OpenShift Container Platform 4.9

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: 2022-01-15

OpenShift Container Platform 4.9 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 4.9 发行注记

Red Hat OpenShift Container Platform 为软件开发人员和 IT 机构提供了一个混合云应用平台。使用这个平台可以在配置和管理成本最小化的情况下，利用安全、可扩展的资源部署新的或已有的应用程序。OpenShift Container Platform 支持大量编程语言和开发平台，如 Java、JavaScript、Python、Ruby 和 PHP。

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

1.1. 关于此版本

OpenShift Container Platform (RHSA-2021:3759) 已正式发布。此发行版本使用带有 CRI-O 运行时的 Kubernetes 1.22。OpenShift Container Platform 4.9 的新功能、改变以及已知的问题包括在此文档中。

OpenShift Container Platform 4.9 集群可以通过 https://cloud.redhat.com/openshift 获得。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 4.9 需要运行在 Red Hat Enterprise Linux (RHEL) 7.9 和 8.4 上，以及 Red Hat Enterprise Linux CoreOS (RHCOS) 4.9。

控制平面（control plane）必须使用 RHCOS，计算（compute）机器可以使用 RHCOS 或 Red Hat Enterprise Linux (RHEL) 7.9 或 8.4。

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

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

1.3. 新功能及功能增强

此版本对以下方面进行了改进

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. 在引导时删除安装 Ignition 配置

之前，使用 **coreos-installer** 程序安装的节点会在 **/boot/ignition/config.ign** 文件中保留安装 Ignition 配置。从 OpenShift Container Platform 4.9 安装镜像开始，在置备节点时会删除该文件。此更改不会影响在以前的 OpenShift Container Platform 版本上安装的集群，因为它们仍然使用较旧的 bootimage。

1.3.2. 安装和升级

1.3.2.1. 使用用户置备的基础架构在 Microsoft Azure Stack Hub 上安装集群

OpenShift Container Platform 4.9 引进了对使用用户置备的基础架构在 Azure Stack Hub 上安装集群的支持。

您可以使用红帽提供的 Azure Resource Manager (ARM) 示例模板来协助部署过程，或自行创建。您也可以自由选择通过其他方法创建所需的资源；ARM 模板仅作示例之用。

详情请参阅使用 ARM 模板在 Azure Stack Hub 上安装集群。

1.3.2.2. 在更新集群前暂停机器健康检查

在升级过程中，集群中的节点可能会临时不可用。对于 worker 节点，机器健康检查可能会认为这样的节点不健康，并重新引导它们。为避免重新引导这样的节点，OpenShift Container Platform 4.9 引入了 **cluster.x-k8s.io/paused=""** 注解，允许您在更新集群前暂停 **MachineHealthCheck** 资源。

如需更多信息，请参阅暂停 MachineHealthCheck 资源。

1.3.2.3. 在机器 CIDR 中增加 Azure 子网的大小

Microsoft Azure 的 OpenShift Container Platform 安装程序现在在机器 CIDR 中创建尽量大的子网。这可让集群使用适当的大小来容纳集群中节点数量的机器 CIDR。

1.3.2.4. 支持中国的 AWS 区域

OpenShift Container Platform 4.9 引入了对中国 AWS 区域的支持。现在，您可以在 **cn-north-1(Beijing)** 和 **cn-northwest-1 (Ningxia)** 区域安装和更新 OpenShift Container Platform 集群。

如需更多信息，请参阅在 AWS 中国上安装集群。

1.3.2.5. 在 baremetal 网络中使用 Virtual Media 扩展集群

在 OpenShift Container Platform 4.9 中，您可以使用 **baremetal** 网络上的 Virtual Media 扩展使用 **provisioning** 网络部署的安装程序置备的集群。当 **ProvisioningNetwork** 配置设置为 **Managed** 时，您可以使用此功能。要使用此功能，您必须在 **provisioning** 自定义资源 (CR) 中将 **virtualMediaViaExternalNetwork** 配置设置设置为 **true**。您还必须编辑机器集以使用 API VIP 地址。详情请参阅准备使用 baremetal 网络上的 Virtual Media 进行部署 。

1.3.2.6. 从 OpenShift Container Platform 4.8 升级到 4.9 时所需的管理员确认

OpenShift Container Platform 4.9 使用 Kubernetes 1.22，它删除了大量已弃用的 **v1beta1** API。

OpenShift Container Platform 4.8.14 引入了一项要求，即管理员必须先提供手动确认，然后才能从 OpenShift Container Platform 4.8 升级到 4.9。这有助于防止升级到 OpenShift Container Platform 4.9 后出现问题，其中已删除的 API 仍在由运行或与集群交互的工作负载、工具或其他组件使用。管理员必须针对将要删除的任何 API 评估其集群，并迁移受影响的组件，以使用适当的新 API 版本。完成此操作后，管理员可以向管理员提供确认。

所有 OpenShift Container Platform 4.8 集群都需要此管理员确认，然后才能升级到 OpenShift Container Platform 4.9。

如需更多信息，请参阅准备升级到 OpenShift Container Platform 4.9 。

1.3.2.7. 支持在使用 PCI 直通的 RHOSP 部署中安装

OpenShift Container Platform 4.9 引进了在依赖于 PCI 直通 的 Red Hat OpenStack Platform(RHOSP) 部署上安装的支持。

1.3.2.8. 将 etcd 版本 3.4 升级到 3.5

OpenShift Container Platform 4.9 支持 etcd 3.5。在升级集群前，请验证是否存在有效的 etcd 备份。etcd 备份可确保在发生升级失败时可以恢复集群。在 OpenShift Container Platform 4.9 中，etcd 升级是

自动的。根据集群的转换状态到版本 4.9，etcd 备份可能会可用。但是，建议在集群升级开始前验证备份是否存在。

1.3.2.9. 使用安装程序置备的基础架构在 IBM Cloud 上安装集群

OpenShift Container Platform 4.9 引进了对使用安装程序置备的基础架构在 IBM Cloud® 上安装集群的支持。该流程与裸机上的安装程序置备的基础架构几乎相同，但有以下区别：

- IBM Cloud 上 OpenShift Container Platform 4.9 安装程序置备的安装需要 **provisioning** 网络、IPMI 和 PXE 引导。红帽不支持在 IBM Cloud 上使用 Redfish 和虚拟介质进行部署。
- 您必须在 IBM Cloud 上创建和配置公共和私有 VLAN。
- 在开始安装过程前，IBM Cloud 节点必须可用。因此，您必须首先创建 IBM 云节点。
- 您必须准备 provisioner 节点。
- 您必须在公共的 **baremetal** 网络中安装和配置 DHCP 服务器。
- 您必须配置 **install-config.yaml** 文件，以便每个节点都使用 IPMI 指向 BMC，并将 IPMI 权限级别设置为 **OPERATOR**。

详情请参阅在 IBM Cloud 上部署安装程序置备的集群。

1.3.2.10. 改进了对安装程序置备的集群中的 Fujitsu 硬件的支持

在 Fujitsu 硬件上部署安装程序置备的集群并使用 Fujitsu 集成 Remote Management Controller (iRMC) 时，OpenShift Container Platform 4.9 添加了对 worker 节点的 BIOS 配置支持。详情请参阅为 worker 节点配置 BIOS。

1.3.3. Web 控制台

1.3.3.1. 从 Node 页面访问节点日志

在这个版本中，管理员可以从 **Node** 页面访问节点日志。要查看节点日志，您可以通过单击 **Logs** 选项卡在单个日志文件和日志日志单元之间切换。

1.3.3.2. 按节点类型划分集群利用率

现在，您可以在集群仪表板上的 **Cluster 使用率** 卡中按节点类型过滤。创建时，其他节点类型将显示在列表中。

1.3.3.3. 用户首选项

在这个版本中，添加了一个**用户首选项**页用于进行自定义设置，如默认项目、视角和拓扑视图。

1.3.3.4. 从项目列表中隐藏默认项目

在这个版本中，您可以从 web 控制台刊头的 **Project** 下拉菜单中隐藏 **default projects**默认项目。在搜索和过滤前，您仍然可以切换为显示 **default projects**。

1.3.3.5. 在 web 控制台中添加用户首选项

在这个版本中，您可以在 web 控制台中添加用户首选项。用户可以选择自己的默认透视图、项目、拓扑和其他首选项。

1.3.3.6. Developer Perspective (开发者视角)

- 现在，您可以通过 Git 存储库导入 devfile、Dockerfile 或构建器镜像来进一步自定义部署。您还可以编辑文件导入类型并选择不同的策略来导入文件。
- 现在，通过开发者控制台中的更新的 **Pipeline builder** 用户界面中的 **Add task** 和 **Quick Search** 来在管道中 添加新任务。用户现在可以添加 **Tekton Hub** 中的任务。
- 要编辑构建配置，您可以使用 **Developer** 视角的 **Builds** 视图中的 **Edit BuildConfig** 选项。用户可以使用 **Form view** 和 **YAML view** 来编辑构建配置。
- 您可以使用拓扑 **Graph view** 的上下文菜单添加服务或创建与 Operator 支持的服务的连接。
- 您可以使用拓扑 **Graph view** 的上下文菜单中的 **+Add** 操作在应用程序组中添加服务或删除服务。
- 现在，OpenShift Pipelines Operator 启用的 **Pipelines Repository list** 视图中提供了对 **pipeline as code** 的初始支持。
- 对拓扑的 **Observe** 页面中的 **Application Monitoring** 部分进行了可用性增强。

1.3.4. IBM Z 和 LinuxONE

在这个版本中，IBM Z 和 LinuxONE 与 OpenShift Container Platform 4.9 兼容。可以使用 z/VM 或 RHEL KVM 进行安装。有关安装说明，请参阅以下文档：

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

主要改进
IBM Z 和 LinuxONE 中的 OpenShift Container Platform 4.9 支持以下新功能：

- Helm
- 支持多个网络接口
- Service Binding Operator

支持的功能
IBM Z 和 LinuxONE 也支持以下功能：

- 目前，支持以下 Operator：
  - Cluster Logging Operator
  - NFD Operator
  - OpenShift Elasticsearch Operator

    - Local Storage Operator
    - Service Binding Operator
- 加密数据存储在 etcd 中
- 多路径（Multipathing）
- 使用 iSCSI 的持久性存储
- 使用本地卷的持久性存储（本地存储 Operator）
- 使用 hostPath 的持久性存储
- 使用 Fibre Channel 持久性存储
- 使用 Raw Block 的持久性存储
- OVN-Kubernetes
- 三节点集群支持
- SCSI 磁盘中的 z/VM 模拟 FBA 设备
- 4K FCP 块设备

以下功能仅适用于 IBM Z 和 LinuxONE 上的 OpenShift Container Platform 4.9：

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

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

- 以下 OpenShift Container Platform 技术预览功能不被支持：
    - 精度时间协议 (PTP) 硬件
- 以下 OpenShift Container Platform 功能不被支持：
    - 使用机器健康检查功能自动修复损坏的机器
    - CodeReady Containers (CRC)
    - 在节点上控制过量使用和管理容器密度
    - CSI 卷克隆
    - CSI 卷快照
    - FIPS 加密
    - Multus CNI 插件
    - NVMe
    - OpenShift Metering
    - OpenShift Virtualization

    - 在 OpenShift Container Platform 部署过程中启用 Tang 模式磁盘加密。
- worker 节点必须运行 Red Hat Enterprise Linux CoreOS（RHCOS）
- 必须使用 NFS 或其他支持的存储协议来置备持久性共享存储
- 必须使用本地存储（如 iSCSI、FC 或者带有 DASD、FCP 或 EDEV/FBA 的 LSO）置备持久性非共享存储

1.3.5. IBM Power 系统

在这个版本中，IBM Power Systems 与 OpenShift Container Platform 4.9 兼容。有关安装说明，请参阅以下文档：

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

主要改进
使用 OpenShift Container Platform 4.9 的 IBM Power 系统支持以下新功能：

- Helm
- 支持 Power10
- 支持多个网络接口
- Service Binding Operator

支持的功能
IBM Power 系统还支持以下功能：

- 目前，支持以下 Operator：
    - Cluster Logging Operator
    - NFD Operator
    - OpenShift Elasticsearch Operator
    - Local Storage Operator
    - Cluster Network Operator
    - Service Binding Operator
- 多路径（Multipathing）
- 使用 iSCSI 的持久性存储
- 使用本地卷的持久性存储（本地存储 Operator）
- 使用 hostPath 的持久性存储
- 使用 Fibre Channel 持久性存储
- 使用 Raw Block 的持久性存储

- OVN-Kubernetes
- 4K 磁盘支持
- NVMe
- 加密数据存储在 etcd 中
- 三节点集群支持
- Multus SR-IOV

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

- 以下 OpenShift Container Platform 技术预览功能不被支持：
  - 精度时间协议 (PTP) 硬件
- 以下 OpenShift Container Platform 功能不被支持：
  - 使用机器健康检查功能自动修复损坏的机器
  - CodeReady Containers (CRC)
  - 在节点上控制过量使用和管理容器密度
  - FIPS 加密
  - OpenShift Metering
  - OpenShift Virtualization
  - 在 OpenShift Container Platform 部署过程中启用 Tang 模式磁盘加密。
- worker 节点必须运行 Red Hat Enterprise Linux CoreOS（RHCOS）
- 持久性存储必须是使用本地卷、网络文件系统（NFS）或 Container Storage Interface（CSI）的 Filesystem 类型

1.3.6. 安全性与合规性

1.3.6.1. 使用自定义规则配置审计日志策略

现在，您可以更精细地控制 OpenShift Container Platform 的审计日志记录级别。您可以使用自定义规则为不同的组指定不同的审计策略配置集（**Default**、**WriteRequestBodies**、**AllRequestBodies** 或 **None**）。

如需更多信息，请参阅使用自定义规则配置审计日志策略。

1.3.6.2. 禁用审计日志

现在，您可以使用 **None** audit 策略配置集禁用 OpenShift Container Platform 审计日志记录。

警告

不建议禁用审计日志记录，除非您完全意识到在进行故障排除时无法记录数据的风险。如果禁用审计日志记录且出现支持情况，您可能需要启用审计日志记录并重现问题，才能正确排除故障。

如需更多信息，请参阅禁用审计日志记录。

1.3.6.3. 自定义 OAuth 服务器 URL

现在，您可以自定义内部 OAuth 服务器的 URL。如需更多信息，请参阅自定义内部 OAuth 服务器 URL。

1.3.6.4. 网络绑定磁盘加密 (NBDE)

OpenShift Container Platform 4.9 提供了持续维护 NBDE 配置系统的新程序。NBDE 允许您加密物理和虚拟机上的硬盘驱动器的根卷，而无需在重启机器时手动输入密码。如需更多信息，请参阅关于磁盘加密技术。

