OpenShift Container Platform 4.12

发行注记

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

Last Updated: 2023-03-18

OpenShift Container Platform 4.12 发行注记

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

法律通告

摘要

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

目录

第 1 章 OPENSHIFT CONTAINER PLATFORM 4.12 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-2022:7399) 现已正式发布。此发行版本使用了带有 CRI-O 运行时的 Kubernetes 1.25 。OpenShift Container Platform 4.12 的新功能、改变以及已知的问题包括在此文档中。

OpenShift Container Platform 4.12 集群位于 https://console.redhat.com/openshift。使用 OpenShift Container Platform 的 Red Hat OpenShift Cluster Manager 应用程序，您可以将 OpenShift 集群部署到内部环境或云环境中。

OpenShift Container Platform 4.12 需要运行在 Red Hat Enterprise Linux (RHEL) 8.6 和 Red Hat Enterprise Linux CoreOS 4.12 上。

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

从 OpenShift Container Platform 4.12 开始，对于发现版本号为偶数的版本提供了一个额外 6 个月的延长更新支持 (EUS) 阶段，使其从 18 个月延长到两年。如需更新相关信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策。

OpenShift Container Platform 4.8 是一个延长更新支持（EUS）发行版本。如需了解更多与 Red Hat OpenShift EUS 相关的信息，请参阅 OpenShift 生命周期和 OpenShift EUS 概述。

版本 4.8 的维护支持于 2023 年 1 月结束，并进入到延长生命周期阶段。如需更新相关信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策。

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

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

1.3. 新功能及功能增强

此版本对以下方面进行了改进。

1.3.1. Red Hat Enterprise Linux CoreOS (RHCOS)

1.3.1.1. 新集群的默认控制台现在由安装平台决定

从 OpenShift Container Platform 4.12 引导镜像安装的 Red Hat Enterprise Linux CoreOS (RHCOS) 节点现在使用特定于平台的默认控制台。云平台上的默认控制台对应于该云供应商期望的特定系统控制台。VMware 和 OpenStack 镜像现在使用一个主图形控制台和一个从串行控制台。其他裸机安装现在默认只

使用图形控制台，且不启用串行控制台。使用 **coreos-installer** 进行的安装可能会覆盖现有的默认值并启用串行控制台。

现有节点不受影响。现有集群上的新节点应该不会受到影响，因为它们通常从最初用来安装集群的引导镜像安装。

有关如何启用串行控制台的详情，请查看以下文档：

- 默认控制台配置.
- 修改实时安装 ISO 镜像以启用串行控制台。
- 修改实时安装 PXE 环境以启用串行控制台。

1.3.1.2. IBM zSystems 和 LinuxONE 上的 IBM Secure Execution （技术预览）

OpenShift Container Platform 现在支持为 IBM zSystems 和 LinuxONE (s390x 架构)上的 IBM Secure Execution 配置 Red Hat Enterprise Linux CoreOS (RHCOS) 节点作为技术预览功能。IBM Secure Execution 是一种硬件增强，可为 KVM 客户机保护内存边界。IBM Secure Execution 为集群工作负载提供最高级别的隔离和安全，您可以使用支持 IBM Secure Execution 的 QCOW2 引导镜像启用它。

要使用 IBM Secure Execution，您需要有主机机器的主机密钥，且必须在 Ignition 配置文件中指定它们。IBM Secure Execution 会使用 LUKS 加密自动加密引导卷。

如需更多信息，请参阅使用 IBM Secure Execution 安装 RHCOS 。

1.3.1.3. RHCOS 现在使用 RHEL 8.6

RHCOS 现在在 OpenShift Container Platform 4.12 中使用 Red Hat Enterprise Linux (RHEL) 8.6 软件包。这可让您获得最新的修复、功能和增强，以及最新的硬件支持和驱动程序更新。OpenShift Container Platform 4.10 是一个延长更新支持（EUS）版本，其整个生命周期中将继续使用 RHEL 8.4 EUS 软件包。

1.3.2. 安装和升级

1.3.2.1. 在安装过程中指定 AWS 中的负载均衡器类型

从 OpenShift Container Platform 4.12 开始，您可以在安装过程中将 Network Load Balancer (NLB) 或 Classic 指定为持久负载均衡器类型。之后，如果删除了 Ingress Controller，负载均衡器类型会在安装过程中保留配置的 lbType。

如需更多信息，请参阅使用网络自定义在 AWS 上安装集群。

1.3.2.2. 当安装到一个带有 Local Zone 子网的现有 Virtual Private Cloud (VPC) 中时，将 worker 节点扩展到 AWS 边缘。

在这个版本中，您可以将 OpenShift Container Platform 安装到带有安装程序置备的基础架构的现有 VPC 中，将 worker 节点扩展到 Local Zones 子网。安装程序将在 AWS 网络的边缘上置备 worker 节点，该网络使用 NoSchedule 污点为用户应用程序指定。在本地区位置部署的应用程序为最终用户提供低延迟。

如需更多信息，请参阅使用 AWS 本地区安装集群。

1.3.2.3. Google Cloud Platform Marketplace 产品

OpenShift Container Platform 现在包括在 GCP Marketplace 中。使用 GCP Marketplace 镜像安装 OpenShift Container Platform 可让您创建由 GCP 按使用付费（按小时、每个内核）的自我管理的集群部署，同时仍然被红帽直接支持。

有关使用安装程序置备的基础架构安装的更多信息，请参阅使用 GCP Marketplace 镜像。有关使用用户置备的基础架构的更多信息，请参阅在 GCP 中创建额外的 worker 机器。

1.3.2.4. 在 GCP 和 Azure 上的安装过程中对 bootstrap 进行故障排除会失败

安装程序现在从 GCP 和 Azure 上的 bootstrap 和 control plane 主机收集串口控制台日志。此日志数据被添加到标准 bootstrap 日志捆绑包中。

如需更多信息，请参阅故障排除安装问题。

1.3.2.5. IBM Cloud VPC 正式发布

IBM Cloud VPC 现在包括在 OpenShift Container Platform 4.12 中。

有关安装集群的更多信息，请参阅准备在 IBM Cloud VPC 上安装。

1.3.2.6. 从 OpenShift Container Platform 4.11 升级到 4.12 时，需要管理员确认

OpenShift Container Platform 4.12 使用 Kubernetes 1.25，它删除了几个已弃用的 API。

集群管理员必须在从 OpenShift Container Platform 4.11 升级到 4.12 前提供手动确认。这有助于防止升级到 OpenShift Container Platform 4.12 后出现问题，其中已删除的 API 仍在由运行或与集群交互的工作负载、工具或其他组件使用。管理员必须针对将要删除的任何 API 评估其集群，并迁移受影响的组件，以使用适当的新 API 版本。完成此操作后，管理员可以向管理员提供确认。

所有 OpenShift Container Platform 4.11 集群都需要此管理员确认，然后才能升级到 OpenShift Container Platform 4.12。

如需更多信息，请参阅准备升级到 OpenShift Container Platform 4.12。

1.3.2.7. 在安装集群时启用功能集

从 OpenShift Container Platform 4.12 开始，您可以在安装过程中启用功能集。功能集是 OpenShift Container Platform 功能的集合，默认情况下不启用。

有关在安装过程中启用功能集的更多信息，请参阅使用功能门启用 OpenShift Container Platform 功能。

1.3.2.8. OpenShift Container Platform on ARM

OpenShift Container Platform 4.12 现在支持基于 ARM 架构的 Azure 安装程序置备的基础架构。AWS Graviton 3 处理器现在可用于集群部署，在 OpenShift Container Platform 4.11 中也支持。有关实例可用性和安装文档的更多信息，请参阅支持的安装方法

1.3.2.9. 使用 oc-mirror CLI 插件，以 OCI 格式镜像基于文件的目录 Operator 镜像（技术预览）

使用 oc-mirror CLI 插件以 OCI 格式而不是 Docker v2 格式镜像基于文件的目录 Operator 镜像，现在作为技术预览提供。

如需更多信息，请参阅以 OCI 格式镜像基于文件的目录 Operator 镜像。

1.3.2.10. 在 GCP 上安装 OpenShift Container Platform 集群到共享 VPC 中（技术预览）

在 OpenShift Container Platform 4.12 中，您可以在 GCP 上将集群安装到共享 VPC 中作为技术预览。在这个安装方法中，集群被配置为使用来自不同 GCP 项目的 VPC。共享 VPC 可让组织将资源从多个项目连接到一个通用 VPC 网络。您可以使用来自该网络的内部 IP 地址，在组织内安全、高效地通信。

如需更多信息，请参阅在 GCP 上安装集群到共享 VPC 中。

1.3.2.11. 在没有置备（provisioning）网络的情况下，裸机安装中 Ironic API 的一致性 IP 地址

在这个版本中，在没有 provisioning 网络的裸机安装中，Ironic API 服务可以通过代理服务器访问。此代理服务器为 Ironic API 服务提供一致的 IP 地址。如果包含 **metal3-ironic** 的 Metal3 pod 被重新定位到另一个 pod，一致的代理地址可确保与 Ironic API 服务持续通信。

1.3.2.12. 使用服务帐户身份验证在 GCP 上安装 OpenShift Container Platform

在 OpenShift Container Platform 4.12 中，您可以使用附加了服务帐户的虚拟机在 GCP 上安装集群。这可让您执行安装，而无需使用服务帐户 JSON 文件。

如需更多信息，请参阅创建 GCP 服务帐户。

1.3.2.13. OpenShift Container Platform 集群置备的 AWS 资源的 propagateUserTags 参数

在 OpenShift Container Platform 4.12 中，**propagateUserTags** 参数是一个标记，它指示 in-cluster Operator 在 Operator 创建的 AWS 资源标签中包含指定的用户标签。

如需更多信息，请参阅可选配置参数。

1.3.2.14. Ironic 容器镜像使用 RHEL 9 基础镜像

在早期版本的 OpenShift Container Platform 中，Ironic 容器镜像使用 Red Hat Enterprise Linux (RHEL) 8 作为基础镜像。在 OpenShift Container Platform 4.12 中，Ironic 容器镜像使用 RHEL 9 作为基础镜像。RHEL 9 基础镜像添加了对 CentOS Stream 9、Python 3.8 和 Python 3.9 的支持。

有关 Ironic 置备服务的更多信息，请参阅在裸机上部署安装程序置备的集群。

1.3.2.15. 在 RHOSP 上运行的集群的云供应商配置更新

在 OpenShift Container Platform 4.12 中，在 Red Hat OpenStack Platform (RHOSP) 上运行的集群从旧的 OpenStack 云供应商切换到外部 Cloud Controller Manager (CCM)。此更改遵循 Kubernetes 的变化，它从 in-tree（传统的云供应商）变为使用 Cloud Controller Manager 实施的外部云供应商。

如需更多信息，请参阅 OpenStack Cloud Controller Manager。

1.3.2.16. 支持 RHOSP 分布式计算节点上的工作负载

在 OpenShift Container Platform 4.12 中，验证到有分布式计算节点 (DCN) 架构的 Red Hat OpenStack Platform (RHOSP) 云的集群部署。这些部署的参考架构是即将推出的。

有关这类部署的简要概述，请参阅使用 OpenStack 部署集群的博客文章。

1.3.2.17. AWS Outposts 上的 OpenShift Container Platform （技术预览）

OpenShift Container Platform 4.12 现在作为技术预览在 AWS Outposts 平台上被支持。使用 AWS Outposts，您可以部署基于边缘的 worker 节点，同时将 AWS 区域用于 control plane 节点。如需更多信息，请参阅在 AWS Outposts 上使用远程 worker 在 AWS 上安装集群 。

1.3.2.18. 基于代理的安装支持两种输入模式

基于代理的安装支持两种输入模式：

- **install-config.yaml** file
- **agent-config.yaml** file

可选

- Zero Touch Provisioning (ZTP) 清单

使用首选模式，您可以配置 **install-config.yaml** 文件，并在 **agent-config.yaml** 文件中指定基于 Agent 的特定设置。如需更多信息，请参阅关于基于代理的 OpenShift Container Platform 安装程序。

1.3.2.19. 基于代理的安装支持以 FIPS 兼容模式安装 OpenShift Container Platform 集群

基于代理的 OpenShift Container Platform 安装程序支持联邦信息处理标准 (FIPS) 兼容模式的 OpenShift Container Platform 集群。您必须在 **install-config.yaml** 文件中将 **fips** 字段的值设置为 **True**。如需更多信息，请参阅关于 FIPS 合规性。

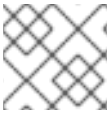
1.3.2.20. 在断开连接的环境中部署基于代理的 OpenShift Container Platform 集群

您可以在断开连接的环境中执行基于代理的安装。要创建在断开连接的环境中使用的镜像，**install-config.yaml** 文件中的 **imageContentSources** 部分必须包含镜像信息或 **registry.conf** 文件（如果使用 ZTP 清单）。这些文件中使用的实际配置设置由 **oc adm release mirror** 或 **oc mirror** 命令提供。如需更多信息，请参阅了解断开连接的安装镜像。

1.3.2.21. 基于代理的安装支持单堆栈和双栈网络

您可以使用以下 IP 地址配置创建代理 ISO 镜像：

- IPv4
- IPv6
- IPv4 和 IPv6 并行 (dual-stack)



注意

IPv6 仅在裸机平台上被支持。

如需更多信息，请参阅 双和单 IP 堆栈集群。

1.3.2.22. 部署的 OpenShift Container Platform 集群的代理可用作 hub 集群

您可以为 Kubernetes Operator 安装多集群引擎，并使用基于 Agent 的 OpenShift Container Platform 安装程序部署 hub 集群。如需更多信息，请参阅为 Kubernetes Operator 的多集群引擎准备基于 Agent 的集群。

1.3.2.23. 基于代理的安装执行安装验证

基于代理的 OpenShift Container Platform 安装程序在其上执行验证：

- 安装镜像生成 ：检查用户提供的清单以获取有效性和兼容性。
- 安装：安装服务检查可用于安装的硬件，并发出可通过 **openshift-install agent wait-for** 子命令检索的验证事件。

如需更多信息，请参阅安装验证。

1.3.2.24. 在基于代理的安装中配置静态网络

使用基于代理的 OpenShift Container Platform 安装程序，您可以在创建代理 ISO 镜像之前为 IPv4、IPv6 或双栈 (IPv4 和 IPv6) 配置静态 IP 地址。如果您使用 ZTP 清单，您可以将静态地址添加到 **agent-config.yaml** 文件的 **hosts** 部分，或者在 **NMStateConfig.yaml** 文件中。请注意，地址的配置必须遵循 NMState 的语法规则，如 NMState 状态示例中所述。

注意

IPv6 仅在裸机平台上被支持。

如需更多信息，请参阅关于网络。

1.3.2.25. 基于代理的安装中的基于 CLI 的自动化部署

通过基于代理的 OpenShift Container Platform 安装程序，您可以定义安装配置，为所有节点生成 ISO，然后通过使用生成的 ISO 引导目标系统来进行无人值守安装。如需更多信息，请参阅使用基于代理的 OpenShift Container Platform 安装程序安装 OpenShift Container Platform 集群。

1.3.2.26. 基于代理的安装支持在 instalation 时进行特定于主机的配置

您可以在基于 Agent 的安装中以 NMState 格式、根设备提示和角色配置主机名、网络配置。

如需更多信息，请参阅关于 root 设备提示。

1.3.2.27. 基于代理的安装支持 DHCP

使用基于代理的 OpenShift Container Platform 安装程序，您可以部署到依赖 DHCP 的环境，以便为所有节点配置网络，只要您知道至少一个系统将收到的 IP。这个 IP 是必需的，以便所有节点都将其作为一个交互的点。如需更多信息，请参阅 DHCP。

1.3.3. 安装后配置

1.3.3.1. vSphere 集群上的 CSI 驱动程序安装

要在 vSphere 上运行的集群中安装 CSI 驱动程序，必须满足以下要求：

- 硬件版本 15 或更高版本的虚拟机
- 不支持 VMware vSphere 版本 7.0 更新 2 或更高版本，但不包括版本 8。
- 不支持 vCenter 7.0 更新 2 或更高版本，但不包括版本 8. vCenter 8。
- 集群中还没有安装第三方 CSI 驱动程序
  如果集群中存在第三方 CSI 驱动程序，OpenShift Container Platform 不会覆盖它。

虽然低于上述版本的组件仍被支持，但已被弃用。这些版本仍被完全支持，但 OpenShift Container Platform 版本 4.12 需要 vSphere 虚拟硬件版本 15 或更高版本。如需更多信息，请参阅已弃用和删除的功能。

如果无法满足上述要求，则会阻止 OpenShift Container Platform 升级到 OpenShift Container Platform 4.13 或更高版本。

1.3.3.2. 集群功能

添加了以下新集群功能：

- 控制台（Console）
- Insights
- 存储
- CSISnapshot

添加了一组新的预定义集群功能 **v4.12**。这包括 **v4.11** 的所有功能，以及当前发行版本中添加的新功能。

如需更多信息，请参阅链接 ：启用集群功能。

1.3.3.3. 带有多架构计算机器的 OpenShift Container Platform （技术预览）

带有多架构计算机器的 OpenShift Container Platform 4.12 现在支持镜像流中列出的清单镜像。如需有关清单列表镜像的更多信息，请参阅在 OpenShift Container Platform 集群上配置多架构计算机器 。

在带有多架构计算机器的集群中，您现在可以覆盖 Operator 的 **Subscription** 对象中的节点关联性，以将 pod 调度到 Operator 支持的架构的节点上。如需更多信息，请参阅使用节点关联性来控制安装 Operator 的位置。

1.3.4. Web 控制台

1.3.4.1. 管理员视角

在这个版本中，web 控制台的 **Administrator** 视角有几个更新。

- 如果集群正在升级，OpenShift Container Platform Web 控制台会显示一个 **ConsoleNotification**。升级完成后，会删除通知。
- Action 和 Kebab 菜单中提供了 **Deployment** 资源的 ***restart rollout*** 选项，以及 **DeploymentConfig** 资源的 ***retry rollouts*** 选项。
- 您可以在 **All Clusters** 下拉列表中查看支持的集群列表。支持的集群包括 OpenShift Container Platform、OpenShift Container Platform Service on AWS (ROSA)、Azure Red Hat OpenShift (ARO)、ROKS 和 Red Hat OpenShift Dedicated。

1.3.4.1.1. OpenShift Container Platform web 控制台中的多架构计算机器

console-operator 现在扫描所有节点并构建一组集群节点运行的所有架构类型，并将其传递给 **console-config.yaml**。**console-operator** 可以在带有值 **amd64**、**arm64**、**ppc64le** 或 **s390x** 的架构中安装。

如需有关多架构计算机器的更多信息，请参阅在 OpenShift 集群上配置多架构计算机器。

1.3.4.1.2. 动态插件正式发布

此功能以前作为技术预览功能在 OpenShift Container Platform 4.10 中引入，现在在 OpenShift Container Platform 4.12 中正式发布。使用动态插件，您可以在 web 控制台中原生构建高质量和唯一的用户体验。您可以：

- 添加自定义页面。
- 增加了除管理员和开发人员之外的其他视角。
- 添加导航项。
- 在资源页面中添加制表符和操作。
- 扩展现有页面。

如需更多信息，请参阅动态插件概述。

1.3.4.2. Developer Perspective (开发者视角)

在这个版本中，web 控制台的 **Developer** 视角有几个更新。您可以执行以下操作：

- 使用 **+Add** 页面中的 **Export application** 选项，以 ZIP 文件格式将应用程序导出到另一个项目或集群。
- 创建 Kafka 事件 sink 从特定源接收事件并将其发送到 Kafka 主题。
- 在 **User Preferences → Applications** 页面中设置默认资源首选项。另外，您可以选择另一个资源类型作为默认值。
  - 另外，还可点 **Add** 页面中的 **Import from Git → Advanced options → Resource type** 并从下拉列表中选择资源。
- 在 **Pod** 页面的 **Details** 选项卡中，设置 pod 的 **status.HostIP** 节点 IP 地址。
- 当任何资源达到配额时，请参阅 **Topology** 和 **Add** 页面中的资源配额警报标签。警报标签链接将您带到 **ResourceQuotas** 列表页面。如果警报标签链接用于单个资源配额，它会进入 **ResourceQuota** 详情页面。
  - 对于部署，如果有与资源配额相关的任何错误，则拓扑节点侧面板中会显示一个警报。另外，超过资源配额时，部署节点会显示一个黄色边框。
- 使用表单或 YAML 视图自定义以下 UI 项：
  - 用户可见的视角
  - 快速开始对用户可见
  - 项目可以访问的集群角色
  - **+Add** 页面中可见的操作
  - **Developer Catalog**中的项目类型
- 通过执行以下操作来查看 **Pipeline details** 和 **PipelineRun details** 页可间性的通用更新：
  - 使用鼠标轮设置缩放。

- 将鼠标悬停在任务上，以查看任务详情。
- 使用标准图标来放大，缩小，适用于屏幕，然后重置视图。
- 仅限 **PipelineRun** 详情页面 ：在特定的缩放条件中，任务更改的背景颜色表示错误或警告状态。您可以将鼠标悬停在图标上，以查看总任务数量和完成的任务数量。

1.3.4.2.1. Helm 页改进

在 OpenShift Container Platform 4.12 中，您可以在 **Helm** 页面中进行以下内容：

- 使用 **Create** 按钮创建 Helm 发行版本和仓库。
- 创建、更新或删除集群范围的 Helm 仓库或命名空间范围 Helm Chart 仓库。
- 在 **Repositories** 页面中，查看现有 Helm Chart 仓库列表及其范围。
- 在 **Helm Releases** 页面中查看新创建的 Helm 发行版本。

