OpenShift Container Platform 4.14

发行注记

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

Last Updated: 2025-10-23

OpenShift Container Platform 4.14 发行注记

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

Legal Notice

Abstract

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

Table of Contents

第 1 章 OPENSHIFT CONTAINER PLATFORM 4.14 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-2023:5006)现已正式发布。此发行版本使用 Kubernetes 1.27 和 CRI-O 运行时。OpenShift Container Platform 4.14 的新功能、改变以及已知的问题包括在此文档中。

OpenShift Container Platform 4.14 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 Container Platform 集群部署到内部环境或云环境中。

OpenShift Container Platform 4.14 在 Red Hat Enterprise Linux (RHEL) 8.6 及以后的 RHEL 8 版本中被支持，它在 OpenShift Container Platform 4.14 生命周期结束前发布。OpenShift Container Platform 4.14 在 Red Hat Enterprise Linux CoreOS (RHCOS) 4.14 上也支持。要了解 RHCOS 使用的 RHEL 版本，请参阅 Red Hat Enterprise Linux CoreOS (RHCOS)和 OpenShift Container Platform 的 RHEL 版本 （知识库文章）。

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

对于 **x86_64** 架构上的 OpenShift Container Platform 4.12，红帽添加了一个 6 个月的延长更新支持 (EUS) 阶段，将总生命周期从 18 个月延长至 24 个月。对于在 64 位 ARM (**aarch64**)、IBM Power®(**ppc64le**) 和 IBM Z®(**s390x**) 架构上运行的 OpenShift Container Platform 4.12，EUS 生命周期将保持 18 个月。

从 OpenShift Container Platform 4.14 开始，在所有支持的构架中，包括 **x86_64**、64 位 ARM (**arch64**)、IBM Power® (**ppc64le**) 和 IBM Z® (**s390x**) 架构的 EUS 阶段，总的生命周期为 24 个月。

从 OpenShift Container Platform 4.14 开始，红帽提供了一个为期 12 个月的额外 EUS 附加组件，它表示为 *Additional EUS Term 2*，将生命周期从 24 个月延长至 36 个月。在 OpenShift Container Platform 的所有架构变体中提供了 Additional EUS Term 2。

有关这个支持的更多信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

版本 4.12 的维护支持于 2024 年 7 月 17 日结束，将进入延长的更新支持阶段。如需更新相关信息，请参阅 Red Hat OpenShift Container Platform 生命周期政策 。

从 4.14 发行版本开始，为了简化对红帽所提供的 Operator 的管理和维护，红帽引入了三个新的生命周期类别：Platform Aligned, Platform Agnostic, 和 Rolling Stream这些生命周期类别为集群管理员提供了额外的简易性和透明度，以更好地了解每个 Operator 的生命周期策略，并以可预测的支持界限来计划对集群进行维护和升级。如需更多信息，请参阅 OpenShift Operator 生命周期。

OpenShift Container Platform 专为 FIPS 设计。当以 FIPS 模式运行 Red Hat Enterprise Linux (RHEL) 或 Red Hat Enterprise Linux CoreOS (RHCOS)时，OpenShift Container Platform 核心组件使用 RHEL 加密库，在 **x86_64**、**ppc64le**、**s390x** 架构上提交给 NIST 的 FIPS 140-2/140-3 Validation。

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

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

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

1.3. 新功能及功能增强

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. RHCOS 现在使用 RHEL 9.2

RHCOS 现在在 OpenShift Container Platform 4.14 中使用 Red Hat Enterprise Linux (RHEL) 9.2 软件包。这些软件包可确保 OpenShift Container Platform 实例收到最新的修复、功能、增强功能、硬件支持和驱动程序更新。不包括在这个更改中，OpenShift Container Platform 4.12 是一个延长更新支持 (EUS) 版本，它将继续对整个生命周期使用 RHEL 8.6 EUS 软件包。

1.3.1.1.1. 使用 RHEL 9.2 升级到 OpenShift Container Platform 的注意事项

因为 OpenShift Container Platform 4.14 现在使用基于 RHEL 9.2 的 RHCOS，所以在升级前请考虑以下方面：

- RHEL 8.6 和 RHEL 9.2 之间可能会更改了一些组件配置选项和服务，这意味着现有机器配置文件可能不再有效。
- 如果您自定义了默认 OpenSSH **/etc/ssh/sshd_config** 服务器配置文件，您需要根据红帽知识库文章进行更新。
- RHCOS 容器主机不支持 RHEL 6 基础镜像容器，但在 RHEL 8 worker 节点上支持。如需更多信息，请参阅红帽容器兼容性列表。
- 有些设备驱动程序已弃用，请参阅RHEL 文档 以了解更多信息。

1.3.2. 安装和更新

1.3.2.1. 使用共享 VPC 在 Amazon Web Services (AWS) 上安装集群

在 OpenShift Container Platform 4.14 中，您可以在使用共享虚拟私有云 (VPC) 的 AWS 上安装集群，其私有托管区位于与集群不同的帐户中。如需更多信息，请参阅在 AWS 上安装集群到现有的 VPC 中。

1.3.2.2. 在 AWS 上的集群 bootstrap 过程中启用 S3 存储桶

在这个版本中，您可以选择在 AWS 上的集群 bootstrap 过程中自动删除 S3 存储桶。如果您有一个用于防止删除 S3 存储桶的安全策略时，此选项很有用。

1.3.2.3. 使用 NAT 网关在 Microsoft Azure 上安装集群（技术预览）

在 OpenShift Container Platform 4.14 中，您可以安装使用 NAT 网关进行出站网络的集群。这作为技术预览提供 (TP)。如需更多信息，请参阅 其他 Azure 配置参数。

1.3.2.4. 使用 pd-balanced 磁盘类型在 Google Cloud Platform (GCP) 上安装集群

在 OpenShift Container Platform 4.14 中，您可以使用 **pd-balanced** 磁盘类型在 GCP 上安装集群。此磁盘类型仅适用于计算节点，不能用于 control plane 节点。如需更多信息，请参阅其他 GCP 配置参数。

1.3.2.5. OpenShift Container Platform 4.14 中的可选功能

对于 OpenShift Container Platform 4.14，您可以在安装过程中禁用 **Build**、**DeploymentConfig**、**ImageRegistry** 和 **MachineAPI** 功能。只有在使用用户置备的基础架构安装集群时，才能禁用 **MachineAPI** 功能。如需更多信息，请参阅集群功能。

1.3.2.6. 使用 Azure AD Workload Identity 安装集群

现在，您可以将 Microsoft Azure 集群配置为使用 Azure AD Workload Identity。使用 Azure AD Workload Identity 时，集群组件使用在集群外管理的短期安全凭证。

如需有关 Azure 上 OpenShift Container Platform 集群的短期凭证实现的更多信息，请参阅 Azure AD Workload Identity。

要了解如何在安装过程中配置此凭证管理策略，请参阅配置 Azure 集群以使用短期凭证。

1.3.2.7. Microsoft Azure 的用户定义的标签现已正式发布

Microsoft Azure 的用户定义的标签功能以前在 OpenShift Container Platform 4.13 中作为技术预览引进，现在在 OpenShift Container Platform 4.14 中正式发布。如需更多信息，请参阅为 Azure 配置用户定义的标签。

1.3.2.8. Azure 的机密虚拟机（技术预览）

您可以在 Azure 上安装集群时启用机密虚拟机。您可以在安装过程中使用机密计算来加密虚拟机客户机状态存储。这个功能只是一个技术预览，它存在一些已知的问题，这些问题在本文档的已知问题部分列出。如需更多信息，请参阅 启用机密虚拟机。

1.3.2.9. Azure 的可信启动（技术预览）

在 Azure 上安装集群时，您可以启用可信启动功能（技术预览）。这些功能包括安全引导和虚拟化受信任的平台模块。如需更多信息，请参阅为 Azure 虚拟机启用可信启动。

1.3.2.10. Google Cloud Platform 的用户定义的标签和标签（技术预览）

现在，您可以在 Google Cloud Platform (GCP) 中配置用户定义的标签和标签，以对资源进行分组，以及管理资源访问和成本。用户定义的标签只能应用到使用 OpenShift Container Platform 安装程序及其核心组件创建的资源。用户定义的标签只能应用到使用 OpenShift Container Platform Image Registry Operator 创建的资源。如需更多信息，请参阅为 GCP 管理用户定义的标签和标签。

1.3.2.11. 在受限网络中的 Microsoft Azure 上安装 OpenShift Container Platform 集群

在 OpenShift Container Platform 4.14 中，您可以在受限网络中为安装程序置备的基础架构 (IPI) 和用户置备的基础架构 (UPI) 在 Microsoft Azure 上安装集群。对于 IPI，您可以在现有 Azure Virtual Network (VNet) 上创建安装发行内容的内部镜像。对于 UPI，您可以使用您提供的基础架构在 Microsoft Azure 上安装集群。如需更多信息，请参阅在受限网络中在 Azure 上安装集群，以及在使用用户置备的基础架构的受限网络的 Azure 上安装集群。

1.3.2.12. 使用 by-path 设备别名指定安装磁盘

现在，您可以使用 by-path 设备别名指定安装磁盘，如 **deviceName: "/dev/disk/by-path/pci-**

0000:01:00.0-scsi-0:0:0:0"，在使用安装程序置备的基础架构在裸机上安装集群时。您还可以在基于代理的安装过程中指定此参数。这种类型的磁盘别名在重启后保留。如需更多信息，请参阅为裸机配置 install-config.yaml 文件，或为基于代理的安装配置 root 设备提示。

1.3.2.13. 将现有 AWS 安全组应用到集群

默认情况下，安装程序会创建安全组并将其附加到 control plane 和计算机器。不可修改与默认安全组关联的规则。

使用 OpenShift Container Platform 4.14 时，如果您将集群部署到现有的 Amazon Virtual Private Cloud (VPC) 中，您可以将额外的现有 AWS 安全组应用到 control plane 和计算机器。这些安全组必须与您要将集群部署到的 VPC 关联。应用自定义安全组可帮助您满足机构的安全需求，在这种情况下，您需要控制这些机器的传入或传出流量。如需更多信息，请参阅将现有 AWS 安全组应用到集群。

1.3.2.14. 从 OpenShift Container Platform 4.13 更新至 4.14 时所需的管理员确认

OpenShift Container Platform 4.14 使用 Kubernetes 1.27，它删除了已弃用的 API。

集群管理员必须在从 OpenShift Container Platform 4.13 升级到 4.14 前提供手动确认。这有助于防止升级到 OpenShift Container Platform 4.14 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 4.13 集群都需要此管理员确认，然后才能升级到 OpenShift Container Platform 4.14。

如需更多信息，请参阅准备升级到 OpenShift Container Platform 4.14。

1.3.2.15. Nutanix 的三节点集群支持

从 OpenShift Container Platform 4.14 开始，在 Nutanix 上部署三节点集群。这种类型的 OpenShift Container Platform 集群是一个更有效的资源集群。它只包含三个 control plane 机器，它们也充当计算机器。如需更多信息，请参阅在 Nutanix 上安装三节点集群。

1.3.2.16. 使用机密虚拟机在 GCP 上安装集群已正式发布

在 OpenShift Container Platform 4.14 中，在安装集群时使用机密虚拟机已正式发布。64 位 ARM 架构目前不支持机密虚拟机。如需更多信息，请参阅 启用机密虚拟机。

1.3.2.17. RHOSP 的根卷类型参数现在可用

现在，您可以使用 **rootVolume.types** 参数在 RHOSP 中指定一个或多个根卷类型。此参数可用于 control plane 和计算机器。

1.3.2.18. vSphere 节点的静态 IP 地址

您可以在没有动态主机配置协议 (DHCP) 的环境中置备带有静态 IP 地址的 bootstrap、control plane 和计算节点。

重要

vSphere 节点的静态 IP 地址只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

在部署集群以使用静态 IP 地址运行节点后，您可以扩展机器以使用这些静态 IP 地址之一。另外，您可以使用机器集将机器配置为使用配置的静态 IP 地址之一。

如需更多信息，请参阅在 vSphere 上安装集群中的"静态 IP 地址"部分。

1.3.2.19. Bare Metal Host CR 的额外验证

Bare Metal Host 自定义资源 (CR) 现在包含 **ValidatingWebhooks** 参数。使用这个参数，Bare Metal Operator 会在接受 CR 前捕获任何配置错误，并将配置错误返回给用户。

1.3.2.20. 在 AWS 本地区中快速安装集群

对于 OpenShift Container Platform 4.14，您可以在 Amazon Web Services (AWS) 上快速安装集群，以将计算节点扩展到 Local Zone 位置。在向安装配置文件中添加区名称后，安装程序会在每个 Local Zone 上完全自动创建所需资源、网络和计算。如需更多信息，请参阅在 AWS 本地区中快速引入集群。

1.3.2.21. 使用手动维护的云凭证的集群简化的安装和更新体验

此发行版本包括更改，用于改进安装和更新以手动模式使用 Cloud Credential Operator (CCO) 的集群进行云供应商身份验证。**oc adm release extract** 命令的以下参数简化了云凭证的手动配置：

--included

使用此参数只提取特定集群配置所需的清单。
如果您使用集群功能禁用一个或多个可选组件，在安装或更新集群前，不再需要删除任何禁用组件的 **CredentialsRequest** CR。

在以后的发行版本中，这个参数可能会使 CCO 实用程序 (**ccoctl**) **--enable-tech-preview** 参数成为不必要的。

--install-config

在安装集群前，使用此参数指定 **install-config.yaml** 文件的位置。
通过引用 **install-config.yaml** 文件，extract 命令可以决定您要创建的集群配置的各个方面。在集群更新过程中不需要此参数，因为 **oc** 可以连接到集群以确定其配置。

在这个版本中，不再需要使用 **--cloud** 参数指定要安装的云平台。因此，从 OpenShift Container Platform 4.14 开始，-- **cloud** 参数已弃用。

要了解如何使用这些参数，请参阅您的配置安装过程以及准备使用手动维护凭证更新集群 中的步骤。

1.3.2.22. 使用预先存在的 RHCOS 镜像模板在 vSphere 主机上快速安装 RHCOS

OpenShift Container Platform 4.14 包括了一个新的 VMware vSphere 配置参数，用于安装程序置备的基础架构： **模板**。通过使用此参数，您现在可以在安装配置文件中指定已存在的 Red Hat Enterprise Linux CoreOS (RHCOS) 镜像模板或虚拟机的绝对路径。然后，安装程序可以使用镜像模板或虚拟机在

vSphere 主机上快速安装 RHCOS。

这个安装方法是在 vSphere 主机上上传 RHCOS 镜像的替代方案。

重要

在为 **template** 参数设置 path 值前，请确保 OpenShift Container Platform 发行版本中的默认 RHCOS 引导镜像与 RHCOS 镜像模板或虚拟机版本匹配；否则，集群安装可能会失败。

1.3.2.23. 64 位 ARM 上的 OpenShift Container Platform

OpenShift Container Platform 4.14 现在支持基于 64 位 ARM 架构的 Google Cloud Platform 安装程序置备的和用户置备的基础架构。现在，您可以在 64 位 ARM 集群中使用 **oc mirror** CLI 插件断开连接的环境。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。

1.3.2.24. 为 Microsoft Azure 集群使用自定义 RHCOS 镜像

默认情况下，安装程序会下载并安装用于引导 control plane 和计算机器的 Red Hat Enterprise Linux CoreOS (RHCOS) 镜像。在这个版本中，您可以通过修改安装配置文件 (**install-config.yaml**) 来指定自定义 RHCOS 镜像来覆盖默认行为。在部署集群前，您可以修改以下安装参数：

- **compute.platorm.azure.osImage.publisher**
- **compute.platorm.azure.osImage.offer**
- **compute.platorm.azure.osImage.sku**
- **compute.platorm.azure.osImage.version**
- **controlPlane.platorm.azure.osImage.publisher**
- **controlPlane.platorm.azure.osImage.offer**
- **controlPlane.platorm.azure.osImage.sku**
- **controlPlane.platorm.azure.osImage.version**
- **platform.azure.defaultMachinePlatform.osImage.publisher**
- **platform.azure.defaultMachinePlatform.osImage.offer**
- **platform.azure.defaultMachinePlatform.osImage.sku**
- **platform.azure.defaultMachinePlatform.osImage.version**

有关这些参数的更多信息，请参阅 其他 Azure 配置参数。

1.3.2.25. 在云供应商上安装单节点 OpenShift

OpenShift Container Platform 4.14 扩展了在云供应商上安装单节点 OpenShift 的支持。单节点 OpenShift 的安装选项包括 Amazon Web Services (AWS)、Google Cloud Platform (GCP)和 Microsoft Azure。有关支持的平台的更多信息，请参阅支持的单一节点 openshift 的云供应商。

1.3.3. 安装后配置

1.3.3.1. 带有多架构计算机器的 OpenShift Container Platform 集群

现在，在 Google Cloud Platform (GCP) 上支持带有多架构计算机器的 OpenShift Container Platform 4.14 集群作为第 2 天操作。现在，裸机安装中使用多架构计算机器的 OpenShift Container Platform 集群已正式发布。有关使用多架构计算机器和支持的平台的集群的更多信息，请参阅关于带有多架构计算机器的集群。

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。现在您可以执行以下操作：

- 在列表视图或搜索页面中带有精确搜索功能缩小资源列表。当您有类似命名的资源且标准搜索功能没有缩小搜索范围时，这个操作很有用。
- 点工具栏上的 **Help** 按钮并点下拉列表中的 **Share Feedback** 来提供有关功能并报告错误的直接反馈。
- 在 YAML 编辑器中显示和隐藏工具提示。因为工具提示仍然存在，所以每次进入到页面时，您不需要更改工具提示。
- 为所有用户配置 web 终端镜像。如需更多信息，请参阅配置 Web 终端。

1.3.4.1.1. 动态插件增强

在这个版本中，您可以添加自定义指标仪表板，并使用 **QueryBowser** 扩展集群的 **Overview** 页面。OpenShift Container Platform 发行版本添加额外的扩展点，以便您可以添加不同类型的模式，设置活跃命名空间，提供自定义错误页面，并为动态插件设置代理超时。

如需更多信息，请参阅 OpenShift Container Platform 控制台 API 中的动态插件引用和 **QueryBrowser**。

1.3.4.1.2. OperatorHub 中基于操作系统的过滤

在这个版本中，OperatorHub 会根据节点的操作系统过滤，因为集群可以包含异构节点。

1.3.4.1.3. 支持在 web 控制台中安装特定的 Operator 版本

在这个版本中，您可以根据控制台中的 **OperatorHub** 页面中的所选频道，从 Operator 的可用版本列表中选择。另外，您可以在可用时查看该频道和版本的元数据。当选择旧版本时，需要手动批准更新策略，否则 Operator 会立即更新到该频道的最新版本。

如需更多信息，请参阅在 web 控制台中安装 Operator 的特定版本。

1.3.4.1.4. 对 AWS STS 的 OperatorHub 支持

在这个版本中，OperatorHub 会检测 Amazon Web Services (AWS) 集群是否使用安全令牌服务(STS)。当检测到时，在安装 Operator 前会显示一个"Cluster in STS Mode" 通知，以确保它正确运行。**Operator 安装**页面也被修改，以添加所需的**角色 ARN** 字段。如需更多信息，请参阅云供应商上的 Operator 的令牌身份验证。

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。现在您可以执行以下操作：

- 更改当前会话的 web 终端的默认超时时间。如需更多信息，请参阅为会话配置 web 终端超时。
- 在 **Topology** 视图和 Serverless Service **List** and **Detail** 页中测试 web 控制台中的 Serverless 功能，以便您可以使用带有 CloudEvent 或 HTTP 请求的 Serverless 功能。
- 查看 **BuildConfigs** 和 Shipwright 构建的最新构建的状态、开始时间和持续时间。您还可以在 **Details** 页面中查看此信息。

1.3.4.2.1. 新的快速开始

在这个版本中，存在新的快速启动，您可以在其中发现开发人员工具，如安装 Cryostat Operator 并使用 helm chart 使用 JBoss EAP 入门。

1.3.4.2.2. OpenShift Pipelines 页改进

在 OpenShift Container Platform 4.14 中，您可以在 **Pipelines** 页面中看到以下导航改进：

- 在 Git 导入流中自动检测 Pipelines 作为代码 (PAC)。
- 示例目录中的 Serverless 功能。

1.3.5. OpenShift CLI (oc)

1.3.5.1. 为使用 oc-mirror 的目录支持多架构 OCI 本地镜像

在 OpenShift Container Platform 4.14 中，oc-mirror 支持目录的多架构 OCI 本地镜像。

OCI 布局由 **index.json** 文件组成，用于标识磁盘上保存的镜像。此 **index.json** 文件可以引用任意数量的单个或多架构镜像。但是，oc-mirror 仅在给定的 OCI 布局中一次引用单个镜像。存储在 OCI 布局中的镜像可以是单一架构镜像，即镜像清单或多架构镜像，即清单列表。

ImageSetConfiguration 存储 OCI 镜像。在处理目录后，目录内容会添加代表布局中所有镜像内容的新层。ImageBuilder 被修改，以处理单架构和多架构镜像的镜像更新。

1.3.5.2. 使用 Web 浏览器登录 CLI

在 OpenShift Container Platform 4.14 中，为 **oc login** 命令提供了一个新的 **oc** 命令行 (CLI) 选项 **--web**。

有了这个增强，您可以使用 Web 浏览器登录，因此您不需要将访问令牌插入到命令行中。

如需更多信息，请参阅使用 Web 浏览器登录到 OpenShift CLI。

1.3.5.3. oc new-build 的增强

新的 **oc** CLI 标志 **--import-mode** 已添加到 **oc new-build** 命令中。有了这个增强，您可以将 **--import-mode** 标志设置为 **Legacy** 或 **PreserverOriginal**，以便使用单个子清单或所有清单来触发构建。

1.3.5.4. oc new-app 的增强

新的 **oc** CLI 标志 **--import-mode** 已添加到 **oc new-app** 命令中。有了这个增强，您可以将 **--import-mode** 标志设置为 **Legacy** 或 **PreserverOriginal**，然后使用单个子清单或所有清单创建新应用程序。

如需更多信息，请参阅设置导入模式。

1.3.6. IBM Z 和 IBM LinuxONE

在这个版本中，IBM Z® 和 IBM® LinuxONE 与 OpenShift Container Platform 4.14 兼容。可以使用 z/VM 或 Red Hat Enterprise Linux (RHEL) 内核的虚拟机 (KVM) 执行安装。有关安装说明，请参阅以下文档：

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

重要

Compute 节点必须运行 Red Hat Enterprise Linux CoreOS (RHCOS)。

1.3.6.1. IBM Z 和 IBM LinuxONE 主要改进

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

OpenShift Container Platform 4.14 上的 IBM Z® 和 IBM® LinuxONE 发行版本为 OpenShift Container Platform 组件和概念提供了改进和新功能。

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

- 使用 z/VM 支持的安装程序
- 在单一节点上安装
- 托管 control plane（技术预览）
- 多架构计算节点
- oc-mirror 插件

1.3.6.2. IBM 安全执行

OpenShift Container Platform 现在支持为 IBM Z® 和 IBM® LinuxONE (s390x 架构)上的 IBM Secure Execution 配置 Red Hat Enterprise Linux CoreOS (RHCOS)节点。

有关安装说明，请参阅以下文档：

- 使用 IBM 安全执行安装 RHCOS

1.3.7. IBM Power

IBM Power® 现在与 OpenShift Container Platform 4.14 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

重要

Compute 节点必须运行 Red Hat Enterprise Linux CoreOS (RHCOS)。

1.3.7.1. IBM Power 主要改进

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

OpenShift Container Platform 4.14 上的 IBM Power® 发行版本为 OpenShift Container Platform 组件添加了改进和新功能。

此发行版本引进了对 IBM Power® 的以下功能的支持：

- IBM Power® Virtual Server Block CSI Driver Operator （技术预览）
- 在单一节点上安装
- 托管 control plane（技术预览）
- 多架构计算节点
- oc-mirror 插件

1.3.8. IBM Power、IBM Z 和 IBM LinuxONE 支持列表

表 1.1. OpenShift Container Platform 功能

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
备用身份验证供应商	支持	支持
使用 Local Storage Operator 自动设备发现	不支持	支持
使用机器健康检查功能自动修复损坏的机器	不支持	不支持
IBM Cloud 的云控制器管理器	支持	不支持
在节点上控制过量使用和管理容器密度	不支持	不支持
Cron 作业	支持	支持
Descheduler	支持	支持
Egress IP	支持	支持
加密数据存储在 etcd 中	支持	支持
FIPS 加密	支持	支持

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
Helm	支持	支持
Pod 横向自动扩展	支持	支持
IBM 安全执行	不支持	支持
IBM Power® Virtual Server Block CSI Driver Operator （技术预览）	支持	不支持
IBM Power® Virtual Server 的安装程序置备的基础架构启用（技术预览）	支持	不支持
在单一节点上安装	支持	支持
IPv6	支持	支持
用户定义项目的监控	支持	支持
多架构计算节点	支持	支持
多路径（Multipathing）	支持	支持
网络绑定磁盘加密 - 外部 Tang 服务器	支持	支持
Non-volatile memory express drive (NVMe)	支持	不支持
oc-mirror 插件	支持	支持
OpenShift CLI (**oc**) 插件	支持	支持
Operator API	支持	支持
OpenShift Virtualization	不支持	不支持
OVN-Kubernetes，包括 IPsec 加密	支持	支持
PodDisruptionBudget	支持	支持
精度时间协议 (PTP) 硬件	不支持	不支持
Red Hat OpenShift Local	不支持	不支持
Scheduler 配置集	支持	支持

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
流控制传输协议 (SCTP)	支持	支持
支持多个网络接口	支持	支持
三节点集群支持	支持	支持
拓扑管理器	支持	不支持
SCSI 磁盘中的 z/VM 模拟 FBA 设备	不支持	支持
4K FCP 块设备	支持	支持

表 1.2. 持久性存储选项

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

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

表 1.3. Operator

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
Cluster Logging Operator	支持	支持
Cluster Resource Override Operator	支持	支持

功能	IBM Power®	IBM Z® 和 IBM® LinuxONE
Compliance Operator	支持	支持
File Integrity Operator	支持	支持
HyperShift Operator	技术预览	技术预览
Local Storage Operator	支持	支持
MetalLB Operator	支持	支持
Network Observability Operator	支持	支持
NFD Operator	支持	支持
NMState Operator	支持	支持
OpenShift Elasticsearch Operator	支持	支持
Vertical Pod Autoscaler Operator	支持	支持

表 1.4. Multus CNI 插件

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

表 1.5. CSI 卷

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

1.3.9. 认证和授权

1.3.9.1. SCC 抢占防止

在这个版本中，您可以要求工作负载使用特定的安全性上下文约束 (SCC)。通过设置特定的 SCC，您可以防止您希望在集群中被另一个 SCC 抢占的 SCC。如需更多信息，请参阅配置工作负载以需要特定的 SCC。

1.3.9.2. Pod 安全准入特权命名空间

在这个版本中，以下系统命名空间总是被设置为 **privileged** pod 安全准入配置集：

- **default**
- **kube-public**
- **kube-system**

如需更多信息，请参阅特权命名空间。

1.3.9.3. 修改的命名空间中禁用 Pod 安全准入同步

在这个版本中，如果用户从 label-synchronized 命名空间中的自动标记值手动修改 pod 安全准入标签，则会为该标签禁用同步。如有必要，用户可以再次启用同步。如需更多信息，请参阅 Pod 安全准入同步命名空间排除。

1.3.9.4. 基于 OLM 的 Operator 支持 AWS STS

在这个版本中，Amazon Web Services (AWS) 集群上的 Operator Lifecycle Manager (OLM) 管理的一些 Operator 可以在带有 Security Token Service (STS) 的手动模式中使用 Cloud Credential Operator (CCO)。这些 Operator 使用在集群外管理的有限权限短期凭证进行身份验证。如需更多信息，请参阅云供应商上的 Operator 的令牌身份验证。

1.3.9.5. 身份验证 Operator 在连接检查过程中遵循 noProxy

在这个版本中，如果设置了 **noProxy** 字段，且在没有集群范围代理的情况下可以访问路由，则 Authentication Operator 将绕过代理，并直接通过配置的 ingress 路由执行连接检查。在以前的版本中，无论 **noProxy** 设置如何，身份验证 Operator 始终通过集群范围代理执行连接检查。如需更多信息，请参阅配置集群范围代理。

1.3.10. 网络

1.3.10.1. 在 vSphere 双栈集群中将 IPv6 作为主 IP 地址系列

在 vSphere 上安装过程中，您可以将 IPv6 配置为双栈集群上的主 IP 地址系列。要在安装新集群时启用此功能，请在机器网络、集群网络、服务网络、API VIP 和入口 VIP 的 IPv4 地址系列前指定 IPv6 地址系列。

- 安装程序置备的基础架构：使用双栈网络进行部署
- 用户置备的基础架构：网络配置参数

1.3.10.2. OVN-Kubernetes 网络插件的多个外部网关支持

OVN-Kubernetes 网络插件支持为特定工作负载定义额外的默认网关。支持 IPv4 和 IPv6 地址系列。您可以使用 **AdminPolicyBasedExternalRoute** 对象定义每个默认网关，您可以在其中指定两种类型的下一跃点、静态和动态：

- 静态下一跃点：外部网关的一个或多个 IP 地址
- 动态下一跃点： pod 选择的 pod 和命名空间选择器的组合，以及与所选 pod 关联的网络附加定义名称。

您定义的下一个跃点由您指定的命名空间选择器限定。然后，您可以将外部网关用于与命名空间选择器匹配的特定工作负载。

如需更多信息，请参阅通过二级网络接口 配置外部网关。

1.3.10.3. Ingress Node Firewall Operator 已正式发布

Ingress Node Firewall Operator 在 OpenShift Container Platform 4.12 中被指定了一个技术预览功能。在这个版本中，Ingress Node Firewall Operator 已正式发布。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. OVS 的非保留 CPU 的动态使用

在这个版本中，Open vSwitch (OVS) 网络堆栈可以动态使用非保留 CPU。默认情况下，这种非保留 CPU 的动态使用发生在机器配置池中应用有性能配置集的节点。可用的非保留 CPU 的动态使用可最大化 OVS 的计算资源，并在高需求期间为工作负载最小化网络延迟。OVS 仍然无法在 **Guaranteed** QoS pod 中动态使用分配给容器的隔离 CPU。这种分离可避免对关键应用程序工作负载造成中断。

注意

当 Node Tuning Operator 识别性能条件来激活使用非保留 CPU 时，OVN-Kubernetes 配置 CPU 上运行的 OVS 守护进程的 CPU 关联性对齐。在这个窗口中，如果一个 **Guaranteed** QoS pod 启动，它可能会遇到延迟激增。

1.3.10.5. 多个 IP 地址的双栈配置

在以前的 Whereabouts IPAM CNI 插件版本中，每个网络接口只能分配一个 IP 地址。

现在，Whereabouts 支持分配任意数量的 IP 地址来支持双栈 IPv4/IPv6 功能。请参阅动态为双栈 IP 地址分配创建配置。

1.3.10.6. 排除 NUMA 感知调度的 SR-IOV 网络拓扑

在这个版本中，您可以将 SR-IOV 网络的 Non-Uniform Memory Access (NUMA)节点公告到拓扑管理器。如果没有为 SR-IOV 网络公告 NUMA 节点，您可以在 NUMA 感知 pod 调度过程中允许更灵活的 SR-IOV 网络部署。

例如，在某些情况下，最好在单个 NUMA 节点上为 pod 最大化 CPU 和内存资源。如果没有为 Topology Manager 提供有关 pod 的 SR-IOV 网络资源的 NUMA 节点的提示，拓扑管理器可能会将 SR-IOV 网络资源和 pod CPU 和内存资源部署到不同的 NUMA 节点。在以前的 OpenShift Container Platform 版本中，Topology Manager 会尝试将所有资源放在同一个 NUMA 节点上。

如需有关在 NUMA 感知 pod 调度过程中更灵活的 SR-IOV 网络部署的更多信息，请参阅为 NUMA 感知调度排除 SR-IOV 网络拓扑。

1.3.10.7. 更新至 HAProxy 2.6

在这个版本中，OpenShift Container Platform 更新至 HAProxy 2.6。

1.3.10.8. 支持在 Ingress Controller 中使用 sidecar 日志记录配置最大长度

在以前的版本中，Ingress Controller 中 syslog 信息的最大长度为 1024 字节。现在，可以增加最大值。如需更多信息，请参阅允许 Ingress Controller 在使用 sidecar 时修改 HAProxy 日志长度 。

