



OpenShift Container Platform 4.5

发行注记

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

OpenShift Container Platform 4.5 发行注记

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

法律通告

Copyright © 2021 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

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

目录

第 1 章 OPENSIFT CONTAINER PLATFORM 4.5 发行注记	3
1.1. 关于此版本	3
1.2. 新功能及功能增强	3
1.3. 主要的技术变化	15
1.4. 弃用和删除的功能	16
1.5. 程序错误修复	20
1.6. 技术预览功能	40
1.7. 已知问题	41
1.8. 异步勘误更新	44
第 2 章 OPENSIFT CONTAINER PLATFORM 版本政策	64

第 1 章 OPENSIFT CONTAINER PLATFORM 4.5 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

Red Hat OpenShift Container Platform (RHBA-2020:2409) 现已发布。此发行版本使用 [Kubernetes 1.18](#) 和 CRI-O 运行时。OpenShift Container Platform 4.5 的新功能、改变以及已知的问题包括在此文档中。

红帽没有公开发布 OpenShift Container Platform 4.5.0，而是直接发布了 OpenShift Container Platform 4.5.1 作为正式发行版本 (GA)。

OpenShift Container Platform 4.5 集群位于 <https://cloud.redhat.com/openshift>。您可以通过 OpenShift Container Platform 的 Red Hat OpenShift Cluster Manager 应用程序在内部环境或云环境中部署 OpenShift 集群。

OpenShift Container Platform 4.5 需要运行在 RHEL 7，7.7 或 7.8，以及 Red Hat Enterprise Linux CoreOS (RHCOS) 4.5 上。

您必须使用 Red Hat Enterprise Linux CoreOS (RHCOS) 作为 control plane（也称为 master）的系统，而 compute（也称为 worker）机器可以使用 RHCOS，或 RHEL 7（7.7 及更新版本）。



重要

因为只有 RHEL 7 版本 7.7 或更新版本支持计算机器，所以不能将 RHEL 计算机器升级到版本 8。

随着 OpenShift Container Platform 4.5 的发布，版本 4.2 现在已结束其生命周期。如需更新相关信息，请参阅 [Red Hat OpenShift Container Platform 生命周期政策](#)。

1.2. 新功能及功能增强

此版本对以下方面进行了改进

1.2.1. 安装和升级

1.2.1.1. 使用安装程序置备的基础架构在 vSphere 上安装集群

OpenShift Container Platform 4.5 支持使用安装程序置备的基础架构在 vSphere 上安装集群。

1.2.1.2. 使用用户置备的基础架构和共享 VPC 在 GCP 上安装集群

OpenShift Container Platform 4.5 引进了对使用用户置备的基础架构和共享 VPC 在 Google Cloud Platform (GCP) 上安装集群的支持。

1.2.1.3. 三节点裸机部署

您可在没有 worker 的 OpenShift Container Platform 中安装和运行三节点集群。这为部署、开发和测试提供了较小的、效率更高的集群。

在以前的版本中，这个功能是一个技术预览。OpenShift Container Platform 4.5 已完全支持这个功能。

如需更多信息，请参阅 [运行三节点集群](#)。

1.2.1.4. 受限网络集群升级改进

在受限网络集群升级过程中，如果镜像签名作为一个配置映射存在于集群中时，Cluster Version Operator (CVO) 现在可在验证发行的镜像。因此，在受限网络环境中的升级不再需要使用 **--force** 标志。

现在，通过运行增强的 **oc adm release mirror** 命令改进了升级工作流。以下操作会被执行：

- 在镜像 (mirror) 过程中从发行版本中拉取镜像 (image) 签名。
- 将签名配置映射直接应用到连接的集群。

1.2.1.5. 迁移 Azure 私有 DNS 区域

现在，提供了一个新的 **openshift-install migrate** 命令用于迁移 Azure 私有 DNS 区域。如果您在 Azure 上安装了使用安装程序置备的基础架构的 OpenShift Container Platform 版本 4.2 或 4.3 集群，您的集群可能会使用传统的私有 DNS 区域。如果这样做，您需要将其迁移到私有 DNS 区的新类型中。

1.2.1.6. 内置 install-config.yaml 支持字段的帮助信息

现在提供了一个新的 **openshift-install explain** 命令，可列出支持的 **install-config.yaml** 文件版本，其中包括对每个资源的简短描述。它还详细介绍了哪些字段是强制的，并指定了它们的默认值。使用 **explain** 命令可减少在创建或自定义 **install-config.yaml** 文件时不断查找配置选项的需要。

1.2.1.7. 使用 KMS 密钥加密 EBS 实例卷

现在，可以定义一个 KMS 密钥来加密 EBS 实例卷。如果您在部署到 AWS 时有明确的合规和安全准则时，这非常有用。通过设置可选的 **kmsKeyARN** 字段，可在 **install-config.yaml** 文件中配置 KMS 密钥。例如：

```
apiVersion: v1
baseDomain: example.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    aws:
      rootVolume:
        kmsKeyARN: arn:aws:kms:us-east-2:563456982459:key/4f5265b4-16f7-xxxx-xxxx-
xxxxxxxxxxxxx
...
```

如果没有指定密钥，则会使用帐户针对特定地区的默认 KMS 密钥。

1.2.1.8. 在 AWS 中带有多个 CIDR 的已存在的 VPC 中安装

现在，您可以在 AWS 中的一个带有多个 CIDR 的 VPC 上安装 OpenShift Container Platform。这可让您为机器网络选择从属 CIDR。当 VPC 由安装程序置备时，它不会创建多个 CIDR，或在子网间配置路由。用户置备的基础架构和安装程序置备的基础架构的安装 workflows 都支持在带有多个 CIDR 的已存在的 VPC 上进行安装。

1.2.1.9. 在 AWS Virtual Private Cloud (VPC) DHCP 选项集中添加自定义域名

现在可将自定义域名添加到 AWS Virtual Private Cloud (VPC) DHCP 选项集。这会在使用自定义 DHCP 选项时为新节点启用证书签名请求 (CSR) 批准。

1.2.1.10. 使用 Ironic 的 IPv6 置备裸机主机

Ironic 现已包括了使用 UEFI 网络堆栈的 IPv6 置备所需的二进制文件。现在，您可以使用 Ironic 的 IPv6 来置备裸机主机。**snpnoly.efi** bootloader 可执行代码和兼容的 iPXE 库现在包括在 **tftboot** 目录中。

1.2.1.11. RHOSP 上集群的自定义网络和子网

OpenShift Container Platform 4.5 现在支持在依赖于现有网络和子网的 Red Hat OpenStack Platform (RHOSP) 上安装集群。

1.2.1.12. 用于 RHOSP 上集群的额外网络

OpenShift Container Platform 4.5 引入了对在 RHOSP 上运行的集群中的多个网络的支持。您可以在安装过程中为 control plane 和计算机器指定这些网络。

1.2.1.13. 改进了使用 Kuryr 的集群的 RHOSP 负载均衡器的升级体验

使用 Kuryr 的集群现在改进了对从 13 升级到 16 的 RHOSP 集群上的 Octavia 负载均衡服务的支持。例如，这些集群现在支持 Octavia OVN 供应商驱动程序。

如需更多信息，请参阅 [Octavia OVN 驱动程序](#)。

1.2.1.14. 安装 RPM 软件包时接受的多个版本方案

安装 RPM 软件包时，OpenShift Container Platform 现在接受三部分和两个部分的版本方案。三部分版本名方案采用 **x.y.z** 格式，两部分版本名方案则采用 **x.y** 格式。使用其中任何一种方案的软件包都可以被安装。如需更多信息，请参阅 [BZ#1826213](#)。

