 使用量。(BZ#1899107)
- 在以前的版本中，更改身份验证资源的 **serviceAccountIssuer** 字段更新 **kubi-apiserver** 以使用新签发者验证令牌，并用上一个签发者拒绝令牌。因为 **kubi-apiserver** 不支持多个签发者，所以更改 **serviceAccountIssuer** 可能会破坏依赖绑定令牌的应用程序。除非应用程序在现有令牌从 **kubi-apiserver** 接收 **401** 响应时对新令牌进行编码，否则无效令牌的使用将继续直到硬件重启，或者无效令牌的有效期超过 80%，此时 kubelet 将请求一个新令牌。
  作为临时解决方案，只有在中断可以接受时更改 **serviceAccountIssuer** 字段，且重启所有 pod 是一个选项。(BZ#1905573)
- 在以前的版本中，**create role binding** 表单上缺少角色名称。此更新显示 **create role binding** 表单的角色名称。（BZ#1905788）
- 在以前的版本中，对客户端节流的一个低限制会导致集群中安装的 CRD 数量增加。因此，客户端代码对到达 API 发现的请求进行限制。在这个版本中，限制数会增加到当前数量的两倍，从而降低了客户端节流的频率。(BZ#1906332)
- 当使用不正确的用户名验证镜像签名时，无法验证镜像签名。使用正确的用户名会导致镜像签名验证可以正常工作。(BZ#1906796)
- 在以前的版本中，如果触发器从同一代理进入 Knative Service（KSVC）和 In Memory Channel（IMC），Knative 资源不会显示在 **Topology** 视图中。在这个版本中，Knative 数据会被正确返回，这可以使 **Topology** 视图正确显示 Knative 资源。（BZ#1907827）
- 在以前的版本中，在更改 **oc debug command** 的过程中会丢失 init 容器的支持。因此，init 容器无法被调试。在这个版本中，增加了对 **oc debug command** 中的 init 容器的支持，从而可以调试 init 容器。（BZ#1913109）

- 在以前的版本中，**Operator sync** 执行期间缺少配置状态更新不会出现最新的（已应用的）swift 配置。此更新修复了同步过程，以将配置的状态与配置的 spec 值匹配。因此，配置状态和配置规格现在与当前应用的配置同步。（BZ#1916857）
- 在以前的版本中，间隔 DNS 错误会在节点的 **/etc/hosts** 文件中创建无效条目。此更新过滤 DNS 请求中的出错信息。这最终会返回有效记录，它会提示 **dns-node-resolver** 不再创建无效的 **/etc/hosts** 条目。（BZ#1916907）
- 在以前的版本中，置备接口可能会在某些情况下丢失其 IPv6 link-local 地址，从而导致置备更多 worker。这个问题现已解决。（BZ#1918779）

1.8.13.3. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.14. RHBA-2021:0424 - OpenShift Container Platform 4.6.17 程序错误修复和安全更新

发布日期：2021 年 2 月 15 日

OpenShift Container Platform release 4.6.17 现已正式发布,其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:0424 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:0423 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.17 --pullspecs
```

1.8.14.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.15. RHBA-2021:0510 - OpenShift Container Platform 4.6.18 程序错误修复更新

发布日期：2021 年 2 月 22 日

OpenShift Container Platform release 4.6.18 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:0510 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0511 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.18 --pullspecs
```

1.8.15.1. 功能

1.8.15.1.1. Insights Operator 的改进

在这个版本中，Insights Operator 会为 **ContainerRuntimeConfig** 对象收集信息。这个信息对故障排除非常有用。如需更多信息，请参阅 BZ#1891544。

1.8.15.1.2. 支持轮转云供应商凭证

在这个版本中，您可以手动更新 Cloud Credential Operator（CCO）用来管理云供应商凭证的 secret。如需更多信息，请参阅手动轮转云供应商凭证。

1.8.15.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.16. RHBA-2021:0634 - OpenShift Container Platform 4.6.19 程序错误修复更新

发布日期：2021 年 3 月 1 日

OpenShift Container Platform release 4.6.19 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:0634 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0633 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.19 --pullspecs
```

1.8.16.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.17. RHBA-2021:0674 - OpenShift Container Platform 4.6.20 程序漏洞修复更新

发布日期：2021 年 3 月 9 日

OpenShift Container Platform release 4.6.20 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:0674 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0673 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.20 --pullspecs
```

