OpenShift Container Platform 4.19

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: 2025-09-24

OpenShift Container Platform 4.19 发行注记

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

Legal Notice

Abstract

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。

Table of Contents

第 1 章 OPENSHIFT CONTAINER PLATFORM 4.19 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-2024:11038)现已正式发布。此发行版本使用 Kubernetes 1.32，带有 CRI-O 运行时。OpenShift Container Platform 4.19 的新功能、改变以及已知的问题包括在此文档中。

OpenShift Container Platform 4.19 集群位于 https://console.redhat.com/openshift。在 Red Hat Hybrid Cloud 控制台中，您可以将 OpenShift Container Platform 集群部署到内部环境或云环境中。

对于 control plane 和计算机器，需要使用 RHCOS 机器。

对于为奇数的版本（如 OpenShift Container Platform 4.19），在所有支持的构架中，包括 **x86_64**, 64-bit ARM (**aarch64**), IBM Power® (**ppc64le**), 和 IBM Z® (**s390x**) 的支持生命周期为 18 个月。有关所有版本支持的更多信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

从 OpenShift Container Platform 4.14 版本开始，红帽通过三个新的生命周期分类（平台 Aligned、平台 Agnostic 和 Rolling Stream）简化红帽所提供的集群 Operator 的管理。这些生命周期类别为集群管理员提供了额外的简易性和透明度，以更好地了解每个 Operator 的生命周期策略，并以可预测的支持界限来计划对集群进行维护和升级。如需更多信息，请参阅 OpenShift Operator 生命周期。

OpenShift Container Platform 专为 FIPS 设计。当以 FIPS 模式运行 Red Hat Enterprise Linux (RHEL) 或 Red Hat Enterprise Linux CoreOS (RHCOS) 时，OpenShift Container Platform 核心组件使用 RHEL 加密库，只有在 **x86_64**, **ppc64le**, 和 **s390x** 架构上的库被提交到 NIST 进行 FIPS 140-2/140-3 Validation。

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

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

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

1.3. 新功能及功能增强

OpenShift Container Platform 4.19 IBM Power 支持以下新功能：

- 支持 IBM Power®11

此版本对以下方面进行了改进：

1.3.1. 认证和授权

1.3.1.1. 使用外部 OIDC 身份提供程序启用直接身份验证（技术预览）

在这个版本中，您可以启用直接与外部 OpenID Connect (OIDC) 身份提供程序集成来发布令牌以进行身份验证。这会绕过内置的 OAuth 服务器，并直接使用外部身份提供程序。

通过直接与外部 OIDC 供应商集成，您可以利用首选 OIDC 供应商的高级功能，而不受内置 OAuth 服务器的功能的限制。您的机构可以从单一接口管理用户和组，同时简化跨多个集群和混合环境的身份验证。您还可以与现有工具和解决方案集成。

直接身份验证作为一个技术预览功能提供。

如需更多信息，请参阅使用外部 OIDC 身份提供程序启用直接身份验证。

1.3.1.2. 默认启用 ServiceAccountTokenNodeBinding Kubernetes 功能

在 OpenShift Container Platform 4.19 中，默认启用了 **ServiceAccountTokenNodeBinding** 功能，并与上游 Kubernetes 行为保持一致。除了现有的绑定选项外，此功能还允许服务帐户令牌直接绑定到节点对象。这个变化的好处是：在删除绑定节点时通过自动使令牌无效增强了安全性，并更好地防止跨不同节点的令牌重播攻击（token replay attack）。

1.3.2. 文档

1.3.2.1. 合并了 etcd 文档

此发行版本包含一个 *etcd* 部分，它整合了所有有关 OpenShift Container Platform etcd 的现有文档。如需更多信息，请参阅 etcd 的概述。

1.3.2.2. 教程指南

OpenShift Container Platform 4.19 现在包含一个*教程*指南，它替代了以前版本中的 *Getting started* 指南。现有教程已被更新，指南现在只侧重于实际动手操作的内容。它还为红帽 OpenShift Container Platform 提供其他推荐的实践学习资源。

如需更多信息，请参阅 Tutorials。

1.3.3. 边缘计算

1.3.3.1. 使用 RHACM PolicyGenerator 资源管理 GitOps ZTP 集群策略（正式发布）

现在，您可以使用 **PolicyGenerator** 资源和 Red Hat Advanced Cluster Management (RHACM) 来使用 GitOps ZTP 为受管集群部署策略。**PolicyGenerator** API 是 Open Cluster Management 标准的一部分，它提供了一种通用的修补资源方法，这无法通过 **PolicyGenTemplate** API 来实现。使用 **PolicyGenTemplate** 资源管理和部署策略将在即将发布的 OpenShift Container Platform 发行版本中弃用。

如需更多信息，请参阅使用 PolicyGenerator 资源配置受管集群策略。

1.3.3.2. 配置本地仲裁节点（技术预览）

您可以配置带有两个 control plane 节点的 OpenShift Container Platform 集群，以及一个本地仲裁程序节点，以便在降低集群的基础架构成本时保持高可用性 (HA)。此配置只支持裸机安装。

本地仲裁程序节点是一个低成本、共存的机器，它参与 control plane 仲裁决策。与标准的 control plane 节点不同，仲裁程序节点不会运行完整的 control plane 服务集合。通过此配置，只使用两个置备的 control plane 节点而不是三个就可以维护集群的高可用性（HA）。

要启用此功能，您必须在 **install-config.yaml** 文件中定义仲裁程序机器池并启用 **TechPreviewNoUpgrade** 功能集。

配置本地仲裁节点作为技术预览功能提供。如需更多信息，请参阅配置本地仲裁程序节点。

1.3.3.3. 协调重启配置更改

此发行版本将重启策略添加到 ZTP 引用中，由 Topology Aware Lifecycle Manager (TALM) 应用，以便在配置更改需要重启时协调 spoke 集群的重启，如延迟调整更改。应用重启策略时，TALM 会重启所选集群上的目标 **MachineConfigPool** 对象中的所有节点。

您可以通过策略应用所有配置更新，然后触发单个协调重启，而不是在每次重启后重新引导节点。

如需更多信息，请参阅协调重启以了解配置更改。

1.3.4. 扩展 (OLM v1)

1.3.4.1. 集群扩展的 preflight 权限检查（技术预览）

在这个版本中，在尝试安装扩展时，Operator Controller 会空运行（dry run）安装过程。此空运行会验证指定的服务帐户是否具有捆绑包定义的角色和绑定所需的基于角色的访问控制(RBAC)规则。

如果服务帐户缺少任何所需的 RBAC 规则，preflight 检查会在实际安装进行前失败，并生成报告。

如需更多信息，请参阅集群扩展的 Preflight 权限检查（技术预览）

1.3.4.2. 在特定命名空间中部署集群扩展（技术预览）

在这个版本中，您可以使用 **OwnNamespace** 或 **SingleNamespace** 安装模式在一个特定的命名空间中部署一个扩展，它作为 **registry+v1** Operator 捆绑包的一个技术预览功能。

如需更多信息，请参阅在特定命名空间中部署集群扩展（技术预览）

1.3.5. 硬件加速器

1.3.5.1. 动态加速器 Slicer Operator （技术预览）

在这个版本中，您可以使用 Dynamic Accelerator Slicer (DAS) Operator 在 OpenShift Container Platform 中动态分片 GPU 加速器，而不是依赖节点引导时定义的静态分片 GPU。这可让您根据特定工作负载需求动态分片 GPU，确保有效的资源利用率。

如需更多信息，请参阅 Dynamic Accelerator Slicer (DAS) Operator。

1.3.6. 托管 control plane

因为托管的 control plane 的发布与 OpenShift Container Platform 不同，所以它有自己的发行注记。如需更多信息，请参阅 托管 control plane 发行注记。

1.3.6.1. Red Hat OpenStack Platform (RHOSP) 17.1 上的托管 control plane （技术预览）

在 RHOSP 17.1 上的托管 control plane 现在作为技术预览被支持。

如需更多信息，请参阅在 OpenStack 上部署托管的 control plane 。

1.3.7. IBM Power

OpenShift Container Platform 4.19 上的 IBM Power® 发行版本为 OpenShift Container Platform 组件添加了改进和新功能。

此发行版本引进了对 IBM Power 中的以下功能的支持：

- 使用国防信息系统局安全技术实施指南(DISA STIG)扩展 Compliance Operator 支持

1.3.8. IBM Z 和 IBM LinuxONE

OpenShift Container Platform 4.19 上的 IBM Z® 和 IBM® LinuxONE 版本为 OpenShift Container Platform 组件增加了改进和新功能。

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

- 支持 IBM® z17 和 IBM® LinuxONE 5
- 通过 IBM® Crypto Express (CEX) 引导卷 Linux 统一密钥设置(LUKS)加密

IBM Power、IBM Z 和 IBM LinuxONE 支持列表

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

表 1.1. CSI 卷

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

表 1.2. Multus CNI 插件

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

表 1.3. OpenShift Container Platform 功能

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
使用 OpenShift CLI (**oc**) 将计算节点添加到内部集群	支持	支持
备用身份验证供应商	支持	支持
基于代理的安装程序	支持	支持
支持的安装程序	支持	支持
使用 Local Storage Operator 自动设备发现	不支持	支持
使用机器健康检查功能自动修复损坏的机器	不支持	不支持
IBM Cloud® 的云控制器管理器。	支持	不支持
在节点上控制过量使用和管理容器密度	不支持	不支持
CPU Manager	支持	支持
Cron 作业	支持	支持
Descheduler	支持	支持
Egress IP	支持	支持
加密数据存储在 etcd 中	支持	支持
FIPS 加密	支持	支持
Helm	支持	支持
Pod 横向自动扩展	支持	支持
托管 control plane	支持	支持
IBM 安全执行	不支持	支持
IBM Power® Virtual Server 的安装程序置备的基础架构支持	支持	不支持
在单一节点上安装	支持	支持
IPv6	支持	支持

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
用户定义项目的监控	支持	支持
多架构计算节点	支持	支持
多架构 control plane	支持	支持
多路径（Multipathing）	支持	支持
网络绑定磁盘加密 - 外部 Tang 服务器	支持	支持
Non-volatile memory express drives (NVMe)	支持	不支持
NX-gzip for Power10 （硬件加速）	支持	不支持
oc-mirror 插件	支持	支持
OpenShift CLI (**oc**) 插件	支持	支持
Operator API	支持	支持
OpenShift Virtualization	不支持	支持
OVN-Kubernetes，包括 IPsec 加密	支持	支持
PodDisruptionBudget	支持	支持
精度时间协议 (PTP) 硬件	不支持	不支持
Red Hat OpenShift Local	不支持	不支持
Scheduler 配置集	支持	支持
安全引导	不支持	支持
流控制传输协议 (SCTP)	支持	支持
支持多个网络接口	支持	支持
openshift-install 工具支持 IBM Power® 上的各种 SMT 级别 (Hardware Acceleration)	支持	不支持
三节点集群支持	支持	支持
拓扑管理器	支持	不支持

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
SCSI 磁盘中的 z/VM 模拟 FBA 设备	不支持	支持
4K FCP 块设备	支持	支持

表 1.4. Operator

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
cert-manager Operator for Red Hat OpenShift	支持	支持
Cluster Logging Operator	支持	支持
Cluster Resource Override Operator	支持	支持
Compliance Operator	支持	支持
Cost Management Metrics Operator	支持	支持
File Integrity Operator	支持	支持
HyperShift Operator	支持	支持
IBM Power® Virtual Server Block CSI Driver Operator	支持	不支持
Ingress Node Firewall Operator	支持	支持
Local Storage Operator	支持	支持
MetalLB Operator	支持	支持
Network Observability Operator	支持	支持
NFD Operator	支持	支持
NMState Operator	支持	支持
OpenShift Elasticsearch Operator	支持	支持
Vertical Pod Autoscaler Operator	支持	支持

表 1.5. 持久性存储选项

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

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

1.3.9. Insights Operator

1.3.9.1. Insights Runtime Extractor 已正式发布

在 OpenShift Container Platform 4.18 中，Insights Operator 引入了 *Insights Runtime Extractor* 工作负载数据收集功能作为技术预览功能，以帮助红帽更好地了解容器的工作负载。现在，在 4.19 版本中，这个功能已正式发布。Insights Runtime Extractor 功能收集运行时工作负载数据并将其发送到红帽。

1.3.10. 安装和更新

1.3.10.1. 集群 API 替换 IBM Cloud 安装中的 Terraform

在 OpenShift Container Platform 4.19 中，安装程序使用 Cluster API 而不是 Terraform 在 IBM Cloud 上安装时置备集群基础架构。

1.3.10.2. 在 Malaysia 和 Thailand 区域的 AWS 上安装集群

现在，您可以在 CC (**ap-southeast-5**) 和 Thailand (**ap-southeast-7**) 区域在 Amazon Web Services (AWS)上安装 OpenShift Container Platform 集群。

如需更多信息，请参阅支持的 Amazon Web Services (AWS)区域。

1.3.10.3. Cluster API 替换 Microsoft Azure Stack Hub 安装中的 Terraform

在 OpenShift Container Platform 4.19 中，安装程序使用 Cluster API 而不是 Terraform 在 Microsoft Azure Stack Hub 上的安装程序置备的基础架构安装过程中置备集群。

1.3.10.4. 添加了对其他 Microsoft Azure 实例类型的支持

基于 64 位 x86 架构的机器类型的额外 Microsoft Azure 实例类型已使用 OpenShift Container Platform 4.19 测试。

对于 Dxv6 机器集，测试了以下实例类型：

- **StandardDdsv6Family**
- **StandardDldsv6Family**
- **StandardDlsv6Family**
- **StandardDsv6Family**

对于 Lsv4 和 Lasv4 机器系列，测试了以下实例类型：

- **standardLasv4Family**
- **standardLsv4Family**

对于 ND 和 NV 机器集，测试了以下实例类型：

- **StandardNVadsV710v5Family**
- **Standard NDASv4_A100 Family**

如需更多信息，请参阅 Tested instance types for Azure and Azure documentation（Microsoft 文档）

1.3.10.5. Microsoft Azure 中虚拟机的出站访问将停用

2025 年 9 月 30 日，Microsoft Azure 中所有虚拟机(VM)的默认出站访问连接将停用。为提高安全性，Azure 正在转向一个安全的默认模型，该模型将关闭对互联网的默认出站访问。但是，不需要更改 OpenShift Container Platform。默认情况下，安装程序会为负载均衡器创建一个出站规则。

如需更多信息，请参阅 Azure Updates (Microsoft 文档)、Azure 的出站连接方法 (Microsoft 文档)和 准备在 Azure 上安装集群。

1.3.10.6. GCP 的其他机密计算平台

在这个版本中，您可以在 GCP 上使用额外的机密计算（Confidential Computing）平台。安装前可在 **install-config.yaml** 文件中启用新的支持的平台，或使用机器集和 control plane 机器集在安装后配置，如下：

- **AMDEncryptedVirtualization**，它启用了带有 AMD Secure Encrypted Virtualization (AMD SEV) 的机密计算
- **AMDEncryptedVirtualizationNestedPaging**，它启用了带有 AMD Secure Encrypted Virtualization Secure Nested Paging (AMD SEV-SNP) 的机密计算
- **IntelTrustedDomainExtensions**，它启用了带有 Intel Trusted Domain Extensions (Intel TDX) 的机密计算

如需更多信息，请参阅 Google Cloud Platform 的安装配置参数，使用机器集(control plane) 配置机密虚拟机，以及使用机器集(compute) 配置机密虚拟机。

1.3.10.7. 使用用户置备的 DNS 在 Google Cloud Platform (GCP) 上安装集群（技术预览）

在这个版本中，您可以启用用户置备的域名服务器(DNS) 而不是默认的集群置备 DNS 解决方案。例如，您的机构的安全策略可能不允许使用公共 DNS 服务，如 Google Cloud DNS。您只能为 API 和 Ingress 服务器的 IP 地址管理 DNS。如果使用这个功能，您必须提供自己的 DNS 解决方案，其中包含 **api.<cluster_name>.<base_domain>.** 和 ***.apps.<cluster_name>.<base_domain>.** 的记录。启用用户置备的 DNS 作为技术预览提供。

如需更多信息，请参阅启用用户管理的 DNS。

1.3.10.8. 使用多个磁盘在 VMware vSphere 上安装集群（技术预览）

在这个版本中，您可以使用多个存储磁盘在 VMware vSphere 上安装集群（技术预览功能）。您可以将这些额外磁盘分配给集群中的特殊功能，如 etcd 存储。

如需更多信息，请参阅可选 vSphere 配置参数。

1.3.10.9. 在 Microsoft Azure 上安装时启用引导诊断集合

在这个版本中，您可以在 Microsoft Azure 上安装集群时启用引导诊断集合。引导诊断是 Azure 虚拟机(VM)的调试功能，用于识别虚拟机引导失败。您可以为计算机器、control plane 机器或所有机器在 **install-config.yaml** 文件中设置 **bootDiagnostics** 参数。

如需更多信息，请参阅其他 Azure 配置参数。

1.3.10.10. 从 OpenShift Container Platform 4.18 更新至 4.19 时所需的管理员确认

OpenShift Container Platform 4.19 使用 Kubernetes 1.32，它删除了几个已弃用的 API。

集群管理员必须在从 OpenShift Container Platform 4.18 升级到 4.19 前提供手动确认。这有助于防止升级到 OpenShift Container Platform 4.19 后出现问题，防止仍然使用已删除的 API 运行工作负载、工具或于集群进行交互的组件。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 4.18 集群都需要此管理员确认，然后才能升级到 OpenShift Container Platform 4.19。

如需更多信息，请参阅 准备升级到 OpenShift Container Platform 4.19。

1.3.10.11. OpenShift zones 支持 vSphere 主机组（技术预览）

在这个版本中，您可以将 OpenShift Container Platform 故障域映射到 VMware vSphere 主机组。这可让您使用 vSphere 扩展集群配置提供的高可用性。此功能在 OpenShift Container Platform 4.19 中作为技术预览提供。

有关在安装时配置主机组的详情，请参考 VMware vSphere 主机组启用。

有关为现有集群配置主机组的详情，请参考在 vSphere 上为集群指定多个主机组。

1.3.10.12. Nutanix 支持基于代理的安装程序

在这个版本中，您可以使用基于代理的安装程序在 Nutanix 上安装集群。通过在 **install-config.yaml** 文件中将 **platform** 参数设置为 **nutanix** 来启用，在 Nutanix 上安装集群。

如需更多信息，请参阅基于代理的安装程序文档中的 所需的配置参数。

1.3.11. Machine Config Operator

1.3.11.1. 功能的新命名

Red Hat Enterprise Linux CoreOS (RHCOS) 镜像分层 现在称为 *OpenShift 的镜像模式*。作为此更改的一部分，*on-cluster layering* 现在称为 *on-cluster 镜像模式*，*out-of-cluster layering* 现在称为 *out-of-cluster 镜像模式*。

更新的引导镜像 功能现在被称为 *引导镜像管理*。

1.3.11.2. OpenShift 的镜像模式现已正式发布

OpenShift 的镜像模式（以前称为 on-cluster layering）现已正式发布 (GA)。在升级到 GA 时引进了以下更改：

- API 版本现在是 **machineconfiguration.openshift.io/v1**。新版本包括以下更改：
  - **baseImagePullSecret** 参数现在是可选的。如果没有指定，则使用默认的 **global-pull-secret-copy**。
  - 不再需要 **buildInputs** 参数。之前在 **buildInputs** 参数下的所有参数都会提升一个级别。
  - **containerfileArch** 参数现在支持多个架构。在以前的版本中，只支持 **noarch**。
  - 所需的 **imageBuilderType** 现在为 **Job**。在以前的版本中，所需的构建器是 **PodImageBuilder**。
  - **renderedImagePushspec** 参数现在是 **renderedImagePushSpec**。
  - 不再需要 **buildOutputs** 和 **currentImagePullSecret** 参数。
- **oc describe MachineOSConfig** 和 **oc describe MachineOSBuild** 命令的输出有多处区别。
- **global-pull-secret-copy** 会自动添加到 **openshift-machine-config-operator** 命名空间中。
- 现在，您可以通过从 **MachineOSConfig** 对象中删除标签将 on-cluster 自定义分层镜像恢复到基础镜像。
- 现在，您可以通过删除关联的 **MachineOSBuild** 对象来自动删除 on-cluster 自定义分层镜像。
- Machine Config Operator 的 **must-gather** 现在包含 **MachineOSConfig** 和 **MachineOSBuild** 对象中的数据。
- 现在在断开连接的环境中支持集群分层。
- 现在，单一节点 OpenShift (SNO) 集群中支持集群分层。

1.3.11.3. 现在，Google Cloud Platform (GCP) 和 Amazon Web Services (AWS) 的引导镜像管理是默认的

引导镜像管理功能（以前称为更新的引导镜像）现在是 Google Cloud Platform (GCP) 和 Amazon Web Services (AWS) 集群中的默认行为。因此，在升级到 OpenShift Container Platform 4.19 后，集群中的引导镜像会自动更新至 4.19 版本。在这个版本中，Machine Config Operator (MCO)会再次更新集群中的引导镜像。引导镜像与机器集关联，在扩展新节点时使用。您在更新后创建的所有新节点都基于新版本。当前节点不受此功能的影响。

在升级到 4.19 之前，您必须选择不使用此默认行为，或在继续操作前确认这个更改。如需更多信息，请参阅禁用引导镜像管理。

注意

受管引导镜像功能仅适用于 GCP 和 AWS 集群。对于所有其他平台，MCO 不使用每个集群更新更新引导镜像。

1.3.11.4. 对 Machine Config Operator 证书的更改

安装程序创建的 Machine Config Server (MCS) CA 捆绑包现在存储在 **openshift-machine-config-operator** 命名空间中的 **machine-config-server-ca** 配置映射中。该捆绑包以前存储在 **kube-system** 命名空间中的 **root-ca** configmap 中。更新为 OpenShift Container Platform 4.19 的集群不再使用 **root-ca** configmap。进行这个改变的原因是，明确表明此 CA 捆绑包由 Machine Config Operator (MCO) 管理。

MCS 签名密钥存储在 **openshift-machine-config-operator** 命名空间中的 **machine-config-server-ca** secret 中。

MCS CA 和 MCS 证书在 10 年内有效，并且 MCO 在大约 8 年内自动轮转。在升级到 OpenShift Container Platform 4.19 后，CA 签名密钥不存在。因此，当 MCO 证书控制器启动时，CA 捆绑包会立即被视为过期。这个过期行为会导致证书立即轮转，即使集群还没有到 10 年。在这之后，下一个轮转会在标准的 8 年内进行。