1.2.1.15. 调试信息不再需要 SSH 配置

从 bootstrap 主机收集调试信息不再需要 SSH 配置。如需更多信息，请参阅 [BZ#1811453](#)。

1.2.1.16. Master 节点可以命名为任何有效的主机名

Master 节点现在可以命名为任何有效的主机名。如需更多信息，请参阅 [BZ#1804944](#)。

1.2.1.17. 在以前的 RHOSP 版本上支持 Octavia OVN 供应商驱动程序

在 RHOSP 支持 Octavia OVN provider 驱动程序之前部署的 OpenShift Container Platform 集群现在可以使用该驱动程序。如需更多信息，请参阅 [BZ#1847181](#)。

1.2.1.18. Octavia OVN provider 驱动支持在同一端口上的多个监听程序

现在，**ovn-octavia** 驱动支持在同一个端口中的多个不同协议的监听程序。之前，在 **ovn-octavia** 驱动程序上不支持这个功能。但现在它已被支持，因此无需阻止它。这意味着，例如，在使用 **ovn-octavia** 时 DNS 服务可以在 TCP 和 UDP 协议中公开端口 53。如需更多信息，请参阅 [BZ#1846452](#)。

1.2.2. 安全性

1.2.2.1. 在受限网络安装中使用 **oauth-proxy** 镜像流

现在，通过使用 **oauth-proxy** 镜像流，受限网络安装的外部组件现在可以使用 **oauth-proxy** 镜像。

1.2.3. 镜像

1.2.3.1. 使用文件对发行版本镜像进行镜像处理 (mirror)

现在，您可以将发现版本的镜像从一个 registry 镜像到一个文件，或从一个文件镜像到 registry。

1.2.3.2. 镜像发行版本镜像签名

oc adm release mirror 命令被扩展，现在它也会创建并应用包含发行镜像签名的配置映射清单，Cluster Version Operator 可使用它来验证镜像的发行版本。

1.2.4. 机器 API

1.2.4.1. AWS 机器集支持 spot 实例

AWS 机器集现在支持 spot 实例。您可以创建一个机器集把集群部署为 spot 实例。与 on-demand 实例相比，这可以节约成本。您可以通过在机器集 YAML 文件中的 **providerSpec** 字段中添加以下行来配置 spot 实例：

```
providerSpec:
  value:
    spotMarketOptions: {}
```

1.2.4.2. 自动缩放的最小机器数为 0

现在，您可以将机器自动扩展的最小副本数设置为 **0**。这样，自动扩展可以在零台机器和根据工作负载所需的资源需要的机器数量之间进行缩放，以提高性价比。

如需更多信息，请参阅 [MachineAutoscaler 资源定义](#)。

1.2.4.3. 带有空 selector 的 MachineHealthCheck 资源会监控所有机器

现在，包含空 **selector** 字段的 **MachineHealthCheck** 资源会监控所有机器。

有关 **MachineHealthCheck** 资源中的 **selector** 字段的更多信息，请参阅 [Sample MachineHealthCheck 资源](#)。

1.2.4.4. 使用 **oc explain** 查看机器和机器集字段的信息

现在为机器和机器集自定义资源提供了完整的 OpenAPI 模式。**oc explain** 命令现在提供机器和机器集 API 资源中包含的字段描述。

1.2.5. 节点

1.2.5.1. 提供了新的 descheduler 策略（技术预览）

descheduler 现在允许您配置 **RemovePodsHavingTooManyRestarts** 策略。此策略确保已经多次重启的 pod 将从节点中删除。同样，Descheduler Operator 现在支持完整的上游 descheduler 策略名称，允许更多的一对一配置。

如需更多信息，请参阅 [Descheduler 策略](#)。

1.2.5.2. Vertical Pod Autoscaler Operator（技术预览）

OpenShift Container Platform 4.5 引进了 Vertical Pod Autoscaler Operator (VPA)。VPA 会自动检查 pod 中容器的运行状况和当前的 CPU 和内存资源，并根据它所了解的用量值更新资源限值和请求。您可以创建独立的自定义资源 (CR) 来指示 VPA 如何更新与工作负载对象关联的所有 pod，如 **Deployment**、**Deployment Config**、**StatefulSet**、**Job**、**DaemonSet**、**ReplicaSet** 或 **ReplicationController**。VPA 可帮助您了解 Pod 的最佳 CPU 和内存使用情况，并可以通过 pod 生命周期自动维护 pod 资源。

1.2.5.3. 在 RHOSP 上进行反关联性 control plane 节点调度

如果 RHOSP 部署上有单独的物理主机，则 control plane 节点会在所有这些物理主机上进行调度。

1.2.6. 集群监控

1.2.6.1. 监控您自己的服务（技术预览）

在进一步增强监控您自己的服务方面有以下改进：

- 允许将您自己的服务的指标与集群指标进行比较。
- 在记录和警报规则中允许在用户命名空间中使用服务指标。
- 为 Alertmanager API 添加多租户支持。
- 添加了部署具有高可用性的用户记录和警报规则的功能。
- 增加了使用 Thanos Querier 内省 Thanos Store 的功能。
- 从 web 控制台的一个视图中访问所有服务的指标。

如需更多信息，请参阅 [监控您自己的服务](#)。

1.2.7. 集群日志记录

1.2.7.1. Elasticsearch 版本升级

OpenShift Container Platform 4.5 中的集群日志记录现在使用 Elasticsearch 6.8.1 作为默认日志存储。

新的 Elasticsearch 版本引入了新的 Elasticsearch 数据模型。使用新的数据模型时，数据不再按类型（设备和应用程序）和项目进行索引。数据仅按类型索引：

- 之前在 OpenShift Container Platform 4.4 中的 **project-** 索引中的应用程序日志现在位于一组带有 **app-** 前缀的索引中。

- 以前在 `.operations-` 索引中使用的基础架构日志现在包括在 `infra-` 索引中。
- 审计日志保存在 `audit-` 索引中。

由于新的数据模型，更新不会将现有的自定义 Kibana 索引模式和视觉化迁移到新版本。您必须重新创建 Kibana 索引模式和视觉化，以便在更新后匹配新索引。

Elasticsearch 6.x 还包含一个新的安全插件 - Open Distro for Elasticsearch。Open Distro for Elasticsearch 提供了一组完整的高级安全功能，以保持数据的安全。

1.2.7.2. 新的 Elasticsearch 日志保留功能

新的索引管理功能依赖于 Elasticsearch 的滚动 (rollover) 功能来维护索引。您可以配置，在从集群中删除数据前保留数据的时长。索引管理功能代替 Curator。在 OpenShift Container Platform 4.5 中，Curator 用于移除 OpenShift Container Platform 4.5 之前的 Elasticsearch 索引格式的数据，它将在以后的版本中删除。

1.2.7.3. Web 控制台中的 Kibana 链接已移动

启动 Kibana 的链接已从 **Monitoring** 菜单移到 OpenShift Container Platform 控制台  顶部的 **Application Launcher**。

1.2.8. Web 控制台

1.2.8.1. OperatorHub 中 Operator 的新基础架构功能过滤器

现在，您可以按照 OperatorHub 中的 **Infrastructure Features** 来过滤 Operator。例如，如果希望 Operator 在断开连接的环境中工作，请选择 **Disconnected**。