1.3.10.9. 控制台中的 nmstate Operator 更新

在这个版本中，您可以从 web 控制台访问 NMstate Operator 和资源，如 **NodeNetworkState** (NNS)、**NodeNetworkConfigurationPolicy** (NNCP) 和 **NodeNetworkConfigurationEnhancement** (NNCE)。在控制台的 **Administrator** 视角中，您可以通过 **Networking** 页访问 NNCP、从 **NodeNetworkConfigurationPolicy** 页访问 NNCE，从 **NodeNetworkState** 页访问 NNS。有关 NMState 资源以及如何在控制台中更新它们的更多信息，请参阅更新节点网络配置。

1.3.10.10. OVN-Kubernetes 网络插件支持 IBM Cloud 上的 IPsec

现在，在使用 OVN-Kubernetes 网络插件的 IBM Cloud Platform 上支持 IPsec，这是 OpenShift Container Platform 4.14 中的默认设置。如需更多信息，请参阅配置 IPsec 加密。

1.3.10.11. OVN-Kubernetes 网络插件支持外部流量的 IPsec 加密（技术预览）

OpenShift Container Platform 现在支持加密外部流量，也称为*南北流量*。IPsec 已支持加密 pod 间的网络流量，称为 *东西流量*。您可以组合使用这两个功能来为 OpenShift Container Platform 集群提供完整的转换加密。这作为技术预览功能提供。

要使用这个功能，您需要为网络基础架构定义一个 IPsec 配置。如需更多信息，请参阅为外部 IPsec 端点启用 IPsec 加密。

1.3.10.12. 单堆栈 IPv6 支持 Kubernetes NMstate

在这个版本中，您可以在单堆栈 IPv6 集群中使用 Kubernetes NMState Operator。

1.3.10.13. 出口服务资源以管理负载均衡器后面的 pod 的出口流量（技术预览）

在这个版本中，您可以使用 **EgressService** 自定义资源 (CR) 来管理负载均衡器服务后面的 pod 的出口流量。这作为技术预览功能提供。

您可以使用以下方法使用 **EgressService** CR 管理出口流量：

- 将负载均衡器服务的 IP 地址分配为负载均衡器服务后面的 pod 的源 IP 地址。
- 将负载均衡器后面的 pod 的出口流量分配给与默认节点网络不同的网络。

如需更多信息，请参阅配置出口服务。

1.3.10.14. MetalLB 的 BGPPeer 资源中的 VRF 规格（技术预览）

在这个版本中，您可以在 **BGPPeer** 自定义资源中指定虚拟路由和转发 (VRF) 实例。MetalLB 可以通过属于 VRF 的接口公告服务。这作为技术预览功能提供。如需更多信息，请参阅通过网络 VRF 公开服务。

1.3.10.15. NMState 的 NodeNetworkConfigurationPolicy 资源中的 VRF 规格（技术预览）

在这个版本中，您可以使用 **NodeNetworkConfigurationPolicy** 自定义资源将虚拟路由和转发 (VRF) 实例与网络接口关联。通过将 VRF 实例与网络接口关联，您可以支持流量隔离、独立路由决策和网络资源的逻辑分离。此功能作为技术预览功能提供。如需更多信息，请参阅示例：带有 VRF 实例网络配置策略的网络接口。

1.3.10.16. 对 Broadcom BCM57504 的支持现在是 GA

对 Broadcom BCM57504 网络接口控制器的支持现在可用于 SR-IOV Network Operator.For 的更多信息，请参阅支持的设备。

1.3.10.17. OVN-Kubernetes 作为二级网络提供

在这个版本中，Red Hat OpenShift Networking OVN-Kubernetes 网络插件允许为 pod 配置二级网络接口。作为二级网络，OVN-Kubernetes 支持第 2 层交换和 localnet 交换拓扑网络。有关 OVN-Kubernetes 作为二级网络的更多信息，请参阅 OVN-Kubernetes 额外网络配置。

1.3.10.18. 在基于 OVN-Kubernetes 的集群部署中禁用了全局 IP 转发

从这个版本开始，全局 IP 地址转发在基于 OVN-Kubernetes 的集群部署中被禁用，以防止应用节点作为路由器为集群管理员所造成的意料外的效果。OVN-Kubernetes 现在在每个管理的接口上启用和限制转发。

您可以使用 **Network** 资源中的 **gatewayConfig.ipForwarding** 规格来控制 OVN-Kubernetes 管理接口上所有流量的 IP 转发。指定 **Restricted** 来仅转发与 OVN-Kubernetes 相关的所有流量。指定 **Global** 以允许转发所有 IP 流量。对于新安装，默认值为 **Restricted**。升级到 4.14 的集群不受此更改的影响；IP 转发行为保持不变，并持续启用。有关全局启用 IP 转发的更多信息，请参阅全局启用 IP 转发。

1.3.10.19. Admin Network Policy （技术预览）

管理网络策略作为技术预览功能提供。在运行 OVN-Kubernetes CNI 插件的集群中，您可以启用 **AdminNetworkPolicy** 和 **BaselineAdminNetworkPolicy** 资源，它们是 Network Policy V2 API 的一部分。集群管理员可以在创建命名空间前为整个集群应用集群范围的策略和保护。网络管理员可以通过强制无法覆盖的网络流量控制来保护集群。如果需要，网络管理员可以实施可选的基准网络流量控制，这些流量可以被集群中的用户覆盖。目前，这些 API 仅支持集群内流量的策略。

1.3.10.20. pod 的 MAC-VLAN、IP-VLAN 和 VLAN 子接口创建

在这个版本中，基于容器命名空间中的主接口创建 MAC-VLAN、IP-VLAN 和 VLAN 子接口已正式发布。您可以使用此功能在单独的网络附加定义中创建 master 接口作为 pod 网络配置的一部分。然后，您可以在这个接口上基于 VLAN、MACVLAN 或 IPVLAN，而无需了解节点的网络配置。如需更多信息，请参阅关于在容器网络命名空间中配置 master 接口。

1.3.10.21. 支持 all-multicast 模式

OpenShift Container Platform 发行版本现在支持使用 tuning CNI 插件配置 all-multicast 模式。在这个版本中，不再需要为 pod 的安全性上下文约束 (SCC) 授予 **NET_ADMIN** 功能，从而最大程度降低 pod 的潜在漏洞来提高安全性。

有关 all-multicast 模式的详情，请参阅关于 all-multicast 模式。

1.3.10.22. 使用 TAP 设备插件提高网络灵活性

此发行版本引入了一个新的 Container Network Interface (CNI) 网络插件类型：TAP 设备插件。您可以使用此插件在容器中创建TAP 设备，它允许用户空间程序处理网络帧，并充当从接收帧的接口，并将帧发送到用户空间应用，而不是通过传统的网络接口。有关更多信息，请参阅 TAP 额外网络的配置。

1.3.10.23. 支持使用TAP CNI 插件运行带有内核访问权限的 rootless DPDK 工作负载

在 OpenShift Container Platform 版本 4.14 及更高版本中，需要将流量注入内核的 DPDK 应用程序可以通过TAP CNI 插件在非特权 pod 中运行。如需更多信息，请参阅使用TAP CNI 运行具有内核访问权限的无根 DPDK 工作负载。

1.3.10.24. 使用 Ingress Controller 或 Route 对象设置或删除特定的 HTTP 标头

现在，可以使用 Ingress Controller 或特定路由全局设置或删除某些 HTTP 请求和响应标头。您可以设置或删除以下标头：

- X-Frame-Options
- X-Cache-Info
- X-XSS-Protection
- X-Source
- X-SSL-Client-Cert
- X-Target
- Content-Location
- Content-Language

如需更多信息，请参阅在 Ingress Controller 中设置或删除 HTTP 请求和响应标头，并在路由中设置或删除 HTTP 请求标头和响应标头。

1.3.10.25. 额外网络接口上的出口 IP 已正式发布

您可以在额外网络接口中使用出口 IP 地址。此功能为 OpenShift Container Platform 管理员提供了对网络方面（如路由、寻址、分段和安全策略）的更高级别控制。您还可以根据特定网络接口路由工作负载流量，如流量分段或满足特殊要求。

如需更多信息，请参阅在附加网络接口中使用出口 IP 的注意事项。

1.3.10.26. SR-IOV 网络策略更新过程中并行节点排空

在这个版本中，您可以将 SR-IOV Network Operator 配置为在网络策略更新过程中并行排空节点。并行排空节点的选项可以更快地推出 SR-IOV 网络配置。您可以使用 **SriovNetworkPoolConfig** 自定义资源配置并行节点排空，并在 Operator 可以并行排空池中定义最大节点数量。

如需更多信息，请参阅在 SR-IOV 网络策略更新过程中配置并行节点排空。

1.3.11. 容器镜像仓库（Registry）

1.3.11.1. 可选 Image Registry Operator

在这个版本中，Image Registry Operator 是一个可选组件。当不需要 Image Registry Operator 时，此功能有助于减少 Telco 环境中 OpenShift Container Platform 的整体资源占用空间。有关禁用 Image Registry Operator 的更多信息，请参阅选择集群功能。

1.3.12. 存储

1.3.12.1. 在 LVMS 中支持 OR 逻辑

在这个版本中，逻辑卷管理器 (LVM) 集群自定义资源 (CR) 在 **deviceSelector** 设置中提供 **OR** 逻辑。在以前的版本中，只能为使用 **AND** 逻辑的设备路径指定 **paths** 设置。在这个版本中，您还可以指定 **optionalPaths** 设置，它支持 **OR** 逻辑。如需更多信息，请参阅使用逻辑卷管理器存储的持久性存储中的 CR 示例。

1.3.12.2. 支持 LVMS 中的 ext4

在这个版本中，逻辑卷管理器 (LVM) 集群自定义资源 (CR) 支持 **ext4** 文件系统，其 **fstype** 设置在 **deviceClasses** 下。默认文件系统为 **xfs**。如需更多信息，请参阅使用逻辑卷管理器存储的持久性存储中的 CR 示例。

1.3.12.3. 标准化的 STS 配置工作流

OpenShift Container Platform 4.14 提供了简化且标准化的步骤，以使用 AWS Elastic File Storage (EFS) Container Storage Interface (CSI) Driver Operator 配置安全令牌服务 (STS)。

如需更多信息，请参阅获取安全令牌服务的角色 Amazon 资源名称。

1.3.12.4. Read Write Once Pod 访问模式（技术预览）

OpenShift Container Platform 4.14 为名为 ReadWriteOncePod (RWOP) 的持久性卷声明 (PVC) 引入了一个新的访问模式，该模式只能在单一节点上的单个 pod 中使用。这与现有的 ReadWriteOnce 访问模式进行比较，其中一个 PV 或 PVC 可以被多个 pod 在单一节点中使用。这作为技术预览功能提供。

如需更多信息，请参阅访问模式。

1.3.12.5. GCP Filestore 存储 CSI Driver Operator 已正式发布

OpenShift Container Platform 可以使用 Google Compute Platform (GCP) 文件存储存储的 Container Storage Interface (CSI) 驱动程序置备持久性卷 (PV)。GCP Filestore CSI Driver Operator 在 OpenShift Container Platform 4.12 中引进了，且支持技术预览。GCP Filestore CSI Driver Operator 现已正式发布。如需更多信息，请参阅 Google Compute Platform Filestore CSI Driver Operator 。

1.3.12.6. VMware vSphere 自动 CSI 迁移

VMware vSphere 功能的自动 CSI 迁移会自动将树内对象转换为其对应的 CSI 表示，理想情况下，用户必须完全透明。虽然引用 in-tree 存储插件的存储类继续工作，但请考虑将默认存储类切换到 CSI 存储类。

在 OpenShift Container Platform 4.14 中，在所有情况下都默认启用 vSphere 的 CSI 迁移，且管理员不需要操作。

如果您使用 vSphere in-tree 持久性卷 (PV)，并希望从 OpenShift Container Platform 4.12 或 4.13 升级到 4.14，请将 vSphere vCenter 和 ESXI 主机更新至 7.0 Update 3L 或 8.0 Update 2，否则 OpenShift Container Platform 升级会被阻断。如果您不想更新 vSphere，可以通过执行管理员确认步骤来执行 OpenShift Container Platform 更新：但是，使用管理员确认时可能会出现已知的问题。在继续管理员确认前，请仔细阅读知识库文章。

如需更多信息，请参阅 CSI 自动迁移。

1.3.12.7. Secret Store CSI Driver Operator （技术预览）

Secret Store Container Storage Interface (CSI) Driver Operator, **secrets-store.csi.k8s.io**，允许 OpenShift Container Platform 将存储在企业级外部 secret 中的多个 secret、密钥和证书作为内联临时卷挂载到 pod 中。Secrets Store CSI Driver Operator 使用 gRPC 与供应商通信，以从指定的外部 secret 存储获取挂载内容。附加卷后，其中的数据将挂载到容器的文件系统。这作为技术预览功能提供。有关 Secret Store CSI 驱动程序的更多信息，请参阅 Secret Store CSI 驱动程序 。

有关使用 Secret Store CSI Driver Operator 将 secret 从外部 secret 存储挂载到 CSI 卷的详情，请参阅使用外部 secret 存储向 pod 提供敏感数据。

1.3.12.8. 支持 NFS 的 Azure File 已正式发布

OpenShift Container Platform 4.14 支持 Azure File Container Storage Interface (CSI) Driver Operator，并正式发布 Network File System (NFS)。

如需更多信息，请参阅 NFS 支持。

1.3.13. Oracle® Cloud Infrastructure

现在，您可以使用 Assisted 安装程序或基于代理的安装程序在 Oracle® Cloud Infrastructure (OCI) 上安装 OpenShift Container Platform 集群。要在 OCI 上安装 OpenShift Container Platform 集群，请选择以下安装选项之一：

- 使用辅助安装程序在 Oracle® Cloud Infrastructure (OCI) 上安装集群
- 使用基于代理的安装程序在 Oracle® Cloud Infrastructure (OCI) 上安装集群

1.3.14. Operator 生命周期

1.3.14.1. Operator Lifecycle Manager (OLM) 1.0 （技术预览）

自 OpenShift Container Platform 4 初始发行以来，Operator Lifecycle Manager (OLM) 已包含在 OpenShift Container Platform 4 中。OpenShift Container Platform 4.14 引入了用于 OLM 的下一代迭代组件作为技术预览功能，在这个阶段称为 *OLM 1.0*。此更新的框架改变了很多属于以前版本的 OLM 的概念，并添加了新功能。

在 OpenShift Container Platform 4.14 中 OLM 1.0 的技术预览阶段，管理员可以探索以下功能：

支持 GitOps 工作流的全声明性模型

OLM 1.0 通过两个 API 简化了 Operator 管理：

- 一个新的 **Operator** API **operators.operators.operatorframework.io** 由新的 Operator Controller 组件提供，通过将面向用户的 API 整合到单个对象来简化已安装的 Operator 的管理。这让管理员和 SRE 能够使用 GitOps 原则自动化进程并定义所需的状态。
- **Catalog** API 由新 catalogd 组件提供，充当 OLM 1.0 的基础，为 on-cluster 客户端解包目录，以便用户可以发现可安装的内容，如 Operator 和 Kubernetes 扩展。这可让您提高所有可用 Operator 捆绑包版本的可见性，包括它们的详情、频道和更新边缘。

如需更多信息，请参阅 Operator Controller 和 Catalogd。

改进了对 Operator 更新的控制

通过改进对目录内容的了解，管理员可以指定用于安装和更新的目标版本。这可让管理员对 Operator 更新的目标版本进行更多控制。如需更多信息，请参阅从目录安装 Operator。

灵活的 Operator 打包格式

管理员可以使用基于文件的目录来安装和管理以下类型的内容：

- 基于 OLM 的 Operator，类似于现有的 OLM 体验
- *普通捆绑包*，它们是任意 Kubernetes 清单的静态集合

另外，捆绑包大小不再受 etcd 值大小限制。如需更多信息，请参阅在 OLM 1.0 中管理普通捆绑包。

注意

对于 OpenShift Container Platform 4.14，适用于 OLM 1.0 的流程仅基于 CLI。另外，管理员也可以使用普通方法（如 **Import YAML** 和 **Search** 页面）在 web 控制台中创建和查看相关对象。但是，现有的 **OperatorHub** 和 **Installed Operators** 页面还不会显示 OLM 1.0 组件。

如需更多信息，请参阅关于 Operator Lifecycle Manager 1.0。

1.3.15. Operator 开发

1.3.15.1. 云供应商上的 Operator 的令牌身份验证：AWS STS

在这个版本中，由 Operator Lifecycle Manager (OLM) 管理的 Operator 可以在使用安全令牌服务(STS)的 Amazon Web Services (AWS) 集群中运行时支持令牌身份验证。Cloud Credential Operator (CCO) 更新至半自动置备某些有限权限、短期凭证，只要 Operator 作者启用了其 Operator 来支持 AWS STS。有关启用基于 OLM 的 Operator 来使用 AWS STS 支持基于 CCO 的工作流的更多信息，请参阅云供应商上的 Operator 的令牌身份验证。

1.3.15.2. 配置支持多个平台的 Operator 项目

在这个版本中，Operator 作者可以配置其 Operator 项目，并支持多个架构和操作系统或 *平台*。Operator 作者可通过执行以下操作为多个平台配置支持：

- 构建指定 Operator 支持的平台的清单列表。
- 设置 Operator 的节点关联性以支持多架构计算机器。

如需更多信息，请参阅为多平台支持配置 Operator 项目。

1.3.16. Builds

- 在这个版本中，OpenShift Container Platform 4.14 中已正式发布 Source-to-Image (S2I) 工具。您可以使用 S2I 工具从源代码构建容器镜像，并将应用程序代码转换为可随时部署的容器镜像。此功能增强了平台支持可重复生成的容器化应用程序开发的能力。如需更多信息，请参阅使用 Source-to-Image (S2I)工具。
- 在这个版本中，OpenShift Container Platform 4.14 中已正式发布 Build CSI Volumes 功能。

1.3.17. Machine Config Operator

1.3.17.1. 处理 registry 证书颁发机构

Machine Config Operator 现在为镜像 registry 处理分布证书颁发机构。这个更改不会影响最终用户。

1.3.17.2. Prometheus 中可用的其他指标

在这个版本中，您可以查询额外的指标来更密切地监控机器和机器配置池的状态。

有关如何使用 Prometheus 的更多信息，请参阅查看可用指标的列表。

1.3.17.3. 支持离线 Tang 置备

在这个版本中，您可以使用 Tang-enforced、网络绑定磁盘加密 (NBDE) 置备 OpenShift Container Platform 集群，该集群在第一次引导过程中无法访问。

如需更多信息，请参阅配置加密阈值和配置磁盘加密和镜像。

1.3.17.4. 证书现在由 Machine Config Daemon 处理

在以前的 OpenShift Container Platform 版本中，MCO 直接从机器配置文件读取和处理证书。这会导致轮转问题并创建不需要的情况，比如证书会停留在暂停的机器配置池后面。

在这个版本中，证书不再从 bootstrap 模板到机器配置文件。相反，它们直接放入 Ignition 对象中，使用控制器配置写入磁盘，并在常规集群操作期间由 Machine Config Daemon (MCD) 处理。然后，使用 **ControllerConfig** 资源可以看到 certs。

Machine Config Controller (MCC) 包含以下证书数据：

- **/etc/kubernetes/kubelet-ca.crt**
- **/etc/kubernetes/static-pod-resources/configmaps/cloud-config/ca-bundle.pem**
- **/etc/pki/ca-trust/source/anchors/openshift-config-user-ca-bundle.crt**

MCC 还处理镜像 registry 证书及其关联的用户捆绑包证书。这意味着证书不会由机器配置池状态绑定，并更及时地轮转。以前在机器配置文件中列出的 CA 已被删除，在集群安装过程中找到的模板文件将不再存在。有关如何访问这些证书的更多信息，请参阅查看和与证书交互。

1.3.18. 机器 API

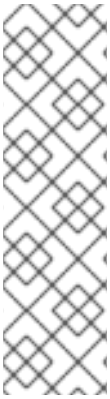
1.3.18.1. 支持 Nutanix 集群上的 control plane 机器集

在这个版本中，Nutanix 集群支持 control plane 机器集。如需更多信息，请参阅开始使用 Control Plane Machine Set Operator。

1.3.18.2. 支持 RHOSP 集群上的 control plane 机器集

在这个版本中，在 RHOSP 上运行的集群支持 control plane 机器集。

如需更多信息，请参阅开始使用 Control Plane Machine Set Operator 。



注意

对于具有根卷可用区且在升级到 4.14 的 RHOSP 上运行的集群，您必须将 control plane 机器聚合到一个服务器组中，然后才能启用 control plane 机器集。要进行必要的更改，请按照 OpenShift on OpenStack 上具有可用区的说明： 在 OpenShift 部署期间无效 Compute ServerGroup 设置。

对于配置有至少一个区且在 RHOSP 上运行的计算区的集群，它只适用于版本 4.14，根卷现在还必须配置至少一个区。如果没有更改此配置更改，则无法为集群生成 control plane 机器集。要进行必要的更改，请按照带有计算可用区的 OpenStack 上相关 OpenShift 中的说明：Missing rootVolume availability zone。

1.3.18.3. 支持将 AWS 机器分配给放置组

在这个版本中，您可以配置机器集来部署现有 AWS 放置组中的机器。您可以将此功能与 Elastic Fabric Adapter (EFA) 实例一起使用，以提高指定放置组内机器的网络性能。您可以将此功能用于 compute 和 control plane 机器集。

1.3.18.4. Azure 机密虚拟机和可信启动（技术预览）

在这个版本中，您可以配置机器集来部署使用 Azure 机密虚拟机、可信启动或两者的机器。这些机器可以使用统一可扩展固件接口 (UEFI) 安全功能，如安全引导或专用虚拟信任平台模块 (vTPM) 实例。

您可以将此功能用于 compute 和 control plane 机器集。

1.3.19. 节点

1.3.19.1. 大型集群的 descheduler 资源限值

在这个版本中，descheduler 操作对象的资源限值会被删除。这可让 descheduler 用于带有许多节点和 pod 的大型集群，而不会因为内存不足错误而失败。

1.3.19.2. Pod 拓扑分布约束 matchLabelKeys 参数现已正式发布

用于配置 pod 拓扑分布限制的 **matchLabelKeys** 参数现在包括在 OpenShift Container Platform 4.14 中。在以前的版本中，通过启用 **TechPreviewNoUpgrade** 功能集，该参数作为技术预览提供。**matchLabelKeys** 参数取 pod 标签键列表，以选择要计算分布的 pod。

如需更多信息，请参阅使用 pod 拓扑分布限制控制 pod 放置。

1.3.19.3. 启用 MaxUnavailableStatefulSet （技术预览）

在这个版本中，通过启用 **TechPreviewNoUpgrade** 功能集，**MaxUnavailableStatefulSet** 功能集配置参数作为技术预览功能提供。现在，您可以定义在更新过程中不可用的 **StatefulSet** pod 的最大数量，从而减少升级时应用程序停机时间。

如需更多信息，请参阅了解功能门。

1.3.19.4. Pod 中断预算 (PDB) 不健康的 pod 驱除策略。

在这个版本中，为 pod 中断预算 (PDB) 指定不健康 pod 驱除策略在 OpenShift Container Platform 中正式发布，已从 **TechPreviewNoUpgrade** featureSet 中删除。这有助于在节点排空过程中驱除出现故障的应用程序。

如需更多信息，请参阅为不健康的 pod 指定驱除策略。

1.3.19.5. Linux Control Groups 版本 2 现在是默认的

从 OpenShift Container Platform 4.14 开始，新安装默认使用 Control Groups 版本 2，也称为 cgroup v2、cgroup2 或 cgroupsv2。此功能增强包括很多 bug 修复、性能改进，以及与新功能集成的功能。在 OpenShift Container Platform 4.14. cgroup v1 之前，仍可以使用 cgroup v1。cgroup v1 仍可通过将 **node.config** 对象中的 **cgroupMode** 字段改为 **v1** 来使用。

如需更多信息，请参阅在节点上配置 Linux cgroup 版本 。

1.3.19.6. Cron Job 时区正式发布

为 cron 任务调度设置时区现已正式发布。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。

1.3.20. 监控

这个版本的监控堆栈包括以下新功能和修改的功能：

1.3.20.1. 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** 更新到 2.9.2
- **node-exporter** 更新到 1.6.1
- **prom-label-proxy** 更新到 0.7.0
- Prometheus 更新到 2.46.0
- **prometheus-operator** 更新到 0.67.1

1.3.20.2. 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 **KubeDeploymentRolloutStuck** 警报，以监控部署已有 15 分钟没有任何进展。
  - 添加了 **NodeSystemSaturation** 警报，以监控节点上的资源饱和。
  - 添加了 **NodeSystemdServiceFailed** 警报来监控节点上的 systemd 服务。
  - 添加了 **NodeMemoryMajorPagesFaults** 警报，以监控节点上的主要页面错误。
  - 添加了 **PrometheusSDRefreshFailure** 警报，以监控失败的 Prometheus 服务发现。

- **已更改**
  - 修改了 **KubeAggregatedAPIDown** 警报和 **KubeAggregatedAPIErrors** 警报，以仅评估 **apiserver** 作业的指标。
  - 修改 **KubeCPUOvercommit** 警报，以仅评估 **kube-state-metrics** 作业的指标。
  - 修改 **NodeHighNumberConntrackEntriesUsed**,**NodeNetworkReceiveErrs** 和 **NodeNetworkTransmitErrs** 警报，以评估 **node-exporter** 作业的指标。
- **删除**
  - 删除了不可行的 **MultipleContainersOOMKilled** 警报。其他警报涵盖内存压力不足的节点。

1.3.20.3. 基于核心平台指标创建警报的新选项

在这个版本中，管理员可以根据核心平台指标创建新的警报规则。现在，您可以通过调整阈值和更改标签来修改现有平台警报规则的设置。您还可以通过根据 **openshift-monitoring** 命名空间中的核心平台指标构建查询表达式来定义和添加新的自定义警报规则。此功能在 OpenShift Container Platform 4.12 版本中作为技术预览功能提供，这个功能现在包括在 OpenShift Container Platform 4.14 中。如需更多信息，请参阅为核心平台监控管理警报规则。

1.3.20.4. 为所有监控组件指定资源限值的新选项

在这个版本中，您可以为所有监控组件指定资源请求和限值，包括：

- Alertmanager
- **kube-state-metrics**
- **monitoring-plugin**
- **node-exporter**
- **openshift-state-metrics**
- Prometheus
- Prometheus Adapter
- Prometheus Operator 及其准入 Webhook 服务
- Telemeter Client
- Thanos querier
- Thanos Ruler

在以前的 OpenShift Container Platform 版本中，您只能为 Prometheus、Alertmanager、Thanos Querier 和 Thanos Ruler 设置选项。

1.3.20.5. 配置 node-exporter 收集器的新选项

在这个版本中，您可以为额外的 **node-exporter** 收集器自定义 Cluster Monitoring Operator (CMO) 配置映射设置。以下 **node-exporter** 收集器现在是可选的，您可以在配置映射设置中单独启用或禁用每个节点：

- **ksmd** 收集器
- **mountstats** 收集器
- **processes** 收集器
- **systemd** 收集器

另外，您现在可以从 **netdev** 和 **netclass** 收集器的相关收集器配置中排除网络设备。现在，您可以使用 **maxProcs** 选项设置可运行 node-exporter 的最大进程数。

1.3.20.6. 部署监控 Web 控制台插件资源的新选项

在这个版本中，OpenShift Container Platform Web 控制台的 **Observe** 部分中的监控页面被部署为动态插件。在这个版本中，Cluster Monitoring Operator (CMO) 是部署 OpenShift Container Platform Web 控制台监控插件资源的组件。现在，您可以使用 CMO 设置来配置控制台监控插件资源的以下功能：

- 节点选择器
- 容限（Tolerations）
- 拓扑分布限制
- 资源请求
- 资源限值

1.3.21. Network Observability Operator

Network Observability Operator 发行版本独立于 OpenShift Container Platform 次版本流的更新。更新可以通过单一的滚动流提供，该流在所有当前支持的 OpenShift Container Platform 4 版本中被支持。有关 Network Observability Operator 的新功能、功能增强和程序错误修复的信息，请参阅 Network Observability 发行注记。

1.3.22. 可伸缩性和性能

1.3.22.1. PAO must-gather 镜像添加到默认 must-gather 镜像

在这个版本中，Performance Addon Operator (PAO) must-gather 镜像不再需要作为 **must-gather** 命令的参数，以捕获与低延迟调整相关的调试数据。PAO must-gather 镜像的功能现在在没有镜像参数的 **must-gather** 命令使用的默认插件镜像下。有关收集与低延迟调整相关的调试信息的详情，请参考为红帽支持收集低延迟调试数据。

1.3.22.2. 使用 Operator 的 must-gather 镜像收集 NUMA Resources Operator 的数据

在本发行版本中，**must-gather** 工具被更新，以使用 Operator 的 **must-gather** 镜像收集 NUMA Resources Operator 的数据。有关为 NUMA Resources Operator 收集调试信息的更多信息，请参阅收集 NUMA Resources Operator 数据。

1.3.22.3. 为每个 pod 启用对 C-states 的更多控制

在这个版本中，您可以更好地控制 pod 的 C-states。现在，您可以为 C-states 指定最大延迟，而不是完全禁用 C-states。您可以在 **cpu-c-states.crio.io** 注解中配置这个选项。这有助于优化高优先级应用程序中的节能功能，方法是启用一些 shouldower C-states 而不是完全禁用它们。有关控制 pod C-states 的更

多信息，请参阅为高优先级 pod 禁用节能模式。

1.3.22.4. 支持从双栈 hub 集群置备 IPv6 spoke 集群

在这个版本中，您可以从双栈 hub 集群置备 IPv6 地址 spoke 集群。在 ZTP 环境中，托管引导 ISO 的 hub 集群上的 HTTP 服务器现在侦听 IPv4 和 IPv6 网络。置备服务还会检查目标 spoke 集群上的基板管理控制器 (BMC) 地址方案，并为安装介质提供匹配的 URL。这些更新提供了从双栈 hub 集群中置备单堆栈 IPv6 spoke 集群的功能。

1.3.22.5. RHOSP 集群的双栈网络（技术预览）

现在，RHOSP 上运行的集群可以使用双栈网络配置。这是一个技术预览功能。您可以在安装程序置备的基础架构上部署集群时配置双栈网络。

如需更多信息，请参阅使用双栈网络配置集群。

1.3.22.6. RHOSP 集群的安全组管理

在 OpenShift Container Platform 4.14 中，在 RHOSP 上运行的集群的安全性已被改进。默认情况下，OpenStack 云供应商现在将负载均衡器的 **manage-security-groups** 选项设为 **true**，确保只打开集群操作所需的节点端口。在以前的版本中，compute 和 control plane 机器的安全组被配置为为所有传入的流量打开大范围的节点端口。

您可以通过在负载均衡器配置中将 **manage-security-groups** 选项设置为 **false** 来使用以前的配置，并确保安全组规则允许来自节点的 **0.0.0.0/0** 的端口范围 30000 到 32767 的流量。

对于升级到 4.14 的集群，您必须手动删除为所有流量打开部署的 permissive 安全组规则。例如，您必须删除允许从节点的 **0.0.0.0/0**端口范围 30000 到 32767 的流量的规则。

1.3.22.7. 在 GitOps Zero Touch Provisioning (ZTP) 管道中使用带有 PolicyGenTemplate CR 的自定义 CR

现在，除了 **ztp-site-generate** 容器中的 GitOps ZTP 插件提供的基本源 CR 之外，您还可以使用 GitOps ZTP 来包括自定义 CR。如需更多信息，请参阅在 GitOps ZTP 管道中添加自定义内容 。

1.3.22.8. GitOps ZTP 独立于受管集群版本

现在，您可以使用 GitOps ZTP 置备运行不同版本的 OpenShift Container Platform 的受管集群。这意味着 hub 集群和 GitOps ZTP 插件版本可以独立于在受管集群上运行的 OpenShift Container Platform 版本。如需更多信息，请参阅为版本独立准备 GitOps ZTP 站点配置存储库 。

1.3.22.9. 使用 Topology Aware Lifecycle Manager 预缓存用户指定的镜像

在这个版本中，您可以使用 Topology Aware Lifecycle Manager 在单节点 OpenShift 集群上升级应用程序工作负载镜像。如需更多信息，请参阅在单节点 OpenShift 集群上使用 TALM 预缓存用户指定的镜像。

1.3.22.10. 通过 SiteConfig 和 GitOps ZTP 进行磁盘清理选项

在这个版本中，您可以使用 **SiteConfig** CR 中的 **automatedCleaningMode** 字段在安装前删除分区表。如需更多信息，请参阅单节点 OpenShift SiteConfig CR 安装参考 。

1.3.22.11. 支持通过 GitOps ZTP 在 SiteConfig CR 中添加自定义节点标签

在这个版本中，您可以在 **SiteConfig** CR 中添加 **nodeLabels** 字段，以便为受管集群中的节点创建自定义角色。有关如何添加自定义标签的更多信息，请参阅使用 SiteConfig 和 GitOps ZTP 部署受管集群，手动生成 GitOps ZTP 安装和配置 CR，以及 单节点 OpenShift SiteConfig CR 安装参考。