1.3.7. etcd

1.3.7.1. 自动轮转 etcd 证书

在 OpenShift Container Platform 4.9 中，etcd 证书会自动轮转，并由系统管理。

1.3.7.2. API 服务器上的额外 TLS 安全配置集设置

Kubernetes API 服务器 TLS 安全配置集设置现在也受到 etcd 的认可。

1.3.8. 网络

1.3.8.1. linuxptp 服务的改进

OpenShift Container Platform 4.9 对 PTP 包括以下更新：

- 新的 **ptp4lConf** 字段
- 将 **linuxptp** 服务配置为边界时钟的新选项

如需更多信息，请参阅 将 linuxptp 服务配置为边界时钟。

1.3.8.2. 使用 PTP 快速事件通知框架监控 PTP 快速事件

现在，裸机集群提供了 PTP 事件的快速事件通知。PTP Operator 会为每个配置的 PTP 网络接口生成事件通知。事件通过 REST API 为在同一节点上运行的应用提供。快速事件通知由 AMQ Interconnect Operator 提供的高级消息队列协议 (AMQP) 消息总线传输。

如需更多信息，请参阅关于 PTP 和时钟同步错误事件。

1.3.8.3. OVN-Kubernetes 集群网络供应商出口 IP 功能在节点间实现平衡

现在，如果为给定命名空间分配多个出口 IP 地址，则 OVN-Kubernetes 的出口 IP 功能现在会在节点间平衡网络流量。每个 IP 地址必须位于不同的节点上。如需更多信息，请参阅为 OVN-Kubernetes 项目配置出口 IP。

1.3.8.4. SR-IOV 容器化数据平面开发套件 (DPDK) 现已正式发布（GA）

容器化数据平面开发套件 (DPDK) 现在在 OpenShift Container Platform 4.9 中是 GA。如需更多信息，请参阅在DPDK 和 RDMA 模式中使用虚拟功能 (VF)。

1.3.8.5. SR-IOV 支持将 vhost-net 与 Fast Datapath DPDK 应用程序搭配使用

SR-IOV 现在支持 vhost-net 用于 Intel 和 Mellanox NIC 上的 Fast Datapath DPDK 应用程序。您可以通过配置 **SriovNetworkNodePolicy** 资源来启用此功能。如需更多信息，请参阅 SR-IOV 网络配置对象。

1.3.8.6. SR-IOV 支持单节点集群

单节点集群支持 SR-IOV 硬件和 SR-IOV Network Operator。请注意，配置 SR-IOV 网络设备会导致单个节点重新引导，并且您必须为 Operator 配置 **disableDrain** 字段。如需更多信息，请参阅配置 SR-IOV Network Operator。

1.3.8.7. SR-IOV 支持的硬件

OpenShift Container Platform 4.9 添加了对其他 Broadcom 和 Intel 硬件的支持。

- Broadcom BCM57414 和 BCM57508
- Intel E810-CQDA2、E810-XXVDA2 和 E810-XXVDA4

如需更多信息，请参阅支持的设备。

1.3.8.8. MetalLB 负载均衡器

此发行版本引入了 MetalLB Operator。安装和配置 MetalLB Operator 后，您可以部署 MetalLB，为裸机集群上的服务提供原生负载均衡器实现。其他类似裸机的内部基础架构也可以受益。

Operator 引入了自定义资源 **AddressPool**。您可以使用 MetalLB 可分配给服务的 IP 地址范围来配置地址池。当您添加类型为 **LoadBalancer** 的服务时，MetalLB 从池中分配 IP 地址。

在这个发行版本中，红帽只支持在第 2 层模式中使用 MetalLB。

如需更多信息，请参阅关于 MetalLB 和 MetalLB Operator。

1.3.8.9. CNI VRF 插件已正式发布

CNI VRF 插件以前在 OpenShift Container Platform 4.7 中作为技术预览功能引进，现在包括在 OpenShift Container Platform 4.9 中。

如需更多信息，请参阅将二级网络分配给 VRF。

1.3.8.10. Ingress 控制器超时配置参数

此发行版本为 Ingress Controller **tuningOptions** 参数引入了六个超时配置：

- **clientTimeout** 指定连接在等待客户端响应时保持打开的时长。
- **serverFinTimeout** 指定连接在等待服务器响应关闭连接时保持打开的时长。
- **serverTimeout** 指定连接在等待服务器响应时保持打开的时长。
- **clientFinTimeout** 指定连接在等待客户端响应关闭连接时保持打开的时长。
- **tlsInspectDelay** 指定路由器可以保存数据以查找匹配的路由的时长。
- **tunnelTimeout** 指定隧道连接（包括 WebSocket 连接）在隧道闲置期间保持打开的时长。

如需更多信息，请参阅 Ingress 控制器配置参数。

1.3.8.11. 双向 TLS 身份验证

现在，您可以通过设置 **spec.clientTLS** 将 Ingress Controller 配置为启用 mutual TLS (mTLS)身份验证。**clientTLS** 字段指定 Ingress Controller 的配置，以验证客户端证书。

如需更多信息，请参阅配置双向 TLS 身份验证。

1.3.8.12. 自定义 HAProxy 错误代码响应页面

集群管理员可以为 503、404 或两个错误页面指定自定义 HTTP 错误代码响应页面。

如需更多信息，请参阅自定义 HAProxy 错误代码响应页面。

1.3.8.13. provisioningNetworkInterface 配置设置是可选的

在 OpenShift Container Platform 4.9 中，安装程序置备的集群的 **provisioningNetworkInterface** 配置设置是可选的。**provisioningNetworkInterface** 配置设置标识用于 **provisioning** 网络的 NIC 名称。在 OpenShift Container Platform 4.9 中，您也可以在 **install-config.yml** 文件中指定 **bootMACAddress** 配置设置，它可让 Ironic 识别连接到 **provisioning** 网络并与其绑定的 NIC 的 IP 地址。您还可以在 provisioning 自定义资源中省略 **provisioningInterface** 配置设置，以便 provisioning 自定义资源使用 **bootMACAddress** 配置设置。

1.3.8.14. DNS Operator managementState

在 OpenShift Container Platform 4.9 中，现在可以更改 DNS Operator **managementState**。默认情况下，DNS Operator 的 **managementState** 设置为 **Managed**，这意味着 DNS Operator 会主动管理其资源。您可以将其更改为 **Unmanaged**，这意味着 DNS Operator 不管理其资源。

以下是更改 DNS Operator **managementState** 的用例：

- 您是一个开发者，希望测试配置更改来查看它是否解决了 CoreDNS 中的问题。您可以通过将 **managementState** 设置为 **Unmanaged** 来停止 DNS Operator 覆盖更改。
- 您是一个集群管理员，报告了 CoreDNS 的问题，但在解决这个问题前需要应用一个临时解决方案。您可以将 DNS Operator 的 **managementState** 字段设置为 **Unmanaged** 以应用临时解决方案。

如需更多信息，请参阅更改 DNS Operator managementState。

1.3.8.15. 负载均衡器配置，作为 RHOSP 上集群的云供应商选项

对于在 RHOSP 上运行的集群，现在可以将 Octavia 配置为云供应商选项进行负载均衡。

如需更多信息，请参阅设置云供应商选项。

1.3.8.16. 添加了对 TLS 1.3 和 Modern 配置集的支持

此发行版本添加了对 TLS 1.3 和 HAProxy 中的 **Modern** 配置集的 Ingress Controller 支持。

如需更多信息，请参阅 Ingress Controller TLS 安全配置集。

1.3.8.17. 用于 HTTP Strict Transport Security 要求的全局准入插件

集群管理员可以在每个域基础上配置 HTTP Strict Transport Security (HSTS) 验证，并为路由器添加准入插件，名为 **route.openshift.io/RequiredRouteAnnotations**。如果集群管理员将这个插件配置为强制 HSTS，那么任何新创建的路由都必须配置一个兼容的 HSTS 策略，该策略会根据集群 Ingress 配置上的全局设置进行验证，名为 **ingresses.config.openshift.io/cluster**。

如需更多信息，请参阅 HTTP 严格传输安全性。

1.3.8.18. Ingress 空请求策略

在 OpenShift Container Platform 4.9 中，您可以通过设置 **logEmptyRequests** 和 **HTTPEmptyRequests** 字段将 Ingress Controller 配置为记录或忽略空请求。

如需更多信息，请参阅 Ingress 控制器配置参数。

1.3.8.19. 在 web 控制台中创建网络策略

使用 **cluster-admin** 角色登录到 web 控制台，现在您可以从控制台中的表单在集群中的任何命名空间中创建新网络策略。在以前的版本中，这只能在 YAML 中直接完成。

1.3.9. 存储

1.3.9.1. 使用 AWS EBS CSI 驱动程序 operator 的持久性存储已正式发布

OpenShift Container Platform 可以使用 AWS Elastic Block Store（EBS）的 Container Storage Interface（CSI）驱动来置备持久性卷（PV）。此功能以前在 OpenShift Container Platform 4.5 中作为技术预览功能，现在在 OpenShift Container Platform 4.9 中正式发布并启用。

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

1.3.9.2. 使用 Azure Stack Hub CSI Driver Operator 的持久性存储（通用可用性）

OpenShift Container Platform 可以使用 Azure Stack Hub 存储的 CSI 驱动程序置备 PV。Azure Stack Hub 是 Azure Stack 产品组合的一部分，允许您在内部环境中运行应用程序，并在数据中心内提供 Azure 服务。管理此驱动程序的 Azure Stack Hub CSI Driver Operator 对 4.9 来说是新的，并正式发布。

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

1.3.9.3. 使用 AWS EFS CSI Driver Operator 的持久性存储（技术预览）

OpenShift Container Platform 可以使用 AWS Elastic File Service (EFS) 的 CSI 驱动程序置备 PV。管理此驱动程序的 AWS EFS CSI Driver Operator 只是一个技术预览。

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

1.3.9.4. 自动 CSI 迁移支持 GCE（技术预览）

从 OpenShift Container Platform 4.8 开始，树内卷插件自动迁移到其等同的 CSI 驱动程序作为一个技术预览功能提供。此功能现在支持从 Google Compute Engine Persistent Disk (GCE PD) in-tree 插件自动迁移到 Google Cloud Platform (GCP) Persistent Disk CSI 驱动程序。

如需更多信息，请参阅 CSI 自动迁移。

1.3.9.5. 自动 CSI 迁移支持 Azure Disk（技术预览）

从 OpenShift Container Platform 4.8 开始，树内卷插件自动迁移到其等同的 CSI 驱动程序作为一个技术预览功能提供。此功能现在支持从 Azure Disk in-tree 插件自动迁移到 Azure Disk CSI 驱动程序。

如需更多信息，请参阅 CSI 自动迁移。

1.3.9.6. VMware vSphere CSI Driver Operator 会自动创建存储策略（技术预览）

vSphere CSI Operator Driver 存储类现在使用 vSphere 的存储策略。OpenShift Container Platform 会自动创建一个存储策略，该策略以云配置中配置的数据存储为目标。

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

1.3.9.7. 为 Local Storage Operator 提供新的指标

OpenShift Container Platform 4.9 为 Local Storage Operator 提供了以下新指标：

- **lso_discovery_disk_count**：每个节点中发现的设备总数
- **lso_lvset_provisioned_PV_count**: **LocalVolumeSet** 对象创建的 PV 总数
- **lso_lvset_unmatched_disk_count**: Local Storage Operator 没有选择进行置备的磁盘总数，因为不匹配条件
- **lso_lvset_orphaned_symlink_count**: 使用 PV 的设备数，它们不再与 **LocalVolumeSet** 对象标准匹配
- **lso_lv_orphaned_symlink_count** ：包含 PV 的设备数，它们不再符合 **LocalVolume** 对象标准
- **lso_lv_provisioned_PV_count**: **LocalVolume**置备的 PV 总数

如需更多信息，请参阅使用本地卷的持久性存储。

1.3.9.8. 现在提供了 oVirt CSI 驱动程序重新定义大小功能

OpenShift Container Platform 4.9 为 oVirt CSI Driver 添加了重新定义大小功能，用户可以增加其现有持久性卷声明 (PVC) 的大小。在这个功能前，用户必须创建增大大小的新 PVC，并将所有内容从旧的持久性卷 (PV) 移到新 PV，这可能会导致数据丢失。现在，用户可以编辑现有的 PVC，oVirt CSI Driver 将调整底层 oVirt 磁盘的大小。

1.3.10. 容器镜像仓库（Registry）

1.3.10.1. Image Registry 在 Azure Stack Hub 安装中使用 Azure Blob Storage

在 OpenShift Container Platform 4.9 中，集成的 Image Registry 对于使用用户置备的基础架构在 Microsoft Azure Stack Hub 上安装的集群使用 Azure Blob Storage。

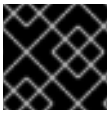
详情请参阅使用 ARM 模板在 Azure Stack Hub 上安装集群。

1.3.11. Operator 生命周期

以下新功能和增强功能与使用 Operator Lifecycle Manager (OLM) 运行 Operator 相关。

1.3.11.1. Operator Lifecycle Manager 升级到 Kubernetes 1.22

从 OpenShift Container Platform 4.9 开始，Operator Lifecycle Manager (OLM) 支持 Kubernetes 1.22。因此，大量 **v1beta1** API 已被删除并更新至 **v1**。依赖于删除的 **v1beta1** API 的 Operator 不会在 OpenShift Container Platform 4.9 上运行。在将集群升级到 OpenShift Container Platform 4.9 之前，集群管理员应需要将其安装的 Operator 升级到**最新**频道。



重要

Kubernetes 1.22 对 **CustomResorceDefinition** API 的 **v1** 引入了几个显著的更改。

1.3.11.2. 基于文件的目录

基于文件的目录是 Operator Lifecycle Manager (OLM) 中目录格式的最新迭代。格式是之前基于纯文本（JSON 或 YAML）和声明式配置演进，现已弃用 SQLite 数据库格式，并且完全向后兼容。此格式的目标是启用 Operator 目录编辑、可组合性和可扩展性。

如需有关基于文件的目录规格的更多信息，请参阅 Operator Framework 打包格式。

有关使用 **opm** CLI 创建基于文件的目录的说明，请参阅管理自定义目录。

1.3.11.3. 对单节点 OpenShift 的 Operator Lifecycle Manager 支持

Operator Lifecycle Manager (OLM) 现在包括在 Single Node OpenShift (SNO) 集群中，启用自助服务 Operator 安装。

1.3.11.4. 对集群管理员错误报告功能的增强

对于管理员，应该可以在不需要了解各种低级别 API 的交互过程或访问 OLM pod 日志的情况下，就可以成功调试这些问题，所以 OpenShift Container Platform 4.9 在 OLM 中引入了以下增强功能，以便为管理员提供更易理解的错误报告和消息：

1.3.11.4.1. 更新 Operator 组状态条件

在以前的版本中，如果命名空间包含多个 Operator 组或找不到服务帐户，Operator 组的状态将无法报告错误。在这个版本中，这些场景更新 Operator 组的状态条件以报告错误。

1.3.11.4.2. 指明安装计划失败的原因

在这个发行版本前，如果安装计划失败，订阅条件不会说明发生失败的原因。现在，如果安装计划失败，订阅状态条件表示失败的原因。

1.3.11.4.3. 指示解决订阅状态冲突

由于依赖项解析会将命名空间中的所有组件视为单个单元，如果发生解析失败，命名空间上的所有订阅现在都会显示错误。

1.3.11.5. 自定义目录源的镜像模板

为避免集群升级可能会使 Operator 安装处于不受支持的状态或没有持续更新路径，您可以启用自动更改 Operator 目录的索引镜像版本作为集群升级的一部分。