1.2.8.2. Developer Perspective (开发者视角)

现在，您可以使用 **Developer** 视角来：

- 在 **Developer Catalog** 中安装 Helm Charts 时可以参阅描述信息及文档
- 卸载、升级和回滚 Helm 发行版本。
- 创建和删除动态 Knative 事件源。
- 部署虚拟机、启动应用程序或删除虚拟机。
- 提供 Git webhook、Triggers 和 Workspaces，管理私有 git 仓库的凭证，并使用更好的日志为 OpenShift Pipelines 进行故障排除。
- 在应用程序部署期间或之后添加健康检查。
- 更有效地进行浏览并固定频繁搜索的项。

1.2.8.3. 简化了从集群仪表板配置警报的步骤

对于在 web 控制台的集群仪表板中显示的 **AlertManagerReceiversNotConfigured** 警报，现在增加了一个新的 **Configure** 链接。这个链接指向 Alertmanager 配置页面。这简化了配置警报的步骤。如需更多信息，请参阅 [BZ#1826489](#)。

1.2.9. 扩展

1.2.9.1. 集群最大限制

针对 OpenShift Container Platform 4.5 的[集群最大限制](#)指导信息已更新。

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

1.2.10. 网络

1.2.10.1. 从 OpenShift SDN 默认 CNI 网络供应商中迁移（技术预览）

现在，您可以从 OpenShift SDN 默认 CNI（Container Network Interface）网络供应商迁移到 OVN-Kubernetes 默认 CNI 网络供应商。

如需更多信息，请参阅 [从 OpenShift SDN 默认 CNI 网络供应商迁移](#)。

1.2.10.2. Ingress Controller 的改进

OpenShift Container Platform 4.5 中引入了两个值得注意的 Ingress Controller 的改进：

- 您可以为 [Ingress Controller](#) 启用访问日志。
- 您可以 [通过 Ingress Controller](#) 指定通配符路由策略。

1.2.10.3. HAProxy 升级至版本 2.0.14

用于 Ingress Controller 的 HAProxy 从 2.0.13 升级到 2.0.14。这个升级提高了路由器重新加载的性能。重新载入的性能的提高对于有数以千记路由的集群最有帮助。

1.2.10.4. HTTP/2 入口支持

现在，您可以在 HAProxy 中启用透明的端到端的 HTTP/2 连接。此功能使应用程序所有者利用 HTTP/2 协议功能，包括单一连接、标头压缩、二进制流等等。

您可以在 HAProxy 中为单独的 Ingress Controller 或整个集群启用 HTTP/2 连接。如需更多信息，请参阅 [HTTP/2 Ingress 连接](#)。

要在从客户端到 HAProxy 的连接中启用 HTTP/2，路由必须指定一个自定义证书。使用默认证书的路由无法使用 HTTP/2。这一限制是避免连接并发问题（如客户端为使用相同证书的不同路由重新使用连接）所必需的。

从 HAProxy 到应用程序 pod 的连接只能将 HTTP/2 用于 re-encrypt 路由，而不适用于 edge-terminated 或 insecure 路由。这个限制来自于，在与后端协商使用 HTTP/2 时，HAProxy 要使用 ALPN（Application-Level Protocol Negotiation），它是一个 TLS 的扩展。这意味着，端到端的 HTTP/2 适用于 passthrough 和 re-encrypt 路由，而不适用于 insecure 或 edge-terminated 路由。



重要

使用 HTTP/2 协议的连接无法升级到 WebSocket 协议。如果您有一个后端应用程序需要允许 WebSocket 连接，则不能允许连接来协商使用 HTTP/2 协议，否则其他 WebSocket 连接将失败。

1.2.11. 开发者体验

1.2.11.1. oc new-app 现在会生成 Deployment 资源

`oc new-app` 命令现在默认生成 **Deployment** 资源，而不是 **DeploymentConfig** 资源。如果要创建 **DeploymentConfig** 资源，可以在调用 `oc new-app` 时使用 `--as-deployment-config` 标志。如需更多信息，请参阅[了解 Deployment 和 DeploymentConfig](#)。

1.2.11.2. 支持镜像 registry CRD 中的节点关联性调度程序

现在支持节点关联性调度程序，以确保镜像 registry 部署可以在基础架构节点不存在的情况下完成。节点关联性调度程序需要手工配置。

如需更多信息，请参阅[使用节点关联性规则控制节点上的 pod 放置](#)。

1.2.11.3. 用于自定义 S3 端点的虚拟托管存储桶

现在，在新的或隐藏的 AWS 区域部署的集群支持虚拟托管存储桶。

1.2.11.4. 构建和镜像流导入过程中节点拉取凭证

如果未明确设置 pull secret，则构建和镜像流导入过程将自动使用用于安装集群的 pull secret。开发人员不需要将这个 pull secret 复制到其命名空间中。

1.2.12. 备份和恢复

1.2.12.1. 安全地关闭和重启集群

现在，您可以安全地关闭并重启 OpenShift Container Platform 4.5 集群。出于维护或者节约资源成本的原因，您可能需要临时关闭集群。

如需更多信息，请参阅[安全地关闭集群](#)。

1.2.13. 灾难恢复

1.2.13.1. 自动 control plane 证书恢复

从 OpenShift Container Platform 4.4.8 开始，现在可以从过期的 control plane 证书中自动恢复。一个例外情况是，您需要手动批准待处理的 **node-bootstrapper** 证书签名请求（CSR）来恢复 kubelet 证书。

如需更多信息，请参阅[恢复已过期的 control plane 证书](#)。

1.2.14. 存储

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

现在，您可以使用 Container Storage Interface（CSI）来部署置备 AWS Elastic Block Store（EBS）持久性存储所需的 CSI 驱动程序。该 Operator 是技术预览。如需更多信息，请参阅[AWS Elastic Block Store CSI Driver Operator](#)。

1.2.14.2. 使用 OpenStack Manila CSI Driver Operator 的持久性存储

现在，您可以使用 CSI 为 OpenStack Manila 共享文件系统服务的 CSI 驱动程序置备持久性卷。如需更多信息，请参阅[OpenStack Manila CSI Driver Operator](#)。

1.2.14.3. 使用 CSI 内联临时卷的持久性存储（技术预览）

现在，您可以使用 CSI 在 Pod 规格中直接指定卷，而不是在持久性卷中指定卷。这个功能在使用 CSI 驱动程序时默认可用。这个功能是一个技术预览功能。如需更多信息，请参阅 [CSI 内联临时卷](#)。

1.2.14.4. 持久性存储的 CSI 卷克隆

现在，OpenShift Container Platform 4.5 已完全支持使用 CSI 进行卷克隆（以前为技术预览功能）。如需更多信息，请参阅 [使用 CSI 卷克隆](#)。

1.2.14.5. 已删除 AWS EFS（技术预览）功能的外部置备程序

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

1.2.15. Operator

1.2.15.1. 用于打包 Operator 和 opm CLI 工具的捆绑格式

Operator 的捆绑格式 (Bundle Format) 是 Operator Framework 引入的新打包格式，从 OpenShift Container Platform 4.5 开始支持。为提高可伸缩性并使上游用户可以更好地托管自己的 catalog，捆绑格式规格简化了 Operator 元数据的发布。



注意

虽然 OpenShift Container Platform 4.5 中弃用了旧软件包清单格式 (Package Manifest Format)，但它仍被支持。红帽提供的 Operator 目前使用 Package Manifest Format。

一个 Operator 捆绑包代表了 Operator 的一个版本，并可与 Operator SDK 一起构建。磁盘上的 *捆绑清单* 会被容器化，并作为 *捆绑包镜像*（一个用来存储 Kubernetes 清单和 Operator 元数据的不可运行的容器镜像）提供。然后，就可以使用容器工具（如 **podman** 和 **docker**）以及容器 registry（如 Quay）管理捆绑镜像的存储和分发。