1.8.17.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.18. RHBA-2021:0753 - OpenShift Container Platform 4.6.21 程序漏洞修复更新

发布日期：2021 年 3 月 16 日

OpenShift Container Platform release 4.6.21 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:0753 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0750 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.21 --pullspecs
```

1.8.18.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.19. RHBA-2021:0825 - OpenShift Container Platform 4.6.22 程序漏洞修复更新

发布日期：2021 年 3 月 23 日

OpenShift Container Platform release 4.6.22 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:0825 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:0826 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.22 --pullspecs
```

1.8.19.1. 程序错误修复

- 在以前的版本中， Zeroconf 库无法正确地对多播 DNS（mDNS）响应进行速率限制。因此，过量 mDNS 流量会产生大量的网络记录。在这个版本中，Zeroconf 库增加了对速率的限制，这可显著减少 mDNS 流量。(BZ#1936539)

- 在以前的版本中，API 服务器可能无法创建资源，当资源配额存在冲突时，资源会返回 409 状态代码。因此，资源将无法创建，您可能需要重试 API 请求。在这个版本中，OpenShift Web 控制台会在收到 409 状态代码时尝试重试请求三次，这通常足以完成请求。如果 409 状态代码持续发生，控制台中会显示一个错误。(BZ#1938230)

- 在以前的版本中，当 Prometheus 容器负载很重时，存活度探测会失败，例如：在 write-ahead logging（WAL）replay 过程中。这个高负载会造成几个问题，并导致空循环无法正常重启。在这个版本中删除了存活度探测，因此负载不再造成无限期重启循环。（BZ#1935586）

- 根据 iptables 重写规则，使用固定源端口通过服务 IP 和 pod IP 连接到服务的客户端可能会遇到端口冲突的问题。在这个版本中，插入了额外的 Open vSwitch（OVS）规则来确保在端口冲突发生时，并执行额外的源网络地址转换（SNAT）来避免上面提到的冲突。因此，连接到服务时不再有端口冲突。（BZ#1937547）

- 在以前的版本中，在 pod 有机会同步前，节点就被标记为 **Ready** 并可以接受 pod。因此，**Pod** 状态可能已经过时。如果节点还没有封锁，则通常会在启动时一直处于**nodeAffinity** 状态。在这个更新中，在节点至少与 PI 服务器同步前，节点不会标记为 **Ready**。因此，在冷集群重启后，pod 不会再卡在 **nodeAffinity** 中。（BZ#1930960）

- 在以前的版本中，当从带有空闲工作负载的早期版本升级集群时，当升级到 OpenShift Container Platform 4.6/4.7 后，闲置工作负载不会在 HTTP 请求中启动，因为更新了 **oc idle** 功能。在这个版本中，闲置更改从端点镜像到 Ingress Operator 启动时的服务。因此，升级后取消闲置工作负载可以正常工作。（BZ#1927364）

1.8.19.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.20. RHBA-2021:0952 - OpenShift Container Platform 4.6.23 程序错误修复和安全更新

发布日期：2021 年 3 月 30 日

OpenShift Container Platform release 4.6.23 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:0952 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:0956 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.23 --pullspecs
```

1.8.20.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.21. RHBA-2021:1153 - OpenShift Container Platform 4.6.25 程序错误修复更新

发布日期：2021 年 4 月 20 日

OpenShift Container Platform release 4.6.25 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:1153 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:1154 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.25 --pullspecs
```

1.8.21.1. 功能

1.8.21.1.1. 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。

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

Insights Operator 现在可以为不健康的 SAP pod 收集数据。当 SDI 安装失败时，可以通过查看哪个初始化 pod 失败来检测到问题。Insights Operator 现在会在 SAP/SDI 命名空间中收集有关失败 pod 的信息。如需更多信息，请参阅 **BZ#1935775**。

1.8.21.1.3. 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 或您的内核可能需要升级。如需更多信息，请参阅 BZ#1939059。

1.8.21.1.4. 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#1942457。

1.8.21.2. 程序错误修复

- 在以前的版本中，在 NetworkManager 启动前，VMware vSphere 元数据中的主机名不会被设置，在以后设置主机名时会忽略此元数据。在这个版本中，如果 vSphere 元数据中有此信息，主机名由 **vsphere-hostname.service** 设置。(BZ#1904825)