将 **olm.catalogImageTemplate** 注解设置为您的目录镜像名称，并在构建镜像标签的模板时使用一个或多个 Kubernetes 集群版本变量。

如需更多信息，请参阅自定义目录源的镜像模板。

1.3.12. Operator 开发

以下新功能和增强功能与使用 Operator SDK 开发 Operator 相关。

1.3.12.1. 高可用性或单节点集群检测和支持

OpenShift Container Platform 集群能够以高可用性 (HA) 模式配置，该模式使用多个节点，或者在非 HA 模式中使用单一节点。单一节点集群（也称为单节点 OpenShift(SNO)）可能会具有更为保守的资源限制。因此，在单一节点集群中安装 Operator 务必要进行相应调整，并且仍然运行良好。

通过访问 OpenShift Container Platform 中提供的集群高可用性模式 API，Operator 作者可使用 Operator SDK 来让 Operator 检测集群的基础架构拓扑，不论是 HA 模式还是非 HA 模式。可以开发使用检测到的集群拓扑的自定义 Operator 逻辑，以自动将 Operator 及其管理的任何 Operands 或工作负载的资源要求切换到最适合拓扑的配置集。

如需更多信息，请参阅高可用性或单节点集群检测和支持。

1.3.12.2. 对网络代理的 Operator 支持

Operator 作者现在可以开发支持网络代理的 Operator。使用代理的 Operator 支持检查 Operator 部署中的环境变量，并将变量传递给所需的 Operands。集群管理员配置对 Operator Lifecycle Manager (OLM) 处理的环境变量的代理支持。如需更多信息，请参阅 Operator SDK 指南来使用 Go、Ansible 和 Helm 开发 Operator。

1.3.12.3. 验证从 Kubernetes 1.22 中删除的 API 的捆绑包清单

现在，您可以使用 **bundle validate** 子命令的 Operator Framework 套件检查从 Kubernetes 1.22 中删除的 API 捆绑包清单。

例如：

```
$ operator-sdk bundle validate .<bundle_dir_or_image> \
  --select-optional suite=operatorframework \
  --optional-values=k8s-version=1.22
```

如果您的捆绑包清单包含从 Kubernetes 1.22 中删除的 API，则命令会显示警告消息。警告消息指明您需要迁移的 API 以及 Kubernetes API 迁移指南的链接。

如需更多信息，请参阅从 Kubernetes 1.22 中删除的 beta API 列表 和 Operator SDK CLI 。

1.3.13. Builds

作为使用 OpenShift Container Platform 进行构建的开发人员，您可以使用以下新功能：

- 您可以挂载构建卷，为运行的构建授予您不想在输出容器镜像中保留的信息的访问权限。构建卷可以提供存储库凭据等敏感信息，这些凭据仅在构建时需要这些凭据或配置。构建卷与构建输入不同，后者的数据可以保留在输出容器镜像中。

- 您可以根据 BuildConfig 状态中记录的信息，配置镜像更改来触发构建。这样，您可以在 GitOps 工作流中的构建中使用 **ImageChange** 触发器。

1.3.14. 镜像

1.3.14.1. 通配符域作为 registry 源

此发行版本引入了在镜像 registry 设置中使用通配符域作为 registry 源的支持。使用通配符域，如 ***.example.com**，您可以将集群设置为从多个子域推送和拉取镜像，而无需手动输入每个子域的镜像。如需更多信息，请参阅镜像控制器配置参数。

1.3.15. 机器 API

1.3.15.1. Red Hat Enterprise Linux (RHEL) 8 现在支持计算机器

从 OpenShift Container Platform 4.9 开始，计算机器可以使用 Red Hat Enterprise Linux (RHEL) 8.4。在以前的版本中，计算机器不支持 RHEL 8。

您无法将 RHEL 7 计算机器升级到 RHEL 8。您必须部署新的 RHEL 8 主机，并且应该删除旧的 RHEL 7 主机。

1.3.16. 节点

1.3.16.1. 调度程序配置集 GA

使用调度程序配置集调度 pod 现已正式发布。这是配置调度程序策略的替代。可用的调度程序配置集如下：

- **LowNodeUtilization**：此配置集尝试在节点间平均分配 pod，以获得每个节点的资源用量较低。

- **HighNodeUtilization**：此配置集会尽量将 pod 放置到尽量少的节点中，以最小化每个节点用量。

- **NoScoring**：这是一个低延迟配置集，通过禁用所有分数（score）插件来实现最快的调度周期。这可能会为更快的调度决策提供更好的要求。

如需更多信息，请参阅使用调度程序配置集调度 pod。

1.3.16.2. 新的 descheduler 配置集和自定义

descheduler 配置集现在可用：

- **SoftTopologyAndDuplicates**：此配置集与 **TopologyAndDuplicates** 相同，但具有软拓扑约束的 pod（如 **whenUnsatisfiable: ScheduleAnyway** ）也被视为驱除。

- **EvictPodsWithLocalStorage**：此配置集允许带有本地存储的 pod 有资格被驱除。

- **EvictPodsWithPVC**：此配置集允许带有持久性卷声明的 pod 有资格驱除。

您还可以自定义 **LifecycleAndUtilization** 配置集的 pod 生命周期值。

如需更多信息，请参阅使用 descheduler 驱除 pod。

1.3.16.3. 多次登录到同一 registry

在将 **docker/config.json** 文件配置为允许 pod 从私有 registry 拉取镜像时，您现在可以列出同一 registry 中的特定存储库，每个存储库都有特定于该 registry 路径的凭证。在以前的版本中，您只能从给定的 registry 中列出一个存储库。现在，您还可以使用特定命名空间定义 registry。

1.3.16.4. 增强的节点资源的监控

节点相关的指标和警报已被改进，您可以更早地表明节点何时受到影响。

1.3.16.5. 使用 Node Health Check Operator 部署节点健康检查（技术预览）

您可以使用 Node Health Check Operator 来部署 **NodeHealthCheck** 控制器。控制器识别不健康的节点，并使用 Poison Pill Operator 来修复不健康的节点。

1.3.17. Red Hat OpenShift Logging

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

1.3.18. 监控

此版本的监控堆栈包括以下新功能和修改后的功能：

1.3.18.1. 监控堆栈组件和依赖项

监控堆栈组件和依赖项的更新包括：

- Prometheus 更新到 2.29.2
- Prometheus Operator 更新到 0.49.0
- Prometheus Adapter 更新到 0.9.0
- Alertmanager 更新到 0.22.2
- Thanos 更新到 0.22.0

1.3.18.2. 警报规则

- New
  - **HighlyAvailableWorkloadIncorrectlySpread** 告知您，当两个具有高可用性监控组件的实例在同一节点上运行并附加持久性卷时，可能会出现的问题。
  - 当节点内核没有可用的文件描述符时，**NodeFileDescriptorLimit** 会触发警报。警告级别警报会以超过 70% 的使用量触发，关键级别的警报会触发超过 90% 的使用量。
  - **PrometheusLabelLimitHit** 检测目标何时超过定义的标签限值。
  - **PrometheusTargetSyncFailure** 会在 Prometheus 无法同步目标时检测。
  - 所有关键警报规则都包含到 runbooks 的链接。

- 增强

  - **AlertManagerReceiversNotConfigured** 和 **KubePodCrashLooping** 现在包含较少的假正状态。

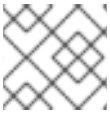
  - **KubeCPUOvercommit** 和 **KubeMemoryOvercommit** 现在在非同构环境中更强大。

  - **NodeFilesystemAlmostOutOfSpace** 警报规则的 **for** 时长设置已从 1 小时改为 30 分钟，以便系统在磁盘空间低时更快地检测。

  - **KubeDeploymentReplicasMismatch** 现在会如预期触发。在以前的版本中，此警报没有触发。

  - 以下警报现在包含一个 **namespace** 标签：

    - **AlertmanagerReceiversNotConfigured**
    - **KubeClientErrors**
    - **KubeCPUOvercommit**
    - **KubeletDown**
    - **KubeMemoryOvercommit**
    - **MultipleContainersOOMKilled**
    - **ThanosQueryGrpcClientErrorRate**
    - **ThanosQueryGrpcServerErrorRate**
    - **ThanosQueryHighDNSFailures**
    - **ThanosQueryHttpRequestQueryErrorRateHigh**
    - **ThanosQueryHttpRequestQueryRangeErrorRateHigh**
    - **ThanosSidecarPrometheusDown**
    - **Watchdog**



注意

红帽不保证指标、记录规则或警报规则的向后兼容。

1.3.18.3. Alertmanager

- 您可以为平台和用户定义的项目监控堆栈添加和配置额外的外部 Alertmanager。
- 您可以禁用本地 Alertmanager 实例。

1.3.18.4. Prometheus

- 您可以为 Prometheus 中的平台监控和用户定义的项目启用和配置远程写入存储。通过此功能，您可以将最接近的指标发送到长期存储。

- 要减少 Prometheus 的总内存消耗，以下同时带有空 **pod** 和 **namespace** 标签的 cAdvisor 指标被丢弃：
  - **container_fs_.***
  - **container_spec_.***
  - **container_blkio_device_usage_total**
  - **container_file_descriptors**
  - **container_sockets**
  - **container_threads_max**
  - **container_threads**
  - **container_start_time_seconds**
  - **container_last_seen**
- 如果没有为平台监控配置持久性存储，升级和集群中断可能会导致数据丢失。当系统检测到没有为平台监控配置持久性存储时，**Degraded** 条件中增加了警告消息。
- 您可以通过在项目中添加 **openshift.io/user-monitoring: "false"** 标签，从 **openshift-user-workload-monitoring** 项目中排除单独用户定义的项目。
- 您可以为 **openshift-user-workload-monitoring** 项目配置 **enforcedTargetLimit** 参数，以设置提取的目标数量的整体限制。

1.3.18.5. 删除 Prometheus UI 链接

第三方 Prometheus UI 的链接已从 OpenShift Container Platform Web 控制台的 **Observe → Metrics** 页面中删除。您仍然可以通过导航到 **openshift-monitoring** 项目中的 **Networking → Routes** 页面来访问 **Administrator 视角** 中 Web 控制台中的 Prometheus UI 的路由。

1.3.18.6. Grafana

因为运行默认 Grafana 仪表板可能会从用户工作负载中获取资源，所以您可以禁用 Grafana 仪表板部署。

1.3.19. Metering

此发行版本删除了 OpenShift Container Platform Metering Operator。

1.3.20. 可伸缩性和性能

1.3.20.1. 特殊资源 Operator（技术预览）

现在，您可以使用特殊资源 Operator (SRO) 来帮助管理现有 OpenShift Container Platform 集群上的内核模块和驱动程序的部署。目前，这是一个技术预览功能。

如需更多信息，请参阅关于特殊资源 Operator。

1.3.20.2. 内存管理器功能（技术预览）

现在，在节点上使用以下拓扑管理器策略之一配置的 pod 都默认启用 Memory Manager 功能：

- **single-numa-node**
- **restricted**

如需更多信息，请参阅拓扑管理器策略。

1.3.20.3. 其他用于延迟测试的工具

OpenShift Container Platform 4.9 引入了两个额外的工具来测量系统延迟：

- **hwladetect** 测量裸机硬件能够达到的基准
- **cyclictest** 在 **hwlatdetect** 通过验证后会调度一个重复的计时器，并测量所需与实际触发时间之间的差别

如需更多信息，请参阅运行延迟测试。

1.3.20.4. 集群最大限制

针对 OpenShift Container Platform 4.9 的集群最大限制指导信息已更新。

重要

此发行版本没有针对 OVN-Kubernetes 测试执行大规模测试。

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

1.3.20.5. Zero touch provisioning（技术预览）

OpenShift Container Platform 4.9 支持 zero touch provisioning (ZTP)，它允许您在远程站点使用裸机设备声明配置来置备新的边缘站点。ZTP 在基础架构部署中使用 GitOps 部署实践集。GitOps 使用 Git 存储库中存储的声明性规范（如 YAML 文件和其他定义的模式）来实现这些任务，从而提供用于部署基础架构的框架。Open Cluster Manager (OCM) 将声明性输出用于多站点部署。如需更多信息，请参阅大规模配置边缘站点。

1.3.21. Insights Operator

1.3.21.1. 导入 RHEL 简单内容访问证书（技术预览）

在 OpenShift Container Platform 4.9 中，Insights Operator 可以从 Red Hat OpenShift Cluster Manager 导入 RHEL Simple Content Access (SCA) 证书。

如需更多信息，请参阅*使用 Insights Operator 导入 RHEL Simple Content Access 证书*。

1.3.21.2. 深入了解 Operator 数据收集功能的增强

在 OpenShift Container Platform 4.9 中，Insights Operator 会收集以下附加信息：

- 集群中的所有 **MachineConfig** 资源定义。
- 在集群中安装的 **PodSecurityPolicies** 的名称。

- 如果已安装，**ClusterLogging** 资源定义。
- 如果 **SamplesImagestreamImportFailing** 警报触发，则来自 **openshift-cluster-samples-operator** 命名空间中的 **ImageStream** 定义和容器日志的最后 100 行。

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

1.3.22. 认证和授权

1.3.22.1. 以手动模式支持带有 Cloud Credential Operator 的 Microsoft Azure Stack Hub

在这个版本中，可以通过以手动模式配置 Cloud Credential Operator (CCO) 在 Microsoft Azure Stack Hub 上安装。

如需更多信息，请参阅使用手动模式。

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

要查看 OpenShift 沙盒容器、新功能、错误修复、已知问题以及异步勘误更新，请参阅 OpenShift 沙盒容器 1.1 发行注记。

1.4. 主要的技术变化

OpenShift Container Platform 4.9 包括以下显著的技术更改。

自动清理 etcd 数据
在 OpenShift Container Platform 4.9 中，etcd 数据由 etcd Operator 自动进行碎片整理。

Octavia OVN NodePort 更改
在以前的版本中，在 Red Hat OpenStack Platform (RHOSP) 部署中，在 NodePort 上打开流量受节点子网的 CIDR 的限制。为了支持使用 Octavia Open Virtual Network (OVN) 供应商的 LoadBalancer 服务，允许 NodePort 流量到 master 和 worker 节点的安全组规则现在改为打开 **0.0.0.0/0**。

OpenStack Platform LoadBalancer 配置更改
Red Hat OpenStack Platform (RHOSP) 云供应商 LoadBalancer 配置现在默认为 **use-octavia=True**。此规则的一个例外是带有 Kuryr 的部署，在这种情况下，**use-octavia** 被设置为 **false**，因为 Kuryr 会自行处理 LoadBalancer 服务。

Ingress Controller 升级到 HAProxy 2.2.15
OpenShift Container Platform Ingress Controller 升级到 HAProxy 版本 2.2.15。

CoreDNS 更新至版本 1.8.4
在 OpenShift Container Platform 4.9 中，CoreDNS 使用版本 1.8.4，其中包括程序错误修正。