如需有关 MCO 证书的更多信息，请参阅 Machine Config Operator 证书。

1.3.12. 机器管理

1.3.12.1. 在 Cluster API 和 Machine API 之间迁移资源（技术预览）

在这个版本中，您可以在 Cluster API 和 Amazon Web Services (AWS) 上的 Machine API 间迁移一些资源作为技术预览功能。如需更多信息，请参阅将 Machine API 资源迁移到集群 API 资源 。

为了支持此功能，OpenShift Container Platform Cluster API 文档现在包含 AWS 集群的额外配置详情。

1.3.12.2. control plane 机器名称的自定义前缀

在这个版本中，您可以自定义 control plane 机器集创建的机器名称前缀。通过修改 **ControlPlaneMachineSet** 自定义资源的 **spec.machineNamePrefix** 参数来启用此功能。

如需更多信息，请参阅在 control plane 机器名称中添加自定义前缀。

1.3.12.3. 在 Amazon Web Services 集群上配置容量保留

在这个版本中，您可以在 Amazon Web Services 集群中部署使用 Capacity Reservations 的机器，包括 On-Demand Capacity Reservations 和 Capacity Blocks for ML。

您可以使用 计算和 control plane 机器集配置这些功能。

1.3.12.4. 支持多个 VMware vSphere 数据磁盘（技术预览）

在这个版本中，您可以将最多 29 个磁盘添加到 vSphere 集群的虚拟机(VM)控制器中作为技术预览功能。此功能可用于 compute 和 control plane 机器集。

1.3.13. 监控

此发行版本中的集群监控堆栈包括以下新功能和修改后的功能：

1.3.13.1. 监控堆栈组件和依赖项更新

此发行版本包括对集群监控堆栈组件和依赖项的以下版本更新：

- Alertmanager 更新到 0.28.1
- Prometheus 更新到 3.2.1
- Prometheus Operator 更新到 0.81.0
- Thanos 更新到 0.37.2
- kube-state-metrics 更新到 2.15.0
- node-exporter 更新到 1.9.1

1.3.13.2. 对警报规则的更改

注意

红帽不保证记录规则或警报规则的向后兼容性。

- 添加了 **PrometheusPossibleNarrowSelectors** 警报，以便在 PromQL 查询或指标重新标记配置使用选择器，这可能不考虑经典直方上 **le** 标签的值，或摘要中的 **quantile** 标签是 Prometheus v3。如需更多信息，请参阅"Prometheus v3 升级"部分。

1.3.13.3. Prometheus v3 升级

此发行版本为 Prometheus 组件引入了一个重大更新，从 v2 转换到 v3。监控堆栈和其他核心组件包括所有必要的调整，以确保平稳升级。但是，一些用户管理的配置可能需要修改。主要更改包括以下项目：

- 经典直方的 **le** 标签值和摘要的定量 **标签值** 在 ingestion 过程中是规范化的。例如，**example_bucket{le="10"}** 指标选择器是 ingested 为 **example_bucket{le="10.0"}**。因此，警报、记录规则、仪表板和重新标记将标签值作为整数（如 **le="10"** ）的配置可能无法正常工作。
  要缓解这个问题，请更新您的选择器：
  - 如果您的查询需要在 Prometheus 升级前和之后覆盖数据，例如，使用正则表达式 **example_bucket{le=~"10 (.0)?"}**。
  - 对于仅在升级后覆盖数据的查询，请使用浮点值，例如 **le="10.0"**。
- 使用 Alertmanager v1 API 通过 **additionalAlertmanagerConfigs** 将警报发送到额外的 Alertmanager 实例的配置不再被支持。
  要缓解这个问题，请升级任何受影响的 Alertmanager 实例来支持 v2 API，从 Alertmanager **v0.16.0** 开始被支持，并更新您的监控配置以使用 v2 方案。

有关 Prometheus v2 和 v3 之间的更改的更多信息，请参阅 Prometheus 3.0 迁移指南。

1.3.13.4. 指标集合配置集已正式发布

OpenShift Container Platform 4.13 引入了为默认平台监控设置指标集合配置集的功能，以收集默认指标数据量或最小指标数据。在 OpenShift Container Platform 4.19 中，指标集合配置集现已正式发布。

如需更多信息，请参阅关于指标集合配置集和删除指标集合配置集。

1.3.13.5. 添加了对外部 Alertmanager 实例的集群代理支持

在这个版本中，外部 Alertmanager 实例使用集群范围的 HTTP 代理设置进行通信。Cluster Monitoring Operator (CMO) 读取集群范围的代理设置，并为 Alertmanager 端点配置适当的代理 URL。

1.3.13.6. 改进了 Cluster Monitoring Operator 的严格验证

在这个版本中，OpenShift Container Platform 4.18 中引入的严格验证有所改进。错误消息现在明确识别受影响的字段，验证区分大小写，以确保更准确和一致的配置。

如需更多信息，请参阅(OCPBUGS-42671)和(OCPBUGS-54516)。

1.3.14. 网络

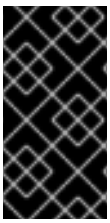
1.3.14.1. 使用外部管理证书创建路由（正式发布）

在这个版本中，OpenShift Container Platform 路由可以使用第三方证书管理解决方案来配置，使用路由 API 中的 **.spec.tls.externalCertificate** 字段。这可让您通过 secret 引用外部管理的 TLS 证书，通过消除手动证书管理来简化流程。通过使用外部受管证书，您可以减少错误，确保证书更新过程，并使 OpenShift 路由器能够及时提供更新的证书。如需更多信息，请参阅使用外部管理的证书创建路由。

1.3.14.2. 支持使用网关 API 配置集群入口流量 (正式发布)

在这个版本中，支持使用网关 API 资源管理集群入口流量的支持正式发布。网关 API 在传输层 L4 和应用程序层 L7 中提供了强大的网络解决方案，用于使用标准化开源生态系统的 OpenShift Container Platform 集群。

如需更多信息，请参阅使用 OpenShift Container Platform 网络 的网关 API 。



重要

网关 API 资源必须符合支持的 OpenShift Container Platform API 面。这意味着，在 OpenShift Container Platform 的 Gateway API 中，您无法使用另一个特定于供应商的资源，如 Istio 的 VirtualService。如需更多信息，请参阅 OpenShift Container Platform 的网关 API 实现。

1.3.14.3. 支持管理网关 API 自定义资源定义(CRD)生命周期

在这个版本中，OpenShift Container Platform 管理网关 API CRD 的生命周期。这意味着 Ingress Operator 处理资源所需的版本控制和管理。必须重新创建并重新部署之前 OpenShift Container Platform 版本中创建的网关 API 资源，以符合 Ingress Operator 所需的规格。

如需更多信息，请参阅 Ingress Operator 准备网关 API 管理成功。

1.3.14.4. Gateway API 自定义资源定义 (CRD) 的更新

OpenShift Container Platform 4.19 将 Red Hat OpenShift Service Mesh 更新至 3.0.2 版本，并将网关 API 更新至 1.2.1 版本。如需更多信息，请参阅 Service Mesh 3.0.0 发行注记 和 Gateway API 1.2.1 changelog。

1.3.14.5. 为集群启用 OVS balance-slb 模式（通用可用性）

您可以在集群运行的基础架构上启用 Open vSwitch (OVS) **balance-slb** 模式，以便两个或者多个物理接口可以共享其网络流量。如需更多信息，请参阅为集群启用 OVS balance-slb 模式。

1.3.14.6. 将 API 和入口负载均衡器分配给特定子网

在这个版本中，您可以在 AWS 上安装 OpenShift Container Platform 集群时分配负载均衡器来自定义部署。此功能确保最佳流量分布、高应用程序可用性、不间断的服务和网络分段。

如需更多信息，请参阅 AWS 上的安装配置参数，并将负载均衡器分配到特定的子网。

1.3.14.7. 用于改进 PTP 普通时钟中的冗余的双端口 NIC （技术预览）

在这个版本中，您可以使用双端口网络接口控制器(NIC) 来提高精确时间协议 (PTP) 普通时钟的冗余。在普通时钟的双端口 NIC 配置中，如果一个端口失败，则备用端口会接管，维护 PTP 时间同步（技术预览）。

注意

您只能在带有双端口 NIC 的 **x86** 架构节点上配置 PTP 普通时钟。

如需更多信息，请参阅使用双端口 NIC 来提高 PTP 普通时钟的冗余。

1.3.14.8. 支持在 SR-IOV Network Operator 中匹配的条件 Webhook

现在，您可以在 **SriovOperatorConfig** 对象中启用 **featureGates.resourceInjectorMatchCondition** 功能，以限制 Network Resources Injector Webhook 的范围。如果启用了此功能，则 Webhook 仅适用于带有二级网络注解 **k8s.v1.cni.cncf.io/networks** 的 pod。

如果禁用了此功能，则 webhook 的 **failurePolicy** 默认设置为 **Ignore**。如果 Webhook 不可用，此配置可能会导致在没有所需的资源注入的情况下 pod 请求 SR-IOV 网络被部署。如果启用了此功能，并且 webhook 不可用，没有注解的 pod 仍然会被部署，从而导致对其他工作负载造成不必要的中断。

如需更多信息，请参阅关于网络资源注入器

1.3.14.9. 使用 DPU Operator 启用 DPU 设备管理

在这个版本中，OpenShift Container Platform 引入了 Data Processing Unit (DPU) Operator，并使用 Operator 管理 DPU 设备。DPU Operator 管理配置了 DPU 的计算节点上组件，如启用数据网络、存储和安全工作负载的卸载。启用 DPU 设备管理可提高集群性能、缩短延迟和增强的安全性，这整体有助于提高集群基础架构的效率。如需更多信息，请参阅关于 DPU 和 DPU Operator。

1.3.14.10. 用户定义的网络的 localnet 拓扑（正式发布）

管理员现在可以使用 **ClusterUserDefinedNetwork** 自定义资源在 **Localnet** 拓扑上部署二级网络。此功能允许连接到 localnet 网络的 pod 和虚拟机出口到物理网络。如需更多信息，请参阅为 Localnet 拓扑创建 ClusterUserDefinedNetwork CR。

1.3.14.11. 为 Linux 网桥 NAD 启用端口隔离（正式发布）

您可以为 Linux 网桥网络附加定义(NAD)启用端口隔离，以便在同一虚拟 LAN (VLAN)上运行的虚拟机或 pod 可以相互隔离。如需更多信息，请参阅为 Linux 网桥 NAD 启用端口隔离 。

1.3.14.12. Whereabouts IPAM CNI 插件的快速 IPAM 配置（技术预览）

要提高 Whereabouts 的性能，特别是当集群中的节点运行大量 pod 时，您现在可以启用 Fast IP 地址管理(IPAM)功能。Fast IPAM 功能使用 **nodeslicepools** （由 Whereabouts Controller 管理）来优化节点的 IP 地址分配。如需更多信息，请参阅 Whereabouts IPAM CNI 插件的 Fast IPAM 配置 。

1.3.14.13. Unnumbered BGP peering （技术预览）

在这个版本中，OpenShift Container Platform 引入了未编号的 BGP peering。作为技术预览提供，您可以使用 BGP peer 自定义资源的 **spec.interface** 字段来配置未编号的 BGP 对等。

1.3.14.14. 创建自定义 DNS 主机名以解决 DNS 连接问题

在无法访问外部 DNS 服务器的断开连接的环境中，您可以通过在 NMState 自定义资源定义(CRD)中指定自定义 DNS 主机名来解决 Kubernetes **NMState** Operator 健康探测问题。如需更多信息，请参阅 创建自定义 DNS 主机名以解决 DNS 连接问题。

1.3.14.15. 删除 PTP 事件 REST API v1 和事件消费者应用程序 sidecar

在这个版本中，PTP 事件 REST API v1 和事件消费者应用程序 sidecar 支持会被删除。

您必须使用兼容 O-RAN 的 PTP 事件 REST API v2 替代。

如需更多信息，请参阅使用 REST API v2 开发 PTP 事件消费者应用程序 。

1.3.14.16. 重新添加启用 RouteExternalCertificate 功能门删除的 secret

如果您为集群启用了 **RouteExternalCertificate** 功能门，您现在可以重新添加之前删除的 secret。(OCPBUGS-33958)

1.3.15. OpenShift CLI (oc)

1.3.15.1. 在 oc-mirror 插件 v2 中镜像和验证镜像签名

从 OpenShift Container Platform 4.19 开始，oc-mirror 插件 v2 支持镜像和验证容器镜像的基于 cosign 标签的签名。

1.3.16. Operator 开发

1.3.16.1. 支持的 Operator 基础镜像

以下 Operator 项目的基础镜像已更新，以便与 OpenShift Container Platform 4.19 兼容。这些基础镜像的运行时功能和配置 API 仍然会有程序错误修复和并提供对相关 CVE 的解决方案。

- 基于 Ansible 的 Operator 项目的基础镜像
- 基于 Helm 的 Operator 项目的基础镜像

如需更多信息，请参阅为 OpenShift Container Platform 4.19 及之后的版本（红帽知识库）为现有基于 Ansible 或 Helm 的 Operator 项目更新基础镜像。

1.3.17. 安装后配置

1.3.17.1. 使用裸机作为服务（技术预览）

在 OpenShift Container Platform 4.19 中，您可以使用裸机作为服务(BMaaS)部署非 OpenShift Container Platform 节点。BMaaS 节点可以运行可能不适用于容器化或虚拟化的工作负载。例如，需要直接访问硬件、执行高性能计算任务或传统应用程序以及独立于集群的运行等工作负载适合使用 BMaaS 部署。

如需更多信息，请参阅使用裸机作为服务。

1.3.18. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.18.1. RHCOS 使用 RHEL 9.6

RHCOS 在 OpenShift Container Platform 4.19 中使用 Red Hat Enterprise Linux (RHEL) 9.6 软件包。这些软件包可确保 OpenShift Container Platform 实例收到最新的修复、功能、增强功能、硬件支持和驱动程序更新。

1.3.19. 可伸缩性和性能

1.3.19.1. 性能配置集内核页大小配置

在这个版本中，您可以指定更大的内核页大小，以提高在禁用实时内核的 ARM 基础架构节点上的内存密集型、高性能工作负载的性能。如需更多信息，请参阅配置内核页大小。

1.3.19.2. cluster-compare 插件的更新

此发行版本包括 **cluster-compare** 插件的以下可用性和功能更新：

- 更有效地匹配捕获组 ：现在，您可以使用改进的捕获组处理更加精确地匹配模板之间的匹配。
- 生成 JUnit 输出：您可以使用 **-o junit** 标志以 **junit** 格式输出结果，从而更轻松地与测试或 CI/CD 系统集成。
- **sprig** 功能支持：**cluster-compare** 插件支持所有 **sprig** 库函数，但 **env** 和 **expandenv** 除外。有关 sprig 库函数的完整列表，请参阅 Sprig Function 文档。

有关可用模板功能的完整列表，请参阅参考模板功能

1.3.19.3. 使用性能配置集调整托管的 control plane

在这个版本中，您可以通过应用性能配置集来调整托管 control plane 中的节点以实现低延迟。如需更多信息，请参阅为托管 control plane 创建性能配置集。

1.3.20. 安全性

1.3.20.1. control plane 现在支持 TLS 1.3 和 Modern TLS 安全配置集

在这个版本中，control plane 支持 TLS 1.3。现在，您可以将 **Modern** TLS 安全配置集用于 control plane。

如需更多信息，请参阅为 control plane 配置 TLS 安全配置集。

1.3.20.2. Red Hat OpenShift 的 External Secrets Operator （技术预览）

在这个版本中，您可以使用 Red Hat OpenShift 的 External Secrets Operator 与外部 secret 存储进行身份验证，检索 secret，并将检索到的 secret 注入原生 Kubernetes secret。Red Hat OpenShift 的 External Secrets Operator 作为技术预览提供。

如需更多信息，请参阅 Red Hat OpenShift 的外部 Secrets Operator 概述

1.3.21. 存储

1.3.21.1. 在断开连接的环境中支持 Secret Store CSI 驱动程序

在这个版本中，secret 存储供应商支持在断开连接的集群中使用 Secrets Store CSI 驱动程序。

如需更多信息，请参阅对断开连接的环境的支持。

1.3.21.2. Azure File 跨订阅支持已正式发布

通过跨订阅支持，您可以在一个 Azure 订阅中有一个 OpenShift Container Platform 集群，并使用 Azure File Container Storage Interface (CSI) 驱动程序将 Azure 文件共享挂载到另一个 Azure 订阅中。订阅必须位于同一租户中。

此功能在 OpenShift Container Platform 4.19 中正式发布。

如需更多信息，请参阅 AWS EFS CSI 跨帐户支持。

1.3.21.3. 卷属性类（技术预览）

卷属性类为管理员提供了描述它们所提供的存储的"类"的方式。不同的类可能对应于不同的服务质量级别。

OpenShift Container Platform 4.19 中的卷属性类仅适用于 AWS Elastic Block Storage (EBS) 和 Google Cloud Platform (GCP) 持久磁盘 (PD) 容器存储接口 (CSI)。

您可以将卷属性类应用到持久性卷声明 (PVC)。如果集群中有新卷属性类，如果需要，您可以使用新卷属性类更新 PVC。

卷属性类具有描述属于它们的卷的参数。如果省略了参数，则在卷置备过程中会使用默认值。如果用户使用带有忽略参数的不同 Volume Attributes Class 应用 PVC，则参数的默认值可能会根据 CSI 驱动程序实现使用。如需更多信息，请参阅相关的 CSI 驱动程序文档。

OpenShift Container Platform 4.19 中提供了卷属性类，且状态为技术预览。

有关更多信息，请参阅卷属性类。

1.3.21.4. 新的 CLI 命令以显示 PVC 使用情况（技术预览）

OpenShift Container Platform 4.19 引入了一个新的命令来查看持久性卷声明使用情况。此功能为技术预览状态。

如需更多信息，请参阅查看 PVC 用量统计。

1.3.21.5. CSI 卷重新定义大小恢复已正式发布

在以前的版本中，您可以将持久性卷声明 (PVC) 扩展到底层存储供应商不支持的大小。在这种情况下，扩展控制器通常会尝试扩展卷并保留失败。

这个新功能允许您恢复并为 PVC 提供另一个调整大小的值。OpenShift Container Platform 4.19 中支持重新定义大小恢复。

有关重新定义卷的大小的更多信息，请参阅 扩展持久性卷。

有关在重新定义卷的大小时恢复的更多信息，请参阅在扩展卷时恢复失败。

1.3.21.6. 支持重新定义 vSphere in-tree 迁移的卷大小

在以前的版本中，从 in-tree 迁移到 Container Storage Interface (CSI)的 VMware vSphere 持久性卷无法调整大小。在 OpenShift Container Platform 4.19 中，支持重新定义迁移的卷大小。这个功能已正式发布。

有关重新定义卷的大小的更多信息，请参阅 扩展持久性卷。

1.3.21.7. 在 vSphere 上禁用和启用存储已正式发布

集群管理员可能希望禁用 VMWare vSphere Container Storage Interface (CSI) 驱动程序作为第 2 天操作，因此 vSphere CSI 驱动程序不与您的 vSphere 设置接口。

此功能在 OpenShift Container Platform 4.17 中引入，为技术预览。此功能现在 OpenShift Container Platform 4.19 中已正式发布。

如需更多信息，请参阅在 vSphere 上禁用和启用存储。

1.3.21.8. 为 vSphere 增加每个节点的最大卷数量（技术预览）

对于 VMware vSphere 版本 7，OpenShift Container Platform 将每个节点的最大卷数量限制为 59。

但是，对于 vSphere 版本 8 或更高版本的 OpenShift Container Platform 4.19，您可以将每个节点的允许数量增加到最多 255 个。否则，默认值保持在 59。

此功能为技术预览状态。

如需更多信息，请参阅为 vSphere 增加每个节点的最大卷。

1.3.21.9. 完全支持在 vSphere 的数据存储之间迁移 CNS 卷

如果在当前数据存储的空间正在被耗尽，或希望移至性能更高的数据存储，您可以在数据存储之间迁移 VMware vSphere Cloud Native Storage (CNS)卷。这适用于附加的卷和分离的卷。

OpenShift Container Platform 现在完全支持使用 vCenter UI 迁移 CNS 卷。迁移的卷应可以按预期工作，不会造成持久性卷无法正常工作。CNS 卷也可以在被 pod 使用时被迁移。

此功能在 OpenShift Container Platform 4.17 中作为开发预览引进，现在在 4.19 中被完全支持。

在数据存储之间迁移 CNS 卷需要 VMware vSphere 8.0.2 或更高版本，或 vSphere 7.0 Update 3o 或更高版本。

如需更多信息，请参阅为 vSphere 在数据存储间迁移 CNS 卷 。

1.3.21.10. Filestore 存储类的 NFS 导出选项已正式发布。

默认情况下，Filestore 实例向共享同一 Google Cloud 项目和虚拟私有云(VPC)网络的所有客户端授予 root 级别的读/写访问权限。网络文件系统(NFS)导出选项可以限制此访问权限限制为 Filestore 实例的某些 IP 范围和特定用户/组 ID。在创建存储类时，您可以使用 **nfs-export-options-on-create** 参数设置这些

选项。

OpenShift Container Platform 4.19 中支持 NFS 导出选项。

如需更多信息，请参阅 NFS 导出选项。

1.3.22. Web 控制台

从 OpenShift Container Platform 4.19 开始，web 控制台中的视角可以统一简化导航、减少上下文切换、简化任务，并为用户提供更加统一的 OpenShift Container Platform 体验。

通过这种统一设计，默认视图中不再有 **Developer** 视角，但*所有* OpenShift Container Platform Web 控制台功能都可以被所有用户发现。如果您不是集群所有者，您可能需要从集群所有者请求权限。如果需要，仍可手动启用 **Developer** 视角。

在 web 控制台中的 **Getting Started** 窗格中，您可以浏览控制台，查找有关设置集群的信息，查看启用 **Developer** 视角的快速启动，并按照链接探索新功能。

1.3.22.1. PatternFly 6 升级

Web 控制台现在使用 Patternfly 6。在 web 控制台中不再支持 Patternfly 4。

此发行版本还在 web 控制台中引进了以下更新。现在您可以执行以下操作：

- 使用 **.spec.customization.logos** 配置中的 **logos** 字段为 light 和 dark 主题指定不同的控制台徽标，允许更全面的品牌。
- 从 web 控制台轻松删除身份提供程序(IDP)，简化身份验证配置，而无需手动 YAML 文件编辑。
- 在 web 控制台中直接设置默认 **StorageClass**。
- 通过按创建日期和时间对 **Created** 列进行排序，快速查找 web 控制台中的特定作业。