- 在以前的版本中，自动生成的 Docker 配置 secret 不包含集成的内部 registry 路由的凭证。因为没有通过任何路由访问 registry 的凭证，所以因为身份验证不足而试图访问 registry 的 Pod 会失败。在这个版本中，所有配置的 registry 路由都到默认的 Docker 凭证 secret，pod 都可通过任何路由访问集成的 registry。（BZ#1931857）

- 在以前的版本中，**/etc/pki/ca-trust/extracted** 文件可能会变得不可写，阻止 Image Registry Operator 将 CA 证书添加到 pod 的信任存储中。在这个版本中，emptyDir 卷被挂载到 **/etc/pki/ca-trust/extracted** 中，卷现在始终可以被 pod 写入。（BZ#1936984）

- 在以前的版本中，OpenShift Container Platform 4.7 的 Machine Config Operator（MCO）修复了在用户置备的基础架构上为 vSphere 配置错误的 **nodeip-configuration** 服务，但不适用于 OpenShift Container Platform 4.6。因此，当将 OpenShift Container Platform 从 4.6.z 升级到不同的 4.6.z 并升级到 4.7 时，如果 control plane 在计算机器完成 4.6.z 升级前完成 4.7 升级，MCO 的 4.7 版本将停止整个升级。此发行版本解决了错误配置的 **nodeip-configuration** 服务的问题，以便升级可以成功完成。（BZ#1940585）

- 在以前的版本中，CPH 请求在不再需要时不会被关闭，从而导致 Go 常规泄漏，从而随着时间的推移增加内存用量。在这个版本中，如果不再需要 HTTP 请求，它们始终会被关闭。（BZ#1941563）

- 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#1944245）

1.8.21.3. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.22. RHBA-2021:1232 - OpenShift Container Platform 4.6.26 程序错误修复更新

发布日期：2021 年 4 月 27 日

OpenShift Container Platform release 4.6.26 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:1232 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:1229 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.26 --pullspecs
```

1.8.22.1. 功能

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

Insights Operator 现在可以从 SAP 集群收集 **Datahubs** 资源。通过这些数据，SAP 集群可以被与 Insights Operator 归档中的非 SAP 集群区分开，即使缺少所有从 SAP 集群收集的数据，否则就无法确定集群是否有 SDI 安装。如需更多信息，请参阅 BZ#1942907。

1.8.22.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.23. RHBA-2021:1427 - OpenShift Container Platform 4.6.27 程序错误修复更新

发布日期：2021 年 5 月 4 日

OpenShift Container Platform release 4.6.27 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:1427 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:1428 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.27 --pullspecs
```

1.8.23.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.24. RHBA-2021:1487 - OpenShift Container Platform 4.6.28 程序错误修复更新

发布日期：2021 年 5 月 12 日

OpenShift Container Platform release 4.6.28 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:1487 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:1488 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.28 --pullspecs
```

1.8.24.1. 程序错误修复

- 在以前的版本中，在安装过程中，SDN pod 会重复崩溃并重启，直到安装的其他部分完成，从而导致安装时间较长。在这个版本中，SDN pod 可以读取部分安装的集群状态，并等待正确的时间继续。因此，SDN pod 不会崩溃，安装也不会延迟。(BZ#1950407)

- 在以前的版本中，Cluster Samples Operator 可能会更改其正在监视的对象的控制器缓存，这会导致 Kubernetes 管理控制器缓存时出现错误。在这个版本中，添加了对 Cluster Samples Operator 如何使用控制器缓存中的信息的修复。因此，Cluster Samples Operator 通过修改控制器缓存不会造成错误。（BZ#1950809）

- 在以前的版本中，从 web 控制台创建示例应用程序可能会失败，因为应用程序的资源不是按顺序创建的。在这个版本中，指定这些资源的创建顺序，从而打造更稳定的创建示例应用程序过程。（BZ#1933666）

1.8.24.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.25. RHBA-2021:1521 - OpenShift Container Platform 4.6.29 程序错误修复更新

发布日期：2021 年 5 月 20 日

OpenShift Container Platform release 4.6.29 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:1521 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:1522 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.29 --pullspecs
```