为云供应商实施云控制器管理器
管理云供应商部署的 Kubernetes 控制器管理器不包括作为供应商对 Azure Stack Hub 的支持。由于使用云控制器管理器是与底层云平台交互的首选方法，因此没有添加此支持的计划。因此，OpenShift Container Platform 中的 Azure Stack Hub 实施使用云控制器管理器。

另外，此发行版本支持使用云控制器管理器用于 Amazon Web Services (AWS)、Microsoft Azure 和 Red Hat OpenStack Platform (RHOSP)（技术预览）。任何添加到 OpenShift Container Platform 的新云平台支持也将使用云控制器管理器。

如需了解更多有关云控制器管理器的信息，请参阅有关此组件的 Kubernetes 文档。

要管理云控制器管理器和云节点管理器部署和生命周期，本发行版本引入了 Cluster Cloud Controller Manager Operator。

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

执行 canary rollout 更新
在 OpenShift Container Platform 4.9 中引入了一个新的执行 Canary rollout 更新的过程。有关此过程的详细概述，请参阅执行 Canforming rollout 更新。

支持大型 Operator 捆绑包
Operator Lifecycle Manager (OLM) 现在使用大量元数据（如大型自定义资源定义 (CRD)清单）压缩 Operator 捆绑包，使其保持在 etcd 设置的 1 MB 限制下。

减少了 Operator Lifecycle Manager 的资源使用量
Operator Lifecycle Management (OLM) 目录 pod 现在更高效，使用较少的 RAM。

Operator 的 "Extras" 公告的默认更新频道
附带 OpenShift Container Platform "Extras"公告（如 RHBA-2021:3760 ）的 Operator 会发布在红帽提供的目录中，并在 Operator Lifecyle Manager(OLM)上运行。从 OpenShift Container Platform 4.9 开始，除了特定于版本 **4.9** 频道外，这些 Operator 现在包含在 **stable** 更新频道中。

对于 OpenShift Container Platform 4.9 及将来的发行版本，**stable** 将是这些 Operator 的默认频道。集群管理员应使用 **stable** 频道，以便在以后进行集群升级时不再需要为 OLM 中这些 Operator 更改更新频道。

如需有关基于 OLM 的 Operator 的更多信息，请参阅红帽提供的 Operator 目录和了解 OperatorHub。有关 OLM 中更新频道的更多信息，请参阅升级已安装的 Operator。

Operator SDK v1.10.1
OpenShift Container Platform 4.9 支持 Operator SDK v1.10.1。请参阅安装 Operator SDK CLI 来安装或更新到这个最新版本。

注意

Operator SDK v1.10.1 支持 Kubernetes 1.21。

如果您之前使用 Operator SDK v1.8.0 创建或维护了任何 Operator 项目，请参阅升级较新版本的 Operator SDK 版本的项目，以确保您的项目已升级以保持与 Operator SDK v1.10.1 的兼容性。

1.5. 弃用和删除的功能

之前版本中的一些功能已被弃用或删除。

弃用的功能仍然包含在 OpenShift Container Platform 中，并将继续被支持。但是，这个功能会在以后的发行版本中被删除，且不建议在新的部署中使用。有关 OpenShift Container Platform 4.9 中已弃用并删除的主要功能的最新列表，请参考下表。表后列出了更详细的、已弃用和删除的功能信息。

在下表中，被标记为以下状态的功能：

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

表 1.1. 过时和删除的功能

功能	OCP 4.7	OCP 4.8	OCP 4.9
软件包清单格式（Operator 框架）	DEP	REM	REM
Operator 目录的 SQLite 数据库格式	GA	GA	DEP
oc adm catalog build	DEP	REM	REM
oc adm catalog mirror 的 **--filter-by-os** 标记	DEP	REM	REM
v1beta1 CRD	DEP	DEP	REM
Docker Registry v1 API	DEP	DEP	REM
Metering Operator	DEP	DEP	REM
调度程序策略	DEP	DEP	DEP
Cluster Samples Operator 的 **ImageChangesInProgress** 条件	DEP	DEP	DEP
Cluster Samples Operator 的 **MigrationInProgress** 条件	DEP	DEP	DEP
使用不带有 **apiVersion** 组的 **v1** 用于 OpenShift Container Platform 资源	DEP	DEP	REM
在 RHCOS 中使用 **dhclient**	DEP	DEP	REM
Cluster Loader	GA	DEP	DEP
使用自己的 RHEL 7 计算机器	DEP	DEP	DEP
Builds 的 **BuildConfig** spec 中的 **lastTriggeredImageID** 字段	GA	DEP	REM
Jenkins Operator	TP	DEP	DEP
基于 Prometheus 的 HPA 定制 metrics adapter	TP	REM	REM
vSphere 6.7 更新 2 或更早版本以及虚拟硬件版本 13	GA	GA	DEP
Red Hat Virtualization(RHV)的 **instance_type_id** 安装配置参数	DEP	DEP	DEP

1.5.1. 已弃用的功能

1.5.1.1. Operator 目录的 SQLite 数据库格式

Operator Lifecycle Manager (OLM) 用于目录和索引镜像的 SQLite 数据库格式已弃用，包括相关的 **opm** CLI 命令。建议集群管理员和目录维护人员熟悉 OpenShift Container Platform 4.9 中引入的新的基于文件的目录格式，并开始迁移目录工作流。

注意

OpenShift Container Platform 4.6 及更新的版本为 Red Hat 提供的默认 Operator 目录 当前仍然以 SQLite 数据库格式提供。

1.5.1.2. vSphere 6.7 更新 2 及更早的集群安装以及虚拟硬件版本 13 现已弃用

在 VMware vSphere 版本 6.7 Update 2 或更早版本以及虚拟硬件版本 13 上安装集群已弃用。对这些版本的支持将在 OpenShift Container Platform 以后的版本结束。

现在，硬件版本 15 是 OpenShift Container Platform 中 vSphere 虚拟机的默认版本。硬件版本 15 将是将来的 OpenShift Container Platform 版本中唯一支持的版本。

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

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

1.5.2. 删除的功能

1.5.2.1. Metering

此发行版本删除了 OpenShift Container Platform Metering Operator 功能。

1.5.2.2. 从 Kubernetes 1.22 中删除 Beta API

Kubernetes 1.22 删除了以下已弃用的 **v1beta1** API。迁移清单和 API 客户端以使用 **v1** API 版本。有关迁移已删除 API 的更多信息，请参阅 Kubernetes 文档。

表 1.2. v1beta1 API 从 Kubernetes 1.22 中删除

资源	API	主要变化
APIService	**apiregistration.k8s.io/v1beta1**	否
CertificateSigningRequest	**certificates.k8s.io/v1beta1**	是
ClusterRole	**rbac.authorization.k8s.io/v1beta1**	否
ClusterRoleBinding	**rbac.authorization.k8s.io/v1beta1**	否
CSIDriver	**storage.k8s.io/v1beta1**	否
CSINode	**storage.k8s.io/v1beta1**	否
CustomResourceDefinition	**apiextensions.k8s.io/v1beta1**	是

资源	API	主要变化
入口	extensions/v1beta1	是
入口	networking.k8s.io/v1beta1	是
IngressClass	networking.k8s.io/v1beta1	否
Lease	coordination.k8s.io/v1beta1	否
LocalSubjectAccessReview	authorization.k8s.io/v1beta1	是
MutatingWebhookConfiguration	admissionregistration.k8s.io/v1beta1	是
PriorityClass	scheduling.k8s.io/v1beta1	否
角色	rbac.authorization.k8s.io/v1beta1	否
RoleBinding	rbac.authorization.k8s.io/v1beta1	否
SelfSubjectAccessReview	authorization.k8s.io/v1beta1	是
StorageClass	storage.k8s.io/v1beta1	否
SubjectAccessReview	authorization.k8s.io/v1beta1	是
TokenReview	authentication.k8s.io/v1beta1	否
ValidatingWebhookConfiguration	admissionregistration.k8s.io/v1beta1	是
VolumeAttachment	storage.k8s.io/v1beta1	否

1.5.2.3. 已删除 descheduler v1beta1 API

OpenShift Container Platform 4.9 中删除了 descheduler 的已弃用 **v1beta1** API。使用 descheduler **v1beta1** API 版本将任何资源迁移到 **v1**。

1.5.2.4. 在 RHCOS 中删除了 dhclient

deprecated **dhclient** 二进制文件已从 RHCOS 中删除。从 OpenShift Container Platform 4.6 开始，RHCOS 切换到使用 **initramfs** 中的 **NetworkManager** 在早期引导过程中配置网络。改为使用 **NetworkManager** 内部 DHCP 客户端进行网络配置。如需更多信息，请参阅 BZ#1908462。

1.5.2.5. 停止更新 lastTriggeredImageID 字段并忽略它

当 **buildConfig.spec.triggers[i].imageChage** 引用的 **ImageStreamTag** 指向一个新镜像时，当前发行版本会停止更新 **buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID**。此发行版本更新了 **buildConfig.status.imageChangeTriggers[i].lastTriggeredImageID** 字段。

另外，Build Image Change Trigger 控制器会忽略 **buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID** 字段。

现在，Build Image Change Trigger 控制器会基于 **buildConfig.status.imageChangeTriggers[i].lastTriggeredImageID** 字段，以及其现在与 **buildConfig.spec.triggers[i].imageChange** 中引用的 **ImageStreamTag** 的镜像 ID 的比较进行构建。

因此，更新需要检查 **buildConfig.spec.triggers[i].imageChange.lastTriggeredImageID** 的脚本和作业。(BUILD-190)

1.5.2.6. 使用没有 apiVersion 组的 v1 用于 OpenShift Container Platform 资源

对于 OpenShift Container Platform 资源中使用没有 **apiVersion** 组的 **v1** 的支持已被删除。包含 ***.openshift.io** 的每个资源都必须与 API index 中找到的 **apiVersion** 值匹配。

1.6. 程序错误修复

API 服务器和身份验证

- 在以前的版本中，加密条件可能会无限期地保留，并报告为某些 Operator 的降级条件。现在，过时的加密条件被正确清除，不再报告不正确。(BZ#1974520)

- 在以前的版本中，API 服务器客户端证书的 CA 在集群生命周期早期轮转，这会阻止 Authentication Operator 创建证书签名请求 (CSR)，因为以前具有相同名称的 CSR 仍然存在。在发送 **TokenReview** 请求时，Kubernetes API 服务器无法将自身身份验证到 OAuth API 服务器，这会导致身份验证失败。现在，在 Authentication Operator 创建 CSR 时会使用生成的名称，因此早期为 API 服务器客户端证书轮转 CA 不再会导致身份验证失败。(BZ#1978193)

裸机硬件置备

- 在以前的版本中，因为创建 initContainers 的顺序，metal3 pod 无法下载 Red Hat Enterprise Linux CoreOS (RHCOS) 镜像。这个问题已通过重新排序 initContainers 创建来解决，以便在 **metal3-machine-os-downloader** initContainer 之前创建 **metal-static-ip-set** initContainer。RHCOS 镜像现在可以按预期下载。(BZ#1973724)

- 在以前的版本中，当在裸机中使用配置为使用 **idrac-virtualmedia** 的主机的安装程序置备安装时，该主机的 **bios_interface** 默认被设置为 **idrac-wsman**。这会导致 BIOS 设置不可用，并出现异常。在使用 **idrac-virtualmedia** 时，通过将 **idrac-redfish** 用于默认 **bios_interface** 解决了此问题。(BZ#1928816)

- 在以前的版本中，在 UEFI 模式中，**ironic-python-agent** 在下载 RHCOS 镜像后会创建一个 UEFI 引导装载程序条目。当基于 RHEL 8.4 使用 RHCOS 镜像时，镜像可能无法使用此条目引导，并输出 BIOS 错误屏幕。这个问题由 **ironic-python-agent** 根据镜像中的 CSV 文件配置引导条目来解决，而不使用固定的引导条目。镜像可以正常引导，且无错误。（BZ#1966129）

- 在以前的版本中，如果在 **install-config** 中设置了 **provisioningHostIP**，它会被分配给 metal3 pod，即使 provisioning 网络已被禁用。这个问题已被解决。(BZ#1972753)

- 在以前的版本中，因为 sushy 资源库不匹配，被支持的安装程序无法置备基于 Supermicro X11/X12 的系统。不匹配会导致安装问题，因为无法将虚拟介质附加到 **Inserted** 和 **WriteProtected** 属性，在 **VirtualMedia.InsertMedia** 请求正文中不允许。这个问题已通过修改 sushy 资源库并添加一个条件来解决，以便在不严格要求时停止发送这些可选属性，从而允许安装超过这个时间点。(BZ#1986238)

- 在以前的版本中，置备状态中的一些错误类型会导致取消置备主机。如果置备到裸机主机的镜像不可用，重启 metal3 pod 后会出现这种情况。在这种情况下，主机将进入取消调配状态。这个问题已通过在置备状态下修改错误操作来解决，以便在镜像不可用时，会报告错误但不会启动取消置备。(BZ#1972374)

Builds

- 在 OpenShift Container Platform 及之后的版本中，对错误 BZ#1884270 修剪了 SSH 协议 URL 进行了修复，以尝试提供 SCP 风格的 URL 功能。此错误导致 **oc new-build** 命令无法选择自动源克隆 secret：构建无法使用 build **.openshift.io/sbuild.openshift.io/source-secret-match-uri-1ource-secret-match-uri-1** 注解来将 SSH 密钥与关联的 secret 映射，因此无法执行 git 克隆。在这个版本中恢复了来自 BZ#1884270 的更改，以便构建可以使用注解并执行 git 克隆。

- 在更新前，集群镜像配置的各种允许和块 registry 配置选项可能会阻止 Cluster Samples Operator 创建镜像流。当发生这种情况时，样本 Operator 将自身标记为 **degraded**，这会影响到 OpenShift Container Platform 的常规安装和升级状态。
  在各种情况下，Cluster Samples Operator 可以引导自身为 **removed**。在这个版本中，这些情况包括 镜像控制器配置参数 阻止使用默认镜像 registry 或通过 **samplesRegistry** 设置 指定的镜像 registry 创建镜像流。Operator 状态还指明集群镜像配置何时阻止创建示例镜像流。

Cloud Compute

- 在以前的版本中，当为新服务器创建根卷且该服务器创建成功时，不会触发卷的自动删除，因为没有删除与卷关联的服务器。在某些情况下，这会导致创建许多额外的卷，如果达到卷的配额，则会导致错误。在这个版本中，当服务器创建调用失败时，新创建的根卷会被删除。(BZ#1943378)

- 在以前的版本中，当使用 **instanceType** 的默认值时，Machine API 在 AWS 上创建 **m4.large** 实例。这与 OpenShift Container Platform 安装程序创建的机器的 **m5.large** 实例类型不同。在这个版本中，当指定默认值时，Machine API 会为 AWS 上的新机器创建 **m5.large** 实例。(BZ#1953063)