1.4. 主要的技术变化

1.4.1. 将 readOnlyRootFilesystem 设置为 true 的 Pod 部署

在这个版本中，Cloud Credential Operator pod 使用 **readOnlyRootFilesystem** 安全上下文设置为 **true** 部署。这提高了安全性，确保容器根文件系统以只读形式挂载。

1.4.2. kube-apiserver 的 loopback 证书的有效性延长到三年

在以前的版本中，Kubernetes API 服务器的自签名 loopback 证书在一年后过期。在这个版本中，证书的过期日期将延长至三年。

1.4.3. 就绪度探测排除了 etcd 检查

API 服务器的就绪度探测已被修改以排除 etcd 检查。这可防止在 etcd 临时不可用时关闭客户端连接。这意味着，客户端连接在 etcd 不可用的情况下保留，并最小化临时 API 服务器中断。

1.4.4. 安装程序自动删除剩余的 Cloud Native Storage (CNS)卷

现在，在删除集群时，OpenShift 安装程序会自动检测并删除 VMware vSphere 上的保留持久性存储卷。这可防止孤立的卷消耗磁盘空间，并在 vCenter 中创建不必要的警报。

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 4.19 中已弃用并删除的主要功能的最新列表，请参考下表。表后列出了更多已弃用和删除的功能的更多详细信息。

在以下表格中，功能被标记为以下状态：

- *不可用*
- *技术预览*
- *公开发行*
- *已弃用*
- *删除*

裸机监控已弃用和删除的功能

表 1.6. 裸机事件中继 Operator tracker

功能	4.17	4.18	4.19
裸机事件中继 Operator	删除	删除	删除

镜像已弃用和删除的功能

表 1.7. 镜像已弃用和删除的 tracker

功能	4.17	4.18	4.19
Cluster Samples Operator	已弃用	已弃用	Deprecated

安装已弃用和删除的功能

表 1.8. 安装已弃用并删除跟踪器

功能	4.17	4.18	4.19
oc adm release extract 的 **--cloud** 参数	已弃用	Deprecated	Deprecated
对 **cluster.local** 域的 CoreDNS 通配符查询	Deprecated	Deprecated	Deprecated
compute.platform.openstack.rootVolume.type for RHOSP	已弃用	已弃用	已弃用
controlPlane.platform.openstack.rootVolume.type for RHOSP	Deprecated	Deprecated	Deprecated

功能	4.17	4.18	4.19
安装程序置备的基础架构集群的 **install-config.yaml** 文件中的 **ingressVIP** 和 **apiVIP** 设置	Deprecated	Deprecated	Deprecated
基于软件包的 RHEL 计算机器	Deprecated	Deprecated	删除
用于 Amazon Web Services (AWS) 的**platform.aws.preserveBootstrapIgnition** 参数	Deprecated	Deprecated	Deprecated
在带有 AWS Outposts 中的计算节点的 AWS 上安装集群	Deprecated	Deprecated	已弃用

已弃用和删除的网络功能

表 1.9. 已弃用和删除的网络功能跟踪器

功能	4.17	4.18	4.19
iptables	已弃用	已弃用	已弃用

节点已弃用和删除的功能

表 1.10. 节点已弃用并删除 tracker

功能	4.17	4.18	4.19
ImageContentSourcePolicy (ICSP) 对象	已弃用	Deprecated	Deprecated
Kubernetes 拓扑标签 **failure-domain.beta.kubernetes.io/zone**	Deprecated	Deprecated	Deprecated
Kubernetes 拓扑标签 **failure-domain.beta.kubernetes.io/region**	已弃用	已弃用	已弃用
cgroup v1	已弃用	已弃用	删除

OpenShift CLI (oc) 已弃用和删除的功能

表 1.11. OpenShift CLI (oc) 已弃用并删除 tracker

功能	4.17	4.18	4.19
oc-mirror plugin v1	公开发行	Deprecated	已弃用

Operator 生命周期和开发已弃用和删除的功能

表 1.12. Operator 生命周期和开发已弃用并删除 tracker

功能	4.17	4.18	4.19
Operator SDK	Deprecated	Deprecated	删除
为基于 Ansible 的 Operator 项目构建工具	Deprecated	Deprecated	删除
为基于 Helm 的 Operator 项目构建工具	Deprecated	Deprecated	删除
为基于 Go 的 Operator 项目构建工具	Deprecated	Deprecated	删除
为基于 Helm 的 Operator 项目构建工具	Deprecated	删除	删除
为基于 Java 的 Operator 项目构建工具	Deprecated	删除	删除
Operator 目录的 SQLite 数据库格式	Deprecated	Deprecated	Deprecated

存储已弃用和删除的功能

表 1.13. 存储已弃用和删除的 tracker

功能	4.17	4.18	4.19
使用 FlexVolume 的持久性存储	Deprecated	Deprecated	Deprecated
AliCloud Disk CSI Driver Operator	删除	删除	删除
共享资源 CSI Driver Operator	Deprecated	删除	删除

更新集群已弃用和删除的功能

表 1.14. 更新集群已弃用并删除 tracker

功能	4.17	4.18	4.19

Web 控制台已弃用和删除的功能

表 1.15. Web 控制台已弃用并删除 tracker

功能	4.17	4.18	4.19
对动态插件 SDK 的 **useModal**	公开发行	公开发行	已弃用
PatternFly 4	已弃用	Deprecated	删除

工作负载已弃用和删除的功能

表 1.16. 工作负载已弃用和删除的 tracker

功能	4.17	4.18	4.19
deploymentConfig 对象	Deprecated	Deprecated	Deprecated

1.5.1. 弃用的功能

1.5.1.1. **oc adm pod-network** 命令已弃用

用于 OpenShift SDN 多租户模式的 **oc adm pod-network** 命令已从 **oc adm --help** 输出中删除。如果使用 **oc adm pod-network** 命令，会显示错误消息，以指示它已被弃用。

1.5.1.2. 对动态插件 SDK 的 useModal

在这个版本中，在动态插件中支持 **useModal** hook 的功能已被弃用。

从这个版本开始，使用 **useOverlay** API hook 启动模态

1.5.2. 删除的功能

1.5.2.1. 已删除 cgroup v1

OpenShift Container Platform 4.16 中已弃用的 cgroup v1 不再被支持，并已从 OpenShift Container Platform 中删除。如果您的集群使用 cgroup v1，您必须先配置 cgroup v2，然后才能升级到 OpenShift Container Platform 4.19。现在，所有工作负载必须与 cgroup v2 兼容。

有关在集群中配置 cgroup v2 的详情，请参考 OpenShift Container Platform 版本 4.18 文档中的配置 Linux cgroup。

有关 cgroup v2 的更多信息，请参阅关于 Linux cgroup version 2 和 Red Hat Enterprise Linux 9 changes in the context of Red Hat OpenShift workloads (红帽博客)。

1.5.2.2. 基于软件包的 RHEL 计算机器

在这个版本中，删除了安装基于打包的 RHEL worker 节点的支持。

RHCOS 镜像分层替换了这个功能，并支持在 worker 节点的基本操作系统上安装额外的软件包。

有关如何在集群中识别和删除 RHEL 节点的详情，请参考 准备从 OpenShift Container Platform 4.18 更新至更新的版本。如需有关镜像分层的更多信息，请参阅 RHCOS 镜像分层。

1.5.2.3. 从 Kubernetes 1.32 中删除的 API

Kubernetes 1.32 删除了以下已弃用的 API，因此您必须迁移清单和 API 客户端以使用适当的 API 版本。有关迁移删除 API 的更多信息，请参阅 Kubernetes 文档。

表 1.17. 从 Kubernetes 1.32 中删除的 API

资源	删除的 API	迁移到	主要变化

资源	删除的 API	迁移到	主要变化
FlowSchema	**flowcontrol.apiserver.k8s.io/v1beta3**	**flowcontrol.apiserver.k8s.io/v1**	否
PriorityLevelConfiguration	**flowcontrol.apiserver.k8s.io/v1beta3**	**flowcontrol.apiserver.k8s.io/v1**	是

1.5.2.4. Operator SDK CLI 和相关的构建和测试工具

在这个版本中，OpenShift Container Platform 不再发布红帽支持的 Operator SDK CLI 工具版本，包括相关的构建和测试工具。

红帽将根据 OpenShift Container Platform 4 （红帽客户门户网站）的产品生命周期，为早期版本的 OpenShift Container Platform 版本提供程序错误修正和支持。

现有 Operator 项目的 Operator 作者可以使用 OpenShift Container Platform 4.18 发布的 Operator SDK CLI 工具版本来维护其项目，并创建针对较新版本的 OpenShift Container Platform 的 Operator 发行版本。如需更多信息，请参阅为 OpenShift Container Platform 4.19 及之后的版本（红帽知识库）为现有基于 Ansible 或 Helm 的 Operator 项目更新基础镜像。

有关 Operator SDK 不支持的、社区维护版本的信息，请参阅 Operator SDK (Operator Framework)。

1.6. 程序错误修复

API 服务器和客户端

- 在以前的版本中，组 **machineconfiguration.openshift.io** 中的 **MachineConfig** 和 **ControllerConfig** 资源的内容没有从审计日志中排除。在这个版本中，它们不包括在审计日志中，因为它们可能包含 secret。(OCPBUGS-55709)
- 在以前的版本中，kube-apiserver 服务级别目标(SLO)警报表达式错误地、独立于总请求数地计算了读取和写入的成功比率。这会导致在中断期间，出现误导的 burn 比率的数据。在这个版本中进行了相关的修复，可以正确地根据请求总数计算成功比率。这使数据更加可靠。(OCPBUGS-49764)
- 在以前的版本中，如果 etcd 访问丢失，删除集群 bootstrap 可能会破坏 kube-apiserver 的就绪情况，这可能会导致停机。在这个版本中，在删除 bootstrap 前会保证每个 kube-apiserver 都有 2 个稳定的 etcd 端点，这可以保持推出时的可用性。(OCPBUGS-48673)
- 在以前的版本中，Static Pod Operator API 允许未设置 **currentRevision** 的，以及多个非零 **targetRevision** 条目的无效节点状态，这会导致节点和安装程序控制器失败。在这个版本中，添加了新的验证规则来强制正确的修订字段，以确保稳定且一致的静态 pod 状态处理。(OCPBUGS-46380)
- 在以前的版本中，节点控制器会从其列表器中应用过时的 **NodeStatus** 数据，从而意外覆盖其他控制器的最新更新。在这个版本中，使用受管字段使控制器在不冲突的情况下更新单独的条目，这样可保留准确和并发节点状态更新。(OCPBUGS-46372)
- 在以前的版本中，用于删除 etcd bootstrap 成员的一个固定的五分钟超时会过早启动。即使有足够的总时间，这也会导致 HA 集群中出现大量失败。在这个版本中，这个小的超时时间会依赖整个 bootstrap 进度启动，这样可确保可靠和仲裁安全的 etcd bootstrap 移除过程。(OCPBUGS-46363)

- 在以前的版本中，在检测两个 kube-apiserver 端点后，Bootstrap 会取消阻塞（包括 bootstrap 实例），从而导致一个持久性实例出现 0% 的可用性。在这个版本中，在多个永久实例就绪前，teardown 会被延迟。这样可确保在推出部署的过程中保持 kube-apiserver 的可用性。(OCPBUGS-46010)

- 在以前的版本中，当临时 control plane 停机时，**networkConfig.status.ServiceNetwork** 不会被填充，当生成的证书没有 SAN 中的 Kubernetes 服务 IP 时，客户端无法通过默认 kubernetes 服务连接到 kube-apiserver。在这个版本中，如果 **networkConfig.status.ServiceNetwork** 是 nil，会跳过证书生成。客户端连接将稳定且有效。(OCPBUGS-45943)

- 在以前的版本中，安装程序会在 etcd 成员被删除前删除 bootstrap 机器。这会导致 HA 集群中的仲裁丢失。在这个版本中，来自 SNO 的检查会扩展到所有拓扑，使用 etcd operator 的 condition 作为安全删除符号，这样可在 bootstrap teardown 过程中确保 etcd 集群稳定性。(OCPBUGS-45482)

- 在以前的版本中，当 CRD 请求处理过程中设置了 image 和 error 字段时，openshift-apiserver 可能会出现 panic，这会导致在某些情况下 API 服务器运行时崩溃和不稳定。在这个版本中，添加了一个保护功能，以便在两个字段未设置时安全地处理问题单来确保不会出现 panic，从而导致更强大的稳定的 CRD 请求处理进程不会崩溃。(OCPBUGS-45861)

裸机硬件置备

- 在以前的版本中，来自 Ironic Python Agent (IPA)的 NetworkManager 日志没有包括在 ramdisk 日志中，而是只包括 ramdisk 日志中的 **dmesg** 日志。在这个版本中，metal3 pod 的 **metal3-ramdisk-logs** 容器中存在 ramdisk 日志现在包含来自主机的整个日志，而不是只使用 **dmesg** 日志和 IPA。(OCPBUGS-56042)

- 在以前的版本中，ramdisk 日志不包括明确的文件分隔符，从而导致一个文件中的内容被合并到另一个文件的随机行中。因此，区分特定内容属于哪个文件会比较困难。在这个版本中，文件条目会包括文件分隔符，因此每个文件都可以与合并到 ramdisk 日志文件的其他文件区分。(OCPBUGS-55743)

- 在以前的版本中，如果您忘记了包含 Redfish 系统 ID，如 **redfish://host/redfish/v1/**，而不是 **redfish://host/redfish/v1/Self**，在 Baseboard Management Console (BMC) URL 中存在一个 JSON 解析问题。在这个版本中，BMO 可以在没有 Redfish 系统 ID 作为有效地址的情况下处理 URL，而不会造成 JSON 解析问题。(OCPBUGS-56026)

- 在以前的版本中，在置备过程中存在一个竞争条件，如果 DHCP 响应速度较慢，可能会导致用于机器和节点对象的不同主机名。这可以防止 worker 节点的 CSR 自动被批准。在这个版本中，竞争条件已被修复，worker 节点的 CSR 现在可以正确地批准。(OCPBUGS-55315)

- 在以前的版本中，某些 SuperMicro 机器模型（如 **ars-111gl-nhr** ）使用不同于其他 SuperMicro 机器的不同虚拟介质设备字符串，这可能会导致虚拟介质引导尝试在这些服务器上失败。在这个版本中，添加了一个额外的条件检查，以检查受影响的特定模型并相应地调整行为，以便 ars-111gl-nhr 等 SuperMicro 模型现在可以从虚拟介质引导。(OCPBUGS-56639)

- 在以前的版本中，在删除具有相关 **DataImage** 的 **BaremetalHost** 后，**DataImage** 仍然存在。在这个版本中，如果在 **BaremetalHost** 被删除后，**DataImage** 会被删除。(OCPBUGS-51294)

Cloud Compute

- 当升级使用与 UEFI 不兼容的引导磁盘的 GCP 集群时，您无法启用 Shielded VM 支持。在以前的版本中，这会阻止创建新的计算机器。在这个版本中，已知 UEFI 不兼容的磁盘会禁用 Shielded VM 支持。这主要会影响客户使用 GCP marketplace 镜像从 OpenShift Container Platform 版本 4.12 升级到 4.13。(OCPBUGS-17079)

- 在以前的版本中，在 Azure 上运行的集群中的虚拟机会失败，因为附加的网络接口控制器(NIC)处于 **ProvisioningFailed** 状态。在这个版本中，Machine API 控制器会检查 NIC 的置备状态，并定期刷新虚拟机以防止这个问题。(OCPBUGS-31515)

- 在以前的版本中，在使用证书签名请求(CSR)具有其他子系统的大型集群中，CSR 批准者计算不相关的、未批准的 CSR 总并阻止进一步批准。在这个版本中，CSR 批准者使用 **signerName** 属性作为过滤器，仅包含它可以被批准的 CSR。因此，当相关 **signerName** 值有大量未批准的 CSR 时，CSR 批准者才会防止新的批准。(OCPBUGS-36404)

- 在以前的版本中，Machine API 控制器只读了区号来填充机器区信息。对于只支持可用性集的 Azure 区域中的机器，集合号代表区，因此 Machine API 控制器不会填充其区信息。在这个版本中，Machine API 控制器引用 Azure fault domain 属性。此属性可用于可用性集和可用性区域，因此控制器在每次情况下都正确读取错误域，机器始终报告一个区域。(OCPBUGS-38570)

- 在以前的版本中，在 GCP 区 API 错误消息中增加粒度会导致机器控制器错误地将带有无效配置的机器标记为有效的，并带有临时云错误。这个行为会阻止无效的机器转换到失败状态。在这个版本中，机器控制器可以正确地处理更精细的错误消息，以便具有无效区或项目 ID 的机器可以正确地变为失败状态。(OCPBUGS-43531)

- 在以前的版本中，缺少链接操作所需的一些权限。链接操作会创建云控制器管理器和 OpenShift Container Platform 所需的其他 Azure 资源所需的子资源。在这个版本中，Azure 的云控制器管理器具有以下链接操作的权限：

  - **Microsoft.Network/applicationGateways/backendAddressPools/join/action**
  - **Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action**
  - **Microsoft.Network/applicationSecurityGroups/joinNetworkSecurityRule/action**
  - **Microsoft.Network/ddosProtectionPlans/join/action**
  - **Microsoft.Network/gatewayLoadBalancerAliases/join/action**
  - **Microsoft.Network/loadBalancers/backendAddressPools/join/action**
  - **Microsoft.Network/loadBalancers/frontendIPConfigurations/join/action**
  - **Microsoft.Network/loadBalancers/inboundNatRules/join/action**
  - **Microsoft.Network/networkInterfaces/join/action**
  - **Microsoft.Network/networkSecurityGroups/join/action**
  - **Microsoft.Network/publicIPAddresses/join/action**
  - **Microsoft.Network/publicIPPrefixes/join/action**
  - **Microsoft.Network/virtualNetworks/subnets/join/action**

  (OCPBUGS-44126)

- 在以前的版本中，缺少链接操作所需的一些权限。链接操作会创建 Machine API 和 OpenShift Container Platform 需要的其他 Azure 资源所需的子资源。在这个版本中，Azure 的 Machine API 供应商具有以下链接操作的权限：

  - **Microsoft.Compute/disks/beginGetAccess/action**

- **Microsoft.KeyVault/vaults/deploy/action**
- **Microsoft.ManagedIdentity/userAssignedIdentities/assign/action**
- **Microsoft.Network/applicationGateways/backendAddressPools/join/action**
- **Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action**
- **Microsoft.Network/applicationSecurityGroups/joinNetworkSecurityRule/action**
- **Microsoft.Network/ddosProtectionPlans/join/action**
- **Microsoft.Network/gatewayLoadBalancerAliases/join/action**
- **Microsoft.Network/loadBalancers/backendAddressPools/join/action**
- **Microsoft.Network/loadBalancers/frontendIPConfigurations/join/action**
- **Microsoft.Network/loadBalancers/inboundNatPools/join/action**
- **Microsoft.Network/loadBalancers/inboundNatRules/join/action**
- **Microsoft.Network/networkInterfaces/join/action**
- **Microsoft.Network/networkSecurityGroups/join/action**
- **Microsoft.Network/publicIPAddresses/join/action**
- **Microsoft.Network/publicIPPrefixes/join/action**
- **Microsoft.Network/virtualNetworks/subnets/join/action**

(OCPBUGS-44130)

- 在以前的版本中，当计算机器设置 CR 中的 **publicIp** 参数设置为 **false** 时，在现有子网中安装 AWS 集群会失败。在这个版本中，确保安装程序在某些环境中为 AWS 集群置备机器时，为 **publicIp** 设置的配置值不再会导致问题。(OCPBUGS-44373)
- 在以前的版本中，使用非 UEFI 磁盘的 GCP 集群无法加载。此发行版本添加了一个检查，以确保磁盘在启用需要 UEFI 的功能（如安全引导）前与 UEFI 兼容。此更改添加了 **compute.images.get** 和 **compute.images.getFromFamily** 权限要求。因此，如果您不需要这些功能，您可以使用非 UEFI 磁盘。(OCPBUGS-44671)
- 在以前的版本中，当 AWS **DHCPOptionSet** 参数配置为使用包含尾部句点(.)的自定义域名时，OpenShift Container Platform 安装会失败。在这个版本中，提取 EC2 实例的主机名并将其转换为 Kubelet 节点名称的逻辑会被更新为修剪尾部周期，以便生成的 Kubernetes 对象名称有效。此参数中的结尾句点不再会导致安装失败。(OCPBUGS-45306)
- 在以前的版本中，Azure 可用性集故障域的数量使用固定值 **2**。此设置适用于大多数 Azure 区域，因为故障域计数通常至少为 2。但是，此设置在 **centraluseuap** 和 **eastusstg** 区域中失败。在这个版本中，区域中的可用性设置故障域的数量会被动态设置。(OCPBUGS-45663)
- 在以前的版本中，当临时 API 服务器断开连接时，Azure 云控制器管理器 panicked。在这个版本中，Azure 云控制器管理器可以正确地从临时断开连接中恢复。(OCPBUGS-45859)

- 在以前的版本中，由于不正确的或缺失的注解，一些服务会处于 pending 状态。在这个版本中，添加到 Azure **service.beta.kubernetes.io/azure-load-balancer-tcp-idle-timeout** 和 GCP **cloud.google.com/network-tier** 注解中的验证可以解决这个问题。(OCPBUGS-48481)

- 在以前的版本中，用于从 AWS 获取供应商 ID 的方法可能无法根据需要为 kubelet 提供这个值。因此，有时机器可能会处于不同的状态，无法完成初始化。在这个版本中，kubelet 启动时会一致设置供应商 ID。(OCPBUGS-50905)

- 在以前的版本中，Azure 云控制器管理器中的一个不正确的端点会导致在 Microsoft Azure Government Cloud 上安装失败。这个问题已在本发行版本中解决。(OCPBUGS-50969)

- 在以前的版本中，Machine API 有时会在 IBM Cloud 上创建过程中检测到不健康的 control plane 节点，并尝试替换该节点。这实际上会销毁集群。在这个版本中，Machine API 只在集群创建过程中尝试替换不健康的计算节点，且不会尝试替换不健康的 control plane 节点。(OCPBUGS-51864)