1.3.22.12. 支持微调 etcd 延迟容错（技术预览）

在这个版本中，您可以将 control plane 硬件速度设置为 **"Standard"**、**"Slower"** 或默认值（""），允许系统决定使用哪个速度。这是一个技术预览功能。如需更多信息，请参阅为 etcd 设置调整参数。

1.3.22.13. 在 SiteConfig 中弃用字段

在这个版本中，**SiteConfig** 自定义资源定义(CRD)中的 **apiVIP** 和 **ingressVIP** 字段已弃用，并使用 plural 表单、**apiVIPs** 和 **ingressVIPs** 替代。

1.3.23. 托管 control plane

1.3.23.1. 在裸机和 OpenShift Virtualization 上，托管的 control plane 正式发布

现在，在裸机和 OpenShift Virtualization 平台上为 OpenShift Container Platform 托管 control plane。在 AWS 上托管的 control plane 仍是一个技术预览功能。

1.3.23.2. 在 AWS 托管的集群中创建 ARM NodePool 对象（技术预览）

在这个发行版本中，您可以在同一个托管的 control plane 的 64 位 ARM 和 AMD64 上调度应用程序工作负载。如需更多信息，请参阅在 AWS 托管的集群中创建 ARM NodePool 对象。

1.3.23.3. 在 IBM Z 上托管 control plane （技术预览）

在这个发行版本中，托管的 control plane 作为 IBM Z 上的技术预览功能提供。如需更多信息，请参阅为 IBM Z 计算节点在 64 位 x84 裸机上配置托管集群（技术预览）。

1.3.23.4. 在 IBM Power 上托管 control plane （技术预览）

在这个发行版本中，托管的 control plane 作为 IBM Power 的技术预览功能提供。如需更多信息，请参阅在 64 位 x86 OpenShift Container Platform 集群上配置托管集群，以便为 IBM Power 计算节点创建托管的 control plane （技术预览）。

1.3.24. Insights Operator

1.3.24.1. 按需收集数据（技术预览）

在 OpenShift Container Platform 4.14 中，Insights Operator 现在可以根据需要运行收集操作。有关根据需要运行收集操作的更多信息，请参阅运行 Insights Operator 收集操作。

1.3.24.2. 作为各个 pod 运行收集操作（技术预览）

在 OpenShift Container Platform 4.14 技术预览集群中，Insights Operator 在单独的 pod 中运行收集操作。这支持新的按需数据收集功能。

1.4. 主要的技术变化

OpenShift Container Platform 4.14 包括以下显著的技术更改。

1.4.1. 云控制器管理器用于其他云供应商

Kubernetes 社区计划弃用 Kubernetes 控制器管理器与底层云平台交互，而是使用云控制器管理器。因此，无法为任何新的云平台添加 Kubernetes 控制器管理器支持。

此发行版本引入了为 Amazon Web Services 和 Microsoft Azure 使用云控制器管理器的正式发布。

要了解有关云控制器管理器的更多信息，请参阅 Kubernetes Cloud Controller Manager 文档。

要管理云控制器管理器和云节点管理器部署和生命周期，请使用 Cluster Cloud Controller Manager Operator。如需更多信息，请参阅*平台 Operator 参考*中的 Cluster Cloud Controller Manager Operator 条目。

1.4.2. 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。

1.4.3. SSH 密钥位置的变化

OpenShift Container Platform 4.14 引入了基于 RHEL 9.2 的 RHCOS。在此次更新之前，SSH 密钥位于 RHCOS 上的 **/home/core/.ssh/authorized_keys** 中。在这个版本中，基于 RHEL 9.2 的 RHCOS 上，SSH 密钥位于 **/home/core/.ssh/authorized_keys.d/ignition** 中。

如果您自定义了默认 OpenSSH **/etc/ssh/sshd_config** 服务器配置文件，您需要根据红帽知识库文章进行更新。

1.4.4. cert-manager Operator 正式发布

Red Hat OpenShift 1.11 的 cert-manager Operator 现在包括在 OpenShift Container Platform 4.14 和 OpenShift Container Platform 4.13 和 OpenShift Container Platform 4.12 中。

1.4.5. 改进了使用 Open Virtual Network (OVN) 优化的扩展和稳定性

OpenShift Container Platform 4.14 引入了对 Open Virtual Network Kubernetes (OVN-K) 的优化，其内

部架构被修改，以减少操作延迟，以消除网络 control plane 扩展和性能。网络流数据现在本地化到集群节点，而不是在 control plane 上集中信息。这可减少操作延迟，并减少 worker 和控制节点之间的集群范围流量。因此，集群网络使用节点数线性扩展，因为每个额外节点都会添加额外的网络容量，这样可优化较大的集群。因为每个节点上的网络流都是本地化的，所以不再需要 RAFT 领导选举机制，并删除了 instability 的主要来源。对本地化网络流数据的一个额外好处是，网络上的节点丢失的影响仅限于故障节点，且对集群的其他网络没有问题，从而使集群对故障场景更具弹性。如需更多信息，请参阅 OVN-Kubernetes 架构。

1.4.6. Operator SDK 1.31.0

OpenShift Container Platform 4.14 支持 Operator SDK 1.31.0。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 1.31.0 支持 Kubernetes 1.26。

如果您之前使用 Operator SDK 1.28.0 创建或维护的 Operator 项目，请更新您的项目以保持与 Operator SDK 1.31.0 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

1.4.7. oc 命令现在默认从 Podman 配置位置存储和检索凭证

在以前的版本中，使用 registry 配置的 OpenShift CLI (**oc**) 命令（如 **oc adm release** 或 **oc image** 命令）从 Docker 配置文件位置（如 ~/**.docker/config.json** ）获取凭证。如果在 Docker 配置位置中没有找到 registry 条目，**oc** 命令会从 Podman 配置文件位置获取凭证，如 **${XDG_RUNTIME_DIR}/containers/auth.json**。

在这个版本中，**oc** 命令会默认使用从 Podman 配置位置获取凭证。如果无法在 Podman 配置位置中找到 registry 条目，**oc** 命令会从 Docker 配置位置获取凭证。

另外，**oc registry login** 命令现在将凭证存储在 Podman 配置位置，而不是 Docker 配置文件位置。

1.4.8. 长时间运行的 pod 请求现在作为 CONNECT 请求记录

在 OpenShift Container Platform 指标中，pod **attach**,**exec**,**log**,**portforward**, 和 **proxy** 请求被记录为 **CONNECT** 请求。

1.4.9. 打开虚拟网络基础架构控制器默认范围

在这个版本中，Controller 使用 **100.88.0.0/16** 作为传输交换机子网的默认 IP 地址范围。不要在您的生产环境基础架构网络中使用这个 IP 范围。(OCPBUGS-20261)

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 4.14 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*

1.5.1. Operator 生命周期和开发已弃用和删除的功能

表 1.6. Operator 生命周期和开发已弃用并删除 tracker

功能	4.12	4.13	4.14
Operator 目录的 SQLite 数据库格式	已弃用	已弃用	已弃用
operators.openshift.io/infrastructure-features 注解	公开发行	公开发行	Deprecated

1.5.2. 镜像已弃用和删除的功能

表 1.7. 镜像已弃用和删除的 tracker

功能	4.12	4.13	4.14
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

1.5.3. 安装已弃用和删除的功能

表 1.8. 安装已弃用并删除跟踪器

功能	4.12	4.13	4.14
oc adm release extract 的 **--cloud** 参数	公开发行	公开发行	Deprecated
对 **cluster.local** 域的 CoreDNS 通配符查询	Deprecated	删除	删除
compute.platform.openstack.rootVolume.type for RHOSP	公开发行	公开发行	已弃用

功能	4.12	4.13	4.14
controlPlane.platform.openstack.rootVolume.type for RHOSP	公开发行	公开发行	Deprecated
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	已弃用	已弃用	Deprecated
Google Cloud Provider 的 **platform.gcp.licenses**	已弃用	已弃用	删除
VMware ESXi 7.0 Update 1 或更早版本	公开发行	删除 [1]	删除
vSphere 7.0 Update 1 或更早版本	已弃用	删除 [1]	删除

1. 对于 OpenShift Container Platform 4.14，您必须在 VMware vSphere 版本 7.0 Update 2 或更高版本的实例（包括 VMware vSphere 版本 8.0）上安装 OpenShift Container Platform 集群，它需要满足您使用的组件的要求。

1.5.4. 存储已弃用和删除的功能

表 1.9. 存储已弃用和删除的 tracker

功能	4.12	4.13	4.14
使用 FlexVolume 的持久性存储	已弃用	已弃用	Deprecated

1.5.5. 构建应用程序已弃用和删除的功能

表 1.10. Service Binding Operator 弃用并删除 tracker

功能	4.12	4.13	4.14
Service Binding Operator	公开发行	已弃用	已弃用

1.5.6. 多架构已弃用和删除的功能

表 1.11. 多架构已弃用并删除 tracker

功能	4.12	4.13	4.14
IBM Power8 所有模型 (**ppc64le**)	已弃用	删除	删除
IBM Power® AC922 (**ppc64le**)	Deprecated	删除	删除
IBM Power® IC922 (**ppc64le**)	Deprecated	删除	删除

功能	4.12	4.13	4.14
IBM Power® LC922 (**ppc64le**)	Deprecated	删除	删除
IBM z13 所有模型 (**s390x**)	已弃用	删除	删除
IBM® LinuxONE Emperor (**s390x**)	已弃用	删除	删除
IBM® LinuxONE Rockhopper (**s390x**)	已弃用	删除	删除
AMD64 (x86_64) v1 CPU	已弃用	删除	删除

1.5.7. 已弃用和删除的网络功能

表 1.12. 已弃用和删除的网络功能跟踪器

功能	4.12	4.13	4.14
RHOSP 上的 Kuryr	已弃用	已弃用	Deprecated
OpenShift SDN 网络插件	公开发行	公开发行	Deprecated

1.5.8. 节点已弃用和删除的功能

表 1.13. 节点已弃用并删除 tracker

功能	4.12	4.13	4.14
ImageContentSourcePolicy (ICSP) 对象	公开发行	已弃用	已弃用
Kubernetes 拓扑标签 **failure-domain.beta.kubernetes.io/zone**	公开发行	已弃用	已弃用
Kubernetes 拓扑标签 **failure-domain.beta.kubernetes.io/region**	公开发行	已弃用	Deprecated

1.5.9. OpenShift CLI (oc) 已弃用和删除的功能

功能	4.12	4.13	4.14
oc-mirror 的 **--include-local-oci-catalogs** 参数	不可用	公开发行	删除
oc-mirror 的 **--use-oci-feature** 参数	公开发行	Deprecated	删除

1.5.10. 工作负载已弃用和删除的功能

表 1.14. 工作负载已弃用和删除的 tracker

功能	4.12	4.13	4.14
deploymentConfig 对象	公开发行	公开发行	Deprecated

1.5.11. 裸机监控已弃用和删除的功能

表 1.15. 裸机事件中继 Operator tracker

功能	4.14	4.15	4.16
裸机事件中继 Operator	删除	删除	删除

1.5.12. 弃用的功能

1.5.12.1. 弃用 OpenShift SDN 网络插件

从 OpenShift Container Platform 4.14 开始，OpenShift SDN CNI 已被弃用。目前，在下一个 OpenShift Container Platform 次发行本中，网络插件不会成为新安装的选项。在以后的发行版本中，计划删除 OpenShift SDN 网络插件，并不再被支持。红帽将在删除前对这个功能提供程序错误修正和支持，但不会再改进这个功能。作为 OpenShift SDN CNI 的替代选择，您可以使用 OVN Kubernetes CNI。

1.5.12.2. Service Binding Operator

Service Binding Operator 已被弃用，并将在 OpenShift Container Platform 4.16 发行版本中删除。红帽将在当前发行生命周期中对这个组件提供重要的程序错误修复和支持，但此组件将不再获得功能增强。

1.5.12.3. DeploymentConfig 资源现已弃用

自 OpenShift Container Platform 4.14 起，**DeploymentConfig** 对象已弃用。**DeploymentConfig** 对象仍被支持，但不建议用于新安装。只有与安全相关的和严重的问题才会被解决。

反之，使用 **Deployment** 对象或其他替代方法为 pod 提供声明性更新。

1.5.12.4. GitOps ZTP 中使用的特定于 Operator 的 CatalogSource CR 已被弃用

在 OpenShift Container Platform 4.14 中，在使用 Topology Aware Lifecycle Manager (TALM)更新 Operator 时，只能使用 **DefaultCatSrc.yaml CatalogSource** CR。所有其他 **CatalogSource** CR 都已弃用，计划在以后的发行版本中删除。红帽将在当前发行生命周期中提供对这个功能的程序漏洞修复和支持，但这个功能将不再获得改进，并将被删除。如需有关 **DefaultCatSrc** CR 的更多信息，请参阅执行 Operator 更新。

1.5.12.5. oc adm release extract 命令的 --cloud 参数

自 OpenShift Container Platform 4.14 起，**oc adm release extract** 命令的 **--cloud** 参数已弃用。介绍 **--included** 和 **--install-config** 参数使 **--cloud** 参数成为不必要的。

如需更多信息，请参阅使用手动维护的云凭证为集群简化安装和更新体验。

1.5.12.6. Red Hat Virtualization (RHV)作为 OpenShift Container Platform 的主机平台

Red Hat Virtualization (RHV) 作为 OpenShift Container Platform 的主机平台已弃用，不再被支持。以后的 OpenShift Container Platform 发行版本中，此平台将从 OpenShift Container Platform 中删除。

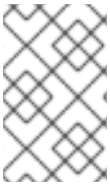
1.5.12.7. 使用 REGISTRY_AUTH_PREFERENCE 环境变量现已弃用

使用 **REGISTRY_AUTH_PREFERENCE** 环境变量指定您的首选位置来获取 OpenShift CLI 的 registry 凭证(**oc**) 命令现已弃用。

OpenShift CLI (**oc**) 命令现在默认从 Podman 配置位置获取凭据，但会回退到检查已弃用的 Docker 配置文件位置。

1.5.12.8. operators.openshift.io/infrastructure-features 注解

从 OpenShift Container Platform 4.14 开始，注解的 **operators.openshift.io/infrastructure-features** 组页弃用，由带有 **features.operators.openshift.io** 命名空间的注解组替代。



注意

目前，Web 控制台继续支持使用之前的注解进行显示和过滤。但是，因为它们已弃用，所以在以后的 OpenShift Container Platform 发行版本中对在 web 控制台中使用它们的支持会被删除，因此建议迁移到新的注解格式。

参阅弃用的基础架构功能注解了解以前的注解信息，参阅基础架构功能注解了解最新的注解信息。

1.5.13. 删除的功能

1.5.13.1. 删除了裸机事件中继 Operator

Bare Metal Event Relay Operator 以前是一个技术预览功能，现在已从 OpenShift Container Platform 中删除。有关 Bare Metal Event Relay Operator 的完整生命周期信息，请参阅 产品生命周期：Bare Metal Event Relay。

1.5.13.2. 从 Kubernetes 1.27 中删除 Beta API

Kubernetes 1.27 删除了以下已弃用的 API，因此您必须迁移清单和 API 客户端以使用适当的 API 版本。有关迁移已删除 API 的更多信息，请参阅 Kubernetes 文档。

表 1.16. 从 Kubernetes 1.27 中删除的 API

资源	删除的 API	迁移到
CSIStorageCapacity	**storage.k8s.io/v1beta1**	**storage.k8s.io/v1**

1.5.13.3. 删除了对 LatencySensitive 功能集的支持

从 OpenShift Container Platform 4.14 开始，删除了对 **LatencySensitive** 功能集的支持。

1.5.13.4. oc registry login 不再将凭证存储在 Docker 配置文件位置

从 OpenShift Container Platform 4.14 开始，**oc registry login** 命令不再将 registry 凭证存储在 Docker 文件位置，如 **~/.docker/config.json**。**oc registry login** 命令现在将凭证存储在 Podman 配置文件位置，如 **${XDG_RUNTIME_DIR}/containers/auth.json**。

1.6. 程序错误修复

1.6.1. API 服务器和客户端

- 在以前的版本中，当使用由安全性上下文约束模拟的 pod 规格创建 pod 控制器时，用户可能会收到 Pod 不满足给定命名空间的 pod 安全级别的警告。在这个版本中，如果 pod 控制器创建在该命名空间中没有违反 pod 安全性的 pod，则不再会收到有关 pod 安全的警告。(OCPBUGS-7267)

- **user:check-access** 有范围令牌授予发送 SelfSubjectAccessReview 请求的权限。在以前的版本中，除非令牌也具有 **user:full** 范围或角色范围，集群没有足够权限来执行访问权限。在这个版本中，集群会授权一个 SelfSubjectAccessReview 请求，因为它具有完整的用户权限或请求上设置的用户角色的权限，以便能够执行访问权限检查。(OCPBUGS-7415)

- 在以前的版本中，当将 **.subjects[].kind** 设置为 **ServiceAccount** 时，pod 安全准入控制器需要设置 **RoleBinding** 对象的 **.subject[].namespace** 字段，以便可以成功将服务帐户绑定到角色。在这个版本中，如果没有指定 **.subject[].namespace**，pod 安全准入控制器将使用 **RoleBinding** 对象的命名空间。(OCPBUGS-160)

- 在以前的版本中，**ValidatingWebhookConfiguration** 和 **MutatingWebhookConfiguration** 对象的所有 webhook 的 **clientConfig** 没有被 **service-ca** 信任捆绑包正确注入 **caBundle**。在这个版本中，**ValidatingWebhookConfiguration** 和 **MutatingWebhookConfiguration** 对象的所有 webhook 的 **clientConfig** 都会获得带有 **service-ca** 信任捆绑包正确注入的 **caBundle**。(OCPBUGS-19318)

- 在以前的版本中，当为 **namedCertificates** 中的 **servingCertificate** 指定了一个无效的 secret 名称时，kube-apiserver 不会变为 **Degraded=True**。在这个版本中，kube-apiserver 会变为 **Degraded=True**，并显示不接受证书的原因，以便更轻松地进行故障排除。(OCPBUGS-8404)

- 在以前的版本中，可观察性仪表板使用大型查询来显示数据，这会导致在有大量节点的集群上频繁超时。在这个版本中，Observability 仪表板使用预先计算的记录规则，以确保在有大量节点的集群上的可靠性。(OCPBUGS-3986)

1.6.2. 裸机硬件置备

- 在以前的版本中，如果裸机的主机名不是由反向 DNS 或 DHCP 提供的，在安装程序置备的基础架构上的裸机集群置备过程中默认为 **localhost**。此问题导致 Kubernetes 节点名称冲突，并阻止部署集群。现在，如果检测到主机名是 **localhost**，则置备代理会将持久主机名设置为 **BareMetalHost** 对象的名称。(OCPBUGS-9072)

1.6.3. Cloud Compute

- 在以前的版本中，Machine API 控制器无法决定使用多个区的 vSphere 集群中的机器区。在这个版本中，区查找逻辑基于虚拟机的主机，因此机器对象代表了正确的区。(OCPBUGS-7249)

- 在以前的版本中，在 **clouds.yaml** 文件中轮转云凭证后，需要重启 OpenStack 机器 API 供应商才能获取新的云凭证。因此，机器集可扩展为零的功能可能会受到影响。在这个版本中，云凭证不再被缓存，供应商会根据需要再次读取对应的 secret。(OCPBUGS-8687)

- 在以前的版本中，Cluster Autoscaler Operator 启动过程中的一些条件会导致一个锁定，阻止 Operator 成功启动并将自身标记为可用。因此，集群会降级。这个版本解决了这个问题。(OCPBUGS-20038)

- 在以前的版本中，用于为 control plane 节点请求客户端凭证的 bootstrap 凭证不包括通用，所有服务帐户组。因此，集群机器批准忽略在这个阶段创建的证书签名请求 (CSR)。在某些情况下，这会阻止 bootstrap 过程中批准 CSR，并导致安装失败。在这个版本中，bootstrap 凭证包括集群机器批准者对服务帐户所需的组。此更改允许机器批准程序在集群生命周期前面从 bootstrap CSR 批准程序接管，并应减少与 CSR 批准相关的 bootstrap 失败。(OCPBUGS-8349)

- 在以前的版本中，如果扩展 Nutanix 集群上的机器超过可用内存来完成操作，机器会处于 **Provisioning** 状态，且无法扩展或缩减。这个问题已在本发行版本中解决。(OCPBUGS-19731)

- 在以前的版本中，对于将 Control Plane Machine Set Operator 配置为使用 **OnDelete** 更新策略的集群，缓存机器的信息会导致 Operator 错误地平衡机器，并在协调过程中将它们放在意外的故障域中。在这个版本中，Operator 会在创建新机器前立即刷新此信息，以便正确标识要放置机器的故障域。(OCPBUGS-15338)

- 在以前的版本中，Control Plane Machine Set Operator 使用 **Infrastructure** 对象规格来决定集群的平台类型。对于从 OpenShift Container Platform 版本 4.5 及更早版本升级的集群，这个实践意味着 Operator 无法正确确定集群是否在 AWS 上运行，因此不会按预期生成 **ControlPlaneMachineSet** 自定义资源(CR)。在这个版本中，Operator 使用 status 平台类型，该类型会在创建时位于所有集群中填充，现在可以为所有集群生成 **ControlPlaneMachineSet** CR。(OCPBUGS-11389)

- 在以前的版本中，当底层 Machine API 机器运行后，由 control plane 机器集创建的机器被视为就绪。在这个版本中，在链接到该机器的节点就绪前，机器不会被视为就绪。(OCPBUGS-7989)

- 在以前的版本中，Control Plane Machine Set Operator 按照字母顺序对故障域进行优先级排序，并将机器从按字母顺序位于后面的失败的域中移动按字母顺序位于较早的失败域中集群，即使这样做并不能改进跨故障域中的机器可用性。在这个版本中，Operator 被更新为优先选择现有机器中存在的故障域，并遵守提供更好可用性的现有故障域。(OCPBUGS-7921)

- 在以前的版本中，当删除使用 control plane 机器集的 vSphere 集群上的 control plane 机器时，有时会创建两个替换机器。在这个版本中，control plane 机器集不再会导致创建额外的机器。(OCPBUGS-7516)

- 在以前的版本中，当机器集中的可用区和子网 ID 不匹配时，会使用机器集规格成功创建机器，且没有指示不匹配的用户。由于不匹配的值可能会导致某些配置出现问题，所以发生这个情况可能会作为警告信息可见。在这个版本中，会记录有关不匹配的警告。(OCPBUGS-6882)

- 在以前的版本中，当在 Nutanix 上创建 OpenShift Container Platform 集群时，它使用 Dynamic Host Configuration Protocol (DHCP)而不是 IP 地址管理(IPAM)网络配置时，DHCP 不会设置虚拟机的名称。在这个版本中，使用 ignition 配置文件中的值设置虚拟机主机名。因此，这个问题已针对 DHCP 和其他网络配置类型解决。(OCPBUGS-6727)

- 在以前的版本中，可以在 **openshift-cluster-api** 命名空间中创建多个集群。此命名空间必须只包含一个集群。在这个版本中，无法在这个命名空间中创建额外的集群。(OCPBUGS-4147)

- 在以前的版本中，从 control plane 机器集自定义资源的 **providerSpec** 字段中清除一些参数会导致 control plane 机器删除和创建循环。在这个版本中，如果这些参数被清除或留空，则这些参数会收到一个默认值，这会解决这个问题。(OCPBUGS-2960)

1.6.4. Cloud Credential Operator

- 在以前的版本中，Cloud Credential Operator 实用程序 (**ccoctl**) 为 AWS GovCloud (US) 和

AWS 中国区域使用不正确的 Amazon Resource Names (ARN) 前缀。不正确的 ARN 前缀会导致 **ccoctl aws create-all** 命令在安装过程中创建 AWS 资源失败。此发行版本将 ARN 前缀更新为正确的值。(OCPBUGS-13549)

- 在以前的版本中，对 Amazon S3 存储桶的安全更改会导致 Cloud Credential Operator 实用程序 (**ccoctl**)命令在安装过程中创建 AWS 资源(**ccoctl aws create-all**)失败。在这个版本中，**ccoctl** 工具被更新来反映 Amazon S3 安全更改。(OCPBUGS-11671)

1.6.5. Cluster Version Operator

- 在以前的版本中，Cluster Version Operator (CVO)不会按预期协调 **SecurityContextConstraints** 资源。CVO 现在可以正确地将 **SecurityContextConstraints** 资源与发行镜像中定义的状态协调，从而恢复对它们的任何不支持的修改。
  希望从以前的 OpenShift Container Platform 版本升级以及根据修改后的系统 **SecurityContextConstraints** 资源运行工作负载的用户必须遵循 知识库文章 中的流程，以确保其工作负载能够在没有修改的系统 **SecurityContextConstraint** 资源的情况下运行。(OCPBUGS-19465)

- 在以前的版本中，当决定首先评估的条件更新风险时，Cluster Version Operator 不会优先选择目标。现在，对于没有应用风险的条件更新，这些更新会在 Cluster Version Operator 检测后更快可用。(OCPBUGS-5469)

1.6.6. 开发人员控制台

- 在以前的版本中，如果您试图在 **Developer** 控制台中编辑 **Helm** Chart 仓库，点 Repositories 选项卡，然后点 **Repositories** 选项卡，通过 Helm Chart 仓库的  菜单选择 **Edit HelmChartRepository**，则 **Error** 页面会显示一个 **404: Page Not Found** 错误。这是因为一个不是最新的组件路径所致。这个问题现已解决。(OCPBUGS-14660)

- 在以前的版本中，区分 **Samples** 页面中列出的样本类型比较困难。在这个版本中，您可以轻松地识别 **Samples** 页面中显示的徽标中的示例类型。(OCPBUGS-7446)

- 在以前的版本中，在 Pipeline **Metrics** 页面中，**TaskRun** 持续时间标图中只可以看到四个图例。在这个版本中，您可以看到 **TaskRun** 持续时间图表的所有图例。(OCPBUGS-19878)

- 在以前的版本中，当在一个未安装 Cluster Samples Operator 的断开连接的集群中使用 **Import JAR** 表单创建应用程序时，会出现一个问题。在这个版本中，**Add** 页面中的 **Import JAR** 表单会在 Java Builder Image 不存在时隐藏 **Topology** 页面。(OCPBUGS-15011)

- 在以前的版本中，如果禁用了集群服务版本 (CSV) 副本，Operator 支持的目录不会显示任何目录项。在这个版本中，即使禁用了 CSV 副本，Operator 支持的目录也会在每个命名空间中显示。(OCPBUGS-14907)

- 在以前的版本中，在 **Import from Git** 和 **Deploy Image** 流中，**Resource Type** 部分被移到 **Advanced** 部分。因此，很难识别创建的资源类型。在这个版本中，**Resource Type** 部分被移到 **General** 部分。(OCPBUGS-7395)

1.6.7. etcd Cluster Operator

- 在以前的版本中，**etcdctl** 二进制文件会无限期地缓存在本地机器上，从而无法对二进制文件进行更新。现在，每次调用 **cluster-backup.sh** 脚本时都会正确更新二进制文件。(OCPBUGS-19499)

1.6.8. 安装程序

- 在以前的版本中，如果您在将 AWS 集群安装到受支持的 secret 分区时没有指定自定义 Red Hat Enterprise Linux CoreOS (RHCOS) Amazon Machine Image (AMI)，安装会失败。在这个版本中，安装程序会在部署集群前验证您在安装配置文件中指定了 RHCOS AMI 的 ID。(OCPBUGS-13636)

- 在以前的版本中，OpenShift Container Platform 安装程序在使用共享 VPC 在 Google Cloud Platform (GCP) 上安装在主机项目中找不到私有托管区。在这个版本中，安装程序会检查主机项目中现有的私有托管区，并使用私有托管区（如果存在）。(OCPBUGS-11736)

- 在以前的版本中，如果您在安装私有 Azure 集群时配置了用户定义的出站路由，集群会错误地使用默认公共负载均衡器部署。使用安装程序置备的基础架构安装集群时发生此行为。在这个版本中，在配置用户定义的路由时，安装程序不再创建公共负载均衡器。(OCPBUGS-9404)

- 在以前的版本中，对于在 RHOSP 上运行的集群，在安装取消置备阶段，安装程序会按顺序删除对象存储容器。这个行为会导致对象的缓慢和低效删除，特别是对于大型容器来说。此问题部分发生，因为使用 Swift 容器随时间积累的对象的镜像流。现在，批量对象删除发生在最多 3 个对 RHOSP API 的调用时，通过每个调用处理较高的对象数来提高效率。此优化可在取消置备过程中加快资源清理速度。(OCPBUGS-9081)

- 在以前的版本中，当堡垒主机在与集群节点相同的 VPC 网络中运行时，对 bootstrap 和集群节点的 SSH 访问会失败。另外，此配置会导致从临时 bootstrap 节点到集群节点的 SSH 访问失败。现在，通过更新 IBM Cloud **SecurityGroupRules** 来支持临时 bootstrap 节点和集群节点之间的 SSH 流量来解决这些问题，并支持从堡垒主机到同一 VPC 网络上的集群节点的 SSH 流量。可以在安装程序置备的基础架构失败时准确收集日志和调试信息以进行分析。(OCPBUGS-8035)

- 在以前的版本中，在卸载私有集群时，安装程序创建的 DNS 记录不会被删除。在这个版本中，安装程序可以正确地删除这些 DNS 记录。(OCPBUGS-7973)

- 在以前的版本中，文档中提供的脚本用于检查 RHOSP API 中的无效 HTTPS 证书，假设 RHOSP 客户端的最新版本。对于没有客户端最新版本的用户，此脚本会失败。现在，在文档中添加了手动说明，用户可以按照这些文档对客户端的任何版本执行检查。(OCPBUGS-7954)

- 在以前的版本中，当在 **agent-config.yaml** 或 **nmstateconfig.yaml** 文件中为基于 Agent 的安装定义静态 IP 地址时，在 bootstrap 过程中可能无法配置配置的静态 IP 地址。因此，主机接口会通过 DHCP 选择一个地址。在这个版本中，解决了时间问题，以确保配置的静态 IP 地址正确应用到主机接口。(OCPBUGS-16219)

- 在以前的版本中，在基于 Agent 的安装过程中，**install-config.yaml** 文件的 **AdditionalTrustBundle** 字段中的证书仅在为镜像设置 **ImageContentSources** 字段时传播到最终镜像。如果没有设置镜像，则额外的证书位于 bootstrap 上，而不是最终镜像。当您设置了代理并希望添加额外的证书时，这可能会导致问题，如 在安装过程中配置集群范围代理 所述。在这个版本中，这些额外证书会传播到最终镜像，无论是否同时设置了 **ImageContentSources** 字段。(OCPBUGS-13535)

- 在以前的版本中，**openshift-install agent create** 命令在运行无效命令时不会返回帮助输出。在这个版本中，在运行无效的 **openshift-install agent create** 命令时会显示帮助输出。(OCPBUGS-10638)

- 在以前的版本中，没有为使用技术预览故障域生成的机器正确设置主网络。因此，带有 ID **control-plane** 的端口目标没有被设置为机器上的主要网络，这可能会导致使用 Kuryr 的安装不当地正常工作。现在，如果设置，该字段被设置为使用正确的端口目标。现在，生成的机器的主要网络已被正确设置，允许使用 Kuryr 的安装完成。(OCPBUGS-10570)

- 在以前的版本中，当在使用包含摘要的 **releaseImage** 时运行 **openshift-install agent create**

image 命令时，命令会生成以下警告信息：**WARNING The ImageContentSources configuration in install-config.yaml should have at-least one source field matching the releaseImage**。这个消息会在每次生成，无论配置 **ImageContentSources** 的方式是什么，并可能导致混淆。在这个版本中，只有在 **ImageContentSources** 被合法设置为与发行镜像匹配的至少一个 source 字段时，才会生成警告信息。(OCPBUGS-10207)

- 在以前的版本中，当运行 **openshift-install agent create image** 命令来生成可引导 ISO 镜像时，命令输出会提供一个指示成功生成的镜像的消息。即使基于 Agent 的安装程序无法从发行镜像中提取基本 ISO 镜像，也会存在此输出消息。在这个版本中，如果基于 Agent 的安装程序找不到基本 ISO 镜像，则命令输出会生成错误消息，这可能代表 **releaseImage** 的问题。(OCPBUGS-9949)

- 在以前的版本中，在使用 passthrough 凭证模式的 GCP 上的共享 VPC 安装可能会失败，因为安装程序使用来自默认服务帐户的凭证。在这个版本中，您可以指定用于创建节点的另一个服务帐户，而不是默认的服务帐户。(OCPBUGS-15421)