1.8.25.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.26. RHBA-2021:1565 - OpenShift Container Platform 4.6.30 程序错误修复和安全更新

发布日期：2021 年 5 月 25 日

OpenShift Container Platform release 4.6.30 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:1565 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:1566 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.30 --pullspecs
```

1.8.26.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.27. RHBA-2021:2100 - OpenShift Container Platform 4.6.31 程序错误修复更新

发布日期：2021 年 6 月 1 日

OpenShift Container Platform release 4.6.31 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2100 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:2101 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.31 --pullspecs
```

1.8.27.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.28. RHBA-2021:2157 - OpenShift Container Platform 4.6.32 程序错误修复更新

发布日期：2021 年 6 月 8 日

OpenShift Container Platform release 4.6.32 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2157 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:2158 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.32 --pullspecs
```

1.8.28.1. 程序错误修复

- 在以前的版本中，当从 **Role** 页面的 **Role Bindings** 选项卡创建新绑定时，web 控制台会预先填充不正确的角色名称和命名空间。在这个版本中，新绑定具有默认的 **cluster-admin** 角色。(BZ#1950490)
- 在以前的版本中，Machine Config Operator **relatedObjects** 资源中缺少命名空间，因此一些内部服务的日志没有在 **must-gather** 中收集。在这个版本中，所需的命名空间添加到 Machine Config Operator **relatedObjects** 资源中，并在 **must-gather** 中收集内部服务的日志。(BZ#1955715)
- 在以前的版本中，如果 CCO 的部署不健康，Cloud Credential Operator（CCO）和 Cluster Version Operator（CVO）都会报告。这会导致在出现问题时出现双重报告。在这个版本中，在部署不健康时，CCO 不再进行报告。（BZ#1958959）
- 在以前的版本中，对于源自服务成员并由负载均衡器重定向到同一成员的流量，Open Virtual Network（OVN）将数据包的源 IP 地址改为负载均衡器的 IP 地址。如果应用了网络策略，则这种类型的流量有时会被不必要地阻止。在这个版本中，Kuryr 会打开到网络策略命名空间中所有服务的 IP 地址的流量，流量不会被阻断。（BZ#1963846）

1.8.28.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.29. RHBA-2021:2267 - OpenShift Container Platform 4.6.34 程序错误修复更新

发布日期：2021 年 6 月 14 日

OpenShift Container Platform release 4.6.34 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2267 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:2268 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.34 --pullspecs
```

1.8.29.1. 功能

1.8.29.1.1. Insights Operator 的改进

在这个版本中，用户可以收集 **virt_platform** 指标。Insights Operator 的规则需要 **virt_platform** 指标来确定集群的虚拟平台。此信息存储在 **config/metric** 文件的 Insights Operator 存档中。如需更多信息，请参阅 BZ#1965219。

1.8.29.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.30. RHBA-2021:2410 - OpenShift Container Platform 4.6.35 程序错误修复更新