1.3.4.2.2. Alertmanager 中的负匹配器

在这个版本中，Alertmanager 支持 **Negative matcher** 选项。使用 **Negative matcher**，您可以将 **Label** 值更新为 Not Equals matcher。负匹配复选框将 **=**（值等于）改为 **!=**（值不等于），将 **=~**（值匹配正则表达式）变为 **!~**（值不匹配正则表达式）。另外，**Use RegEx** 复选框标签被重命名为 **RegEx**。

1.3.5. OpenShift CLI (oc)

1.3.5.1. 使用 Krew 管理 OpenShift CLI 的插件（技术预览）

使用 Krew 为 OpenShift CLI (**oc**) 安装和管理插件现在作为技术预览提供。

如需更多信息，请参阅使用 Krew 管理 CLI 插件。

1.3.6. IBM Z 和 LinuxONE

在这个版本中，IBM Z 和 LinuxONE 与 OpenShift Container Platform 4.12 兼容。可以使用 z/VM 或 RHEL KVM 进行安装。有关安装说明，请参阅以下文档：

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

主要改进
IBM Z 和 LinuxONE 中的 OpenShift Container Platform 4.12 支持以下新功能：

- Cron 作业
- Descheduler
- IPv6
- PodDisruptionBudget

- Scheduler 配置集
- 流控制传输协议 (SCTP)

IBM 安全执行（技术预览）
OpenShift Container Platform 现在支持为 IBM zSystems 和 LinuxONE (s390x 架构)上的 IBM Secure Execution 配置 Red Hat Enterprise Linux CoreOS (RHCOS) 节点作为技术预览功能。

有关安装说明，请参阅以下文档：

- 使用 IBM 安全执行安装 RHCOS

支持的功能
IBM Z 和 LinuxONE 也支持以下功能：

- 目前，支持以下 Operator：
  - Cluster Logging Operator
  - Compliance Operator
  - File Integrity Operator
  - Local Storage Operator
  - NFD Operator
  - NMState Operator
  - OpenShift Elasticsearch Operator
  - Service Binding Operator
  - Vertical Pod Autoscaler Operator
- 支持以下 Multus CNI 插件：
  - Bridge
  - Host-device
  - IPAM
  - IPVLAN
- 备用身份验证供应商
- 使用 Local Storage Operator 自动设备发现
- CSI 卷
  - 克隆
  - 扩展
  - Snapshot
- 加密数据存储在 etcd 中

- Helm
- Pod 横向自动扩展
- 用户定义项目的监控
- 多路径（Multipathing）
- Operator API
- OC CLI 插件
- 使用 iSCSI 的持久性存储
- 使用本地卷的持久性存储（本地存储 Operator）
- 使用 hostPath 的持久性存储
- 使用 Fibre Channel 持久性存储
- 使用 Raw Block 的持久性存储
- OVN-Kubernetes，包括 IPsec 加密
- 支持多个网络接口
- 三节点集群支持
- SCSI 磁盘中的 z/VM 模拟 FBA 设备
- 4K FCP 块设备

以下功能仅适用于 IBM Z 和 4.12 上的 OpenShift Container Platform：

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

限制
以下限制会影响 OpenShift Container Platform 对 IBM Z 和 LinuxONE 的影响：

- 使用机器健康检查功能自动修复损坏的机器
- Red Hat OpenShift Local
- 在节点上控制过量使用和管理容器密度
- NVMe
- OpenShift Metering
- OpenShift Virtualization
- 精度时间协议 (PTP) 硬件
- 在 OpenShift Container Platform 部署过程中启用 Tang 模式磁盘加密
- Compute 节点必须运行 Red Hat Enterprise Linux CoreOS(RHCOS)
- 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

- 必须使用本地存储（如 iSCSI、FC 或者带有 DASD、FCP 或 EDEV/FBA 的 LSO）置备持久性非共享存储

1.3.7. IBM Power

在这个版本中，IBM Power 与 OpenShift Container Platform 4.12 兼容。有关安装说明，请参阅以下文档：

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

主要改进
OpenShift Container Platform 4.12 的 IBM Power 支持以下新功能：

- IBM Cloud 的云控制器管理器
- Cron 作业
- Descheduler
- PodDisruptionBudget
- Scheduler 配置集
- 流控制传输协议 (SCTP)
- 拓扑管理器

支持的功能
IBM Power 还支持以下功能：

- 目前，支持以下 Operator：
  - Cluster Logging Operator
  - Compliance Operator
  - File Integrity Operator
  - Local Storage Operator
  - NFD Operator
  - NMState Operator
  - OpenShift Elasticsearch Operator
  - Cluster Network Operator
  - Service Binding Operator
  - Vertical Pod Autoscaler Operator
- 支持以下 Multus CNI 插件：
  - Bridge

    - Host-device
    - IPAM
    - IPVLAN
- 备用身份验证供应商
- CSI 卷
    - 克隆
    - 扩展
    - Snapshot
- 加密数据存储在 etcd 中
- Helm
- Pod 横向自动扩展
- IPv6
- 用户定义项目的监控
- 多路径（Multipathing）
- Multus SR-IOV
- Operator API
- OC CLI 插件
- OVN-Kubernetes，包括 IPsec 加密
- 使用 iSCSI 的持久性存储
- 使用本地卷的持久性存储（本地存储 Operator）
- 使用 hostPath 的持久性存储
- 使用 Fibre Channel 持久性存储
- 使用 Raw Block 的持久性存储
- 支持多个网络接口
- 支持 Power10
- 三节点集群支持
- 4K 磁盘支持

限制
OpenShift Container Platform 对 IBM Power 的影响如下：

- 使用机器健康检查功能自动修复损坏的机器

- Red Hat OpenShift Local
- 在节点上控制过量使用和管理容器密度
- OpenShift Metering
- OpenShift Virtualization
- 精度时间协议 (PTP) 硬件
- 在 OpenShift Container Platform 部署过程中启用 Tang 模式磁盘加密
- Compute 节点必须运行 Red Hat Enterprise Linux CoreOS(RHCOS)
- 持久性存储必须是使用本地卷、Red Hat OpenShift Data Foundation、网络文件系统(NFS)或 Container Storage Interface(CSI)的 Filesystem 类型

1.3.8. 镜像

新的导入值 **importMode** 已添加到镜像流的 **importPolicy** 参数中。以下字段可用于这个值：

- **Legacy**: **Legacy** 是 **importMode** 的默认值。活跃时，清单列表将被丢弃，并导入单个子清单。平台会按照优先级顺序进行选择：
  1. 标签注解
  2. control plane 架构
  3. Linux/AMD64
  4. 列表中的第一个清单
- **PreserveOriginal** ：当激活时，原始清单将被保留。对于清单列表，将导入清单列表及其所有子清单。

1.3.9. 安全性与合规性

1.3.9.1. Security Profiles Operator

现在，OpenShift Container Platform 4.12 及更新的版本提供了 Security Profiles Operator (SPO)。

SPO 提供了一种将安全计算 (seccomp) 配置集和 SELinux 配置集定义为自定义资源，将配置集同步到给定命名空间中的每个节点。

如需更多信息，请参阅 安全配置集 Operator 概述。

1.3.10. 网络

1.3.10.1. Red Hat OpenShift Networking

Red Hat OpenShift 网络是一个功能、插件和高级网络功能生态系统，其使用 Kubernetes CNI 插件除 Kubernetes CNI 插件之外扩展 Kubernetes 网络，集群需要管理一个或多个混合集群的网络流量。这个网络功能生态系统集成了入口、出口、负载均衡、高性能吞吐量、安全性和集群内部流量管理，并提供基于角色的可观察工具来减少其自然复杂性。

如需更多信息，请参阅关于网络。

1.3.10.2. OVN-Kubernetes 现在是默认的网络插件

安装新集群时，OVN-Kubernetes 网络插件是默认的网络插件。对于所有以前的 OpenShift Container Platform 版本，OpenShift SDN 会保留默认的网络插件。

OVN-Kubernetes 网络插件包含比 OpenShift SDN 更广泛的功能，包括：

- 支持所有现有 OpenShift SDN 功能
- 支持 IPv6 网络
- 支持配置 IPsec 加密
- 对 **NetworkPolicy** API 的完整支持
- 支持 网络策略事件的审计日志记录
- 支持 NetFlow、sFlow 和 IPFIX 格式的网络流跟踪
- 支持 Windows 容器的混合网络
- 支持将硬件卸载到兼容 NIC

与之前的版本相比，OpenShift Container Platform 4.12 在扩展、性能和稳定性方面有大的改进。

如果使用 OpenShift SDN 网络插件，请注意：

- 使用 OpenShift SDN 的现有和将来的部署仍被支持。
- OpenShift SDN 在比 OpenShift Container Platform 4.12 早的版本中保留为默认设置。
- 从 OpenShift Container Platform 4.12 开始，OpenShift SDN 是一个受支持的安装时选项。
- OpenShift SDN 保留功能冻结。

有关 OVN-Kubernetes 的更多信息，包括与 OpenShift SDN 的功能比较列表，请参阅关于 OVN-Kubernetes 网络插件。

有关从 OpenShift SDN 迁移到 OVN-Kubernetes 的详情，请参考从 OpenShift SDN 网络插件迁移。

1.3.10.3. Ingress Node Firewall Operator

在这个版本中，引入了一个新的无状态 Ingress Node Firewall Operator。现在，您可以在节点级别配置防火墙规则。如需更多信息，请参阅 Ingress Node Firewall Operator。

1.3.10.4. 网络指标的改进

以下指标现在可用于 OVN-Kubernetes 网络插件：

- **ovn_controller_southbound_database_connected**
- **ovnkube_master_libovsdb_monitors**
- **ovnkube_master_network_programming_duration_seconds**

- **ovnkube_master_network_programming_ovn_duration_seconds**
- **ovnkube_master_egress_routing_via_host**
- **ovs_vswitchd_interface_resets_total**
- **ovs_vswitchd_interface_rx_dropped_total**
- **ovs_vswitchd_interface_tx_dropped_total**
- **ovs_vswitchd_interface_rx_errors_total**
- **ovs_vswitchd_interface_tx_errors_total**
- **ovs_vswitchd_interface_collisions_total**

删除了以下指标：

- **ovnkube_master_skipped_nbctl_daemon_total**

1.3.10.5. 多区安装程序置备基础架构 VMware vSphere 安装（技术预览）

从 OpenShift Container Platform 4.12 开始，使用安装程序置备的基础架构在单个 vCenter 安装中配置多个 vCenter 数据中心和多个 vCenter 集群的功能现在作为技术预览提供。使用 vCenter 标签，您可以使用此功能将 vCenter 数据中心和计算集群与 openshift-regions 和 openshift-zones 关联。这些关联定义故障域，使应用程序工作负载与特定位置和故障域相关联。

1.3.10.6. 现在支持 VMware vSphere 中的 Kubernetes NMState

从 OpenShift Container Platform 4.12 开始，您可以使用 VMware vSphere 上的 Kubernetes NMState Operator 配置网络设置，如 DNS 服务器或搜索域、VLAN、桥接和接口绑定。

如需更多信息，请参阅关于 Kubernetes NMState Operator。

1.3.10.7. 现在支持 OpenStack 中的 Kubernetes NMState

从 OpenShift Container Platform 4.12 开始，您可以使用 OpenStack 实例上的 Kubernetes NMState Operator 配置网络设置，如 DNS 服务器或搜索域、VLAN、桥接和接口绑定。

如需更多信息，请参阅关于 Kubernetes NMState Operator。

1.3.10.8. 外部 DNS Operator

在 OpenShift Container Platform 4.12 中，External DNS Operator 修改了 AzureDNS 上 ExternalDNS 通配符 TXT 记录的格式。External DNS Operator 使用 ExternalDNS 通配符 TXT 记录中的 **any** 替换了星号。您必须避免 ExternalDNS 通配符 A 和 CNAME 记录具有 **any** 最左边的子域，因为这可能导致冲突。

OpenShift Container Platform 4.12 的 **ExternalDNS** 上游版本为 v0.13.1。

1.3.10.9. 捕获与使用路由和分片关联的指标和遥测

在 OpenShift Container Platform 4.12 中，Cluster Ingress Operator 会导出一个名为 **route_metrics_controller_routes_per_shard** 的新指标。指标的 **shard_name** 标签指定分片的名称。此指标提供每个分片接受的路由总数。

以下指标通过遥测发送。

表 1.1. 通过遥测发送的指标

名称	记录规则表达式	描述
cluster:route_metrics_controller_routes_per_shard:min	**min(route_metrics_controller_routes_per_shard)**	跟踪被任何分片接受的最少路由数量
cluster:route_metrics_controller_routes_per_shard:max	**max(route_metrics_controller_routes_per_shard)**	跟踪被任何分片接受的最大路由数
cluster:route_metrics_controller_routes_per_shard:avg	**avg(route_metrics_controller_routes_per_shard)**	跟踪 **route_metrics_controller_routes_per_shard** 指标的平均值
cluster:route_metrics_controller_routes_per_shard:median	**quantile(0.5, route_metrics_controller_routes_per_shard)**	跟踪 **route_metrics_controller_routes_per_shard** 指标的中位值
cluster:openshift_route_info:tls_termination:sum	通过**(tls_termination)**总结 **(openshift_route_info)**	跟踪每个 **tls_termination** 值的路由数量。**tls_termination** 的可能值为 **edge**、**passthrough** 和 **reencrypt**

1.3.10.10. AWS Load Balancer Operator

在 OpenShift Container Platform 4.12 中，AWS Load Balancer 控制器现在为多个匹配项实现 Kubernetes Ingress 规格。如果 Ingress 中的多个路径与一个请求匹配，则最长匹配的路径优先。如果有两个路径仍然匹配，具有准确路径类型的路径优先于前缀路径类型。

AWS Load Balancer Operator 将 **EnableIPTargetType** 功能门设置为 **false**。AWS Load Balancer 控制器禁用对 **target-type ip** 的服务和入口资源的支持。

OpenShift Container Platform 4.12 的 **aws-load-balancer-controller** 的上游版本是 v2.4.4。

1.3.10.11. Ingress Controller 自动扩展（技术预览）

现在，您可以使用 OpenShift Container Platform Custom Metrics Autoscaler Operator 在部署的集群中根据指标（如可用的 worker 节点数量）来动态地扩展默认的入口控制器。自定义 Metrics Autoscaler 作为技术预览提供。

如需更多信息，请参阅自动扩展 Ingress Controller。

1.3.10.12. HAProxy maxConnections 现在默认为 50,000

在 OpenShift Container Platform 4.12 中，**maxConnections** 设置的默认值现在是 50000。以前，从 OpenShift Container Platform 4.11 开始，**maxConnections** 设置的默认值为 20000。

如需更多信息，请参阅 Ingress Controller 配置参数。

1.3.10.13. 配置 Ingress Controller 以进行手动 DNS 管理

现在，您可以将 Ingress Controller 配置为停止自动 DNS 管理并启动手动 DNS 管理。设置 **dnsManagementPolicy** 参数来指定自动或手动 DNS 管理。

如需更多信息，请参阅配置 Ingress Controller 以手动管理 DNS 。

1.3.10.14. SR-IOV 支持的硬件（单根 I/O 虚拟化）

OpenShift Container Platform 4.12 添加了对以下 SR-IOV 设备的支持：

- MT2892 Family [ConnectX-6 Dx]
- MT2894 Family [ConnectX-6 Lx]
- ConnectX-6 NIC 模式中的 MT42822 BlueField-2
- Silicom STS 系列

如需更多信息，请参阅支持的设备。

1.3.10.15. OvS (Open vSwitch) Hardware Offload 支持的硬件

OpenShift Container Platform 4.12 添加了对以下设备的 OvS Hardware Offload 支持：

- MT2892 系列 [ConnectX-6 Dx]
- MT2894 Family [ConnectX-6 Lx]
- ConnectX-6 NIC 模式中的 MT42822 BlueField-2

如需更多信息，请参阅支持的设备。

1.3.10.16. SR-IOV 支持的多网络策略（技术预览）

OpenShift Container Platform 4.12 添加了对为 SR-IOV 设备配置多网络策略的支持。

现在，您可以为 SR-IOV 额外网络配置多网络。配置 SR-IOV 额外网络是一个技术预览功能，仅支持内核网络接口卡 (NIC)。

如需更多信息，请参阅配置多网络策略。

1.3.10.17. 在 AWS 负载均衡器类型间切换，而不删除 Ingress Controller

您可以更新 Ingress Controller，以便在 AWS Classic Load Balancer (CLB) 和 AWS Network Load Balancer (NLB) 间切换，而无需删除 Ingress Controller。

如需更多信息，请参阅在 AWS 中配置 ingress 集群流量 。

1.3.10.18. IPv6 unsolicited neighbor 公告和 IPv4 gratuitous 地址解析协议现在默认在 SR-IOV CNI 插件中

使用单一根 I/O 虚拟化 (SR-IOV) CNI 插件创建的 Pod，其中 IP 地址管理 CNI 插件已经分配 IP，现在发送 IPv6 unsolicited 邻居公告和/或 IPv4 gratuitous 地址解析协议（在网络中）。此功能增强会通知特定 IP 的新 pod MAC 地址的主机，以使用正确的信息刷新 ARP/NDP 缓存。

如需更多信息，请参阅支持的设备。

1.3.10.19. 支持 CoreDNS 缓存调整

现在，您可以在 CoreDNS 缓存成功和成功 DNS 查询时配置 time-to-live (TTL) 持续时间。

如需更多信息，请参阅调整 CoreDNS 缓存。

1.3.10.20. OVN-Kubernetes 支持配置内部子网

在以前的版本中，OVN-Kubernetes 在内部使用的子网为 **100.64.0.0/16**（IPv4）和 **fd98::/48**（IPv6）无法修改。要在这些子网与基础架构中现有子网重叠时支持实例，现在可以更改这些内部子网以避免重叠。

如需更多信息，请参阅 Cluster Network Operator 配置对象

1.3.10.21. Red Hat OpenStack Platform (RHOSP) 上的出口 IP 支持

RHOSP 与 OpenShift Container Platform 搭配，现在支持自动附加和分离 Egress IP 地址。来自任意数量的命名空间中的一个或多个 pod 的流量，对于集群外的服务具有一个一致的源 IP 地址。此支持适用于 OpenShift SDN 和 OVN-Kubernetes 作为默认网络提供程序。

1.3.10.22. OpenShift SDN 到 OVN-Kubernetes 功能迁移支持

如果您计划从 OpenShift SDN 网络插件迁移到 OVN-Kubernetes 网络插件，则以下功能的配置将自动转换为使用 OVN-Kubernetes：

- 出口 IP 地址
- 出口防火墙
- 多播

如需有关如何迁移到 OVN-Kubernetes 的更多信息，请参阅从 OpenShift SDN 集群网络供应商迁移。

1.3.10.23. Egress 防火墙审计日志记录

对于 OVN-Kubernetes 网络插件，出口防火墙支持使用与网络策略审计日志记录使用的相同机制进行审计日志记录。如需更多信息，请参阅出口防火墙和网络策略规则的日志记录。

1.3.10.24. 从给定地址池中公告 MetalLB

在这个版本中，在 BGP 模式中，您可以使用节点选择器使用特定的 IP 地址池从节点的子集公告 MetalLB 服务。此功能在 OpenShift Container Platform 4.11 中作为技术预览功能引进，现在在 OpenShift Container Platform 4.12 for BGP 模式中正式发布。L2 模式仍是一个技术预览功能。

如需更多信息，请参阅从节点的子集提升 IP 地址池。

1.3.10.25. MetalLB 的额外部署规格

这个版本为 MetalLB 提供了额外的部署规格。当使用自定义资源来部署 MetalLB 时，您可以使用这些额外部署规格来管理在集群中部署和运行 MetalLB **speaker** 和 **controller** pod。例如，您可以使用 MetalLB 部署规格来管理部署 MetalLB pod 的位置，为 MetalLB pod 定义 CPU 限值，并为 MetalLB pod 分配运行时类。

有关 MetalLB 部署规格的更多信息，请参阅 MetalLB 的部署规格。

1.3.10.26. 节点 IP 选择改进

在以前的版本中，集群主机上的 **nodeip-configuration** 服务从默认路由使用的接口选择 IP 地址。如果存在多个路由，该服务将选择具有最低指标值的路由。因此，网络流量可以从不正确的接口分发。

在 OpenShift Container Platform 4.12 中，在 **nodeip-configuration** 服务中添加了一个新的接口，该服务允许用户创建 hint 文件。hint 文件包含变量 **NODEIP_HINT**，可覆盖默认 IP 选择逻辑并从子网 **NODEIP_HINT** 变量中选择特定的节点 IP 地址。使用 **NODEIP_HINT** 变量允许用户指定使用哪些 IP 地址，确保网络流量从正确的接口分发。

如需更多信息，请参阅 可选：覆盖默认节点 IP 选择逻辑。

1.3.10.27. CoreDNS 更新至 1.10.0 版本

在 OpenShift Container Platform 4.12 中，CoreDNS 使用 1.10.0 版本，它包括以下更改：

- 如果 CoreDNS 之前设置为较小的值，CoreDNS 不会扩展查询 UDP 缓冲区的大小。
- CoreDNS 现在始终在 Kubernetes 客户端日志中为每个日志行添加相关日志级别。
- CoreDNS 现在以大约 20ms 的速度重新加载。