有关捆绑格式的详情，请参见 [打包格式](#)。

和捆绑格式一起还引进了新的 **opm** CLI 工具。**opm** CLI 允许您从捆绑包列表中创建和维护 Operator 目录 (catalog) ,相当于一个 "repository"。其结果是一个名为 *index image* (*索引镜像*) 的容器镜像，它可以存储在容器的 registry 中，然后安装到集群中。

索引包含一个指向 Operator 清单内容的指针数据库，可通过在运行容器镜像时提供的已包含 API 进行查询。在 OpenShift Container Platform 中，OLM 可通过引用 **CatalogSource** 对象中的索引镜像作为目录 (catalog)，它会定期轮询镜像，以对集群上安装的 Operator 进行更新。

有关 **opm** 的使用情况，请参阅 [管理定制目录](#)。

1.2.15.2. Operator Lifecycle Manager 对 v1 CRD 的支持

现在，当 Operator 被加载到目录并在集群中部署，Operator Lifecycle Manager (OLM) 支持使用 v1 CustomResourceDefinition (CRD) 的 Operator。以前，OLM 只支持 v1beta1 CRD。OLM 现在以同样的方式管理 v1 和 v1beta1 CRD。

为了支持这一功能，OLM 现在通过确保在升级 CRD 中没有缺少现有 CRD 存储版本来实施 CRD 升级更加安全，从而避免了潜在的数据丢失。

1.2.15.3. 报告 etcd 成员状态条件

etcd 集群 Operator 现在会报告 etcd 成员状态条件。

1.2.15.4. OLM 中对准入 webhook 的支持

验证 (validating) 和变异 (mutating) 准入 webhook 允许 Operator 作者在资源被保存到对象存储并由 Operator 控制器处理前，拦截、修改、接受或拒绝资源。当 webhook 与 Operator 一同提供时，Operator Lifecycle Manager (OLM) 可以管理这些 webhook 的生命周期。

如需了解更多详细信息，请参阅 [Operator Lifecycle Manager 中的管理准入 webhook](#)。

1.2.15.5. 从 openshift-config 命名空间中添加的配置映射配置

现在，可以使用 Insights Operator 从 **openshift-config** 命名空间中添加配置映射配置。这样，您可以查看是否将证书用作集群证书颁发机构，并从 **openshift-config** 命名空间收集其他与集群相关的设置。

1.2.15.6. 只读 Operator API (技术预览)

新的 Operator API 现在以只读模式作为技术预览功能提供。在以前的版本中，使用 Operator Lifecycle Manager (OLM) 安装 Operator 需要集群管理员了解多个 API，包括 **CatalogSource**、**Subscription**、**ClusterServiceVersion** 和 **InstallPlan** 对象。这个单一 Operator API 资源是实现更简化的体验发现和管理 OpenShift Container Platform 集群中 Operator 生命周期的第一步。

目前，只可以通过 CLI 使用，并需要几个手动步骤才能启用。此功能预览可使 Operator 与 Operator 进行交互，作为一类 API 对象。集群管理员可以使用 API 的只读模式发现之前安装的 Operator，例如使用 **oc get operators** 命令。

启用此技术预览功能：

流程

1. 禁用 OLM 的 [Cluster Version Operator \(CVO\) 管理](#)：

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

2. 为 OLM Operator 添加了 **OperatorLifecycleManagerV2=true** 功能门。

- a. 编辑 OLM Operator 的部署：

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


- b. 在部署的 **args** 部分添加以下标记：

```
...
  spec:
    containers:
      - args:
...
      - --feature-gates
      - OperatorLifecycleManagerV2=true
```

- c. 保存您的更改。

3. 如果还没有安装，使用普通的 OperatorHub 方法安装 Operator。这个示例使用在项目 **test-project** 中安装的 etcd Operator。
4. 为已安装的 etcd Operator 创建新的 Operator 资源。
 - a. 将以下内容保存到文件中：

etcd-test-op.yaml 文件

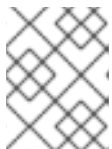
```
apiVersion: operators.coreos.com/v2alpha1
kind: Operator
metadata:
  name: etcd-test
```

- b. 创建资源：

```
$ oc create -f etcd-test-op.yaml
```

5. 要将已安装的 Operator 使用新的 API，将 **operators.coreos.com/etcd-test** 标志（label）应用到与 Operator 相关的以下对象：

- **Subscription**
- **InstallPlan**
- **ClusterServiceVersion**
- Operator 拥有的任何 CRD



注意

在以后的发行版本中，这些对象将自动标记为使用 **Subscription** 对象安装 CSV 的所有 Operator。

例如：

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

6. 确认您的 Operator 已选择新的 API。

- a. 列出所有
- operator**
- 资源：

```
$ oc get operators
```

```
NAME      AGE
etcd-test 17m
```

- b. 检查 Operator 的详情，注意您所标记的对象存在：

```
$ oc describe operators etcd-test
```

```
Name:      etcd-test
Namespace:
Labels:    <none>
Annotations: <none>
API Version: operators.coreos.com/v2alpha1
Kind:      Operator
Metadata:
  Creation Timestamp: 2020-07-02T05:51:17Z
  Generation:        1
  Resource Version:  37727
  Self Link:         /apis/operators.coreos.com/v2alpha1/operators/etcd-test
  UID:               6a441a4d-75fe-4224-a611-7b6c83716909
Status:
  Components:
  Label Selector:
  Match Expressions:
    Key:  operators.coreos.com/etcd-test
    Operator: Exists
  Refs:
  API Version: apiextensions.k8s.io/v1
  Conditions:
  Last Transition Time: 2020-07-02T05:50:40Z
  Message:              no conflicts found
  Reason:               NoConflicts
  Status:               True
  Type:                 NamesAccepted
  Last Transition Time: 2020-07-02T05:50:41Z
  Message:              the initial names have been accepted
  Reason:               InitialNamesAccepted
  Status:               True
  Type:                 Established
  Kind:                 CustomResourceDefinition
  Name:                 etcdclusters.etcd.database.coreos.com 1
  ...
  API Version:          operators.coreos.com/v1alpha1
  Conditions:
  Last Transition Time: 2020-07-02T05:50:39Z
  Message:              all available catalogsources are healthy
  Reason:               AllCatalogSourcesHealthy
  Status:               False
  Type:                 CatalogSourcesUnhealthy
  Kind:                 Subscription
```

```

Name:          etcd 2
Namespace:     test-project
...
API Version:   operators.coreos.com/v1alpha1
Conditions:
  Last Transition Time: 2020-07-02T05:50:43Z
  Last Update Time:   2020-07-02T05:50:43Z
  Status:             True
  Type:               Installed
Kind:          InstallPlan 3
Name:          install-mhzm8
Namespace:     test-project
...
Kind:          ClusterServiceVersion
Name:          etcdoperator.v0.9.4 4
Namespace:     test-project
Events:       <none>

```

- 1** 一个 CRD。
- 2** **Subscription** 对象。
- 3** **InstallPlan** 对象。
- 4** CSV。

1.2.15.7. 升级 Metering 并支持集群范围的代理配置

现在，您可以将 Metering Operator 升级从 4.2 升级到 4.5（通过 4.4）。在以前的版本中，需要卸载当前的 metering 安装，然后才可以重新安装 Metering Operator 的新版本。如需更多信息，请参阅[升级 metering](#)。