发布日期：2021 年 6 月 22 日

OpenShift Container Platform release 4.6.35 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2410 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:2407 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.35 --pullspecs
```

1.8.30.1. 功能

1.8.30.1.1. Insights Operator 的改进

在这个版本中，Insights Operator **Gather** 方法可以从与不健康 Operator 相关的 pod 中收集日志，以及与 Operator 共存在同一命名空间中的 pod。这允许 Insights Operator 确定与 Operator 关联的命名空间，并在捆绑包中包含 pod 日志。因此，Insights Operator 现在从不健康 pod 收集日志，不仅与 Operator 相关，也从 Operator 命名空间中的每个 pod 收集日志。

1.8.30.2. 程序错误修复

- 在以前的版本中，当在带有 IPv4 地址的节点上启动单堆栈 IPv6 集群时，kubelet 可能已经使用 IPv4 IP，而不是节点 IP 的 IPv6 IP。因此，主机网络 pod 会具有 IPv4 IP 而不是 IPv6 IP，这使得它们无法从仅支持 IPv6 的 pod 访问。在这个版本中，node-IP-picking 代码被修复，这会导致 kubelet 使用 IPv6 IP。(BZ#1942488)

- BZ#1953097 修复启用了 CoreDNS **bufsize** 插件，大小为 1232 字节。有些原始 DNS 解析器无法通过大于 512 字节的 UDP 接收 DNS 响应消息。因此，一些 DNS 解析器（如 Go 的内部 DNS 库）无法从 DNS Operator 接收详细的 DNS 响应。在这个版本中，所有服务器的 CoreDNS **bufsize** 设置为 512 字节。现在，UDP DNS 信息会被正确接收。(BZ#1970140)

- 在以前的版本中，执行 HTTP 连接时缺少正确的超时会打开连接。因此，这些连接会聚合到达到最大限制前，因此 Operator 将无法处理传入的事件。在这个版本中，Operator 使用的 HTTP 客户端增加了超时，这样可确保在达到超时后关闭开放连接。（BZ#1959563）

- 在以前的版本中，从通过路由公开的服务中删除 **选择器（selector）** 会导致为服务 pod 创建的 **endpointslices** 重复，这会因为重复的服务器条目而触发 HAProxy 重新加载错误。在这个版本中，在编写 HAProxy 配置文件时会过滤掉意外重复的服务器行，因此从服务中删除选择器不再会导致路由器失败。（BZ#1965329）

1.8.30.3. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.31. RHBA-2021:2498 - OpenShift Container Platform 4.6.36 程序错误修复和安全更新

发布日期：2021 年 6 月 29 日

OpenShift Container Platform release 4.6.36 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2498 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:2499 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.36 --pullspecs
```

1.8.31.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.32. RHBA-2021:2641 - OpenShift Container Platform 4.6.38 程序错误修复和安全更新

发布日期：2021 年 7 月 13 日

OpenShift Container Platform release 4.6.38 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2641 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:2642 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.38 --pullspecs
```

1.8.32.1. 程序错误修复

- 在以前的版本中，当在带有 IPv4 地址的节点上启动单堆栈 IPv6 集群时，kubelet 可能会使用 IPv4 地址而不是 IPv6 地址作为节点 IP 地址。因此，主机网络 pod 会具有 IPv4 地址而不是 IPv6 地址，这使得它们无法从仅支持 IPv6 的 pod 访问。在这个版本中，node-IP-picking 代码被修复，这会导致 kubelet 使用 IPv6 地址。(BZ#1942506)

- 在以前的版本中，CRI-O 日志不包含从中拉取镜像的源的信息。因此，CRI-O 无法判断镜像是否从 registry 镜像中提取。在这个版本中，为 CRI-O 添加有关镜像拉取源的级别日志信息。现在，拉取源会显示在日志的信息级别中。(BZ#1976293)

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

- 在这个版本中，Pipeline ServiceAccount 不使用在为私有 Git 存储库的 **git import** 流中创建的 secret，这会导致这些 Pipelines 失败。在这个版本中，通过在 secret 和 Pipeline ServiceAccount 中添加注解来解决这个问题。私有 Git 存储库的管道现在可以正确运行。（BZ#1970470）

- 在以前的版本中，在切换项目时不是 kubeconfig 中的所有选项都被复制。因此，在 kubeconfig 中切换使用 **Exec** 验证的项目时，信息会丢失。在这个版本中，在切换使用 **oc projects** 和 **Exec** 验证的项目时，会复制所有必要的信息。(BZ#1973613)

- 在以前的版本中，当将第二个内部 IP 地址添加到一个或多个 control plane 节点时，etcd Operator 会因为检测到 IP 地址更改而降级。因此，它不会为节点重新生成 etcd 服务证书。在这个版本中，etcd Operator 会区分新节点的 IP 地址更改。因此，etcd Operator 会重新生成现有节点更改的证书，添加新 IP 地址不再会导致 etcd Operator 降级。(BZ#1965535)

- 在以前的版本中，如果 OpenShift Container Platform Web 控制台中的 Bitbucket 存储库包含带有反斜杠 (\) 或正斜杠 (/) 的分支名称，则为部署创建的拓扑 URL 无法正常工作。这是因为 Bitbucket API BCLOUD-9969 存在问题。当前发行版本可以缓解这个问题。如果分支名称包含反斜杠或正斜杠，则拓扑 URL 指向存储库的默认分支页面。此问题将在 OpenShift Container Platform 以后的发行版本中解决。(BZ#1972694)

1.8.32.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.33. RHBA-2021:2684 - OpenShift Container Platform 4.6.39 程序错误修复更新

发布日期：2021 年 7 月 21 日

OpenShift Container Platform release 4.6.39 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2684 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:2685 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.39 --pullspecs
```