1.3.10.28. 支持 HAProxy 中可配置的重新加载间隔

在这个版本中，集群管理员可以配置重新加载间隔，以强制 HAProxy 在响应路由和端点更新时更频繁地重新载入其配置。默认最小 HAProxy 重新加载间隔为 5 秒。

如需更多信息，请参阅配置 HAProxy 重新加载间隔。

1.3.10.29. 新的 Network Observability Operator 观察网络流量流

现在，您可以安装 Network Observability Operator 来在控制台中观察 OpenShift Container Platform 集群的网络流量。您可以使用不同的图形表示来查看和监控网络流量数据。Network Observability Operator 使用 eBPF 技术来创建网络流。网络流包括了 OpenShift Container Platform 的信息并存储在 Loki 中。您可以使用网络流量信息来详细地进行故障排除和分析。

如需更多信息，请参阅 Network Observability。

1.3.10.30. RHOSP 上二级网络接口的 IPv6

现在，在 RHOSP 上运行的集群中支持用于二级网络接口的 IPv6。

如需更多信息，请参阅启用 RHOSP 上的 pod 的 IPv6 连接 。

1.3.10.31. RHOSP 上负载均衡器的 UDP 支持

因为切换到使用外部 OpenStack 云供应商，UDP 现在对于在该平台上运行的集群提供对 **LoadBalancer** 服务的支持。

1.3.10.32. 为托管的 control plane 部署 SR-IOV Operator （技术预览）

如果配置并部署了托管服务集群，您现在可以为托管集群部署 SR-IOV Operator。如需更多信息，请参阅为托管 control plane 部署 SR-IOV Operator 。

1.3.10.33. 支持 Ingress VIP 和 API VIP 服务的 IPv6 虚拟 IP (VIP)地址

在这个版本中，在安装程序置备的基础架构集群中，**install-config.yaml** 文件中的 **ingressVIP** 和 **apiVIP**

配置设置已弃用。反之，使用 **ingressVIPs** 和 **apiVIPs** 配置设置。这些设置支持使用 Ingress VIP 和 API VIP 服务对需要 IPv4 和 IPv6 访问集群的应用程序的双栈网络。**ingressVIPs** 和 **apiVIPs** 配置设置使用列表格式来指定 IPv4 地址、IPv6 地址或两个 IP 地址格式。列表的顺序决定了每个服务的主 VIP 地址和次 VIP 地址。在使用双栈网络时，主 IP 地址必须来自 IPv4 网络。

1.3.10.34. 支持将 Bluefield-2 网络设备从数据处理单元 (DPU) 模式切换到网络接口控制器 (NIC) 模式（技术预览）

在这个版本中，您可以将 BlueField-2 网络设备从数据处理单元 (DPU) 模式切换到网络接口控制器 (NIC) 模式。

如需更多信息，请参阅将 Bluefield-2 从 DPU 切换到 NIC。

1.3.11. 存储

1.3.11.1. 使用 GCP Filestore Driver Operator 的持久性存储（技术预览）

OpenShift Container Platform 可以使用 Google Compute Platform (GCP) 文件存储的 Container Storage Interface (CSI) 驱动程序置备持久性卷 (PV)。管理此驱动程序的 GCP Filestore CSI Driver Operator 只是一个技术预览。

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

1.3.11.2. AWS Elastic Block Storage auto 迁移的自动 CSI 迁移已正式发布

从 OpenShift Container Platform 4.8 开始，在树内卷插件自动迁移到对应的 Container Storage Interface(CSI)驱动程序作为技术预览。OpenShift Container Platform 4.8 中提供了对 Amazon Web Services (AWS) Elastic Block Storage (EBS) 的支持，OpenShift Container Platform 4.12 现在支持对 AWS EBS 的自动迁移 (GA)。现在，AWS EBS 的 CSI 迁移会被默认启用，且管理员不需要操作。

这个功能会自动将树内对象转换为对应的 CSI 表示，并对用户完全透明。翻译的对象不存储在磁盘上，用户数据不会迁移。

虽然引用 in-tree 存储插件的存储类将继续工作，但我们建议将默认存储类切换到 CSI 存储类。

如需更多信息，请参阅 CSI 自动迁移。

1.3.11.3. GCP PD 自动迁移的自动 CSI 迁移已正式发布

从 OpenShift Container Platform 4.8 开始，在树内卷插件自动迁移到对应的 Container Storage Interface(CSI)驱动程序作为技术预览。OpenShift Container Platform 4.9 提供了对 Google Compute Engine Persistent Disk (GCP PD) 的支持，OpenShift Container Platform 4.12 现在支持对 GCP PD 进行自动迁移 (GA)。现在，GCP PD 的 CSI 迁移是默认启用的，且管理员不需要操作。

这个功能会自动将树内对象转换为对应的 CSI 表示，并对用户完全透明。翻译的对象不存储在磁盘上，用户数据不会迁移。

虽然引用 in-tree 存储插件的存储类将继续工作，但我们建议将默认存储类切换到 CSI 存储类。

如需更多信息，请参阅 CSI 自动迁移。

1.3.11.4. pod 调度的存储容量跟踪已正式发布

这个新功能使用 **CSIStorageCapacity** 对象公开当前可用的存储容量，并增强了对使用 Container Storage Interface (CSI) 卷的 pod 调度与后绑定的调度。目前，唯一支持此功能的 OpenShift Container Platform 存储类型是 OpenShift Data Foundation。

1.3.11.5. VMware vSphere CSI 拓扑已正式发布

OpenShift Container Platform 提供了将 OpenShift Container Platform for vSphere 部署到不同的区域和区域，允许您在多个计算集群中部署，这有助于避免单点故障。

如需更多信息，请参阅 vSphere CSI 拓扑 。

1.3.11.6. 本地临时存储资源管理已正式发布

本地临时存储资源管理功能现已正式发布。借助此功能，您可以通过指定请求和限制来管理本地临时存储。

如需更多信息，请参阅临时存储管理。

1.3.11.7. 卷填充器（技术预览）

卷填充器使用 数据源 来创建预先填充的卷。

目前启用了卷填充，并作为技术预览功能支持。但是，OpenShift Container Platform 不附带任何卷填充器。

如需更多信息，请参阅 卷填充器。

1.3.11.8. VMware vSphere CSI Driver Operator 要求

对于 OpenShift Container Platform 4.12，VMWare vSphere Container Storage Interface (CSI) Driver Operator 需要安装以下最小组件：

- 不支持 VMware vSphere 版本 7.0 更新 2 或更高版本，但不包括版本 8。
- 不支持 vCenter 7.0 更新 2 或更高版本，但不包括版本 8. vCenter 8。
- 硬件版本 15 或更高版本的虚拟机
- 集群中还没有安装第三方 CSI 驱动程序

如果集群中存在第三方 CSI 驱动程序，OpenShift Container Platform 不会覆盖它。存在第三方 CSI 驱动程序可防止 OpenShift Container Platform 升级到 OpenShift Container Platform 4.13 或更高版本。

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

1.3.12. Operator 生命周期

1.3.12.1. 平台 Operator （技术预览）

从 OpenShift Container Platform 4.12 开始，Operator Lifecycle Manager (OLM)引入了 *平台 Operator* 类型作为技术预览功能。平台 Operator 机制依赖于 RukPak 组件（也称为 OpenShift Container Platform 4.12）中的资源来源和管理内容。

平台 Operator 是一个基于 OLM 的 Operator，可在 OpenShift Container Platform 集群的第 0 天操作期间或之后安装，并参与集群的生命周期。作为集群管理员，您可以使用平台 Operator 来进一步自定义 OpenShift Container Platform 安装，以满足您的要求和用例。

如需有关平台 Operator 的更多信息，请参阅管理平台 Operator。有关 RukPak 及其资源的更多信息，请参阅 Operator Framework 打包格式。

1.3.12.2. 控制安装 Operator 的位置

默认情况下，当安装 Operator 时，OpenShift Container Platform 会随机将 Operator pod 安装到其中一个 worker 节点。

在 OpenShift Container Platform 4.12 中，您可以通过向 Operator 的 **Subscription** 对象添加关联性限制来控制 Operator pod 的安装位置。

如需更多信息，请参阅控制安装 Operator 的位置。

1.3.12.3. 为用户创建的 openshift-* 命名空间进行 Pod 安全准入同步

在 OpenShift Container Platform 4.12 中，如果在具有 **openshift-** 前缀的用户创建命名空间中安装 Operator，则默认启用 pod 安全准入同步。在命名空间中创建集群服务版本 (CSV) 后，同步会被启用。同步标签继承命名空间中服务帐户的权限。

如需更多信息，请参阅安全性上下文约束与 pod 安全标准同步。

1.3.13. Operator 开发

1.3.13.1. 配置目录 pod 的安全上下文

您可以使用 **run bundle** 和 **bundle-upgrade** 子命令中的 **--security-context-config** 标志来配置目录 pod 的安全上下文。标志可让 seccomp 配置集符合 pod 安全准入。标志接受 **restricted** 和 **legacy** 值。如果没有指定值，seccomp 配置集默认为 **restricted**。如果您的目录 pod 无法使用受限权限运行，请将标记设置为 **legacy**，如下例所示：

```
$ operator-sdk run bundle \
  --security-context-config=legacy
```

1.3.13.2. 验证从 Kubernetes 1.25 中删除的 API 的捆绑包清单

现在，您可以使用 **bundle validate** 子命令的 Operator Framework 套件检查从 Kubernetes 1.25 中删除的已弃用 API 的捆绑包清单。

例如：

```
$ operator-sdk bundle validate .<bundle_dir_or_image> \
  --select-optional suite=operatorframework \
  --optional-values=k8s-version=1.25
```

如果您的 Operator 请求权限使用从 Kubernetes 1.25 中删除的任何 API，命令会显示警告信息。

如果 Operator 的集群服务版本 (CSV) 中包含了从 Kubernetes 1.25 中删除的任何 API 版本，命令会显示错误消息。

如需更多信息，请参阅从 Kubernetes 1.25 中删除的 Beta API 和 Operator SDK CLI 参考。

1.3.14. 机器 API

1.3.14.1. 控制平面（control plane）机器集

OpenShift Container Platform 4.12 引入了 control plane 机器集。control plane 机器集为 control plane 机器提供管理功能，与为计算机器提供的计算机器集类似。如需更多信息，请参阅管理 control plane 机器。

1.3.14.2. 指定集群自动扩展日志级别详细程度

OpenShift Container Platform 现在支持通过在 **ClusterAutoscaler** 自定义资源中设置 **logVerbosity** 参数来设置集群自动扩展的日志级别详细程度。如需更多信息，请参阅 **ClusterAutoscaler** 资源定义。

1.3.14.3. 启用 Azure 引导诊断

OpenShift Container Platform 现在支持在机器集创建的 Azure 机器上启用引导诊断。如需更多信息，请参阅为计算机器或 control plane 机器 启用 Azure 引导诊断。

1.3.15. Machine Config Operator

1.3.15.1. RHCOS 镜像分层

Red Hat Enterprise Linux CoreOS (RHCOS) 镜像分层允许您在基本 RHCOS 镜像之上添加新镜像。此分层不会修改基本 RHCOS 镜像。相反，它会创建一个*自定义层次镜像*，其中包含所有 RHCOS 功能，并为集群中的特定节点添加额外的功能。

目前，RHCOS 镜像分层允许您根据 红帽 Hotfix 策略与客户体验和参与(CEE)在 RHCOS 镜像上获取并应用 Hotfix 软件包。计划在以后的发行版本，您可以使用 RHCOS 镜像分层来融合第三方软件包，如 Libreswan 或 numactl。

如需更多信息，请参阅 RHCOS 镜像分层。

1.3.16. 节点

1.3.16.1. 更新特定于接口的安全列表（技术预览）

OpenShift Container Platform 现在支持更新默认特定于接口的安全 **sysctl**。

您可以从预定义的列表中添加或删除 **sysctl**。添加 **sysctl** 时，可以在所有节点上设置它们。更新接口特定安全 **sysctl** 列表只是一个技术预览功能。

如需更多信息，请参阅更新特定于接口的安全 sysctl 列表。

1.3.16.2. Cron Job 时区（技术预览）

现在，为 cron 作业调度设置时区是一个技术预览功能。如果没有指定时区，Kubernetes 控制器管理器会解释相对于其本地时区的调度。

如需更多信息，请参阅创建 cron 作业。

1.3.16.3. Linux Control Group 版本 2 提升到技术预览

OpenShift Container Platform 对 Linux Control Group 版本 2 (cgroup v2)的支持被提升到技术预览。cgroup v2 是内核 控制组 的下一个版本。cgroups v2 提供了多个改进，包括统一的层次结构、安全子树

委托、像 压力失速信息 这样的新功能，以及增强的资源管理和隔离。如需更多信息，请参阅 启用 Linux Control Group 版本 2 (cgroup v2)。

1.3.16.4. crun 容器运行时（技术预览）

OpenShift Container Platform 现在在技术预览中支持 crun 容器运行时。您可以使用 **ContainerRuntimeConfig** 自定义资源(CR)在 crun 容器运行时和默认的容器运行时之间切换。如需更多信息，请参阅 关于容器引擎和容器运行时。

1.3.16.5. Self Node Remediation Operator 的改进

OpenShift Container Platform 现在支持 Self Node Remediation Operator 的 control plane 隔离。如果节点出现故障，您可以在 worker 节点和 control plane 节点上遵循补救策略。如需更多信息，请参阅 Control Plane 隔离。

1.3.16.6. Node Health Check Operator 的改进

OpenShift Container Platform 现在支持 Node Health Check Operator 上的 control plane 隔离。如果节点出现故障，您可以在 worker 节点和 control plane 节点上遵循补救策略。如需更多信息，请参阅 Control Plane 隔离。

Node Health Check Operator 现在还包含用于管理 Node Health Checks 的 Web 控制台插件。如需更多信息，请参阅创建节点健康检查。

要安装或升级到 Node Health Check Operator 的最新版本，请使用 **stable** 订阅频道。如需更多信息，请参阅使用 CLI 安装 Node Health Check Operator 。

1.3.17. 监控

此版本的监控堆栈包括以下新功能和修改后的功能。

1.3.17.1. 监控堆栈组件和依赖项更新

此发行版本包括监控堆栈组件和依赖项的以下版本更新：

- kube-state-metrics 2.6.0
- node-exporter 1.4.0
- prom-label-proxy 0.5.0
- Prometheus 2.39.1
- prometheus-adapter 0.10.0
- prometheus-operator 0.60.1
- Thanos 0.28.1

1.3.17.2. 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。

- New
  - 添加了 **TelemeterClientFailures** 警报，它会在集群尝试和失败时以特定时间段内提交 Telemetry 数据触发。当请求失败率达到 15 分钟窗口中请求总速率的 20% 时，警报将触发。
- 已更改
  - **KubeAggregatedAPIDown** 警报现在会在发送通知前等待 900 秒而不是 300 秒。
  - **NodeClockNotSynchronising** 和 **NodeClockSkewDetected** 警报现在只评估 **node-exporter** 作业的指标。
  - **NodeRAIDDegraded** 和 **NodeRAIDDiskFailure** 警报现在包含一个设备标签过滤器，仅匹配 **mmcblk.p.|nvme.|sd.|xvd.|xvd.|dm-.|dasd.+**。
  - 现在，当查询层存在高查询负载时，**PrometheusHighQueryLoad** 和 **ThanosQueryOverload** 警报也会触发。

1.3.17.3. 为监控组件指定 pod 拓扑分布限制的新选项

现在，当 OpenShift Container Platform pod 部署到多个可用区时，您可以使用 pod 拓扑分布约束来控制 Prometheus、Thanos Ruler 和 Alertmanager pod 如何分散到网络拓扑中。

1.3.17.4. 新的选项用于提高 Prometheus Adapter 的数据一致性

现在，您可以为 Prometheus Adapter (PA) 配置可选的 kubelet 服务，以提高多个自动扩展请求之间的数据一致性。启用这个服务监控器可以避免同时向 PA 发送的两个查询可能会产生不同的结果，因为 PA 执行的底层 PromQL 查询可能位于不同的 Prometheus 服务器上。

1.3.17.5. 更新至 Alertmanager 配置以提供额外的 secret 密钥

在这个版本中，如果您将 Alertmanager secret 配置为保存额外的密钥，如果 Alertmanager 配置引用这些密钥的文件（如模板、TLS 证书或令牌），您的配置设置必须使用绝对路径而不是相对路径指向这些密钥。这些键位于 **/etc/alertmanager/config** 目录下。在早期版本的 OpenShift Container Platform 中，您可以使用配置中的相对路径指向这些密钥，因为 Alertmanager 配置文件与密钥位于同一个目录中。

重要

如果要升级到 OpenShift Container Platform 4.12，并为引用为文件的额外 Alertmanager secret 密钥指定相对路径，您必须将这些相对路径改为 Alertmanager 配置中的绝对路径。否则，使用文件的警报接收器将无法发送通知。

1.3.18. 可伸缩性和性能

1.3.18.1. 使用工作负载提示禁用实时程序会从集群中删除 Receive Packet Steering

在默认情况下，systemd 服务为虚拟网络接口设置 Receive Packet Steering (RPS) 掩码。RPS 掩码根据性能配置集中定义的保留 CPU 列表，路由来自虚拟网络接口的请求。在容器级别，**CRI-O** hook 脚本还会为所有虚拟网络设备设置 RPS 掩码。

在这个版本中，如果您将性能配置集中的 **spec.workloadHints.realTime** 设置为 **False**，则系统还会禁用 systemd 服务和设置 RPS 掩码的 **CRI-O** hook 脚本。系统禁用这些 RPS 功能，因为 RPS 通常与需要低延迟、实时工作负载的用例相关。

要保留 RPS 功能，即使您将 **spec.workloadHints.realTime** 设置为 **False**，请参阅红帽知识库解决方案 Performance addons operator 高级配置 中的 *RPS Settings* 部分。

有关配置工作负载提示的更多信息，请参阅了解工作负载提示。

1.3.18.2. tuned 配置集

tuned 配置集现在默认定义了 **fs.aio-max-nr sysctl** 值，改进了默认节点配置集的异步 I/O 性能。

1.3.18.3. 支持新内核功能和选项

低延迟调整已更新，以使用最新的内核功能和选项。2117780 的修复引入了一个新的针对每个 CPU 的 **kthread,ktimers**。这个线程必须固定到正确的 CPU 内核。在这个版本中，没有功能更改，工作负载的隔离是相同的。如需更多信息，请参阅 2102450。

1.3.18.4. 节能配置

在 OpenShift Container Platform 4.12 中，通过启用 C-states 和 OS 控制的 P-states，您可以为关键和非关键工作负载使用不同的节能配置。您可以通过新的 **perPodPowerManagement** 工作负载提示和 **cpu-c-states.crio.io** 和 **cpu-freq-governor.crio.io** CRI-O 注解来应用配置。有关该功能的更多信息，请参阅节能配置。

1.3.18.5. 使用 GitOps ZTP 使用 worker 节点扩展单节点 OpenShift 集群（技术预览）

在 OpenShift Container Platform 4.11 中，引入了一个新的 worker 节点到单节点 OpenShift 集群。此功能现在包括在 GitOps ZTP 中。

如需更多信息，请参阅使用 GitOps ZTP 将 worker 节点添加到单节点 OpenShift 集群 。

1.3.18.6. factory-precaching-cli 工具可以减少 OpenShift Container Platform 和 Operator 的部署时间（技术预览）

在 OpenShift Container Platform 4.12 中，您可以使用 factory-precaching-cli 工具预缓存 OpenShift Container Platform 和 Operator 镜像。然后，您可以将预缓存服务器包含在部署的站点。如需有关 factory-precaching-cli 工具的更多信息，请参阅单节点 OpenShift 部署的预缓存镜像。

1.3.18.7. factory-precaching-cli 工具的 ZTP 集成（技术预览）

在 OpenShift Container Platform 4.12 中，您可以使用 GitOps ZTP 工作流中的 factory-precaching-cli 工具。如需更多信息，请参阅单节点 OpenShift 部署的预缓存镜像。

1.3.18.8. 托管集群中的节点性能优化（技术预览）

现在，您可以使用 Node Tuning Operator 为托管集群中的节点配置 OS 级别性能优化。要配置节点性能优化，您可以在包含 **Tuned** 对象的管理集群中创建配置映射，并在节点池中引用这些配置映射。**Tuned** 对象中防御的调优配置应用到节点池中的节点。如需更多信息，请参阅在托管集群中配置节点调整。

1.3.18.9. 内核模块管理 Operator

内核模块管理 (KMM) Operator 替换了特殊资源 Operator (SRO)。KMM 仅对连接的环境提供以下功能：

- 对于边缘部署支持 hub 和 spoke
- 支持升级的 pre-flight 检查

- 安全引导内核模块签名
- 必须收集日志以帮助进行故障排除
- 二进制固件部署

1.3.18.10. hub 和 spoke 集群支持（技术预览）

对于一个可以访问互联网的环境中的 hub 和 spoke 部署，您可以使用 hub 集群中部署的内核模块管理 (KMM) Operator 来管理将所需的内核模块部署到一个或多个受管集群。

1.3.18.11. Topology Aware Lifecycle Manager (TALM)

Topology Aware Lifecycle Manager (TALM) 现在提供更详细的状态信息和信息，以及重新设计的条件。您可以使用 **ClusterLabelSelector** 字段在选择集群进行更新时具有更大的灵活性。您可以使用超时设置来确定集群是否有更新失败，例如跳过失败的集群并继续升级其他集群，或停止所有集群的策略补救。如需更多信息，请参阅集群更新的 Topology Aware Lifecycle Manager 。