- 在以前的版本中，计算节点的机器集定义无法指定是否应中继端口。这在要求用户为同一机器配置中继和非中继端口的技术中存在问题。此发行版本添加了一个新的字段 **spec.Port.Trunk = bool**，用户可以更加灵活地确定哪些端口会导致中继。如果没有指定值，**spec.Port.Trunk** 将继承 **spec.Trunk** 的值，创建的中继名称与所用端口的名称匹配。(BZ#1964540)

- 在以前的版本中，Machine API Operator 会持续附加新目标，即使它们已经附加。这些对 AWS API 的过多调用会导致大量错误。在这个版本中，Operator 在尝试附加过程前检查是否需要负载均衡器附加。此更改减少了失败 API 请求的频率。(BZ#1965080)

- 在以前的版本中，当为虚拟机使用自动固定时，属性的名称为 **disabled**、**existing** 或 **adjust**。在这个版本中，名称更好地描述了每个策略，**existing** 被移除，因为它在 oVirt 中被阻断。新属性名为 **none** 和 **resize_and_pin**，这与 oVirt 用户界面一致。(BZ#1972747)

- 在以前的版本中，集群自动扩展无法访问 **csidrivers.storage.k8s.io** 或 **csistoragecapacities.storage.k8s.io** 资源，这会导致权限错误。在这个版本中，更新了分配给集群自动扩展的角色，使其包含这些资源的权限。(BZ#1973567)

- 在以前的版本中，可以使用已删除的节点删除机器。这会导致机器无限期处于删除阶段。在这个版本中，您可以正确地删除处于此状态的机器。(BZ#1977369)

- 使用 **boot-from-volume** 镜像时，如果机器控制器重启，创建新实例会泄漏卷。这会导致永远不会清理之前创建的卷。在这个版本中，确保之前创建的卷被修剪或重复使用。(BZ#1983612)

- 在以前的版本中，Red Hat Virtualization (RHV) 供应商会忽略带有 **br-ex** 名称的 NIC 的机器。因为网络类型的 **OVNKubernetes** 会创建一个带有 **br-ex** 名称的 NIC，这会导致机器无法在 OVN-

Kubernetes 上获取 IP 地址。在这个版本中，可以在 RHV 上安装 OpenShift Container Platform，网络设置为 **OVNKubernetes**。(BZ#1984481)

- 在以前的版本中，当使用代理和自定义 CA 证书组合在 Red Hat OpenStack Platform (RHOSP) 上部署时，集群将无法完全正常工作。在这个版本中，代理设置传递给连接自定义 CA 证书时使用的 HTTP 传输，确保所有集群组件都按预期工作。(BZ#1986540)

Cluster Version Operator

- 在以前的版本中，Cluster Version Operator (CVO) 没有遵循代理配置资源中的 **noProxy** 属性。因此，当只有非代理连接完成时，CVO 会被拒绝访问更新建议或发布签名。现在，当代理资源请求直接、未经代理的访问时，CVO 会直接访问上游更新服务和签名存储。(BZ#1978749)

- 在以前的版本中，Cluster Version Operator (CVO) 从代理资源规格属性加载代理配置，而不是从由 Network Operator 验证的状态属性中加载。因此，任何错误配置的值都会阻止 CVO 访问上游更新服务或签名存储。现在，CVO 只从验证的状态属性加载其代理配置。(BZ#1978774)

- 在以前的版本中，Cluster Version Operator (CVO) 不会删除在清单外添加的卷挂载。因此，pod 创建可能会在卷失败时失败。现在，CVO 会删除清单中没有出现的所有卷挂载。(BZ#2004568)

控制台存储插件

- 在以前的版本中，在使用 Ceph 存储时，控制台存储插件不必要的包括命名空间参数的冗余使用。这个程序错误没有客户可见的影响，但插件已被更新，以避免冗余地使用命名空间。(BZ#1982682)

镜像 Registry

- Operator 用于检查 registry 是否应该使用自定义容限 (tolerations) 检查 **spec.nodeSelector** 而不是 **spec.tolerations**。只有在设置了 **spec.nodeSelector** 时，才会应用 **spec.tolerations** 中的自定义容限。在这个版本中，使用字段 **spec.tolerations** 检查是否存在自定义容限。现在，如果设置了 **spec.tolerations**，Operator 将使用自定义容限。(BZ#1973318)

- **configs.imageregistry** 中的 **spec.managementState** 设置为 **Removed**，这会导致镜像修剪器 pod 生成 CronJob 在 **v1.21** 及更高版本中已弃用的警告，而实际应该使用 **batch/v1**。在这个版本中，OpenShift Container Platform **oc** 中使用 **batch/v1** 更新 **batch/v1beta1**。现在，在镜像修剪器 pod 中不再出现已弃用的 CronJob 的警告。(BZ#1976112)

安装程序

- 在以前的版本中，Azure control plane 节点上的网络接口在接口名称中缺少一个连字符。这与其他平台相比不一致，这会导致问题。现在，已添加了缺少的连字符。现在，无论平台是什么，所有 control plane 节点都以相同的形式命名。(BZ#1882490)

- 现在，您可以在 **install-config.yaml** 文件中为 oVirt 配置 **autoPinningPolicy** 和 **hugepages** 字段 。**autoPinningPolicy** 字段允许您自动设置集群的非统一内存访问 (NUMA) 固定设置和 CPU 拓扑更改。**hugepages** 字段允许您设置虚拟机监控程序的 Hugepages。(BZ#1925203)

- 在以前的版本中，当启用了 FIPS 的情况下使用 Ed25519 SSH 密钥类型时，安装程序不会输出任何错误，即使它不能被使用。现在，安装程序会验证 SSH 密钥类型，在启用了 FIPS 不支持 SSH 密钥类型时输出错误。启用 FIPS 时，只允许 RSA 和 ECDSA SSH 密钥类型。(BZ#1962414)

- 在某些情况下，Red Hat OpenStack Platform (RHOSP) 网络中继中没有包含用来指示中继所属集群的标签。因此，集群删除丢失了中继端口并卡在循环中，直到它们超时为止。现在，删除集群会删除标记的端口是父端口的中继。(BZ#1971518)

- 在以前的版本中，当在 Red Hat OpenStack Platform (RHOSP) 上卸载集群时，安装程序会使用低效算法来删除资源。低效算法导致卸载过程需要的时间超过实际需要的时间。安装程序会使用更有效的算法进行更新，该算法会更快速地卸载集群。(BZ#1974598)

- 在以前的版本中，如果将 **AWS_SHARED_CREDENTIALS_FILE** 环境变量设置为空文件，安装程序会提示提供凭证，然后创建一个 **aws/credentials** 文件，忽略环境变量的值，并可能会覆盖现有的凭证。在这个版本中，安装程序被更新以在指定的 文件中存储凭证。如果指定文件具有无效凭据，安装程序会生成错误，而不是覆盖该文件，并可能导致信息丢失。(BZ#1974640)

- 在以前的版本中，当用户在 Azure 上删除与另一个集群共享资源的集群时遇到错误信息，因此很难了解删除失败的原因。在这个版本中，添加了一个错误消息来解释发生失败的原因。(BZ#1976016)

- 在以前的版本中，因为一个拼写错误，Kuryr 部署会根据错误的要求被检查，这意味着使用 Kuryr 的安装可能会成功，即使它们没有满足 Kuryr 的最低要求。在这个版本中消除了错误，允许安装程序检查正确的要求。(BZ#1978213)

- 在更新前，**keepalived** 的入口检查不包括 fall 和 boost 指令，这意味着单个失败的检查可能会导致入口虚拟 IP 故障。此程序错误修复引进了 fallup 指令，并引发了防止此类故障切换的指令。(BZ#1982766)

Kubernetes API 服务器

- 在以前的版本中，当同时创建部署和镜像流时，可能会出现一个竞争条件，从而导致部署控制器在无限循环中创建副本集。API 服务器的镜像策略插件的职责降低，并同时创建部署，镜像流不再会导致无限副本集。(BZ#1925180)、(BZ#1976775)

- 在以前的版本中，安装程序 pod 和 cert-syncer 容器之间出现了竞争，它们写入相同的路径。这可能会导致某些证书留空，并阻止服务器运行。Kubernetes API 服务器证书现在以原子方式编写，以防止在多个进程间发生竞争。(BZ#1971624)

网络

- 使用 OVN-Kubernetes 集群网络供应商时，逻辑流缓存是在没有任何内存限制的情况下配置的。因此，在某些情况下，高内存压力可能会导致节点不可用。在这个版本中，逻辑流缓存默认配置有 1 GB 内存限制。(BZ#1961757)

- 当使用 OVN-Kubernetes 集群网络供应商时，在稍后升级的 OpenShift Container Platform 4.5 集群中创建的任何网络策略都可能会允许或丢弃意外的流量。在以后的 OpenShift Container Platform 版本中，OVN-Kubernetes 使用不同的约定来管理 IP 地址集，在 OpenShift Container Platform 4.5 中创建的任何网络策略都不使用这个规则。现在，在升级过程中，所有网络策略都会迁移到新约定。(BZ#1962387)

- 对于 OVN-Kubernetes 集群网络供应商，当使用 **must-gather** 检索 Open vSwitch (OVS) 日志时，收集的日志记录数据中没有 **INFO** 日志级别。现在，所有日志级别都包含在 OVS 日志记录数据中。(BZ#1970129)

- 在以前的版本中，性能测试表明，服务控制器指标因为标签要求而显著提高卡片。因此，Open Virtual Network (OVN) Prometheus pod 的内存用量被提升。在这个版本中，标签要求会被删除。现在，服务控制器卡性指标和内存用量会减少。(BZ#1974967)

- 在以前的版本中，**ovnkube-trace** 需要在源和/或目标 pod 中安装 iproute，因为它需要检测接口 **link** 索引。如果没有安装 iproute，这会导致 **ovnkube-trace** 在 pod 上失败。现在，您可以从 **/sys/class/net/<interface>/iflink** 而不是 iproute 中获取 **link** 索引。因此，**ovnkube-trace** 不再需要在源和目标 Pod 中安装 iproute。(BZ#1978137)

- 在以前的版本中，Cluster Network Operator (CNO) 为 **network-check-source** 服务部署了一个服务监控器，以便 Prometheus 发现没有正确的注解和基于角色的访问控制 (RBAC)。因此，该

服务及其指标永远不会填充在 Prometheus 中。现在，正确的注解和 RBAC 被添加到 **network-check-source** 服务的命名空间。现在，Prometheus 会提取服务 **network-check-source** 的指标。(BZ#1986061)

- 在以前的版本中，在使用 IPv6 DHCP 时，节点接口地址可能会使用 **/128** 前缀进行租用。因此，OVN-Kubernetes 使用相同的前缀来推断节点的网络，并通过网关将任何其他地址流量（包括流量到其他集群节点）路由到其他地址流量。在这个版本中，OVN-Kubernetes 会检查节点的路由表，并检查节点的接口地址的更广泛的路由条目，并使用该前缀来推断节点的网络。因此，到其他集群节点的流量不再通过网关路由。(BZ#1980135)

- 在以前的版本中，当集群使用 OVN-Kubernetes Container Network Interface 供应商时，尝试添加带有 IPv6 地址的出口路由器失败。在这个版本中，对 IPv6 的支持被添加到 egress router CNI 插件中，并添加添加出口路由器成功。(BZ#1989688)

节点

- 在以前的版本中，在容器中，CRI-O 不会从 **/proc/mounts** 文件创建到 **/etc/mtab** 文件的符号链接。因此，用户无法在容器的 **/etc/mtab** 文件中查看挂载的设备列表。CRI-O 现在添加符号链接。因此，用户可以查看容器的挂载设备。(BZ#1868221)

- 在以前的版本中，如果在创建 pod 后快速删除 pod，kubelet 可能无法正确清理 pod。这会导致 pod 处于终止状态，并可能会影响升级的可用性。在这个版本中，改进了 pod 生命周期逻辑以避免出现这个问题。(BZ#1952224)

- 在以前的版本中，当系统内存用量超过保留内存的 90% 时，**SystemMemoryExceedsReserved** 警报会触发。因此，集群可能会触发过多的警报。该警报的阈值已更改为触发内存的 95%。(BZ#1980844)

- 在以前的版本中，CRI-O 中的一个程序错误会导致 CRI-O 泄漏它所创建进程的子 PID。因此，如果负载不足，systemd 可以创建大量僵尸进程。如果节点缺少 PID，这可能会导致节点失败。已修复 CRI-O 以防止泄漏。因此，不再创建这些僵尸进程。(BZ#2003197)

OpenShift CLI (oc)

- 在以前的版本中，**oc** 命令行工具在镜像 registry 时崩溃，导致一个 **slice bounds out of range** panic 运行是错误，因为在使用 **--max-components** 参数时在片段上有一个未检查的索引操作。在这个版本中，添加了检查以确保组件检查不会请求范围外索引值，以便在使用 **--max-components** 参数时 **oc** 工具不再 panic。(BZ#1786835)

- 在以前的版本中，**oc describe quota** 命令在 **ClusterResourceQuota** 值的 **Used** memory 中显示不一致的单元，这无法预测且难以阅读。在这个版本中，**Used** 内存总是使用与 **Hard** 内存相同的单元，以便 **oc describe quota** 命令显示可预测的值。(BZ#1955292)

- 在以前的版本中，**oc logs** 命令无法用于管道构建，因为缺少客户端设置。客户端设置已在 **oc logs** 命令中修复，现在可以用于管道构建。(BZ#1973643)

Operator Lifecycle Manager (OLM)

- 在以前的版本中，当安装的 Operator 将 **olm.maxOpenShiftVersion** 设置为小于或等于当前版本的次 OpenShift Container Platform 版本时，Operator Lifecycle Manager (OLM) 可升级条件信息是不正确的。这会导致错误信息被修复，它指定了当 **olm.maxOpenShiftVersion** 设置为与当前 OpenShift Container Platform 版本不同的版本时，只阻断次版本和主版本升级。(BZ#1992677)

- 在以前的版本中，当捆绑包出现在索引中时，**opm** 命令无法弃用它们。因此，在同一调用中作为另一个弃用的一部分被截断的捆绑包会报告为缺少的。在这个版本中，在任何弃用前添加了对捆绑包的检查，以区分不存在的捆绑包和已被截断的捆绑包。因此，同一升级路径中弃用的捆绑包不再报告为缺失。(BZ#1950534)

- 当 Operator Lifecycle Manager (OLM) 尝试更新集群中的自定义资源定义 (CRD) 对象时，可能会出现临时错误。这会导致 OLM 永久失败包含 CRD 的安装计划。在这个版本中更新了 OLM，针对资源修改冲突错误重试 CRD 更新。因此，OLM 现在对这类瞬态错误更具弹性。如果 OLM 能够重试并解决冲突错误，安装计划不再会失败。(BZ#1923111)

- **opm index|registry add** 命令试图验证替换的索引中是否存在 Operator 捆绑包，无论它们是否已从索引中截断。当给定软件包的捆绑包已弃用后，命令将始终失败。在这个版本中，更新了 **opm** CLI 来处理这个边缘情况，不再验证是否存在截断的捆绑包。因此，在给定软件包弃用捆绑包后，命令不再会失败。(BZ#1952101)