- 在以前的版本中，在节点就绪前被驱除的 Azure spot 机器可能会处于 **provisioned** 状态。在这个版本中，Azure spot 实例使用 delete-eviction 策略。此策略可确保机器在抢占时正确变为 **failed** 状态。(OCPBUGS-54617)

- 在以前的版本中，一个程序错误修复更改了可用性集配置，它将故障域计数改为使用最大可用值而不是固定值 **2**。这会导致在这个程序错误修复前创建的计算集出现扩展的问题，因为控制器会尝试更改不可变的可用性集。在这个版本中，可用性集在创建后不再被修改，允许受影响的计算机器集正确进行扩展。(OCPBUGS-56653)

- 在以前的版本中，**openshift-cnv** 命名空间组件不提供 **openshift.io/required-scc** 注解。工作负载没有请求所需的安全内容约束 (SCC)。在这个版本中，**openshift.io/required-scc** 注解被添加到 **openshift-cnv** 命名空间组件中，以便工作负载可以请求所需的 SCC。(OCPBUGS-49657)

Cloud Credential Operator

- 在以前的版本中，**aws-sdk-go-v2** 软件开发工具包(SDK)无法在 Amazon Web Services (AWS)安全令牌服务(STS)集群上验证 **AssumeRoleWithWebIdentity** API 操作。在这个版本中，**pod-identity-webhook** 包含一个默认区域，以便这个问题不再保留。(OCPBUGS-41727)

Cluster Autoscaler

- 在以前的版本中，当 Machine Set 缩减并达到其最小大小时，Cluster Autoscaler 可能会保留最后一个剩余的节点，使其带有一个无法调度污点，使其无法作为一个节点被使用。这个问题是由 Cluster Autoscaler 中的计数错误造成的。在这个版本中，计数错误已被修复，当 Machine Set 缩减并达到其最小值时，Cluster Autoscaler 可以正常工作。(OCPBUGS-54231)

- 在以前的版本中，一些集群自动扩展指标不会被初始化，因此不可用。在这个版本中，这些指标会被初始化并可用。(OCPBUGS-25852)

- 在以前的版本中，会因为机器集中失败的机器，导致 Cluster Autoscaler 无法扩展。这是因为 Cluster Autoscaler 以各种非运行阶段计算机器的方式发生。在这个版本中，不正确的问题已被修复，Cluster Autoscaler 可以准确计算机器。(OCPBUGS-11115)

Cluster Resource Override Admission Operator

- 在以前的版本中，Cluster Resource Admission Override Operator 在从 OpenShift Container Platform 4.16 升级到 OpenShift Container Platform 4.17 时无法删除旧的 secret。这会导致 Cluster Resource Override Admission Operator Webhook 停止工作，并阻止在启用了 Cluster Resource Override Admission Operator 的命名空间中创建 pod。在这个版本中，旧的 secret 会被删除，Cluster Resource Override Admission Operator 的错误处理有所改进，并解决了在命名空间中创建 pod 的问题。(OCPBUGS-54886)

- 在以前的版本中，如果您删除了 **clusterresourceoverride-operator** 服务或卸载 Cluster Resource Admission Override Operator，则 **v1.admission.autoscaling.openshift.io** API 服务将无法访问，并阻止集群功能，比如在集群中安装其他 Operator。在这个版本中，如果卸载 Cluster Resource Admission Override Operator，则 **v1.admission.autoscaling.openshift.io** API 服务也会被删除，以便集群功能不会受到影响。(OCPBUGS-48115)

- 在以前的版本中，如果您在 **ClusterResourceOverride** CR 中指定了 **forceSelinuxRelabel** 参数，然后将参数改为另一个值，则更改的值不会反映在 **clusterresourceoverride-configuration** Config Map 中。将 selinux 重新标记临时解决方案功能应用到集群时需要此配置映射。在这个版本中，这个问题已被解决，当 **forceSelinuxRelabel** 参数改变时，clusterresource **override-configuration** Config Map 会收到更新。(OCPBUGS-44649)

Cluster Version Operator

- 在以前的版本中，**ClusterVersion** 条件的状态可以从 **ImplicitlyEnabled** 改为 **ImplicitlyEnabledCapabilities**。在这个版本中，**ClusterVersion** 条件类型已被修复，并从 **ImplicitlyEnabled** 改为 **ImplicitlyEnabledCapabilities**。(OCPBUGS-56771)

- 在以前的版本中，自定义安全上下文约束(SCC)会影响任何由 Cluster Version Operator 生成的 pod，以接收集群版本升级。在这个版本中，OpenShift Container Platform 会为每个 pod 设置一个默认 SCC，以便任何创建的自定义 SCC 都不会影响 pod。(OCPBUGS-31462)

- 在以前的版本中，当 Cluster Operator 升级需要很长时间时，Cluster Version Operator 不会报告任何内容，因为它无法确定升级是否仍在进行中或进程卡住。在这个版本中，为 Cluster Version Operator 报告的 Cluster Version 状态添加了一个新的未知状态，以提醒集群管理员检查集群并避免等待阻止的 Cluster Operator 升级。(OCPBUGS-23514)

ImageStreams

- 在以前的版本中，如果这些 registry 配置了 **NeverContactSource**，则镜像导入会阻止 registry，即使设置了镜像 registry。在这个版本中，当 registry 配置镜像时，镜像导入不再被阻断。这样可确保镜像导入成功，即使原始源在 **ImageDigestMirrorSet** 或 **ImageTagMirrorSet** 资源中被设置为 **NeverContactSource**。(OCPBUGS-44432)

安装程序

- 在以前的版本中，如果您试图安装具有最小特权的 Amazon Web Services (AWS) 集群，且您没有在 **install-config.yaml** 文件中指定实例类型，集群安装会失败。出现这个问题的原因是，安装程序无法找到集群在支持的可用区中可以使用的支持实例类型。例如，**ap-southeast-4** 和 **eu-south-2** 可用区中无法使用 **m6i.xlarge** 默认实例类型。在这个版本中，**openshift-install** 程序需要 **ec2:DescribeInstanceTypeOfferings** AWS 权限来防止在 **m6i.xlarge** 或者另一个支持的实例类型在支持的可用区中不可用的情况。(OCPBUGS-46596)

- 在以前的版本中，安装程序不会阻止用户在裸机上安装单节点集群，这会导致安装失败。在这个版本中，安装程序会防止在不支持的平台上安装单节点集群。(OCPBUGS-56811)

- 在以前的版本中，当您诊断与为 VMware vSphere 运行 **openshift-install destroy cluster** 命令相关的问题时，日志并没有提供足够的信息。因此，无法知道集群没有从虚拟机(VM)中删除的原因。在这个版本中，当销毁集群时会提供更加详细的日志信息。(OCPBUGS-56372)

- 在以前的版本中，当在 Amazon Web Services (AWS)上安装到现有虚拟私有云(VPC)时，在为 control plane 节点的机器集自定义资源和对应的 AWS EC2 实例之间的 AWS Availability Zone 间的子网信息可能会出现潜在的不匹配。因此，当 control plane 节点分散到三个可用区中，且重新创建了差异可能会导致出现不平衡的 control plane，因为两个节点在同一可用区内发生。在这个版本中，它确保了机器集自定义资源中的子网可用区信息以及 EC2 实例中的子网可用区信息匹配，并解决了这个问题。(OCPBUGS-55492)

- 在以前的版本中，当使用 **OVNKubernetes** 网络插件安装集群时，如果插件被指定为 **OVNkubernetes**（小写的 "k"），则安装可能会失败。在这个版本中，无论大小写，安装程序都可以正确地解释插件名称。(OCPBUGS-54606)

- 配置代理后，安装程序会将 **machineNetwork** CIDR 添加到 **noProxy** 字段。在以前的版本中，如果 **machineNetwork** CIDR 也由 **noProxy** 字段中的用户配置，这会导致一个重复的条目，这不被 ignition 允许，并可能会阻止主机正常引导。在这个版本中，如果已设置，安装程序不会将 **machineNetwork** CIDR 添加到 **noProxy** 字段。(OCPBUGS-53183)

- 在以前的版本中，即使用户管理的负载均衡器正在使用中，API 和入口 VIP 也会被自动分配。这个行为并不是预期的。现在，API 和入口 VIP 不再被自动分配。如果没有在 **install-config.yaml** 文件中明确设置这些值，安装会失败并显示错误，提示用户提供它们。(OCPBUGS-53140)

- 在以前的版本中，当使用基于代理的安装程序时，在硬件发现过程中不会检测到光纤通道(FC)多路径卷的 WWN。因此，当指定 **wwn** root 设备提示时，所有多路径 FC 卷都会被排除。在这个版本中，多路径 FC 卷会收集 WWN，因此当存在多个多路径卷时，用户可以使用 **wwn** root 设备提示来选择它们。(OCPBUGS-52994)

- 在以前的版本中，当在 Azure 上安装集群时，安装程序不包括对 NVMe 或 SCSI 的支持，这会阻止使用需要它的虚拟机实例系列。在这个版本中，安装程序可以使用需要 NVMe 或 SCSI 支持的虚拟机实例系列。(OCPBUGS-52658)

- 在以前的版本中，当使用用户提供的加密密钥在 GCP 上安装集群时，安装程序可能无法找到密钥环。在这个版本中，安装程序会找到用户提供的加密密钥环，因此安装不会失败。(OCPBUGS-52203)

- 在以前的版本中，当在 GCP 上安装集群时，如果网络不稳定无法在安装过程中获取 GCP 标签，则安装可能会失败。在这个版本中，安装程序已被改进，可以在安装过程中容忍网络不稳定的情况。(OCPBUGS-50919)

- 在以前的版本中，安装程序没有检查在 VMware vSphere 集群中关闭的 ESXi 主机，这会导致安装失败，因为无法上传 OVA。在这个版本中，安装程序会检查每个 ESXi 主机的电源状态，并跳过任何已关闭的电源，从而解决这个问题并允许成功导入 OVA。(OCPBUGS-50649)

- 在以前的版本中，当使用基于代理的安装程序时，在断开连接的环境中构建 Agent ISO 镜像时，会输出大量 **unable to read image** 的错误信息。在这个版本中，这些错误的信息已被删除，不再出现。(OCPBUGS-50637)

- 在以前的版本中，当在 Azure 上安装集群时，如果没有 IP 地址可用性的正确权限，安装程序会崩溃并带有分段错误。在这个版本中，安装程序会正确识别缺少的权限，并安全地失败。(OCPBUGS-50534)

- 在以前的版本中，当 **ClusterNetwork** 无类别域间路由(CIDR)掩码值大于 **hostPrefix** 值和 **networking.ovnKubernetesConfig.ipv4.internalJoinSubnet** 部分时，安装程序会在 **install-config.yaml** 文件中提供验证检查并返回 Golang 运行时错误。在这个版本中，安装程序仍然失败验证检查，并现在会输出指示无效的 **hostPrefix** 值的描述性错误消息。(OCPBUGS-49784)

- 在以前的版本中，当在 IBM Cloud® 上安装集群时，安装程序无法在 **ca-mon** 区域上安装，即使它可用。在这个版本中，安装程序与最新可用的 IBM Cloud® 区域是最新的。(OCPBUGS-49623)

- 在以前的版本中，当在具有用户提供的公共 IPv4 池的现有 VPC 中只有最小权限的 AWS 上安装集群后，因为缺少权限，集群无法被销毁。在这个版本中，安装程序会传播 **ec2:ReleaseAddress** 权限，以便可以销毁集群。(OCPBUGS-49594)

- 在以前的版本中，VMware vSphere 的安装程序没有为故障域验证 **install-config.yaml** 中提供的

网络数量。如果指定了超过最多的 10 个网络，则安装会使用不受支持的配置继续进行，而不是提供错误信息。在这个版本中，安装程序会验证配置的网络数量，这可以防止使用超过最大限制的配置的问题。(OCPBUGS-49351)

- 在以前的版本中，在带有现有子网(BYO VPC)在 Local 或 Wavelength 区的 AWS 上安装集群会导致边缘子网资源缺少 **kubernetes.io/cluster/<InfraID>:shared** 标签。在这个版本中，确保 **install-config.yaml** 文件中使用的所有子网都有所需的标签。(OCPBUGS-48827)

- 在以前的版本中，一个问题会阻止在安装过程中在 Nutanix 集群的故障域中配置多个子网。这个问题已在本发行版本中解决。(OCPBUGS-49885)

- 在以前的版本中，当在 AWS 上安装集群时，安装程序调查中没有 **ap-southeast-5** 区域，即使 OpenShift Container Platform 支持这个区域。在这个版本中，可以使用 **ap-southeast-5** 区域。(OCPBUGS-47681)

- 在以前的版本中，当销毁在 GCP 上安装的集群时，一些资源可能会保留下来，因为安装程序不会等待所有 destroy 操作都成功完成。在这个版本中，destroy API 会等待以确保正确删除所有资源。(OCPBUGS-47489)

- 在以前的版本中，当在 **us-east-1** 区域的 AWS 上安装集群时，如果 **install-config.yaml** 文件中没有指定区，则安装会失败，因为 **use1-az3** 区不支持 OpenShift Container Platform 支持的任何实例类型。在这个版本中，当安装配置文件中没有指定区时，安装程序会防止使用 **use1-az3** 区。(OCPBUGS-47477)

- 在以前的版本中，当在 GCP 上安装集群时，如果您对项目启用了 **constraints/compute.vmCanIpForward** 约束，安装会失败。在这个版本中，安装程序会在启用了这个约束时禁用它，可以使安装成功完成。(OCPBUGS-46571)

- 在以前的版本中，当在 GCP 上安装集群时，安装程序将无法检测用户是否提供了不存在的加密密钥环，从而导致安装失败。在这个版本中，安装程序会正确地验证用户提供的加密密钥环是否存在，从而防止失败。(OCPBUGS-46488)

- 在以前的版本中，当销毁在 Microsoft Azure 上安装的集群时，bootstrap 节点的入站 NAT 规则和安全组不会被删除。在这个版本中，正确的资源组可确保在集群销毁时所有资源都被删除。(OCPBUGS-45429)

- 在以前的版本中，当在 **ap-southeast-5** 区域中的 AWS 上安装集群时，因为存在不正确的负载均衡器主机名，安装可能会失败。在这个版本中，安装程序已被改进来组成正确的主机名，以便安装可以成功。(OCPBUGS-45289)

- 在以前的版本中，当在 GCP 上安装集群时，安装程序可能无法找到它所创建的服务帐户，因为在 Google 服务器上激活服务帐户的延迟。在这个版本中，安装程序会在尝试使用创建的服务帐户前等待适当的时间。(OCPBUGS-45280)

- 在以前的版本中，当在 AWS 上安装集群时，如果您指定了边缘机器池，但没有指定实例类型，则安装可能会失败。在这个版本中，安装程序需要为边缘机器池提供实例类型。(OCPBUGS-45218)

- 在以前的版本中，当销毁在 GCP 上安装的集群时，带有 **kubernetes-io-cluster-<cluster-id>: owned** 的 PVC 磁盘不会被删除。在这个版本中，安装程序会在销毁集群时正确找到并删除这些资源。(OCPBUGS-45162)

- 在以前的版本中，在断开连接的安装中，当为源配置了多个镜像的 **imageContentSources** 参数时，创建代理 ISO 镜像的命令可能会失败，具体取决于镜像配置序列。在这个版本中，当创建代理 ISO 并解决了这个问题时，会正确处理多个镜像。(OCPBUGS-44938)

- 在以前的版本中，当在 AWS 上安装集群时，如果设置了 **publicIPv4Pool** 参数，但 **ec2:AllocateAddress** 权限不存在，安装会失败。在这个版本中，安装程序需要这个权限存在。(OCPBUGS-44925)

- 在以前的版本中，在共享虚拟私有云(VPC)安装过程中，安装程序会将记录添加到安装程序创建的私有 DNS 区中，而不是将记录添加到集群的专用 DNS 区域。因此，安装会失败。在这个版本中，安装程序会搜索现有的私有 DNS 区域，如果找到，则该区与 **install-config.yaml** 文件提供的网络配对，并解决了这个问题。(OCPBUGS-44641)

- 在以前的版本中，您可以在 Amazon Web Services (AWS) 标签名称中添加空格，但安装程序不支持它们。这种情况会导致安装程序输出 **ERROR failed to fetch Metadata** 信息。在这个版本中，AWS 标签的正则表达式会验证具有空格的任何标签名称，以便安装程序接受这些标签，且不再因为空格而输出错误。(OCPBUGS-44199)

- 在以前的版本中，当销毁在 GCP 上安装的集群时，转发规则、健康检查和防火墙规则不会被删除，从而导致错误。在这个版本中，当集群销毁时，所有资源都会被删除。(OCPBUGS-43779)

- 在以前的版本中，当在 Microsoft Azure 上安装集群时，指定 **Standard_M8-4ms** 实例类型会导致错误，因为实例类型以十进制格式而不是整数格式指定其内存。在这个版本中，安装程序可以正确地解析内存值。(OCPBUGS-42241)

- 在以前的版本中，当在 VMware vSphere 上安装集群时，如果 API 和 Ingress 服务器虚拟 IP 位于机器网络之外，安装可能会失败。在这个版本中，安装程序会包括机器网络中的 API 和 Ingress 服务器虚拟 IP。如果您指定了 API 和 Ingress 服务器虚拟 IP，请确保它们位于机器网络中。(OCPBUGS-36553)

- 在以前的版本中，当在 IBM Power Virtual Server 上安装集群时，如果因为镜像导入错误选择了 Madrid 区域，安装会失败。在这个版本中，安装程序已被修改为使用正确的存储桶名称，使安装可以成功完成。(OCPBUGS-50899)

- 在以前的版本中，当销毁在 IBM Power Virtual Server 上安装的集群时，一些资源（包括网络子网）不会被删除。在这个版本中，当集群销毁时，所有网络资源都会被删除。(OCPBUGS-50657)

- 在以前的版本中，当使用 Assisted Installer 安装集群时，因为拉取镜像时，安装可能会失败。在这个版本中，增加了超时时间，以便安装程序可以完成拉取镜像。(OCPBUGS-50655)

- 在以前的版本中，在一些较慢的 PrismCentral 环境中，当使用 prism-api 调用来加载 RHCOS 镜像时，安装程序会失败。在以前，超时值为 5 分钟。在这个版本中，prism-api 调用超时值是一个在 **install-config.yaml** 文件中的可配置参数（**platform.nutanix.prismAPICallTimeout**），默认值为 10 分钟。(OCPBUGS-48570)

- 在以前的版本中，一个问题会阻止在安装过程中在 Nutanix 集群的故障域中配置多个子网。这个问题已在本发行版本中解决。(OCPBUGS-48044)

- 在以前的版本中，当使用安装程序置备的基础架构在 IBM Power Virtual Server 上安装集群时，安装程序会选择一个随机机器网络，而不是使用用户提供的网络。在这个版本中，安装程序使用用户提供的机器网络。(OCPBUGS-45286)

- 在以前的版本中，当 **openshift-install agent create pxe-files** 命令创建 pxe-files 命令时创建的临时目录在命令完成后不会被删除。在这个版本中，在命令完成后，临时目录会被正确删除。(OCPBUGS-39583)

Machine Config Operator

- 在以前的版本中，**ContainerRuntimeConfig** 会为 **runc** 运行时设置 **--root** 路径不正确。这会导致容器使用不正确的 root 路径运行，并导致容器操作出现问题。在这个版本中，容器运行时的 **--root** 路径是正确的，并与指定的运行时匹配，从而实现一致的操作。(OCPBUGS-47629)

- 在以前的版本中，如果集群包含 Red Hat Enterprise Linux (RHEL) worker 节点，这在 OpenShift Container Platform 4.19 及更新的版本中不再被支持，但用户不会得到警告。在这个版本中，Machine Config Operator 会检测 RHEL 节点，并通知用户与 OpenShift Container Platform 4.19 不兼容。(OCPBUGS-54611)

- 在以前的版本中，当 Machine Config Operator (MCO) 在暂存更新后快速重新引导节点时，更新会失败。在这个版本中，MCO 会在重启系统前等待 staging 操作完成，从而允许更新完成。(OCPBUGS-51150)

- 在以前的版本中，在删除 **MachineOSConfig** 对象后，关联的 **MachineOSBuild** 对象不会被删除。这是因为 **MachineOSBuild** 对象的所有权没有被设置。在这个版本中，所有对象都是为构建创建的，当删除 **MachineOSConfig** 对象时，所有关联的对象都会被删除。(OCPBUGS-44602)

管理控制台

- 在以前的版本中，**开发者视角**中的**项目详情**没有包括"面包屑"导航。在这个版本中，添加了面包屑导航栏。(OCPBUGS-52298)

- 在以前的版本中，在打开 web 终端时打开 **Project** 下拉列表时显示会有问题。在这个版本中，问题已被修复，您可以在 web 终端打开时使用 **Project** 下拉列表。(OCPBUGS-45325)

- 在以前的版本中，在 OpenShift Container Platform Web 控制台中无法重新运行使用解析器的 **PipelineRuns** CR。如果您试图重新运行 CR，则会生成 "Invalid **PipelineRun** configuration, unable to start Pipeline"。在这个版本中，您可以重新运行使用解析器的 **PipelineRuns** CR，而不会遇到这个问题。(OCPBUGS-44265)

- 在以前的版本中，当您使用 **Form View** 在 OpenShift Container Platform Web 控制台中编辑 **Deployment** 或 **DeploymentConfig** API 对象时，在其中一个对象的 YAML 配置中都存在重复的 **ImagePullSecrets** 参数。在这个版本中，确保没有为其中一个对象自动添加重复的 **ImagePullSecrets** 参数。(OCPBUGS-41974)

- 在以前的版本中，会根据 **PipelineRun** 名称获取特定 **Pipelinerun** 的 **TaskRun**。如果两个 **PipelineRuns** 具有相同的名称，则两个 **PipelineRuns** 的 **TaskRun** 都会被获取并显示。在这个版本中，特定 **PipelineRun** 的 **TaskRun** 将基于 **PipelineRun** UID 而不是 **PipelineRun** 名称获取。(OCPBUGS-36658)

- 在以前的版本中，如果没有运行的 pod，**Test Serverless function** 按钮没有响应。在这个版本中，当没有运行的 pod 时，这个按钮会被禁用。(OCPBUGS-32406)

- 在以前的版本中，失败的 **TaskRun** 的结果不会显示在 UI 中。在这个版本中，**TaskRun** 的结果始终可用，即使已失败。(OCPBUGS-23924)