- 在以前的版本中，如果您在 **agent-config.yaml** 或 **nmstateconfig.yaml** 配置文件中定义了比计算节点更多的 control plane 节点，您会收到警告信息。现在，如果您在任一文件中指定了此配置，您会收到错误消息，这表示计算节点无法在任一文件中超过 control plane 节点。(OCPBUGS-14877)

- 在以前的版本中，如果 **agent-config.yaml** 文件中的 **RendezvousIP** 字段使用非规范 IPv6 地址，则基于代理的安装会失败。非规范 IPv6 地址包含前导零，例如 **2001:0db8:0000:0000:0000:0000:0000:0000**。在这个版本中，这些有效的地址可用于 **RendezvousIP**。(OCPBUGS-14121)

- 在以前的版本中，Operator 会缓存云凭证，这会导致在轮转这些凭证时出现身份验证问题。现在，Operator 始终使用最新的凭证。Manila CSI Driver Operator 现在会自动为每个可用的 Manila 共享类型创建一个 OpenShift 存储类。作为此操作的一部分，Operator 会查询 Manila API。(OCPBUGS-14049)

- 在以前的版本中，当配置 **install-config.yaml** 文件以便在基于 Agent 的安装过程中使用时，将 **cpuPartitioning** 字段改为非默认值不会产生警告，以警告用户，基于 Agent 的安装会忽略该字段。在这个版本中，更改 **cpuPartitioning** 字段会导致用户警告，使配置不会影响安装。(OCPBUGS-13662)

- 在以前的版本中，将 Azure 集群安装到现有 Azure Virtual Network (VNet) 可能会失败，因为安装程序会创建一个默认网络安全组，允许从 **0.0.0.0** 的流量。当现有 VNet 在租户中启用了以下规则时失败：**Rule: Network Security Groups should not allow rule with 0.0.0.0/Any Source/Destination IP Addresses - Custom Deny**.在这个版本中，当将集群安装到现有的 VNet 时，安装程序不再会创建默认网络安全组，安装可以成功。(OCPBUGS-11796)

- 在安装过程中，当集群状态为 **installing-pending-user-action** 时，安装不会完成，直到状态解决为止。在以前的版本中，如果您运行 **openshift-install agent wait-for bootstrap-complete** 命令，则不会指示如何解决导致这个状态的问题。在这个版本中，命令输出提供了一个指示必须采取哪些操作来解决这个问题的消息。(OCPBUGS-4998)
  例如，当使用无效的引导磁盘时，**wait-for** 输出现在如下：

  ```
  "level=info msg=Cluster has hosts requiring user input
  level=debug msg=Host master-1 Expected the host to boot from disk, but it booted the installation image - please reboot and fix boot order to boot from disk QEMU_HARDDISK drive-scsi0-0-0-0 (sda, /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0)
  level=debug msg=Host master-2 Expected the host to boot from disk, but it booted the
  ```

> installation image - please reboot and fix boot order to boot from disk QEMU_HARDDISK drive-scsi0-0-0-0 (sda, /dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0) level=info msg=cluster has stopped installing... working to recover installation"

- 在以前的版本中，安装的集群中 **assisted-installer-controller** 也会持续运行，即使集群完成安装。因为 **assisted-service** 在 bootstrap 节点上运行，而不是在云中运行，且 assisted-service 会在 bootstrap 节点重启后离线，所以 **assisted-installer-controller** 无法与 assisted-service 进行通信，以发布更新和上传日志和循环。现在，**assisted-installer-controller** 在不使用 **assisted-service** 的情况下检查集群安装，并在集群安装完成后退出。(OCPBUGS-4240)

- 在以前的版本中，将集群安装到 AWS Commercial Cloud Services (C2S) **us-iso-east-1** 区域会失败，并显示描述 **UnsupportedOperation** 的错误消息。在这个版本中，安装到此区域可以成功。(OCPBUGS-2324)

- 在以前的版本中，在 AWS 上安装可能会失败，因为安装程序没有使用所需的服务端点创建 **cloud.conf** 文件。这会导致机器配置 Operator 创建一个缺少服务端点的空 **cloud.conf** 文件，从而导致错误。在这个版本中，安装程序总是创建 **cloud.conf** 文件，以便安装成功。(OCPBUGS-20401)

- 在以前的版本中，如果您使用基于 Agent 的安装程序安装集群，且 pull secret 有一个 null **auth** 或 **email** 字段，则安装会失败，而不会提供有用的错误。在这个版本中，**openshift-install agent wait-for install-complete** 命令会验证您的 pull secret，并在有 null 字段时通知您。(OCPBUGS-14405)

- 在以前的版本中，**create agent-config-template** 命令只输出带有 **INFO** 的行，但没有有关该命令成功以及模板文件写入的位置的详细信息。现在，如果命令成功，该命令将输出 **INFO Created Agent Config Template in <path> directory**。(OCPBUGS-13408)

- 在以前的版本中，当用户在 **agent-config.yaml** 文件中指定 **vendor** 提示时，会根据错误字段检查该值，以便提示不匹配。在这个版本中，使用 **vendor** 提示可以正确地选择磁盘。(OCPBUGS-13356)

- 在以前的版本中，当在 AWS 上安装集群时将 **metadataService.authentication** 字段设置为 **Required**，不会将 bootstrap 虚拟机配置为使用 IMDSv2 身份验证。如果您将 AWS 帐户配置为阻止 IMDSv1 身份验证，这可能会导致安装失败。在这个版本中，**metadataService.authentication** 字段在设置为 **Required** 时可以正确地将 bootstrap 虚拟机配置为使用 IMDSv2 身份验证。(OCPBUGS-12964)

- 在以前的版本中，如果您在安装私有 Azure 集群时配置了用户定义的出站路由，集群会错误地使用默认公共负载均衡器部署。使用安装程序置备的基础架构安装集群时发生此行为。在这个版本中，在配置用户定义的路由时，安装程序不再创建公共负载均衡器。(OCPBUGS-9404)

- 在以前的版本中，vSphere Terraform **vsphere_virtual_machine** 资源不包括 **firmware** 参数。此问题导致虚拟机的固件默认设置为 **bios**，而不是 **efi**。现在，资源包含 **firmware** 参数，并将 **efi** 设置为参数的默认值，以便虚拟机运行可扩展固件接口(EFI)而不是基本输入/输出系统(BIOS)接口。(OCPBUGS-9378)

- 在以前的版本中，对于在 RHOSP 上运行的集群，在安装取消置备阶段，安装程序会按顺序删除对象存储容器。这个行为会导致对象的缓慢和低效删除，特别是对于大型容器来说。此问题部分发生，因为使用 Swift 容器随时间积累的对象的镜像流。现在，批量对象删除发生在最多 3 个对 RHOSP API 的调用时，通过每个调用处理较高的对象数来提高效率。此优化可在取消置备过程中加快资源清理速度。(OCPBUGS-9081)

- 在以前的版本中，如果您在 Azure 上安装了集群，在没有提供订阅 ID 的情况下使用磁盘加密，安装程序不会退出。这会导致安装启动，然后在以后只失败。在这个版本中，安装程序要求您为加密的 Azure 安装指定一个订阅 ID，如果不提供，则退出并显示错误。(OCPBUGS-8449)

- 在以前的版本中，基于代理的安装程序显示二级检查的结果，如 **ping** 和 **nslookup**，即使安装成功，也会无害地失败。这可能会导致集群成功安装失败。在这个版本中，只有在主安装检查失败时，二级检查才会显示结果，以便您可以使用二级检查来排除失败的安装。(OCPBUGS-8390)

- 使用带有基于代理的安装程序的 IPI **install-config** 会导致日志消息显示任何未使用字段的内容。在以前的版本中，这些警告会输出敏感信息，如密码。在这个版本中，**vsphere** 和 **baremetal** platform 部分中的 credentials 字段的警告信息已被修改，以避免记录任何敏感信息。(OCPBUGS-8203)

- 在以前的版本中，除非节点有自定义的磁盘大小，否则 Azure Stack Hub 上的集群将无法创建新的 control plane 节点，因为无法验证默认的磁盘大小。在这个版本中，默认磁盘大小被设置为 128 GB，安装程序会在 128 到 1023 GB 之间强制实施用户指定的磁盘大小。(OCPBUGS-6759)

- 在以前的版本中，安装程序在使用安装程序置备的基础架构的裸机上安装时，使用端口 80 向 Baseboard Management Controller (BMC) 和部署代理提供镜像。这可能会造成安全问题，因为许多类型的公共流量都使用端口 80。在这个版本中，安装程序使用端口 6180。(OCPBUGS-8509)

1.6.9. Machine Config Operator

- 在以前的版本中，在 AWS 上安装的 OpenShift Container Platform 集群使用 4.1 引导镜像，它无法进行扩展。出现这个问题的原因是，在初始引导一个新机器期间，由 Ignition 配置然后被 MCO 处理并启动的两个 systemd 单元对应用程序 Afterburn 依赖于应用程序 Afterburn。因为 OpenShift Container Platform 4.1 引导镜像不包含 Afterburn，所以这个问题会阻止新节点加入集群。现在，**systemd** 单元包含对 Afterburn 以及不依赖于 Afterburn 的回退代码的额外检查。(OCPBUGS-7559)

1.6.10. 管理控制台

- 在以前的版本中，警报从非 Prometheus 数据源加载，如日志。这会导致所有警报的来源始终显示为 **Prometheus**。在这个版本中，警报源会被正确显示。(OCPBUGS-9907)

- 在以前的版本中，Patternfly 4 存在一个问题：在已经进行选择后，在 master 节点的 logs 部分无法选择或更改日志组件。在这个版本中，当您在 master 节点的 log 部分更改日志组件时，可以刷新页面以重新载入默认选项。(OCPBUGS-18727)

- 在以前的版本中，当查看 **alertmanager-main** 页面的 **Metrics** 选项卡上的路由详情时，会显示一个空页面。在这个版本中，用户权限已被更新，您可以查看 **Metrics** 选项卡上的路由详情。(OCPBUGS-15021)

- 在以前的版本中，Red Hat OpenShift Service on AWS 使用自定义品牌，favicon 会消失，因此使用自定义品牌时不会出现特定的品牌。在这个版本中，Red Hat OpenShift Service on AWS 品牌是品牌 API 的一部分。(OCPBUGS-14716)

- 在以前的版本中，当预期一个代理时，OpenShift Container Platform Web 控制台不会呈现监控 **Dashboard** 页面。因此，websocket 连接会失败。在这个版本中，Web 控制台还会检测来自环境变量的代理设置。(OCPBUGS-14550)

- 在以前的版本中，如果 operator CSV 中使用 **console.openshift.io/disable-operand delete: "true"** 和 **operator.openshift.io/uninstall-message: "some message"** 注解，则卸载指令不会在 web 控制台中显示。在这个版本中，可以选择不使用安装的说明。(OCPBUGS-13782)

- 在以前的版本中，**PersistentVolumeClaims** 命名空间的 **Details** 页中的大小不正确。在这个版本中，对 **PersistentVolumeClaims** 命名空间的 **Details** 页的 Prometheus 查询会包括命名空间标签，显示的大小是正确的。(OCPBUGS-13208)

- 在以前的版本中，在为控制台和下载自定义路由后，下载路由不会在 **ConsoleCLIDownloads** 链接中更新，并指向默认的下载路由。在这个版本中，当设置自定义下载路由时，**ConsoleCLIDownloads** 链接会更新。(OCPBUGS-12990)

- 在以前的版本中，打印预览从列表视图中显示不完整的拓扑信息。在这个版本中，当资源超过一个页面时，会输出一个完整的资源列表。(OCPBUGS-11219)

- 在以前的版本中，用于代理服务的动态插件有较长的响应时间时，会在 30 秒后超时，并带有 **504** 错误消息。在这个版本中，在控制台路由中添加了 5 分钟 HAProxy 超时注解，以匹配大多数浏览器的最大超时时间。(OCPBUGS-9917)

- 在以前的版本中，提供的 API 页面使用提供的 API 的 **displayName**，但这个值并不总是被设置。因此，列表为空，但您仍可以点所有实例来获取新实例的 YAML。在这个版本中，如果没有设置 **displayName**，列表会显示文本。(OCPBUGS-8682)

- 在以前的版本中，**CronJobs** 表和详情视图没有 **挂起** 指示。在这个版本中，**spec.suspend** 添加到 **CronJobs** 的列表和详情视图中。(OCPBUGS-8299)

- 在以前的版本中，当在 console Operator 配置中启用单个插件时，重新部署的控制台会失败。在这个版本中，插件列表是唯一的，pod 会如预期运行。(OCPBUGS-5059)

- 在以前的版本中，在升级插件镜像后，仍然需要旧的插件文件。在这个版本中，当请求 **plugin-entry.js** 资源时，添加了 **?cacheBuster=${getRandomChars()}** 查询字符串。(OCPBUGS-3495)

1.6.11. 监控

- 在此次更新之前，因为 **node-exporter** 收集网络接口信息的方式，在指标提取过程中可能会消耗大量 CPU 资源。此发行版本解决了这个问题，在收集网络接口信息时提高 **node-exporter** 的性能，从而解决了指标提取过程中 CPU 使用量过多的问题。(OCPBUGS-12714)

- 在此次更新之前，Thanos Querier 无法根据节点角色去除重复数据的指标。在这个版本中解决了这个问题，Thanos Querier 现在根据节点角色正确去除重复数据的指标。(OCPBUGS-12525)

- 在此次更新之前，**node-exporter** 的 **btrfs** 收集器总是被启用，这会导致 CPU 使用量增加，因为 Red Hat Enterprise Linux (RHEL)不支持 **btrfs** 存储格式。在这个版本中，**btrfs** 收集器被禁用，从而解决了这个问题。(OCPBUGS-11434)

- 在此次更新之前，对于 **cluster:capacity_cpu_cores:sum** 指标，具有 **infra** 角色，但没有 **master** 角色的节点，不会为 **label_node_role_kubernetes_io** 标签分配 **infra** 的值。在这个版本中，带有 **infra** 角色而非 **master** 角色的节点可以被正确标记为 **infra**。(OCPBUGS-10387)

- 在此次更新之前，缺少启动探测会阻止 Prometheus Adapter pod 安装许多自定义资源定义时启动 Prometheus Adapter pod，因为程序初始化所需的时间比存活度探测允许的内容要长。在这个版本中，Prometheus Adapter pod 被配置为使用一个启动探测，它会在失败前等待五分钟，从而解决了这个问题。(OCPBUGS-7694)

- **node_exporter** 收集器仅用于为物理接口收集网络接口指标，但在更新之前，**node-exporter** 收集器不会在收集这些指标时排除 Calico Virtual 网络接口控制器 (NIC)。在这个版本中，在 **collector.netclass.ignored-devices** 列表中添加了 **cali[a-f0-9]*** 值，以确保没有为 Calico Virtual NIC 收集指标。(OCPBUGS-7282)

- 在这个版本中，Thanos Querier 默认禁用作为安全措施的跨原始资源共享 (CORS) 标头。如果您仍然需要使用 CORS 标头，您可以通过将 **ThanosQuerierConfig** 资源的 **enableCORS** 参数的值设置为 **true** 来启用它们。(OCPBUGS-11889)

1.6.12. 网络

- 在以前的版本中，当在入口控制器上配置客户端 mutual TLS (mTLS)时，CA 捆绑包中的证书颁发机构(CA)证书需要超过 1 MB 的证书撤销列表(CRL)，因为大小限制而无法更新 CRL 配置映射。由于缺少 CRL，具有有效客户端证书的连接可能会被拒绝，并显示以下错误：**unknown ca**。
  在这个版本中，CRL 不再放在配置映射中，路由器现在直接下载 CRL。因此，每个入口控制器的 CRL 配置映射不再存在。现在，CRL 被直接下载，且与有效客户端证书的连接不再被拒绝。(OCPBUGS-6661)

- 在以前的版本中，提供比 OpenShift Container Platform 指定的缓冲区大小为 512 字节的 UDP 响应的不合规上游 DNS 服务器会导致 CoreDNS 抛出溢出错误。因此，它不会为 DNS 查询提供响应。
  在这个版本中，用户可以在 **dnses.operator.openshift.io** 自定义资源(CR)上配置 **protocolStrategy** 字段，成为 **TCP**。将此字段设置为 TCP 时，CoreDNS 将 **TCP** 协议用于上游请求，并解决与不合规上游 DNS 服务器相关的 UDP 溢出问题。(OCPBUGS-6829)

- 在以前的版本中，如果集群管理员使用具有 **NoExecute** 效果的污点配置了 infra 节点，Ingress Operator 的 canary pod 不会被调度到这些 infra 节点上。一段时间后，DaemonSet 配置将被覆盖，pod 将在 infra 节点上终止。
  在这个版本中，Ingress Operator 将 Canary DaemonSet 配置为容许 **node-role.kubernetes.io/infra** 节点污点，该污点指定了 **NoExecute** 效果。因此，无论指定了哪些效果，canary pod 都会调度到 infra 节点上。(OCPBUGS-9274)

- 在以前的版本中，当在入口控制器上配置客户端 mutual TLS (mTLS)时，如果任何客户端证书颁发机构(CA)证书包含证书撤销列表(CRL)分布点，则不同 CA 发布的 CRL 和 CRL 过期，发布 CA 和发布 CA 间的不匹配会导致下载不正确的 CRL。因此，CRL 捆绑包被更新为包含错误下载 CRL 的额外副本，并且缺少所需的 CRL。由于缺少 CRL，具有有效客户端证书的连接可能会被拒绝，并显示以下错误：**unknown ca**。
  在这个版本中，下载的 CRL 由发布它们的 CA 跟踪。当 CRL 过期时，分发 CA 的 CRL 发布点用于下载更新的 CRL。因此，有效的客户端证书不再被拒绝。(OCPBUGS-9464)

- 在以前的版本中，当为 Red Hat OpenShift Service Mesh 启用 Gateway API 时，Ingress Operator 无法配置并会返回以下错误：**the spec.techPreview.controlPlaneMode field is not supported in version 2.4+; use spec.mode**。在这个版本中，**ServiceMeshControlPlane** 自定义资源 (CR) 中的 Service Mesh **spec.techPreview.controlPlaneMode** API 字段已被 **spec.mode** 替代。因此，Ingress Operator 可以创建 **ServiceMeshControlPlane** 自定义资源，网关 API 可以正常工作。(OCPBUGS-10714)

- 在以前的版本中，当为网关 API 网关配置 DNS 时，Ingress Operator 会尝试为网关监听程序创建 DNS 记录，即使监听程序指定了带有集群基域之外的域的主机名。因此，Ingress Operator 会尝试并失败发布 DNS 记录，并会返回以下错误：**failed to publish DNS record to zone**。
  在这个版本中，当为网关监听程序创建 **DNSRecord** 自定义资源 (CR) 时，如果其域位于集群基域外，Ingress Operator 会将 **DNSRecord** 的 DNS 管理策略设置为 **Unmanaged**。因此，Ingress Operator 不再尝试发布记录，日志中将不再有 **failed to publish DNS record to zone** 错误。(OCPBUGS-10875)

- 在以前的版本中，**oc explain route.spec.tls.insecureEdgeTerminationPolicy** 命令记录了可能对某些用户造成混淆的选项。在这个版本中，API 文档已被更新，它会显示 **insecureEdgeTerminationPolicy** 字段的正确可能选项。这仅是对 API 文档的修复。

(OCPBUGS-11393)

- 在以前的版本中，Cluster Network Operator 控制器监控了比必要数量的更广泛的资源，这会导致其协调器被频繁触发。因此，这会增加 Cluster Network Operator 和 **kube-apiserver** 的负载。
  在这个版本中，Cluster Network Operator **allowlist** 控制器会监控其 **cni-sysctl-allowlist** 配置映射的更改。因此，只有在对 **cni-sysctl-allowlist** 配置映射或 **default-cni-sysctl-allowlist** 配置映射进行修改时，才会触发 **allowlist** 控制器协调器，而不是在任何配置映射改变时都触发。因此，Cluter Network Operator API 请求和配置映射请求会减少。(OCPBUGS-11565)

- 与 HaProxy 相关的 **segfault** 失败已解决。用户不应再收到这些错误。(OCPBUGS-11595)

- 在以前的版本中，如果用户在没有端口号的情况下创建 **EndpointSlice** 端口，CoreDNS 意外终止。在这个版本中，验证被添加到 CoreDNS 中，以防止它意外终止。(OCPBUGS-19805)

- 在以前的版本中，当流量只有一个后端服务时，OpenShift 路由器会将流量定向到一个权重为 **0** 的路由。在这个版本中，路由器不再将流量发送到带有权重 **0** 的单一后端的路由。(OCPBUGS-16623)

- 在以前的版本中，Ingress Operator 在没有指定路由上的 **spec.subdomain** 或 **spec.host** 参数的情况下创建其 Canary 路由。通常，这会导致 API 服务器使用集群的 Ingress 域（与默认 Ingress Controller 的域匹配），为 **spec.host** 参数设置默认值。但是，如果您使用 **appsDomain** 选项配置集群来设置替代 Ingress 域，则路由主机将具有替代域。另外，如果您删除了 Canary 路由，则会使用与默认 Ingress Controller 域不匹配的域重新创建路由，这会导致 canary 检查失败。现在，Ingress Controller 在创建 canary 路由时指定 **spec.subdomain** 参数。如果您使用 **appsDomain** 选项配置集群，然后删除 canary 路由，则 Canary 检查不会失败。(OCPBUGS-16089)

- 在以前的版本中，在更新 Operator 状态时，Ingress Operator 不会检查公共托管区中的 DNS 记录状态。这会导致 Ingress Operator 在公共托管区中 DNS 记录出错时将 DNS 状态报告为 **Ready**。现在，Ingress Operator 会检查公共和私有托管区的状态，从而解决了这个问题。(OCPBUGS-15978)

- 在以前的版本中，CoreDNS **bufsize** 设置配置为 512 字节。现在，OpenShift Container Platform CoreDNS 的最大缓冲区大小为 1232 字节。此修改通过减少 DNS 截断和重试的发生来提高 DNS 性能。(OCPBUGS-15605)

- 在以前的版本中，Ingress Operator 会在路由器部署中指定 **spec.template.spec.hostNetwork: true** 参数，而不指定 **spec.template.spec.containers[].ports[].hostPort**。这会导致 API 服务器为每个端口的 **hostPort** 字段设置默认值，Ingress Operator 会检测到为外部更新并尝试恢复它。现在，Ingress Operator 不再错误地执行这些更新。(OCPBUGS-14995)

- 在以前的版本中，DNS Operator 会在启动时在日志中记录 **cluster-dns-operator startup has an error message: [controller-runtime] log.SetLogger(...) was never called, logs will not be displayed:** 错误信息，这会造成用户误解。现在，启动时不会显示错误消息。(OCPBUGS-14395)

- 在以前的版本中，Ingress Operator 保留了为 **NodePort** 和 **ClusterIP** 类型服务的 **spec.internalTrafficPolicy**、**spec.ipFamilies** 和 **spec.ipFamilyPolicy** 字段。然后，API 会为这些字段设置默认值，Ingress Operator 会尝试恢复这些值。在这个版本中，Ingress Operator 指定一个初始值，并修复了由 API 默认值导致的错误。(OCPBUGS-13190)

- 在以前的版本中，所有 DNS 的传输控制协议 (TCP) 连接都是负载均衡的。在这个版本中，TCP 连接被启用为首选本地 DNS 端点。(OCPBUGS-9985)

- 在以前的版本中，对于 Intel E810 NIC，当 pod 被删除时，在 SR-IOV 上重置 MAC 地址会导致失败。这会导致在使用 SR-IOV VF 创建 pod 时会有一个较长的延迟。在这个版本中，容器网络接口 (CNI) 不会解决这个问题。(OCPBUGS-5892)

- 在以前的版本中，在 OpenShift Container Platform 中发现了一个问题，一些 pod 处于 **terminating** 状态。这会影响允许列表控制器的协调循环，这会导致创建多个 pod 的不需要重试。在这个版本中，允许列表控制器只检查属于当前守护进程集的 pod。因此，当一个或多个 pod 未就绪时，重试不再发生。(OCPBUGS-16019)

1.6.13. OpenShift CLI (oc)

- 在以前的版本中，oc-mirror 插件没有正确解释带有 tag 和 digest 的容器镜像引用，并导致以下错误：

  > "localhost:6000/cp/cpd/postgresql:13.7@sha256" is not a valid image reference: invalid reference format

  这个行为已被修复，现在接受并正确镜像引用。(OCPBUGS-11840)

- 在以前的版本中，您收到 **401 - Unauthorized** 错误，其中路径组件数超过预期的最大路径组件。这个问题已通过确保在路径组件数量超过最大路径组件时 oc-mirror 会失败。现在，您可以使用 **--max-nested-paths** 标记（接受整数值）设置最大路径组件。默认情况下，最大路径组件没有限制，设置为 **0**。生成的 **ImageContentSourcePolicy** 将包含到存储库级别的源和镜像引用。(OCPBUGS-8111, OCPBUGS-11910, OCPBUGS-11922)

- 在以前的版本中，oc-mirror 标志 **--short**、**-v** 和 **--verbose** 提供了不正确的版本信息。现在，您可以使用 oc mirror **version** 标志，以了解正确的 oc-mirror 版本。oc-mirror 标志 **--short**,**-v**, 和 **--verbose** 已被弃用，并将不再被支持。(OCPBUGS-7845)

- 在以前的版本中，当在 **imageSetConfig** 中指定了一些镜像摘要时，从 registry 镜像到磁盘会失败，且没有标签。oc-mirror 会将默认标签 **latest** 添加到镜像中。现在，这个问题已通过使用截断的摘要作为标签来解决。(OCPBUGS-2633)

- 在以前的版本中，oc-mirror 会错误地将 Operator 目录添加到 **ImageContentSourcePolicy** 规格中。这是一个意外的行为，因为 Operator 目录通过 **CatalogSource** 资源直接从目标 registry 中使用。这个程序错误已通过确保 oc-mirror 不将 Operator 目录添加为 **ImageContentSourcePolicy** 的条目来解决。(OCPBUGS-10051)

- 在以前的版本中，当 registry 域名不是镜像引用的一部分时，Operator 的镜像会失败。在这个版本中，如果没有指定 registry 域名，则会从 **docker.io** 下载镜像。(OCPBUGS-10348)

- 在以前的版本中，当容器镜像引用中包含 tag 和 digest 时，oc-mirror 会错误地解释它会导致 **invalid reference format** 错误。这个问题已被解决，镜像已被成功镜像（mirror）。(OCPBUGS-11840)

- 在以前的版本中，如果名称以数字开头，则无法创建 **CatalogSource** 资源。在这个版本中，**CatalogSource** 资源名称使用 **cs-** 前缀生成，并与 RFC 1035 兼容。(OCPBUGS-13332)

- 在以前的版本中，当使用 **registry.conf** 文件时，一些镜像没有包含在映射中。在这个版本中，您可以看到映射中包含的镜像，且没有任何错误。(OCPBUGS-13962)

- 在以前的版本中，当在 **--oci-registries-config** 选项中引用的 **registries.conf** 文件中使用了非安全的镜像（mirror）时，oc-mirror 会尝试与 mirror registry 建立 HTTPS 连接。在这个版本中，您可以通过在命令行中指定 **--source-skip-tls** 或 **--source-use-http**，将 oc-mirror 配置为不使用 HTTPS 连接。(OCPBUGS-14402)

- 在以前的版本中，当您试图使用 oc-mirror 插件镜像 OCI 索引时，对镜像进行镜像（mirror）会失败。在这个版本中，您可以使用 oc-mirror 插件镜像 OCI 索引。(OCPBUGS-15329)

- 在以前的版本中，当在低带宽网络上镜像多个大型目录时，因为过期的身份验证令牌导致 **HTTP 401 unauthorized** 错误，镜像会被中断。这个问题现已解决，在启动每个目录的镜像过程前刷新身份验证令牌。(OCPBUGS-20137)

1.6.14. Operator Lifecycle Manager (OLM)

- 在此次更新之前，Operator Lifecycle Manager (OLM) 可能会导致安装失败，因为 API 服务器忙碌时初始化错误。在这个版本中，为初始化错误添加了一个一分钟重试间隔来解决这个问题。(OCPBUGS-13128)

- 在此次更新之前，如果自定义目录在断开连接的环境中使用与默认红帽目录相同的名称，则会出现竞争条件。如果禁用了默认红帽目录，则目录会在 OperatorHub 自定义资源 (CR) 协调后在启动时创建并删除。因此，自定义目录会与默认的红帽目录一起删除。在这个版本中，OperatorHub CR 在删除任何目录前被协调，从而导致竞争条件。(OCPBUGS-9357)

- 在此次更新之前，一些 Operator 的频道以随机顺序显示在 OperatorHub 中。在这个版本中，Operator 频道以字典顺序显示。(OCPBUGS-7910)

- 在此次更新之前，如果所有者引用文件中没有将 controller 标记设置为 true，则 registry pod 不会由自动扩展安全地排空。在这个版本中，controller 标记被设置为 true，排空节点不再需要强制关闭。(OCPBUGS-7431)

- 在此次更新之前，**collect-profiles** pod 可能会因为生成证书的方式导致常规的 CPU 用量激增。在这个版本中，证书是每天生成的，证书的加载被优化，CPU 用量较低。(OCPBUGS-1684)

1.6.15. OpenShift API 服务器

- 在以前的版本中，在更新和打补丁请求 **projects** 时，**metadata.namespace** 字段会自动填充。因此，受影响的请求会生成错误的验证错误。在这个版本中，**projects** 资源不再自动填充。(OCPBUGS-8232)

1.6.16. Red Hat Enterprise Linux CoreOS (RHCOS)

- 在以前的版本中，在 OpenShift Container Platform 中，使用逻辑卷管理器存储的、带有逻辑卷管理器(LVM)元数据的 OpenShift Container Platform 中的 pod 在终止时可能会卡住。这是因为相同的 LVM 设备在容器和主机上的同时处于活动状态。当在使用 OpenShift Virtualization 的 pod 中运行虚拟机时，会针对虚拟机使用 LVM。在这个版本中，RHCOS 默认只尝试设置和访问位于 **/etc/lvm/devices/system.devices** 文件中的设备。这可防止虚拟机客户机内对 LVM 设备进行内容访问。(OCPBUGS-5223)

- 在以前的版本中，Google Cloud Platform（GCP）Confidential Computing 实例中的 pod 可能会一直处于 **ContainerCreating** 状态，这会导致卷挂载失败。在这个版本中，增加了对 Google Cloud Platform 中机密计算实例的 Persistent Disk 存储类型的支持，它可用作 OpenShift Container Platform 中的持久性卷。因此，pod 可以进入 **Running** 状态，并且可以挂载卷。(OCPBUGS-7582)

1.6.17. 存储

- 在以前的版本中，当在 IBM Cloud® 集群上启用集群范围代理时，无法置备卷。(OCPBUGS-18142)

- Storage Operator 对象的 **vsphereStorageDriver** 字段已弃用。此字段用于选择在 OpenShift Container Platform 4.13 vSphere 集群上进行 CSI 迁移，但它对 OpenShift Container Platform 4.14 及更新版本没有影响。(OCPBUGS-13914)

1.7. 技术预览功能

此版本中的一些功能当前还处于技术预览状态。它们并不适用于在生产环境中使用。请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*

1.7.1. 网络功能虚拟化功能

表 1.17. 网络技术预览跟踪器

功能	4.12	4.13	4.14
PTP dual NIC 硬件配置为边界时钟	技术预览	公开发行	公开发行
额外网络接口上的出口 IP	不可用	不可用	公开发行
Intel E810 Westport Channel NIC 作为 PTP grandmaster 时钟	不可用	技术预览	技术预览
双 Intel E810 Westport Channel NIC 作为 PTP grandmaster 时钟	不可用	不可用	技术预览
Ingress Node Firewall Operator	技术预览	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	技术预览	技术预览	技术预览
SR-IOV 网络的多网络策略	技术预览	技术预览	技术预览
OVN-Kubernetes 网络插件作为二级网络	不可用	技术预览	公开发行
更新特定于接口的安全 sysctl 列表	技术预览	技术预览	技术预览
MT2892 系列 [ConnectX-6 Dx] SR-IOV 支持	技术预览	公开发行	公开发行
MT2894 系列 [ConnectX-6 Lx] SR-IOV 支持	技术预览	公开发行	公开发行