- Operator Lifecycle Manager (OLM) 现在可以允许使用目录源资源中的标签将优先级类注入到 registry pod 中。默认目录源是由集群管理的命名空间中的重要组件，后者要求优先级类。在这个版本中，**openshift-marketplace** 命名空间中的所有默认目录源都有一个 **system-cluster-critical** 优先级类。(BZ#1954869)

- Marketplace Operator 使用 leader-for-life 实现，其中含有租期所有者身份的配置映射具有控制器 pod 放置的所有者引用。如果 pod 调度的节点不可用，且 pod 无法终止，则此问题。这使得配置映射无法正确收集垃圾，因此可以选举新的领导。因为较新的 Marketplace Operator 版本无法获得领导选举机制，所以会阻止次要版本集群升级。需要手动清理保存领导选举租期的配置映射，以便释放锁定并完成 Marketplace 组件的升级。此程序错误修复切换为使用 leader-for-lease 选举机制实施。因此，领导选举不会再卡住这种情况。(BZ#1958888)

- 在以前的版本中，为安装计划引进了新的 **Failed** 阶段。如果无法检测正在在其中创建安装计划的命名空间的有效 Operator 组 (OG) 或服务帐户 (SA) 资源，则会将安装计划转变为失败状态。也就是说，第一次协调安装计划时无法检测这些资源，这被视为平均失败。这是来自以下安装计划行为的回归：

  - 如果无法检测 OG 或 SA 资源，则会重新排列安装计划以进行协调。
  - 在达到通知器队列重试限制前创建所需的资源会把安装计划从 **Installing** 阶段转换到 **Complete** 阶段，除非捆绑包解包步骤失败。

  对于同时应用一组清单以安装包含订阅的 Operator 来创建安装计划，以及所需的 OG 和 SA 资源的用户，这个回归会导致一些不正常的行为。在这些情况下，每当 OG 和 SA 协调出现延迟时，安装计划将转变为永久失败状态。

  在这个版本中，删除了将安装计划转换到 **Failed** 阶段的逻辑。现在，对于任何协调错误，安装计划都会重新排队。因此，当没有检测到 OG 时，会设置以下条件：

  ```
  conditions:
   - lastTransitionTime: ""2021-06-23T18:16:00Z""
   lastUpdateTime: ""2021-06-23T18:16:16Z""
   message: attenuated service account query failed - no operator group found that
   is managing this namespace
   reason: InstallCheckFailed
   status: ""False""
   type: Installed
  ```

  创建有效的 OG 时，会设置以下条件：

  ```
  conditions:
   - lastTransitionTime: ""2021-06-23T18:33:37Z""
   lastUpdateTime: ""2021-06-23T18:33:37Z""
   status: ""True""
  ```

  (BZ#1960455)

- 更新目录源时，**Get** 调用将立即对与目录源相关的多个资源进行 **Delete** 调用。在某些情况下，资源已被删除，但该资源仍然存在于缓存中。这允许 **Get** 调用成功，但以下 **Delete** 调用会失败，因为集群中不存在该资源。在这个版本中更新了 Operator Lifecycle Manager (OLM)，如果未找到资源，则忽略 **Delete** 调用返回的错误。因此，OLM 在更新目录源时不再报告错误，因为缓存问题会导致 **Delete** 调用中的 "Resource Not Found" 错误。(BZ#1967621)

- 名称超过 63 个字符限制的集群服务版本 (CSV) 会导致无效的 **ownerref** 标签。在以前的版本中，当 Operator Lifecycle Manager (OLM) 使用 **ownerref** 引用来检索拥有的资源（包括集群角色绑定）时，列表者会因为无效标签返回命名空间中的所有集群角色绑定。在这个版本中更新了 OLM，以使用不同的方法让服务器拒绝无效的 **ownerref** 标签。因此，当 CSV 具有无效名称时，OLM 不再删除集群角色绑定。(BZ#1970910)

- 在以前的版本中，Operator 依赖项在安装后并不总是保留。安装声明依赖项的 Operator 后，同一命名空间中的后续更新和安装可能无法满足之前安装的 Operator 依赖项。在这个版本中，依赖项以及 Operator 的所有声明的属性都会保留在 Operator 的 **ClusterServiceVersion** (CSV) 对象的注解中。因此，在将来的安装中，声明的 Operator 的依赖项仍会受到考虑。(BZ#1978310)

- 在以前的版本中，当删除了带有已弃用捆绑包的 Operator 时，弃用历史记录不会包含在垃圾回收中。因此，如果您重新安装了 Operator，捆绑包版本会显示已弃用的表。在这个版本中，解决了为已弃用的捆绑包更好地垃圾回收问题。(BZ#1982781)

- 在以前的版本中，Operator 兼容性计算中使用集群的 z-stream 版本。因此，OpenShift Container Platform 的微发行版本被阻止。在这个版本中，在 Operator 兼容性比较中忽略了集群 z-stream 版本，解决了这个问题。(BZ#1993286)

OpenShift API 服务器

- 在以前的版本中，对服务的发现端点的一个失败请求可能会使 Operator 报告 **Available=False**。为了提高弹性，已进行了一组改进，以防止一些 Operator 在更新过程中因为各种临时错误而报告 **Available=False**。(BZ#1948089)

OpenShift 更新服务

- 在以前的版本中，当通过 web 控制台创建更新服务应用程序时，会出现无效的主机错误。这是因为默认的 OpenShift Update Service (OSUS) 应用程序名称太长。现在有一个较短的默认名称，不再发生错误。(BZ#1939788)

Red Hat Enterprise Linux CoreOS (RHCOS)

- 在以前的版本中，systemd 无法读取 **/etc/kubernetes** 中的环境文件。SELinux 策略会导致这个问题，kubelet 不会启动。该策略已被修改。kubelet 启动，并读取环境文件。(BZ#1969998)

- 在附加 ECKD DASD 的 s390x 内核虚拟机 (KVM) 中，DASD 看似是常规的 virtio 存储设备，但如果删除了 VTOC，将无法访问。因此，在 KVM 上安装 Red Hat Enterprise Linux CoreOS (RHCOS) 时，您无法使用 DASD 作为 virtio 块设备。**coreos-installer** 程序已被更新，现在当安装目标是一个 virtio 存储设备（如附加到 KVM 的 ECKD DASD）时，它会使用 VTOC-format 分区表安装 Red Hat Enterprise Linux CoreOS（RHCOS）。(BZ#1960485)

- 在以前的版本中，**NetworkManager-wait-online-service** 超时时间过早，这会阻止在 **coreos-installer** 程序启动前建立连接。因此，如果网络启动用时过长，**coreos-installer** 程序将无法获取 Ignition 配置。在这个版本中，**NetworkManager-wait-online-service** 超时被增加到其默认的上游值。因此，**coreos-installer** 程序不再无法获取 Ignition 配置。(BZ#1967483)

路由

- 在以前的版本中，Cluster Network Operator (CNO) 试图清理代理配置时会出现配置偏差，特别是 **no_proxy** 配置。这会导致 **no_proxy** 中缺少特定的 IPv6 CIDR。此修复实施为所有场景更新双栈（IPV4 和 IPV6）的逻辑。(BZ#1981975)

- 在以前的版本中，如果 **dns.config.openshift.io Operator 的 .spec.privateZone** 字段被错误填写，导致 Ingress Operator 无法找到私有托管区，则 Ingress Operator 会被降级。但是，即使修复了 **.spec.privateZone** 字段，Ingress Operator 仍会降级。Ingress Operator 找到托管区并添加 **.apps** 资源记录，但 Ingress Operator 不会重置降级状态。在这个版本中，监视 DNS 配置对象并监控 **spec.privateZone** 字段的更改。它应用适当的逻辑，并相应地更新 Operator 状态。当设置了正确的 **.spec.privateZone** 字段后，Operator 状态将返回到降级（degraded）或 **False**。(BZ#1942657)

Samples

- 在以前的版本中，缺少连接超时会导致长时间的延迟。当 Cluster Samples Operator 的 **managementState** 设置为 **Removed** 时，会测试到 **registry.redhat.io** 的连接。添加了连接超时后，会取消延迟。(BZ#1990140)

存储

- 在以前的版本中，您可以使用正在使用的 PV 删除 **LocalVolumeSet**，这需要手动清理。在这个版本中，所有发布的 PV 都会自动清理。(BZ#1862429)

- 在以前的版本中，**oc get volumesnapshotcontent** 命令不会显示卷快照的命名空间，这意味着卷快照没有被唯一标识。此命令现在显示卷快照的命名空间。(BZ#1965263)

- 在以前的版本中，当与使用自签名证书的 Red Hat OpenStack Platform (RHOSP) 端点通信时，Manila CSI Operator 会使用自定义传输。因为这个自定义传输不会使用代理环境变量，所以 Manila CSI Operator 无法与 Manila 进行通信。在这个版本中，自定义传输会消耗代理环境变量。因此，Manila CSI Operator 现在可以使用代理和自定义 CA 证书。(BZ#1960152)

- 在以前的版本中，Cinder CSI Driver Operator 没有使用配置的代理连接到 Red Hat OpenStack Platform (RHOSP) API，这会导致安装失败。在这个版本中，Cinder CSI Driver Operator 部署中包含了一个注解，用于确保容器上设置了代理环境变量。因此，安装不再会失败。(BZ#1985391)

- Local Storage Operator 检查新添加的块设备的频率已从 5 秒改为 60 秒，以减少它的 CPU 消耗。(BZ#1994035)

- 在以前的版本中，与 Manila CSI Operator 通信失败会降级集群。在这个版本中，与 Manila CSI Operator 端点通信失败时会导致一个非严重错误。因此，Manila CSI Operator 被禁用，而不是降级集群。(BZ#2001958)

- 在以前的版本中，Local Storage Operator 会删除孤立的持久性卷 (PV)，并有 10 秒的延迟，延迟是累积的。当同时删除多个持久性卷声明 (PVC) 时，可能需要几分钟或数小时才能删除其 PV。因此，在几个小时内，新 PVC 对应的本地磁盘不可用。在这个版本中，10 秒的延迟被移除。因此，会检测到 PV，并更快地为新 PVC 提供对应的本地磁盘。(BZ#2007684)

Web 控制台（管理员视角）

- 在以前的版本中，**PF4** 表中的所有行都在重新渲染。在这个版本中，**React.memo** 中的内容被打包，因此内容不会在每个滚动事件中恢复。(BZ#1856355)

- 在以前的版本中，OpenShift Container Platform Web 控制台中的 **Cluster Utilization** 中的图表以混淆的方式显示数据时间跨度。例如，如果选择了 6 小时的时间范围选项，但数据仅存在于最后三个小时，则这三个数据点被扩展以填充整个图表。前三个小时不会被显示。这可能会导致混淆，使用户认为图表显示了完整的 6 小时时间跨度。为避免混淆，图表现在在缺少信息的地方显示空白。在本例中，图表显示整个 6 小时的时间跨度，数据从第四个小时开始。前三个小时为空。(BZ#1904155)

- 在以前的版本中，web 控制台中的 **NetworkPolicy** 不会被转换为韩语或中文。在这个版本中，当使用韩语或中文查看 web 控制台时，**NetworkPolicy** 会正确翻译。(BZ#1965930)

- 在以前的版本中，**Console Overview** 部分的 **Needs Attention** 状态的问题显示 Operator 为 **upgrading**，即使它们没有升级。在这个版本中解决了 **Needs Attention** 状态的问题，以便显示 Operator 的正确状态。(BZ#1967047)

- 在以前的版本中，失败的 Cluster Service Version (CSV) 的警报显示一个通用的 **status.message**，这个信息无法帮助对失败的 CSV 进行故障排除。在这个版本中，复制的 CSV 显示帮助信息以及原始 CSV 的链接来进行故障排除。(BZ#1967658)

- 在以前的版本中，用户无法使用 masthead 中的下拉选项和键盘。在这个版本中，用户可以使用键盘访问下拉选项。(BZ#1967979)

- 在以前的版本中，用于与所有者匹配的 Operator 拥有的资源会返回错误匹配项。因此，有时 Operator 拥有的资源页面的 **Managed by** 链接会链接到不正确的 URL。在这个版本中，更新了功能逻辑来正确匹配拥有的 Operator。因此，**Managed by** 链接现在链接到正确的 URL。(BZ#1970011)

- 在以前的版本中，Operator **Hub** Web 控制台界面会导致用户出现不相关的安装计划。在这个版本中，Operator **OperatorHub** 将用户链接到 Operator **Subscription** 详情选项卡，以查看安装进度。(BZ#1970466)

- 在以前的版本中，**OAuth 详情**页面上的 **Add** 下拉列表中的项目没有国际化。在这个版本中，这些项目实现了国际化，改进了使用非英语的用户的用户体验。(BZ#1970604)

- 在以前的版本中，一个无效的本地化属性会阻止某些信息被国际化。在这个版本中，删除了无效的属性。因此，这些信息已国际化，非英语用户的用户体验也得到改进。(BZ#1970980)

- 在这个版本中，删除了在列表页面中利用资源链接时出现的工具提示，因为这些信息并不会改善用户体验。(BZ#1971532)

- 在以前的版本中，控制台 pod 使用 **preferredDuringSchedulingIgnoredDuringExecution** 反关联性规则进行部署，这有时会导致两个控制台 pod 调度到同一 control plane 节点上。在这个版本中，将规则改为 **requiredDuringSchedulingIgnoredDuringExecution**，以便在条件匹配时 pod 必须调度到不同的节点上。(BZ#1975379)

- 在以前的版本中，卸载 Operator 无法删除所有启用的插件。在这个版本中，卸载 Operator 会删除所有启用的插件。(BZ#1975820)

- 在以前的版本中，前端 Operator Lifecycle Manager (OLM) 描述符处理只使用第一个 x-descriptor 在操作对象详情页面中呈现属性。因此，如果为某个属性定义了多个 x-descriptors，并且列表中的第一个无效或不支持，则它不会如预期显示。在这个版本中更新了描述符验证逻辑，以便优先选择受支持的 x-descriptors 而不是不支持的 x-descriptors。因此，使用列表中第一个有效且受支持的 x 描述符在 **Operand 详情** 页面上呈现描述符解密的属性。(BZ#1976072)

- 在以前的版本中，字符串数据用于编码的 secret。因此，web 控制台没有正确上传二进制 secret 数据。在这个版本中对 secret 进行编码，并使用数据而不是 API 中的字符串数据。现在，二进制 secret 可以被正确地上传。(BZ#1978724)

- 在以前的版本中，当手动终止在集群中运行的进程时，终端 **ps -aux** 命令显示某些进程没有被清除。这会导致进程保留，使集群处于无效状态。在这个版本中，所有进程都在集群中正确终止，且不会出现在终端上列出的活动进程列表中。(BZ#1979571)

- 在以前的版本中，当将默认 pull secret 添加到新项目并上传多个 registry 的凭证时，**Project Details** 页面中只列出第一个凭证。也没有指示该列表已被截断。因此，当用户点击 **Default pull secret** 中的项目详情时，只会列出第一个凭证。在这个版本中，确保所有凭据都已列出，并通知用户如果当前页面中未列出这些凭证，则存在其他凭证。(BZ#1980704)