1.3.18.12. 挂载命名空间封装（技术预览）

封装是将所有特定于 Kubernetes 的挂载点的过程移到备用命名空间，以减少 default 命名空间中大量挂载点的可见性和性能影响。在以前的版本中，OpenShift Container Platform 中已透明地部署命名空间封装，专门用于使用 GitOps ZTP 安装的分布式单元 (DU)。在 OpenShift Container Platform v4.12 中，这个功能现在作为一个可配置的选项提供。

标准的主机操作系统使用 systemd 持续扫描所有挂载命名空间：标准 Linux 挂载和 Kubernetes 用来操作的大量挂载。Kubelet 和 CRI-O 的当前实现都使用所有容器和 Kubelet 挂载点的顶级命名空间。在私有命名空间中封装这些特定于容器的挂载点可减少 systemd 开销并提高了 CPU 性能。封装也可以通过将 Kubernetes 特定挂载点存储在非特权用户安全检查的位置来提高安全性。

如需更多信息，请参阅使用挂载命名空间封装优化 CPU 使用量。

1.3.18.13. 更改使用 GitOps ZTP 部署的单节点 OpenShift 集群中设置的工作负载分区 CPU

您可以使用 GitOps ZTP 在单节点 OpenShift 集群中配置工作负载分区 CPU。要做到这一点，您可以使用 **SiteConfig** 自定义资源 (CR) 的 **cpuset** 字段指定集群管理 CPU 资源，以及组 **PolicyGenTemplate** CR 的 **reserved** 字段。为 **cpuset** 设置的值应与工作负载分区的集群 **PerformanceProfile** CR **.spec.cpu.reserved** 字段中设置的值匹配。

如需更多信息，请参阅工作负载分区。

1.3.18.14. RHACM hub 模板功能现在可用于 GitOps ZTP

hub 模板功能现在可用于使用 Red Hat Advanced Cluster Management (RHACM) 和 Topology Aware Lifecycle Manager (TALM) 的 GitOps ZTP。hub-side 集群模板减少了对带有辅助配置但具有不同值的很多集群创建单独的策略的需求。如需更多信息，请参阅在 PolicyGenTemplate CR 中使用 hub 模板 。

1.3.18.15. ArgoCD 受管集群限制

RHACM 使用 **SiteConfig** CR 为 ArgoCD 生成第 1 天受管集群安装 CR。每个 ArgoCD 应用程序都可以管理最多 300 个 **SiteConfig** CR。如需更多信息，请参阅使用 ArgoCD 配置 hub 集群 。

1.3.18.16. GitOps ZTP 支持在 PolicyGenTemplate CR 中配置策略合规评估超时

在 GitOps ZTP v4.11+ 中，默认的策略合规评估超时值可用于 **PolicyGenTemplate** 自定义资源(CR)。这个值指定相关的 **ConfigurationPolicy** CR 在 RHACM 重新评估集群策略前处于策略合规或不合规状态的时长。

现在，您可以为 **PolicyGenTemplate** CR 中的所有策略覆盖默认评估间隔。

如需更多信息，请参阅为 PolicyGenTemplate CR 配置策略合规性评估超时 。

1.3.18.17. 为受管集群指定平台类型

Assisted Installer 目前支持以下 OpenShift Container Platform 平台：

- 裸机
- **vSphere**
- 无

单节点 OpenShift 不支持 **VSphere**。

1.3.18.18. 将 hub 集群配置为使用未经身份验证的 registry

此发行版本支持在配置 hub 集群时使用未经身份验证的 registry。不需要身份验证的 registry 列在 **AgentServiceConfig** 资源的 **spec.unauthenticatedRegistries** 下。任何此列表中的 registry 都不需要在用于 spoke 集群安装的 pull secret 中有一个条目。**assisted-service** 通过确保包含用于安装的每个镜像 registry 的身份验证信息来验证 pull secret。

如需更多信息，请参阅配置 hub 集群以使用未经身份验证的 registry 。

1.3.19. Insights Operator

1.3.19.1. Insights 警报

在 OpenShift Container Platform 4.12 中，现在以警报的形式向用户提供有效的 Insights 建议。您可以使用 Alertmanager 查看并配置这些警报。

1.3.19.2. 深入了解 Operator 数据收集功能的增强

在 OpenShift Container Platform 4.12 中，Insights Operator 现在收集以下指标：

- **console_helm_uninstalls_total**
- **console_helm_upgrades_total**

1.3.20. 认证和授权

1.3.20.1. RHOSP 上的应用程序凭证

现在，您可以在 Red Hat OpenStack Platform (RHOSP) 上运行的集群的 **clouds.yaml** 文件中指定应用程序凭证。应用凭据是在配置文件中嵌入用户帐户详细信息的替代选择。例如，请参阅 **clouds.yaml** 文件的以下部分，其中包含用户帐户详情：

```
clouds:
  openstack:
```

```
      auth:
        auth_url: https://127.0.0.1:13000
        password: thepassword
        project_domain_name: Default
        project_name: theprojectname
        user_domain_name: Default
        username: theusername
      region_name: regionOne
```

将该部分与使用应用程序凭证的比较：

```
clouds:
  openstack:
    auth:
      auth_url: https://127.0.0.1:13000
      application_credential_id: '5dc185489adc4b0f854532e1af81ffe0'
      application_credential_secret:
'PDCTKans2bPBbaEqBLiT_IajG8e5J_nJB4kvQHjaAy6ufhod0Zl0NkNoBzjn_bWSYzk587ieIGSlT11c4pV
ehA'
      auth_type: "v3applicationcredential"
      region_name: regionOne
```

要将应用程序凭证作为 RHOSP 管理员与集群一起使用，请创建凭证。然后，当您安装集群时，在 **clouds.yaml** 文件中使用它们。另外，您可以创建 **clouds.yaml** 文件，并将其轮转到现有集群中。

1.3.21. 托管 control plane（技术预览）

1.3.21.1. HyperShift API beta 版本现在可用

hypershift.openshift.io API 的默认版本是 OpenShift Container Platform 上托管 control plane 的 API，现在是 v1beta1。目前，对于一个现有的集群，不支持从 alpha 更新到 beta。

1.3.21.2. 托管 control plane 的版本控制

OpenShift Container Platform 的每个主版本、次版本或补丁版本都会发布 HyperShift Operator。HyperShift 命令行界面 (CLI) 作为每个 HyperShift Operator 发行版本的一部分发布。

HostedCluster 和 **NodePool** API 资源在 API 的 beta 版本中提供，并遵循与 OpenShift Container Platform 和 Kubernetes 类似的策略。

1.3.21.3. 在托管集群中备份和恢复 etcd

如果您在 OpenShift Container Platform 上使用托管的 control plane，可以通过生成 etcd 快照来备份和恢复 etcd，并将其上传到稍后可以检索它的位置，如 S3 存储桶。之后，您可以恢复快照。如需更多信息，请参阅在托管集群中备份和恢复 etcd。

1.3.21.4. AWS 区域托管的集群的灾难恢复

对于托管集群需要灾难恢复的情况，您可以将托管集群恢复到 AWS 中的同一区域。如需更多信息，请参阅 AWS 区域中的托管集群的灾难恢复。

1.3.22. Red Hat Virtualization（RHV）

此发行版本为 Red Hat Virtualization (RHV) 提供了几个更新。在这个版本中：

- oVirt CSI 驱动程序日志记录被修改并带有新的错误消息，以提高日志的清晰性和可读性。
- 在 OpenShift Container Platform 中更改时，集群 API 供应商会自动更新 oVirt 和 Red Hat Virtualization (RHV) 凭证。

1.4. 主要的技术变化

OpenShift Container Platform 4.12 包括以下显著的技术更改。

AWS 安全令牌服务区域端点
Cloud Credential Operator 实用程序(**ccoctl**)现在创建使用 AWS 安全令牌服务(AWS STS) 的区域端点的 secret。此方法与 AWS 推荐的最佳实践一致。

凭证请求目录参数，以使用 Cloud Credential Operator 实用程序删除 GCP 资源
在这个版本中，当使用 Cloud Credential Operator 实用程序删除 GCP 资源时，您必须指定包含组件 **CredentialsRequest** 对象文件的目录。

以后对 pod 安全准入的限制强制
目前，pod 安全违反情况会显示为警告并在审计日志中记录，但不会导致 pod 被拒绝。

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

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

如果您要收到 pod 安全漏洞，请查看以下资源：

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

目录源和受限 pod 安全准入执行
使用基于 SQLite 的目录格式构建的目录源以及在 OpenShift Container Platform 4.11 无法运行受限 pod 安全强制前发布的 **opm** CLI 工具的版本。

在 OpenShift Container Platform 4.12 中，命名空间默认没有限制 pod 安全强制，默认目录源安全模式被设置为 **legacy**。

如果您不想在受限 pod 安全强制下运行基于 SQLite 的目录源 pod，则不需要更新 OpenShift Container Platform 4.12 中的目录源。但是，为了确保目录源在以后的 OpenShift Container Platform 版本中运行，您必须更新目录源以便在受限 pod 安全强制下运行。

作为目录作者，您可以通过完成以下任一操作来启用与受限 pod 安全强制的兼容性：

- 将您的目录迁移到基于文件的目录格式。

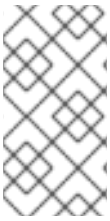
- 使用 OpenShift Container Platform 4.11 或更高版本发布的 **opm** CLI 工具版本更新您的目录镜像。

如果您不想更新 SQLite 数据库目录镜像，或将目录迁移到基于文件的目录格式，您可以将目录配置为使用升级的权限运行。

如需更多信息，请参阅目录源和 Pod 安全准入。

Operator SDK 1.25.4

OpenShift Container Platform 4.12 支持 Operator SDK 1.25.4。请参阅安装 Operator SDK CLI 来安装或更新到这个最新版本。



注意

Operator SDK 1.25.4 支持 Kubernetes 1.25。

如需更多信息，请参阅从 Kubernetes 1.25 中删除 Beta API 和 Validating bundle manifests for APIs removed from Kubernetes 1.25。

如果您之前使用 Operator SDK 1.22.0 创建或维护的 Operator 项目，请更新您的项目以保持与 Operator SDK 1.25.4 的兼容性。

- 更新基于 Go 的 Operator 项目
- 更新基于 Ansible 的 Operator 项目
- 更新基于 Helm 的 Operator 项目
- 更新基于 Helm 的 Operator 项目
- 更新基于 Java 的 Operator 项目

LVM Operator 现在被称为逻辑卷管理器存储

之前由 Red Hat OpenShift Data Foundation 提供的 LVM Operator 需要通过 OpenShift Data Foundation 安装。在 OpenShift Container Platform v4.12 中，LVM Operator 已重命名为 *Logical Volume Manager Storage*。现在，您可以从 OpenShift Operator 目录将其作为独立的 Operator 安装。逻辑卷管理器存储在单个有限资源 OpenShift 集群中提供块存储的动态置备。

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

在以下表格中，功能被标记为以下状态：

- *公开发行*
- *已弃用*
- *删除*

Operator 弃用和删除的功能

表 1.2. Operator 已弃用并删除 tracker

表 1.2. Operator 已弃用并删除 tracker

功能	4.10	4.11	4.12
Operator 目录的 SQLite 数据库格式	已弃用	已弃用	已弃用

镜像已弃用和删除的功能

表 1.3. 镜像已弃用和删除的 tracker

功能	4.10	4.11	4.12
Cluster Samples Operator 的 **ImageChangesInProgress** 条件	已弃用	已弃用	已弃用
Cluster Samples Operator 的 **MigrationInProgress** 条件	已弃用	已弃用	已弃用
从安装有效负载中删除 Jenkins 镜像	公开发行	删除	删除

监控已弃用和删除的功能

表 1.4. 监控已弃用和删除的 tracker

功能	4.10	4.11	4.12
监控堆栈中的 Grafana 组件	已弃用	删除	删除
访问监控堆栈中的 Prometheus 和 Grafana UI	已弃用	删除	删除

安装已弃用和删除的功能

表 1.5. 安装已弃用并删除跟踪器

功能	4.10	4.11	4.12
vSphere 6.7 更新 2 或更早版本	已弃用	删除	删除
vSphere 7.0 Update 1 或更早版本	公开发行	已弃用	已弃用
VMware ESXi 6.7 更新 2 或更早版本	已弃用	删除	删除
VMware ESXi 7.0 Update 1 或更早版本	公开发行	已弃用	已弃用
对 **cluster.local** 域的 CoreDNS 通配符查询	公开发行	公开发行	已弃用
安装程序置备的基础架构集群的 **install-config.yaml** 文件中的 **ingressVIP** 和 **apiVIP** 设置	公开发行	公开发行	已弃用

更新集群已弃用和删除的功能

表 1.6. 更新集群已弃用并删除 tracker

功能	4.10	4.11	4.12
虚拟硬件版本 13	已弃用	删除	删除

存储已弃用和删除的功能

表 1.7. 存储已弃用和删除的 tracker

功能	4.10	4.11	4.12
snapshot.storage.k8s.io/v1beta1 API 端点	已弃用	删除	删除
使用 FlexVolume 的持久性存储	已弃用	已弃用	已弃用

认证和授权已弃用和删除的功能

表 1.8. 认证和授权已弃用和删除的 tracker

功能	4.10	4.11	4.12
自动生成服务帐户令牌 secret	公开发行	删除	删除

特定的硬件和驱动程序启用已弃用和删除的功能

表 1.9. 专用硬件和驱动程序启用已弃用并删除跟踪器

功能	4.10	4.11	4.12
Special Resource Operator (SRO)	技术预览	技术预览	删除

多架构已弃用和删除的功能

表 1.10. 多架构已弃用并删除 tracker

功能	4.10	4.11	4.12
IBM POWER8 所有模型 (**ppc64le**)	公开发行	公开发行	已弃用
IBM IBM POWER9 AC922 (**ppc64le**)	公开发行	公开发行	已弃用
IBM IBM POWER9 IC922 (**ppc64le**)	公开发行	公开发行	已弃用
IBM IBM POWER9 LC922 (**ppc64le**)	公开发行	公开发行	已弃用

功能	4.10	4.11	4.12
IBM z13 所有模型 (**s390x**)	公开发行	公开发行	已弃用
IBM LinuxONE Emperor (**s390x**)	公开发行	公开发行	已弃用
IBM LinuxONE Rockhopper (**s390x**)	公开发行	公开发行	已弃用
AMD64 (x86_64) v1 CPU	公开发行	公开发行	已弃用

已弃用和删除的网络功能

表 1.11. 已弃用和删除的网络功能跟踪器

功能	4.10	4.11	4.12
RHOSP 上的 Kuryr	公开发行	公开发行	已弃用

1.5.1. 已弃用的功能

1.5.1.1. Red Hat Virtualization(RHV)作为 OpenShift Container Platform 的主机平台已弃用

即将推出的 OpenShift Container Platform 版本中将弃用 Red Hat Virtualization(RHV)。对 RHV 上的 OpenShift Container Platform 的支持将在未来的 OpenShift Container Platform 版本中删除，目前还计划为从 OpenShift Container Platform 4.14 开始删除。

1.5.1.2. cluster.local 域的通配符 DNS 查询已弃用

CoreDNS 将停止支持通配符 DNS 查询 **cluster.local** 域下的名称。这些查询将在 OpenShift Container Platform 4.12 中解决，就像在早期版本中一样，但将在以后的 OpenShift Container Platform 发行版本中删除支持。

1.5.1.3. ppc64le、s390x 和 x86_64 v1 CPU 架构上的特定硬件模型已弃用

在 OpenShift Container Platform 4.12 中，对 RHCOS 功能的支持已弃用：

- IBM POWER8 所有模型 (ppc64le)
- IBM POWER9 AC922 (ppc64le)
- IBM POWER9 IC922 (ppc64le)
- IBM POWER9 LC922 (ppc64le)
- IBM z13 所有模型 (s390x)
- LinuxONE Emperor (s390x)
- LinuxONE Rockhopper (s390x)

- AMD64 (x86_64) v1 CPU

虽然 OpenShift Container Platform 4.12 中完全支持这些硬件模型，但红帽建议您使用后续的硬件模型。

1.5.1.4. Kuryr 支持在 RHOSP 上运行的集群

在 OpenShift Container Platform 4.12 中，在 RHOSP 上运行的集群上对 Kuryr 的支持已弃用。这个支持最早不会在早于 OpenShift Container Platform 4.14 的版本中被删除。

1.5.2. 删除的功能

1.5.2.1. 从 Kubernetes 1.25 中删除的 beta API

Kubernetes 1.25 删除了以下弃用的 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 1.12. 从 Kubernetes 1.25 中删除的 API

资源	删除的 API	迁移到	主要变化
CronJob	**batch/v1beta1**	**batch/v1**	否
EndpointSlice	**discovery.k8s.io/v1beta1**	**discovery.k8s.io/v1**	是
事件	**events.k8s.io/v1beta1**	**events.k8s.io/v1**	是
HorizontalPodAutoscaler	**autoscaling/v2beta1**	**autoscaling/v2**	否
PodDisruptionBudget	**policy/v1beta1**	**policy/v1**	是
PodSecurityPolicy	**policy/v1beta1**	Pod Security Admission [1]	是
RuntimeClass	**node.k8s.io/v1beta1**	**node.k8s.io/v1**	否

1. 如需有关 OpenShift Container Platform 中 pod 安全准入的更多信息，请参阅了解和管理 pod 安全准入。

1.5.2.2. oc registry login 命令的空文件和 stdout 支持

oc registry login 命令的 **--registry-config** 和 **--to option** 选项现在停止接受空文件。这些选项将继续处理不存在的文件。将输出写入 **-** (stdout) 的功能也被删除。

1.5.2.3. 删除了对 OpenShift CLI (oc) 的 RHEL 7 支持

删除了在 OpenShift CLI (**oc**) 中使用 Red Hat Enterprise Linux (RHEL) 7 的支持。如果您在 RHEL 中使用 OpenShift CLI (**oc**)，则必须使用 RHEL 8 或更高版本。

1.5.2.4. OpenShift CLI (oc) 命令已被删除

本发行版本中删除了以下 OpenShift CLI(**oc**)命令：

- **oc adm migrate etcd-ttl**
- **oc adm migrate image-references**
- **oc adm migrate legacy-hpa**
- **oc adm migrate storage**

1.5.2.5. 从监控堆栈中删除的 Grafana 组件

Grafana 组件不再是 OpenShift Container Platform 4.12 监控堆栈的一部分。另外，也可进入 OpenShift Container Platform Web 控制台中的 **Observe → Dashboards** 来查看监控仪表板。

1.5.2.6. Prometheus 和 Grafana 用户界面访问从监控堆栈中删除

从 OpenShift Container Platform 4.12 监控堆栈中删除了对第三方 Prometheus 和 Grafana 用户界面的访问。另外，点 OpenShift Container Platform Web 控制台中的 **Observe** 来查看用于监控组件的警报、指标、仪表板和指标目标。

1.5.2.7. 删除了对虚拟硬件版本 13 的支持

在 OpenShift Container Platform 4.11 中，删除了对虚拟硬件版本 13 的支持。OpenShift Container Platform 4.9 中弃用了对虚拟硬件版本 13 的支持。红帽建议您使用虚拟硬件版本 15 或更高版本。

1.5.2.8. 删除了对 snapshot v1beta1 API 端点的支持

在 OpenShift Container Platform 4.11 中，删除了 **snapshot.storage.k8s.io/v1beta1** API 端点的支持。OpenShift Container Platform 4.7 中弃用了对 **snapshot.storage.k8s.io/v1beta1** API 端点的支持。红帽建议您使用 **snapshot.storage.k8s.io/v1**。所有以 **v1beta1** 创建的对象都可通过 v1 端点获得。

1.5.2.9. 删除了手动部署自定义调度程序的支持

此发行版本删除了手动部署自定义调度程序的支持。使用 Red Hat OpenShift 的 Secondary Scheduler Operator 代替在 OpenShift Container Platform 中部署自定义二级调度程序。

1.5.2.10. 删除了对使用 OpenShiftSDN 部署单节点 OpenShift 的支持

此发行版本删除了部署带有 OpenShiftSDN 的单节点 OpenShift 集群的支持。OVN-Kubernetes 是单节点 OpenShift 部署的默认网络解决方案。

1.5.2.11. 从安装有效负载中删除 Jenkins 镜像

- OpenShift Container Platform 4.11 将 "OpenShift Jenkins" 和 "OpenShift Agent Base" 镜像移到 **registry.redhat.io** 的 **ocp-tools-4** 存储库中，以便红帽可以在 OpenShift Container Platform 生命周期外生成和更新镜像。在以前的版本中，这些镜像位于 OpenShift Container Platform 安装有效负载以及 **registry.redhat.io** 的 **openshift4** 存储库中。如需更多信息，请参阅 OpenShift Jenkins。
- OpenShift Container Platform 4.11 从其有效负载中删除 "OpenShift Jenkins Maven" 和 "NodeJS Agent" 镜像。在以前的版本中，OpenShift Container Platform 4.10 弃用了这些镜像。红帽不再生成这些镜像，它们不能从 **registry.redhat.io** 的 **ocp-tools-4** 存储库中提供。