- 在以前的版本中，在只执行 control plane 升级时，控制台会警告用户必须在 60 天内更新计算节点。在这个版本中，控制台不再显示这个无效的警报。(OCPBUGS-56077)

- 在以前的版本中，**Notification Drawer** 中的 **Critical Alerts** 部分无法折叠。在这个版本中，这个部分可以折叠。(OCPBUGS-55702)

- 在以前的版本中，当查看已安装的 Operator 列表时，如果当前选择的项目与 Operator Lifecycle Manager (OLM)中禁用复制的 CSV 时，当前选择的项目与 Operator Lifecycle Manager (OLM) 中禁用了 Operator 的默认命名空间，则 Operator 会在列表中显示两次。在这个版本中，Operator 只显示一次。(OCPBUGS-54601)

- 在以前的版本中，到 **Installed Operators** 页中的 **OperatorHub** 的链接会触发硬重新加载。在这个版本中，这个链接不再触发硬重新加载。(OCPBUGS-54536)
- 在以前的版本中，在 **Create VolumeSnapshot** 页中从项目选择器中选择 **All Projects** 会导致页未找到错误。在这个版本中，VolumeSnapshot 列表页会被正确显示。(OCPBUGS-53227)
- 在以前的版本中，计算 pod 容器计数不正确的逻辑会导致它不准确。在这个版本中，添加了 count 逻辑的 **Ready** 和 **Started** 状态，因此会显示正确的 pod 容器计数，它由 **oc** CLI 组成。(OCPBUGS-53118)
- 在以前的版本中，**节点日志**部分上面的 **Select** 菜单在打开时将无法被关闭，除非再次点击 **Select** 菜单的切换，或者点 Select's 菜单项中的一个。在这个版本中，在点菜单外的部分，或键盘上相应的键后，**Select** 菜单可以关闭。(OCPBUGS-52316)
- 在以前的版本中，在计算相对时间时，共享时间戳组件会引用未定义属性。因此，在控制台中显示的次数都没有正确显示相对字符串，如 **Just now** 或 **Less than a minute ago**。在这个版本中，这个问题已被解决，在控制台中正确呈现相对时间字符串。(OCPBUGS-51202)
- 在以前的版本中，**Observe** 菜单只根据用于监控的当前用户和控制台配置显示。这会导致可观察插件添加的其他项目被隐藏。在这个版本中，**Observe** 菜单还显示来自不同可观察性插件的项目。(OCPBUGS-50693)
- 在以前的版本中，当第一次登录到控制台时，自动视角检测会使控制台处理错误用户点的特定 URL，导致控制台加载不同的页。在这个版本中，会正确处理当前路径。(OCPBUGS-50650)
- 在以前的版本中，当在 web 控制台的、来自插件的水平导航中创建新标签页时，会出现问题。在这个版本中，您可以使用插件在 web 控制台水平导航中创建标签页。(OCPBUGS-49996)
- 在以前的版本中，如果 **ClusterVersion** 没有收到 **Completed** 更新，Cluster Settings 页不会在集群更新过程中正确显示。在这个版本中，即使 **ClusterVersion** 没有收到 **Completed** 更新，**Cluster Setting** 页也会正确显示。(OCPBUGS-49839)
- 在以前的版本中，CLI 下载页面中的链接不会被操作系统排序。在这个版本中，链接按字母顺序按照其操作系统进行排序。(OCPBUGS-48413)
- 在以前的版本中，**OperatorHub** 模式的主 **Action** 按钮中可能会出现多个外部链接图标。在这个版本中，只会显示单个外部链接图标。(OCPBUGS-46555)
- 在以前的版本中，当显示了另一个 **User Preference** 选项卡时，点 Red Hat OpenShift Lightspeed modal 中的 **Don't again show** 链接不会正确地进入到常规的 **User Preference** 选项卡。在这个版本中，点 **Don't again show** 可以正确进入 **User Preference** 选项卡。(OCPBUGS-46511)
- 在以前的版本中，控制台插件可以在 **Console plugin enablement** modal 中多次启用，从而导致插件的多个条目出现 Console Operator 配置。在这个版本中，如果一个插件已启用则无法再启用。(OCPBUGS-44595)
- 在以前的版本中，OpenShift Container Platform Web 控制台登录页总是允许您点 **Login** 按钮。您在不输入用户名或密码时，或已点了 **Login** 按钮的情况下仍然可以再点。在这个版本中，**Login** 按钮被禁用，因此在没有输入用户名或密码的情况下无法点 **Login**。(OCPBUGS-43610)
- 在以前的版本中，在 **Operator 安装** 状态页中只选择根据名称的 **PackageManifest**。在某些情况下，这会导致使用不正确的 **PackageManifest** 来显示徽标和供应商，因为可能存在名称冲突。在这个版本中，**PackageManifests** 可以根据名称和标签选择器选择，以确保为当前安装选择正确的项。因此，Operator 安装状态页始终会显示正确的徽标和供应商。(OCPBUGS-21755)

监控

- 在以前的版本中，如果 scrape 失败，Prometheus 会错误地认为来自下一个的 scrape 抽样是重复的，并丢弃它们。这个问题只会影响到失败的 scrape 后的下一个 scrape，其后的 scrape 可以被正确处理。在这个版本中，失败后的下一个 scrape 可以被正确处理，确保不会错误地丢弃有效的示例。(OCPBUGS-53025)

网络

- 在以前的版本中，当 pod 使用 CNI 插件进行 DHCP 地址分配时，pod 的网络接口可能会意外删除。因此，当 pod 的 DHCP 租期过期时，DHCP 代理在尝试重新创建新租期时会进入循环，从而导致节点变得无响应。在这个版本中，如果网络接口不存在，DHCP 租期维护会终止。因此，接口删除可以被安全地处理，确保节点的稳定性。(OCPBUGS-45272)

- 在以前的版本中，Kubernetes NMState Operator Operator 不会创建 **nmstate-console-plugin** pod，因为 **pluginPort** 模板存在问题。在这个版本中，修复模板可确保 Operator 现在可以成功创建 **nmstate-console-plugin** pod。(OCPBUGS-54295)

- 在以前的版本中，Whereabouts 协调器中的 pod 控制器没有将命名空间传递给领导选举功能，因此 pod 控制器不会删除孤立的分配。这会导致重复日志错误消息。在这个版本中，命名空间被传递，并正确删除孤立的分配。(OCPBUGS-53397)

- 在以前的版本中，**SriovOperatorConfig** Operator 删除了在 **SriovOperatorConfig** 资源中具有默认值的任何参数。这种情况会导致资源输出中缺少某些信息。在这个版本中，Operator 使用 PATCH 方法用于 API 服务器来保留带有默认值的参数，以便在资源输出中缺少任何信息。(OCPBUGS-53346)

- 在以前的版本中，**SriovNetworkNodePolicy** 对象协调器与每个节点资源更新执行。这会导致 SR-IOV Operator pod 消耗过量资源，并过度使用日志条目。此发行版本更改了行为，以便协调器仅在节点标签更改时运行，从而减少资源消耗和日志条目生成。(OCPBUGS-52955)

- 在以前的版本中，当升级到最新版本的 OpenShift Container Platform 时，带有 **clusterNetwork** 参数的集群会列出同一 IP 地址系列的多个网络进入 **crashloopbackoff** 状态。在这个版本中，确保使用此配置的集群在集群升级过程中不再进入 **crashloopbackoff** 状态。(OCPBUGS-49994)

- 在以前的版本中，**resolv-prepender** 服务比预期触发。这种情况会导致服务失败，并导致主机 DNS 配置错误设置。在这个版本中，**resolv-prepender** 服务的配置被更新，以便在服务触发早于预期时，不再会导致主机 DNS 设置配置不正确。(OCPBUGS-49436)

- 在以前的版本中，只有将 **platform** 参数设置为 **baremetal** 的部署才会启用 **nmstate-configuration** 服务。但是，您也可以使用 Assisted Installer 来配置裸机部署，方法是将 **platform** 参数设置为 **None**，但 NMState **br-ex** 网络桥接创建功能无法使用这个安装方法。在这个版本中，**nmstate-configuration** 服务被移到集群安装路径中的基础目录，以便任何 **platform** 参数设置为 **None** 的部署都不会影响 NMState **br-ex** 网络桥接创建功能。(OCPBUGS-48566)

- 在以前的版本中，对于将网关模式设置为 **local** 的第 2 层或第 3 层拓扑网络，OVN-Kubernetes 重启时会遇到问题。造成这个问题导致 Egress IP 被选为网络的主 IP 地址。在这个版本中，一个修复可确保不再发生此行为。(OCPBUGS-46585)

- 在以前的版本中，基于 DNS 的出口防火墙错误地阻止创建在大写字符中包含 DNS 名称的防火墙规则。在这个版本中，对出口防火墙的修复意味着，创建一个包含大写的 DNS 名称的防火墙规则。(OCPBUGS-46564)

- 在以前的版本中，当 pod 在分配 IPv6 协议的节点中运行时，pod 无法与双栈集群中的 OVN-Kubernetes 服务通信。这会导致带有 IP 系列的流量，**egressIP** 不适用于丢弃。在这个版本中，只有用于删除出口 IP 系列的 IP 系列的源网络地址转换(SNAT)，从而消除了丢弃流量的风险。

(OCPBUGS-46543)

- 在以前的版本中，当您在清单对象的自定义 **br-ex** 网桥配置中使用静态 IP 地址时，会添加一个竞争条件，并导致节点重启操作进一步影响集群的部署。在这个版本中，**nodeip-configuration** 服务在 **br-ex** 网桥启动后启动，从而防止竞争条件和节点重新引导。(OCPBUGS-46072)

- 在以前的版本中，HAProxy 路由器错误地假设只有 SHA1 leaf 证书被 HAProxy 拒绝，从而导致路由器因为不拒绝 SHA1 中间证书而失败。在这个版本中，路由器会检查并拒绝所有非自签名 SHA1 证书，从而防止崩溃并提高了集群稳定性。(OCPBUGS-45290)

- 在以前的版本中，当节点重启 **openvswitch** 守护进程时，**nmstate-handler** 容器无法访问 OpenVSwitch (OVS)数据库，这会导致所有与 OVS 相关的 NNCP 配置失败。在这个版本中，这个问题已被解决。**nmstate-handler** 容器可以访问 OVS 数据库，即使在重启节点上的 OVS 进程后。**nmstate-handler** 不再需要手动重启。(OCPBUGS-44596)

- 在以前的版本中，当指定 **protocol** 参数时，不会强制 **MultiNetworkPolicy** API，但在集群配置中不会强制使用 **port** 参数。这种情况导致所有网络流量都连接到集群。在这个版本中，**multiNetworkPolicy** API 策略只允许从 **protocol** 参数指定的端口的连接，以便只有特定流量到达集群。(OCPBUGS-44354)

- 在以前的版本中，HAProxy 在重新载入其配置时打开闲置连接，直到下次客户端使用闲置连接或 **hard-stop-after** 周期过来发送请求。此发行版本添加了一个新的 **IdleConnectionTerminationPolicy** API 字段，用来控制重新载入过程中闲置连接的 HAProxy 行为。新的默认设置是 **Immediate**，这意味着 HAProxy 在重新载入其配置时立即终止任何闲置连接。可以使用 **IdleConnectionTerminationPolicy** 的 **Deferred** 设置来指定之前的行为。(OCPBUGS-43745)

- 在以前的版本中，如果在发送大于网络 MTU 的 UDP 数据包时，如果应用程序没有使用路径 MTU 发现(PMTUD)机制，则 **OVN** 软件包的问题会导致在对数据包进行碎片时丢弃数据包。在这个版本中，**OVN** 软件包已被修复，大型 UDP 数据包会被正确碎片并通过网络发送。(OCPBUGS-43649)

- 在以前的版本中，在 OVN-Kubernetes **Localnet** 网络中带有二级接口的 pod，它插入到 **br-ex** 接口桥接被同一节点上的其他 pod 访问，但使用默认网络进行通信。不同节点上 pod 之间的通信不会受到影响。在这个版本中，可以在同一节点上运行的 **Localnet** pod 和默认网络 pod 之间的通信，但 **Localnet** 网络中使用的 IP 地址必须与主机网络位于同一个子网中。(OCPBUGS-43004)

- 在以前的版本中，当对正在运行的集群进行特定的网络更改时，**ovs-configuration** 服务永久创建一个 **NetworkManager** 连接配置集，配置集被错误地保存到存储中。此配置文件将在重新引导操作中保留，并导致 **ovs-configuration** 服务失败。在这个版本中，**ovs-configuration** 清理过程被更新以删除任何不必要的文件，从而防止此类文件在重启操作后造成问题。(OCPBUGS-41489)

- 在以前的版本中，**parseIPList** 功能无法处理包含有效和无效的 IP 地址或 CIDR 范围的 IP 地址列表。当函数遇到无效的条目并跳过处理有效条目时，这会导致函数返回空字符串。在这个版本中，**haproxy.router.openshift.io/ip_allowlist** 路由注解会跳过任何无效的 IP 地址或 CIDR 范围，以便 **parseIPList** 功能可以处理所有列出的条目。(OCPBUGS-39403)

- 在以前的版本中，HAProxy 路由器缺少 **router.openshift.io/haproxy.health.check.interval** 注解的越界验证。如果您设置了超过 HAProxy 路由器可以处理的最大值，则 **router-default** pod 无法访问 **Ready** 状态。在这个版本中，路由器会验证注解的值，并排除没有绑定的值。路由器现在按预期工作。(OCPBUGS-38078)

- 在以前的版本中，在某些情况下，节点的网关 IP 地址已更改，并导致管理到集群子网的静态路由

的 **OVN** 集群路由器，来添加新网关 IP 地址的新静态路由，而无需删除原始网关 IP 地址。因此，一个过时的路由仍指向交换机子网，这会导致在出口流量传输过程中出现间歇性下降。在这个版本中，应用到 **OVN** 集群路由器的补丁可确保如果网关 IP 地址有变化，**OVN** 集群路由器会使用新的网关 IP 地址更新现有的静态路由。stale 路由不再指向 **OVN** 集群路由器，以便出口流量流不会丢弃。(OCPBUGS-32754)

- 在以前的版本中，当从 ingress 转换失败到路由转换失败时，没有记录事件。在这个版本中，会记录失败转换的错误。(OCPBUGS-29354)
- 在以前的版本中，PowerVS 安装程序使用硬编码列表支持的机器类型。但是，在添加新类型时，这个列表并不总是更新的。在这个版本中，数据中心会查询以获取当前支持的类型列表。(OCPBUGS-49940)
- 在以前的版本中，当定义了 RootDiskHint 且安装失败并带有错误 **Requested installation disk is not part of the host's valid disks**，则很难确定可用作提示的有效磁盘名称。在这个版本中，为可接受的磁盘列表添加了日志记录，以便用户可以快速确定根磁盘提示应该是什么。(OCPBUGS-43578)
- 在以前的版本中，当出现 API 服务器中断或临时连接问题时，**oc adm node-image monitor** 命令会返回 EOF 错误。这会导致命令终止。在这个版本中，命令会检测 API 服务器中断和临时连接问题，并在不终止命令的情况下重新连接到 API 服务器。(OCPBUGS-38975)
- 在以前的版本中，当创建虚拟机(VM)且 IP 池中没有 IP 地址时，虚拟机不会启动。**virt-launcher-<vm_name>** pod 中生成了一个错误消息，但信息与问题源不同。在这个版本中，如果 IP 池中没有 IP 地址，**virt-launcher-<vm-name>** pod 包含一个类似以下示例的清晰错误消息：

  > Warning ErrorAllocatingPod 4s (x7 over 79s) ovnk-controlplane failed to update pod localnet-ipam/virt-launcher-vmb-localnet-ipam-hlnmf: failed to assign pod addresses for localnet-ipam/ipam-localnet-nad/localnet-ipam/virt-launcher-vmb-localnet-ipam-hlnmf: failed to allocate new IPs for tenantblue-network: subnet address pool exhausted

  (OCPBUGS-54245)

节点

- 在以前的版本中，如果您的集群使用 Zscaler 并扫描所有传输，则拉取镜像时可能会出现超时问题。此问题是由于镜像拉取的一个硬编码超时值造成的。CRI-O 的拉取进度超时现在增加到 30 秒。因此，之前受影响的集群应该不会遇到超时问题。(OCPBUGS-54662)
- 在以前的版本中，使用 **container_logreader_t** SELinux 域的容器要查看容器日志（位于主机的 **/var/log** 位置）无法访问日志。这是因为 **var/log/containers** 位置中的日志是符号链接。在这个版本中，容器可以如预期监视日志。(OCPBUGS-48555)
- 在以前的版本中，当文件处于循环操作时，**json.NewDecoder** 文件中会出现一个文件结束错误。这个错误会导致应用程序对在多个命名空间中存在的命名空间策略不一致。此问题可能会导致集群的安全漏洞。在这个版本中，在进入每个循环操作时，会将一个新的策略缓冲添加到 **json.NewDecoder** 文件中，并为多个命名空间添加一个测试问题单。因此，策略缓冲为 JSON 策略文件提供可靠的解码过程，以便命名空间策略在没有任何问题的情况下接收更新。(OCPBUGS-48195)
- 在以前的版本中，镜像引用摘要计算中存在一个问题，这会导致基于 **schemaVersion 1** 镜像创建失败的容器。此问题会阻止新部署的创建。在这个版本中，镜像摘要计算已被修复，可以安装新的 Operator。(OCPBUGS-42844)

- 在以前的版本中，对于 **policy.json** 文件中的有效负载镜像带有 Sigstore 验证的技术预览集群，基础镜像中的 Podman 版本不支持 Sigstore 配置。缺少支持会导致新节点不可用。在这个版本中，这个问题已被解决，节点可用。(OCPBUGS-38809)

- 在以前的版本中，在 pod 被删除后，最后一个保证 pod 的 CPU 被接受到节点会保留分配。此行为会导致调度域不一致。在这个版本中，分配给保证 pod 的 CPU 会如预期返回到可用 CPU 资源池，确保后续 pod 的 CPU 调度正确。(OCPBUGS-17792)

Node Tuning Operator (NTO)

- 在以前的版本中，当将性能配置集应用到节点时，OpenShift Container Platform 根据节点上的 CPU 单元的厂商标识符选择适当的配置集。因此，如果 CPU 使用无法识别的不同供应商标识符，OpenShift Container Platform 无法包括正确的配置集。例如，标识符可能包含 APM，而不是 ARM。在这个版本中，对于使用 ARM 架构的 CPU，Operator 现在只根据架构选择配置集，而不是厂商标识符。因此，会应用正确的配置集。(OCPBUGS-52352)

Observability（可观察性）

- 在以前的版本中，**Silence details** 页有一个不正确的链接 URL，它缺少 **namespace** 参数，这会导致用户无法在 dev 控制台中为特定版本静默特定的警报。这会导致警报管理不佳。在这个版本中，**SilencedAlertsList** 中的未定义链接已使用活跃命名空间修复。现在，"No Alert found' 错误已被解决，OpenShift Container Platform Monitoring 中的 **Alert details** 页会被正确导航。(OCPBUGS-48142)

- 在以前的版本中，控制台更新已弃用的 PatternFly 4，呈现监控插件表的不正确的布局。在这个版本中，表和风格升级到 PatternFly 5，并可以被正确呈现。(OCPBUGS-47535)

- 在以前的版本中，命名空间传递给警报图上的完整集群查询，这会导致使用租期 API 路径。API 缺少检索数据的权限，因此警报图表中没有显示任何数据。在这个版本中，命名空间不再传递给警报图的完整集群查询。现在，使用非租期 API 路径，因为此 API 具有检索数据的正确权限。警报图中没有数据。(OCPBUGS-45896)

- 在以前的版本中，Red Hat Advanced Cluster Management (RHACM) Alerting UI 重构更新会导致 **isEmpty** 检查在 **Observe > Metrics** 菜单中缺失。缺少的检查会颠倒 **Show all Series** 和 **Hide all Series** 状态的行为。此发行版本重新增加了 **isEmpty** 检查，因此当系列被隐藏时会显示 **Show all Series**，但系列显示时会显示 **Hide all Series**。(OCPBUGS-45816)

- 在以前的版本中，在 **Observe → Alerting → Silences** 选项卡中，**DateTime** 组件更改了事件及其值的排序。由于这个问题，您无法在 web 控制台中编辑 silent 警报的 **until** 参数。在这个版本中，对 **DateTime** 组件进行了修复，现在可以针对一个静默警告编辑 **until** 参数。(OCPBUGS-45801)

- 在以前的版本中，绑定基于栏图中的第一个条。如果条大小大于第一个条，则条会超过条图的边界。在这个版本中，一个条的边界是基于最大条设置的，因此条的边界不再会超过边界。(OCPBUGS-45174)

oc-mirror

- 在以前的版本中，oc-mirror 插件 v2 在本地缓存填充阶段不会显示任何进度输出。对于涉及大量镜像的镜像的镜像配置，这可能会导致进程变得无响应或卡住。在这个版本中，添加了一个进度条来提供缓存填充状态，允许用户查看缓存填充的当前进度。(OCPBUGS-56563)

- 在以前的版本中，当使用 oc-mirror 插件 v2 镜像 Operator 时，一些社区 Operator 带有长的 **skips** 和 **replaces** 项列表，并替换其频道图形中的条目会导致镜像过程耗尽内存并失败。在这个版本中，oc-mirror 插件 v2 通过避免重复评估多个 **skips** 和 **replaces** 小节中的条目来提高过滤逻辑，从而导致在 Operator 镜像过程中更好地处理内存。(OCPBUGS-52471)

- 在以前的版本中，当使用相同的工作目录重新运行 oc-mirror 插件 v2 时，之前运行中的现有 **tar** 归档文件不会被删除。这会导致混合使用过时的新归档，这可能会在推送到目标 registry 时造成镜像失败。在这个版本中，oc-mirror 插件 v2 会在每次运行时自动删除旧的 **tar** 归档文件，确保工作目录仅包含当前执行中的存档(OCPBUGS-56433)

- 在以前的版本中，如果源 registry 在镜像复制过程中响应以下 HTTP 状态代码，则 oc-mirror 插件 v2 会出错：502, 503, 504。在这个版本中，oc-mirror 插件 v2 会在遇到这些临时服务器错误时自动重试复制操作。(OCPBUGS-56185)

- 在以前的版本中，当镜像一个 Helm Chart 时，在引用中包含带有标签和摘要的容器镜像时，oc-mirror 插件 v2 会失败并显示以下错误：

  > Docker references with both a tag and digest are currently not supported.