功能	4.12	4.13	4.14
ConnectX-6 NIC 模式的 MT42822 BlueField-2 的 SR-IOV 支持	技术预览	公开发行	公开发行
Silicom STS 系列的 SR-IOV 支持	技术预览	公开发行	公开发行
MT2892 系列 [ConnectX-6 Dx] OvS Hardware Offload 支持	技术预览	公开发行	公开发行
MT2894 系列 [ConnectX-6 Lx] OvS Hardware Offload 支持	技术预览	公开发行	公开发行
ConnectX-6 NIC 模式的 MT42822 BlueField-2 的 OvS Hardware Offload 支持	技术预览	公开发行	公开发行
将 Bluefield-2 从 DPU 切换到 NIC	技术预览	公开发行	公开发行
Intel E810-XXVDA4T	不可用	公开发行	公开发行
出口服务自定义资源	不可用	不可用	技术预览
BGPPeer 自定义资源中的 VRF 规格	不可用	不可用	技术预览
NodeNetworkConfigurationPolicy 自定义资源中的 VRF 规格	不可用	不可用	技术预览
Admin Network Policy (**AdminNetworkPolicy**)	不可用	不可用	技术预览
IPsec 外部流量 (north-south)	不可用	不可用	技术预览

1.7.2. 存储技术预览功能

表 1.18. 存储技术预览

功能	4.12	4.13	4.14
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
Google Filestore CSI Driver Operator	技术预览	技术预览	公开发行
CSI 自动迁移 (Azure 文件、VMware vSphere)	技术预览	公开发行	公开发行
CSI inline 临时卷	技术预览	公开发行	公开发行
IBM Power® Virtual Server Block CSI Driver Operator	不可用	技术预览	技术预览
Azure File CSI Operator Driver 的 NFS 支持	正式发布	正式发布	正式发布
Read Write Once Pod 访问模式	不可用	不可用	技术预览

功能	4.12	4.13	4.14
在 OpenShift 构建中构建 CSI 卷	技术预览	技术预览	公开发行
OpenShift 构建中的共享资源 CSI 驱动程序	技术预览	技术预览	技术预览
Secret Store CSI Driver Operator	不可用	不可用	技术预览

1.7.3. 安装技术预览功能

表 1.19. 安装技术预览

功能	4.12	4.13	4.14
使用 kvc 向节点添加内核模块	技术预览	技术预览	技术预览
Azure 标记	不可用	技术预览	公开发行
为 SR-IOV 设备启用 NIC 分区	不可用	技术预览	技术预览
GCP 机密虚拟机	不可用	技术预览	公开发行
Google Cloud Platform (GCP) 的用户定义的标记和标签	不可用	不可用	技术预览
使用安装程序置备的基础架构在 Alibaba Cloud 上安装集群	技术预览	技术预览	技术预览
在 RHEL 中的 BuildConfig 中挂载共享权利	技术预览	技术预览	技术预览
多架构计算机器	技术预览	公开发行	公开发行
AWS Outposts 平台	技术预览	技术预览	技术预览
在带有虚拟机的 Oracle® Cloud Infrastructure (OCI) 上安装 OpenShift Container Platform	N/A	N/A	公开发行
在裸机上的 Oracle® Cloud Infrastructure (OCI)上安装 OpenShift Container Platform	N/A	开发者预览	开发者预览
可选择 Cluster Inventory	技术预览	技术预览	技术预览
使用 vSphere 的静态 IP 地址（仅限IPI）	不可用	不可用	技术预览

1.7.4. 节点技术预览功能

表 1.20. 节点技术预览

功能	4.12	4.13	4.14
Linux Control Group 版本 2 (cgroup v2)	技术预览	公开发行	公开发行
crun 容器运行时	技术预览	公开发行	公开发行
Cron job 时区	技术预览	技术预览	公开发行
MaxUnavailableStatefulSet 功能集	不可用	不可用	技术预览

1.7.5. 多架构技术预览功能

表 1.21. 多架构技术预览

功能	4.12	4.13	4.14
IBM Z® 和 IBM® LinuxONE 上的 IBM Secure Execution	技术预览	公开发行	公开发行
使用安装程序置备的基础架构的 IBM Power® Virtual Server	不可用	技术预览	技术预览
arm64 构架上的 **kdump**	技术预览	技术预览	技术预览
s390x 架构上的 **kdump**	技术预览	技术预览	技术预览
ppc64le 架构上的 **kdump**	技术预览	技术预览	技术预览

1.7.6. 专用硬件和驱动程序启用技术预览功能

表 1.22. 专用硬件和驱动程序启用技术预览

功能	4.12	4.13	4.14
驱动程序工具包	公开发行	公开发行	公开发行
hub 和 spoke 集群的支持	技术预览	公开发行	公开发行

1.7.7. 可扩展性和性能技术预览功能

表 1.23. 可扩展性和性能技术预览

功能	4.12	4.13	4.14
调整 etcd 延迟容错功能	不可用	不可用	技术预览
超线程感知 CPU Manager 策略	技术预览	技术预览	技术预览

功能	4.12	4.13	4.14
Node Observability Operator	技术预览	技术预览	技术预览
factory-precaching-cli 工具	不可用	技术预览	技术预览
使用 worker 节点的单节点 OpenShift 集群扩展	技术预览	公开发行	公开发行
Topology Aware Lifecycle Manager (TALM)	技术预览	公开发行	公开发行
挂载命名空间封装	不可用	技术预览	技术预览
使用 NUMA Resources Operator 进行 NUMA 感知调度	技术预览	公开发行	公开发行
HTTP 传输替换了 PTP 和裸机事件的 AMQP	不可用	技术预览	技术预览
三节点集群和标准集群的工作负载分区	不可用	技术预览	公开发行

1.7.8. Operator 生命周期和开发技术预览功能

表 1.24. Operator 生命周期和开发技术预览

功能	4.12	4.13	4.14
Operator Lifecycle Manager (OLM) v1	不可用	不可用	技术预览
RukPak	技术预览	技术预览	技术预览
平台 Operator	技术预览	技术预览	技术预览
混合 Helm Operator	技术预览	技术预览	技术预览
基于 Java 的 Operator	技术预览	技术预览	技术预览

1.7.9. 监控技术预览功能

表 1.25. 监控技术预览

功能	4.12	4.13	4.14
基于平台监控指标的警报规则	技术预览	技术预览	公开发行
指标集合配置集	不可用	技术预览	技术预览

1.7.10. 托管 control plane 技术预览功能

表 1.26. 托管 control plane 技术预览

功能	4.12	4.13	4.14
在 Amazon Web Services (AWS) 上托管 OpenShift Container Platform 的 control plane。	技术预览	技术预览	技术预览
在裸机上托管 OpenShift Container Platform 的 control plane	技术预览	技术预览	公开发行
在 OpenShift Virtualization 上为 OpenShift Container Platform 托管 control plane	不可用	技术预览	公开发行
在 AWS 上托管 ARM64 OpenShift Container Platform 集群的 control plane	不可用	技术预览	技术预览
在 IBM Power 上托管 OpenShift Container Platform 的 control plane	不可用	不可用	技术预览
在 IBM Z 上托管 OpenShift Container Platform 的 control plane	不可用	不可用	技术预览

1.7.11. 机器管理技术预览功能

表 1.27. 机器管理技术预览

功能	4.12	4.13	4.14
使用 Amazon Web Services 的集群 API 管理机器	技术预览	技术预览	技术预览
使用 Google Cloud 的集群 API 管理机器	技术预览	技术预览	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	公开发行
Google Cloud Platform 的云控制器管理器	技术预览	技术预览	技术预览
IBM Cloud Power VS 的云控制器管理器	不可用	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	公开发行
Nutanix 的云控制器管理器	技术预览	公开发行	公开发行
VMware vSphere 的云控制器管理器	技术预览	公开发行	公开发行

1.7.12. 认证和授权技术预览功能

表 1.28. 认证和授权技术预览

功能	4.12	4.13	4.14
Pod 安全准入限制强制	技术预览	技术预览	技术预览

1.7.13. Machine Config Operator 技术预览功能

表 1.29. Machine Config Operator 技术预览

功能	4.12	4.13	4.14
Red Hat Enterprise Linux CoreOS (RHCOS) 镜像分层	技术预览	公开发行	公开发行

1.8. 已知问题

- **libreswan** 中存在一个回归问题，会导致某些启用了 IPsec 的节点丢失与同一集群中其他节点上的 pod 的通信。要解决这个问题，请考虑为集群禁用 IPsec。(OCPBUGS-42952)
- 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 4.14 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)

- **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)
- 如果安装程序无法获取与 Google Cloud Platform (GCP)服务帐户关联的所有项目，安装会失败，并显示 **context deadline exceeded** 错误消息。
  当满足以下条件时会出现这种情况：
  - 服务帐户可以访问过多的项目。
  - 安装程序使用以下命令之一运行：
    - **openshift-install create install-config**

      错误消息

      > FATAL failed to fetch Install Config: failed to fetch dependency of "Install Config": failed to fetch dependency of "Base Domain": failed to generate asset "Platform": failed to get projects: context deadline exceeded

    - **openshift-install create cluster** 没有现有安装配置文件 (**install-config.yaml**)

      错误消息

      > FATAL failed to fetch Metadata: failed to fetch dependency of "Metadata": failed to fetch dependency of "Cluster ID": failed to fetch dependency of "Install Config": failed to fetch dependency of "Base Domain": failed to generate asset "Platform": failed to get projects: context deadline exceeded

    - 带有现有安装配置文件创建清单的 **openshift-install**

      错误消息

      > ERROR failed to fetch Master Machines: failed to load asset "Install Config": failed to create install config: platform.gcp.project: Internal error: context deadline exceeded

      作为临时解决方案，如果您有一个安装配置文件，使用特定的项目 ID 更新该文件，使其使用 **platform.gcp.projectID**。否则，手动创建安装配置文件，并输入特定的项目 ID。再次运行安装程序，指定该文件。(OCPBUGS-15238)
- 在大型计算节点上引导失败。(OCPBUGS-20075)
- 当您在 IBM Power® 上部署带有 Network Type 为 **OVNKubernetes** 的集群时，计算节点可能会因为内核堆栈溢出而重启。作为临时解决方案，您可以使用 Network Type 为 **OpenShiftSDN** 部署集群。(RHEL-3901)

- 以下已知问题适用于使用版本 candidate 3 或 4 将 OpenShift Container Platform 部署更新至版本 4.14 的用户：
  在引入节点识别功能后，一些以 root 身份运行的 pod 会被更新为运行非特权。对于升级到 OpenShift Container Platform 4.14 的早期访问版本的用户，试图升级到官方版本的 4.14 可能无法进行。在这种情况下，Network Operator 报告以下状态，表示更新的问题：**DaemonSet "/openshift-network-node-identity/network-node-identity" update is rolling**。

  作为临时解决方案，您可以通过运行以下命令来删除 **openshift-network-node-identify** 命名空间中的所有 pod：**oc delete --force=true -n openshift-network-node-identity --all pods**。运行此命令后，更新将继续。

  有关早期访问的更多信息，candidate-4.14 频道。

- 目前，用户无法通过更新 **openshift-multus** 命名空间中的 **cni-sysctl-allowlist** 配置映射来修改**特定于接口**的安全 sysctl 列表。作为临时解决方案，您可以手动修改或使用 DaemonSet，也可以修改节点或节点上的 **/etc/cni/tuning/allowlist.conf** 文件。(OCPBUGS-11046)

- 在 OpenShift Container Platform 4.14 中，所有节点都使用 Linux 控制组版本 2 (cgroup v2) 进行内部资源管理，以便与默认的 RHEL 9 配置保持一致。但是，如果您在集群中应用性能配置集，与性能配置集关联的低延迟调整功能不支持 cgroup v2。
  因此，如果您应用一个性能配置集，集群的所有节点都会重启，并切回到 cgroup v1 配置。此重启包括 control plane 节点和不是由性能配置集为目标的 worker 节点。

  要将集群中的所有节点恢复到 cgroups v2 配置，您必须编辑 **Node** 资源。如需更多信息，请参阅配置 Linux cgroup v2 。您无法通过删除最后一个性能配置集将集群恢复到 cgroups v2 配置。(OCPBUGS-16976)

- AWS **M4** 和 **C4** 实例可能无法在使用 OpenShift Container Platform 4.14 安装的集群中正确引导。没有当前的临时解决方案。(OCPBUGS-17154)

- 本发行版本中存在一个已知问题，可防止使用安装程序置备的基础架构在 Alibaba Cloud 上安装集群。在 Alibaba Cloud 上安装集群是本发行版本中的技术预览功能。(OCPBUGS-20552)

- 对于具有根卷可用区且在升级到 4.14 的 RHOSP 上运行的集群，您必须将 control plane 机器聚合到一个服务器组中，然后才能启用 control plane 机器集。要进行必要的更改，请按照知识库文章中的说明操作。(OCPBUGS-13300)

- 对于配置有至少一个区且在 RHOSP 上运行的计算区的集群，它只适用于版本 4.14，根卷现在还必须配置至少一个区。如果没有更改此配置更改，则无法为集群生成 control plane 机器集。要进行必要的更改，请按照知识库文章中的说明操作。(OCPBUGS-15997)

- 目前，当删除使用 SR-IOV 网络设备的 pod 时，可能会出现错误。这个错误是由 RHEL 9 中的更改造成的，其中之前网络接口的名称会在重命名时添加到其替代名称列表中。因此，当删除附加到 SR-IOV 虚拟功能 (VF) 的 pod 时，VF 会返回具有新的意外名称的池，如 **dev69**，而不是其原始名称，如 **ensf0v2**。虽然这个错误不严重，但 Multus 和 SR-IOV 日志可能会在系统自行恢复时显示错误。由于这个错误，删除 pod 可能需要几秒钟时间。(OCPBUGS-11281, OCPBUGS-18822, RHEL-5988)

- 从 **RHEL 5.14.0-284.28.1.el9_2** 开始，如果您使用特定的 MAC 地址配置 SR-IOV 虚拟功能，则 i40e 驱动程序中可能会出现配置错误。因此，Intel 7xx 系列 NIC 可能会有连接问题。作为临时解决方案，请避免在 Pod 资源的 **metadata.annotations** 字段中指定 MAC 地址。反之，使用驱动程序分配给虚拟功能的默认地址。(RHEL-7168, OCPBUGS-19536, OCPBUGS-19407, OCPBUGS-18873)

- 目前，在 **Tuned** 资源的 **profile** 字段中使用斜杠（如绑定设备）定义 **sysctl** 值可能无法正常工作。**sysctl** 选项名称中的斜杠值没有正确映射到 **/proc** 文件系统。作为临时解决方案，创建一个

MachineConfig 资源，该资源使用 **/etc/sysctl.d** 节点目录中的所需值放置配置文件。(RHEL-3707)

- 目前，由于 Kubernetes 存在问题，CPU Manager 无法将来自最后一个 pod 的 CPU 资源从接受到节点返回到可用 CPU 资源池。如果后续 pod 被接受到节点，则可以分配这些资源。但是，这会变为最后一个 pod，再次显示 CPU 管理器无法将此 pod 的资源返回到可用的池。
此问题会影响 CPU 负载均衡功能，因为这些功能取决于 CPU Manager 将 CPU 释放到可用池。因此，非保证的 pod 可能会以较少的 CPU 运行。作为临时解决方案，请在受影响节点上调度具有 **best-effort** CPU Manager 策略的 pod。此 pod 将是最后允许的一个 pod，确保资源已正确释放到可用池。(OCPBUGS-17792)

- 目前，Machine Config Operator (MCO) 可能会为自定义池应用不正确的 cgroup 版本参数，因为 MCO 如何处理 worker 池和自定义池的机器配置。因此，自定义池中的节点可能具有不正确的 cgroup 内核参数，从而导致行为无法预计。作为临时解决方案，请只为 worker 和 control plane 池指定 cgroup 版本内核参数。(OCPBUGS-19352)

- 目前，由于物理网络设备上的 **udev** 规则应用程序和默认请求的每秒应用程序(RPS)掩码到所有网络设备之间有一个竞争条件，一些物理网络设备可能具有错误的 RPS 掩码配置。因此，性能下降可能会影响带有错误 RPS 掩码配置的物理网络设备。预计即将推出的 z-stream 版本会包括此问题的一个修复。(OCPBUGS-21845)

- 在传统的单根 I/O 虚拟化 (SR-IOV) 中的 Broadcom 网络接口控制器不支持 SRIOV VLAN 的服务质量 (QoS) 和标签协议标识符 (TPID) 设置。这会影响 Broadcom BCM57414、Broadcom BCM57508 和 Broadcom BCM57504。(RHEL-9881)

- 当您在使用双栈网络的环境中创建托管集群时，您可能会遇到以下与 DNS 相关的问题：

  - **service-ca-operator** pod 中的 **CrashLoopBackOff** 状态：当 pod 试图通过托管的 control plane 访问 Kubernetes API 服务器时，pod 无法访问服务器，因为 **kube-system** 命名空间中的 data plane 代理无法解析请求。出现这个问题的原因是，前端使用 IP 地址，后端使用 pod 无法解析的 DNS 名称。

  - Pod 处于 **ContainerCreating** 状态 ：出现这个问题，因为 **openshift-service-ca-operator** 无法生成 DNS pod 需要 DNS 解析的 **metrics-tls** secret。因此，pod 无法解析 Kubernetes API 服务器。

  要解决这个问题，请按照 为双堆栈网络配置 DNS 中的指南来配置 DNS 服务器设置。(OCPBUGS-22753, OCPBUGS-23234)

- 在 OpenShift Container Platform 托管的 control plane 中，没有测试以下 Operator 和组件 (OCPSTRAT-605)：

  - Performance Addon Operator
  - OpenShift 沙盒容器
  - Red Hat OpenShift GitOps
  - Red Hat OpenShift Service Mesh
  - Red Hat OpenShift Pipelines
  - Red Hat OpenShift Dev Spaces
  - 红帽单点登录技术
  - OpenShift Container Platform Web 控制台中的 Web 终端

  - 应用程序的迁移工具包

- 在 OpenShift Container Platform 托管的 control plane 中，在托管集群中安装 File Integrity Operator 会失败。(OCPBUGS-3410)

- 在 OpenShift Container Platform 托管的 control plane 中，Vertical Pod Autoscaler Operator 无法在一个托管的集群中安装。(PODAUTO-65)

- 在托管 OpenShift Container Platform 的 control plane 中，在裸机和 OpenShift Virtualization 平台上，自动修复功能被禁用。(OCPBUGS-20028)

- 在 OpenShift Container Platform 托管 control plane 中，不支持使用带有 AWS Secrets Manager 或 AWS Systems Manager Parameter Store 的 Secrets Store CSI Driver Operator。(OCPBUGS-18711)

- 在 OpenShift Container Platform 托管的 control plane 中，**default**, **kube-system**, 和 **kube-public** 命名空间没有正确排除在 pod 安全准入中。(OCPBUGS-22379)

- 在 OpenShift Virtualization 上的托管 control plane 中，worker 节点重启后可能会丢失网络连接。(OCPBUGS-23208)

- 在 OpenShift Container Platform 托管的 control plane 中，HyperShift Operator 仅在 Operator 初始化过程中提取发行版本元数据一次。当您在管理集群中进行更改或创建托管集群时，HyperShift Operator 不会刷新发行版本元数据。作为临时解决方案，请通过删除 pod 部署来重启 HyperShift Operator。(OCPBUGS-29110)

- 在 OpenShift Container Platform 托管的 control plane 中，当您在断开连接的环境中为 **ImageDigestMirrorSet** 和 **ImageContentSourcePolicy** 对象创建自定义资源定义 (CRD) 时，Hy HyperShift Operator 只为 **ImageDigestMirrorSet** CRD 创建对象，忽略 **ImageContentSourcePolicy** CRD。作为临时解决方案，在 **ImageDigestMirrorSet** CRD 中复制 **ImageContentSourcePolicies** 对象配置。(OCPBUGS-29466)

- 在 OpenShift Container Platform 托管 control plane 中，当在断开连接的环境中创建托管集群时，如果您没有明确在 **HostedCluster** 资源中设置 **hypershift.openshift.io/control-plane-operator-image** 注解，则托管集群部署会失败，并显示错误。(OCPBUGS-29494)

- 由于删除节点污点失败，在 vSphere 上安装基于代理的会失败，这会导致安装处于待处理状态。单节点 OpenShift 集群不会受到影响。您可以运行以下命令来手动删除节点污点，从而解决这个问题：

  ```
  $ oc adm taint nodes <node_name>
  node.cloudprovider.kubernetes.io/uninitialized:NoSchedule-
  ```

  (OCPBUGS-20049)

- 使用 Azure 机密虚拟机存在一个已知问题，本发行版本中是一个技术预览功能。不支持将集群配置为加密受管磁盘以及 Azure VM Guest State (VMGS) blob，并带有平台管理的密钥(PMK)或客户管理的密钥(CMK)。要避免这个问题，请通过将 **securityEncryptionType** 参数的值设置为 **VMGuestStateOnly** 来启用 VMGS blob 的加密。(OCPBUGS-18379)

- 使用 Azure 机密虚拟机存在一个已知问题，本发行版本中是一个技术预览功能。安装配置为使用这个功能的集群会失败，因为 control plane 置备过程会在 30 分钟后超时。
  如果出现这种情况，您可以第二次运行 **openshift-install create cluster** 命令来完成安装。

  要避免这个问题，您可以使用机器集在现有集群上启用机密虚拟机。(OCPBUGS-18488)

- 当您在裸机平台上为 OpenShift Container Platform 运行托管的 control plane 时，如果 worker 节点失败，另一个节点也不会自动添加到托管集群中，即使其他代理可用。作为临时解决方案，请手动删除与故障 worker 节点关联的机器。(MGMT-15939)

- 由于源目录捆绑包了一个特定于架构的 **opm** 二进制文件，因此您必须从该架构运行镜像。例如，如果要镜像 ppc64le 目录，则必须从 ppc64le 架构上运行的系统运行 oc-mirror。(OCPBUGS-22264)

- 如果多个 OpenShift Container Platform 组指向同一 LDAP 组，则只同步一个 OpenShift Container Platform 组。当多个组指向同一 LDAP 组时，**oc adm groups sync** 命令会显示一个警告，表示只有一个组有资格映射。(OCPBUGS-11123)

- 当在禁用安全引导的节点中安装 **bootMode** 设置为 **UEFISecureBoot** 的 OpenShift Container Platform 时，安装会失败。后续尝试安装启用了安全引导机制的 OpenShift Container Platform 通常会进行。(OCPBUGS-19884)

- 在 OpenShift Container Platform 4.14 中，带有 Ignition 版本 3.4 的 **MachineConfig** 对象可能无法扫描带有 **CrashLoopBackOff** 错误的 **api-collector** pod，从而导致 Compliance Operator 无法按预期工作。(OCPBUGS-18025)

- 在 OpenShift Container Platform 4.14 中，不支持将 IPv6 出口 IP 分配给不是主网络接口的网络接口。这是一个已知问题，并将在以后的 OpenShift Container Platform 版本中解决。(OCPBUGS-17637)

- 在由 HyperShift Operator 管理的集群中安装 Run Once Duration Override Operator (RODOO)。(OCPBUGS-17533)

- 当您在 OpenShift Container Platform 集群上运行 CNF 延迟测试时，**oslat** 测试有时会返回大于 20 微秒的结果。这会导致 **oslat** 测试失败。(RHEL-9279)

- 当您将 **preempt-rt** 补丁与实时内核一起使用，并更新网络中断的 SMP 关联性时，对应的 IRQ 线程不会立即接收更新。相反，更新会在收到下一个中断时生效，然后线程会迁移到正确的内核。(RHEL-9148)

- 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 Westport Channel e810 NIC 中的全局导航 satellite 系统(GNSS)模块配置为 grandmaster 时钟(T-GM)可以报告 GPS **FIX** 状态以及 GNSS 模块和 GNSS constellation satellites 之间的 GNSS 偏移。
  当前 T-GM 实现不使用 **ubxtool** CLI 来探测 **ublox** 模块来读取 GNSS 偏移和 GPS **FIX** 值。相反，它使用 **gpsd** 服务来读取 GPS **FIX** 信息。这是因为 **ubxtool** CLI 的当前实现需要 2 秒才能接收响应，每个调用都会增加 CPU 用量 3 倍。(OCPBUGS-17422)

- 在来自 GNSS 的 PTP grandmaster 时钟中，当 GNSS 信号丢失时，数字阶段锁定循环(DPLL)时钟状态可能会以 2 种方式改变：它可以过渡到解锁，或者可以进入 holdover 状态。目前，驱动程序默认将 DPLL 状态转换为解锁。上游更改目前正在开发来处理冻结状态功能，并配置使用哪些状态机器处理。(RHELPLAN-164754)

- DPLL 子系统和 DPLL 支持目前没有在 Intel Westport Channel e810 NIC ice 驱动程序中启用。(RHELPLAN-165955)

- 当前 grandmaster 时钟(T-GM)实现具有来自 GNSS 的单一 NMEA 句子生成器，而无需备份 NMEA 生成器。如果在到 e810 NIC 的过程中 NMEA 句子丢失，则 T-GM 无法同步网络同步链中

的设备，而 PTP Operator 会报告错误。当 NMEA 字符串丢失时，可以报告 **FREERUN** 事件。(OCPBUGS-19838)

- 目前，由于设置容器的 cgroup 层次结构的不同，使用 **crun** OCI 运行时的容器以及 **PerformanceProfile** 配置会遇到性能下降。作为临时解决方案，请使用 **runc** OCI 容器运行时。虽然 **runc** 容器运行时在容器启动、关闭操作和 **exec** 探测过程中的性能较低，但 **crun** 和 **runc** 容器运行时的功能相同。预计即将推出的 z-stream 版本会包括此问题的一个修复。(OCPBUGS-20492)

- 在运行时启用和禁用 IPsec 后存在一个已知问题，导致集群处于不健康状态，并显示错误消息：**an unknown error has occurred: MultipleErrors**。(OCPBUGS-19408)

- 使用调度到 control plane 节点的 Microsoft Azure File NFS 卷创建 pod 会导致挂载被拒绝。要临时解决这个问题：如果您的 control plane 节点可以调度，pod 可以在 worker 节点上运行，使用 **nodeSelector** 或 Affinity 将 pod 调度到 worker 节点上。(OCPBUGS-18581)

- 对于在 RHOSP 17.1 上运行并使用网络功能虚拟化 (NFV) 的集群，RHOSP 中的已知问题会阻止成功部署。这个问题还没有临时解决方案。联系红帽支持以请求热修补代码。(BZ#2228643)

- 不支持 RHOSP 17.1 上的 Kuryr 安装。

- 目前，在 OpenShift Container Platform 4.14 中升级到 HAProxy 版本 2.6.13 会导致对重新加密流量的 P99 延迟增加。当入口流量的卷将 **IngressController** 自定义资源 (CR) 的 HAProxy 组件置于可考虑的负载下时，会观察到这个行为。延迟增加并不会影响整体吞吐量，它仍然是一致的。默认 **IngressController** CR 配置有 4 个 HAProxy 线程。如果您在高入口流量条件中遇到了 P99 延迟，特别是使用重新加密流量，建议增加 HAProxy 线程的数量来缩短延迟。(OCPBUGS-18936)

- 对于 4.14 和 Google Cloud Platform (GCP) 上的单节点 OpenShift，Cloud Network Config Controller (CNCC) 进入 **CrashLoopBackOff** 状态存在一个已知问题。当 CNCC 试图访问 GCP 内部负载均衡器地址时，生成的 hairpin 流量不会在 GCP 上的 OVN-Kubernetes 共享网关模式中正确阻止，从而导致它被丢弃。在这种情况下，Cluster Network Operator 会显示 **Progressing=true** 状态。目前，这个问题还没有临时解决方案。(OCPBUGS-20554)

- 在有保证 CPU 且禁用中断请求(IRQ)负载平衡的单节点 OpenShift 上，容器启动时可能会出现大量延迟激增。(OCPBUGS-22901)

- 在部署具有大量 pod 的应用程序时，一些配置了 CPU 限制，部署可能会失败。解决办法是重新部署应用程序。(RHEL-7232)

- 在禁用功能的单节点 OpenShift 中，**openshift-controller-manager-operator** 可能会持续重启。作为临时解决方案，请启用构建功能，或者手动创建 **builds.config.openshift.io** CRD。执行以下步骤手动创建 **builds.config.openshift.io** CRD：

  1. 运行以下命令来提取发行清单：

     ```
     $ oc adm release extract --to manifests
     ```

  2. 在 **manifests** 目录和子目录中搜索 **builds.config.openshift.io** ：

     ```
     $ grep -r builds.config.openshift.io manifests
     ```

     预期输出

     ```
     manifests/0000_10_openshift-controller-manager-operator_01_build.crd.yaml:  name:
     ```

```
builds.config.openshift.io
```

3. 应用 **0000_10_openshift-controller-manager-operator_01_build.crd.yaml** 中指定的配置：

```
$ oc apply -f manifests/0000_10_openshift-controller-manager-
operator_01_build.crd.yaml
```

(OCPBUGS-21778)

- 存在一个已知问题：防止在 Microsoft Azure Stack Hub 上将集群安装到此版本的 OpenShift Container Platform。如需了解更多详细信息和临时解决方案，请参阅红帽知识库文章。(OCPBUGS-20548)

- Microsoft Azure 集群在版本 4.14.2 之前在 OpenShift Container Platform 4.14 版本中使用 Azure AD Workload Identity 存在一个已知问题。最近更改 **eastus** 区域中新 Azure 存储帐户的默认安全设置会阻止安装在该区域中使用 Azure AD Workload Identity 的集群。目前，其他区域不会受到影响，但将来可能会受到影响。
这个问题已在 OpenShift Container Platform 4.14.2 中解决。

  要临时解决这个问题，请在 配置 Azure 集群以使用简短凭证的 步骤中手动创建允许在运行 **ccoctl azure create-all** 前允许公共访问权限的存储帐户。

  执行以下步骤：

  1. 运行以下 Azure CLI 命令，为存储帐户创建资源组：

```
$ az group create --name <oidc_resource_group_name> --location <azure_region>
```

  2. 运行以下 Azure CLI 命令，创建一个允许公共访问的存储帐户：

```
$ az storage account create --name <storage_account_name> --resource-group
<oidc_resource_group_name> --location <azure_region> --sku Standard_LRS --kind
StorageV2 --allow-blob-public-access true
```

  3. 当使用 **ccoctl** 工具通过运行以下命令来处理所有 **CredentialsRequest** 对象时，您必须指定上一步中创建的资源。

```
$ ccoctl azure create-all \
  --name=<azure_infra_name> \
  --output-dir=<ccoctl_output_dir> \
  --region=<azure_region> \
  --subscription-id=<azure_subscription_id> \
  --credentials-requests-dir=<path_to_credentials_requests_directory> \
  --dnszone-resource-group-name=<azure_dns_zone_resource_group_name> \
  --tenant-id=<azure_tenant_id> \
  --storage-account-name=<storage_account_name> \
  --oidc-resource-group-name=<oidc_resource_group-name>
```

  (OCPBUGS-22651)

- 当使用静态 IP 寻址和 Tang 加密安装 OpenShift Container Platform 集群时，节点在没有网络设置的情况下启动。此条件可防止节点访问 Tang 服务器，从而导致安装失败。要解决此条件，您必须将每个节点的网络设置设置为 **ip** 安装程序参数。

1. 对于安装程序置备的基础架构，在安装前通过执行以下步骤为每个节点提供 **ip** 安装程序参数。

   a. 创建清单。

   b. 对于每个节点，使用注解修改 **BareMetalHost** 自定义资源，使其包含网络设置。例如：

```
$ cd ~/clusterconfigs/openshift
$ vim openshift-worker-0.yaml
```

```
apiVersion: metal3.io/v1alpha1
kind: BareMetalHost
metadata:
  annotations:
    bmac.agent-install.openshift.io/installer-args: '["--append-karg", "ip=<static_ip>::
<gateway>:<netmask>:<hostname_1>:<interface>:none", "--save-partindex", "1", "-
n"]' 1 2 3 4 5
    inspect.metal3.io: disabled
    bmac.agent-install.openshift.io/hostname: <fqdn> 6
    bmac.agent-install.openshift.io/role: <role> 7

  generation: 1
  name: openshift-worker-0
  namespace: mynamespace
spec:
  automatedCleaningMode: disabled
  bmc:
    address: idrac-virtualmedia://<bmc_ip>/redfish/v1/Systems/System.Embedded.1
8
    credentialsName: bmc-secret-openshift-worker-0
    disableCertificateVerification: true
  bootMACAddress: 94:6D:AE:AB:EE:E8
  bootMode: "UEFI"
  rootDeviceHints:
    deviceName: /dev/sda
```