但是，升级到 OpenShift Container Platform 4.11 不会从 4.10 及更早的版本中删除 "OpenShift Jenkins Maven" 和 "NodeJS Agent" 镜像。红帽根据 OpenShift Container Platform 生命周期政策，通过 4.10 发行版本生命周期结束为这些镜像提供程序错误修正和支持。

如需更多信息，请参阅 OpenShift Jenkins。

1.5.3. 将来的 Kubernetes API 删除

OpenShift Container Platform 的下一个次发行版本将使用 Kubernetes 1.26。目前，Kubernetes 1.26 已计划删除几个已弃用的 API。

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

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

1.6. 程序错误修复

API 服务器和客户端

- 在以前的版本中，在收到 **workloadIsBeingUpdatedTooLong** 错误后，Cluster Authentication Operator 状态被设置为 **progressing = false**。同时，在定义 **inertia** 时保留了 **degraded = false**。因此，由于缩短的进度以及增加的降级时间会导致一个问题：**progressing = false** 和 **degraded = false** 会在还不成熟的情况下被设置。这会导致 OpenShift CI 测试出现不一致的情况（因为假定了一个不正确的健康状态）。这个问题已通过在返回 **workloadIsBeingUpdatedTooLong** 错误后删除 **progressing = false** 设置来解决。现在，因为没有 **progressing = false** 状态，OpenShift CI 测试更为一致。(BZ#2111842)

裸机硬件置备

- 在最近版本的服务器固件中，服务器操作之间的时间有所增加。当 OpenShift Container Platform 安装程序等待 Baseboard Management Controller (BMC) 的响应时，这会导致安装程序置备的基础架构安装过程中出现超时。新的 **python3-sushy** 发行版本会增加与 BMC 联系的服务器端尝试的数量。这个更新帐户会延长等待时间，并避免在安装过程中出现超时问题。(OCPBUGS-4097)

- 在此次更新之前，Ironic 置备服务不支持使用弱 eTags 和严格的 eTag 验证的 Baseboard Management Controller (BMC)。按照设计，如果 BMC 提供弱 eTag，Ironic 会返回两个 eTags：原始的 eTag 和原始 eTag 转换为强格式，以便与不支持弱 eTags 的 BMC 兼容性。虽然 Ironic 可以发送两个 eTags，但使用严格的 eTag 验证的 BMC 会拒绝此类请求，因为存在第二个 eTag。因此，在某些较旧的服务器硬件上，裸机置备会失败，并显示以下错误：**HTTP 412 Precondition Failed**。在 OpenShift Container Platform 4.12 及更新的版本中，如果提供了弱 eTag，则此行为更改和 Ironic 不再尝试发送两个 eTags。相反，如果 Redfish 请求依赖 eTag 验证错误，Ironic 使用已知临时解决方案重试请求。这可最小化具有严格 eTag 验证的机器上裸机置备失败的风险。(OCPBUGS-3479)

- 在此次更新之前，当 Redfish 系统具有 Settings URI 时，Ironic 置备服务总是尝试使用此 URI 来更改引导相关的 BIOS 设置。但是，如果 Baseboard Management Controller (BMC) 带有 Settings URI，但不支持使用此设置 URI 更改特定的 BIOS 设置，裸机置备会失败。在 OpenShift Container Platform 4.12 及更高版本中，如果系统具有 Settings URI，Ironic 会在继续操作前使用 Settings URI 来验证它是否可以更改特定的 BIOS 设置。否则，Ironic 使用 System URI 实现更改。此额外逻辑可确保 Ironic 可以应用与引导相关的 BIOS 设置更改，裸机置备可以成功。(OCPBUGS-2052)

Builds

- 默认情况下，Buildah 会输出日志文件的步骤，包括环境变量的内容，其中可能包括 构建输入 secret。虽然您可以使用 **--quiet** 构建参数来禁止打印这些环境变量，但如果使用 Source-to-image(S2I)构建策略，则此参数将不可用。当前发行版本解决了这个问题。要禁止打印环境变量，请在构建配置中设置 **BUILDAH_QUIET** 环境变量：

```
sourceStrategy:
...
  env:
    - name: "BUILDAH_QUIET"
      value: "true"
```

(BZ#2099991)

Cloud Compute

- 在以前的版本中，实例不会被设置为遵守自动重启的 GCP 基础架构默认选项。因此，可以在不使用基础架构默认自动重启的情况下创建实例。这有时意味着实例在 GCP 中终止，但相关机器仍然列在 **Running** 状态，因为它们不会自动重启。在这个版本中，传递自动重启选项的代码已被改进，以更好地检测并传递用户的默认选项选择。现在，实例会正确使用基础架构默认，并在用户请求默认功能时自动重启。(OCPBUGS-4504)

- **PodDisruptionBudget** 对象的 **v1beta1** 版本现在在 Kubernetes 中弃用。在这个版本中，对 **v1beta1** 的内部引用被 **v1** 替换。这个变化是集群自动扩展的内部，不需要用户操作，而不是 准备升级到 OpenShift Container Platform 4.12 Red Hat 知识库文章。(OCPBUGS-1484)

- 在以前的版本中，GCP 机器控制器每 10 小时协调机器状态。其他提供程序将此值设置为 10 分钟，以便在短时间内检测到 Machine API 系统之外的更改。GCP 的较长的协调周期可能会导致意外的问题，如缺少证书签名请求(CSR)批准，因为延长周期没有检测到外部 IP 地址。在这个版本中，GCP 机器控制器被更新来每 10 分钟协调一次与其他平台一致，以便更早地获取外部更改。(OCPBUGS-4499)

- 在以前的版本中，因为 Cluster Machine Approver Operator 的部署错误配置，启用 **TechPreviewNoUpgrade** 功能集会导致错误和 sporadic Operator 降级。因为启用了 **TechPreviewNoUpgrade** 功能集的集群使用 Cluster Machine Approver Operator 的两个实例，且两个部署都使用相同的端口集合，所以会出现单节点拓扑错误冲突。在这个版本中，Cluster Machine Approver Operator 部署被更新，为不同的部署使用不同的一组端口。(OCPBUGS-2621)

- 在以前的版本中，Azure 中的零功能扩展依赖于静态编译的实例类型列表，将实例类型的名称映射到 CPU 数量以及分配给实例类型的内存量。此列表随着时间的推移会变得过时。在这个版本中，有关实例类型大小的信息直接从 Azure API 动态收集，以防止列表过时。(OCPBUGS-2558)

- 在以前的版本中，Machine API 终止处理器 pod 不会在 spot 实例中启动。因此，如果实例终止，在污点 spot 实例上运行的 pod 不会收到终止信号。这可能会导致工作负载应用程序中丢失数据。在这个版本中，Machine API 终止处理器部署被修改为容许在带有污点的 spot 实例上运行的污点和容限，现在接收终止信号。(OCPBUGS-1274)

- 在以前的版本中，Azure 集群的错误消息没有说明无法为只使用内部发布策略的断开连接的安装使用公共 IP 地址创建新机器。在这个版本中，会更新错误消息以提高清晰性。(OCPBUGS-519)

- 在以前的版本中，Cloud Controller Manager Operator 不会检查 AWS 集群的 **cloud-config** 配置文件。因此，无法使用配置文件将额外的设置传递给 AWS 云控制器管理器组件。在这个版本中，Cloud Controller Manager Operator 会检查基础架构资源，并解析对 **cloud-config** 配置文件的引用，以便用户可以配置额外的设置。(BZ#2104373)

- 在以前的版本中，当 Azure 添加了新实例类型并在之前没有它的实例类型启用加速网络支持时，机器控制器中的 Azure 实例列表已过时。因此，机器控制器无法使用之前不支持加速网络的实例

类型创建机器，即使它们在 Azure 上支持此功能。在这个版本中，在创建机器前从 Azure API 检索所需的实例类型信息，以便机器控制器可以使用新的和更新实例类型创建机器。在这个版本中，还适用于将来添加的任何实例类型。(BZ#2108647)

- 在以前的版本中，在使用 Cluster API 供应商时，集群自动扩展不会考虑 CSI 驱动程序的 AWS、IBM Cloud 和 Alibaba Cloud 拓扑标签。因此，当在横向扩展事件期间尝试平衡节点时，自动扩展不会正确处理带有拓扑标签的节点。在这个版本中，自动扩展的自定义处理器被更新，以便遵循该标签。自动缩放器现在可以平衡由 AWS、IBM Cloud 或 Alibaba CSI 标签标记的类似节点组。(BZ#2001027)

- 在以前的版本中，Power VS 云供应商无法从 DHCP 服务器获取机器 IP 地址。更改 IP 地址不会更新节点，这会导致一些不一致，如待处理的证书签名请求。在这个版本中，Power VS 云提供商被更新为从 DHCP 服务器获取机器 IP 地址，以便节点的 IP 地址与计算机 IP 地址一致。(BZ#2111474)

- 在以前的版本中，无法在带有无效配置的 OpenShift Container Platform 早期版本中创建的机器被删除。在这个版本中，防止创建带有无效配置的机器的 Webhook 不再阻止删除现有的无效机器。现在，用户可以通过在这些机器上手动删除终结器来成功从其集群中删除这些机器。(BZ#2101736)

- 在以前的版本中，由 **NetworkManager** 不作为守护进程或连续模式运行导致的 DHCP 租期时间短短，从而导致机器在初始置备过程中卡住，永远不会成为集群中的节点。在这个版本中，会添加额外的检查，以便在机器处于这个状态下，它会被自动删除并自动重新创建。从 Machine API 控制器重启后，受此网络状况影响的机器可能会成为节点。(BZ#2115090)

- 在以前的版本中，当使用 IBM Cloud 中不存在的机器配置集创建新 **Machine** 资源时，机器会停留在 **Provisioning** 阶段。在这个版本中，验证被添加到 IBM Cloud Machine API 供应商中，以确保机器配置集存在，机器 API 会拒绝具有无效机器配置集的机器。(BZ#2062579)

- 在以前的版本中，AWS 的 Machine API 供应商不会验证机器规格中定义的安全组是否存在。本例中不使用返回错误，而是使用默认的安全组，它不应该用于 OpenShift Container Platform 机器，并在不通知用户使用默认组的情况下成功创建机器。在这个版本中，当用户在机器规格中设置不正确或空安全组名称时，Machine API 会返回错误。(BZ#2060068)

- 在以前的版本中，Machine API 供应商 Azure 不会将实例类型的用户提供值视为区分大小写。当实例类型正确但与问题单不匹配时，这会导致误报错误。在这个版本中，实例类型转换为小写字符，以便用户获得正确的结果，而不会为不匹配的情况产生假错误。(BZ#2085390)

- 在以前的版本中，在尝试访问对象前，机器对象的注解中没有检查 nil 值。这种情况罕见，但在协调机器时会导致机器控制器 panic。在这个版本中，会检查 nil 值，机器控制器可以在没有注解的情况下协调机器。(BZ#2106733)

- 在以前的版本中，集群 CPU 和内存用量的集群自动扩展指标永远不会达到或超过 **ClusterAutoscaler** 资源设定的限制。因此，因为资源限制，当集群自动扩展无法扩展时，不会触发警报。在这个版本中，向集群自动扩展添加了一个名为 **cluster_autoscaler_skipped_scale_events_count** 的新指标，以便更准确地检测达到或超过资源限值。现在，当集群自动扩展无法扩展集群时，警报将触发，因为它已达到集群资源限制。(BZ#1997396)

- 在以前的版本中，当 Machine API 供应商无法获取机器 IP 地址时，它不会设置内部 DNS 名称，机器证书签名请求不会被自动批准。在这个版本中，Power VS 计算机提供程序被更新，将服务器名称设置为内部 DNS 名称，即使它无法获取 IP 地址。(BZ#2111467)

- 在以前的版本中，Machine API vSphere 机器控制器在克隆虚拟机时设置 **PowerOn** 标志。这会创建一个 **PowerOn** 任务，表示机器控制器不知道。如果该 **PowerOn** 任务失败，机器会一直处于 **Provisioned** 阶段，但永远不会处于开机状态。在这个版本中，克隆序列会被修改以避免出现

这个问题。另外，机器控制器现在在失败时重试打开，并正确报告失败。(BZ#2087981, OCPBUGS-954)

- 在这个版本中，AWS 安全组会在创建后立即标记，而不是在创建后标记。这意味着向 AWS 发送较少的请求，所需的用户权限会降低。(BZ#2098054, OCPBUGS-3094)

- 在以前的版本中，如果在身份验证失败后尝试某些 RHOSP 操作，RHOSP 传统云供应商中的一个错误会导致崩溃。例如，关闭服务器会导致 Kubernetes 控制器管理器从 RHOSP 获取触发此错误的服务器信息。因此，如果初始云身份验证失败或者配置不正确，则关闭服务器会导致 Kubernetes 控制器管理器崩溃。在这个版本中，RHOSP 旧云供应商被更新为不会尝试任何 RHOSP API 调用（如果之前没有成功身份验证）。现在，关闭带有无效云凭证的服务器不再会导致 Kubernetes 控制器管理器崩溃。(BZ#2102383)

开发人员控制台

- 在以前的版本中，**openshift-config** 命名空间对 **HelmChartRepository** 自定义资源进行了硬编码，它是 **ProjectHelmChartRepository** 自定义资源的同一命名空间。这导致用户无法在其所需命名空间中添加私有 **ProjectHelmChartRepository** 自定义资源。因此，用户无法访问 **openshift-config** 命名空间中的 secret 和 configmap。在这个版本中修复了带有 **namespace** 字段的 **ProjectHelmChartRepository** 自定义资源定义，该字段可通过具有正确权限的用户从所选命名空间中读取 secret 和 configmap。另外，用户可以将 secret 和 configmap 添加到可访问的命名空间中，他们可以在使用创建资源的命名空间中添加私有 Helm Chart 仓库。(BZ#2071792)

镜像 Registry

- 在以前的版本中，镜像触发器控制器没有更改对象的权限。因此，镜像触发器注解无法在某些资源上工作。在这个版本中，会创建一个集群角色绑定，为控制器提供根据注解更新对象所需的权限。(BZ#2055620)

- 在以前的版本中，Image Registry Operator 对于 **node-ca** 守护进程集没有 **progressing** 条件，并使用来自一个不正确对象的 **generation**。因此，在 Operator 仍在运行时，**node-ca** 守护进程集可能会被标记为 **degraded**。在这个版本中添加了 **progressing** 条件，这表示安装没有完成。因此，Image Registry Operator 可以成功安装 **node-ca** 守护进程集，安装程序会等待它被完全部署。([BZ#2093440)

安装程序

- 在以前的版本中，支持的用户定义的标签数量是 8，保留的 OpenShift Container Platform 标签是 2 个用于 AWS 资源。在这个版本中，支持的用户定义标签的数量是 25，对于 AWS 资源，保留的 OpenShift Container Platform 标签为 25。现在，您可以在安装过程中最多添加 25 个用户标签。(CFE#592)

- 在以前的版本中，在 Amazon Web Services 上安装集群启动，然后在 IAM 管理用户没有分配 **s3:GetBucketPolicy** 权限时失败。在这个版本中，将此策略添加到清单中，安装程序用来确保分配了所有所需的权限。现在，安装程序会停止安装，并显示 IAM 管理用户缺少 **s3:GetBucketPolicy** 权限的警告。(BZ#2109388)

- 在以前的版本中，当 Azure DCasv5-series 或 DCadsv5-series 指定为 control plane 节点时，在 Microsoft Azure 上安装集群会失败。在这个版本中，安装程序会停止带有错误的安装，这代表 secret 虚拟机还不被支持。(BZ#2055247)

- 在以前的版本中，在 control plane 机器运行前，无法收集 bootstrap 日志。在这个版本中，收集 bootstrap 日志只需要 bootstrap 机器可用即可。(BZ#2105341)

- 在以前的版本中，如果因为服务帐户的权限不足而无法在 Google Cloud Platform 上安装，则生成的错误消息不在失败原因中提及这个问题。在这个版本中，错误消息进行了改进，它指示用户检查分配给服务帐户的权限。(BZ#2103236)

- 在以前的版本中，当 Google Cloud provider (GCP)上安装因为指定了无效的 GCP 区域时，生成的错误消息不会在失败原因中提及这个问题。这个版本改进了错误消息，它现在指出区域无效。(BZ#2102324)

- 在以前的版本中，如果 Hive 使用旧版本的 install-config.yaml 文件，使用 Hive 的集群安装可能会失败。在这个版本中，安装程序可以接受 Hive 提供的 **install-config.yaml** 文件的旧版本。(BZ#2098299)

- 在以前的版本中，如果 **apiVIP** 和 **ingressVIP** 参数以不同方式表示地址，则安装程序会错误地允许 apiVIP 和 ingressVIP 参数使用相同的 IPv6 地址，如以缩写格式列出地址。在这个版本中，无论格式是什么，安装程序可以正确地验证这两个参数，每个参数都需要单独的 IP 地址。(BZ#2103144)

- 在以前的版本中，如果集群名称超过 22 个字符，使用安装程序卸载集群将无法删除在 GCP 上安装的集群中的所有资源。在这个版本中，使用安装程序卸载集群会在长时间集群名称的情况下正确找到并删除所有 GCP 集群资源。(BZ#2076646)

- 在以前的版本中，当在带有 **machineNetwork** 参数中定义的多个网络的 Red Hat OpenStack Platform (RHOSP) 上安装集群时，安装程序只为第一个网络创建安全组规则。在这个版本中，安装程序会为 **machineNetwork** 中定义的所有网络创建安全组规则，以便用户在安装后不再需要手动编辑安全组规则。(BZ#2095323)

- 在以前的版本中，用户可以在 OpenStack 上安装集群时手动将 API 和 Ingress 虚拟 IP 地址设置为与 DHCP 服务器的分配池冲突的值。这可能导致 DHCP 服务器为新机器分配其中一个 VIP 地址，这无法启动。在这个版本中，安装程序会验证用户提供的 VIP 地址，以确保它们不会与任何 DHCP 池冲突。(BZ#1944365)

- 在以前的版本中，当使用嵌入在文件夹中的数据中心在 vSphere 上安装集群时，安装程序无法找到数据中心对象，从而导致安装失败。在这个版本中，安装程序可以遍历包含 datacenter 对象的目录，以便安装可以成功。(BZ#2097691)

- 在以前的版本中，当使用带有安装程序置备的基础架构的 arm64 架构在 Azure 上安装集群时，**hyperVGeneration** V1 的镜像定义资源会错误地具有 **x64** 的架构值。在这个版本中，**hyperVGeneration** V1 的镜像定义资源具有 **Arm64** 的正确架构值。(OCPBUGS-3639)

- 在以前的版本中，当在 VMware vSphere 上安装集群时，如果用户在 **install-config.yaml** 文件的 **failureDomain** 部分中指定了用户定义的文件夹，则安装可能会失败。在这个版本中，安装程序会在 **install-config.yaml** 文件的 **failureDomain** 部分中正确验证用户定义的文件夹。(OCPBUGS-3343)

- 在以前的版本中，当在 VMware vSphere 上安装失败后销毁部分部署的集群时，一些虚拟机文件夹不会被销毁。这个错误可能会在使用多个 vSphere 数据中心或多个 vSphere 集群配置的集群中发生。在这个版本中，在安装失败后销毁部分部署的集群时，所有安装程序置备的基础架构都会被正确删除。(OCPBUGS-1489)

- 在以前的版本中，当在 VMware vSphere 上安装集群时，如果用户指定了 **platform.vsphere.vcenters** 参数，则安装会失败，但没有在 **install-config.yaml** 文件中指定 **platform.vsphere.failureDomains.topology.networks** 参数。在这个版本中，安装程序会在指定 **platform.vsphere.vcenters** 时警告用户，在指定 platform.vsphere.vcenters 时需要 **platform.vsphere.failureDomains.topology.networks** 字段。(OCPBUGS-1698)

- 在以前的版本中，当在 VMware vSphere 上安装集群时，如果用户定义了 **platform.vsphere.vcenters** 和 **platform.vsphere.failureDomains** 参数，则安装会失败，但没有定义 **platform.vsphere.defaultMachinePlatform.zones** 或 **compute.platform.vsphere.zones** 和 **controlPlane.platform.vsphere.zones**。在这个版本中，安装程序会验证用户在安装前在多区域或多区部署中定义了 **zones** 参数。(OCPBUGS-1490)

Kubernetes Controller Manager

- 在以前的版本中，Kubernetes Controller Manager Operator 在没有监控堆栈存在的环境中报告 **degraded**。在这个版本中，Kubernetes Controller Manager Operator 会在监控堆栈不存在时跳过检查监控是否有降级的情况。(BZ#2118286)

- 在这个版本中，Kubernetes Controller Manager 警告 (**KubeControllerManagerDown**、**PodDisruptionBudgetAtLimit**、**PodDisruptionBudgetLimit** 和 **GarbageCollectorSyncFailed**) 带有指向 Github runbooks 的链接。runbooks 可帮助用户了解调试这些警报。(BZ#2001409)

Kubernetes 调度程序

- 在以前的版本中，在删除二级调度程序自定义资源后，二级调度程序部署不会被删除。因此，Second Schedule Operator 和 Operand 没有被完全卸载。在这个版本中，在二级调度程序自定义资源中设置了正确的所有者引用，以便它指向二级调度程序部署。因此，当删除二级调度程序自定义资源时，从属调度程序部署会被删除。(BZ#2100923)

- 对于 OpenShift Container Platform 4.12 发行版本，descheduler 现在可将事件发布到 API 组，因为发行版本为 descheduler 的配置集添加了额外的基于角色的访问控制 (RBAC) 规则。(OCPBUGS-2330)