1.8.33.1. 程序错误修复

- 在以前的版本中，当以非 root 用户身份运行 **oc image extract** 命令时，它会失败并显示 **operation not permitted** 错误。这是因为在解压缩期间设置扩展属性的权限不足。在这个版本中，只有在以 root 用户身份运行命令时，才会设置扩展的安全属性，以便命令适用于 root 用户和非 root 用户。(BZ#1969929)

- 在以前的版本中，当在 Developer 控制台中将服务集群设置为本地的标签更改时，用户将无法创建 Knative 服务。在这个版本中，Knative 服务使用 **cluster-local** 的最新支持标签，以便用户以 cluster-local 用户身份从 Developer Console 创建 Knative 服务。(BZ1978159)

1.8.33.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.34. RHBA-2021:2767 - OpenShift Container Platform 4.6.40 程序错误修复更新

发布日期：2021 年 7 月 28 日

OpenShift Container Platform release 4.6.40 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2767 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:2768 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.40 --pullspecs
```

1.8.34.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.35. RHBA-2021:2886 - OpenShift Container Platform 4.6.41 程序错误修复更新

发布日期：2021 年 8 月 4 日

OpenShift Container Platform release 4.6.41 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:2886 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:2888 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.41 --pullspecs
```

1.8.35.1. 功能

1.8.35.1.1. 按策略划分的构建数量的新 Telemetry 指标

Telemetry 包括一个新的 **openshift:build_by_strategy:sum** 量表指标，它将按照策略类型向 Telemeter 客户端发送构建数量。此指标可让站点可靠性工程师（SRE）和产品经理查看在 OpenShift Container Platform 集群上运行的构建类型。(BZ#1969964)

1.8.35.2. 程序错误修复

- 在以前的版本中，当在带有 IPv4 地址的节点上启动单堆栈 IPv6 集群时，kubelet 可能已经使用 IPv4 IP，而不是节点 IP 的 IPv6 IP。因此，主机网络 pod 会具有 IPv4 IP 而不是 IPv6 IP，这使得它们无法从仅支持 IPv6 的 pod 访问。在这个版本中，node-IP-picking 代码被修复，这会导致 kubelet 使用 IPv6 IP。(BZ#1942506)

1.8.35.3. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.36. RHBA-2021:3008 - OpenShift Container Platform 4.6.42 程序错误修复和安全更新

发布日期：2021 年 8 月 11 日

OpenShift Container Platform release 4.6.42 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3008 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3009 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.42 --pullspecs
```

1.8.36.1. 程序错误修复

- 在以前的版本中，主机网络 pod 具有 IPv4 IP，使其无法从只有 IPv6 的 pod 进行访问。在这个版本中修复了 **node-IP-picing** 代码，以便节点具有 IPv6 IP。因此，主机网络 pod 现在可以访问。(BZ1942506)

1.8.36.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.37. RHBA-2021:3197 - OpenShift Container Platform 4.6.43 程序错误修复更新

发布日期：2021 年 8 月 25 日

OpenShift Container Platform release 4.6.43 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3197 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3198 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.43 --pullspecs
```

1.8.37.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.38. RHBA-2021:3395 - OpenShift Container Platform 4.6.44 程序错误修复更新

发布日期：2021 年 9 月 8 日

OpenShift Container Platform release 4.6.44 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3395 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3396 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.44 --pullspecs
```

1.8.38.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.39. RHBA-2021:3517 - OpenShift Container Platform 4.6.45 程序错误修复更新

发布日期：2021 年 9 月 22 日

OpenShift Container Platform release 4.6.45 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3517 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:3518 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.45 --pullspecs
```

1.8.39.1. 功能

1.8.39.1.1. 集群的新最低存储要求

安装 OpenShift Container Platform 集群所需的最小存储从 120 GB 减少到 100 GB。这个更新适用于所有支持的平台。

1.8.39.2. 程序错误修复

- 在以前的版本中，当使用无效的镜像流或未解析镜像创建部署时，会导致部署控制器和 API 服务器的 **imagepolicy** 插件之间处于不一致的状态。因此，可能会导致无限数量的副本集并达到 etcd 配额限制，这可能会使整个 OpenShift Container Platform 集群崩溃。在这个版本中，API 服务器的 **imagepolicy** 插件降低了职责。因此，部署中不会出现不一致的镜像流解析。(BZ#1981784).