对于 **ip** 设置，替换：

1. **<static_ip>**，使用节点的静态 IP 地址，例如 **192.168.1.100**
2. **<gateway>**，使用网络网关的 IP 地址，例如 **192.168.1.1**
3. **<netmask>**，使用网络掩码，例如 **255.255.255.0**
4. **<hostname_1>**，使用节点主机名，如 **node1.example.com**
5. **<interface>**，使用网络接口的名称，如 **eth0**
6. **<fqdn>**，使用节点的完全限定域名
7. **<role>**，使用 **worker** 或 **master**，以反映节点的角色
8. **<bmc_ip>**，使用 BMC IP 地址，以及 BMC 的协议和路径。

c. 将文件保存到 **clusterconfigs/openshift** 目录中。

d. 创建集群。

2. 当使用 Assisted Installer 安装时，在安装前使用 API 修改每个节点的安装程序参数，以将网络设置附加为 **ip** 安装程序参数。例如：

```
$ curl https://api.openshift.com/api/assisted-install/v2/infra-
envs/${infra_env_id}/hosts/${host_id}/installer-args \
-X PATCH \
-H "Authorization: Bearer ${API_TOKEN}" \
-H "Content-Type: application/json" \
-d '
   {
    "args": [
     "--append-karg",
     "ip=<static_ip>::<gateway>:<netmask>:<hostname_1>:<interface>:none", 1 2
3 4 5
     "--save-partindex",
     "1",
     "-n"
    ]
   }
 ' | jq
```

对于以前的网络设置，替换：

1. **<static_ip>**，使用节点的静态 IP 地址，例如 **192.168.1.100**
2. **<gateway>**，使用网络网关的 IP 地址，例如 **192.168.1.1**
3. **<netmask>**，使用网络掩码，例如 **255.255.255.0**
4. **<hostname_1>**，使用节点主机名，如 **node1.example.com**
5. **<interface>**，使用网络接口的名称，如 **eth0**。

联系红帽支持以获取更多详细信息和帮助。

(OCPBUGS-17895)

- 此发行版本中存在一个已知问题，会阻止在 Web Terminal Operator 安装后访问它。这个问题将在以后的 OpenShift Container Platform 发行版本中解决。(OCPBUGS-14463)
- 将 Cluster Network Operator 从版本 4.13 升级到 4.14 时存在一个已知问题。转换为新的 OVN Kubernetes 互连多区架构可能会导致数据包丢弃，从而导致网络中断。这对带有将 **routingViaHost** 设置为 **true** 的本地网关模式中的 East/West 流量有影响。(OCPBUGS-38891)
- OpenShift Container Platform 4.14 中的 HAProxy 存在一个已知问题，涉及发送无效的 **Transfer-Encoding** 标头的应用程序。这个问题会导致在 pod 公开发送这些无效标头的路由时丢失对 pod 的外部访问。如需了解更多详细信息，请参阅红帽知识库文章。(OCPBUGS-43095)

1.9. 异步勘误更新

OpenShift Container Platform 4.14 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 4.14 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 4.14 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.14.z）的具体信息会包括在相应的子章节中。此外，在发行公告中因为空间限制没有包括在其中的勘误内容也会包括在这里的相应的子章节中。

重要

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

1.9.1. RHSA-2025:16165 - OpenShift Container Platform 4.14.57 程序错误修复和安全更新

发布日期：2525 年 9 月 25 日

OpenShift Container Platform release 4.14.57 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:16165 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:16163 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.57 --pullspecs
```

1.9.1.1. 程序错误修复

- 在此次更新之前，因为受影响版本中缺少应用程序编程接口(API)端点证书，集群安装会失败。这会导致证书没有响应的问题和安装问题。在这个版本中，在托管 control plane 集群安装过程中的证书问题已解决，Advanced Cluster Management (ACM)代理不会停滞。(OCPBUGS-61176)

1.9.1.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.2. RHSA-2025:14855 - OpenShift Container Platform 4.14.56 程序错误修复和安全更新

发布日期： 2025 年 9 月 4 日

OpenShift Container Platform release 4.14.56 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:14855 公告中。此更新没有 RPM 软件包。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

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 4.14.56 --pullspecs
```

1.9.2.1. 程序错误修复

- 在此次更新之前，当 **openshift-ptp** pod 在重启过程中停止时，openshift-ptp pod 的 sidecar 会崩溃。因此，时钟类指标不可用。在这个版本中，**openshift-ptp** pod 的 sidecar 不会在重启后停止。因此，时钟类指标可用。(OCPBUGS-59233)

1.9.2.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.3. RHSA-2025:13289 - OpenShift Container Platform 4.14.55 程序错误修复和安全更新

发布日期：25 年 8 月 14 日

OpenShift Container Platform release 4.14.55 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:13289 公告中。此更新没有 RPM 软件包。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

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 4.14.55 --pullspecs
```

1.9.3.1. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.4. RHSA-2025:11669 - OpenShift Container Platform 4.14.54 程序错误修复和安全更新

发布日期：2025 年 7 月 31 日

OpenShift Container Platform 版本 4.14.54 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:11669 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:11670 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.54 --pullspecs
```

1.9.4.1. 程序错误修复

- 在此次更新之前，当端口进入有故障状态时，Precision Time Protocol (PTP) pod 不会屏蔽初始概述指标。因此，新接口会出现一个保持不变的值，显示不正确或过时的数据。
  在这个版本中，PTP pod 可以正确地对指标数据进行掩码和别名处理，确保正确更新接口数据。(OCPBUGS-55309)

1.9.4.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.5. RHSA-2025:9759 - OpenShift Container Platform 4.14.53 程序错误修复和安全更新

发布日期： 2025 年 7 月 2 日

OpenShift Container Platform 版本 4.14.53 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:9759 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:9760 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.53 --pullspecs
```

1.9.5.1. 程序错误修复

- 在以前的版本中，如果用户添加了带有 Subject Alternative Name (SAN) 的自定义证书，其与 **hc.spec.services.servicePublishingStrategy** 参数中定义的 Kubernetes API 服务器(KAS)主机名冲突，则生成新有效负载时不会包含 KAS 证书。这会导致为尝试加入托管 control plane 集群的新节点进行证书验证问题。在这个版本中，会实施一个新的验证来主动识别和警报用户有关冲突的问题，确保不再会发生这个程序错误。(OCPBUGS-57321)

- 在以前的版本中，因为不正确的格式化的代理设置，代理环境变量处理错误会导致外部二进制文件错误，以及构建失败。在这个版本中，在没有配置时，这个问题可以通过从构建过程中排除代理变量来解决。在这个版本中，构建不会因为这些变量而失败。(OCPBUGS-56951)

- 在以前的版本中，使用托管 control plane 和 **Kyverno** 策略引擎部署 OpenShift Container Platform 集群会导致 **Konnectity** 服务无法将 API pod 请求代理到验证 Webhook。这导致在集群中创建额外的组。在这个版本中，**Konnectity** 服务代理问题已解决，用户可以成功创建额外的组。(OCPBUGS-55936)

- 在以前的版本中，在 Time-Grandmaster (T-GM) 导入过程中，如果全局导航 Satellite 系统 (GNSS) 源被重新分配，则系统会在在 DPLL (Digital Phase-Locked Loop) 进入锁定状态之前，错误地宣布 **S2** 的 **T-GM-STATUS**。这个并不成熟的公告破坏了 T-GM 的稳定性，并导致在 GNSS reacquisition 后出现不准确的状态。在这个版本中，DPLL 在声明 **S2** 状态前，会根据 GNSS 源验证 T-GM 状态。这个变化提高了 T-GM 的稳定性，并确保在 GNSS reacquisition 后发送状态公告。(OCPBUGS-55467)

1.9.5.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.6. RHSA-2025:7702 - OpenShift Container Platform 4.14.52 程序错误修复和安全更新

发布日期： 2025 年 5 月 21 日

OpenShift Container Platform 版本 4.14.52 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:7702 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:7704 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.52 --pullspecs
```

1.9.6.1. 程序错误修复

- 在以前的版本中，如果当前项目与其默认命名空间匹配且复制的 CSV 在 Operator Lifecycle Manager (OLM) 中禁用，Operator 会错误地在已安装的 Operator 列表中出现两次。在这个版本中，Operator 只显示一次。(OCPBUGS-55942)
- 在以前的版本中，OpenShift Container Platform 版本 4.14.52 及更新的版本保留在 stable-4.14 频道中，而不是切换到 eus-4.14 频道。这会导致在尝试检索更新信息时 'VersionNotFound' 错误。因为 stable-4.14 频道中没有找到版本，所以推荐的更新不可用。在这个版本中，安装程序会将 4.14.52 及更新版本定向到 Extended Update Support (EUS) 频道，确保版本收到推荐的更新通知，而 **VersonNotFound** 错误将不再显示。(OCPBUGS-55193)
- 在以前的版本中，当用户或升级修改 **openshift-host-network** 命名空间时，网络策略无法正确将 VXLAN 虚拟网络 ID 参数 **VNID** 设置为 **0**。在这个版本中，在修改命名空间后会正确设置 VNID 参数。(OCPBUGS-54868)
- 在以前的版本中，集群节点会因为 Open Virtual Network (OVN)-Kubernetes 不正确的远程端口绑定而重复丢失通信。这会影响跨节点的 pod 通信。在这个版本中，远程端口绑定功能会被 OVN 直接处理，提高了集群节点通信的可靠性。(OCPBUGS-48522)
- 在以前的版本中，当您在 IBM Cloud® 上将集群安装到现有的 Virtual Private Cloud (VPC) 中时，安装程序会检索不支持的 VPC 区域。如果您试图安装到遵循不支持的 VPC 区域（按字母顺序使用）的 VPC 区域，安装程序会崩溃。在这个版本中，安装程序会忽略资源查找过程中没有完全可用的 VPC 区域。(OCPBUGS-48196)

1.9.6.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.7. RHSA-2025:4177 - OpenShift Container Platform 4.14.51 程序错误修复和安全更新

发布日期：2025 年 4 月 30 日

OpenShift Container Platform release 4.14.51 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:4177 公告中。此更新没有 RPM 软件包。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

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 4.14.51 --pullspecs
```

1.9.7.1. 程序错误修复

- 在以前的版本中，更新到 IBM Cloud® Cloud Internet Services (CIS)的实现会影响上游 Terraform 插件。如果您试图在 IBM Cloud® 上创建面向外部的集群，则会出现以下错误：

```
ERROR Error: Plugin did not respond
ERROR
ERROR with module.cis.ibm_cis_dns_record.kubernetes_api_internal[0],
ERROR on cis/main.tf line 27, in resource "ibm_cis_dns_record" "kubernetes_api_internal":
ERROR 27: resource "ibm_cis_dns_record" "kubernetes_api_internal"
```

在这个版本中，您可以使用安装程序在没有插件问题的情况下在 OpenShift Container Platform 上创建外部集群。(OCPBUGS-54264)。

- 在以前的版本中，web 控制台中的 **Observe** 部分不会显示来自插件的项，除非设置了与监控相关的特定标记。这些标记会阻止其他插件，如日志记录、分布式追踪平台、网络可观察性等，在 **Observe** 部分中添加项目。在这个版本中，会删除监控标记，以便其他插件可以在 **Observe** 部分中添加项目。(OCPBUGS-53437)

- 在以前的版本中，在 **condition.Status** 中，Ignition-server 控制器通过在每个协调循环中更新具有相同消息的该条件来超载 Kubernetes 代理服务器(KAS)。在这个版本中，控制器会检查消息并验证它是现有消息，以便 KAS 不会超载。(OCPBUGS-53433)

- 在以前的版本中，自定义安全性上下文约束(SCC)会影响 Cluster Version Operator 从接收集群版本升级生成的 pod。在这个版本中，OpenShift Container Platform 会为每个 pod 设置一个默认 SCC，以便任何创建的自定义 SCC 都不会影响 pod。(OCPBUGS-50592)

- 在以前的版本中，大于集群设置的最大传输单元(MTU)值的用户数据报协议(UDP)数据包无法使用服务发送到数据包的端点。在这个版本中，无论数据包大小是什么，会使用 pod IP 地址而不是服务 IP 地址，以便 UDP 数据包可以发送到端点。(OCPBUGS-50584)

1.9.7.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.8. RHSA-2025:3569 - OpenShift Container Platform 4.14.50 程序错误修复和安全更新

发布日期： 2025 年 4 月 9 日

OpenShift Container Platform release 4.14.50 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:3569 公告中。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.50 --pullspecs
```

1.9.8.1. 程序错误修复

- 在以前的版本中，在 VMware vSphere 上安装集群需要指定 vSphere 数据存储的完整路径。在这个版本中，安装程序会接受到数据存储的完整路径和相对路径。(OCPBUGS-54260)

- 在以前的版本中，如果 **ClusterVersion** 没有收到 **Completed** 更新，**Cluster Settings** 页不会在集群更新过程中正确显示。在这个版本中，即使 **ClusterVersion** 没有收到 **Completed** 更新，**Cluster Setting** 页也会正确显示。(OCPBUGS-54167)

- 在以前的版本中，无法将不正确的地址传递给集群中的 Kubernetes EndpointSlice。这个问题导

致无法在 IPv6 断开连接的环境中的基于 Agent 的集群中安装 MetalLB Operator。在这个版本中，修复修改了地址评估方法。Red Hat Marketplace pod 现在可以成功连接到集群 API 服务器，以便安装 MetalLB Operator 并在 IPv6 断开连接的环境中处理入口流量。(OCPBUGS-53314)

- 在以前的版本中，在 web 控制台的 **Administrator 视角**的 **Home** > **Overview** > **Status** 窗格中，代码迁移操作无法正确处理外部标签。需要这些外部标签，以防止静默的警报通知添加到 **Status** 窗格中。由于 **Status** 窗格无法正确处理外部标签，窗格中提供了指向 **Alert 详情**页的链接，但在点链接时会生成 "no matching alerts found" 信息。在这个版本中，**Status** 窗格接受外部标签，以便点击警报链接到正确的 **Alert** 详情页。(OCPBUGS-51118)

1.9.8.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.9. RHSA-2025:2710 - OpenShift Container Platform 4.14.49 程序错误修复和安全更新

发布日期：2025 年 3 月 19 日

OpenShift Container Platform 版本 4.14.49 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:2710 公告中。此更新中包括的 RPM 软件包由 RHSA-2025:2712 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.49 --pullspecs
```

1.9.9.1. 程序错误修复

- 在以前的版本中，在集群中删除计算节点后，置备 **PersistentVolume** (PV)资源会失败，并显示如下信息：**The object <virtual machine ID> has already been deleted or has not been completely created**。在这个版本中，一个修复可确保在计算节点被删除时，这个删除不会影响 PV 资源的置备。(OCPBUGS-51045)

- 在以前的版本中，当有与请求匹配的准入 Webhook 时，对 **deploymentconfig/scale** 子资源的请求将失败。在这个版本中，这个问题已被解决，对 **deploymentconfig/scale** 子资源的请求可以成功。(OCPBUGS-50477)

- 在以前的版本中，当您使用 **Form View** 在 OpenShift Container Platform Web 控制台中编辑 **Deployment** 或 **DeploymentConfig** API 对象时，在其中一个对象的 YAML 配置中都存在重复的 **ImagePullSecrets** 参数。在这个版本中，确保没有为其中一个对象自动添加重复的 **ImagePullSecrets** 参数。(OCPBUGS-49753)

1.9.9.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.10. RHSA-2025:1451 - OpenShift Container Platform 4.14.48 程序错误修复和安全更新

发布日期：2025 年 2 月 19 日

OpenShift Container Platform 版本 4.14.48 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:1451 公告中。此更新中包括的 RPM 软件包由 RHSA-2025:1453 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.48 --pullspecs
```

1.9.10.1. 程序错误修复

- 在以前的版本中，无效的或无法访问的身份提供程序 (IDP) 会阻止对托管 control plane 的更新。在这个版本中，**HostedCluster** 对象中的 **ValidIDPConfiguration** 条件会报告 IDP 错误，因此这些错误不会阻止对托管 control plane 的更新。(OCPBUGS-49405)

1.9.10.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.11. RHSA-2025:0840 - OpenShift Container Platform 4.14.46 程序错误修复和安全更新

发布日期： 2025 年 2 月 6 日

OpenShift Container Platform 版本 4.14.46 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:0840 公告中。此更新中包括的 RPM 软件包由 RHSA-2025:0842 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.46 --pullspecs
```

1.9.11.1. 程序错误修复

- 在以前的版本中，如果您打开终端会话，crun 会停止容器，然后从它断开连接。在这个版本中，这个问题已解决。(OCPBUGS-48752)
- 在以前的版本中，如果您创建了一个只带有"finally"任务的管道，则无法从**编辑管道**表单中删除 "finally" 管道任务。在这个版本中，您可以从**编辑管道**表单中删除 "finally" 任务，从而解决了这个问题。(OCPBUGS-46603)

1.9.11.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.12. RHSA-2025:0364 - OpenShift Container Platform 4.14.45 程序错误修复和安全更新

发布日期： 2025 年 1 月 22 日

OpenShift Container Platform 版本 4.14.45 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:0364 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:0367 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.45 --pullspecs
```

1.9.12.1. 程序错误修复

- 在以前的版本中，当使用 **SiteConfig** 自定义资源(CR)删除集群或节点时，**BareMetalHost** CR 可能会处于 **Deprovisioning** 状态。这个程序错误已被解决，以确保顺序删除正确。在这个版本中，需要 Red Hat OpenShift GitOps 1.13 或更高版本。(OCPBUGS-48339)
- 在以前的版本中，机器控制器无法保存实例模板克隆操作的 VMware vSphere 任务 ID。这会导致机器进入 **Provisioning** 状态并关闭电源。在这个版本中，VMware vSphere 机器控制器可以检测到这个状态并从这个状态恢复。(OCPBUGS-48245)
- 在以前的版本中，在节点重启过程中，在更新操作过程中，与重新引导机器交互的节点在短时间内进入 **Ready=Unknown** 状态。这会导致 Control Plane Machine Set Operator 进入 **UnavailableReplicas** 条件，然后是 **Available=false** 状态。**Available=false** 状态触发需要紧急操作的警报，但在这种情况下，只在短时间内需要干预，直到节点重启为止。在这个版本中，当节点进入 unready 状态时，会提供一个节点 unreadiness 的宽限期，如果节点进入 unready 状态，则 Control Plane Machine Set Operator 不会立即进入 **UnavailableReplicas** 条件或 **Available=false** 状态。(OCPBUGS-48211)
- 在以前的版本中，用于计算通过特定年龄删除机器删除的机器的优先级的算法，作为优先级等于删除的首选机器。在这个版本中，按年龄排序的未标记机器的优先级会减少，因此它们永远不会与明确标记为删除的机器冲突。该算法也已更新，以确保机器的年龄排序保证到 10 年。(OCPBUGS-47659)
- 在以前的版本中，当将 OpenShift Container Platform 集群从 4.14 升级到 4.15 时，**vCenterCluster** 参数没有使用 **use-connection-form.ts** 配置文件中的值填充。因此，VMware vSphere GUI 没有显示 VMware vSphere vCenter 信息。在这个版本中，对 **Infrastructure** 自定义资源(CR)的更新可确保 GUI 检查 **vCenterCluster** 值的 **cloud-provider-config** 配置映射。(OCPBUGS-45323)

1.9.12.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.13. RHSA-2025:0029 - OpenShift Container Platform 4.14.44 程序错误修复和安全更新

发布日期： 2025 年 1 月 9 日

OpenShift Container Platform release 4.14.44 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2025:0029 公告中。此更新中包括的 RPM 软件包由 RHBA-2025:0032 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.44 --pullspecs
```

1.9.13.1. 程序错误修复

- 在以前的版本中，在 Operator 的关闭操作过程中，Single-Root I/O Virtualization (SR-IOV) Operator 不会使获取租期过期。这会影响 Operator 的新实例，因为新实例可用前，它需要等待租期过期。在这个版本中，对 Operator 关闭逻辑的更新可确保 Operator 关闭时 Operator 过期租期。(OCPBUGS-44726)

- 在以前的版本中，当尝试使用 Operator Lifecycle Manager (OLM)升级 Operator 时，升级会被阻断，并出现 **error validating existing CRs against new CRD's schema** 信息。OLM 存在一个问题，在验证新的 Operator 版本的一个已存在的自定义资源定义（CRD）时会错误地报告存在不兼容问题。在这个版本中，验证过程已进行了修正，Operator 升级不再被阻断。(OCPBUGS-46595)

- 在以前的版本中，**aws-sdk-go-v2** 软件开发工具包(SDK)无法在 Amazon Web Services (AWS)安全令牌服务(STS)集群上验证 **AssumeRoleWithWebIdentity** API 操作。在这个版本中，**pod-identity-webhook** 包含一个默认区域，身份验证问题不再存在。(OCPBUGS-46487)

- 在以前的版本中，当使用基于代理的安装程序在带有不正确的日期的节点上安装集群时，集群安装会失败。在这个版本中，补丁应用到基于代理的安装程序中存在的实时 ISO 时间同步。补丁修复了日期问题，并使用额外的网络时间协议(NTP)服务器列表配置 **/etc/chrony.conf** 文件。现在，您可以在 **agent-config.yaml** 中设置这些额外的 NTP 服务器，而不会遇到集群安装问题。(OCPBUGS-45464)

- 在以前的版本中，当将 resources 字段添加到有效负载时，在 Pipeline 中添加参数时会出现错误，因为资源已弃用。在这个版本中，resources 字段已从有效负载中删除，您可以在 Pipeline 中添加参数而不会出现错误。(OCPBUGS-39368)

1.9.13.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.14. RHSA-2024:11031 - OpenShift Container Platform 4.14.43 程序错误修复和安全更新

发布日期：2024 年 12 月 18 日

OpenShift Container Platform release 4.14.43 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:11031 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:11034 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.43 --pullspecs
```

1.9.14.1. 程序错误修复

- 在以前的版本中，每个 DNS 1123 子域名称标准在 Kubernetes 对象名称中不允许在结尾带有句点。如果您使用包含结尾句点的自定义域名配置了 AWS DHCP 选项，则提取 EC2 实例主机名并将其转换为 Kubelet 节点的逻辑不会删除主机名结尾的句点。在这个版本中，相关逻辑被更新，现在会删除结尾的句点，因子在 DHCP 选项集中的域名中可以在结尾使用句点。(OCPBUGS-46057)

- 在以前的版本中，基于 control plane 的集群无法通过 **oc login** 命令进行身份验证。在选择 **Display Token** 后，当尝试获取令牌时 web 浏览器会显示一个错误。在这个版本中，**cloud.ibm.com** 和其他基于云的端点不再被代理，身份验证可以成功。(OCPBUGS-44279)

1.9.14.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.15. RHSA-2024:10523 - OpenShift Container Platform 4.14.42 程序错误修复和安全更新

发布日期： 2024 年 12 月 5 日

OpenShift Container Platform release 4.14.42 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:10523 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:10526 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.42 --pullspecs
```

1.9.15.1. 程序错误修复

- 在以前的版本中，证书签名请求 (CSR) 的批准机制会失败，因为 CSR 的节点名称和内部 DNS 条目在字符问题单差异方面不匹配。在这个版本中，对 CSR 的批准机制的更新会跳过区分大小写的检查，以便具有匹配节点名称和内部 DNS 条目的 CSR 不会因为字符问题单的不同而失败。(OCPBUGS-44774)

- 在以前的版本中，当 Cluster Version Operator (CVO) pod 在初始化同步工作时重启时，Operator 会中断对阻止的升级请求的保护。阻塞的请求被意外接受。在这个版本中，CVO 重启后对被阻断的升级请求进行保护。(OCPBUGS-44704)

- 在以前的版本中，当 Cluster Resource Override Operator 无法完全部署其操作对象控制器时，Operator 将重启这个过程。每次 Operator 尝试部署过程时，Operator 都会创建一组新的 secret。这会导致在部署了 Cluster Resource Override Operator 的命名空间中创建大量 secret。在这个版本中，固定版本可以正确地处理服务帐户注解，并只创建一组 secret。(OCPBUGS-44435)

1.9.15.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.16. RHSA-2024:9620 - OpenShift Container Platform 4.14.41 程序错误修复和安全更新

发布日期： 2024 年 11 月 20 日

OpenShift Container Platform release 4.14.41 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:9620 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:9623 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.41 --pullspecs
```

1.9.16.1. 程序错误修复

- 在以前的版本中，vSphere **resolv-prepender** 脚本上的 Machine Config Operator (MCO)使用了与 OpenShift Container Platform 4 旧引导镜像版本不兼容的 systemd 指令。在这个版本中，OpenShift Container Platform 节点与旧的引导镜像兼容，包含以下解决方案之一：使用手动干预或升级到带有此修复的发行版本，使用引导镜像 4.13 或更高版本进行扩展。(OCPBUGS-42111)

1.9.16.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.17. RHSA-2024:8697 - OpenShift Container Platform 4.14.40 程序错误修复和安全更新

发布日期： 2024 年 11 月 7 日

OpenShift Container Platform release 4.14.40 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:8697 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:8700 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.40 --pullspecs
```

1.9.17.1. 程序错误修复

- 在以前的版本中，如果集群没有使用手动模式凭证且没有启用 **backupdr** API，在 Google Cloud 上安装的集群 Cloud Credential Operator (CCO)会输入一个 **Degraded=True**。在这个版本中，当使用这个环境配置集群时，集群不会进入 degraded 状态。(OCPBUGS-43821)

- 在以前的版本中，当尝试使用 **oc import-image** 命令在托管的 control plane 集群中导入镜像时，命令会失败，因为访问私有镜像 registry 的问题。在这个版本中，对托管 control plane 集群中的 **openshift-apiserver** pod 的更新可以解析使用 data plane 的名称，以便 **oc import-image** 命令现在可以与私有镜像 registry 正常工作。(OCPBUGS-43468)

- 在以前的版本中，对于托管 control plane，使用镜像发行镜像的集群可能会导致现有节点池使用托管的集群操作系统版本，而不是 **NodePool** 版本。在这个版本中，可以确保节点池使用自己的版本。(OCPBUGS-43368)

- 在以前的版本中，当您使用 **must-gather** 工具时，Multus Container Network Interface (CNI) 日志文件 **multus.log** 存储在节点的文件系统中。这会导致工具在节点上生成不必要的调试 pod。在这个版本中，Multus CNI 不再创建一个 **multus.log** 文件，而是使用 CNI 插件模式检查 **openshift-multus** 命名空间中的 Multus DaemonSet pod 的日志。(OCPBUGS-43058)

- 在以前的版本中，当将镜像 registry 配置为使用位于集群资源组以外的资源组中的 Microsoft Azure 存储帐户时，Image Registry Operator 会降级。这是因为验证错误。在这个版本中，对 Operator 的更新只允许使用存储帐户密钥进行身份验证。不需要验证其他身份验证要求。(OCPBUGS-42935)

1.9.17.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.18. RHSA-2024:8235 - OpenShift Container Platform 4.14.39 程序错误修复和安全更新

发布日期：2024 年 10 月 23 日

OpenShift Container Platform release 4.14.39 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:8235 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:8238 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.39 --pullspecs
```

1.9.18.1. 功能增强

这个 z-stream 发行版本包括以下增强：

1.9.18.1.1. 使用 Insights Operator 从 Prometheus 指标收集数据

- Insights Operator (IO)现在从 Prometheus 的 **haproxy_exporter_server_threshold** 指标收集数据。(OCPBUGS-41918)

1.9.18.2. 程序错误修复

- 在以前的版本中，如果 Windows 节点的端口 9637 上的连接被拒绝，Kubelet Service Monitor 因为 CRI-O 不在 Windows 节点上运行而抛出一个 **target down** 警报。在这个版本中，Windows 节点不包括在 Kubelet Service Monitor 中。(OCPBUGS-42603)
- 在以前的版本中，当 Node Tuning Operator (NTO)使用 **PerformanceProfiles** 规格进行配置时，它会创建一个 **ocp-tuned-one-shot systemd** 服务，该服务在 kubelet 之前运行并阻止 NTO 执行。这导致 Podman 无法获取镜像。在这个版本中，支持 **/etc/mco/proxy.env** 中定义的集群范围代理环境变量。这允许 Podman 将 NTO 镜像拉取到需要使用 http (s)代理进行集群外连接的环境中。(OCPBUGS-42567)
- 在以前的版本中，当 **Pod** 资源中设置了 **spec.securityContext.runAsGroup** 属性时，组 ID 不会添加到容器内的 **/etc/group** 中。在这个版本中，这个问题已解决。(OCPBUGS-41246)
- 在以前的版本中，如果块设备的序列号中存在特殊或无效字符，则检查过程会失败，且无法转义 **lsblk** 命令。在这个版本中，这个问题已解决。(OCPBUGS-39019)
- 在以前的版本中，在安装 Pipelines Operator 后，用户仍然可以在 Pipeline 模板可用前创建部署。在这个版本中，如果所选资源无法使用管道模板，**Import from Git** 页面上的 **Create** 按钮会被禁用。(OCPBUGS-37353)
- 在以前的版本中，节点注册问题会阻止您使用 Redfish Virtual Media 在集群中添加 xFusion 裸机节点。出现这个问题的原因是，硬件与 Redfish 不兼容。在这个版本中，您可以在集群中添加 xFusion 裸机节点。(OCPBUGS-32266)

1.9.18.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.19. RHSA-2024:7184 - OpenShift Container Platform 4.14.38 程序错误修复和安全更新

发布日期：2024 年 10 月 3 日

OpenShift Container Platform release 4.14.38 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:7184 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:7187 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.38 --pullspecs
```

1.9.19.1. 功能增强

这个 z-stream 发行版本包括以下增强：

1.9.19.1.1. 向后移植可配置子网

- 此发行版本包括可用于配置 masquerade 的可配置子网。您还可以使用可配置的子网加入和转换子网，以防止与本地基础架构中使用的 IP 地址重叠。(OCPBUGS-38440)

1.9.19.2. 程序错误修复

- 在以前的版本中，在 Hosted Cluster 镜像配置中指定的 **AdditionalTrustedCA** 字段不会按预期协调到 **openshift-config** 命名空间中，且组件不可用。在这个版本中，这个问题已解决。(OCPBUGS-42184)

- 在以前的版本中，如果 **registryPoll** 字段为 **none**，Operator Lifecycle Manager (OLM) 目录源 pod 不会从节点失败中恢复。在这个版本中，OLM **CatalogSource** registry pod 从集群节点失败中恢复，并解决了这个问题。(OCPBUGS-42150)

- 在以前的版本中，如果您使用代理创建托管集群，使集群从计算节点访问 control plane，则计算节点将不可用。在这个版本中，为节点更新代理设置，以便节点可以使用代理成功与 control plane 通信。(OCPBUGS-42021)

- 在以前的版本中，当 Operator Lifecycle Manager (OLM)评估潜在的升级时，它会将动态客户端列表用于集群中的所有自定义资源(CR)实例。具有大量 CR 的集群可能会遇到 **apiserver** 超时和升级停滞的问题。在这个版本中，这个问题已解决。(OCPBUGS-42017)

- 在以前的版本中，OpenShift Container Platform Web 控制台 **Topology** 视图只能显示最多 100 个节点。如果您试图查看超过 100 个节点，Web 控制台会输出 **Loading is taking longer than expected.** 错误消息。在这个版本中，web 控制台的 **MAX_NODES_LIMIT** 参数设置为 **200**，以便 Web 控制台最多显示 200 个节点。(OCPBUGS-41581)

- 在以前的版本中，当将托管集群配置为使用具有 **http** 或 **https** 端点的身份提供程序(IdP)时，IdP 主机名在通过代理发送时不会解析。在这个版本中，DNS 查找操作会在 IdP 流量通过代理发送前检查 IdP，因此只有带有主机名的 IdP 只能由数据平面解析，并由 Control Plane Operator (CPO) 验证。(OCPBUGS-41374)

- 在以前的版本中，当启动或重启集群中的大量 secret 时，Cloud Credential Operator (CCO)会生成错误。CCO 尝试同时获取 secret。在这个版本中，CCO 以 100 批处理获取 secret，并解决了这个问题。(OCPBUGS-41236)

- 在以前的版本中，节点就绪的宽限期与上游行为不一致。有时，宽限期会导致节点在 **Ready** 和 **Not ready** 状态之间循环。在这个版本中，这个问题已被解决，宽限期不会使节点在两个状态间进行循环。(OCPBUGS-39378)

- 在以前的版本中，**openvswitch** 服务在集群升级后使用旧的集群配置，这会导致 **openvswitch** 服务停止。在这个版本中，**openvswitch** 服务在集群升级后重启，以便服务使用较新的集群配置。(OCPBUGS-39192)

- 在以前的版本中，在托管集群的 control plane 中运行的 Operator 代理是通过在 data plane 中运行的 Konnectity 代理 pod 上的代理设置执行的。因此，无法基于应用程序协议区分是否需要代理。
  对于 OpenShift Container Platform，通过 HTTPS 或 HTTP 协议的 IdP 通信必须经过代理，但 LDAP 通信不能代理。这种类型的代理还忽略依赖于主机名的 **NO_PROXY** 条目，因为此时流量已到达 Konnectity 代理。这意味着只有目标 IP 地址可用。在这个版本中，在托管的集群中，通过 **konnectivity-https-proxy** 和 **konnectivity-socks5-proxy** 在 control plane 中调用代理，以便代理流量从 Konnectivity 代理停止。因此，针对 LDAP 服务器的流量不再会被代理。其他 HTTPS 或 HTTPS 流量被正确代理。指定主机名时，会遵守 **NO_PROXY** 设置。(OCPBUGS-38066)

- 在以前的版本中，Konnectity 代理中发生 IDP 通信的代理。通过时间流量达到 Konnectivity，其协议和主机名不再可用。因此，OAUTH 服务器 pod 无法正确进行代理。它无法区分需要代理 (HTTP 或 HTTPS)和不需要代理的协议 (LDAP)。另外，它不遵循 **HostedCluster.spec.configuration.proxy** spec 中配置的 **no_proxy** 变量。
  在这个版本中，您可以在 OAUTH 服务器的 Konnectity sidecar 上配置代理，以便正确路由流量，并遵循您的 **no_proxy** 设置。因此，当为托管集群配置代理时，OAUTH 服务器可以与身份提供程序正确通信。(OCPBUGS-38060)

1.9.19.3. 已知问题

- 在 AWS 上部署自助管理的私有托管集群会失败，因为 **bootstrap-kubeconfig** 文件使用了不正确的 **api-server** 端口。因此，AWS 实例会被置备，但无法作为节点加入托管集群。(OCPBUGS-42221)

1.9.19.4. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.20. RHSA-2024:6689 - OpenShift Container Platform 4.14.37 程序错误修复和安全更新

发布日期：2024 年 9 月 19 日

OpenShift Container Platform release 4.14.37 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:6689 公告中。此更新没有 RPM 软件包。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

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 4.14.37 --pullspecs
```