在这个版本中，支持集群范围的代理配置。另外，上游仓库从 operator-framework 机构移到 kube-reporting 中。

1.2.16. OpenShift virtualization

1.2.16.1. OpenShift Container Platform 4.5 上的 OpenShift Virtualization 支持

Red Hat OpenShift Virtualization 支持在 OpenShift Container Platform 4.5 中使用。OpenShift Virtualization（以前称为容器原生虚拟化）可让您将传统虚拟机（VM）附加到 OpenShift Container Platform 中，与容器一同运行，并作为原生 Kubernetes 对象管理。

1.3. 主要的技术变化

OpenShift Container Platform 4.5 包括以下显著的技术更改。

Operator SDK v0.17.2

OpenShift Container Platform 4.5 支持 Operator SDK v0.17.2，它包括以下显著的技术改变：

- **new**、**add api**、**add crd** 和 **generate crds** 命令增加了 **--crd-version** 标记，因此用户可以使用 **v1** CRD。默认设置为 **v1beta1**。

基于 Ansible 的 Operator 的增强包括：

- 支持基于 Ansible 的 Operator Watches 文件中的相对 Ansible 角色和 playbook 路径。
- 日志的事件统计数据输出到 Operator 日志。

基于 Helm 的 Operator 的增强包括

- 支持 Prometheus 指标。

支持 `terminationGracePeriod` 参数

OpenShift Container Platform 现在使用 CRI-O 容器运行时正确支持 `terminationGracePeriodSeconds` 参数。

API 服务器健康探测的 `/readyz` 配置

所有使用用户置备的基础架构的 OpenShift Container Platform 4.5 集群都必须配置为使用 `/readyz` 端点进行 API 服务器健康检查才能被支持。任何使用 OpenShift Container Platform 4.5 之前版本安装的用户置备基础架构的集群都必须被重新配置为使用 `/readyz`。

使用用户置备的基础架构未配置 `/readyz` 的集群可能会在 API 服务器重启时出现 API 故障。API 服务器可以在配置更改、证书更新或 control plane 机器重启等事件后重启。负载均衡器必须配置为，从 API 服务器关闭 `/readyz` 端点到从池中删除 API 服务器实例时最多需要 30 秒。在时间范围内，必须删除或添加 `readyz` 端点，这要看它返回的是错误还是健康。建议您每 5 秒或 10 秒进行就绪度检查，连续两个成功请求代表健康状态，连续三个失败请求代表不健康。

如需更多信息，请参阅用户置备的基础架构安装文档中的云供应商的网络拓扑要求。

已为 OpenShift Container Platform 发行版本重命名了二进制 `sha256sum.txt.sig` 文件

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

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

1.4. 弃用和删除的功能

之前版本中的一些功能已被弃用或删除。

弃用的功能仍然包含在 OpenShift Container Platform 中，并将继续被支持。但是，这个功能会在以后的发行版本中被删除，且不建议在新的部署中使用。有关 OpenShift Container Platform 4.5 中已弃用并删除的主要功能的最新列表，请参考下表。表后列出了更详细的、已弃用和删除的功能信息。

在下表中，被标记为以下状态的功能：

- **GA:** 正式发行
- **DEP:** 已弃用
- **REM:** 删除

表 1.1. 过时和删除的功能

功能	OCP 4.3	OCP 4.4	OCP 4.5
Service Catalog	DEP	DEP	REM

功能	OCP 4.3	OCP 4.4	OCP 4.5
Template Service Broker	DEP	DEP	REM
OpenShift Ansible Service Broker	DEP	REM	REM
OperatorSource	DEP	DEP	DEP
CatalogSourceConfig	DEP	DEP	REM
Operator Framework 的软件包清单格式	GA	DEP	DEP
v1beta1 CRD	GA	GA	DEP
AWS EFS 的外部置备程序（技术预览）	REM	REM	REM

1.4.1. 已弃用的功能

1.4.1.1. Jenkins Pipeline 构建策略

Jenkins Pipeline 构建策略现已弃用。您应该直接在 Jenkins 上使用 Jenkinsfile 或使用 OpenShift Pipelines。

1.4.1.2. v1beta1 CRD

自定义资源定义（CRD）的 `apiextensions.k8s.io/v1beta1` API 版本现已弃用。在以后的 OpenShift Container Platform 发行版本中会把它删除。

如需相关详细信息，请参阅 [Operator Lifecycle Manager 中的 v1 CRD 支持](#)。

1.4.1.3. 不再使用自定义标签

`flavor.template.kubevirt.io/Custom` 标签不再用于识别自定义类型。

1.4.1.4. OperatorSource 和 CatalogSourceConfig 对象会阻止集群升级

在一些 OpenShift Container Platform 版本中，**OperatorSource** 和 **CatalogSourceConfig** 对象已弃用。从 OpenShift Container Platform 4.4 开始，如果集群中存在任何自定义 **OperatorSource** 或 **CatalogSourceConfig** 对象，则 **marketplace** 集群 Operator 会设置一个 `Upgradeable=false` 条件并发出一个 **Warning** 警报。这意味着，如果这些对象仍然被安装，则升级到 OpenShift Container Platform 4.5 的过程会被阻止。



注意

在这种情况下，仍允许升级到 OpenShift Container Platform 4.4 z-stream 版本。

在 OpenShift Container Platform 4.5 中，**OperatorSource** 对象仍为弃用状态，仅用于使用默认 **OperatorSource** 对象。但是，**CatalogSourceConfig** 对象现已被删除。

如需了解如何直接使用 **CatalogSource** 对象转换 **OperatorSource** 和 **CatalogSourceConfig** 对象，请参阅 [OpenShift Container Platform 4.4 发行注记](#)，这可以清除警报并将集群升级到 OpenShift Container Platform 4.5。

1.4.1.5. Ignition 配置规格 v2

现在，在部署新节点时，v2 Ignition 配置规格已弃用，作为全新 OpenShift Container Platform 4.6 安装的一部分。v2 Ignition 配置规格仍支持机器配置。

如果您创建了自定义 Ignition v2 spec 配置来部署新集群，必须在安装新的 OpenShift Container Platform 4.6 集群时将其转换为 spec v3。您应该使用 [Ignition Config Converter 工具](#) 来完成转换过程。通常 v2 可以直接转换为 v3。在某些边缘情形中，可能需要修改输出来给出 spec v2 假设的配置详情。

1.4.2. 删除的功能

1.4.2.1. 已删除的 OpenShift CLI 命令和标志

以下 **oc** 命令和标志会受到影响：

- **oc policy can-i** 命令在 OpenShift Container Platform 3.9 中已启用并被删除。您需要使用 **oc auth can-i** 替代它。
- 以前 **oc new-app** 和 **oc new-build** 命令中使用的 **--image** 标志在 OpenShift Container Platform 3.2 中弃用，并已被删除。在这些命令中需要使用 **--image-stream** 标志。
- 以前在 **oc set volumes** 命令中使用的 **--list** 标志在 OpenShift Container Platform 3.3 中弃用，并已被删除。**oc set volumes** 列出卷时没有标志。
- 以前在 **oc process** 命令中使用的 **-t** 标志已在 OpenShift Container Platform 3.11 中弃用，并已被删除。在这个命令中需要使用 **--template** 标志。
- 以前在 **oc process** 命令中使用的 **--output-version** 标志已在 OpenShift Container Platform 3.11 中弃用，并已被删除。这个标志已经被忽略。
- 以前在 **oc set deployment-hook** 命令中使用的 **-v** 标志已在 OpenShift Container Platform 3.11 中弃用，并已被删除。在这个命令中需要使用 **--volumes** 标志。
- 以前在 **oc status** 命令中使用的 **-v** 和 **--verbose** 的标志在 OpenShift Container Platform 3.11 中已弃用，并已被删除。在这个命令中需要使用 **--suggest** 标志。