- 在以前的版本中，当用户将默认浏览器语言改为简体中文时，Web 控制台的 **Overview** 页面中的集群使用资源指标以英语和简体中文字符显示。在这个版本中，用户可以完全使用所选语言查看集群使用资源。(BZ#1982079)

- 在以前的版本中，当语言改为简体中文时，集群使用量统计与 **project**、**pod** 和 **node** 的左菜单中的转换不匹配。在这个版本中，简化了中文翻译，因此集群利用率指标与 **top consumers** 过滤器一致。(BZ#1982090)

- 在以前的版本中，用户从服务帐户中看到错误而不是默认的 pull secret。这会导致项目详情屏幕上的信息不完整。用户必须访问 default ServiceAccount，才能查看整个默认 pull secret 列表。在这个版本中，用户可以从项目详情页面上的默认 ServiceAccount 中查看 pull secret 的整个列表。(BZ#1983091)

- 在以前的版本中，如果您在查看 **Terminal** 选项卡时重新定义节点或 pod 的网页大小，有时浏览器会显示两个垂直滚动栏。现在，控制台已被更新，只有在窗口调整大小时才会显示一个滚动栏。(BZ#1983220)

- 在以前的版本中，当使用单一节点开发人员配置集安装 OpenShift Container Platform 4.8.2 时，Web 控制台不会被部署。如果没有为创建安装计划的命名空间检测到有效的 Operator 组或服务帐户，则安装计划会被置于失败状态。未做进一步尝试。在这个版本中，失败的安装计划会被设置为再次运行，直到检测到 Operator 组或服务帐户为止。(BZ#1986129)

- 在以前的版本中，在 **Events Dashboard** 中，**More** 和 **Show Less** 都没有国际化，从而导致用户体验不佳。在这个版本中，它们被国际化。(BZ#1986754)

- 在以前的版本中，在 **Console** 页面中构建服务的完全限定域名 (FQDN) 的逻辑缺失。因此，服务详情页面中缺少 FQDN 信息。在这个版本中，增加了构造 FQDN 的逻辑，以便该服务的 FQDN 信息在页面中现在可用。(BZ#1996816)

Web 控制台 (开发者视角)

- 在以前的版本中，kamelet 类型的 **sink** 与源 kamelets 一起显示在事件源的目录中。在当前发行版本中，事件源的目录仅显示类型为 **source** 的 kamelet。(BZ#1971544)

- 在以前的版本中，日志文件包含在一行中，没有任何换行符。在当前版本中，日志文件包含预期的换行符，以及日志标头周围的额外换行符。(BZ#1985080)

1.7. 技术预览功能

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

技术预览功能支持范围

在下表中，功能被标记为以下状态：

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

表 1.3. 技术预览

功能	OCP 4.7	OCP 4.8	OCP 4.9
精度时间协议 (PTP)	TP	TP	TP
oc CLI 插件	TP	GA	GA
Descheduler	GA	GA	GA
HPA 用于内存使用	GA	GA	GA
服务绑定	TP	TP	TP
使用 Cinder 的原始块	TP	GA	GA
CSI 卷快照	GA	GA	GA
CSI 卷扩展	TP	TP	TP
vSphere 问题检测器（vSphere Problem Detector） Operator	GA	GA	GA
CSI Azure Disk Driver Operator	-	TP	TP
CSI Azure Stack Hub Driver Operator	-	-	GA
CSI GCP PD Driver Operator	TP	GA	GA
CSI OpenStack Cinder Driver Operator	GA	GA	GA
CSI AWS EBS Driver Operator	TP	TP	GA
CSI AWS EFS Driver Operator	-	-	TP
CSI 自动迁移	-	TP	TP
CSI inline 临时卷	TP	TP	TP
CSI vSphere Driver Operator	-	TP	TP
使用 Local Storage Operator 进行自动设备发现和置备	TP	TP	TP
OpenShift Pipelines	TP	GA	GA
OpenShift GitOps	TP	GA	GA
OpenShift 沙盒容器	-	TP	TP
Vertical Pod Autoscaler	TP	GA	GA

功能	OCP 4.7	OCP 4.8	OCP 4.9
Cron 作业	TP	GA	GA
PodDisruptionBudget	TP	GA	GA
使用 kvc 向节点添加内核模块	TP	TP	TP
Egress router CNI 插件	TP	GA	GA
Scheduler 配置集	TP	TP	GA
非抢占优先级类	TP	TP	TP
Kubernetes NMState Operator	TP	TP	TP
支持的安装程序	TP	TP	TP
AWS 安全令牌服务（STS）	TP	GA	GA
kdump	TP	TP	TP
OpenShift Serverless	-	GA	GA
无服务器功能	-	TP	TP
支持数据平面开发套件 (DPDK)	TP	TP	GA
内存管理器功能	-	-	TP
CNI VRF 插件	TP	TP	GA
Cluster Cloud Controller Manager Operator	-	-	GA
AWS 的云控制器管理器	-	-	TP
Azure 的云控制器管理器	-	-	TP
OpenStack 的云控制器管理器	-	-	TP
驱动程序工具包	-	TP	TP
Special Resource Operator (SRO)	-	-	TP
Node Health Check Operator	-	-	TP

1.8. 已知问题

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

  警告

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

  使用以下脚本撤销对发现端点的未经身份验证的访问：

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

  此脚本从以下集群角色绑定中删除未经身份验证的对象：

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

  (BZ#1821771)

- **oc annotate** 命令不适用于包含了等号（**=**）的 LDAP 组名称，因为命令使用等号作为注释名称和值之间的分隔符。作为临时解决方案，使用 **oc patch** 或 **oc edit** 添加注解。(BZ#1917280)

- 集群管理员可以为 503、404 或两个错误页面指定自定义 HTTP 错误代码响应页面。如果没有为自定义错误代码响应页面指定正确的格式，则会出现路由器 pod 中断且无法解析。路由器不会重新加载来反映自定义错误代码页面更新。作为临时解决方案，您可以使用 **oc rsh** 命令在本地访问路由器 pod。然后，在服务自定义 http 错误代码页面的所有路由器 pod 中运行 **reload-haproxy** ：

```
$ oc -n openshift-ingress rsh router-default-6647d984d8-q7b58
sh-4.4$ bash -x /var/lib/haproxy/reload-haproxy
```

或者，您可以注释路由来强制重新加载。(BZ#1990020), (BZ#2003961)

- 一个 Open Virtual Network（OVN）程序错误会导致 Octavia 负载均衡器的持久性连接问题。创建 Octavia 负载均衡器时，OVN 可能不会将它们插入到一些 Neutron 子网中。对于某些 Neutron 子网，这些负载平衡器可能无法访问。这个问题会影响 Neutron 子网，在配置 Kuryr 时，每个 OpenShift 命名空间都会随机创建它们。因此，当出现这个问题时，从受此问题影响的 OpenShift 命名空间无法访问实施 OpenShift **Service** 对象的负载均衡器。由于这个程序错误，不建议在带有 OVN 和 OVN Octavia 的 Red Hat OpenStack Platform（RHOSP）16.1 上使用 Kuryr SDN 的 OpenShift Container Platform 4.8 部署。以后的 RHOSP 发行版本中会解决这个问题。(BZ#1937392)

- 当需要集群范围代理才能访问 RHOSP API 时，如果在带有 Kuryr 的 Red Hat OpenStack Platform (RHOSP) 上安装需要使用集群范围代理，则将无法正常工作。(BZ#1985486)

- 由于一个竞争条件，Red Hat OpenStack Platform (RHOSP) 云供应商可能无法正确启动。因此，LoadBalancer 服务可能永远不会设置 **EXTERNAL-IP**。作为临时解决方案，您可以使用 BZ#2004542 中所述的步骤重启 kube-controller-manager pod。

- 安装 OpenShift Container Platform 时，安装程序不会提供 **ap-northeast-3** AWS 区域作为选项，即使它是一个受支持的 AWS 区域。作为临时解决方案，您可以从安装提示符中选择不同的 AWS 区域，然后在安装集群前更新所生成的 **install-config.yaml** 文件中的区域信息。(BZ#1996544)

- 当在 **us-east-1** 区域中的 AWS 上安装集群时，无法使用本地 AWS 区域。作为临时解决方案，您必须在安装集群时在 **install-config.yaml** 文件中指定非本地可用区。(BZ#1997059)

- 您只能在带有公共端点（如 ARM 端点）的 Azure Stack Hub 上安装 OpenShift Container Platform，这些端点使用由公开信任的证书颁发机构 (CA) 签名的证书进行保护。在以后的 OpenShift Container Platform z-stream 发行版本中会添加对内部 CA 的支持。(BZ#2012173)

- 集群管理员可以为 503、404 或两个错误页面指定自定义 HTTP 错误代码响应页面。路由器不会重新加载来反映自定义错误代码页面更新。作为临时解决方案，路由器 pod 中的 rsh 在为自定义 http 错误代码页面提供服务的所有路由器 pod 中运行 **reload-haproxy** ：

```
$ oc -n openshift-ingress rsh router-default-6647d984d8-q7b58
sh-4.4$ bash -x /var/lib/haproxy/reload-haproxy
```

或者，您可以注释路由来强制重新加载。(BZ#1990020)

- 此发行版本包含一个已知问题。如果您自定义 OpenShift OAuth 路由的主机名和证书，Jenkins 不再信任 OAuth 服务器端点。因此，如果用户依赖 OpenShift OAuth 集成来管理身份和访问权限，用户就无法登录 Jenkins 控制台。目前还没有可用的临时解决方案。(BZ#1991448)

- 由于某些高品质监控指标被意外丢弃，因此在此发行版本中不提供以下容器性能输入和输出指标： **pod**、**qos** 和 **System**。
这个问题不存在临时解决方案。要跟踪生产工作负载的这些指标，请不要升级到初始 4.9 版本。(BZ#2008120)

- 由于存在软件定义的网络策略，特殊 Resource Operator (SRO) 可能无法在 Google Cloud Platform 上安装。因此，simple-kmod pod 不会被创建。这个问题已在 OpenShift Container Platform 4.9.4 发行版本中解决。(BZ#1996916)

- 在 OpenShift Container Platform 4.9 中，具有集群角色的用户如果对部署或部署配置没有编辑权限，则无法使用控制台扩展部署或部署配置。(BZ#1886888)

- 在 OpenShift Container Platform 4.9 中，当 **Developer 控制台**中存在最小或没有数据时，大多数监控图表或图形（如 CPU 消耗、内存用量和带宽）都会显示 -1 到 1 的范围。但是，这些值都不能低于零，因此负值不正确。(BZ#1904106)

- 因为 **cgroups** 不匹配，**ip vrf exec** 命令无法正常工作。因此，无法在 OpenShift 容器集内使用此命令。要使用虚拟路由和转发 (VRF)，应用程序必须可识别 VRF，并直接绑定到 VRF 接口。(BZ#1995631)

- 非统一内存访问 (NUMA) 错误可能会导致容器出现不必要的 NUMA 固定，这可能导致延迟或性能下降。拓扑管理器可以使用 **single-numa-node** 拓扑管理策略可满足的资源将容器固定到多个 NUMA 节点。容器会被固定到有保证服务质量 (QoS) 的 pod。作为临时解决方案，当容器内存资源请求大于 **single-numa-node** 策略时， 不要启动保证的 QoS pod。(BZ#1999603)

- 有时，选择要删除的 pod 不会被删除。当集群耗尽资源时会出现这种情况。要重新声明资源，系统会选择一个或多个 pod 进行删除。由于资源较低，导致处理速度较慢，删除操作可能会超过既定的删除宽限期，从而导致失败。如果发生这种情况，请手动删除 pod。然后，集群会重新声明释放的资源。(BZ#1997476)

- 在等待 Open vSwitch (OVS) 端口绑定时，pod 可能会处于 **ContainerCreating** 状态并超时。报告的事件是 **failed to configure pod interface: timed out waiting for OVS port binding**。当为 OVN-Kubernetes 插件创建多个 pod 时，可能会出现此问题。(BZ#2005598)

- 重启出口节点后，**lr-policy-list** 包含错误，如重复记录或丢失的内部 IP 地址。预期结果是 **lr-policy-list** 具有与重启出口节点前相同的记录。作为临时解决方案，您可以重启 **ovn-kubemaster** pod。(BZ#1995887)

- 当包含分布式网关端口的逻辑路由器上启用 IP 多播中继时，多播流量不会在分布式网关端口上正确转发。因此，OVN-Kubernetes 中的 IP 多播功能无法正常工作。(BZ#2010374)

- 在 Web 控制台的 **Administrator** 视角中，一个页面应该在节点列表可用前显示节点列表，这会导致页面变得无响应。没有临时解决方案，但会在以后的版本中解决这个问题。(BZ#2013088)

- Operator Lifecycle Manager (OLM) 结合使用时间戳检查和过时的 API 调用，这些调用不适用于 **skipRange** 升级，以确定是否需要对特定订阅执行升级。对于使用 **skipRange** 升级的 Operator，升级过程中会有一个延迟，可能需要长达 15 分钟才能完成解决，并可能会在更长时间内被阻止。
  作为临时解决方案，集群管理员可以删除 **openshift-operator-lifecycle-manager** 命名空间中的 **catalog-operator** pod。这会导致自动重新创建 pod，从而导致触发 **skipRange** 升级。(BZ#2002276)

- 目前，当在启用了 FIPS 模式的 Google Cloud Platform 上启动 Red Hat Enterprise Linux (RHEL) 8 时，当尝试从 Red Hat Update Infrastructure(RHUI)安装软件包时，RHEL 8 无法下载元数据。作为临时解决方案，您可以禁用 RHUI 存储库，并使用红帽订阅管理来获取内容。(BZ#2001464), (BZ#1997516).