Machine Config Operator

- 在以前的版本中，只有在 Operator 的守护进程同步成功时，才会同步 Machine Config Operator (MCO)包含重要证书的 **ControllerConfig** 资源。按照设计，守护进程同步期间的未就绪节点阻止守护进程同步成功，因此未就绪的节点间接阻止 **ControllerConfig** 资源，因此这些证书无法同步。这会导致因为无法轮转 **ControllerConfig** 资源中包含的证书而出现未就绪节点时集群降级。在这个版本中，**ControllerConfig** 资源的同步不再依赖于守护进程同步成功，因此如果守护进程同步失败，**ControllerConfig** 资源现在可以继续同步。这意味着，未就绪节点不再阻止 **ControllerConfig** 资源同步，因此即使存在未就绪节点，证书也会继续更新。(BZ#2034883)

管理控制台

- 在以前的版本中，**Operator** 详情页会尝试显示多个错误消息，但错误消息组件一次只能显示一个错误消息。因此，不会显示相关的错误消息。在这个版本中，**Operator** 详情页面只显示第一个错误消息，以便用户看到相关错误。(OCPBUGS-3927)

- 在以前的版本中，Azure Red Hat OpenShift 的产品名在 Customer Case Management (CCM) 中不正确。因此，控制台必须使用相同的不正确的产品名称来正确地填充 CCM 中的字段。更新 CCM 中的产品名称后，还需要更新控制台。在这个版本中，与 CCM 相同的产品名称会在控制台的链接后面使用正确的 Azure 产品名称正确填充。(OCPBUGS-869)

- 在以前的版本中，当插件页面出现错误时，在离开错误页面时，错误不会被重置，在进入到一个不是造成错误的页面时，错误仍会保留。在这个版本中，当用户进入到新页面时，错误状态将重置为默认值，错误将不再在新页面中被保留。(BZ#2117738, OCPBUGS-523)

- 在以前的版本中，当选择了 ***All Namespaces*** 时，安装的 **Operator** 的 **Operator** 详情 栏中的 ***View it here*** 链接被错误地构建。因此，在 **All Projects** 中的集群服务版本（CSV）的 **Operator** 详情页面的链接是一个无效的路由。在这个版本中，到安装 CVS 的命名空间的 ***View it here*** 链接现在会被正确构建，链接可以正常工作。(OCPBUGS-184)

- 在以前的版本中，带有超过五个数字的行号会导致一个显示问题，行号覆盖了行号和行内容之间的垂直划分器，使得读起来变得更加困难。在这个版本中，行号可用的空间量增加到不再有行号，行号不再覆盖垂直划分器。(OCPBUGS-183)

- 在以前的版本中，在 Web 控制台的管理员视角中，在 **Cluster Settings** 页面中的 **Default update server** 弹出窗口中的 ***Learn more about the OpenShift local update services*** 链接会产生 404 错误。在这个版本中，这个链接可以正常工作。(BZ#2098234)

- 在以前的版本中，**MatchExpression** 组件没有考虑数组类型值。因此，使用这个组件通过表单只能输入单个值。在这个版本中，**MatchExpression** 组件接受以逗号分隔的值作为数组。(BZ#207690)

- 在以前的版本中，对模型进行冗余检查会导致重新载入标签页，偶尔会导致标签页内容被重新渲染。在这个版本中，删除了冗余模型检查，模型只检查一次。因此，标签内容不会波动，不再重新渲染。(BZ#2037329)

- 在以前的版本中，当从 OpenShift Dedicated 节点页面中的操作列表中选择 **edit** 标签时，不会请求响应，并返回 Web hook 错误。这个问题已被解决，因此只有在编辑失败时才会返回错误消息。(BZ#2102098)

- 在以前的版本中，如果问题处于待处理状态，点 **Insights** 链接会使页面崩溃。作为临时解决方案，您可以在点 **Insights** 链接前等待变量变为 **initialized**。因此，Insights 页面会如预期打开。(BZ#2052662)

- 在以前的版本中，当 **MachineConfigPool** 资源暂停时，用于取消暂停 **Resume rollouts** 的选项。现在，信息已被更新，现在为 **Resume updates**。(BZ#2094240)

- 在以前的版本中，在计算 master 和 worker 节点时使用了错误的计算方法。在这个版本中，当节点同时具有 **master** 和 worker 角色时，会计算正确的 **worker** 节点。(BZ#1951901)

- 在以前的版本中，**ImageManifestVuln** 的 **react-router** 路由冲突会导致尝试呈现带有 **~new** 名称的 **ImageManifestVuln** 的详情页面。现在，容器安全插件已被更新以删除冲突路由，并确保 Operator 详情页面中使用动态列表和详情页面扩展。因此，控制台会显示 **ImageManifestVuln** 的正确创建、列表和详情页。(BZ#2080260)

- 在以前的版本中，不完整的 YAML 不会同步。偶尔会向用户显示不完整的 YAML。在这个版本中，同步的 YAML 始终会显示。(BZ#2084453)

- 在以前的版本中，当安装需要创建自定义资源 (CR) 的 Operator 以供使用时，**Create resource** 按钮可能无法安装 CR，因为它指向不正确的命名空间。在这个版本中，**Create resource** 按钮可以正常工作。(BZ#2094502)

- 在以前的版本中，**Cluster update** 模态无法正确显示错误。因此，**Cluster update** 模态在出现错误时不会显示或解释它们。在这个版本中，**Cluster update** 模态可以正确地显示错误。(BZ#2096350)

监控

- 在此次更新之前，因为一个调度问题，集群管理员无法区分 pod 未就绪，因为它无法通过 kubelet 启动。在这两种情况下，**KubePodNotReady** 警报都会触发。在这个版本中，**KubePodNotScheduled** 警报会在 pod 未就绪时触发，而 **KubePodNotReady** 警报会在 pod 未就绪时触发，因为 kubelet 无法启动它。(OCPBUGS-4431)

- 在此次更新之前，**node_exporter** 将报告有关虚拟网络接口的指标，如 **tun** 接口、**br** 接口和 **ovn-k8s-mp** 接口。在这个版本中，这些虚拟接口的指标将不再收集，这减少了监控资源消耗。(OCPBUGS-1321)

- 在此次更新之前，Alertmanager pod 启动可能会因为 DNS 解析较慢而超时，Alertmanager pod 不会启动。在这个版本中，超时值增加到七分钟，这可防止 pod 启动超时。(BZ#2083226)

- 在此次更新之前，如果 Prometheus Operator 运行或调度 Prometheus pod，系统不会提供失败的底层原因。在这个版本中，如果 Prometheus pod 没有运行或调度，Cluster Monitoring

Operator 会使用故障原因更新 **clusterOperator** 监控状态，这可用于排除底层问题。(BZ#2043518)

- 在此次更新之前，如果您从 OpenShift Container Platform Web 控制台中的 **Developer** 视角创建了警报静默，则会包括与警报不匹配的外部标签。因此，警报不会被静默。在这个版本中，在 **Developer** 视角中创建静默时，外部标签会被排除，以便新创建的静默可以正常工作。(BZ#2084504)

- 在以前的版本中，如果您启用了专用于用户定义的项目的 Alertmanager 实例，在某些情况下可能会出现错误配置，您也不会告知用户定义的项目 Alertmanager 配置映射设置不会加载 Alertmanager 的主实例或专用于用户定义的项目的实例。在这个版本中，如果发生此错误配置，Cluster Monitoring Operator 现在会显示一个信息，告知您问题并提供解决步骤。(BZ#2099939)

- 在此次更新之前，如果 Cluster Monitoring Operator (CMO)无法更新 Prometheus，CMO 不会验证以前的部署是否在运行，并报告集群监控是否仍在运行，即使其中一个 Prometheus pod 仍在运行。在这个版本中，CMO 检查在这种情况下运行 Prometheus pod，并在没有 Prometheus pod 运行时报告集群监控不可用。(BZ#2039411)

- 在此次更新之前，如果您将 OpsGenie 配置为警报接收器，日志中会出现 **api_key** 和 **api_key_file** 相互排斥的警告，并且 **api_key** 具有优先权。即使您没有定义 **api_key_file**，也会出现这个警告。在这个版本中，只有在您定义了 **api_key** 和 **api_key_file** 时，这个警告才会出现在日志中。(BZ#2093892)

- 在此次更新之前，Telemeter Client (TC) 仅在手动重启时载入新的 pull secret。因此，如果 pull secret 已更改或更新，且 TC 尚未重启，则 TC 无法与服务器进行身份验证。在这个版本中解决了这个问题，以便在 secret 被轮转时，部署会自动重启，并使用更新的令牌进行身份验证。(BZ#2114721)

网络

- 在以前的版本中，处于 terminating 状态的路由器会延迟 **oc cp** 命令，这会延迟 **oc adm must-gather** 命令直到 pod 终止为止。在这个版本中，会为每个发出的 **oc cp** 命令设置一个超时，以防止延迟 **must-gather** 命令运行。因此，终止 pod 不再延迟 **must-gather** 命令。(BZ#2103283)

- 在以前的版本中，Ingress Controller 无法同时配置 **Private** 端点发布策略类型和 PROXY 协议。在这个版本中，用户可以使用 **Private** 端点发布策略类型和 PROXY 协议配置 Ingress Controller。(BZ#2104481)

- 在以前的版本中，**routeSelector** 参数在路由器部署前清除 Ingress Controller 的路由状态。因此，路由状态会错误地重新填充。为了避免使用过时的数据，路由状态检测已被更新，不再依赖于 Kubernetes 对象缓存。另外，这个更新还包括一个修复，用于检查路由部署时的生成 ID，以确定路由状态。因此，路由状态使用 **routeSelector** 更新一致清除。(BZ#2101878)

- 在以前的版本中，从早于 4.8 的 OpenShift Container Platform 版本升级的集群可能会有孤立的 **Route** 对象。这是因为早期版本的 OpenShift Container Platform 将 **Ingress** 对象转换为 **Route** 对象，而与给定 **Ingress** 对象的指示 **IngressClass** 无关。在这个版本中，在 Ingress-to-Route 转换后，集群管理员会发送一个有关集群中任何孤立 Route 对象的警报。在这个版本中，添加了另一个警报，通知集群管理员有关没有指定 **IngressClass** 的 Ingress 对象。(BZ#1962502)

- 在以前的版本中，如果没有创建路由器部署所依赖的 **configmap**，则路由器部署不会进行。在这个版本中，如果默认入口控制器部署正在进行，集群 Operator 会报告 **ingress progressing=true**。这会导致用户使用 **oc get co** 命令调试 ingress 控制器的问题。(BZ#2066560)

- 在以前的版本中，当将错误创建的网络策略添加到 OVN-Kubernetes 缓存中时，会导致 OVN-Kubernetes 领导进入 **crashloopbackoff** 状态。在这个版本中，OVN-Kubernetes 领导不会通过跳过删除 nil 策略来进入 **crashloopbackoff** 状态。(BZ#2091238)

- 在以前的版本中，在删除具有相同命名空间或名称的 60 秒内重新创建带有相同命名空间的 EgressIP pod，从而导致配置错误的 SNAT。因此，数据包可能会没有 nodeIP 而不是 EgressIP SNAT。在这个版本中，流量会将 pod 保留为 EgressIP 而不是 nodeIP。(BZ#2097243)。

- 在以前的版本中，由于 ACL 中的从 **arp** 到 **arp ll nd** 的更改，会导致带有 **arp** 的旧的访问控制列表 (ACL) 出现一个 **unexpectedly found multiple equivalent ACLs (arp v/s arp||nd)** 错误。这导致网络策略被正确创建。在这个版本中，只有 **arp** 匹配的旧 ACL 已被删除，以便只有带有新的 **arp ll nd** 匹配项的 ACL 才能正确创建网络策略，且不会在 **ovnkube-master** 上出现错误。注意：这会影响客户从旧版本升级到 4.8.14、4.9.32、4.10.13 或更高版本。(BZ#2095852)。

- 在这个版本中，CoreDNS 更新至 1.10.0 版本，它基于 Kubernetes 1.25。这会保留 CoreDNS 版本和 OpenShift Container Platform 4.12，它也基于 Kubernetes 1.25，并与另一个版本保持一致。(OCPBUGS-1731)

- 在这个版本中，OpenShift Container Platform 路由器使用 **k8s.io/client-go** 版本 1.25.2，它支持 Kubernetes 1.25。这会保留 **openshift-router** 和 OpenShift Container Platform 4.12，它也基于 Kubernetes 1.25，并相互保持一致。(OCPBUGS-1730)

- 在这个版本中，Ingress Operator 使用 **k8s.io/client-go** 版本 1.25.2，它支持 Kubernetes 1.25。这会保留 Ingress Operator 和 OpenShift Container Platform 4.12，它也基于 Kubernetes 1.25，并相互保持一致。(OCPBUGS-1554)

- 在以前的版本中，DNS Operator 不会协调 **openshift-dns** 命名空间。由于 OpenShift Container Platform 4.12 需要 **openshift-dns** 命名空间具有 pod-security 标签，这会导致在集群更新时缺少命名空间。如果没有 pod-security 标签，pod 无法启动。在这个版本中，DNS Operator 会协调 **openshift-dns** 命名空间，现在 pod-security 标签存在。因此，pod 会如预期启动。(OCPBUGS-1549)

- 在以前的版本中，**ingresscontroller.spec.tuniningOptions.reloadInterval** 不支持十进制数字作为有效的参数值，因为 Ingress Operator 内部将指定的值转换为毫秒，这是不被支持的时间单位。这导致 Ingress Controller 被删除。在这个版本中，**ingresscontroller.spec.tuningOptions.reloadInterval** 现在支持十进制数字，用户可以删除之前不支持的带有 **reloadInterval** 参数值的 Ingress Controller。(OCPBUGS-236)

- 在以前的版本中，Cluster DNS Operator 使用基于 Kubernetes 1.24 的 GO Kubernetes 库，而 OpenShift Container Platform 4.12 基于 Kubernetes 1.25。在这个版本中，GO Kubernetes API 是 v1.25.2，它将 Cluster DNS Operator 与使用 Kubernetes 1.25 API 的 OpenShift Container Platform 4.12 保持一致。（链接：OCPBUGS-1558）

- 在以前的版本中，当重新创建 **network-operator** pod 时，将 **disableNetworkDiagnostics** 配置设置为 **true** 不会被持久保留。在这个版本中，network'operator.openshift.io/cluster 的 **disableNetworkDiagnostics** 配置属性在 network operator 重启后不再重置为默认值。(OCPBUGS-392)

- 在以前的版本中，**ovn-kubernetes** 没有在 **br-ex** 网桥中配置绑定接口的正确 MAC 地址。因此，对主 Kubernetes 接口使用绑定的节点无法加入集群。在这个版本中，**ovn-kubernetes** 配置 **br-ex** 网桥中绑定接口的正确 MAC 地址，并为主 Kubernetes 接口使用绑定的节点成功加入集群。(BZ2096413)

- 在以前的版本中，当 Ingress Operator 配置为启用 mTLS 时，Operator 不会检查 CRL 是否需要更新，直到有些其他事件导致它协调。因此，用于 mTLS 的 CRL 可能已过时。在这个版本中，Ingress Operator 会在任何 CRL 过期时自动协调，并在其 **nextUpdate** 字段指定的时间更新 CRL。(BZ#2117524)

节点

- 在以前的版本中，符号链接错误消息被输出为原始数据，而不是将其格式化为错误，因此很难理解。在这个版本中，错误消息被正确格式化，以便可以轻松地理解。(BZ#1977660)

- 在以前的版本中，当将性能配置集应用到节点时，kubelet 硬驱除阈值与 Kubernetes 默认值不同。在这个版本中，默认值已更新，以匹配预期的 Kubernetes 默认值。(OCPBUGS-4362)。

OpenShift CLI (oc)

- 当目标命名空间缺少适当的安全级别时，OpenShift Container Platform 4.12 发行版本解决了在目标节点上输入 debug 会话的问题。这会导致 **oc** CLI 提示您输入 pod 安全错误消息。如果现有命名空间不包含适当的安全级别，OpenShift Container Platform 现在会在目标节点上进入 **oc** debug 模式时创建一个临时命名空间。(OCPBUGS-852)

- 在以前的版本中，在 macOS arm64 架构中，需要手动签名 **oc** 二进制文件。因此，**oc** 二进制文件无法按预期工作。在这个版本中，实现了一个自签发的二进制，用于对应 **oc**。因此，macOS arm64 构架中的 **oc** 二进制文件可以正常工作。(BZ#2059125)

- 在以前的版本中，**must-gather** 会尝试收集服务器上不存在的资源。因此，**must-gather** 会输出错误信息。现在，在收集资源前，**must-gather** 会检查资源是否存在。因此，当在服务器中收集不存在的资源时，**must-gather** 不再打印错误。(BZ#2095708)

- OpenShift Container Platform 4.12 发行版本更新了 **oc-mirror** 库，以便库可以支持多架构平台镜像。这意味着，在镜像一个平台发行有效负载时，您可以从更广泛的架构中进行选择，如 **arm64**。(OCPBUGS-617)

Operator Lifecycle Manager (OLM)

- 在 OpenShift Container Platform 4.12 版本前，**package-server-manager** 控制器不会恢复对 **package-server** 集群服务版本(CSV) 所做的任何更改，因为 **on-cluster** 功能存在问题。这些持久性更改可能会影响 Operator 在集群中启动的方式。对于 OpenShift Container Platform 4.12，**package-server-manager** 控制器始终将 **package-server** CSV 重建到其原始状态，因此在集群升级操作后，对 CSV 的修改不会保留。**on-cluster** 功能不再控制 **package-server** CSV 的状态。(OCPBUGS-867)

- 在以前的版本中，Operator Lifecycle Manager (OLM)会尝试更新命名空间以应用标签，即使命名空间中存在该标签。因此，更新请求会增加 API 和 etcd 服务的工作负载。在这个版本中，OLM 在发布更新前将现有标签与命名空间中预期的标签进行比较。因此，OLM 不再尝试对命名空间进行不必要的更新请求。(BZ#2105045)

- 在以前的版本中，Operator Lifecycle Manager (OLM) 可防止因 **ClusterVersion** 自定义资源的 **spec.DesiredVersion** 字段错误地计算不应阻断的次版本集群升级。在这个版本中，当应该支持升级时，OLM 不再阻止集群升级。(BZ#2097557)

- 在以前的版本中，协调器会在不生成资源副本的情况下更新资源的注解。这会导致一个终止协调器进程的错误。在这个版本中，协调器不再因为错误而停止。(BZ#2105045)

- **package-server-manifest** (PSM) 是一个控制器，可确保在集群中安装正确的 **package-server** Cluster Service Version (CSV)。在以前的版本中，因为在协调功能中存在一个逻辑错误 (on-cluster 对象可能会影响预期的对象)，所以对 **package-server** CSV 的更改没有被恢复。用户可能会对 **package-server** CSV 进行了修改，这些修改不会被恢复。另外，集群升级不会更新 **package-server** CSV 的 YAML。在这个版本中，预期的 CSV 版本总是从头开始构建，这删除了 on-cluster 对象对预期值的影响。因此，PSM 现在会恢复对 **package-server** CSV 的任何修改尝试，集群升级现在会部署预期的 **package-server** CSV。(OCPBUGS-858)

- 在以前的版本中，OLM 会根据 Operator 的 CRD 状态升级 Operator。CRD 根据 group/version/kind (GVK) 标识符定义的顺序列出组件引用。共享同一组件的 Operator 可能会导

致 GVK 更改 Operator 的组件列表，这会导致 OLM 需要更多系统资源来持续更新 CRD 的状态。在这个版本中，Operator Lifecycle Manager (OLM) 会根据 Operator 组件引用升级 Operator。对 Operator 的自定义资源定义(CRD) 状态的更改不会影响 OLM Operator 升级过程。(OCPBUGS-3795)

Operator SDK

- 在这个版本中，您可以通过在 pod 规格中包含 **securityContext** 配置字段来为 registry pod 设置安全上下文。这将为 pod 中的所有容器应用安全上下文。**securityContext** 字段还定义 pod 的权限。(BZ#2091864)

File Integrity Operator

- 在以前的版本中，File Integrity Operator 使用 Operator 权限中的 **openshift-file-integrity** 命名空间部署模板。当 Operator 试图在命名空间中创建对象时，因为权限问题会失败。在这个版本中，OLM 使用的部署资源被更新为使用正确的命名空间，修复权限问题，以便用户可以在非默认命名空间中安装和使用 Operator。(BZ#2104897)

- 在以前的版本中，File Integrity Operator 的底层依赖项改变了警报和通知是如何处理的，Operator 不会发送指标。在这个版本中，Operator 确保指标端点正确，并在启动时可访问。(BZ#2115821)

- 在以前的版本中，File Integrity Operator 发布的警报没有设置命名空间。这使得用户难以了解警报来自哪里，或者负责发出该警报的组件。在这个版本中，Operator 会在警报中包含它安装到的命名空间，以便更轻松地缩小组件需要注意的内容。(BZ#2101393)

- 在以前的版本中，File Integrity Operator 在升级过程中无法正确处理修改警报。因此，警报不包括安装 Operator 的命名空间。在这个版本中，Operator 会在警报中包含它安装到的命名空间，以便更轻松地缩小组件需要注意的内容。(BZ#2112394)

- 在以前的版本中，因为底层 OLM 更新导致 File Integrity Operator 的服务帐户所有权，从 0.1.24 到 0.1.29 的更新无法正常工作。在这个版本中，Operator 默认为升级到 0.1.30。(BZ#2109153)