1.4.2.2. oc run OpenShift CLI 命令现在只创建 pod

现在，**oc run** 命令只用来创建 pod。使用 **oc create** 命令来创建其他资源。

1.4.2.3. Service Catalog、Template Service Broker 以及它们的 Operator



重要

Service Catalog 在 OpenShift Container Platform 4 中不会被默认安装，但如果已安装，它会阻止升级到 OpenShift Container Platform 4.5。

从 OpenShift Container Platform 4.2 开始，Service Catalog、Template Service Broker、Ansible Service Broker 以及它们的 Operator 已被弃用。OpenShift Container Platform 4.4 删除了 Ansible Service Broker，包括 Ansible Service Broker Operator 和相关的 API 和 APB。

Service Catalog、Template Service Broker 及其关联 Operator 现已从 OpenShift Container Platform 4.5 中删除，包括相关的 `.servicecatalog.k8s.io/v1beta1` API。



注意

OpenShift Container Platform 4.5 中仍然提供模板，但不再由 Template Service Broker 处理。在默认情况下，Samples Operator 处理基于 Red Hat Enterprise Linux (RHEL) 的 OpenShift Container Platform 镜像流和模板。如需更多信息，请参阅 [Configuring the Samples Operator](#)。

在 4.4 中，`service-catalog-controller-manager` 和 `service-catalog-apiserver` 集群 Operator 还会设置为 `Upgradeable=false`。这意味着，如果在升级时它们已安装，则会阻止升级到下一个次版本（在这里是 4.) 5。然而，升级到 z-stream 发行本，如 4.4.z，仍被允许。

如果在 4.4 中启用了 Service Catalog 和 Template Service Broker，特别是如果将其管理状态设为 **Managed** 时，则 web 控制台会警告集群管理员这些功能仍被启用。在集群 4.4 集群中，以下警报可以在 **Monitoring** → **Alerting** 页面中查看，其严重性级别为 **Warning**：

- **ServiceCatalogAPIServerEnabled**
- **ServiceCatalogControllerManagerEnabled**
- **TemplateServiceBrokerEnabled**

如果它们仍然在 4.4 集群中启用，集群管理员可以参阅 OpenShift Container Platform 4.4 文档中的[卸载 Service Catalog](#) 和 [卸载 Template Service Broker](#) 部分来卸载它们，这将可以使集群升级到 4.5。

在 4.5 中，会在 `openshift-service-catalog-removed` 命名空间中创建一对作业在集群升级过程中运行。它们的行为取决于服务目录的管理状态：

- **Removed:** 作业删除以下服务目录项：
 - Operator
 - 命名空间
 - 自定义资源 (CR)
 - **ClusterRole** 对象
 - **ClusterRoleBinding** 对象
- **Unmanaged:** 作业跳过删除且不做任何操作。
- **Managed:** 作业在日志中报告错误。这个状态不太可能发生，因为升级会被禁止。作业不执行其他操作。

在以后的 OpenShift Container Platform 发行版本中，Jobs 和 `openshift-service-catalog-removed` 命名空间将会被删除。



注意

OpenShift Container Platform 4.5 删除了所有红帽提供的服务代理 (service broker)。升级过程不会删除用户安装的其他代理。这是为了避免删除任何可能已使用代理部署的服务。用户必须手动删除这些代理。

1.4.2.4. CatalogSourceConfig 对象已删除

CatalogSourceConfig 对象现已删除。如需了解更多详细信息，请参阅 [OperatorSource](#) 和 [CatalogSourceConfig](#) 对象来阻止集群升级。

1.4.2.5. 从示例镜像流中删除的镜像

以下镜像不再包含在 OpenShift Container Platform 提供的样本镜像流中：

```
registry.redhat.io/dotnet/dotnet-30-rhel7:3.0
registry.redhat.io/dotnet/dotnet-30-runtime-rhel7:3.0
registry.redhat.io/openjdk/openjdk-11-rhel8:1.1
registry.redhat.io/rhoar-nodejs-tech-preview/rhoar-nodejs-10-webapp
registry.redhat.io/rhscl/mongodb-32-rhel7
registry.redhat.io/rhscl/python-35-rhel7
registry.redhat.io/rhdm-7/rhdm-decisioncentral-rhel8:7.5.1
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.5.0
registry.redhat.io/rhdm-7/rhdm-kieserver-rhel8:7.5.1
registry.redhat.io/rhdm-7-tech-preview/rhdm-optaweb-employee-rostering-rhel8:7.5.0
registry.redhat.io/rhdm-7-tech-preview/rhdm-optaweb-employee-rostering-rhel8:7.5.1
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.5.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-monitoring-rhel8:7.5.1
registry.redhat.io/rhpam-7/rhpam-businesscentral-rhel8:7.5.0
registry.redhat.io/rhpam-7/rhpam-businesscentral-rhel8:7.5.1
registry.redhat.io/rhpam-7/rhpam-kieserver-rhel8:7.5.0
registry.redhat.io/rhpam-7/rhpam-kieserver-rhel8:7.5.1
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.5.0
registry.redhat.io/rhpam-7/rhpam-smartrouter-rhel8:7.5.1
registry.redhat.io/rhscl/ruby-23-rhel7
```

1.4.2.6. 已删除 AWS EFS（技术预览）功能的外部置备程序

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

1.5. 程序错误修复

apiserver-auth

- 在以前的版本中，**oc login** 会执行 HTTP 请求来确定要用来连接到远程登录服务器的 CA 捆绑包。这会在每次尝试登陆时在 OAuth 服务器日志中产生一个 **remote error: tls: bad certificate** 错误，即使登陆是成功的。服务器证书链现在从不安全 TLS 握手中检索，因此正确的 CA 捆绑包会被选择，OAuth 服务器在登录尝试时不再记录证书错误。(BZ#1819688)
- 在以前的版本中，OAuth 服务器 pod 的不完整安全上下文可能会在 pod 获取可恢复默认行为的自定义安全上下文约束 (SCC) 时崩溃。OAuth 服务器 pod 的安全上下文被修改，自定义 SCC 不再阻止 OAuth 服务器 pod 运行。(BZ#1824800)
- 在以前的版本中，Cluster Authentication Operator 总是会为任何 OIDC 身份提供程序禁用质询身份验证流程，这意味着无法使用 **oc login** 进行登录。现在，当配置 OIDC 身份提供程序时，Cluster Authentication Operator 会检查是否允许资源所有者密码凭证授权。现在，您可以使用 **oc login** 在允许使用 Resource Owner Password Credentials 进行授权的 OIDC 身份提供程序中进行登陆。(BZ#1727983)

- 在以前的版本中，Cluster Authentication Operator 无法正确关闭到 OAuth 服务器的连接，从而导致 OAuth 服务器打开连接的增长速度大于关闭的速度。现在，连接可以被正确关闭，Cluster Authentication Operator 不会影响其自身有效负载的服务。(BZ#1826341)
- 在以前的版本中，如果配置期间连接到 kube-apiserver 时出错，oauth-proxy 容器会出错并退出。如果 kube-apiserver 和控制器不稳定或者速度较快，则会导致多次容器重启。现在，当 oauth-proxy 容器启动时，允许多次尝试对 kube-apiserver 执行检查，因此只有在底层基础架构真正有问题时，它才会失败。(BZ#1779388)