1.9.20.1. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.21. RHSA-2024:6406 - OpenShift Container Platform 4.14.36 程序错误修复和安全更新

发布日期：2024 年 9 月 11 日

OpenShift Container Platform release 4.14.36 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:6406 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:6412 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.36 --pullspecs
```

1.9.21.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.21.1.1. 将 CENTOS 8 引用更新为 CENTOS 9

- CENTOS 8 最近结束其生命周期。此发行版本更新了 CENTOS 8 引用 CENTOS 9。(OCPBUGS-39160)

1.9.21.1.2. 收集 Ingress Controller 证书

- Insights Operator 现在收集有关所有 Ingress Controller 证书的信息(NotBefore 和 NotAfter 日期)。它将数据聚合到路径 'aggregated/ingress_controllers_certs.json' 中的一个 JSON 文件中。(OCPBUGS-37673)

1.9.21.2. PTP grandmaster 时钟的自动秒处理

PTP Operator 现在通过使用全局位置系统(GPS)公告自动更新 leap second 文件。

闰秒信息存储在 **openshift-ptp** 命名空间中的名为 **leap-configmap** 的自动生成的 **ConfigMap** 资源中。

如需更多信息，请参阅为 PTP grandmaster 时钟配置动态 leap 秒处理 。

1.9.21.3. 程序错误修复

- 在以前的版本中，如果删除了虚拟机(VM)且网络接口控制器(NIC)仍然存在，Microsoft Azure 虚拟机验证检查会崩溃。在这个版本中，验证检查会在不崩溃的情况下安全地处理问题。(OCPBUGS-39413)

- 在以前的版本中，当 Cluster Monitoring Operator (CMO)为 Prometheus 远程写入端点配置了代理功能时，集群范围的代理的 **spec.noProxy** 字段不会被考虑。在这个版本中，CMO 不再为具有根据 **noProxy** 字段绕过代理的 URL 的任何远程写入端点配置代理功能。(OCPBUGS-39176)

- 在以前的版本中，当运行 **oc logs -f <pod>** 时，日志不会在轮转日志文件后输出任何内容。在这个版本中，kubelet 会在文件轮转并解决这个问题后输出日志文件。(OCPBUGS-38959)

- 在以前的版本中，OpenShift Container Platform Web 控制台无法重启裸机节点。此发行版本解决了这个问题，以便您可以使用 OpenShift Container Platform Web 控制台重启裸机节点。(OCPBUGS-38053)

- 在以前的版本中，当 Cloud Credential Operator (CCO)检查 passthrough 模式权限是否正确时，CCO 有时会收到来自 Google Cloud API 的响应，有关项目的无效权限。这个错误导致 CCO 进入降级状态，并影响集群的安装。在这个版本中，CCO 会专门检查这个错误，以便单独诊断它，而不影响集群安装。(OCPBUGS-37823)

- 在以前的版本中，TuneD 配置集可能会在自定义资源(CR)更新后不必要地重新载入额外的时间。在这个版本中，TuneD 对象已被删除，TuneD 配置集会在 TuneD 配置集 Kubernetes 对象中直接执行。因此，这个问题已被解决。(OCPBUGS-37754)

1.9.21.4. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.22. RHSA-2024:5433 - OpenShift Container Platform 4.14.35 程序错误修复和安全更新

发布日期： 2024 年 8 月 22 日

OpenShift Container Platform release 4.14.35 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:5433 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:5436 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.35 --pullspecs
```

1.9.22.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.22.1.1. 使用机器集配置容量保留

- OpenShift Container Platform release 4.14.35 引入了对 Microsoft Azure 集群上的 Capacity Reservation with Capacity Reservation groups 的支持。如需更多信息，请参阅 *使用计算机器集为 compute 或 control plane 机器集配置容量保留*。(OCPCLOUD-1646)

1.9.22.1.2. 更新至 Kubernetes v1.27.16

- 此发行版本包含从更新到 Kubernetes v1.27.16 的更新。(OCPBUGS-37623)

1.9.22.2. 程序错误修复

- 在以前的版本中，**OVNKubernetesNorthdInactive** 警报不会如预期触发。在这个版本中，这个问题已解决。(OCPBUGS-38073)

- 在以前的版本中，如果机器配置池 (MCP) 的 **maxUnavailable** 值高于不可用节点的数量，这会导致如果 cordoned 节点位于节点列表中的特定位置，则它们会接收到更新。在这个版本中，修正了这个问题，确保 cordoned 节点不会添加到队列中来接收更新。(OCPBUGS-37738)

- 在以前的版本中，在用户从 **HostedCluster** 对象中删除 **ImageContentSources** 字段后，**HostedClusterConfigOperator** 不会删除 **ImageDigestMirrorSet** (IDMS) 对象。这会导致 IDMS 对象保留在 **HostedCluster** 对象中。在这个版本中，**HostedClusterConfigOperator** 会删除 **HostedCluster** 对象中的所有 IDMS 资源，以便不再有这个问题。(OCPBUGS-37175)

- 在以前的版本中，当将节点的默认网关设置为 **vlan** 且多个网络管理器连接具有相同的名称时，节点会失败，因为它无法配置默认的 OVN-Kubernetes 网桥。在这个版本中，**configure-ovs.sh** shell 脚本包含一个 **nmcli connection show uuid** 命令，它会在存在许多具有相同名称的连接时检索正确的网络管理器连接。(OCPBUGS-33590)

1.9.22.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.23. RHSA-2024:4960 - OpenShift Container Platform 4.14.34 程序错误修复和安全更新

发布日期： 2024 年 8 月 7 日

OpenShift Container Platform 版本 4.14.34 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:4960 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:4963 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.34 --pullspecs
```

1.9.23.1. 功能增强

1.9.23.1.1. 在 Ingress Controller API 中添加 connectTimeout tuning 选项

- IngressController API 使用新的 tuning 选项 **ingresscontroller.spec.tuningOptions.connectTimeout** 更新，它定义了路由器在建立与后端服务器的连接时等待的时间。(OCPBUGS-36555)

1.9.23.1.2. 使用 Insights Operator 收集 Prometheus 和 AlertManager 资源

- Insights Operator 现在收集 **openshift-monitoring** 命名空间之外的 **Prometheus** 和 **AlertManager** 资源。(OCPBUGS-36380)

1.9.23.2. 程序错误修复

- 在以前的版本中，AWS HyperShift 集群利用其 VPC 的主要 CIDR 范围在数据平面上生成安全组规则。因此，将 AWS HyperShift 集群安装到具有多个 CIDR 范围的 AWS VPC 中可能会导致生成的安全组规则不足。在这个版本中，安全组规则会根据提供的 Machine CIDR 范围生成，从而解决这个问题。(OCPBUGS-36159)

- 在以前的版本中，当 pod 指定没有匹配节点的节点选择器时，Kubernetes 调度程序会出现以下错误： "Observed a panic: integer divide by zero"。在这个版本中，Kubernetes 调度程序代码库中的问题已解决，当 pod 指定没有匹配节点的节点选择器时，Kubernetes 调度程序不再 panic。(OCPBUGS-36397)

- 在以前的版本中，如果之前安装和配置了相同的 Operator，安装 Operator 有时可能会失败。这是因为缓存问题。在这个版本中，Operator Lifecycle Manager (OLM)被更新来在此场景中正确安装 Operator，并解决了这个问题。(OCPBUGS-36452)

- 在以前的版本中，Ingress Operator 无法成功更新 canary 路由，因为 Operator 没有更新现有路由上的 **spec.host** 或 **spec.subdomain** 的权限。在这个版本中，Operator ServiceAccount 的集群角色中添加了所需的权限，Ingress Operator 可以更新 canary 路由。(OCPBUGS-36467)

- 在以前的版本中，当将 routing-via-host 设置为共享网关模式的 OVN-Kubernetes 设置时，其默认值，OVN-Kubernetes 无法正确处理混合非碎片和从集群入口 IP 层中的碎片数据包的流量流。在这个版本中，OVN-Kubernetes 可以正确地重新集合并处理入口上的外部流量 IP 数据包片段。(OCPBUGS-36554)

- 在以前的版本中，在 Amazon Web Services (AWS)安全令牌服务(STS)中，Cloud Credential Operator (CCO)在 **CredentialsRequest** 中检查 **awsSTSIAMRoleARN** 以创建 secret。当 **awsSTSIAMRoleARN** 不存在时，CCO 会记录错误。在这个版本中，CCO 不再记录错误，并解决了这个问题。(OCPBUGS-36716)

- 在以前的版本中，Open vSwitch (OVS)固定流程设置主线程的 CPU 关联性，但其他 CPU 线程如果已经创建，则不会提取这个关联性。因此，一些 OVS 线程不在正确的 CPU 集上运行，并可能会干扰服务质量(QoS)类为 **Guaranteed** 的 pod 的性能。在这个版本中，OVS 固定过程会更新每个 OVS 线程的关联性，确保所有 OVS 线程都在正确的 CPU 集上运行。(OCPBUGS-37197)

1.9.23.3. 已知问题

- 在安装和配置了 SR-IOV Network Operator 的集群上，带有 SR-IOV VF 的二级接口的 pod 会失败，并显示出错信息： **SRIOV-CNI failed to configure VF "failed to set vf 0 vlan configuration - id 0, qos 0 和 proto 802.1q: invalid argument"**。要解决这个问题，请在升级 OpenShift Container Platform 前升级 SR-IOV Network Operator。这样可确保对这个问题的修复包含在 SR-IOV Network Operator 中。(OCPBUGS-38091)

1.9.23.4. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.24. RHSA-2024:4479 - OpenShift Container Platform 4.14.33 程序错误修复和安全更新

发布日期：2024 年 7 月 17 日

OpenShift Container Platform 版本 4.14.33 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:4479 公告中。此更新中没有 RPM 软件包。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

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 4.14.33 --pullspecs
```

1.9.24.1. 程序错误修复

- 在以前的版本中，使用 OpenShift Container Platform 的 4.1 和 4.2 引导镜像启动的节点在置备过程中会卡住，因为 **machine-config-daemon-firstboot.service** 存在不兼容的 machine-config-daemon 二进制代码。在这个版本中，二进制文件已被更新，这个问题已解决。(OCPBUGS-

36776)

- 在以前的版本中，OpenShift Container Platform 4.14 中引入了对依赖项目标的更改，它会阻止断开连接的 ARO 安装在升级到受影响的版本后扩展新节点。在这个版本中，在升级到 OpenShift Container Platform 4.14 后，断开连接的 ARO 安装可以扩展新节点。(OCPBUGS-36593)

- 在以前的版本中，如果在与当前部署相同的主机上的 OSTree 级别执行新部署，但在不同的 stateroot 中，则 OSTree 会将它们视为相等。这个行为错误地阻止引导装载程序在调用 **set-default** 时更新，因为 OSTree 没有将两个 stateroot 识别为部署的不同因素。在这个版本中，通过修改 OSTree 逻辑来分析 stateroot，OSTree 可以正确地将默认部署设置为具有不同 stateroot 的新部署。(OCPBUGS-36437)

- 在以前的版本中，**HighOverallControlPlaneCPU** 警报根据具有高可用性的多节点集群条件触发警告。因此，在单节点 OpenShift 集群中触发误导警报，因为配置与环境标准不匹配。在这个版本中，重新定义警报逻辑，以使用单节点 OpenShift 的查询和阈值，以及帐户进行工作负载分区设置。因此，单节点 OpenShift 集群中的 CPU 使用率警报准确且与单节点配置相关。(OCPBUGS-31354)

- 在以前的版本中，DNS Operator 不会验证集群是否在至少两个可用区中有带有准备就绪的可用 CPU 的节点，DNS 守护进程集不会对滚动更新使用 surge。因此，所有节点都位于同一可用区的集群会重复为集群 DNS 服务发出 **TopologyAwareHintsDisabled** 事件。在这个版本中，**TopologyAwareHintsDisabled** 事件不会再在其节点没有存在于多个可用区的集群中发出，从而解决了这个问题。(OCPBUGS-5943)

1.9.24.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.25. RHSA-2024:4329 - OpenShift Container Platform 4.14.32 程序错误修复和安全更新

发布日期： 2024 年 7 月 11 日

OpenShift Container Platform r版本 4.14.32 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:4329 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:4332 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.32 --pullspecs
```

1.9.25.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.25.1.1. 管道插件的新自定义资源定义

此发行版本更新了管道插件，以支持自定义资源定义(CRD) **ClusterTriggerBinding**、**TriggerTemplate** 和 **EventListener** 的最新 Pipeline Trigger API 版本。(OCPBUGS-35723)

1.9.25.1.2. 控制器用于清理 etcd

此发行版本引入了一个控制器，用于对 Hypershift 上托管集群的 etcd 进行碎片整理。(OCPBUGS-35723)

1.9.25.2. 程序错误修复

- 在以前的版本中，**alertmanager-trusted-ca-bundle ConfigMap** 没有注入用户定义的 Alertmanager 容器，这会阻止验证 HTTPS web 服务器接收警报通知。在这个版本中，可信 CA 捆绑包 **ConfigMap** 被挂载到 **/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem** 路径的 Alertmanager 容器中。(OCPBUGS-36416)

- 在以前的版本中，对于从旧版本 OpenShift Container Platform 更新的集群，在启用了 OVN 的集群上启用 **kdump** 有时会阻止节点重新加入集群或返回到 **Ready** 状态。在这个版本中，从旧的 OpenShift Container Platform 版本中删除了有问题的过时的数据，并确保始终清理这种类型的过时的数据。该节点现在可以正确启动并重新加入集群。(OCPBUGS-36356)

- 在以前的版本中，**growpart** 中的一个 bug 会导致设备锁定，这会阻止 LUKS 加密设备打开。系统将无法成功引导。在这个版本中，**growpart** 已从进程中删除，系统将成功引导。(OCPBUGS-35989)

- 在以前的版本中，如果用户置备的基础架构是从旧版本更新的，在 Infrastructure 对象中可能会缺少 **failureDomains**，这会导致某些检查失败。在这个版本中，如果 **infrastructures.config.openshift.io** 中没有提供 **failureDomains** fallback，则从 **cloudConfig** 合并。(OCPBUGS-35913)

- 在以前的版本中，当在 VMware vSphere 上安装集群时，如果 ESXi 主机处于维护模式，则安装会失败，因为安装程序无法从主机检索版本信息。在这个版本中，安装程序不会尝试从处于维护模式的 ESXi 主机检索版本信息，从而允许安装继续进行。(OCPBUGS-35827)

- 在以前的版本中，systemd 中的一个 bug 可能会导致 **coreos-multipath-trigger.service** 单元永久挂起。系统将无法完成引导。在这个版本中，systemd 被删除，引导可以成功。(OCPBUGS-35750)

- 在以前的版本中，registry 覆盖由管理端的集群管理员配置，应用到非相关的 data-plane 组件。在这个版本中，registry 覆盖不再应用到这些组件。(OCPBUGS-35549)。

- 在以前的版本中，OpenShift Cluster Manager 容器没有正确的 TLS 证书。因此，镜像流无法用于断开连接的部署。在这个版本中，TLS 证书作为投射卷添加。(OCPBUGS-35482)

- 在以前的版本中，在断开连接的环境中，HyperShift Operator 会忽略 registry 覆盖。因此，对节点池的更改会被忽略，节点池会遇到错误。在这个版本中，元数据检查器在 HyperShift Operator 协调过程中可以正常工作，并正确填充覆盖镜像。(OCPBUGS-35401)

- 在以前的版本中，因为 Hypershift CLI 存在问题，Hypershift 上的 secrets-store CSI 驱动程序无法挂载 secret。在这个版本中，驱动程序可以挂载卷，并解决了这个问题。(OCPBUGS-35183)

- 在以前的版本中，减少网络队列无法满足 **!ens0** 等规则的预期工作。这是因为在生成的调优配置集中重复了感叹号。在这个版本中，重复不再发生，因此会按预期应用规则。(OCPBUGS-35012)

- 在以前的版本中，一个竞争条件意味着 Kubelet 可能会报告与卷调整大小相关的错误。在这个版本中，竞争条件已被修复，不再会输出 false 错误。(OCPBUGS-33964)

- 在以前的版本中，在编辑 vSphere 连接时，转义的字符串不会被正确处理，从而导致 vSphere 配置被破坏。在这个版本中，转义字符串可以正常工作，vSphere 配置不再会破坏。(OCPBUGS-33942)

- 在以前的版本中，当将节点的默认网关设置为 **vlan** 且多个网络管理器连接具有相同的名称时，节点会失败，因为它无法配置默认的 OVN-Kubernetes 网桥。在这个版本中，**configure-ovs.sh** shell 脚本包含一个 **nmcli connection show uuid** 命令，它会在存在许多具有相同名称的连接时检索正确的网络管理器连接。(OCPBUGS-33590)

- 在以前的版本中，当在节点上手动重启 **kubelet** 服务时，一些状态文件会在假设的节点重启后被删除，这会导致 kubelet 重置 CPU Manager 状态。在状态重置后，CPU Manager 将新的 CPU 分配计算到运行工作负载。因此，新的和初始 **cpuset** 配置可能有所不同。在这个版本中，kubelet 重启后会正确恢复 **cpuset** 配置。(OCPBUGS-32472)

1.9.25.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.26. RHSA-2024:4010 - OpenShift Container Platform 4.14.31 程序错误修复和安全更新

发布日期：2024 年 6 月 26 日

OpenShift Container Platform r版本 4.14.31 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:4010 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:4013 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.31 --pullspecs
```

1.9.26.1. 程序错误修复

- 在以前的版本中，从主机获取节点名称的逻辑不会考虑多个值，并在为包含空格的名称返回多个值时意外终止。在这个版本中，逻辑被更新为只使用第一个返回的主机名作为节点名称，并解决了这个问题。(OCPBUGS-34716)

1.9.26.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.27. RHSA-2024:3881 - OpenShift Container Platform 4.14.30 程序错误修复和安全更新

发布日期：2024 年 6 月 19 日

OpenShift Container Platform 版本 4.14.30 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:3881 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:3918 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.30 --pullspecs
```

1.9.27.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.27.1.1. 在 pull secret 密码中可以使用冒号字符

此发行版本添加了在 OpenShift Container Platform Assisted Installer 的 pull secret 密码中包含冒号字符的功能。(OCPBUGS-35034)

1.9.27.1.2. 为 Cinder CSI 驱动程序配置拓扑功能

在以前的版本中，Cinder CSI Driver 的拓扑功能始终活跃，因为您无法禁用拓扑功能。在这个版本中，拓扑功能基于计算和存储可用区，您可以禁用拓扑功能。(OCPBUGS-34792)

1.9.27.2. 程序错误修复

- 在以前的版本中，OpenShift Container Platform Assisted Installer 会报告已安装的 SATA SDD 作为可移动，且不使用其中任何一个作为安装目标。在这个版本中，可移动磁盘可以进行安装，并解决了这个问题。(OCPBUGS-35085)
- 在以前的版本中，Amazon Web Services (AWS)策略问题会阻止 Cluster API Provider AWS 检索所需的域信息。因此，使用自定义域安装 AWS 托管的集群会失败。在这个版本中，策略问题已解决。(OCPBUGS-34856)
- 在以前的版本中，当您删除集群或 BareMetal Host (BMH)时，会在集群删除过程中创建一个 **PreprovImage** 镜像。因此，集群资源会卡住。在这个版本中，在删除阶段前为电源创建一个例外，并解决了这个问题。(OCPBUGS-34814)。
- 在以前的版本中，当您在 Image Registry Operator 配置中启用了带有 **regionEndpoint** 的 **virtualHostedStyle** 参数时，镜像 registry 会忽略 **virtualHostedStyle**，且无法启动。此发行版本丢弃了 **virtualHostedStyle** 的使用，并使用 **ForcePathStyle** 替代解决了这个问题。(OCPBUGS-34668)
- 在以前的版本中，当从 4.15.8 升级到 OpenShift Container Platform 4.15.11 时，**metal3-ironic** 和 **metal3-ironic-inspector** pod 可能会因为与 FIPS 模式启用相关的安装失败。在这个版本中，这个问题已被解决。(OCPBUGS-34657)。
- 在以前的版本中，OVN-Kubernetes 网络插件无法向对等点发送 gratuitous Address resolution Protocol (ARP) 请求，以告知它们新节点的中访问控制 (MAC) 地址，因为在某些情况下会导致将 Egress IP 地址从一个节点传输到另一个节点失败。这会导致故障转移问题。在这个版本中，OVN-Kubernetes 网络插件可以正确地告知对等新节点的介质访问控制 (MAC) 地址，而不会造成故障转移问题。(OCPBUGS-34570)
- 在以前的版本中，如果您在 bootstrap 过程中使用了 **wait-for-ceo** 命令，则命令不会在失败时报告错误消息。在这个版本中，命令会在 **bootkube** 脚本中报告错误消息，供您查看。(OCPBUGS-34495)
- 在以前的版本中，安装程序不支持 **ca-west-1** Amazon Web Services (AWS)区域。在这个版本中，支持 **ca-west-1** 区域，这个问题已解决。(OCPBUGS-34024)

1.9.27.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.28. RHBA-2024:3697 - OpenShift Container Platform 4.14.29 程序错误修复和安全更新

发布日期：2024 年 6 月 13 日

OpenShift Container Platform 版本 4.14.29 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-2024:3697 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:3700 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.29 --pullspecs
```

1.9.28.1. 程序错误修复

- 在以前的版本中，对于 Red Hat OpenStack Platform (RHOSP)上的 OpenShift Container Platform 部署，**MachineSet** 对象无法正确应用 **Port Security** 参数的值。这意味着 RHOSP 服务器端口中的 **port_security_enabled** 参数具有意外值。在这个版本中，**MachineSet** 对象会如预期应用 **port_security_enabled** 标志。(OCPBUGS-32428)

- 在以前的版本中，当 **IngressController** 对象配置了客户端 SSL/TLS 时，但没有 **clientca-configmap** 终结器，Ingress Operator 会尝试在不检查 **IngressController** 对象标记为删除的情况下添加终结器。因此，如果 **IngressController** 配置了客户端 SSL/TLS，然后被删除，Operator 会正确删除终结器。然后，Operator 会重复并错误，尝试更新 **IngressController** 对象，以将终结器重新添加，从而导致 Operator 日志中出现错误消息。在这个版本中，Ingress Operator 不再将 **clientca-configmap** finalizer 添加到标记为删除的 **IngressController** 对象中。因此，Ingress Operator 不再尝试执行错误更新，不再记录相关的错误。(OCPBUGS-34410)

1.9.28.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.29. RHSA-2024:3523 - OpenShift Container Platform 4.14.28 程序错误修复更新和安全更新

发布日期： 2024 年 6 月 10 日

OpenShift Container Platform 版本 4.14.28 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:3523 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:3526 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.28 --pullspecs
```

1.9.29.1. 程序错误修复

- 在以前的版本中，HyperShift Operator 没有使用 **RegistryOverrides** 机制来检查内部 registry 中的镜像。在这个版本中，元数据检查器在 HyperShift Operator 协调过程中可以正常工作，并正确填充 **OverrideImages**。(OCPBUGS-33844)

- 在以前的版本中，托管 Control Planes (HCP) 的 recycler pod 没有在断开连接的环境中启动。在这个版本中，HCP recycler-pod 镜像指向 OpenShift Container Platform 有效负载引用，这个问题已解决。(OCPBUGS-33843)

- 在以前的版本中，**imageRegistryOverrides** 的信息仅在 HyperShift Operator 初始化上提取一次，且不会刷新。在这个版本中，HyperShift Operator 从管理集群检索新的 **ImageContentSourcePolicy** 文件，并将它们添加到每个协调循环中的 HyperShift Operator 和 Control Plane Operator 中。(OCPBUGS-33713)

- 在以前的版本中，如果 chart 名称不同，Helm 插件索引视图不会显示与 Helm CLI 相同的 chart 数量。在这个版本中，Helm 目录会查找 **chart.openshift.io/name** 和 **charts.openshift.io/provider**，以便所有版本都分组到单个目录标题中。(OCPBUGS-33321)

1.9.29.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.30. RHSA-2024:3331 - OpenShift Container Platform 4.14.27 程序错误修复更新和安全更新

发布日期：2024 年 5 月 30 日

OpenShift Container Platform 版本 4.14.27 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:3331 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:3335 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.27 --pullspecs
```

1.9.30.1. 程序错误修复

- 在以前的版本中，如果您配置了有大量内部服务或用户管理的负载均衡器 IP 地址的 OpenShift Container Platform 集群，则会出现 OVN-Kubernetes 服务的延迟启动时间。当 OVN-Kubernetes 服务试图在节点上安装 **iptables** 规则时，会发生此延迟。在这个版本中，OVN-Kubernetes 服务可在几秒钟内处理大量服务。另外，您可以访问新日志来查看在节点上安装 **iptables** 规则的状态。(OCPBUGS-33537)

- 在以前的版本中，OpenShift Container Platform web 控制台中的 **Topology** 视图不会显示虚拟机(VM)节点和其他非VM 组件之间的视觉连接器。在这个版本中，视觉连接器会显示组件的交互活动。(OCPBUGS-33640)

- 在以前的版本中，OpenShift Container Platform Web 控制台的 masthead 元素中的徽标可能会超过 60 像素。这会导致 masthead 在高度增加。在这个版本中，masthead 徽标有一个 **max-height** 为 60 pixels 的限制。(OCPBUGS-33635)

1.9.30.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.31. RHSA-2024:2869 - OpenShift Container Platform 4.14.26 程序错误修复更新和安全更新

发布日期：2024 年 5 月 23 日

OpenShift Container Platform 版本 4.14.26 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:2869 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:2873 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.26 --pullspecs
```

1.9.31.1. 功能增强

这个 z-stream 发行版本包括以下增强：

1.9.31.1.1. OperatorHub 过滤器从 FIPS 模式重命名为 Designed for FIPS

- 在以前的版本中，OperatorHub 包括一个名为 **FIPS Mode** 的过滤器。在这个版本中，该过滤器被命名为 **Designed for FIPS**。(OCPBUGS-33110)

1.9.31.2. 程序错误修复

- 在以前的版本中，当 **ContainerRuntimeConfig** 资源作为单节点 OpenShift Container Platform 安装的额外清单创建时，bootstrap 会失败并显示以下错误消息："more than one ContainerRuntimeConfig found that match MCP labels"。在这个版本中，修正了对 **ContainerRuntimeConfig** 资源的不正确的处理，这个问题已解决。(OCPBUGS-30153)

- 在以前的版本中，**NodePort** 流量转发存在一个问题，会导致 TCP 流量被定向到处于终止状态的 pod。在这个版本中，端点选择逻辑会完全实现 **KEP-1669 ProxyTerminatingEndpoints**，这个问题已被解决。(OCPBUGS-32319)

- 在以前的版本中，对于 Red Hat OpenStack Platform (RHOSP)上的 OpenShift Container Platform 部署，**MachineSet** 对象无法正确应用 **Port Security** 参数的值。在这个版本中，**MachineSet** 对象会如预期应用 **port_security_enabled** 标志。(OCPBUGS-32428)

- 在以前的版本中，因为驱动程序中存在一个问题，无法配置 Workload Identity 集群上的 Azure File 中的静态持久性卷。在这个版本中，这个问题已被解决，静态持久性卷可以正确挂载。(OCPBUGS-33039)

- 在以前的版本中，负载平衡算法中存在一个缺陷，导致内存用量增加，并存在过量内存消耗的风险。在这个版本中，负载均衡的服务过滤逻辑被更新，这个问题已解决。(OCPBUGS-33389)

- 在以前的版本中，当尝试擦除磁盘时 Ironic Python Agent (IPA) 会失败，因为它预期一个错误的字节扇区大小，这会导致节点置备失败。在这个版本中，IPA 检查磁盘扇区大小，节点置备会成功。(OCPBUGS-33452)

- 在以前的版本中，在使用表单视图编辑路由时尝试删除一个备用服务时，无法从 Route 中删除备用服务。在这个版本中，备用服务可以被删除，这个问题已解决。(OCPBUGS-33462)

- 在以前的版本中，**vsphere-problem-detector** Operator 无法连接到 vCenter，因为 Operator 没有配置 HTTP (S) 代理。在这个版本中，**vsphere-problem-detector** operator 使用与集群的其余部分相同的 HTTP (S) 代理，这个问题已解决。(OCPBUGS-33467)

1.9.31.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.32. RHBA-2024:2789 - OpenShift Container Platform 4.14.25 程序错误修复更新

发布日期： 2024 年 5 月 16 日

OpenShift Container Platform 版本 4.14.25 现已正式发布。其程序错误修正列表包括在 RHBA-2024:2789 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:2792 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.25 --pullspecs
```

1.9.32.1. 程序错误修复

- 在以前的版本中，即使 CRI-O 停止容器，使用 **exec** 命令创建的一些容器进程也会保留。因此，闲置进程会导致跟踪问题，从而导致进程泄漏和失效状态。在这个版本中，CRI-O 跟踪为容器处理的 **exec** 调用，并确保在容器停止时作为 **exec** 调用一部分创建的进程被终止。(OCPBUGS-32482)

- 在以前的版本中，大于 Go 编程语言可以解析的超时值无法被正确验证。因此，大于 HAProxy 可解析的超时值会导致 HAProxy 出现问题。在这个版本中，如果指定的超时值大于可以解析的值，则它会被限制为 HAProxy 可以解析的最大值。因此，HAProxy 不再会存在问题。(OCPBUGS-30773)

- 在以前的版本中，当用户导入镜像流标签时，**ImageContentSourcePolicy** (ICSP) 不能与 **ImageDigestMirrorSet** (IDMS) 和 **ImageTagMirrorSet** (ITMS) 共存。OpenShift Container Platform 忽略用户创建的 IDMS/ITMS，并优先使用 ICSP。在这个版本中，镜像流标签可以共存，因为当 ICSP 存在时导入镜像流标签现在遵循 IDMS/ITMS。(OCPBUGS-31509)

- 在以前的版本中，在涉及暂停和取消暂停机器配置池的 OpenShift Container Platform 集群上执行 Control Plane Only 更新后，在取消暂停操作后会进行两个重启操作。这个额外的重启没有被预期，由性能配置集控制器针对 **MachineConfigPool** 对象中列出的旧的 **MachineConfig** 对象进行协调。在这个版本中，性能配置集控制器针对 **MachineConfigPool** 对象中列出的最新的 **MachineConfig** 对象进行协调，以便不会发生额外的重启。(OCPBUGS-32980)

- 在以前的版本中，在 OpenShift Container Platform 4.14.14 中引入的内核回归问题会导致在挂载到 CephFS 存储的节点中崩溃和重新引导内核问题。在这个发行版本中，回归问题已被修复，内核回归问题不再发生。(OCPBUGS-33251)

- 在以前的版本中，**ovs-if-br-ex.nmconnection.*** 文件会导致 **ovs-configuration.service** 失败，这会导致节点被移到 **NotReady** 状态。在这个版本中，**ovs-if-br-ex.nmconnection.*** 文件已从 **/etc/NetworkManager/system-connections** 中删除，因此这个问题不再存在。(OCPBUGS-32341)

1.9.32.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.33. RHSA-2024:2668 - OpenShift Container Platform 4.14.24 程序错误修复更新和安全更新