- 在以前的版本中，File Integrity Operator 守护进程使用 **ClusterRoles** 参数而不是 **Roles** 参数进行最新的权限更改。因此，OLM 无法更新 Operator。在这个版本中，Operator 守护进程会恢复到使用 **Roles** 参数，并从旧版本更新到 0.1.29 版本。(BZ#2108475)

Compliance Operator

- 在以前的版本中，Compliance Operator 使用 Operator SDK 的旧版本，这是构建 Operator 的依赖项。这会导致 Operator SDK 使用的已弃用 Kubernetes 功能的警报。在这个版本中，Compliance Operator 更新至 0.1.55 版本，其中包括 Operator SDK 的更新版本。(BZ#2098581)

- 在以前的版本中，为 **rhcos4-high-master-sysctl-kernel-yama-ptrace-scope** 和 **rhcos4-sysctl-kernel-core-pattern** 规则应用自动补救会导致后续这些规则失败，即使它们已被修复。这个版本解决了这个问题。(BZ#2094382)

- 在以前的版本中，Compliance Operator 硬编码通知到 default 命名空间。因此，如果 Operator 安装在不同的命名空间中，则不会出现来自 Operator 的通知。这个版本解决了这个问题。(BZ#2060726)

- 在以前的版本中，当在没有 Ignition 规格的情况下解析机器配置时，Compliance Operator 无法获取 API 资源。这会导致 **api-check-pods** 检查崩溃循环。在这个版本中，Compliance Operator 被更新为在没有 Ignition 规格的情况下安全地处理机器配置池。(BZ#2117268)

- 在以前的版本中，Compliance Operator 将机器配置处于卡住状态，因为它无法决定机器配置和 kubelet 配置之间的关系。这是因为机器配置名称的假设不正确。在这个版本中，Compliance Operator 可以确定 kubelet 配置是否是机器配置的一个子集。(BZ#2102511)

OpenShift API 服务器

- 在以前的版本中，添加成员可能会从组中删除以前的成员。因此，用户会丢失组特权。在这个版本中，依赖项已被禁止，用户不再丢失组特权。(OCPBUGS-533)

Red Hat Enterprise Linux CoreOS (RHCOS)

- 在以前的版本中，升级到 Podman 4.0 会阻止用户使用 RHCOS 上带有 toolbox 容器的自定义镜像。在这个版本中更新了 toolbox 库代码来考虑新的 Podman 行为，因此用户现在可以按预期使用带有 toolbox 的自定义镜像。(BZ#2048789)

- 在以前的版本中，**podman exec** 命令无法与嵌套容器正常工作。用户在使用 **oc debug** 命令访问节点时遇到这个问题，然后使用 **toolbox** 命令运行容器。因此，用户无法在 RHCOS 上重复使用 toolbox。在这个版本中更新了 toolbox 库代码来考虑此行为，因此用户现在可以在 RHCOS 上重复使用 toolboxes。(BZ#1915537)

- 在这个版本中，运行 **toolbox** 命令会在启动容器前检查默认镜像的更新。这提高了安全性，并为用户提供最新的程序错误修复。(BZ#2049591)

- 在以前的版本中，升级到 Podman 4.0 会阻止用户在 RHCOS 上运行 **toolbox** 命令。在这个版本中更新了 toolbox 库代码来考虑新的 Podman 行为，因此用户现在可以按预期在 RHCOS 上运行 **toolbox**。(BZ#2093040)

- 在以前的版本中，**rpm-ostree** 不支持自定义 SELinux 策略模块，因此不会在更新后与系统的其余部分一起更新。这在不相关的组件中可能会出现故障。待处理的 SELinux 用户空间的改进将包括在以后的 OpenShift Container Platform 版本中，在这个版本中，为 RHCOS 提供了一个临时解决方案，它将根据需要在引导时重建和重新载入 SELinux 策略。(OCPBUGS-595)

可伸缩性和性能

- tuned 配置集已被修改，会为在当前的 Red Hat Enterprise Linux (RHEL) 内核补丁中新添加的、针对每个特定 CPU 的 kthreads (**ktimers**) 分配相同的优先级作为 **ksoftirqd** 和 **rcuc**。如需更多信息，请参阅 OCPBUGS-3475, BZ#2117780 和 BZ#2122220。

- 在以前的版本中，重启 **tuned** 服务会导致 **irqbalance** 配置不正确，从而导致在隔离的 CPU 上再次提供 IRQ 操作，从而违反隔离保证。在这个版本中，**irqbalance** 服务配置会在 **tuned** 服务重启后（因为被明确请求或因为错误）被正确保留，因此保留的 CPU 隔离保证会满足 IRQ 服务。(OCPBUGS-585)

- 在以前的版本中，当 tuned 守护进程因为 Cluster Node Tuning Operator 的一部分而重启时，会重置中断处理程序的 CPU 关联性，并导致调优被破坏。在这个版本中，tuned 中的 **irqbalance** 插件被禁用，OpenShift Container Platform 现在依赖于 **CRI-O** 和 **irqbalance** 间的逻辑和交互。(BZ#2105123)

- 在以前的版本中，当节点有负载时，为每个新的 **veth** 设备所执行的低延迟 hook 脚本用时过长。这会在 pod 启动事件期间累积延迟，从而导致 **kube-apiserver** 的推出部署时间较慢，有时会超过 5 分钟的推出部署的超时设置。在这个版本中，容器启动时间应该会比较短且在 5 分钟阈值中。(BZ#2109965)。

- 在以前的版本中，**oslat** 控制线程与其中一个测试线程共存，这会导致测量的延迟激增。在这个版本中，**oslat** 运行程序为控制线程保留一个 CPU，这意味着测试使用较少的 CPU 来运行忙碌的线程。(BZ#2051443)

- 延迟测量工具（也称为 **oslat**、**cyclictest** 和 **hwlatdetect**）现在在完全隔离的 CPU 上运行，且没有在后台运行 helper 进程（这会而导致延迟激增），从而提供了更准确的延迟测量。(OCPBUGS-2618)

- 在以前的版本中，虽然 **group-du-sno-ranGen.yaml** 的引用 **PolicyGenTemplate** 包含了两个 **StorageClass** 条目，但生成的策略仅包含一个。在这个版本中，生成的策略包括这两个策略。(BZ#2049306)。

存储

- 在以前的版本中，检查通用临时卷会失败。在这个版本中，检查可扩展卷现在包括通用临时卷。(BZ#2082773)

- 在以前的版本中，如果 vSphere 有多个 secret，vSphere CSI Operator 会随机选择一个 secret，并有时会导致 Operator 重启。在这个版本中，当 vCenter CSI Operator 中有多个 secret 时会出现一个警告。(BZ#2108473)

- 在以前的版本中，当 Container Storage Interface (CSI) 驱动程序无法从节点卸载卷时，OpenShift Container Platform 会分离卷。CSI 规格不允许在不卸载的情况下分离卷，驱动可能会进入 **undocumented** 状态。在这个版本中，CSI 驱动程序仅在不健康节点上卸载前被分离，从而防止出现 **undocumented** 的状态。(BZ#2049306)

- 在以前的版本中，Manila CSI Driver Operator 的 VolumeSnapshotClass 缺少注解。因此，Manila CSI 快照无法找到 secret，无法使用默认 VolumeSnapshotClass 创建快照。在这个版本中解决了这个问题，secret 名称和命名空间包含在默认的 VolumeSnapshotClass 中。现在，用户可以使用默认的 VolumeSnapshotClass 在 Manila CSI Driver Operator 中创建快照。(BZ#2057637)

- 用户现在可以选择在 Azure File 上使用实验性 VHD 功能。要选择它，用户必须在存储类中指定 **fstype** 参数，并使用 **--enable-vhd=true** 启用它。如果使用 **fstype**，且功能没有设为 **true**，则卷将无法置备。
要不使用 VHD 功能，请从存储类中删除 **fstype** 参数。(BZ#2080449)

- 在以前的版本中，如果 vSphere 有多个 secret，vSphere CSI Operator 会随机选择一个 secret，并有时会导致 Operator 重启。在这个版本中，当 vCenter CSI Operator 中有多个 secret 时会出现一个警告。(BZ#2108473)

Web 控制台 (开发者视角)

- 在以前的版本中，用户无法在添加和编辑表单中取消选择 Git secret。因此，必须重新创建资源。在这个版本中，添加选项以在所选 secret 选项列表中选择 **No Secret** 解决了这个问题。因此，用户可以轻松选择、取消选择或分离任何附加的 secret。(BZ#2089221)

- 在 OpenShift Container Platform 4.9 中，当开发者视角中只有非常少的数据或没有数据，大多数监控图表 (CPU 消耗、内存用量和带宽) 会显示 -1 到 1 范围内的数据。但是这些值都不能低于零。这将在以后的发行版本中解决。(BZ#1904106)

- 在此次更新之前，当部署用户定义的 Alertmanager 服务时，用户无法在 OpenShift Container Platform Web 控制台的开发者视角中静默警报，因为 Web 控制台会将请求转发到 **openshift-monitoring** 命名空间中的平台 Alertmanager 服务。在这个版本中，当您在 web 控制台中查看 **Developer** 视角并尝试静默警报时，请求会被转发到正确的 Alertmanager 服务。(OCPBUGS-1789)

- 在以前的版本中，**Add Helm Chart Repositories** 表单中有一个已知问题来扩展项目的 Developer Catalog。**Quick Start** 指南显示您可以在所需命名空间中添加 **ProjectHelmChartRepository** CR，但没有提到需要从 kubeadmin 执行这个权限。这个问题已解决，现在 **Quickstart** 提到了创建 **ProjectHelmChartRepository** CR 的正确步骤。(BZ#2057306)

1.7. 技术预览功能

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

技术预览功能支持范围

在以下表格中，功能被标记为以下状态：

- *技术预览*
- *公开发行*
- *不可用*
- *已弃用*

网络功能虚拟化功能

表 1.13. 网络技术预览跟踪器

功能	4.10	4.11	4.12
PTP 单 NIC 硬件配置为边界时钟	技术预览	公开发行	公开发行
PTP dual NIC 硬件配置为边界时钟	不可用	技术预览	技术预览
带有边界时钟的 PTP 事件	技术预览	公开发行	公开发行
二级网络的 Pod 级别绑定	公开发行	公开发行	公开发行
外部 DNS Operator	技术预览	公开发行	公开发行
AWS Load Balancer Operator	不可用	技术预览	技术预览
Ingress Node Firewall Operator	不可用	不可用	技术预览
通过 BGP 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	不可用	技术预览	公开发行
通过 L2 模式，使用节点的一个子集（由特定的 IP 地址池指定）中的 MetalLB 服务进行广告	不可用	技术预览	技术预览
SR-IOV 网络的多网络策略	不可用	不可用	技术预览
更新特定于接口的安全 sysctl 列表	不可用	不可用	技术预览
MT2892 系列 [ConnectX-6 Dx] SR-IOV 支持	不可用	不可用	技术预览
MT2894 系列 [ConnectX-6 Lx] SR-IOV 支持	不可用	不可用	技术预览

功能	4.10	4.11	4.12
ConnectX-6 NIC 模式的 MT42822 BlueField-2 的 SR-IOV 支持	不可用	不可用	技术预览
Silicom STS 系列的 SR-IOV 支持	不可用	不可用	技术预览
MT2892 系列 [ConnectX-6 Dx] OvS Hardware Offload 支持	不可用	不可用	技术预览
MT2894 系列 [ConnectX-6 Lx] OvS Hardware Offload 支持	不可用	不可用	技术预览
ConnectX-6 NIC 模式的 MT42822 BlueField-2 的 OvS Hardware Offload 支持	不可用	不可用	技术预览
将 Bluefield-2 从 DPU 切换到 NIC	不可用	不可用	技术预览

存储技术预览功能

表 1.14. 存储技术预览

功能	4.10	4.11	4.12
共享资源 CSI 驱动程序和 OpenShift 构建中的 CSI 卷	技术预览	技术预览	技术预览
CSI 卷扩展	技术预览	公开发行	公开发行
CSI Azure File Driver Operator	技术预览	公开发行	公开发行
CSI Google Filestore Driver Operator	不可用	不可用	技术预览
CSI 自动迁移 (Azure 文件、VMware vSphere)	技术预览	技术预览	技术预览
CSI 自动迁移（Azure Disk、OpenStack Cinder）	技术预览	公开发行	公开发行
CSI 自动迁移 (AWS EBS、GCP 磁盘)	技术预览	技术预览	公开发行
CSI inline 临时卷	技术预览	技术预览	技术预览
CSI 通用临时卷	不可用	公开发行	公开发行
共享资源 CSI 驱动程序	技术预览	技术预览	技术预览
CSI Google Filestore Driver Operator	不可用	不可用	技术预览
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

安装技术预览功能

表 1.15. 安装技术预览

功能	4.10	4.11	4.12
使用 kvc 向节点添加内核模块	技术预览	技术预览	技术预览
IBM Cloud VPC 集群	技术预览	技术预览	公开发行
可选择 Cluster Inventory	技术预览	技术预览	技术预览
多架构计算机器	不可用	技术预览	技术预览
使用 oc-mirror CLI 插件断开连接镜像镜像	技术预览	公开发行	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
基于代理的 OpenShift Container Platform 安装程序	不可用	不可用	公开发行
AWS Outposts 平台	不可用	不可用	技术预览

节点技术预览功能

表 1.16. 节点技术预览

功能	4.10	4.11	4.12
非抢占优先级类	技术预览	技术预览	技术预览
Node Health Check Operator	技术预览	公开发行	公开发行
Linux Control Group 版本 2 (cgroup v2)	不可用	不可用	技术预览
crun 容器运行时	不可用	不可用	技术预览

多架构技术预览功能

表 1.17. 多架构技术预览

功能	4.10	4.11	4.12
x86_64 架构上的 **kdump**	技术预览	公开发行	公开发行
arm64 构架上的 **kdump**	不可用	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

功能	4.10	4.11	4.12
IBM zSystems 和 LinuxONE 上的 IBM Secure Execution	不可用	不可用	技术预览

Serverless 技术预览功能

表 1.18. Serverless 技术预览跟踪程序

功能	4.10	4.11	4.12
无服务器功能	技术预览	技术预览	技术预览

专用硬件和驱动程序启用技术预览功能

表 1.19. 专用硬件和驱动程序启用技术预览

功能	4.10	4.11	4.12
驱动程序工具包	技术预览	技术预览	公开发行
Special Resource Operator (SRO)	技术预览	技术预览	不可用
hub 和 spoke 集群的支持	不可用	不可用	技术预览

Web 控制台技术预览功能

表 1.20. Web 控制台技术预览跟踪程序

功能	4.10	4.11	4.12
多集群控制台	技术预览	技术预览	技术预览
动态插件	技术预览	技术预览	公开发行

可扩展性和性能技术预览功能

表 1.21. 可扩展性和性能技术预览

功能	4.10	4.11	4.12
超线程感知 CPU Manager 策略	技术预览	技术预览	技术预览
Node Observability Operator	不可用	技术预览	技术预览
factory-precaching-cli 工具	不可用	不可用	技术预览

功能	4.10	4.11	4.12
使用 GitOps ZTP 将 worker 节点添加到单节点 OpenShift 集群	不可用	不可用	技术预览
Topology Aware Lifecycle Manager (TALM)	技术预览	技术预览	公开发行
挂载命名空间封装	不可用	不可用	技术预览

Operator 技术预览功能

表 1.22. Operator 技术预览

功能	4.10	4.11	4.12
混合 Helm Operator	技术预览	技术预览	技术预览
基于 Java 的 Operator	不可用	技术预览	技术预览
Node Observability Operator	不可用	不可用	技术预览
Network Observability Operator	不可用	不可用	公开发行
平台 Operator	不可用	不可用	技术预览
RukPak	不可用	不可用	技术预览
Cert-manager Operator	技术预览	技术预览	技术预览

监控技术预览功能

表 1.23. 监控技术预览

功能	4.10	4.11	4.12
用户定义的项目监控的警报路由	技术预览	公开发行	公开发行
基于平台监控指标的警报规则	不可用	技术预览	技术预览

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

表 1.24. RHOSP 技术预览

功能	4.10	4.11	4.12
支持 RHOSP DCN	技术预览	技术预览	技术预览

功能	4.10	4.11	4.12
支持 RHOSP 上集群的外部云供应商	技术预览	技术预览	公开发行
RHOSP 上集群的 OVS 硬件卸载	技术预览	公开发行	公开发行

架构技术预览功能

表 1.25. 架构技术预览

功能	4.10	4.11	4.12
在裸机上托管 OpenShift Container Platform 的 control plane	不可用	不可用	技术预览
在 Amazon Web Services (AWS) 上托管 OpenShift Container Platform 的 control plane。	不可用	技术预览	技术预览

机器管理技术预览功能

表 1.26. 机器管理技术预览

功能	4.10	4.11	4.12
使用 Cluster API 管理机器	不可用	技术预览	技术预览
Cron job 时区	不可用	不可用	技术预览
Alibaba Cloud 的云控制器管理器	技术预览	技术预览	技术预览
Amazon Web Services 的云控制器管理器	技术预览	技术预览	技术预览
Google Cloud Platform 的云控制器管理器	技术预览	技术预览	技术预览
Microsoft Azure 的云控制器管理器	技术预览	技术预览	技术预览
Red Hat OpenStack Platform(RHOSP)的云控制器管理器	技术预览	技术预览	公开发行
VMware vSphere 的云控制器管理器	技术预览	技术预览	技术预览
自定义 Metrics Autoscaler Operator	不可用	技术预览	技术预览

1.8. 已知问题

- 在 OpenShift Container Platform 4.1 中，匿名用户可以访问发现端点。之后的版本会取消对这端点的访问，以减少可能的安全漏洞攻击面。一些发现端点被转发到聚合的 API 服务器。但是，升级的集群中会保留未经身份验证的访问，因此现有用例不会中断。

如果您是一个从 OpenShift Container Platform 4.1 升级到 4.12 的集群的集群管理员，您可以撤销或继续允许未经身份验证的访问。除非对未经身份验证的访问有特殊需要，否则您应该撤销它。如果您继续允许未经身份验证的访问，请注意相关的风险。

警告

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

使用以下脚本撤销对发现端点的未经身份验证的访问：

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

此脚本从以下集群角色绑定中删除未经身份验证的对象：

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

(BZ#1821771)

- 在有些情况下，IBM Cloud VPC 集群可能无法安装，因为有些 worker 机器没有启动。相反，这些 worker 机器保留在 **Provisioned** 阶段。
  这个问题有一个临时解决方案。在执行初始安装的主机上，删除失败的机器并再次运行安装程序。

  1. 验证 master API 服务器的内部应用负载均衡器 (ALB) 的状态是 **active**。
     a. 运行以下命令识别集群的基础架构 ID：

     ```
     $ oc get infrastructure/cluster -ojson | jq -r '.status.infrastructureName'
     ```

     b. 登录到集群的 IBM Cloud 帐户，并以集群的正确区域为目标。
     c. 运行以下命令验证内部 ALB 状态是否为 **active** ：

```
$ ibmcloud is lb <cluster_ID>-kubernetes-api-private  --output json | jq -r
'.provisioning_status'
```

2. 运行以下命令，识别处于 **Provisioned** 阶段的机器：

```
$ oc get machine -n openshift-machine-api
```

输出示例

```
NAME                                PHASE        TYPE      REGION    ZONE       AGE
example-public-1-x4gpn-master-0     Running      bx2-4x16  us-east   us-east-1  23h
example-public-1-x4gpn-master-1     Running      bx2-4x16  us-east   us-east-2  23h
example-public-1-x4gpn-master-2     Running      bx2-4x16  us-east   us-east-3  23h
example-public-1-x4gpn-worker-1-xqzzm  Running      bx2-4x16  us-east   us-east-1
22h
example-public-1-x4gpn-worker-2-vg9w6  Provisioned  bx2-4x16  us-east   us-east-2
22h
example-public-1-x4gpn-worker-3-2f7zd  Provisioned  bx2-4x16  us-east   us-east-3
22h
```

3. 运行以下命令来删除每个失败的机器：

```
$ oc delete machine <name_of_machine> -n openshift-machine-api
```

4. 等待已删除的 worker 机器被替换，最多可能需要 10 分钟。

5. 运行以下命令，验证新 worker 机器是否处于 **Running** 阶段：

```
$ oc get machine -n openshift-machine-api
```

输出示例

```
NAME                                PHASE    TYPE      REGION    ZONE       AGE
example-public-1-x4gpn-master-0     Running  bx2-4x16  us-east   us-east-1  23h
example-public-1-x4gpn-master-1     Running  bx2-4x16  us-east   us-east-2  23h
example-public-1-x4gpn-master-2     Running  bx2-4x16  us-east   us-east-3  23h
example-public-1-x4gpn-worker-1-xqzzm  Running  bx2-4x16  us-east   us-east-1  23h
example-public-1-x4gpn-worker-2-mnlsz  Running  bx2-4x16  us-east   us-east-2
8m2s
example-public-1-x4gpn-worker-3-7nz4q  Running  bx2-4x16  us-east   us-east-3
7m24s
```

6. 运行以下命令来完成安装。再次运行安装程序可确保正确初始化集群的 **kubeconfig** ：

```
$ ./openshift-install wait-for install-complete
```

(OCPBUGS#1327)