1.8.39.3. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.40. RHBA-2021:3643 - OpenShift Container Platform 4.6.46 程序错误修复和安全更新

发布日期：2021 年 9 月 29 日

OpenShift Container Platform release 4.6.46 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:3643 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3642 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.46 --pullspecs
```

1.8.40.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.41. RHBA-2021:3737 - OpenShift Container Platform 4.6.47 程序错误修复更新

发布日期：2021 年 10 月 13 日

OpenShift Container Platform release 4.6.47 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3737 公告中。这个版本没有 RPM 软件包。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.47 --pullspecs
```

1.8.41.1. 程序错误修复

- 在以前的版本中，使用自定义 CA 证书连接到 Red Hat OpenStack Platform(RHOSP)端点的 HTTP 传输缺少代理设置。因此，在 RHOSP 上部署集群时，集群无法完全运行。当连接自定义

CA 证书时，这个更新会将代理设置传递给 HTTP 传输。因此，所有集群组件都可以正常工作。(BZ#2002752)

1.8.41.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.42. RHBA-2021:3829 - OpenShift Container Platform 4.6.48 程序错误修复更新

发布日期：2021 年 10 月 20 日

OpenShift Container Platform release 4.6.48 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3829 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:3828 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.48 --pullspecs
```

1.8.42.1. 功能

1.8.42.1.1. Kubernetes 1.19.14 的更新

此更新包含 Kubernetes 1.19.14 的更改。更多信息可在以下更改日志中找到：1. 19.14、1.19.1 3、1.19.12、1.19.11、1. 19.10、1. 19.9、1.19.8、1.1 9.7、1.19.6、1.19.5。

1.8.42.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.43. RHBA-2021:4009 - OpenShift Container Platform 4.6.49 程序错误修复和安全更新

发布日期：2021 年 11 月 3 日

OpenShift Container Platform release 4.6.49 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:4009 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:4008 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.49 --pullspecs
```

1.8.43.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.44. RHBA-2021:4800 - OpenShift Container Platform 4.6.51 程序错误修复和安全更新

发布日期：2021 年 12 月 2 日

OpenShift Container Platform release 4.6.51 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:4800 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:4799 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.51 --pullspecs
```

1.8.44.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.45. RHBA-2021:5010 - OpenShift Container Platform 4.6.52 程序错误修复和安全更新

发布日期：2021 年 12 月 14 日

OpenShift Container Platform release 4.6.52 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2021:5010 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:5009 公告提供。

此版本包括 CVE-2021-44228、CVE-2021-45046、CVE -2021-4104 和 CVE-2021-4125 的关键安全更新，所有这些都涉及 Apache Log4j 实用程序。这些漏洞的修复由 RHSA-2021:5106、RHSA-2021:5141 和 RHSA-2021:5186 公告 提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.52 --pullspecs
```

1.8.45.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.46. RHBA-2022:0025 - OpenShift Container Platform 4.6.53 程序错误修复和安全更新

发布日期：2022 年 1 月 12 日

OpenShift Container Platform release 4.6.53 现已正式发布，其中包括安全更新。其程序错误修正信息包括在 RHBA-2022:0025 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:0024 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.53 --pullspecs
```

1.8.46.1. 程序错误修复

- 在以前的版本中，在统一可扩展固件接口(UEFI)模式中，**ironic-python-agent** 在下载 Red Hat Enterprise Linux CoreOS(RHCOS)镜像后创建一个 UEFI 引导装载程序条目。当使用基于 Red

Hat Enterprise Linux(RHEL)8.4 的 RHCOS 镜像时，镜像可能无法使用此条目引导。因此，如果引导镜像时使用 **ironic-python-agent** 安装的条目，则引导可能会失败并输出 BIOS 错误屏幕。在这个版本中，**ironic-python-agent** 根据镜像中的 CSV 文件配置引导条目，而不是使用固定的引导条目。因此，镜像在没有错误的情况下正确引导。(BZ#2025495)

1.8.46.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.47. RHBA-2022:0180 - OpenShift Container Platform 4.6.54 程序错误修复和安全更新

发布日期：2022 年 1 月 26 日

OpenShift Container Platform release 4.6.54 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2022:0180 公告中。这个版本没有 RPM 软件包。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.54 --pullspecs
```