  在这个版本中，oc-mirror 插件 v2 支持 Helm chart 使用标签和摘要引用镜像。工具使用摘要作为源来 mirror 镜像，并在目的地应用标签。(OCPBUGS-54891)

- 在以前的版本中，在镜像清理过程中，如果删除镜像时出现错误，oc-mirror 插件 v2 将停止删除过程。在这个版本中，oc-mirror 插件 v2 将继续尝试删除剩余的镜像，即使遇到错误也是如此。进程完成后，它会显示任何失败的删除列表。(OCPBUGS-54653)

- 在以前的版本中，如果在 **ImageSetConfiguration** 文件中指定无效的 Operator，可以在 mirror-to-disk (m2d)阶段镜像空目录。这会导致在后续的 disk-to-mirror (d2m)阶段失败。在这个版本中，oc-mirror 插件 v2 通过验证配置中的 Operator 引用来防止镜像空目录，确保更可靠的镜像过程。(OCPBUGS-52588)

- 在以前的版本中，当将 oc-mirror 插件 v2 与 **-dry-run** 标志搭配使用时，工作目录中的 **cluster-resources** 文件夹会被清除。因此，之前生成的文件（如 **idms-oc-mirror.yaml** 和 **itms-oc-mirror.yaml** ）已被删除。在这个版本中，**cluster-resources** 文件夹不再在空运行操作过程中清除，保留任何之前生成的配置文件。(OCPBUGS-50963)

- 在以前的版本中，即使出现镜像错误，oc-mirror 插件 v2 也会返回一个退出状态 **0** (成功)。因此，oc-mirror 插件 v2 在自动工作流中运行失败可能会无法探测到。在这个版本中，oc-mirror 插件 v2 已被更新，以在镜像失败时返回非 **0** 退出状态。尽管修复了这个问题，用户也不应该只依赖自动化工作流中的退出状态。建议用户手动检查 oc-mirror 插件 v2 生成的 **mirroring_errors_XXX_XXX.txt** 文件来识别潜在的问题。(OCPBUGS-49880)

- 在以前的版本中，当使用内部 oc-mirror 保留关键字（如在目标中的 **release-images** 或 **--from** 路径标记），操作可能会失败或出现意外行为。在这个版本中，oc-mirror 插件 v2 可以正确地处理目标或源路径中使用的保留关键字。(OCPBUGS-42862)

OpenShift CLI (oc)

- 在以前的版本中，如果您尝试使用 **oc adm node-image** 命令将节点添加到断开连接的环境中，则命令无法访问私有 registry 镜像，从而导致节点添加失败。只有集群最初安装了从 (mirror.openshift.com)下载的安装程序二进制文件时，才会发生这个错误。在这个版本中，实现了一个修复，可以成功在断开连接的环境中创建镜像拉取(pull)和节点。(OCPBUGS-53106)

- 对于使用基于 Agent 的安装程序安装版本 4.15.0 到 4.15.26 的集群，从 CoreOS 中构建的 root 证书会添加到 user-ca-bundle 中，即使用户没有显式指定它们。在以前的版本中，当使用 **oc adm node-image create** 命令将节点添加到这些集群时，从集群的 user-ca-bundle 获取的 **additionalTrustBundle** 太大，从而导致无法添加节点。在这个版本中，在生成 **additionalTrustBundle** 时过滤内置证书，以便只包括用户配置的证书，并可以成功添加节点。(OCPBUGS-43990)

- 在以前的版本中，**oc adm inspect --all-namespaces** 命令构建了一个程序错误，意味着 must-gather 无法正确收集有关租期、**csistoragecapacities** 和 assisted-installer 命名空间的信息。在这个版本中，这个问题已被解决，must-gather 将正确收集信息。(OCPBUGS-44857)

- 在以前的版本中，**oc adm node-image create --pxe generated** 命令不会只创建 Preboot Execution Environment (PXE) 工件。相反，命令使用 **node-joiner** pod 中的其他工件创建了 PXE 工件，并将它们全部存储在错误的子目录中。另外，PXE 工件错误地带有 **agent** 前缀，而不是 **node**。在这个版本中，生成的 PXE 工件存储在正确的目录中，并接收正确的前缀。(OCPBUGS-45311)

Operator Lifecycle Manager (OLM)

- 在以前的版本中，如果 Operator 没有所需的 **olm.managed=true** 标签，Operator 可能会失败，并进入 **CrashLoopBackOff** 状态。当发生这种情况时，日志不会报告状态为 error。因此，很难诊断失败。在这个版本中，这种类型的失败报告为错误。(OCPBUGS-56034)

- 在以前的版本中，Machine Config Operator (MCO)不会搜索 **/etc/docker/certs.d** 目录来挂载镜像所需的证书。因此，Operator Controller 和目录启动失败，因为它们无法访问在此目录中托管的证书。在这个版本中，这个问题已被解决。(OCPBUGS-54175)

- 在此发行版本中，集群扩展更新有时会失败，并显示 **CRDUpgradeCheck** 资源：**unknown change, refusing to determine that change is safe**这个错误的原因是 OLM v1 计算版本模式之间的区别。在这个版本中解决了这个问题。(OCPBUGS-53019)

- 在以前的版本中，Operator Controller 有时无法正确挂载 CA 证书。因此，Operator Controller 无法连接到 catalogd，因为 TLS 证书验证错误。在这个版本中解决了这个问题。(OCPBUGS-49860)

- 在以前的版本中，在挂载 Operator Controller 和目录 pod 前，OLM v1 不会等待证书进入就绪状态。这些更新解决了这个问题。OCPBUGS-48830 和 (OCPBUGS-49418)

- 在以前的版本中，OLM v1 不会应用 Operator 捆绑包中集群扩展作者提供的所有元数据。因此，OLM v1 没有应用在 **metadata/properties.yaml** 文件中指定的属性，如更新约束。在这个版本中解决了这个问题。(OCPBUGS-44808)

Operator Controller Manager

- 在以前的版本中，无论默认代理设置是什么，**HTTP_PROXY**, **http_proxy**, **HTTPS_PROXY**, **https_proxy**, **NO_PROXY**, 和 **no_proxy** 变量都会在构建容器中设置。在这个版本中，只有在默认值中定义且不是 null 时，才会添加变量。(OCPBUGS-55642)

- 在以前的版本中，在嵌入式凭证过期前，不会重新生成为内部 Image Registry 生成的镜像 pull secret，从而导致镜像 pull secret 无效的时间。在这个版本中，在嵌入式凭证过期前，镜像 pull secret 会被刷新。(OCPBUGS-50507)

- 在以前的版本中，OLM v1 不会搜索 **/etc/docker/** 目录以挂载镜像所需的证书。因此，OLM v1 无法挂载自定义证书。在这个版本中解决了这个问题。(OCPBUGS-48795)

- 在以前的版本中，OLM v1 会在常规集群维护过程中发生的临时中断期间发送错误消息，如领导选举。在这个版本中解决了这个问题。(OCPBUGS-48765)

- 在以前的版本中，Operator Lifecycle Manager (OLM) Classic 在尝试协调同一命名空间中的 Operator 期间时会错误地报告 **Subscription** 资源失败。当发生这种情况时，Operator 无法安装。在这个版本中解决了这个问题。(OCPBUGS-48486)

- 在以前的版本中，当每个安装的 Operator 协调时，OLM (Classic) 会为每个已安装的 Operator 生成一个目录源快照。这个行为会导致 CPU 使用率高。在这个版本中，OLM (Classic)缓存目录源，并将调用限制为 gRPC 远程过程调用(gRPC)服务器来解决这个问题。(OCPBUGS-48468)

Performance Addon Operator

- 在以前的版本中，如果您在性能配置集中指定了较长的隔离 CPU 字符串，如 **0,1,2,...,512**, **tuned**, Machine Config Operator 和 **rpm-ostree** 组件无法按预期处理字符串。因此，在应用性能配置集后，缺少预期的内核参数。系统会以静默方式失败，且没有报告的错误。在这个版本中，性能配置集中的隔离 CPU 的字符串转换为顺序范围，如 **0-512**。因此，在大多数场景中，内核参数会如预期应用。(OCPBUGS-45264)

注意

这个问题可能仍然发生在性能配置集中隔离 CPU 的某些输入，比如一个较长的奇数数字 **1,3,5,...,511**。

- 在以前的版本中，Performance Profile Creator (PPC)无法为其逻辑处理器有不同内核 ID 编号（每个插槽）的计算节点构建性能配置集，且节点存在于同一节点池中。例如，对于具有逻辑处理器 **2** 和 **18** 的两个计算节点，PPC 会失败，其中一个节点分组为核心 ID **2**，其他节点组为核心 ID **9**。
  在这个版本中，PPC 不再无法创建性能配置集，因为 PPC 现在可以为具有其逻辑处理器的不同内核 ID 号的集群构建性能配置集。PPC 现在输出一条警告信息，表示谨慎使用生成的性能配置集，因为不同的内核 ID 号可能会影响系统优化和隔离管理任务。(OCPBUGS-44372)

Samples Operator

- 在以前的版本中，Samples Operator 更新了 **Progressing** 条件中的 **lastTransitionTime** spec，即使条件没有改变。这使得 Operator 的 stable 比它不太稳定。在这个版本中，**lastTransitionTime** spec 仅在 **Progressing** 条件更改时更新。(OCPBUGS-54591)

- 在以前的版本中，在 **Progressing** 条件中未排序的镜像流名称会导致不必要的更新。这会导致过量用户更新，并降低了系统性能。在这个版本中，**activeImageStreams** 功能排序会属于镜像导入。此操作提高了 Cluster Samples Operator 的效率，减少了不必要的更新，并提高了整体性能。(OCPBUGS-54590)

- 在以前的版本中，Samples Operator 为所有集群 Operator 建立监视，这会导致在任何 Operator 发生变化时运行 Samples Operator 的同步循环。在这个版本中，Samples Operator 只监视需要监控的 Operator。(OCPBUGS-54589)

存储

- 在以前的版本中，使用 **oc adm top pvc** 命令不会显示带有受限网络配置的集群的持久性卷声明(PVC)的用量统计，如在断开连接的环境中具有代理或集群的集群。在这个版本中，可以为这些环境中的集群获取用量统计。(OCPBUGS-54168)

- 在以前的版本中，如果 vCenter 地址不正确，VMware vSphere CSI 驱动程序 Operator 进入 panic 模式。在这个版本中，这个问题已被解决。(OCPBUGS-43273)

- 在以前的版本中，带有 C3-standard-2、C3-standard-4、N4-standard-2 和 N4-standard-4 节点的 Google Cloud Platform (GCP) Persistent Disk 集群可能会错误地超过最大可附加磁盘号，这应该为 16，这可以防止您成功创建或将卷附加到 pod。在这个版本中，不会超过最大值，因此不会影响成功创建或将卷附加到 pod。(OCPBUGS-39258)

- 在以前的版本中，当删除持久性卷(PV)时，Local Storage Operator (LSO)不会可靠地重新创建符号链接。在这个版本中，在创建 PV 时，在查找新符号链接前会选择之前指定的符号链接。(OCPBUGS-31059)

- 在以前的版本中，当 Cloud Credential Operator (CCO)没有为 Container Storage Interface (CSI)驱动程序 Operator 提供凭证时，CSI 驱动程序 Operator 会一直保留在 **Progressing=true** 中，并显示 **operator is waiting for deployment/unavailable**。在这个版本中，当进度状态持续为 15 分钟或更长时间时，Operator 会变为 **Degraded=True**。(OCPBUGS-24588)

- 在以前的版本中，名称为 53 个字符的计算节点，在使用 hostpath Container Storage Interface (CSI)驱动程序时，当 external-provisioner 上使用 **--enable-node-deployment** 标志时，卷置备会失败。在这个版本中，这个问题已被解决，且计算节点长度没有限制。(OCPBUGS-49805)

- 在以前的版本中，当使用托管 control plane 创建托管集群时，在 Azure Red Hat OpenShift 上，Azure Disk Container Storage Interface (CSI)驱动程序将无法成功置备卷。在这个版本中，这个问题已被解决，Azure Disk CSI 驱动程序可以成功置备卷。(OCPBUGS-46575)

- 在以前的版本中，当这些设备分区时，附加到多路径设备的互联网小型计算机系统接口(iSCSI)和光纤通道设备无法正确解析。在这个版本中，一个修复可确保分区多路径设备现在可以正确地解决。(OCPBUGS-46038)

- 在以前的版本中，当使用指定标签创建托管集群时，AWS EBS 驱动程序、Driver Operator、快照控制器和快照 Webhook pod 不会将这些指定的标签传播到它们。在这个版本中，指定的标签会被传播。(OCPBUGS-45073)

- 在以前的版本中，Manila Container Storage Interface (CSI)驱动程序在不需要的主机上运行服务。这是因为 Manila CSI 驱动程序为控制器和节点(worker)服务使用一个二进制文件。在这个版本中，CSI 驱动程序控制器 pod 只运行控制器服务，CSI 驱动程序节点 pod 只运行节点服务。(OCPBUGS-54447)

- 在以前的版本中，Container Storage Interface (CSI) Operator 在日志中会发出警告，这些项目会在以后会变得严重。在这个版本中，不再发出警告。(OCPBUGS-44374)

- 在以前的版本中，如果 vCenter 地址不正确，VMWare vSphere CSI 驱动程序 Operator 会 panic。在这个版本中，这个问题已被解决。(OCPBUGS-43273)

Red Hat Enterprise Linux CoreOS (RHCOS)

- 在以前的版本中，**GRUB** 引导装载程序不会在 RHCOS 节点上自动更新。因此，当在 RHEL 8 上创建节点并随后更新至 RHEL 时，**GRUB** 无法加载内核，因为它使用旧的 **GRUB** 版本不支持的格式。在这个版本中，在更新 OpenShift Container Platform 4.18 过程中强制使用 **GRUB** 引导装载程序更新，因此在 OpenShift Container Platform 4.19 中不会出现这个问题。(OCPBUGS-55144)

1.7. 技术预览功能状态

此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。请注意红帽客户门户网站中的以下支持范围：

技术预览功能支持范围

在以下表格中，功能被标记为以下状态：

- *不可用*

- *技术预览*

- *公开发行*
- *已弃用*
- *删除*

认证和授权技术预览功能

表 1.18. 认证和授权技术预览

功能	4.17	4.18	4.19
Pod 安全准入限制强制	技术预览	技术预览	技术预览
使用外部 OIDC 身份提供程序直接验证	不可用	不可用	技术预览

Edge 计算技术预览功能

表 1.19. Edge 计算技术预览

功能	4.17	4.18	4.19
加速置备 GitOps ZTP	技术预览	技术预览	技术预览
使用 TPM 和 PCR 保护启用磁盘加密	技术预览	技术预览	技术预览
配置本地仲裁节点	不可用	不可用	技术预览

扩展技术预览功能

表 1.20. 扩展技术预览

功能	4.17	4.18	4.19
Operator Lifecycle Manager (OLM) v1	技术预览	公开发行	公开发行
使用 sigstore 签名进行容器镜像的 OLM v1 运行时验证	不可用	技术预览	技术预览
OLM v1 权限 preflight 检查集群扩展	不可用	不可用	技术预览
OLM v1 在指定命名空间中部署集群扩展	不可用	不可用	技术预览

安装技术预览功能

表 1.21. 安装技术预览

功能	4.17	4.18	4.19
使用 kvc 向节点添加内核模块	技术预览	技术预览	技术预览

功能	4.17	4.18	4.19
为 SR-IOV 设备启用 NIC 分区	公开发行	公开发行	公开发行
Google Cloud Platform (GCP) 的用户定义的标记和标签	公开发行	公开发行	公开发行
使用 Assisted Installer 在 Alibaba Cloud 上安装集群	技术预览	技术预览	技术预览
使用机密虚拟机在 Microsoft Azure 上安装集群	不可用	技术预览	公开发行
在 RHEL 中的 BuildConfig 中挂载共享权利	技术预览	技术预览	技术预览
OpenShift zones 支持 vSphere 主机组	不可用	不可用	技术预览
可选择 Cluster Inventory	技术预览	技术预览	技术预览
使用 Cluster API 实现在 GCP 上安装集群	公开发行	公开发行	公开发行
在 GCP 上启用用户置备的 DNS	不可用	不可用	技术预览
使用多个网络接口控制器在 VMware vSphere 上安装集群	不可用	技术预览	技术预览
使用裸机作为服务	不可用	不可用	技术预览

Machine Config Operator 技术预览功能

表 1.22. Machine Config Operator 技术预览

功能	4.17	4.18	4.19
改进了 MCO 状态报告 (**oc get machineconfigpool**)	技术预览	技术预览	技术预览
OpenShift/On-cluster RHCOS 镜像分层的镜像模式	技术预览	技术预览	公开发行

机器管理技术预览功能

表 1.23. 机器管理技术预览

功能	4.17	4.18	4.19
使用 Amazon Web Services 的集群 API 管理机器	技术预览	技术预览	技术预览
使用 Google Cloud Platform 的 Cluster API 管理机器	技术预览	技术预览	技术预览
使用 Microsoft Azure 的 Cluster API 管理机器	不可用	技术预览	技术预览

功能	4.17	4.18	4.19
使用 VMware vSphere 的集群 API 管理机器	技术预览	技术预览	技术预览
使用裸机的集群 API 管理虚拟机	不可用	不可用	技术预览
IBM Power® Virtual Server 的云控制器管理器	技术预览	技术预览	技术预览
使用计算机器集在现有 VMware vSphere 集群中添加多个子网	不可用	技术预览	技术预览
使用机器集为 Microsoft Azure 虚拟机配置可信启动	技术预览	技术预览	公开发行
使用机器集配置 Azure 机密虚拟机	技术预览	技术预览	公开发行

监控技术预览功能

表 1.24. 监控技术预览

功能	4.17	4.18	4.19
指标集合配置集	技术预览	技术预览	公开发行

多架构技术预览功能

表 1.25. 多架构技术预览

功能	4.17	4.18	4.19
arm64 构架上的 **kdump**	技术预览	技术预览	技术预览
s390x 架构上的 **kdump**	技术预览	技术预览	技术预览
ppc64le 架构上的 **kdump**	技术预览	技术预览	技术预览
支持配置镜像流导入模式行为	不可用	技术预览	技术预览

网络功能虚拟化功能

表 1.26. 网络技术预览跟踪器

功能	4.17	4.18	4.19
eBPF manager Operator	技术预览	技术预览	技术预览
通过 L2 模式，使用节点的一个子集（由特定的 IP 地址池指定）中的 MetalLB 服务进行广告	技术预览	技术预览	技术预览

功能	4.17	4.18	4.19
更新特定于接口的安全 sysctl 列表	技术预览	技术预览	技术预览
出口服务自定义资源	技术预览	技术预览	技术预览
BGPPeer 自定义资源中的 VRF 规格	技术预览	技术预览	技术预览
NodeNetworkConfigurationPolicy 自定义资源中的 VRF 规格	技术预览	技术预览	公开发行
SR-IOV VF 的主机网络设置	公开发行	公开发行	公开发行
MetalLB 和 FRR-K8s 集成	公开发行	公开发行	公开发行
PTP grandmaster 时钟的自动秒处理	公开发行	公开发行	公开发行
PTP 事件 REST API v2	公开发行	公开发行	公开发行
在裸机上的 OVN-Kubernetes 自定义 **br-ex** 网桥	公开发行	公开发行	公开发行
vSphere 和 RHOSP 上的 OVN-Kubernetes 自定义 **br-ex** 网桥	技术预览	技术预览	技术预览
从 OpenShift SDN 实时迁移 OVN-Kubernetes	公开发行	不可用	不可用
用户定义的网络分段	技术预览	公开发行	公开发行
动态配置管理器	不可用	技术预览	技术预览
SR-IOV Network Operator 支持 Intel C741 Emmitsburg 芯片组	不可用	技术预览	技术预览
用于 Ingress 管理的网关 API 和 Istio	不可用	技术预览	公开发行
PTP 普通时钟的双端口 NIC	不可用	不可用	技术预览
DPU Operator	不可用	不可用	技术预览
Whereabouts IPAM CNI 插件的 fast IPAM	不可用	不可用	技术预览
Unnumbered BGP peering	不可用	不可用	技术预览

节点技术预览功能

表 1.27. 节点技术预览

功能	4.17	4.18	4.19
MaxUnavailableStatefulSet 功能集	技术预览	技术预览	技术预览
sigstore 支持	技术预览	技术预览	技术预览

OpenShift CLI (oc) 技术预览功能

表 1.28. OpenShift CLI (oc) 技术预览

功能	4.17	4.18	4.19
oc-mirror 插件 v2	技术预览	公开发行	公开发行
oc-mirror 插件 v2 enclave 支持	技术预览	公开发行	公开发行
oc-mirror 插件 v2 删除功能	技术预览	公开发行	公开发行

Operator 生命周期和开发技术预览功能

表 1.29. Operator 生命周期和开发技术预览

功能	4.17	4.18	4.19
Operator Lifecycle Manager (OLM) v1	技术预览	公开发行	公开发行
为基于 Helm 的 Operator 项目构建工具	Deprecated	删除	删除
为基于 Java 的 Operator 项目构建工具	Deprecated	删除	删除

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

表 1.30. RHOSP 技术预览

功能	4.17	4.18	4.19
RHOSP 集成到 Cluster CAPI Operator	技术预览	技术预览	技术预览
在本地磁盘上带有 **rootVolumes** 和 **etcd** 的 control plane	公开发行	公开发行	公开发行
在 RHOSP 17.1 上托管 control plane	不可用	不可用	技术预览

可扩展性和性能技术预览功能

表 1.31. 可扩展性和性能技术预览

功能	4.17	4.18	4.19
factory-precaching-cli 工具	技术预览	技术预览	技术预览
超线程感知 CPU Manager 策略	技术预览	技术预览	技术预览
挂载命名空间封装	技术预览	技术预览	技术预览
Node Observability Operator	技术预览	技术预览	技术预览
增加 etcd 数据库大小	技术预览	技术预览	技术预览
使用 RHACM **PolicyGenerator** 资源管理 GitOps ZTP 集群策略	技术预览	技术预览	公开发行
固定镜像设置	技术预览	技术预览	技术预览
托管 control plane 上支持的 NUMA 感知调度	不可用	不可用	技术预览