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

- 当 MetalLB 使用 OVN-Kubernetes Container Network Interface 网络供应商以第 2 层模式运行时，而不是具有发言人 pod 响应 ARP 或 NDP 请求的单个节点，集群中的每个节点都会响应该请求。ARP 响应的意外数量可能类似于 ARP 欺骗攻击。尽管经验与设计不同，但只要主机或子网

上的任何软件没有配置为阻止 ARP，流量就会路由到该服务。此程序错误已在 OpenShift Container Platform 发行版本中解决。(BZ#1987445)

- 当 Tang 磁盘加密和静态 IP 地址配置应用到 VMWare vSphere 用户置备的基础架构集群中时，节点在最初置备后无法正确引导。(BZ#1975701)

- Operator 必须列出 Operator Lifecycle Manager (OLM) 的相关镜像才能从本地源运行。目前，如果没有定义 **ClusterServiceVersion** (CSV)对象的 **relatedImages** 参数，**opm render** 不会填充相关的镜像。计划在后续的版本中修复此问题。(BZ#2000379)

- 在以前的版本中，Open vSwitch (OVS) 在每个 OpenShift Container Platform 集群节点上运行，节点导出器代理从节点上收集 OVS CPU 和内存指标。现在，OVS 作为 systemd 单元在集群节点上运行，并且不会收集指标。计划在后续的版本中修复此问题。OVS 数据包指标仍然收集。(BZ#2002868)

- 用于隐藏或显示 OpenShift Container Platform Web 控制台中的 **Storage → Overview** 页面的标记被错误配置。因此，部署包含 OpenShift Cluster Storage 的集群后，概览页面将无法看到。计划在后续的版本中修复此问题。(BZ#2013132)

- 在 OpenShift Container Platform 4.6 及之后的版本中，pull 的镜像引用必须指定以下红帽 registry：

  - **registry.redhat.io**
  - **registry.access.redhat.com**
  - **quay.io**

  否则，如果没有指定这些 registry，则构建 Pod 无法拉取镜像。

  作为临时解决方案，在镜像拉取规格中使用完全限定名称，如 **registry.redhat.io/ubi8/ubi:latest** 和 **registry.access.redhat.com/rhel7.7:latest**。

  另外，您还可以通过添加允许镜像短名称的 registry 来更新镜像 registry 设置。(BZ#2011293)

- 在 OpenShift Container Platform 4.8 之前，默认的负载平衡算法是 **leastconn**。在 OpenShift Container Platform 4.8.0 中，对于非透传的路由，默认设置为 **random**。切换到 **random** 与需要使用长时间运行的 websocket 连接的环境不兼容，因为它显著提高了这些环境中的内存消耗。为缓解这种显著内存消耗，在 OpenShift Container Platform 4.9 中默认负载均衡算法被恢复为 **leastconn**。一旦有一个不会产生大量内存用量的解决方案可用后，在以后的 OpenShift Container Platform 发行版本中，默认值将更改为 **random**。
  您可以输入以下命令来检查默认设置：

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

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

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

  (BZ#2015829)

- 当指定托管在本地 registry 中的镜像时，**oc adm release extract --tools** 命令会失败。(BZ#1823143)

- 在 OpenShift Container Platform 单一节点配置中，使用实时内核(**kernel-rt**)时 pod 创建时间比使用非实时内核时慢两倍。使用 **kernel-rt** 时，较慢的 pod 创建时间会影响支持的最大 pod 数量，因为节点重启后会影响到恢复时间。
  作为临时解决方案，当使用 **kernel-rt** 时，您可以通过使用 **rcupdate.rcu_normal_after_boot=0** 内核参数引导来缩短恢复时间。这需要一个实时内核版本 **kernel-rt-4.18.0-305.16.1.rt7.88.el8_4** 或更高版本。这个已知问题适用于 OpenShift Container Platform 版本 4.8.15 及更新的版本。(BZ#1975356)

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

- SNO 集群置备过程中出现了一个错误，**bootkube** 会尝试在集群 bootstrap 过程末尾使用 **oc**。kube API 收到关闭请求，这会导致集群 bootstrap 过程失败。(BZ#2010665)

- 因为修改的引导表条目，在同一主机上成功部署 OpenShift Container Platform 版本 4.8 后部署 OpenShift Container Platform 版本 4.9 SNO 集群会失败。(BZ#2011306)

- 当 OpenShift Container Platform 版本 4.8.5 中部署了基于 DPDK 的工作负载时，inbox iavf 驱动程序会出现不稳定的问题。当在运行 RHEL for Real Time 8 的主机上部署 DPDK 工作负载时，这个问题也显而易见。安装了 Intel XXV710 NIC 的主机中会发生这个问题。(BZ#2000180)

- PTP Operator 部署的 **linuxptp** 子系统中出现时钟跳过错误。报告的错误信息为：**clock jumped backward or running slower than expected!**。在 OpenShift Container Platform 版本 4.8 或 4.9 集群中安装 Intel Columbiaville E810 NIC 的主机中会出现错误。此错误可能与 Intel ice 驱动程序相关，而不是 **linuxptp** 子系统中的错误。(BZ#2013478)

- 有时，在 DU 节点安装零接触置备(ZTP)安装过程中，Operator 安装会失败。**InstallPlan** API 报告了错误。报告的错误消息为： **Bundle unpacking failed。Reason: DeadlineExceeded**。如果 Operator 安装任务超过 600 秒，则会出现错误。
  作为临时解决方案，请通过对失败 Operator 运行以下 **oc** 命令来重试 Operator 安装：

  1. 删除目录源：

     ```
     $ oc -n openshift-marketplace delete catsrc <failed_operator_name>
     ```

  2. 删除安装计划：

     ```
     $ oc -n <failed_operator_namespace> delete ip <failed_operator_install_plan>
     ```

  3. 删除订阅，并等待相关的自定义资源策略重新创建 Operator **CatalogSource** 和 **Subscription** 资源：

     ```
     $ oc -n <failed_operator_namespace> delete sub <failed_operator_subscription>
     ```

     预期结果

     Operator **InstallPlan** 和 **ClusterServiceVersion** 资源会被创建并安装 Operator。

     (BZ#2021456)

- SR-IOV Operator 和 Machine Config Operator (MCO) 之间存在一个竞争条件，这会在 DU 节点的 ZTP 安装过程中以不同的方式出现，并且以不同的方式列出其自身。竞争条件可能会导致以下错误：
  - 当 ZTP 安装过程完成置备 DU 节点时，有时不会应用性能配置集配置。当 ZTP 安装过程完成置备 DU 节点时，性能配置集配置不会应用到节点，**MachineConfigPool** 资源会处于 **Updating** 状态。
    作为临时解决方案，请执行以下步骤。

    1. 获取失败的 DU 节点的名称：

    ```
    $ oc get mcp
    ```

    输出示例

    ```
    NAME           CONFIG                                 UPDATED   UPDATING   DEGRADED
    control-plane-1   rendered-control-plane-1-90fe2b00c718   False     True       False
    compute-1         rendered-compute-1-31197fc6da09         True      False      False
    ```

    2. 取消控制出现故障的节点，并等待 **machine-config-daemon** 应用性能配置集。例如：

    ```
    $ oc adm uncordon compute-compute-1-31197fc6da09
    ```

    预期结果

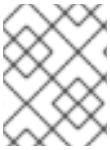
    machine-config-daemon 将性能配置集配置应用到节点。

  - 有时，性能配置集配置不会在 DU 节点配置期间应用。作为临时解决方案，请更改在 DU 节点上应用策略的顺序。首先应用 Machine Config Operator (MCO) 和 Performance Addon Operator (PAO) 策略，然后应用 SR-IOV 策略。
  - 在 DU 节点的策略配置期间，重新引导可能需要十分钟时间。这个实例不需要临时解决方案。系统最终会恢复。
    (BZ#2021151)

1.9. 异步勘误更新

OpenShift Container Platform 4.9 的安全更新、程序漏洞修正、功能增强更新将会通过红帽网络以异步勘误的形式发布。所有的 OpenShift Container Platform 4.9 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 4.9 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.9.z）的具体信息会包括在相应的子章节中。此外，在发行公告中因为空间限制没有包括在其中的勘误内容也会包括在这里的相应的子章节中。

重要

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

1.9.1. RHSA-2021:3759 - OpenShift Container Platform 4.9.0 镜像发行版本、程序错误修正和安全更新公告

发布日期：2021 年 10 月 18 日

OpenShift Container Platform release 4.9.0 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2021:3759 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3758 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.0 容器镜像列表

1.9.2. RHBA-2021:3935 - OpenShift Container Platform 4.9.4 程序错误修复和安全更新

发布日期：2021 年 10 月 26 日

OpenShift Container Platform release 4.9.4 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:3935 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:3934 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.4 容器镜像列表

1.9.2.1. 增强

SamplesImagestreamImportFailing 警报中实施了一个新的条件收集器，它会在触发时收集 **openshift-cluster-samples-operator** 命名空间的日志和镜像流。通过额外的数据收集，可以从外部 registry 中拉取镜像流时深入了解问题。(**BZ#1966153**)

1.9.2.2. 程序错误修复

- 在以前的版本中，在节点列表可用前，**Nodes** 页面会呈现。在这个版本中，当节点列表可用时，**Nodes** 页面可以正常工作。(**BZ#2013088**)

1.9.2.3. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.9.3. RHBA-2021:4005 - OpenShift Container Platform 4.9.5 程序错误修复更新

发布日期：2021 年 11 月 1 日

OpenShift Container Platform release 4.9.5 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:4005 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:4004 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.5 容器镜像列表

1.9.3.1. 已知问题

- 用于在 OpenShift Container Platform Web 控制台中隐藏或显示 **Storage → Overview** 页面的标记被错误配置。因此，在部署包含 OpenShift Cluster Storage 的集群后，**Overview** 页面会不可见。计划在以后的版本中对此程序错误进行修复。(BZ#2013132)

1.9.3.2. 程序错误修复

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

1.9.3.3. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.9.4. RHBA-2021:4119 - OpenShift Container Platform 4.9.6 程序错误修复和安全更新

发布日期：2021 年 11 月 10 日

OpenShift Container Platform release 4.9.6 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-2021:4119 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:4118 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.6 容器镜像列表

1.9.4.1. 已知问题

- 当前 opt-in 混淆无法在带有 OVN 的集群中工作，因为 **hostsubnets.network.openshift.io** 目前不在 OVN 集群中。(BZ#2014633)

1.9.4.2. 程序错误修复

- 在以前的版本中，**nmstate-handler** pod 的锁定实现中有一个错误会导致多个节点获得控制。在这个版本中修复了锁定实现，只有一个节点可以控制锁定。(BZ#1954309)
- 在以前的版本中，OpenStack 类别验证可以接受使用错误的单元不符合 RAM 要求的类别。在这个版本中，正确的单元用于将最小 RAM 与 OpenStack 返回的值进行比较。(BZ#2009787)
- 在以前的版本中，因为 control plane 节点缺少 Ingress 安全组规则，OpenStack 上的 OpenShift Container Platform 部署会在 OpenStack 上部署，因为带有未指定 worker 的紧凑集群会失败。在这个版本中，当 control plane 可以调度时，将 Ingress 安全组添加到 OpenStack 中。(BZ#2016267)
- 在以前的版本中，一些 **cAdvisor** 指标被丢弃，以减少整体内存消耗，但控制台中的 **Utilization** 仪表板不会显示任何结果。在这个版本中，仪表板可以正确地显示。(BZ#2018455)

1.9.4.3. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.9.5. RHBA-2021:4579 - OpenShift Container Platform 4.9.7 程序错误修复更新

发布日期：2021 年 11 月 15 日

OpenShift Container Platform release 4.9.7 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:4579 公告中。这个版本没有 RPM 软件包。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.7 容器镜像列表

1.9.5.1. 功能

1.9.5.1.1. Kubernetes 1.22.2 中的更新

此更新包含 Kubernetes 1.22.2 的更改。可在以下更改日志中找到更多信息： 1.22.2。

1.9.5.2. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 在次版本中更新集群 以获取相关说明。

1.9.6. RHBA-2021:4712 - OpenShift Container Platform 4.9.8 程序错误修复更新

发布日期：2021 年 11 月 22 日

OpenShift Container Platform release 4.9.8 现已正式发布。此更新包括的程序错误修正信息包括在 RHBA-2021:4712 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:4711 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.8 容器镜像列表

1.9.6.1. 程序错误修复

- 在以前的版本中，如果您添加或删除了 **SriovNetworkNodePolicy** 自定义资源(CR)，而任何一个 SriovNetworkNodeState CR 有一个值大于 **Succeeded** 的 **syncStatus** 对象，SR-IOV 网络配置守护进程 pod 将会对节点进行连接，并将其标记为不可调度。在这个版本中解决了这个问题。(**BZ#2002508**)

1.9.6.2. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 在次版本中更新集群 以获取相关说明。

1.9.7. RHBA-2021:4834 - OpenShift Container Platform 4.9.9 程序错误修复和安全更新

发布日期：2021 年 11 月 29 日

OpenShift Container Platform release 4.9.9 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-2021:4834 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:4833 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.9 容器镜像列表

1.9.7.1. 功能

1.9.7.1.1. Kubernetes 1.22.3 更新

此更新包含 Kubernetes 1.22.3 中的更改。有关更多信息，请参见以下更改日志： 1.22.3。

1.9.7.2. 程序错误修复

- 在以前的版本中，Cluster Version Operator(CVO)在决定是否覆盖清单时会忽略 **spec.overrides[].group**。因此，覆盖的条目可能与多个资源匹配，这些资源可能会覆盖超过管理员预期的资源。此外，覆盖的无效组条目被视为匹配项，kube **admin 用户** 可能已在使用无效的组值而无需注意。在这个版本中，CVO 在应用配置的覆盖时需要组匹配。因此，CVO 不再与带有单个覆盖的多个清单匹配。相反，CVO 仅将清单与正确的组匹配。**以前** 使用无效组的 kubeadmin 用户必须更新至正确的组，以便其覆盖继续匹配。(**BZ#2022570**)

1.9.7.3. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 在次版本中更新集群 以获取相关说明。

1.9.8. RHBA-2021:4889 - OpenShift Container Platform 4.9.10 程序错误修复更新

发布日期：2021 年 12 月 6 日

OpenShift Container Platform release 4.9.10 现已正式发布。此更新包括的程序错误修正列在 RHBA-2021:4889 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:4888 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.10 容器镜像列表

1.9.8.1. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 在次版本中更新集群 以获取相关说明。

1.9.9. RHBA-2021:5003 - OpenShift Container Platform 4.9.11 程序错误修复和安全更新

发布日期：2021 年 12 月 13 日

OpenShift Container Platform release 4.9.11 现已正式发布。此更新包括的程序错误修正列在 RHBA-2021:5003 公告中。此更新中包括的 RPM 软件包由 RHSA-2021:5002 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.11 容器镜像列表

1.9.9.1. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 在次版本中更新集群 以获取相关说明。

1.9.10. RHBA-2021:5214 - OpenShift Container Platform 4.9.12 程序错误修复更新

发布日期：2022 年 1 月 4 日

OpenShift Container Platform release 4.9.12 现已正式发布。此更新包括的程序错误修正列在 RHBA-2021:5214 公告中。此更新中包括的 RPM 软件包由 RHBA-2021:5213 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.12 容器镜像列表

1.9.10.1. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 在次版本中更新集群 以获取相关说明。

1.9.11. RHBA-2022:0029 - OpenShift Container Platform 4.9.13 程序错误修复更新

发布日期：2022 年 1 月 10 日

OpenShift Container Platform release 4.9.13 现已正式发布。此更新包括的程序错误修正列在 RHBA-2022:0029 公告中。这个版本没有 RPM 软件包。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。参阅以下章节以获得此发行版本中与容器镜像相关的信息。

OpenShift Container Platform 4.9.13 容器镜像列表

1.9.11.1. 程序错误修复

- 在以前的版本中，Windows 文件路径不接受冒号字符，该字符会在 Windows 机器上阻止镜像。在这个版本中，冒号被替换为破折号，允许在 Windows 机器上进行镜像(mirror)。(**BZ#1903545**)
- 在以前的版本中，属于集群的 *Custom API Name 证书的证书* 的文件权限不一致 。在这个版本中，权限始终设置为 **0600**。(**BZ#1977730**)

1.9.11.2. 升级

要将现有 OpenShift Container Platform 4.9 集群升级到此最新版本，请参阅使用 CLI 在次版本中更新集群 以获取相关说明。