1.8.47.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.48. RHBA-2022:0566 - OpenShift Container Platform 4.6.55 程序错误修复和安全更新

发布日期：2022 年 2 月 23 日

OpenShift Container Platform release 4.6.55 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2022:0566 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:0565 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.55 --pullspecs
```

1.8.48.1. 功能

1.8.48.1.1. 用于 Whereabouts CNI IPAM 插件的 IP 协调

关于 Whereabouts CNI IPAM 插件的新增强，添加了 IP 协调作业 **ip-reconciler**，它作为 Kubernetes cronjob 运行。在以前的版本中，如果 **CNI DEL** 请求没有完成 pod，则 pod 的 IP 地址会保留分配，即使它们没有被使用。现在，这些 IP 地址会定期收集并被重新分配。(BZ#2028968)

1.8.48.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.49. RHBA-2022:0867 - OpenShift Container Platform 4.6.56 程序错误修复和安全更新

发布日期：2022 年 3 月 23 日

OpenShift Container Platform release 4.6.56 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2022:0867 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:0866 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.56 --pullspecs
```

1.8.49.1. 程序错误修复

- 在以前的版本中，Red Hat OpenStack Platform(RHOSP)凭证 secret 创建和 **kube-controller-manager** 启动之间的错误会阻止 RHOSP 凭证正确配置。因此，RHOSP 中不会创建 **LoadBalancer** 服务。此更新会在 **kube-controller-manager** 启动时获取 RHOSP 凭证。因此，RHOSP secret 凭证现在可以正确初始化。(**BZ#2059677**)

1.8.49.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.50. RHBA-2022:1621 - OpenShift Container Platform 4.6.57 程序错误修复更新和安全更新

发布日期： 2022 年 5 月 4 日

OpenShift Container Platform release 4.6.57 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2022:1621 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:1620 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.57 --pullspecs
```

1.8.50.1. 删除的功能

从 OpenShift Container Platform 4.6.57 开始，在 Microsoft Azure 集群上以 mint 模式使用 Cloud Credential Operator(CCO)的支持已从 OpenShift Container Platform 4.6 中删除。此更改的原因是 Microsoft 的 Azure AD Graph API 将于 2022 年 6 月 30 日停用 ，并被向后移植到 z-stream 更新中所有支持的 OpenShift Container Platform 版本。如需更多信息，请参阅为 Microsoft Azure 删除对 minting 凭证的支持。

1.8.50.2. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.51. RHSA-2022:2264 - OpenShift Container Platform 4.6.58 程序错误修复和安全更新

发布日期： 2022 年 5 月 25 日

OpenShift Container Platform release 4.6.58 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHSA-2022:2264 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:2263 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.58 --pullspecs
```

1.8.51.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.52. RHBA-2022:4948 - OpenShift Container Platform 4.6.59 程序错误修复和安全更新

发布日期： 2022 年 6 月 17 日

OpenShift Container Platform release 4.6.59 现已正式发布，其中包括安全更新。此更新包括的程序错误修正信息包括在 RHBA-2022:4948 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:4947 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.59 --pullspecs
```

1.8.52.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.53. RHBA-2022:5572 - OpenShift Container Platform 4.6.60 程序错误修复更新

发布日期： 2022 年 7 月 21 日

OpenShift Container Platform release 4.6.60 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2022:5572 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:5571 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.60 --pullspecs
```

1.8.53.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.8.54. RHSA-2022:6262 - OpenShift Container Platform 4.6.61 程序错误修复更新

发布日期： 2022 年 9 月 9 日

OpenShift Container Platform release 4.6.61 现已正式发布，其中包括安全修复。此更新包括的程序错误修正信息包括在 RHSA-2022:6262 公告中。此更新中包括的 RPM 软件包由 RHBA-2022:6261 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.6.61 --pullspecs
```

1.8.54.1. 更新

要将现有 OpenShift Container Platform 4.6 集群更新至此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。