存储技术预览功能

表 1.32. 存储技术预览

功能	4.17	4.18	4.19
AWS EFS 存储 CSI 使用指标	公开发行	公开发行	公开发行
使用 Local Storage Operator 进行自动设备发现和置备	技术预览	技术预览	技术预览
Azure File CSI 快照支持	技术预览	技术预览	技术预览
Azure File 跨订阅支持	不可用	不可用	公开发行
OpenShift 构建中的共享资源 CSI 驱动程序	技术预览	技术预览	技术预览
Secret Store CSI Driver Operator	技术预览	公开发行	公开发行
CIFS/SMB CSI Driver Operator	技术预览	公开发行	公开发行
VMware vSphere 多个 vCenter 支持	技术预览	公开发行	公开发行
在 vSphere 上禁用/启用存储	技术预览	技术预览	公开发行
为 vSphere 增加每个节点的最大卷数量	不可用	不可用	技术预览
RWX/RWO SELinux Mount	开发者预览	开发者预览	开发者预览

功能	4.17	4.18	4.19
在数据存储之间迁移 CNS 卷	开发者预览	开发者预览	公开发行
CSI 卷组快照	不可用	技术预览	技术预览
GCP PD 支持 C3/N4 实例类型和 hyperdisk-balanced 磁盘	不可用	公开发行	公开发行
GCP Filestore 支持工作负载身份	公开发行	公开发行	公开发行
OpenStack Manila 支持 CSI 调整大小	不可用	公开发行	公开发行
卷属性类	不可用	不可用	技术预览

Web 控制台技术预览功能

表 1.33. Web 控制台技术预览跟踪程序

功能	4.17	4.18	4.19
OpenShift Container Platform Web 控制台中的 Red Hat OpenShift Lightspeed	技术预览	技术预览	技术预览

1.8. 已知问题

- 在 OpenShift Container Platform 4.19 中，使用 IPsec 进行网络加密的集群可能会遇到 pod 到 pod 连接的问题。这可防止某些节点上的某些 pod 访问其他节点上的服务，从而导致连接超时。内部测试无法在具有 120 个节点或更少的集群中重现此问题。这个问题还没有临时解决方案。(OCPBUGS-55453)
- 在墨西哥中心区域 **mx-central-1** 的 AWS 上安装的 OpenShift Container Platform 集群无法销毁。(OCPBUGS-56020)
- 在 Azure 上安装集群时，如果您将任何 **compute.platform.azure.identity.type**、**controlplane.platform.azure.identity.type** 或 **platform.azure.defaultMachinePlatform.identity.type** 字段值设置为 **None**，您的集群无法从 Azure Container Registry 拉取镜像。您可以通过提供用户身份或将 identity 字段留空来避免此问题。在这两种情况下，安装程序会生成用户分配的身份。(OCPBUGS-56008)
- 在以前的版本中，kubelet 不会考虑在 **syncPod** 方法中运行的探测，它会定期检查 pod 的状态，并在正常探测外进行就绪度探测。在这个版本中，当 kubelet 错误地计算 **readinessProbe** 周期时，会修复一个程序错误。但是，pod 作者可能会看到配置了就绪度探测的 pod 的就绪度延迟可能会增加。这个行为对于配置的探测更为准确。如需更多信息，请参阅(OCPBUGS-50522)
- 当 grandmaster 时钟 (T-GM) 过渡到 **Locked** 状态时，存在一个已知问题。这会在 Digital Phase-Locked Loop (DPLL) 完成其过渡到 **Locked-HO-Acquired** 状态之前，并在全局导航 Satellite 系统(GNSS)时间源恢复后进行。(OCPBUGS-49826)
- 在 AWS 上安装集群时，如果您在运行任何 **openshift-install create** 命令前没有配置 AWS 凭证，安装程序会失败。(OCPBUGS-56658)

- **must-gather** 工具不会收集从 OpenShift Container Platform 4.14 升级的集群的 IPsec 信息。出现这个问题的原因是 **networks.operator.openshift.io cluster** CR 中的 **ipsecConfig** 配置有一个空的构造 **{}**。空构造传递给 OpenShift Container Platform 的升级版本。这个问题的一个临时解决方案是，在 Cluster Network Operator (CNO) CR 中运行以下命令，使用 **ipsecConfig** 配置：

```
$ oc patch networks.operator.openshift.io cluster --type=merge -p \
  '{
  "spec":{
    "defaultNetwork":{
      "ovnKubernetesConfig":{
        "ipsecConfig":{
          "mode":"Full"
        }}}}}'
```

  运行命令后，CNO 会收集您可以检查的 **must-gather** 日志。

  (OCPBUGS-52367)

- 网关 API 和 Amazon Web Services (AWS)、Google Cloud Platform (GCP)和 Microsoft Azure 私有集群中存在一个已知问题。为网关置备的负载均衡器始终配置为外部，这可能会导致错误或意外行为：

  - 在 AWS 私有集群中，负载均衡器会处于 **pending** 状态，并报告错误： **Error sync load balancer: failed to ensure load balancer: could not find any appropriate subnets for the ELB**。
  - 在 GCP 和 Azure 私有集群中，当负载均衡器没有外部 IP 地址时，使用外部 IP 地址置备负载均衡器。

  这个问题不支持临时解决方案。(OCPBUGS-57440)

- 如果崩溃，**mlx5_core** NIC 驱动程序会导致内存不足问题， **kdump** 不会将 **vmcore** 文件保存在 **/var/crash** 中。要保存 **vmcore** 文件，请使用 **crashkernel** 设置为 **kdump** 内核保留 1024 MB 内存。(OCPBUGS-54520,RHEL-90663)

- 在 4 代 Intel Xeon 处理器上存在一个已知问题。(OCPBUGS-42495)

- 目前，使用 **guaranteed** QoS 类和请求整个 CPU 的 pod 可能无法在节点重启或 kubelet 重启后自动重启。此问题可能会在配置了静态 CPU Manager 策略的节点并使用 **full-pcpus-only** 的规格中发生，当节点上的大多数或所有 CPU 都已由此类工作负载分配时。作为临时解决方案，请手动删除并重新创建受影响的 pod。(OCPBUGS-43280)

- 目前，当 **irqbalance** 服务在特定 AArch64 机器上运行时，缓冲区溢出问题可能会导致服务崩溃。因此，对延迟敏感的工作负载可能会受到在 CPU 中没有正确分布的非受管中断的影响，从而导致性能下降。当前没有解决此问题的方法。(RHEL-89986)

- 目前，在配置了 SR-IOV 网络虚拟功能的集群中，负责网络设备重命名和由 Node Tuning Operator 管理的 TuneD 服务的系统服务之间可能会出现竞争条件。因此，在节点重启后 TuneD 配置集可能会降级，从而导致性能下降。作为临时解决方案，重启 TuneD pod 以恢复配置集状态。(OCPBUGS-41934)

- 由于 RHEL-83435，运行 OpenShift Container Platform 4.19 的集群无法挂载从 VMware vSAN Files 导出的 NFS 卷。要避免这个问题，请确保在 8.0 P05 或更高版本的最新版本中运行 VMware ESXi 和 vSAN。(OCPBUGS-55978)

1.9. 异步勘误更新

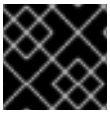
OpenShift Container Platform 4.19 的安全更新、程序错误修正、功能增强更新将会通过红帽网络以异步勘误的形式发布。所有的 OpenShift Container Platform 4.19 勘误都可以通过红帽客户门户网站获得。OpenShift Container Platform 生命周期 包括了详细的与异步勘误相关的内容。

红帽客户门户网站的用户可以在红帽订阅管理（RHSM）帐户设置中启用勘误通知功能。当勘误通知被启用后，每当用户注册的系统相关勘误被发布时，用户会收到电子邮件通知。

注意

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

本节的内容将会持续更新，以提供以后发行的与 OpenShift Container Platform 4.19 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.19.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-2025:14823 - OpenShift Container Platform 4.19.10 镜像发行版本、程序错误修正和安全更新公告

发布日期： 2025 年 9 月 2 日

OpenShift Container Platform release 4.19.10 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHBA-2025:14823 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:14817 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.10 --pullspecs
```

1.9.1.1. 功能增强

- 与 on-cluster 镜像模式一起使用的 **MachineOSConfig** 对象的名称现在必须与您要部署自定义分层镜像的机器配置池相同。这个更改可防止在每个机器配置池中使用多个 **MachineOSConfig** 对象。(OCPBUGS-60414)

1.9.1.2. 程序错误修复

- 在此次更新之前，当管理集群使用很多镜像存储库配置时，托管 Control Plane (HCP)不会按顺序查询有效负载存储库，从而导致托管集群部署在断开连接的环境中失败（如果第一个镜像不可用）。系统出错，而不是搜索下一个可用镜像。在这个版本中，HCP 有效负载会迭代整个镜像列表，直到找到可用镜像，允许部署按预期成功。(OCPBUGS-57141)

- 在此次更新之前，当在版本 4.19 中使用零接触置备(ZTP)部署单节点 OpenShift 时，在主接口上配置了很多 IP 地址时，**apiserver** pod 将无法连接到 etcd。因此，etcd 证书不包括所有配置的 IP 地址，从而导致传输层安全(TLS)验证错误。在这个版本中，**apiserver** pod 可以在这些配置中

成功连接到 etcd，允许带有许多主接口 IP 地址的单节点 OpenShift 部署正确初始化。(OCPBUGS-59285)

- 在此次更新之前，IBM Cloud 不包含在验证检查中的单节点 OpenShift 安装中，从而导致在 IBM Cloud 上安装单节点 OpenShift 时造成验证错误。在这个版本中，IBM Cloud 支持单节点 OpenShift 安装改进了 IBM Cloud 上最终用户的安装体验。(OCPBUGS-59607)

- 在此次更新之前，**Delete** 工作流会错误地显示 **工作流模式：diskToMirror / delete**，从而导致用户对正确的工作流模式的混乱。在这个版本中，**工作流模式：删除** 在删除操作过程中显示。(OCPBUGS-59761)

- 在此次更新之前，在不同容器镜像间共享重复的镜像会导致 **oc-mirror** 中错误的计算，用于 Helm chart 的总镜像镜像。因此，一些 Helm 镜像不会被镜像。在这个版本中，**oc-mirror** 中镜像 Helm 镜像的错误计数已被修复，提高了镜像镜像计数的准确性。(OCPBUGS-60086)

- 在此次更新之前，**HorizontalPodAutoscaler** 将 **istiod-openshift-gateway** 临时扩展为两个副本，从而导致因为测试只需要一个副本而造成持续集成(CI)失败。在这个版本中，**HorizontalPodAutoscaler** 扩展会被调整，以支持 **istiod-openshift-gateway** 的单一副本。(OCPBUGS-60204)

- 在此次更新之前，在 4.15 之前升级到版本，或新版本的 4.15 部署 **MachineConfigNode** 自定义资源定义(CRD)，尽管还只是一个技术预览。因此，因为不需要 CRD，集群无法升级。在这个版本中，技术预览 **MachineConfigNode** CRD 已从默认集群中删除，确保没有升级。(OCPBUGS-60265)

- 在此次更新之前，在作为主网络堆栈的双栈集群中，裸机安装程序置备基础架构(IP)会错误地为虚拟介质 ISO 镜像提供 IPv4 URL。这会导致仅在 IPv6 网络配置的 Baseboard Management Controller (BMC)上失败，因为 BMC 无法访问 IPv4 地址。在这个版本中，安装程序逻辑已被更新，在 BMC 使用 IPv6 地址时始终提供 IPv6 URL，安装过程现在可以成功完成。(OCPBUGS-60402)

- 在此次更新之前，Amazon Web Services (AWS) **machinesets** 可以有一个 null **userDataSecret** 名称，从而导致机器处于置备状态。在这个版本中，需要一个非空的 **userDataSecret** 名称，防止出现意外的机器行为。(OCPBUGS-60427)

- 在此次更新之前，限制会阻止证书的有效性超过签名者的有效性。这会影响 **localhost-recovery.kubeconfig**，因为 node-system-admin-client 证书被错误地生成了一年的生命周期，而不是预期的两年，从而导致 **localhost-recovery.kubeconfig** 过期。在这个版本中，signer 证书的有效性会延长到三年，确保 node-system-admin-client 证书现在具有两年的生命周期。(OCPBUGS-60495)

- 在此次更新之前，使用版本 4.13 或更早版本创建的 AWS 上的 OpenShift Container Platform 集群无法更新到 4.19 版本。使用版本 4.14 及之后的版本创建的集群默认具有 AWS **cloud-conf** ConfigMap，从 OpenShift Container Platform 4.19 开始需要此 ConfigMap。在这个版本中，Cloud Controller Manager Operator 被更新为在集群中不存在时创建默认的 **cloud-conf** ConfigMap。这个更改可让使用版本 4.13 或更早版本创建的集群更新至 4.19 版本。(OCPBUGS-60950)

1.9.1.3. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.2. RHSA-2025:13848 - OpenShift Container Platform 4.19.9 镜像发行版本、程序错误修正和安全更新公告

发布日期：25 年 8 月 19 日

OpenShift Container Platform release 4.19.9 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:13848 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:13827 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.9 --pullspecs
```

1.9.2.1. 功能增强

- 在这个版本中，您可以在托管的 control plane 上安装 NUMA Resources Operator，启用 NUMA 感知调度支持。如需更多信息，请参阅为托管 control plane 创建 NUMAResourcesOperator 自定义资源。此功能增强作为技术预览功能提供。

1.9.2.2. 程序错误修复

- 在此次更新之前，4.1 和 4.2 的引导镜像无法与 OpenShift Container Platform 4.19 一起使用，并导致集群操作降级。在这个版本中，为可扩展固件接口(EFI)和固件组件安装静态 Grand Unified Bootloader (GRUB)配置，集群通常在节点扩展过程中运行。(OCPBUGS-52485)

- 在此次更新之前，Google Cloud Platform (GCP)机器 API 会被顺序协调处理阻止。因此，在 GCP 集成过程中，用户会出现节点扩展缓慢的问题。在这个版本中，通过启用许多协调过程的并行执行来提高 GCP 机器 API 性能。因此，GCP 节点扩展性能提高了。(OCPBUGS-59386)

- 在此次更新之前，用户使用 VPA 中带有上游问题的版本配置 OpenShift Container Platform Vertical Pod Autoscaler (VPA)自定义推荐器。因此，这个问题会在 VPA 更新中造成不稳定。在这个版本中，自定义 VPA 检查点垃圾收集器不会删除未跟踪的检查点，并防止 OpenShift Container Platform 中的不稳定。因此，OpenShift Container Platform VPA 更新是稳定的，且不会发生恒定的 pod 重新调度。(OCPBUGS-59638)

- 在此次更新之前，机器配置守护进程在 VMware vSphere 基础架构上的 OpenShift Container Platform 4.16 清单应用程序过程中失败域名系统(DNS)查找。因此，在 OpenShift Container Platform 4.16 升级过程中，用户 DNS 查找会失败，从而无限期停止升级。在这个版本中，实施使用 backoff 的远程操作系统更新重试，以避免因为 CoreDNS pod 在升级过程中重启而失败。(OCPBUGS-59899)

- 在此次更新之前，因为增加了协调尝试限制，集群升级会失败。此失败会导致 Prometheus pod 不可用，并导致服务降级。在这个版本中，Operator 在报告失败前允许额外的协调尝试。因此，集群升级测试的稳定性有所改进，减少失败率并增强升级可靠性。(OCPBUGS-59932)

- 在此次更新之前，OpenShift Container Platform Precision Time Protocol (PTP) pod 的 sidecar 在终止后意外重启，并导致时钟类终止失败，并显示 **退出代码 7** 错误。因此，指标不可用。在这个版本中，sidecar 重启不会导致 OpenShift Container Platform PTP pod 中的时钟类终止错误，且不会在重启过程中停止。(OCPBUGS-59970)

- 在此次更新之前，当用户升级到 OpenShift Container Platform 4.19 时，Machine Config Operator (MCO)会轮转传输层安全(TLS)证书。这会导致节点在扩展过程中无法加入集群的问题。在这个版本中，MCO 提供了一个自定义 ARO 资源，它决定所需的主题备用名称(SAN) IP 地址，并在轮转的 TLS 证书中添加它。因此，节点可以在扩展过程中加入集群。(OCPBUGS-59978)

- 在此次更新之前，**ResourceEventStream** 代码格式中的一个插入错误会在用户连接到事件流时导致错误消息不正确。在这个版本中，事件流中错误消息的干预格式是正确的。因此，用户会在连接到事件流时看到准确的错误消息。(OCPBUGS-60039)

- 在此次更新之前，通信列表项目中的主节点端口没有绑定，并导致主节点上缺少通信流和服务不可用。在这个版本中，控制器管理器上的端口关闭，且只在 **localhost** 中可用。因此，该服务绑定到正确的端口。(OCPBUGS-60132)

- 在此次更新之前，**MachineSet** 自定义资源会因为多个 arch 注解标签而发生。因此，机器更新会失败。在这个版本中，通过允许 **{{capacity.cluster-autoscaler.kubernetes.io/labels}}** 注解中的多个标签来解决这个问题，并正确解析 architecture 值。因此，Machine Config Operator 在更新过程中不会失败。(OCPBUGS-60224)

- 在此次更新之前，**LeaderWorkerSet** Operator 描述已过时。因此，用户会出现不正确的描述。在这个版本中，**LeaderWorkerSet** Operator 描述已被更新，描述会准确描述这个概念。(OCPBUGS-60225)

- 在此次更新之前，**cloud-event-proxy** sidecar 进程终止，并导致通知 API 处于 **clockClass=0** 状态，即使 pod 恢复也是如此。因此，在 sidecar 进程终止后通知 API 会保留不活跃。在这个版本中，**cloud-event-proxy** 进程恢复不会导致通知 API 的 **clockClass=0** 状态。现在，当 **cloud-event-proxy** 恢复时，通知 API 可以正确地更新 **clockClass** 变量。(OCPBUGS-60261)

- 在此次更新之前，在 OVN-K 托管的集群公开敏感数据中新网络数据类型不足。因此，用户数据会被公开。在这个版本中，anonymizer 被更新，以发现和模糊新的网络数据类型，并确保安全通信。(OCPBUGS-60295)

1.9.2.3. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.3. RHSA-2025:12341 - OpenShift Container Platform 4.19.7 镜像发行版本、程序错误修正和安全更新公告

发布日期： 2025 年 8 月 5 日

OpenShift Container Platform release 4.19.7 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:12341 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:12342 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.7 --pullspecs
```

1.9.3.1. 功能增强

- KubeVirt Container Storage Interface (CSI)驱动程序现在支持卷扩展。用户可以在其租户集群中动态增加其持久性卷的大小。此功能简化了存储管理，实现更灵活且可扩展的基础架构。(OCPBUGS-58239)

1.9.3.2. 程序错误修复

- 在此次更新之前，因为使用相同的 **CreateProjectModal** 扩展点的多个插件导致控制台模式中的插件冲突。因此，只使用一个插件扩展，且无法更改列表顺序。在这个版本中，对插件存储的更

新会按照控制台 Operator 配置中定义的相同顺序解析扩展。因此，任何有权限更新 Operator 配置的人员都可以设置插件的优先级。(OCPBUGS-56280)

- 在此次更新之前，当您在 **Overview** 页面中的 **AlertmanagerReceiversNotConfigured** 警报中点 **Configure** 时，会出现运行时错误。在这个版本中，改进的导航处理可确保点 **Configure** 时不会发生运行时错误。(OCPBUGS-57105)

- 在此次更新之前，**/metrics/usage** 端点已更新，以包含 authentication 和 Cross-Site Request Forgery (CSRF)保护。因此，对此端点的请求启动失败并显示 "forbidden" 错误消息，因为请求 Cookie 中缺少必要的 CSRF 令牌。在这个版本中，CSRF 令牌被添加到 **/metrics/usage** 请求 cookie 中，它解决了 "forbidden" 错误消息。(OCPBUGS-58331)

- 在此次更新之前，当为带有没有指定客户端 secret 的 Open ID 集群的 **HostedCluster** 资源配置 OpenID Connect (OIDC)供应商时，会自动生成默认 secret 名称。因此，您无法配置 OIDC 公共客户端，因为这些客户端无法使用客户端 secret。在这个版本中，当不提供客户端 secret 时，不会生成默认 secret 名称。因此，您可以配置 OIDC 公共客户端。(OCPBUGS-58683)

- 在此次更新之前，当裸机主机(BMH)标记为 **Provisioned** 或 **ExternallyProvisioned** 时，系统会尝试取消置备它，或者首先将其关闭，并附加到 BMH 的 **DataImage** 也会防止删除。此问题会阻止或减慢主机删除速度，从而造成操作效率降低。在这个版本中，如果 BMH 具有 **分离的注解** 状态并删除，BMH 会过渡到 delete 状态，允许直接删除。(OCPBUGS-59133)

- 在此次更新之前，因为下载和控制台 pod 的节点选择器不匹配，所以 control plane 节点上的下载过程不一致。因此，下载被调度到随机节点上，这会导致潜在的资源争用和子优化性能。在这个版本中，下载的工作负载在 control plane 节点上持续调度，这可以提高资源分配。(OCPBUGS-59488)

- 在此次更新之前，因为过时的网络地址转换(NAT)处理，集群升级到 OpenShift Container Platform 4.18 会导致出口 IP 分配不一致。只有在 OVN-Kubernetes 控制器停机时，才会出现这个问题。因此，会发生重复的逻辑路由器策略和出口 IP 使用情况，这会导致流量流和中断不一致。在这个版本中，出口 IP 分配清理确保在 OpenShift Container Platform 4.18 集群中一致且可靠的出口 IP 分配。(OCPBUGS-59530)

- 在此次更新之前，如果您登录到控制台时没有足够权限，则 **get started** message occupied over space on pages。这个问题导致无法完全显示重要状态信息，如 **没有找到资源**。因此，会显示截断的信息版本。在这个版本中，**get started** 消息被调整大小，并删除页面的 disable 属性，以使用较少的屏幕空间，并允许滚动。在这个版本中，用户可以查看所有页面的完整状态和信息。现在，您可以查看所有页面的完整状态和信息。因此，**开始** 的内容通过滚动滚动保持完全可访问，这样可确保新用户指南和重要系统消息的可见性。(OCPBUGS-59639)

- 在此次更新之前，当您克隆一个长度为零的 **.tar** 文件时，**oc-mirror** 会因为空存档文件无限期运行。因此，当对 0 字节 **.tar** 文件进行镜像时，不会发生任何进度。在这个版本中，会检测到 0 字节 **.tar** 文件并报告为错误，这可防止 **oc-mirror** 挂起。(OCPBUGS-59779)

- 在此次更新之前，**oc-mirror** 不会检测使用别名子图的 Helm Chart 镜像。因此，在镜像后缺少 Helm Chart 镜像。在这个版本中，**oc-mirror** 会检测并镜像带有别名的子图的 Helm Chart 镜像。(OCPBUGS-59799)

1.9.3.3. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.4. RHSA-2025:11673 - OpenShift Container Platform 4.19.6 镜像发行版本、程序错误修正和安全更新公告

发布日期： 2025 年 7 月 29 日

OpenShift Container Platform release 4.19.6 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:11673 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:11674 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.6 --pullspecs
```