裸机硬件置备

- 因为在使用 IPv4 网络时，UEFI 引导过程会使用 ipxe.efi 二进制文件，所以引导过程会报告没有找到网络设备。因此，PXE 引导的机器将没有网络设备。现在，dnsmasq.conf 文件已被更新来为 IPv4 网络使用 snponly.efi 二进制文件。使用 PXE 启动的机器会使用 UEFI 网络驱动程序，因此它们会带有网络连接并可以被部署。(BZ#1830161)
- 如果集群在安装过程中有联网问题（例如，镜像下载速度过慢），则安装可能会失败。为了解决这个问题，已将 PXE 引导改为包括重新尝试，并为裸机置备程序与要置备的节点之间的通信增加网络最多重试次数。现在，安装程序可以处理网络较慢的情况。(BZ#1822763)

Build

- 在开始构建之前，OpenShift Container Platform 构建器会解析提供的 Dockerfile 并重新构建用于构建的修改版本。这个过程包括添加标签，并处理在 FROM 指令中命名镜像的替换。生成的 Dockerfile 并不能总是正确地重建 ENV 和 LABEL 指令，有时生成的 Dockerfile 会包含 = 字符，虽然原始的 Dockerfile 中没有包括它们。这会导致构建失败，并出现语法错误。现在，在生成修改的 Dockerfile 时使用了原始文件中的 ENV 和 LABEL 指令，从而解决了这个问题。(BZ#1821858)
- 在以前的版本中，当构建 pod init 容器出现故障时，最后几行错误日志没有被附加到构建中。因此，诊断 init 容器的构建错误（如不正确的 Git URL）会变得比较困难。现在，构建控制器已被更新，在 init 容器出现故障时错误日志会附加到构建中。现在，构建失败会比较容易进行诊断。(BZ#1809862)
- 在以前的版本中，由镜像导入失败或无效 Dockerfile 导致的构建失败仅归类为通用构建错误。要诊断这类错误，需要使用非默认的构建日志记录级别。现在，为失败的镜像导入和无效 Dockerfile 增加了新的故障原因。与失败镜像导入或无效 Dockerfile 相关的构建失败现在可在构建对象状态中识别。(BZ#1809861)
- 在以前的版本中，构建标签生成和验证不包括完整的 Kubernetes 验证例程。因为会创建了一个无效的构建标签值，具有特定有效构建配置名称的构建会失败。构建控制器和构建 API 服务器现在使用完整的 Kubernetes 验证例程，以确保添加的构建标签满足标签标准。具有任何有效构建配置名称的构建将生成有效的构建标签值。(BZ#1777337)
- 以前 Buildah 以文字形式解释 Dockerfile 中的变量，而不是解析变量中包含的值。因此，当 Dockerfile 包含变量时，构建将失败。Buildah 已被更新以可以正确处理 Dockerfile 变量。现在，Buildah 在构建容器镜像时将正确解析 Dockerfile 环境变量值。(BZ#1810174)
- OpenShift 4 禁用了 RunOnceDuration 准入插件，activeDeadlineSeconds 值不能被自动应用到构建 pods。将 activeDeadlineSeconds 设置为 nil 的 Pod 会与包含 NotTerminating 范围的资源配额匹配。之后，由于配额限制，构建 pod 无法在带有 NotTerminating 范围定义的资源配额的命名空间中启动。现在，构建控制器会为构建 pod 应用一个适当的默认 activeDeadlineSeconds 值。现在，构建 pod 可以在带有 NotTerminating 范围定义的资源配额的命名空间中启动。(BZ#1829447)

Cloud compute

- 集群自动扩展需要跨节点和机器对象的供应商 ID 完全匹配。在以前的版本中，如果机器配置中包含混合有大写和小写字母的资源组名称，集群自动扩展器将在十五分钟后终止机器，因为没有找到匹配项。现在资源组名称都会被处理，所有字符都为小写。现在，即使在使用大写和小写字母输入资源组名称时，也会正确地识别匹配的供应商 ID。(BZ#1837341)
- 在以前的版本中，当创建或更新机器集时，机器和机器集规格中的 **metadata** 字段不会被验证。无效的元数据会导致控制器无法处理对象。现在，当机器集被创建或更新时，**metadata** 字段会被验证，无效的条目会返回错误。现在，在创建机器集前可以识别无效的元数据，以防止后续的对象处理错误。(BZ#1702089)
- 有时在进行缩减操作时，机器集中的最后一台机器会包含删除注解。如果在删除前达到最小机器集，则自动扩展不会删除该机器。在以前的版本中，在缩减后不会删除最后一台机器的删除注解。这个问题已被修复，它改变了在缩减操纵后机器注解的取消标记的方式。现在，注解不再保留在机器集中的最后一台机器上。(BZ#1820410)
- 在以前的版本中，分配给 worker 节点的 AWS Identity and Access Management (IAM) 角色没有足够的权限访问 AWS Key Management Service (KMS) 密钥来解密挂载时的 Amazon Elastic Block Store (EBS) 卷。因此，Amazon Elastic Compute Cloud (EC2) 实例会被接受，但它们可能无法启动，因为它们无法从其根驱动器中读取。现在，可以授予 EC2 实例所需的权限，以便使用客户管理的密钥对 KMS 加密的 EBS 卷进行解密。现在，当使用客户管理的密钥加密 EBS 卷时，实例具有所需的权利来成功启动。(BZ#1815219)
- 机器集规格中的 **replicas** 字段可设置为 nil。在以前的版本中，如果自动扩展无法决定机器集中的副本数，将无法进行自动扩展操作。现在，如果没有设置 **replicas** 字段，自动扩展程序会根据机器集，观察到的最后副本数来决定缩放。现在，即使机器集规格中的 **replicas** 字段设置为 nil，自动扩展操作也可以进行，假设机器集控制器最近已同步到 **MachineSet.Status.Replicas** 的副本数。(BZ#1820654)
- 在以前的版本中，自动扩展 (autoscaler) 会在每次调用 **DeleteNodes** 时减少一个节点组的大小，即使现有节点删除还没有完成。这会导致集群的所需节点数量低于最低要求。现在，如果节点的机器已经有删除时间戳，节点组的大小不会被进一步缩小。这可防止自动扩展在调用 **DeleteNodes** 时将节点数减小到小于所需容量的情况发生。(BZ#1804738)

Cloud Credential Operator

- 当原始集群使用 OpenShift Container Platform 4.1 安装时，Cloud Credential Operator (CCO) 可能会导致崩溃。CCO 无法协调 **CredentialsRequest** 对象中的权限请求。在这个版本中更新了 CCO，不再假设 **Infrastructure** 字段中的这些部分是可用的。因此，CCO 现在可以与最初使用 OCP 4.1 安装的集群一起工作。(BZ#1813343)
- Cloud Credential Operator (CCO) 不再绕过安全上下文约束 (SCC)。在以前的版本中，CCO 运行所使用的权限会超过 CCO 执行其任务所需的权限。在这个版本中，不再有不必要的、CCO 绕过 SCC 限制的情况。(BZ#1806892)

Cluster Version Operator

- Cluster Version Operator (CVO) 有一个竞争条件，它会将一个超时更新协调周期视为成功更新。这只适用于受限网络集群，其中的 Operator 超时时会试图获取发行版本的签名。此程序错误导致 CVO 进入其 shuffled-manifest 协调模式，如果清单以组件无法处理的顺序被应用，则可能会破坏集群。CVO 现在把超时更新视为失败，因此在更新成功前不再会进入协调模式。(BZ#1843526)
- 只有在 CVO 日志中记录了更新期间推出部署的失败信息，且只有一般错误消息报告到 **ClusterVersion** 对象。这会在出现问题时，使用户和团队进行故障排除的难度增大，除非查看 CVO 日志。在这个版本中修正了这个问题，CVO 为 **ClusterVersion** 对象的推出提供了底层的错误信息。因此，在升级过程中对部署的推出进行故障排除会变得更加容易。(BZ#1768260)