发布日期： 2024 年 5 月 9 日

OpenShift Container Platform 版本 4.14.24 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:2668 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:2672 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.24 --pullspecs
```

1.9.33.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.33.1.1. IPv6 unsolicited neighbor 公告现在默认在 macvlan CNI 插件中

- 使用 macvlan CNI 插件创建的 Pod，其中 IP 地址管理 CNI 插件已分配 IP 地址，现在默认将 IPv6 unsolicited 邻居公告发送到网络。这会通知主机具有特定 IP 地址的新 pod 的 MAC 地址，以刷新 IPv6 邻居缓存。(OCPBUGS-33066)

1.9.33.2. 程序错误修复

- 在以前的版本中，如果集群使用代理安装，且代理信息包含转义的字符（格式为 **%XX** ），安装会失败。在这个发行版本中，这个问题已被解决。(OCPBUGS-33010)
- 在以前的版本中，在 OpenShift Container Platform 托管的 control plane 中，当您在断开连接的环境中为 **ImageDigestMirrorSet** 和 **ImageContentSourcePolicy** 对象创建自定义资源定义 (CRD) 时，Hy HyperShift Operator 只为 **ImageDigestMirrorSet** CRD 创建对象，忽略 **ImageContentSourcePolicy** CRD。在这个版本中，HyperShift Operator 为 **ImageDigestMirrorSet** 和 **ImageContentSourcePolicy** CRD 创建对象。(OCPBUGS-32471)
- 在以前的版本中，在执行集群更新时，暂停的 MachineConfigPools 节点可能会被错误地取消暂停。在这个版本中，暂停的 MachineConfigPools 节点会在执行集群更新时正确暂停。(OCPBUGS-32168)
- 在以前的版本中，镜像 registry 不支持 Amazon Web Services (AWS) 区域 **ca-west-1**。在这个版本中，镜像 registry 可以部署到此区域中。(OCPBUGS-31857)
- 在以前的版本中，Terraform 会使用为 control plane 设置的策略创建计算服务器组。因此，compute 服务器组会忽略 **install-config.yaml** 文件的 **serverGroupPolicy** 属性。在这个版本中，compute MachinePool 的 **install-config.yaml** 文件中的服务器组策略会在 Terraform 流中的安装时正确应用。(OCPBUGS-31756)

1.9.33.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.34. RHBA-2024:2051 - OpenShift Container Platform 4.14.23 程序错误修复更新和安全更新

发布日期： 2024 年 5 月 2 日

OpenShift Container Platform 版本 4.14.23 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-2024:2051 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:2054 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.23 --pullspecs
```

1.9.34.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.34.1.1. 额外跃点的出口 IP 验证步骤

- 在以前的版本中，如果出口 IP 由主接口以外的任何接口托管，则没有验证来确定是否需要下一个跃点。在这个版本中，IP 将检查主路由表，并确定是否需要下一个跃点。(OCPBUGS-31854)

1.9.34.1.2. RT 内核的新配置集丢弃不支持的参数

- 在以前的版本中，**net.core.busy_read**、**net.core.busy_poll** 和 **kernel.numa_balancing sysctl** 参数在 RT 内核中不存在，因此不受支持。在这个版本中，添加了 **openshift-node-performance-rt** 配置集，如果检测到 RT 内核，这会在应用前丢弃不支持的内核参数。(OCPBUGS-31905)

1.9.34.1.3. OLM 默认源的禁用选项

- 在以前的版本中，在断开连接的环境中禁用 Operator Lifecycle Manager (OLM) 默认源。在这个版本中，**OperatorHubSpec** 字段集成到 **hostedcluster.Spec.Configuration** API 中，以便于创建过程中禁用并启用默认源。CLI 还包括用于此功能的标志。(OCPBUGS-32221)

1.9.34.2. 程序错误修复

- 在以前的版本中，无论其关联的节点是什么，Node Tuning Operator (NTO) 会检查是否有共享相同优先级的配置集。该进程用于将 NTO 用于首先收集配置集，检查优先级冲突，然后过滤相关节点。因此，如果两个不同的节点上存在多个性能配置集，则会将错误优先级警告转储到日志中。在这个版本中，这个过程的步骤已被修改，以便 NTO 会首先过滤关联的节点，然后检查优先级冲突。(OCPBUGS-31735)

- 在以前的版本中，存在一个根本问题，阻止出口 IPv6 使用多网络接口控制器 (NIC) 处理弹性 IP (EIP)。在这个版本中，这个问题已被解决。(OCPBUGS-31853)

- 在以前的版本中，当关闭闲置连接被错误地重复使用时，某些 HTTP 客户端会在升级到 OpenShift Container Platform 4.14 后导致 Ingress 流量降级。在这个版本中，这个问题已被解决。(OCPBUGS-32437)

- 在以前的版本中，镜像 registry 的 Azure 路径修复作业会错误地需要存在客户端和租户 ID 才能正常工作，这会导致有效的配置生成验证错误。在这个版本中，添加了一个与缺失的客户端和租户 ID 的 key-in 连接的检查。(OCPBUGS-32450)

1.9.34.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.35. RHSA-2024:1891 - OpenShift Container Platform 4.14.22 程序错误修复更新和安全更新

发布日期： 2024 年 4 月 25 日

OpenShift Container Platform 版本 4.14.22 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1891 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:1897 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.22 --pullspecs
```

1.9.35.1. 功能增强

1.9.35.1.1. 验证配置的 control plane 副本数

- 在以前的版本中，您可以将 control plane 副本的数量设置为无效的值，如 **2**。在这个版本中，添加了一个验证，以防止在 ISO 生成时间配置 control plane 副本。(OCPBUGS-31885)

1.9.35.2. 程序错误修复

- 在以前的版本中，**network-tools** 镜像是一个调试工具，其中包含 Wireshark 网络协议分析器。wireshark 依赖于 **gstreamer1** 软件包，此软件包具有特定的许可要求。在这个版本中，**gstreamer1** 软件包已从 **network-tools** 镜像中删除，镜像现在包含 **wireshark-cli** 软件包。(OCPBUGS-31862)

- 在以前的版本中，当集群关闭或休眠时，外部邻居可能会更改其 Media Access Control (MAC) 地址。虽然 Gratuitous 地址解析协议 (GARP) 应该告知其他与这个更改相关的邻居，但集群不会处理 GARP。重启集群后，邻居可能不再从 OVN-Kubernetes 集群网络提供，因为使用了过时的 MAC 地址。在这个版本中，更新启用了老化的机制，以便每 300 秒定期更新邻居的 MAC 地址。(OCPBUGS-11710)

1.9.35.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.36. RHSA-2024:1765 - OpenShift Container Platform 4.14.21 程序错误修复更新和安全更新

发布日期：2024 年 4 月 18 日

OpenShift Container Platform 版本 4.14.21 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1765 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:1768 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.21 --pullspecs
```

1.9.36.1. 程序错误修复

- 在以前的版本中，控制台后端代理服务器会将操作对象列表请求发送到公共 API 服务器端点。这在某些情况下会导致证书颁发机构 (CA) 问题。在这个版本中，代理配置已被更新，以指向解决了这个问题的内部 API 服务器端点。(OCPBUGS-29783)

1.9.36.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.37. RHSA-2024:1681 - OpenShift Container Platform 4.14.20 程序错误修复更新和安全更新

发布日期： 2024 年 4 月 8 日

OpenShift Container Platform 版本 4.14.20 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1681 公告中。此更新没有 RPM 软件包。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.20 --pullspecs
```

1.9.37.1. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.38. RHBA-2024:1564 - OpenShift Container Platform 4.14.19 程序错误修复更新和安全更新

发布日期：2024 年 4 月 3 日

OpenShift Container Platform release 4.14.19 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-2024:1564 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:1567 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.19 --pullspecs
```

1.9.38.1. 程序错误修复

- 在以前的版本中，当由 Admin Policy Based (APP) 控制器处理时，没有 IP 状态的 pod 无法触发新的协调循环，这会导致将其配置添加到北向 DB 中丢失。在这个版本中，每次事件更改时，控制器将继续由控制器处理没有 IP 的 pod，直到其 IP 字段被填充，控制器可以完成协调循环。(OCPBUGS-29342)

1.9.38.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.39. RHSA-2024:1458 - OpenShift Container Platform 4.14.18 程序错误修复更新和安全更新

发布日期： 2024 年 3 月 27 日

OpenShift Container Platform release 4.14.18 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:1458 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:1461 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.18 --pullspecs
```

1.9.39.1. 程序错误修复

- 在以前的版本中，在某些情况下，安装程序会失败，并显示出错信息：**unexpected end of JSON input**。在这个版本中，错误消息已被明确，推荐用户在 **install-config.yaml** 配置文件中设置 **serviceAccount** 字段来修复问题。(OCPBUGS-30027)

1.9.39.2. 已知问题

- 目前，不支持在安装 OpenShift Container Platform 集群时提供性能配置集作为额外清单。(OCPBUGS-18640)

1.9.39.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.40. RHBA-2024:1260 - OpenShift Container Platform 4.14.17 程序错误修复更新

发布日期： 2024 年 3 月 20 日

OpenShift Container Platform 版本 4.14.17 现已正式发布。其程序错误修正列表包括在 RHBA-2024:1260 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:1263 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.17 --pullspecs
```

1.9.40.1. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.41. RHBA-2024:1205 - OpenShift Container Platform 4.14.16 程序错误修复更新

发布日期：2024 年 3 月 13 日

OpenShift Container Platform 版本 4.14.16 现已正式发布。其程序错误修正列表包括在 RHBA-2024:1205 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:1208 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.16 --pullspecs
```

1.9.41.1. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.42. RHBA-2024:1046 - OpenShift Container Platform 4.14.15 程序错误修复更新

发布日期：2024 年 3 月 4 日

OpenShift Container Platform release 4.14.15 现已正式发布。其程序错误修正列表包括在 RHBA-2024:1046 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:1049 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.15 --pullspecs
```

1.9.42.1. 程序错误修复

- 在以前的版本中，**manila-csi-driver-controller-metrics** 服务具有空端点，因为应用程序选择器的名称不正确。在这个版本中，应用程序选择器名称被改为 **openstack-manila-csi**，这个问题已被修复。(OCPBUGS-23443)
- 在以前的版本中，用于提供镜像凭证的 Amazon Web Services (AWS) 代码被从 OpenShift Container Platform 4.14 中的 kubelet 中删除。因此，在没有指定 pull secret 的情况下从 Amazon Elastic Container Registry (ECR) 拉取镜像会失败，因为 kubelet 无法验证自己并将凭证传递给容器运行时。在这个版本中，配置了一个单独的凭证供应商，它负责为 kubelet 提供 ECR 凭证。现在，kubelet 可以从 ECR 拉取私有镜像。(OCPBUGS-29630)
- 在以前的版本中，OpenShift Container Platform 4.14 发行版本引入了一个更改，让用户在从 OpenShift Container Platform 版本 4.13 更新至 4.14 时会丢失镜像。对默认内部 registry 的更改会导致 registry 在使用 Microsoft Azure 对象存储时使用不正确的路径。在这个版本中，使用正确的路径，并将作业添加到 registry operator 中，该 operator 会将任何 Blob 推送到使用错误的存储路径的 registry 中，这会有效地将两个不同的存储路径合并到一个路径中。(OCPBUGS-29604)

注意

在这个版本中，Azure Stack Hub 上无法正常工作。对于在升级到 4.14.14 及更新的版本时使用 OpenShift Container Platform 版本 4.14.0 到 4.14.13 的 Azure Stack Hub 用户，需要完成手动步骤来将其对象 Blob 移到正确的存储路径。请参阅红帽知识库文章。

- 在以前的版本中，在 Microsoft Azure 区域上运行的机器集，没有可用区支持总是为 Spot 实例创建 **AvailabilitySets** 对象。此操作会导致 Spot 实例失败，因为实例不支持可用性集。现在，机器集不会为在非配置的区域中运行的 Spot 实例创建 **AvailabilitySets** 对象。(OCPBUGS-29152)

1.9.42.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.43. RHSA-2024:0941 - OpenShift Container Platform 4.14.14 程序错误修复和安全更新

发布日期： 2024 年 2 月 28 日

OpenShift Container Platform release 4.14.14 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:0941 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:0944 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.14 --pullspecs
```

1.9.43.1. 功能增强

这个 z-stream 发行版本包括以下改进：

1.9.43.1.1. 为 IPI 添加"队列"区域支持

- 在以前的版本中，安装程序无法为"eu-es"区域在 IBM Cloud VPC 上安装集群，但它被支持。在这个版本中，安装程序会为"eu-es"区域在 IBM Cloud VPC 上成功安装集群。(OCPBUGS-19398)

1.9.43.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.44. RHSA-2024:0837 - OpenShift Container Platform 4.14.13 程序错误修复和安全更新

发布日期： 2024 年 2 月 21 日

OpenShift Container Platform release 4.14.13 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:0837 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:0840 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.13 --pullspecs
```

1.9.44.1. 程序错误修复

- 在以前的版本中，Kubelet 使用不正确的 **unconfined_service_t** 标签运行，这会导致与 SELinux 相关的错误。在这个版本中，这个问题已被解决，kubelet 使用 **kubelet_exec_t** 标签运行。(OCPBUGS-22270)

1.9.44.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.45. RHSA-2024:0735 - OpenShift Container Platform 4.14.12 程序错误修复和安全更新

发布日期：2024 年 2 月 13 日

OpenShift Container Platform 版本 4.14.12 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:0735 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:0738 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.12 --pullspecs
```

1.9.45.1. 功能

这个 z-stream 发行版本包含了以下功能：

1.9.45.1.1. 使用带有 PTP Operator 的双 Intel E810 Westport Channel NIC 作为 grandmaster 时钟

- 现在，您可以通过创建一个配置这两个 NIC 的 **PtpConfig** 自定义资源(CR)，将 **linuxptp** 服务配置为双 Intel E810 Westport Channel NIC 的 grandmaster 时钟(T-GM)。主机系统时钟与连接到 GNSS 时间源的 NIC 同步。第二个 NIC 同步到由连接到 GNSS 的 NIC 提供的 1PPS 时间输出。如需更多信息，请参阅将 linuxptp 服务配置为双 E810 Westport Channel NIC 的 grandmaster 时钟。(RHBA-2024:0734)

1.9.45.2. 程序错误修复

- 在以前的版本中，release-to-channel 策略和 **oc-mirror** 行为会导致软件包的选择性镜像出现错误。当有选择地镜像软件包的最新（以及默认）频道，且新版本引入了一个新的频道，当前的默认频道会无效，且自动分配新默认频道会失败。在这个版本中，这个问题已被解决。现在，您可以在 **ImageSetConfig** CR 中定义可覆盖 **currentDefault** 频道的 **defaultChannel** 字段。(OCPBUGS-28871)

- 在以前的版本中，EFS CSI 驱动程序容器的 CPU 限制可能会导致性能下降。在这个版本中，EFS CSI 驱动程序容器中的 CPU 限制已被删除。(OCPBUGS-28823)

- 在以前的版本中，当使用 **routingViaHost** 模式时，访问 **ExternalTrafficPolicy=Local** 负载均衡器服务会破坏。在这个版本中，这个问题已被解决。(OCPBUGS-28789)

- 在以前的版本中，当部署了 HostedCluster 且用户定义了 KAS **AdvertiseAddress** 时，它与当前部署冲突，与 Service、Cluster 或 Machine 网络等其他网络重叠，这会导致部署失败。在这个版本中，添加了 **AdvertiseAddress** 的网络验证。(OCPBUGS-20547)

1.9.45.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.46. RHSA-2024:0642 - OpenShift Container Platform 4.14.11 程序错误修复和安全更新

发布日期： 2024 年 2 月 7 日

OpenShift Container Platform 版本 4.14.11 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:0642 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:0645 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.11 --pullspecs
```

1.9.46.1. 功能

这个 z-stream 发行版本包含了以下功能：

1.9.46.1.1. 启用关于 cron 计划的位置配置

- Whereabouts 协调调度被硬编码为每天运行一次，且无法重新配置。在这个版本中，**ConfigMap** 启用了 whereabouts cron schedule 的配置。如需更多信息，请参阅配置 Whereabouts IP 协调器调度。

1.9.46.2. 程序错误修复

- 在以前的版本中，更新 OpenShift Container Platform 可能会导致 DNS 查询失败，因为上游为使用 CoreDNS 1.10.1 的非EDNS 查询返回大于 512 字节的有效负载。在这个版本中，具有不合规上游的集群会在溢出错误时重试 TCP，这会阻止在更新时中断功能。(OCPBUGS-28200)

- 在以前的版本中，因为环境变量中的拼写错误，每次重启时 **node.env** 文件都会被覆盖。在这个版本中，对 **node.env** 的编辑在重启后会被保留。(OCPBUGS-27362)

- 在以前的版本中，**container_t** 无法访问直接渲染基础架构 (DRI) 设备。在这个版本中，策略已被更新，**container_t** 现在可以访问设备插件公开的 DRI 设备和 GPU 设备。(OCPBUGS-27275)

- 在以前的版本中，pod 从 Whereabouts CNI 插件创建的池中分配 IP 地址，在节点强制重启后会处于 **ContainerCreating** 状态。在这个版本中，在节点强制重启后与 IP 分配关联的 Whereabouts CNI 插件问题被解决。(OCPBUGS-26553)

1.9.46.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.47. RHSA-2024:0290 - OpenShift Container Platform 4.14.10 程序错误修复和安全更新

发布日期：2024 年 1 月 23 日

OpenShift Container Platform release 4.14.10 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:0290 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:0293 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.10 --pullspecs
```

1.9.47.1. 程序错误修复

- 在以前的版本中，当 Cloud Credential Operator (CCO)处于默认模式时，CCO 使用不正确的客户端进行根凭证查询。CCO 无法查找预期的 secret，并在 **cco_credentials_mode** 指标中错误地报告 **credsremoved** 模式。在这个版本中，CCO 使用正确的客户端，以确保准确报告 **cco_credentials_mode** 指标。(OCPBUGS-26512)

1.9.47.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.48. RHSA-2024:0204 - OpenShift Container Platform 4.14.9 程序错误修复和安全更新

发布日期：2024 年 1 月 17 日

OpenShift Container Platform release 4.14.9 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:0204 公告中。此更新中包括的 RPM 软件包由 RHSA-2024:0207 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.9 --pullspecs
```

1.9.48.1. 程序错误修复

- 在以前的版本中，Cluster Version Operator (CVO) 持续检索更新建议，并根据当前集群状态评估已知的条件更新风险。CVO 更改会导致风险评估失败，以防止 CVO 获取新的更新建议。这个程序错误会导致 CVO 无法注意到更新建议服务可以改进的风险声明。在这个版本中，CVO 继续轮询更新建议服务，无论是否成功评估更新风险。(OCPBUGS-26207)
- 在以前的版本中，对镜像发行版本使用 eus-* 频道会导致使用 oc-mirror 插件进行镜像失败。这是因为 oc-mirror 插件不会确认 eus-* 频道只有偶数号。在这个版本中，oc-mirror 插件的发布用户应该可以使用 eus-* 频道用于镜像版本。(OCPBUGS-26065)

1.9.48.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.49. RHSA-2024:0050 - OpenShift Container Platform 4.14.8 程序错误修复和安全更新

发布日期： 2024 年 1 月 9 日

OpenShift Container Platform release 4.14.8 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2024:0050 公告中。此更新中包括的 RPM 软件包由 RHBA-2024:0053 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.8 --pullspecs
```

1.9.49.1. 功能

这个 z-stream 发行版本中包括以下功能：

- 在这个版本中，Telemetry 数据从发生 pod 安全准入违反情况的集群收集。收集的数据是出错命名空间、OpenShift Container Platform 系统命名空间或自定义命名空间。此数据收集有助于红帽评估客户以后对 pod 安全准入全局限制强制的集群就绪。如需有关 pod 安全准入的更多信息，

请参阅 了解和管理 pod 安全准入。(OCPBUGS-25384)

- 在以前的版本中，用户无法使用分层产品将 OpenShift 的 Azure 身份功能用于短期的身份验证令牌。在这个版本中，OLM 管理的 Operator 通过启用这个支持来提高安全性。(OCPBUGS-25275)

1.9.49.2. 程序错误修复

- 在以前的版本中，当在禁用了安全引导(Secure Boot)的节点中安装带有 **bootMode** 设置为 **UEFISecureBoot** 的 OpenShift Container Platform 时，安装会失败。在这个版本中，后续尝试安装启用了安全引导(Secure Boot)的 OpenShift Container Platform 会正常进行。(OCPBUGS-19884)

- 在以前的版本中，当在 Google Cloud Platform 上使用区域 PD 时，安装程序将无法销毁集群。在这个版本中，会找到复制区域，磁盘会被正确删除。(OCPBUGS-22770)

- 在以前的版本中，如果没有在 control plane 节点中指定 **additionalSecurityGroupIDs** 字段，则不会使用 **defaultMachinePlatform** 小节中的 **additionalSecurityGroupID**。在这个版本中，如果没有在 control plane 节点中指定 **additionalSecurityGroupIDs** 字段，则会使用 **defaultMachinePlatform** 小节中的 **additionalSecurityGroupID**。(OCPBUGS-22771)

1.9.49.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.50. RHSA-2023:7831 - OpenShift Container Platform 4.14.7 程序错误修复和安全更新

发布日期：2024 年 1 月 3 日

OpenShift Container Platform release 4.14.7 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2023:7831 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:7834 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.7 --pullspecs
```

1.9.50.1. 程序错误修复

- 在以前的版本中，当重启 IPsec pod 时，它会终止现有的策略。在这个版本中，IPsec 服务也会重启，它会重新恢复现有的策略并解决问题。(OCPBUGS-24633)

- 在以前的版本中，更新 control plane 机器集自定义资源以引用无效资源，如无效的网络名称或镜像，它会创建一个处于置备状态的 control plane 机器，且无法被删除。在这个版本中，这个问题已被解决。(OCPBUGS-23202)

- 在以前的版本中，应用性能配置集会导致 tuned 配置集报告 **DEGRADED** 条件。这是因为生成的 tuned 配置集试图设置第二个 sysctl 值。在这个版本中，sysctl 值不再由 tuned 设置，而是仅由 **sysctl.d** 文件设置。(OCPBUGS-25305)

1.9.50.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.51. RHSA-2023:7682 - OpenShift Container Platform 4.14.6 程序错误修复和安全更新

发布日期：2023 年 12 月 12 日

OpenShift Container Platform release 4.14.6 现已正式发布，其中包括安全更新。其程序错误修正列表包括在 RHSA-2023:7682 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:7685 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.6 --pullspecs
```

1.9.51.1. 功能

这个 z-stream 发行版本中包含以下 PTP 功能：

1.9.51.1.1. 在 PTP Operator 中使用特定于硬件的 NIC 功能

- 提供了新的 PTP Operator 硬件插件，允许您将硬件特定功能用于 PTP Operator 支持的 NIC。目前支持 Intel Westport 频道 E810 NIC。如需更多信息，请参阅 E810 硬件配置参考。

1.9.51.1.2. 为 PTP grandmaster 时钟使用 GNSS 时间同步

- PTP Operator 现在支持从连接到 grandmaster 时钟(T-GM)的 Global Navigation Satellite 系统(GNSS)源接收精度 PTP 时间。如需更多信息，请参阅将 linuxptp 服务配置为 grandmaster 时钟。

1.9.51.2. 程序错误修复

- 在以前的版本中，当从双栈集群中部署 IPv6 主机时，问题会阻止 Baseboard Management Controller (BMC)接收正确的回调 URL。相反，BMC 会收到 IPv4 URL。在这个版本中，这个问题不再发生，因为 URL 的 IP 版本取决于 BMC 地址的 IP 版本。(OCPBUGS-23903)

- 在以前的版本中，在有保证 CPU 且禁用中断请求(IRQ)负载均衡的单节点 OpenShift 中，容器启动时可能会出现大量延迟激增。在这个版本中，这个问题不再发生。(OCPBUGS-22901) (OCPBUGS-24281)

1.9.51.3. 已知问题

- 对于 PTP 时间同步，需要 DPLL 阶段偏移监控才能完全确定 grandmaster 时钟(T-GM)状态。这目前在 in-tree ice 驱动程序 DPLL API 中没有，它会创建一个用于决定 grandmaster 状态的盲点。

1.9.51.4. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.52. RHSA-2023:7599 - OpenShift Container Platform 4.14.5 程序错误修复和安全更新

发布日期：2023 年 12 月 5 日

OpenShift Container Platform release 4.14.5 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-2023:7599 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:7603 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.5 --pullspecs
```

1.9.52.1. 程序错误修复

- 在以前的版本中，当构建功能没有启用时，当尝试与构建 informer 同步时，ConfigObserver 控制器将失败。在这个版本中，当构建功能没有启用时，ConfigObserver 会成功启动。(OCPBUGS-23490) (OCPBUGS-21778)
- 在以前的版本中，Cloud Credential Operator (CCO)不支持更新 **kube-system** 命名空间中的 VMware vSphere root secret (**vsphere-creds**)。这导致组件 secret 无法正确同步。在这个版本中，CCO 支持更新 vSphere root secret，并在同步时重置 secret 数据。(OCPBUGS-23426)
- 在以前的版本中，当部署有大量 pod 的应用程序时，一些配置了 CPU 限制，部署可能会失败。在这个版本中，这个问题不再发生。(RHEL-7232)

1.9.52.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.53. RHSA-2023:7470 - OpenShift Container Platform 4.14.4 程序错误修复和安全更新

发布日期：2023 年 11 月 29 日

OpenShift Container Platform release 4.14.4 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-2023:7470 公告中。此更新中包括的 RPM 软件包由 RHSA-2023:7473 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.4 --pullspecs
```

1.9.53.1. 程序错误修复

- 在以前的版本中，当您在 **install-config.yaml** 配置文件的 **kmsKeyARN** 部分指定密钥管理服务(KMS)加密密钥时，在 Amazon Web Services (AWS)上安装集群时，在集群安装操作过程中不会添加权限角色。在这个版本中，在配置文件中指定密钥后，会在集群中添加一组额外的密钥，以便集群成功安装。如果您在配置文件中指定了 **credentialsMode** 参数，则忽略所有 KMS 加密密钥。(OCPBUGS-22774)

1.9.53.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.54. RHSA-2023:7315 - OpenShift Container Platform 4.14.3 程序错误修复和安全更新

发布日期：2023 年 11 月 21 日

OpenShift Container Platform release 4.14.3 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-2023:7315 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:7321 公告提供。

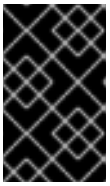
因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.3 --pullspecs
```

1.9.54.1. 程序错误修复

- 在以前的版本中，如果集群中有任何 **ImageContentSourcePolicy** (ICSP)对象，则无法使用 **ImageDigestMirrorSet** (IDMS) 和 **ImageTagMirrorSet** (ITMS) 对象。因此，要使用 IDMS 或 ITMS 对象，您需要删除集群中的任何 ICSP 对象，这需要重启集群。在这个版本中，ICSP、IDMS 和 ITMS 对象可以同时在同一集群中正常工作。因此，您可以在安装集群后使用任意或全部三种类型的对象来配置存储库镜像。如需更多信息，请参阅了解镜像 registry 存储库镜像。(RHIBMCS-185)



重要

使用 ICSP 对象配置存储库镜像是一个已弃用的功能。弃用的功能仍然包含在 OpenShift Container Platform 中，并被支持。但是，可能会在以后的发行版本中删除。由于它已被弃用，因此避免将其用于新部署。

- 在以前的版本中，如果节点包含额外的端口，且 **enable_port_security** 参数设置为 **false**，则不会为部署创建 **LoadBalancer** 服务。在这个版本中，会为包含带有此设置的额外端口的部署创建 **LoadBalancer** 服务。(OCPBUGS-22974)

- 在以前的版本中，**ClusterAutoscaler** 资源会进入 **CrashBackoff** 循环，用于使用 Container Storage Interface (CSI)实现配置的节点。此发行版本更新了依赖项，以便 **ClusterAutoscaler** 资源不再进入以这种方式配置的节点的 **CrashBackoff** 中。(OCPBUGS-23270)

1.9.54.2. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.55. RHSA-2023:6837 - OpenShift Container Platform 4.14.2 程序错误修复和安全更新

发布日期：2023 年 11 月 15 日

OpenShift Container Platform release 4.14.2 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-2023:6837 公告中。此更新中包括的 RPM 软件包由 RHSA-2023:6840 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.2 --pullspecs
```

1.9.55.1. 程序错误修复

- 在以前的版本中，在 **eastus** 区域中更改新 Microsoft Azure 存储帐户的默认安全设置会阻止在该区域中使用 Azure AD Workload Identity 的 OpenShift Container Platform 集群安装。这个版本已经解决了这个问题。(OCPBUGS-22651)
- 在以前的版本中，Docker 构建部署会失败，因为内联 Dockerfile hook 没有保留所复制的文件的修改时间。在这个版本中，当在容器间复制工件来保留时间戳时，在 **cp** 命令中添加 '-p' 标志。(OCPBUGS-23006)
- 在以前的版本中，Image Registry Operator 对 Storage Account List 端点发出 API 调用，因为每 5 分钟获取访问密钥的一部分。在有很多 OpenShift Container Platform (OCP)集群的项目中，这可能会导致 API 限制在尝试创建新集群时造成 429 错误。在这个版本中，调用之间的时间从 5 分钟增加到 20 分钟。(OCPBUGS-22127)
- 在以前的版本中，cloud-controller-manager (CCM) 服务帐户中省略了 Azure Managed Identity 角色，这意味着 CCM 无法正确管理使用私有发布方法部署到现有 VNets 的环境中的 **Service** 类型 **LoadBalancer**。在这个版本中，缺少的角色被添加到 CCO 实用程序 (**ccoctl**) 中，以便 Azure Managed Identity 安装可以使用私有发布将现有的 VNet 添加至现有的 VNet 中。(OCPBUGS-21926)
- 此补丁为 Azure 设置启用出口 IP，它们使用出站规则来实现出站连接。Azure 中的架构限制可防止次要 IP 作为出口 IP 在此类设置中具有出站连接。这意味着匹配的 pod 没有到互联网的出站连接，但可以访问基础架构网络中的外部服务器，这是出口 IP 的预期用例。(OCPBUGS-21785)
- 在以前的版本中，当 MetalLB Operator 的控制器在分配 IP 和未分配的负载均衡器服务时，它会重启一个空内部状态，这可能会中断工作负载。在这个版本中，MetalLB 的控制器被修改为首先处理已分配 IP 的服务。(OCPBUGS-16267)
- 在以前的版本中，如果您创建了名称与 OpenShift Container Platform 或 Kubernetes 资源使用的集群角色相同的 Operator 组，Operator Lifecycle Manager (OLM) 将覆盖集群角色。在这个版本中，如果您创建一个与 OpenShift Container Platform 或 Kubernetes 使用的集群角色冲突的 Operator 组，OLM 会根据以下语法生成唯一的集群角色名称：

  命名语法

  ```
  olm.og.<operator_group_name>.<admin_edit_or_view>-<hash_value>
  ```

  OLM 仅为与 OpenShift Container Platform 和 Kubernetes 使用的一组定义的集群角色冲突的 Operator 组生成唯一名称。您必须确保 Operator 组的名称不会与集群中存在的其他集群角色冲突。

  OLM 为与以下集群角色冲突的 Operator 组生成唯一名称：

  - **aggregate-olm**
  - **alert-routing**
  - **cluster**
  - **cluster-monitoring**
  - **monitoring**

- **monitoring-rules**
- **packagemanifests-v1**
- **registry**
- **storage**
  (OCPBUGS-19789)

1.9.55.2. 已知问题

- 本发行版本中存在一个已知问题，可防止使用安装程序置备的基础架构在 Alibaba Cloud 上安装集群。在 Alibaba Cloud 上安装集群是本发行版本中的技术预览功能。(OCPBUGS-20552)

1.9.55.3. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.56. RHBA-2023:6153 - OpenShift Container Platform 4.14.1 程序错误修复更新

发布日期：2023 年 11 月 1 日

OpenShift Container Platform 版本 4.14.1 现已正式发布。其程序错误修正列表包括在 RHBA-2023:6153 公告中。此更新中包括的 RPM 软件包由 RHBA-2023:6152 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.1 --pullspecs
```

1.9.56.1. 更新

要将现有 OpenShift Container Platform 4.14 集群更新至此最新版本，请参阅使用 CLI 更新集群。

1.9.57. RHSA-2023:5006 - OpenShift Container Platform 4.14.0 镜像发行版本、程序错误修正和安全更新公告

发布日期：2023 年 10 月 31 日

OpenShift Container Platform 版本 4.14.0 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-2023:5006 公告中。此更新中包括的 RPM 软件包由 RHSA-2023:5009 公告提供。其安全更新列表包括在 RHSA-2023:6143 公告中。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。

您可以运行以下命令来查看此发行版本中的容器镜像：

```
$ oc adm release info 4.14.0 --pullspecs
```