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

- 由于在某些镜像索引中包含旧镜像，运行 **oc adm catalog mirror** 和 **oc image mirror** 可能会导致以下错误： **error: unable to retrieve source image**。作为临时解决方案，您可以使用 **--skip-**

missing 选项绕过错误并继续下载镜像索引。如需更多信息，请参阅 Service Mesh Operator 镜像失败。

- 在 RHOSP 上的 OpenShift Container Platform 中使用出口 IP 地址功能时，您可以将浮动 IP 地址分配给保留端口，以便为出口流量具有可预测的 SNAT 地址。浮动 IP 地址关联必须由安装 OpenShift Container Platform 集群的同一用户创建。否则，由于权限不足，出口 IP 地址的任何删除或移动操作都会无限期挂起。发生此问题时，具有足够特权的用户必须手动取消设置浮动 IP 地址关联来解决这个问题。(OCPBUGS-4902)

- Nutanix 安装中存在一个已知问题：如果您使用带有 Prism Central 2022.x 的 4096 位证书，则安装会失败。反之，使用 2048 位证书。(KCS)

- 删除双向转发检测 (BFD) 配置集并删除添加到边框网关协议 (BGP) 对等资源中的 **bfdProfile** 不会禁用 BFD。相反，BGP 对等点开始使用默认的 BFD 配置集。要从 BGP peer 资源禁用 BFD，请删除 BGP 对等配置，并在没有 BFD 配置集的情况下重新创建它。(BZ#2050824)

- 由于一个未解析的元数据 API 问题，您无法在 RHOSP 16.1 上安装使用裸机 worker 的集群。RHOSP 16.2 上的集群不受此问题的影响。(BZ#2033953)

- 不支持 **loadBalancerSourceRanges** 属性，因此会被忽略，在 RHOSP 上运行的集群中的负载均衡器类型服务中，并使用 OVN Octavia 供应商。这个问题还没有临时解决方案。(OCPBUGS-2789)

- 目录源更新后，OLM 需要时间来更新订阅状态。这意味着，当 Topology Aware Lifecycle Manager (TALM) 决定是否需要补救时，订阅策略的状态可能会继续显示为合规。因此，在订阅策略中指定的 Operator 不会进行升级。作为临时解决方案，请在目录源策略的 **spec** 部分包含一个 **status** 字段，如下所示：

```
metadata:
  name: redhat-operators-disconnected
spec:
  displayName: disconnected-redhat-operators
  image: registry.example.com:5000/disconnected-redhat-operators/disconnected-redhat-operator-index:v4.11
status:
  connectionState:
    lastObservedState: READY
```

  这可减少 OLM 拉取新索引镜像并使 pod 就绪的延迟，从而减少目录源策略补救和订阅状态更新之间的时间。如果问题仍然存在，且订阅策略状态更新仍较晚，您可以使用相同的订阅策略应用另一个 **ClusterGroupUpdate** CR，或者具有不同名称相同的 **ClusterGroupUpdate** CR。(OCPBUGS-2813)

- 如果所有选择的集群在 **ClusterGroupUpdate** CR 启动后，TALM 会跳过补救策略。使用修改后的目录源策略和同一 **ClusterGroupUpdate** CR 中的订阅策略更新 Operator 不会被完成。订阅策略会被跳过，因为它仍然合规，直到强制实施目录源更改。作为临时解决方案，请在 **common-subscription** 策略中添加以下对 CR 的更改，例如：

```
metadata.annotations.upgrade: "1"
```

  这会在 **ClusterGroupUpdate** CR 开始前使策略不合规。(OCPBUGS-2812)

- 在单节点 OpenShift 实例上，重新引导而不排空节点以删除所有正在运行的 pod 可能会导致工作负载容器恢复出现问题。重启后，工作负载会在所有设备插件就绪前重启，从而导致资源不可用或在错误的 NUMA 节点上运行的工作负载。当所有设备插件在重启恢复过程中重新注册时，可以重启工作负载 pod。(OCPBUGS-2180)

- 默认 **dataset_comparison** 目前为 **ieee1588**。推荐的 dataset_comparison 是 **G.8275.x**。计划在以后的 OpenShift Container Platform 版本中修复。在短期内，您可以手动更新 ptp 配置，使其包含推荐的 **dataset_comparison**。(OCPBUGS-2336)

- 默认 **step_threshold** 是 0.0。推荐的 **step_threshold** 是 2.0。计划在以后的 OpenShift Container Platform 版本中修复。在短期内，您可以手动更新 ptp 配置，使其包含推荐的 **step_threshold**。(OCPBUGS-3005)

- **BMCEventSubscription** CR 无法在 ACM 部署的多集群环境中为 spoke 集群创建 Redfish 订阅，其中 metal3 服务只在 hub 集群上运行。解决方法是通过直接调用 Redfish API 来创建订阅，例如运行以下命令：

```
curl -X POST -i --insecure -u "<BMC_username>:<BMC_password>"
https://<BMC_IP>/redfish/v1/EventService/Subscriptions \
   -H 'Content-Type: application/json' \
   --data-raw '{
   "Protocol": "Redfish",
   "Context": "any string is valid",
   "Destination": "https://hw-event-proxy-openshift-bare-metal-
events.apps.example.com/webhook",
   "EventTypes": ["Alert"]
   }'
```

  您应该会收到 **201 Created** 响应和一个带有 **Location: /redfish/v1/EventService/Subscriptions/<sub_id>** 的标头，它表示成功创建了 Redfish 事件订阅。(OCPBUGSM-43707)

- 当使用 GitOps ZTP 管道在断开连接的环境中安装单节点 OpenShift 集群时，应该在集群中应用两个 **CatalogSource** CR。**CatalogSource** CR 中的一个会在多个节点重启后删除。作为临时解决方案，您可以更改目录源的默认名称，如 **certified-operators** 和 **redhat-operators**。(OCPBUGSM-46245)

- 如果在用于执行集群升级的订阅策略中指定无效的订阅频道，则 Topology Aware Lifecycle Manager 会在策略强制后显示成功升级，因为 **Subscription** 状态保持 **AtLatestKnown**。(OCPBUGSM-43618)

- 当应用到集群中的多个节点时，**SiteConfig** 磁盘分区定义会失败。当使用 **SiteConfig** CR 置备紧凑集群时，在多个节点上创建一个有效的 **diskPartition** 配置会失败，并显示 Kustomize 插件错误。(OCPBUGSM-44403)

- 如果当前禁用了安全引导，且尝试使用 ZTP 来启用它，集群安装不会启动。当通过 ZTP 启用安全引导时，引导选项会在附加虚拟 CD 前进行配置。因此，从现有的硬盘引导时会打开安全引导。集群安装会卡住，因为系统永远不会从 CD 启动。(OCPBUGSM-45085)

- 使用 Red Hat Advanced Cluster Management (RHACM)，当虚拟介质在将镜像写入磁盘后没有断开 ISO 时，Dell PowerEdge R640 服务器上的 spoke 集群部署会被阻止。作为临时解决方案，请通过 iDRAC 控制台中的 Virtual Media 选项卡手动断开 ISO。(OCPBUGSM-45884)

- 依赖于高分辨率计时器的低延迟应用程序来唤醒线程可能会遇到比预期更高的延迟。虽然预期的唤醒延迟时间为 20us，但运行 cyclictest 工具的 cyclictest 工具时可能会看到超过这个值的延迟 (24 小时或更长)。测试表明，对于抽样的 99.999999%，唤醒延迟都低于 20us。(RHELPLAN-138733)

- Intel 的 Chapman Beach NIC 必须安装在 bifurcated PCIe 插槽中，以确保两个端口都可见。RHEL 8.6 中的当前 devlink 工具中也存在一个限制，这会阻止在 bifurcated PCIe 插槽中配置 2 个端口。(RHELPLAN-142458)

- 当端口停机时禁用 SR-IOV VF 可能会导致 Intel NIC 的 3-4 秒延迟。(RHELPLAN-126931)
- 使用 Intel NIC 时，当为 SR-IOV VF 分配 IPV6 地址时，IPV6 流量会停止。(RHELPLAN-137741)
- 当使用 VLAN 剥离卸载时，使用 iavf 驱动程序无法正确设置卸载标记 (**ol_flag**)。(RHELPLAN-141240)
- 如果分配在 ice 驱动程序的配置更改期间失败，则可能会出现死锁。(RHELPLAN-130855)
- 使用 Intel NIC 时，SR-IOV VF 会发送带有错误 MAC 地址的 GARP 数据包。(RHELPLAN-140971)
- 当使用 GitOps ZTP 方法管理集群并删除还没有完成安装的集群时，hub 集群上的集群命名空间清理可能会无限期地挂起。要完成命名空间删除，请从集群命名空间中的两个 CR 中删除 **baremetalhost.metal3.io** finalizer：

  1. 从 BareMetalHost CR **.spec.bmc.credentialsName** 指向的 secret 中删除终结器。
  2. 从 **BareMetalHost** CR 中删除终结器。当从命名空间中删除这些终结器时，终止会在几秒钟内完成。(OCPBUGS-3029)

- 在 OCP 4.12 中添加了一个新功能，使 UDP GRO 也会使所有 veth 设备为每个可用的 CPU 都有一个 RX 队列（以前每个 veth 都有一个队列）。这些队列由 OVN 动态配置，延迟调整和此队列创建之间没有同步。延迟调优逻辑监控 veth NIC 创建事件，并在所有队列被正确创建前开始配置 RPS 队列 cpu 掩码。这意味着没有配置某些 RPS 队列掩码。因为不是所有 NIC 队列都正确配置，实时应用程序（使用对时间敏感的 cpu 与其它容器中的服务进行通信）可能会有延迟激增的问题。不使用内核网络堆栈的应用程序不会受到影响。(OCPBUGS-4194)
- 平台 Operator 和 RukPak 的已知问题：
  - 删除平台 Operator 会导致删除底层资源。这个级联删除逻辑只能删除基于 Operator Lifecycle Manager (OLM) Operator 的捆绑格式中定义的资源。如果平台 Operator 创建在捆绑格式之外定义的资源，则平台 Operator 负责处理这个清理交互。在将 cert-manager Operator 安装为平台 Operator 时，可以观察此行为，然后将其删除。预期的行为是，命名空间保留在 cert-manager Operator 创建后。
  - 平台 Operator 管理器没有比较集群范围的 **BundleDeployment** 资源的当前状态和所需状态的逻辑。这使得有足够基于角色的访问控制(RBAC)的用户无法手动修改底层 **BundleDeployment** 资源，并可能导致用户将其权限升级到 **cluster-admin** 角色的情况。默认情况下，您应该将对此资源的访问权限限制为明确需要访问的少量用户。在这个技术预览版本中，**BundleDeployment** 资源唯一支持的客户端是平台 Operator 管理器组件。
  - OLM 的 Marketplace 组件是一个可禁用的可选集群功能。这在技术预览版本中有影响，因为平台 Operator 目前只从由 Marketplace 组件管理的 **redhat-operators** 目录源提供。作为临时解决方案，集群管理员可以手动创建此目录源。
  - RukPak 置备程序实施无法检查它们管理的资源的健康状态。这代表，生成的 **BundleDeployment** 资源状态会出现在拥有它的 **PlatformOperator** 资源。如果 **registry+v1** 捆绑包包含可成功应用到集群的清单，但在运行时会失败，如引用不存在的镜像的 **Deployment** 对象，则结果会反映到单个 **PlatformOperator** 和 **BundleDeployment** 资源中。
  - 集群管理员在创建集群前配置 **PlatformOperator** 时，无法轻松确定所需的软件包名称，需要参考一个已存在的集群或参考产品文档中的示例。没有适当的验证逻辑可以确保单独配置的 **PlatformOperator** 资源能够成功推出集群。

- 当在 oc-mirror CLI 插件中使用技术预览 OCI 功能时，镜像目录会嵌入所有 Operator 捆绑包，而不是仅在镜像设置配置文件中指定的那些上过滤。(OCPBUGS-5085)

- 您运行基于 Agent 的 OpenShift Container Platform 安装程序时，存在一个已知问题：从上一发行版本的生成 ISO 镜像生成 ISO 镜像。此时会显示一条错误消息，并显示与发行版本不匹配。作为临时解决方案，请创建并使用新目录。(OCPBUGS#5159)

- **install-config.yaml** 文件中定义的功能不适用于基于 Agent 的 OpenShift Container Platform 安装。目前，还没有临时解决方案。(OCPBUGS#5129)

- 使用 OVN 驱动程序创建的 RHOSP 上完全填充的负载均衡器可以包含处于待处理创建状态的池。此问题可能会导致 RHOSP 上部署的集群出现问题。要解决这个问题，更新您的 RHOSP 软件包。(BZ#2042976)

- RHOSP 上的批量负载平衡器成员更新对于 **PUT** 请求可能会返回 500 代码 。此问题可能会导致 RHOSP 上部署的集群出现问题。要解决这个问题，更新您的 RHOSP 软件包。(BZ#2100135)

- 使用外部云供应商的集群在轮转后无法检索更新的凭证。以下平台会受到影响：

  - Alibaba Cloud
  - IBM Cloud VPC
  - IBM Power
  - OpenShift Virtualization
  - RHOSP

  作为临时解决方案，请运行以下命令重启 **openshift-cloud-controller-manager** pod：

  ```
  $ oc delete pods --all -n openshift-cloud-controller-manager
  ```

  (OCPBUGS-5036)

- 当 **cloud-provider-openstack** 尝试使用 API 在 OVN 负载均衡器上创建健康监控器时，存在一个已知问题。这些运行状况监视器会处于 **PENDING_CREATE** 状态。删除后，关联的负载均衡器会处于 **PENDING_UPDATE** 状态。没有临时解决方案。(BZ#2143732)

- 由于一个已知问题，要使用在 RHOSP 上运行的集群的有状态 IPv6 网络，您必须在 worker 节点的内核参数中包含 **ip=dhcp,dhcpv6**。(OCPBUGS-2104)

- 当虚拟功能(VF)已存在时，无法在物理功能(PF)上创建 macvlan。此问题会影响 Intel E810 NIC。(BZ#2120585)

- 目前，在 IPv4 OpenShift Container Platform 集群中手动配置 IPv6 地址和路由时存在一个已知问题。当转换为双栈集群时，新创建的 pod 会保留在 **ContainerCreating** 状态。目前，还没有临时解决方案。计划在以后的 OpenShift Container Platform 发行版本中解决这个问题。(OCPBUGS-4411)

- 当在 IBM Public Cloud 上安装的 OVN 集群有 60 个 worker 节点时，同时创建 2000 或更多服务和路由对象可能会导致同时创建的 pod 处于 **ContainerCreating** 状态。如果发生这个问题，输入 **oc describe pod <podname>** 命令会显示带有以下警告信息的事件：**FailedCreatePodSandBox...failed to configure pod interface: timed out waiting for OVS port binding (ovn-installed)**。当前没有解决此问题的方法。(OCPBUGS-3470)

- 当在使用 OVN-Kubernetes 网络供应商的集群中替换 control plane 机器时，与 OVN-

Kubernetes 相关的 pod 可能无法在替换的机器上启动。当发生这种情况时，新机器上缺少网络会阻止 etcd 替换旧机器。因此，集群会处于这个状态，并可能会降级。当 control plane 被手动替换或被 control plane 机器集替换 时，可能会发生此行为。
目前还没有临时解决方案来解决这个问题。要避免这个问题，禁用 control plane 机器集，如果集群使用 OVN-Kubernetes 网络供应商，则不要手动替换 control plane 机器。(**OCPBUGS-5306**)

1.9. 异步勘误更新

OpenShift Container Platform 4.12 的安全更新、程序漏洞修正、功能增强更新将会通过红帽网络以异步勘误的形式发布。所有的 OpenShift Container Platform 4.12 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 4.12 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.12.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-2022:7399 - OpenShift Container Platform 4.12.0 镜像发行版本、程序错误修正和安全更新公告

发布于：2023 年 1 月 17 日

OpenShift Container Platform release 4.12.0 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-2022:7399 公告中。此更新中包括的 RPM 软件包由 RHSA-2022:7398 公告提供。

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

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 4.12.0 --pullspecs
```

1.9.1.1. 功能

1.9.1.1.1. 二级网络的 pod 级别绑定的正式发布

在这个版本中，使用 pod 级别绑定已正式发布。

1.9.2. RHSA-2023:0449 - OpenShift Container Platform 4.12.1 程序错误修复和安全更新

发布于：2022 年 1 月 30 日

OpenShift Container Platform 版本 4.12.1 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-2023:0449 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:0448 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.12.1 --pullspecs
```

1.9.2.1. 程序错误修复

- 在以前的版本中，由于 OpenStack 云供应商中的一个错误检查，负载均衡器会在所有 Octavia 负载均衡器被创建时填充外部 IP 地址。这会增加处理负载均衡器的时间。在这个版本中，负载均衡器仍然按顺序创建，外部 IP 地址会逐一填充。(OCPBUGS-5403)
- 在以前的版本中，当无法访问 Swift 时，**cluster-image-registry-operator** 会默认使用持久性卷声明(PVC)。在这个版本中，无法连接到 Red Hat OpenStack Platform (RHOSP) API 或其他事件失败，从而导致 **cluster-image-registry-operator** 重试探测。在重试过程中，只有在正确找到 RHOSP 目录且不包含对象存储时，才会默认为 PVC；或者，如果 RHOSP 目录存在，并且当前用户没有列出容器的权限。(OCPBUGS-5154)

1.9.2.2. 更新

要将现有 OpenShift Container Platform 4.12 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.9.3. RHSA-2023:0569 - OpenShift Container Platform 4.12.2 程序错误修复和安全更新

发布于：2023 年 2 月 7 日

OpenShift Container Platform release 4.12.2 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-2023:0569 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:0568 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.12.2 --pullspecs
```

1.9.3.1. 更新

要将现有 OpenShift Container Platform 4.12 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.9.4. RHSA-2023:0728 - OpenShift Container Platform 4.12.3 程序错误修复和安全更新

发布于：2023 年 2 月 16 日

OpenShift Container Platform release 4.12.3 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2023:0728 公告中。此更新中包括的 RPM 软件包由 RHSA-2023:0727 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.12.3 --pullspecs
```

1.9.4.1. 程序错误修复

- 在以前的版本中，当在使用 OVN-Kubernetes 网络供应商的集群中替换 control plane 机器时，与 OVN-Kubernetes 相关的 pod 有时不会在替换机器上启动，并阻止 etcd 替换旧的机器。在这个版本中，与 OVN-Kubernetes 相关的 pod 会如预期在替换机器中启动。(OCPBUGS-6494)

1.9.4.2. 更新

要将现有 OpenShift Container Platform 4.12 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.9.5. RHSA-2023:0769 - OpenShift Container Platform 4.12.4 程序错误修复和安全更新

发布于：2023 年 2 月 20 日

OpenShift Container Platform release 4.12.4 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-2023:0769 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:0768 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.12.4 --pullspecs
```

1.9.5.1. 更新

要将现有 OpenShift Container Platform 4.12 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.9.6. RHSA-2023:0890 - OpenShift Container Platform 4.12.5 程序错误修复和安全更新

发布于：2023 年 2 月 28 日

OpenShift Container Platform release 4.12.5 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-2023:0890 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:0889 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.12.5 --pullspecs
```

1.9.6.1. 程序错误修复

- 在以前的版本中，在仓库列表中，您只能在状态为 **Succeeded** 或 **Failed** 时看到 PipelineRuns，当状态为 **Running** 时。在这个版本中，当触发 **PipelineRuns** 时，您可以在仓库列表中看到状态为 **Running**。(OCPBUGS-6816)

- 在以前的版本中，当创建 **Secret** 时，**Start Pipeline** 模型会创建一个无效的 JSON 值，因此 Secret 不可用，**PipelineRun** 可能会失败。在这个版本中，**Start Pipeline** 模型会为 **Secret** 创建有效的 JSON 值。现在，您可以在启动管道时创建有效的 Secret。(OCPBUGS-6671)

- 在以前的版本中，当 **BindableKinds** 资源没有状态时，Web 控制台会崩溃、获取并在循环中显示相同的数据。在这个版本中，您可以将 **BindableKinds** 资源状态数组设置为 **[]**，预期它在没有 status 字段的情况下存在。因此，网页浏览器或应用程序不会崩溃。(OCPBUGS-4072)

- 在以前的版本中，当从 OpenShift Container Platform 中删除一个 Knative (**kn**) 服务时，关联的 **<kn-service-name>-github-webhook-secret** 不会被删除。在这个版本中，所有相关 Webhook secret 都会被删除。现在，您可以创建一个与已删除名称相同的 Knative (**kn**) 服务。(OCPBUGS-7437)

1.9.6.2. 更新

要将现有 OpenShift Container Platform 4.12 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.9.7. RHSA-2023:1034 - OpenShift Container Platform 4.12.6 程序错误修复和安全更新

发布于：2023 年 3 月 7 日

OpenShift Container Platform release 4.12.6 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 RHBA-2023:1034 公告中。此更新中包括的 RPM 软件包由 RHSA-2023:1033 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.12.6 --pullspecs
```

1.9.7.1. 更新

要将现有 OpenShift Container Platform 4.12 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。

1.9.8. RHBA-2023:1163 - OpenShift Container Platform 4.12.7 程序错误修复更新

发布于：2023 年 3 月 13 日

OpenShift Container Platform release 4.12.7 现已正式发布。其程序错误修正列表包括在 RHBA-2023:1163 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:1162 公告提供。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.12.7 --pullspecs
```

1.9.8.1. 更新

要将现有 OpenShift Container Platform 4.12 集群更新到此最新版本，请参阅使用 CLI 更新集群 以获取相关说明。