1.9.4.1. 功能增强

- KubeVirt Container Storage Interface (CSI)驱动程序现在支持卷扩展。用户可以在其租户集群中动态增加其持久性卷的大小。此功能简化了存储管理，实现更灵活且可扩展的基础架构。(OCPBUGS-58239)

1.9.4.2. 程序错误修复

- 在此次更新之前，**/metrics/usage** 端点已更新，以包含 authentication 和 Cross-Site Request Forgery (CSRF)保护。因此，对此端点的请求启动失败并显示 "forbidden" 错误消息，因为请求 Cookie 中缺少必要的 CSRF 令牌。在这个版本中，CSRF 令牌被添加到 **/metrics/usage** 请求 Cookie 中，从而解析 "forbidden" 错误消息。(OCPBUGS-58331)

- 在此次更新之前，**console.flag/model** 扩展点无法正常工作，防止在提供相关的模型时正确设置标志。在这个版本中，**console.flag/model** 可以正常工作，并在提供关联的模型时正确设置标记。(OCPBUGS-59513)

1.9.4.3. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.5. RHSA-2025:11363 - OpenShift Container Platform 4.19.5 镜像发行版本、程序错误修正和安全更新公告

发布日期： 2025 年 7 月 22 日

OpenShift Container Platform release 4.19.5 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:11363 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:11364 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.5 --pullspecs
```

1.9.5.1. 程序错误修复

- 在此次更新之前，捆绑包解包作业不会从创建它们的 catalog-operator 继承 control-plane 容错。因此，捆绑包解包作业只在 worker 节点上运行。如果因为污点而没有 worker 节点可用，则 admins 无法在集群中安装或升级 Operator。在这个版本中，control-plane 容限被用于捆绑解包作业，以便作业在 control plane 的主节点上执行。(OCPBUGS-59258)

- 在此次更新之前，因为 'OVNkubernetes'caused 数据包丢弃状态更新导致出口互联网协议(IP)处理不稳定。这些数据包丢弃受影响的网络流量流。在这个版本中，'OVNkubernetes'pods 一致使用它们分配的出口 IP。因此，丢弃的软件包会减少，并改进了网络流量流。(OCPBUGS-59234)

- 在此次更新之前，Amazon Web Services (AWS) Cloud Provider 不会为 AWS Load Balancer 设置 **HTTP:10256/healthz** 的默认 ping 目标。对于在 AWS 上运行的 LoadBalancer 服务，AWS 中创建的 Load Balancer 对象具有 **TCP:32518** 的 ping 目标。因此，集群范围的服务健康探测无法正常工作，该服务在升级过程中停机。在这个版本中，云配置 **ClusterServiceLoadBalancerHealthProbeMode** 属性设置为 **Shared**，以确保将配置传递给 AWS Cloud Provider。因此，AWS Load Balancers 具有 **HTTP:10256/healthz** 的正确健康检查 ping 目标。(OCPBUGS-59101)

- 在此次更新之前，Machine **Operator** (MCO)会安装 **podman-etcd** 代理，以便在等待 RPM Package Manager (RPM)版本访问存储库时启用测试。在这个版本中，MCO 安装的代理会被删除，因为 RPM 版本可用。(OCPBUGS-58894)

- 在此次更新之前，当运行 **oc-mirror v2** disk-to-mirror 工作流时，在没有有效镜像 tar 文件的情况下，返回的错误消息无法正确识别问题。在这个版本中，**oc-mirror v2** 工作流会返回错误消息，指出 **没有与 "mirror_[0-9]{6}\.tar" 找到的 tar 存档**。(OCPBUGS-58341)

- 在此次更新之前，构建控制器会搜索链接用于常规使用的 secret，而不是专门用于镜像拉取。在这个版本中，当控制器搜索默认镜像 pull secret 时，构建会使用链接到服务帐户的 **ImagePullSecrets**。(OCPBUGS-57951)

- 在此次更新之前，组合规格和状态更新列表会触发不必要的固件升级，从而导致系统停机。在这个版本中，当添加 Baseboard Management Controller (BMC) URL 时，固件升级优化会跳过不必要的固件升级。(OCPBUGS-56765)

- 在此次更新之前，当您在 **oc-mirror v2** 的 **imageSetConfiguration** 参数中定义 **blockedImages** 值时，您需要提供大量镜像引用列表来从镜像中排除。此要求有时会阻止镜像排除镜像，因为镜像摘要在执行之间有所变化。在这个版本中，您可以将正则表达式用于 **blockedImages** 值，以方便从镜像中排除镜像。(OCPBUGS-56728)

- 在此次更新之前，**Observe > Metrics > query > QueryKebab > Export as csv**drop 项没有处理未定义的 title 元素。因此，您无法在 OpenShift Container Platform Lister 版本 4.16、4.17 和 4.18 的 **Metrics** 选项卡中导出 CSV 文件以获取某些查询。在这个版本中，所有查询的指标下载可以正确地处理下拉菜单中的对象属性。因此，所有查询的 CSV 导出可在 **Metrics** 页面中正常工作。(OCPBUGS-52592)

1.9.5.2. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.6. RHSA-2025:10771 - OpenShift Container Platform 4.19.4 镜像发行版本、程序错误修正和安全更新公告

发布日期：2025 年 7 月 15 日

OpenShift Container Platform 版本 4.19.4 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-2025:10771 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:10772 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.4 --pullspecs
```

1.9.6.1. 程序错误修复

- 在以前的版本中，当启用 Gateway API 功能时，它会安装一个带有一个 pod 副本和关联的 **PodDisruptionBudget** 设置的 Istio control plane。 **PodDisruptionBudget** 设置阻止唯一的 pod 副本被驱除，阻止集群升级。在这个版本中，Ingress Operator 会阻止 Istio control plane 配置允许集群升级的 **PodDisruptionBudget** 设置。(OCPBUGS-58394)

- 在以前的版本中，当使用表单视图点 **Edit HorizontalPodAutoscaler** 时，会出现运行时错误。在这个版本中，**Edit HorizontalPodAutoscaler** 表单视图会如预期显示。(OCPBUGS-58377)

- 在以前的版本中，**console.tab/horizontalNav href** 值中允许使用正斜杠。从 4.15 版本开始存在一个回归的问题，导致在 **href** 值中使用正斜杠无法正常工作。在这个版本中，**console.tab/horizontalNav href** 值中的正斜杠可以按预期正常工作。(OCPBUGS-58375)

- 在以前的版本中，当托管集群使用代理 URL （如 **http://user:pass@host** ）配置时，身份验证标头不会被 Konnectivity 代理转发到用户代理，从而导致身份验证失败。在这个版本中，当在代理 URL 中指定用户和密码时，会发送正确的身份验证标头。(OCPBUGS-58335)

- 在以前的版本中，控制台后端中的端点子集由 **TokenReview** 请求决定到 API 服务器。在某些情况下，API 服务器会限制这些请求，从而导致 UI 中的负载时间较慢。在这个版本中，**TokenReview** gating 已从我们的除一个以外的所有端点中删除，从而提高了性能。(OCPBUGS-58316)

- 在以前的版本中，oc-mirror 插件 v2 将多个请求发送到容器 registry 的请求会导致容器 registry 拒绝一些请求，并带有 **too many requests** 错误。在这个版本中，对几个相关参数的默认值进行了调整，以减少发送到容器 registry 的请求。(OCPBUGS-58279)

- 在以前的版本中，kubelet 服务器证书在证书轮转后不会更新，因为未授权访问 API 服务器会导致集群以不健康状态启动。在这个版本中，kubelet 服务器证书会在证书轮转后更新，以确保健康的集群状态。(OCPBUGS-58116)

- 在以前的版本中，当内部安装程序置备的基础架构部署使用 Cilium 容器网络接口(CNI)时，将流量重定向到负载均衡器的防火墙规则无效。在这个版本中，该规则可用于 Cilium CNI 和 **OVNKubernetes**。(OCPBUGS-57781)

- 在以前的版本中，使用 **-dry-run=server** 选项删除 **istag** 资源会意外导致从服务器中删除镜像的实际。这是因为 **oc delete istag** 命令中错误地实施了 dry-run 选项造成的意外删除。在这个版本中，dry-run 选项与 **oc delete istag** 命令相关联，可以防止意外删除镜像对象，在使用 **--dry-run=server** 选项时，istag 对象可以保持不变。(OCPBUGS-57206)

- 在以前的版本中，如果该组位于原始服务器创建的不同订阅中，Azure API 的过期版本会阻止为机器集指定 Capacity Reservation Group。在这个版本中，OpenShift Container Platform 使用与此配置兼容的 Azure API 的更新版本。(OCPBUGS-56163)

1.9.6.2. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.7. RHBA-2025:10290 - OpenShift Container Platform 4.19.3 镜像发行版本、程序错误修正和安全更新公告

发布日期： 2025 年 7 月 8 日

OpenShift Container Platform 版本 4.19.3 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHBA-2025:10290 公告中。此更新中包括的 RPM 软件包由 RHSA-2025:10291 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.3 --pullspecs
```

1.9.7.1. 程序错误修复

- 在以前的版本中，当 **oc adm node-image create** 命令失败时，不会生成有用的错误消息。在这个版本中，**oc adm node-image create** 命令会在命令失败时提供错误消息。(OCPBUGS-58077)
- 在以前的版本中，当内部安装程序置备的基础架构部署使用 Cilium 容器网络接口(CNI)时，将流量重定向到负载均衡器的防火墙规则无效。在这个版本中，该规则可用于 Cilium CNI 和 **OVNKubernetes**。(OCPBUGS-57781)
- 在以前的版本中，当您在 **oc-mirror v2** 的 **imageSetConfiguration** 参数中定义 **blockedImages** 值时，您需要提供大量镜像引用列表来从镜像中排除。此要求有时会阻止镜像排除镜像，因为镜像摘要在执行之间有所变化。在这个版本中，您可以将正则表达式用于 **blockedImages** 值，以方便从镜像中排除镜像。(OCPBUGS-56728)
- 在以前的版本中，在 OpenShift Container Platform 节点和 pod 中运行的带有大型数据包的某些流量模式会触发 OpenShift Container Platform 主机发送互联网控制消息协议(ICMP)需要 frag 到另一个 OpenShift Container Platform 主机。这种情形降低了集群中可行的最大传输单元(MTU)。因此，执行 **ip route show cache** 命令会生成缓存的路由，其 MTU 低于物理链接。数据包被丢弃，OpenShift Container Platform 组件会降级，因为主机没有发送带有大型数据包的 pod 到 pod 流量。在这个版本中，NF Tables 规则可防止 OpenShift Container Platform 节点降低其 MTU 以响应具有大型数据包的流量模式。(OCPBUGS-55997)
- 在以前的版本中，您需要将 vSAN 文件更新至 8.0 P05 或更高版本，以便运行 OpenShift Container Platform 4.19 的集群挂载从 VMWare vSAN Files 导出的网络文件系统(NFS)卷。在这个版本中，您不需要升级现有的 vSAN File Services 版本来挂载 VMWare vSAN File 卷。(OCPBUGS-55978)

1.9.7.2. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.8. RHSA-2025:9750 - OpenShift Container Platform 4.19.2 镜像发行版本、程序错误修正和安全更新公告

发布日期： 2025 年 7 月 1 日

OpenShift Container Platform 版本 4.19.2 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:9750 公告中。此更新中包括的 RPM 软件包由 RHSA-2025:9751 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.2 --pullspecs
```

1.9.8.1. 程序错误修复

- 在以前的版本中，安装程序只检查安装配置中的第一个计算机器池条目，以确定是否禁用 Machine Config Operator (MCO)引导镜像管理功能。如果指定了多个计算池（Amazon Web Services (AWS)边缘节点，但另一个计算机器池具有自定义 Amazon Machine Image (AMI)，则安装程序不会禁用 MCO 引导镜像管理，而自定义 AMI 会被 MCO 覆盖。在这个版本中，安装程序会检查所有计算机器池条目，并在找到自定义镜像时禁用 MCO 引导镜像管理。(OCPBUGS-58060)

- 在以前的版本中，如果用户为 Amazon Web Services (AWS)或 Google Cloud Platform (GCP)指定自定义引导镜像，Machine Config Operator (MCO)会在安装过程中使用默认引导镜像覆盖它。在这个版本中，为 MCO 配置添加了一个清单生成，在指定自定义镜像时在安装过程中禁用默认引导镜像。(OCPBUGS-57796)

- 在以前的版本中，**oc-mirror** 插件中的一个验证问题会导致命令拒绝 **file://.** 引用。尝试使用 **file://.** 的用户收到一个错误消息 **content filepath is tainted**。在这个版本中，**oc-mirror** 插件可以正确地验证 '.' 目录引用。(OCPBUGS-57786)

- 在以前的版本中，**oc-mirror v2** 命令在其操作过程中没有使用正确的过滤的目录，这会导致错误，如比配置中指定的更多 Operator，并在 disk-to-mirror 工作流过程中尝试连接到目录 registry。在这个版本中，使用正确的过滤的目录。(OCPBUGS-57784)

- 在以前的版本中，当打开 **Create Project** 模态或触发 Networking 页中的模态时，Red Hat OpenShift Lightspeed UI 会消失。这是因为使用 **useModal** hook 的模态导致模态相互覆盖。在这个版本中，模态不再相互覆盖，允许同时显示多个 UI 元素。(OCPBUGS-57755)

- 在以前的版本中，HAProxy 配置使用 **/version** 端点进行健康检查，从而导致生成不可靠的健康检查。在这个版本中，存活度探测已被自定义，在 IBM Cloud 上使用 **/livez?exclude=etcd&exclude=log** 以获得更准确的健康检查，以避免因为 Hypershift 上的不当探测配置而保留 **/version**。(OCPBUGS-57485)

- 在以前的版本中，当找不到 AWS 凭证且调查正在尝试 AWS 区域时，安装程序会失败，阻止用户创建 **install-config** 文件。在这个版本中，当未设置 AWS 凭证时，安装程序不再会失败，允许用户在调查过程中输入它们。(OCPBUGS-57394)

- 在以前的版本中，在 web 控制台中克隆持久性卷声明(PVC)会因为不支持的存储大小的单元 **B** 造成错误。因此，因为对存储大小单元的解析不正确，用户在克隆 Red Hat OpenShift 控制台 PVC 时遇到错误。在这个版本中，从 Red Hat OpenShift 控制台 PVC 中删除了对 **B** 作为存储大小的单元的支持。(OCPBUGS-57391)

- 在以前的版本中，Operator Lifecycle Manager (OLM) v1 用于安装 **olm.maxOpenShiftVersion** 设置为 **4.19** 的 Operator。由于 OLM v1 解析浮动点格式 **olm.maxOpenShiftVersion'values 的逻辑有问题，系统无法防止升级到 OpenShift Container Platform。在这个版本中，当安装有 olm.maxOpenShiftVersion:4.19 的 Operator 时，对 'olm.maxOpenShiftOpenShiftVersion** 的解析逻辑已被修正。(OCPBUGS-56852)

- 在以前的版本中，因为缺少权限，一个 **keepalived** 健康检查脚本会失败。这可能会导致在使用共享入口服务的环境中错误地分配入口虚拟 IP 地址(VIP)。在这个版本中，必要的权限被添加到容器中，因此健康检查现在可以正常工作。(OCPBUGS-56623)

1.9.8.2. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.9. RHSA-2025:9278 - OpenShift Container Platform 4.19.1 镜像发行版本、程序错误修正和安全更新公告

发布日期： 2025 年 6 月 24 日

OpenShift Container Platform 版本 4.19.1 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-2025:9278 公告中。此更新中包括的 RPM 软件包由 RHSA-2025:9279 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.1 --pullspecs
```

1.9.9.1. 程序错误修复

- 在以前的版本中，当您为 Assisted Installer 安装后添加 vCenter 云凭证时，会触发一个程序错误，因为云供应商配置的 **ConfigMap** 对象存在无效的 ConfigMap 对象。因此，会显示 **missing vcenterplaceholder** 错误。在这个版本中，**ConfigMap** 数据是正确的，且不会显示错误。(OCPBUGS-57384)

- 在以前的版本中，在集群中的 API 调用过程中出现网络问题会导致 Operator Lifecycle Manager (OLM)经典中的超时。因此，因为超时问题，Operator 安装会失败。在这个版本中，目录缓存刷新间隔已被更新，以解决超时问题。因此，Operator 安装超时的可能性会减少。(OCPBUGS-57352)

- 在以前的版本中，Operator Lifecycle Manager (OLM)经典中的 Operator 组协调会因为聚合规则选择器的顺序而触发不必要的 **ClusterRole** 更新。因此，会发生不必要的 API 服务器写入。在这个版本中，一个程序错误修复可确保聚合规则中的 **ClusterRoleSelectors** 数组确定顺序，从而减少不必要的 API 服务器写入并改进了集群稳定性。(OCPBUGS-57279)

- 在以前的版本中，忽略 assisted-service 的安装配置中的 **AdditionalTrustBundlePolicy** 设置会导致联邦信息处理标准(FIPS)和其他安装配置覆盖。在这个版本中，安装配置包含一个 **AdditionalTrustBundlePolicy** 字段，您可以设置它来确保 FIPS 和其他安装配置覆盖功能可以正常工作。(OCPBUGS-57208)

- 在以前的版本中，**/metrics** 端点的身份验证过程缺少令牌检查，并导致未授权请求。因此，OpenShift Container Platform 控制台容易出现 **TargetDown** 警报。在这个版本中，对未授权请求的令牌检查发生在请求上下文中的用户令牌。因此，对 OpenShift Container Platform 控制台的未授权请求不会导致 **TargetDown** 警报。(OCPBUGS-57180)

- 在以前的版本中，当屏幕缩小时，**Started** 列会被隐藏。因此，**VirtualizedTable** 组件会因为缺少排序功能而出现故障，表排序功能会在 **PipelineRun** 列表页面中受到影响。在这个版本中，表组件会正确地处理缺少的排序功能，以降低屏幕大小。(OCPBUGS-57110)

- 在以前的版本中，如果您为主题配置了 masthead 徽标，但对主题的其余部分使用默认设置，用户界面中显示的徽标不一致。在这个版本中，masthead 徽标显示 light 和 dark 主题的默认选项，改进了接口一致性。(OCPBUGS-57054)

- 在以前的版本中，因为 Network Load Balancer (NLB)的无效安全组配置，集群安装会失败。此失败会阻止两个主子网的流量用于 bootstrap。在这个版本中，安全组允许引导的主要子网的流量，并且集群安装不会因为其他主子网上的安全组限制而失败。(OCPBUGS-57039)

- 在以前的版本中，没有项目访问权限的用户会在 **Roles** 页面中看到一个不完整的角色列表，因为 API 组访问权限不正确。在这个版本中，没有项目访问权限的用户无法在 **Roles** 页面中看到不完整的角色列表。(OCPBUGS-56987)

- 在以前的版本中，**node-image create** 命令修改目录权限，并导致用户主目录在操作过程中丢失原始权限。在这个版本中，**node-image create** 命令在使用 **rsync** 工具在文件复制过程中保留文件权限，并确保用户目录在操作过程中保留原始权限。(OCPBUGS-56905)

- 在以前的版本中，**ImageSetConfiguration** 文件中允许镜像名称中的 **delete** 关键字，该文件不被支持。因此，用户在镜像时遇到错误。在这个版本中，在 **ImageSetConfiguration** 文件中以 **delete** 结尾的镜像名称的错误已被删除。现在，用户可以成功镜像名称以 **delete** 结尾的镜像。(OCPBUGS-56798)

- 在以前的版本中，**Observe Alerting** 字段中的用户界面显示信息警报的错误警报严重性图标。在这个版本中，**Observe Alerting** 字段中的警报严重性图标匹配。因此，警报图标一致，减少了用户的潜在混淆。(OCPBUGS-56470)

- 在以前的版本中，如果您在 **oc-mirror** 命令中使用了未授权的访问配置文件，则同步镜像集时会显示一个 **Unauthorized** 错误。在这个版本中，Docker 配置被更新为使用自定义授权文件进行身份验证。您可以在不遇到 **Unauthorized** 错误的情况下成功同步您的镜像集。(OCPBUGS-55701)

1.9.9.2. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.10. RHSA-2024:11038 - OpenShift Container Platform 4.19.0 镜像发行版本、程序错误修正和安全更新公告

发布日期：2025 年 6 月 17 日

OpenShift Container Platform 版本 4.19.0 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-2024:11038 公告中。此更新中包括的 RPM 软件包由 RHEA-2025:2851 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.19.0 --pullspecs
```

1.9.10.1. 更新

要将 OpenShift Container Platform 4.19 集群更新至此最新版本，请参阅使用 CLI 更新集群。

第 2 章 其他发行注记

没有包括在核心的 OpenShift Container Platform 4.19 发行注记 中的额外的相关组件和产品的发行注记包括在以下文档中。

重要

以下发行注记仅用于下游红帽产品；不包括相关产品的上游或社区发行注记。

A

AWS Load Balancer Operator

B

为 Red Hat OpenShift 构建

C

cert-manager Operator for Red Hat OpenShift

Cluster Observability Operator (COO)

Compliance Operator

Custom Metrics Autoscaler Operator

D

Red Hat Developer Hub Operator

E

外部 DNS Operator

F

File Integrity Operator

H

托管 control plane

K

kube Descheduler Operator

M

Migration Toolkit for Containers (MTC)

N

Network Observability Operator

Network-bound Disk Encryption (NBDE) Tang Server Operator

O

OpenShift API for Data Protection (OADP)

Red Hat OpenShift Dev Spaces

Red Hat OpenShift Distributed Tracing Platform

Red Hat OpenShift GitOps Red Hat OpenShift Local (Upstream CRC 文档)

Red Hat OpenShift Pipelines

OpenShift沙盒容器

Red Hat OpenShift Serverless
HEKETIRed Hat OpenShift Service Mesh 2.x Red Hat OpenShift Service Mesh 3.xHEKETIRedHatOpenShift support for Windows Containers

P

Power monitoring for Red Hat OpenShift

R

Run Once Duration Override Operator

S

Secondary Scheduler Operator for Red Hat OpenShift

Security Profiles Operator