控制台 Kubevirt 插件

- 在这个发行版本中，如果将虚拟机配置为使用无效或者不推荐的总线类型的磁盘，所创建的 VM 视图中的 **Disks** 选项卡会显示一个磁盘接口警告。(BZ#1803780)
- 在以前的版本中，所有 **DataVolume** 对象都归类为 VM 磁盘导入。这个不正确的分类会导致对于没有所有者引用虚拟机的 **DataVolume** 对象来说，**Activity** 卡会消失。在这个版本中，只有所有者引用虚拟机的 **DataVolume** 对象被归类为 VM 磁盘导入，对于没有所有者引用虚拟机的 **DataVolume** 对象不会丢失 **Activity** 卡。(BZ#1815138)
- 在以前的版本中，当删除虚拟机磁盘时，**DataVolume** 对象及其关联的持久性卷声明 (PVC) 不会被删除。这些对象只有在虚拟机被删除时才被删除，因此没有在删除虚拟机的过程中保留 **DataVolume** 对象的选项。在这个发行版本中，用户可以在删除虚拟机磁盘或虚拟机时选择保留或删除 **DataVolume** 对象和 PVC。这不适用于使用 CD-ROM 模态删除的磁盘。(BZ#1820192)
- 在以前的版本中，清单中的磁盘数量与磁盘列表中的磁盘数量不匹配。现在，清单视图已被更新，以分别单独显示 CD-ROM 和磁盘。(BZ#1803677)
- 在以前的版本中，无法使用 VM 向导使用的默认 YAML 创建虚拟机，因为默认的 YAML 虚拟机模板不包含 VM 向导所需的值。在本发行版本中，默认的 YAML 虚拟机模板包含所有需要的值。(BZ#1793962)
- 以前，web 控制台会错误地把一个失败的虚拟机迁移报告为成功。现在，在迁移虚拟机时，如果迁移失败，web 控制台可以正确地报告。(BZ#1806974)
- 在以前的版本中，VM 向导不会以正确格式生成 **cloud-init** 配置，因此不会在虚拟机中应用它。在这个版本中，向导生成的格式已被修正，VM 向导中提供的 **cloud-init** 配置会应用到虚拟机。(BZ#1821024)
- 在以前的版本中，VM 模板中的差错没有反映在虚拟机向导创建的最终虚拟机中，这会导致在创建虚拟机后 vCPU 的数量会被加倍。在这个发行版本中，创建虚拟机时会反映虚拟机模板中的插槽、内核和线程数量，其显示的 vCPU 数量是正确的。(BZ#1810372)
- VM 模板列表的 URL 更改导致用户在删除虚拟机模板后被重定向到错误页面。这个版本里已经修复了 URL。(BZ#1810379)
- 在以前的版本中，当删除运行的虚拟机时，相关的 VMI 会出现在虚拟机列表中，状态为 **VM error**。在这个版本中，已删除相关虚拟机的已过时的 VMI 不再被列出。(BZ#1803666)
- 在以前的版本中，磁盘导入只会预期 VM 导入的资源。因此，来自于 VM 模板或 VMI 的导入活动的 VM 资源链接会指向一个不存在的虚拟机。在这个版本中，导入过程可以识别来自 VM 模板和 VMI 的导入资源，相关链接会指向正确的资源。(BZ#1840661)
- 在本发行版本中，VM 磁盘导入过程不再报告值为 **NaN%** 的进程。(BZ#1836801)
- 在以前的版本中，虚拟机向导使用 **virtIO** 作为 VM root 磁盘的默认接口，而不是使用通用模板中指定的接口。但是 **virtIO** 并不适用于所有操作系统。在这个版本中，会根据使用的通用模板来为操作系统选择正确的默认接口。(BZ#1803132)

控制台 Metal3 插件

- 在以前的版本中，web 控制台中的 **Powering on/off** 信息和裸机主机链接之间没有空格。现在，添加了一个空格以使信息可以更好地读取。(BZ#1819614)
- 在以前的版本中，对于裸机安装，当有些节点不可用时，**Bare Metal Host Details** 页将无法加载。现在，**Bare Metal Host Details** 页会被改为 0 个 pod。(BZ#1827490)

Web 控制台 (开发者视角)

- 在以前的版本中，**Topology** 视图中无法查看与 Knative 服务关联的 pod 或资源列表。在这个版本中，当选择 Knative 服务时，侧边栏会显示一个 pod 列表以及一个链接来查看日志。[\(BZ#1801752\)](#)
- 当使用 **Monitoring** 界面中的 **metrics** 标签页中的 PromQL 编辑器编辑一个存在的查询时，鼠标光标会移到行的最后。在这个版本中，PromQL 编辑器可以正常工作。[\(BZ#1806114\)](#)
- 对于 Knative 镜像，在 **Add → From Git** 选项中，**Routing** 的 **Advanced Options** 不提供预先获取的容器端口选项。另外，如果创建了没有更新默认端口值 **8080** 的服务，则修订不会显示。在这个版本中，如果需要使用另外一个端口，用户可以使用下拉列表从可用的端口选项中选择或手工输入。修订版本会如预期显示。[\(BZ#1806552\)](#)
- 在以前的版本中，使用 CLI 创建的 Knative 服务无法使用控制台进行编辑，因为无法获取镜像。现在，如果编辑时未找到关联的镜像流，则会使用用户在 YAML 文件中为容器镜像提供的值。这允许用户使用控制台编辑服务，即使服务是使用 CLI 创建的。[\(BZ#1806994\)](#)
- 在 **Topology** 视图中，为 Knative 服务编辑在外部镜像 registry 中的镜像名不会创建新的修订版本。在这个版本中，当服务名称改变时会创建一个新的服务修订版本。[\(BZ#1807868\)](#)
- 当使用 **Add → Container Image** 选项，然后从内部 registry 选项中选择 **Image stream** 标签时，**ImageStreams** 下拉列表不会列出从 **OpenShift** 命名空间部署镜像的选项。但是，您可以通过 CLI 访问它们。在这个版本中，所有用户可通过控制台和 CLI 访问 **OpenShift** 命名空间中的镜像。[\(BZ#1822112\)](#)
- 以前，在 **Pipeline Builder** 中，当编辑了一个引用没有存在的任务的管道时，整个屏幕将变为白色。在这个版本中，会显示一个图标表示需要一个操作，并显示下拉列表来方便地更新任务引用。[\(BZ#1839883\)](#)
- 在 **Pipelines Details** 页中，当修改了 **Parameters** 和 **Resources** 标签页中存在的项时，即使新的变化被检测到，**Save** 按钮也会被禁用。现在修改了验证标准，**Save** 按钮可以正常使用来提交更改。[\(BZ#1804852\)](#)
- 在 **Add → From Git** 选项中，如果选择了 **Deployment** 或 **Knative Services** 资源选项，则由 OpenShift Pipelines Operator 提供的 Pipeline 模板将失败。这个版本添加了对使用资源类型和运行时来确定 Pipeline 模板的支持，从而可以提供特定于资源的 Pipeline 模板。[\(BZ#1796185\)](#)
- 当使用 **Pipeline Builder** 创建 Pipeline，并且使用了类型数组的 Task 参数时，Pipeline 不会启动。在这个版本中，支持数组和字符串类型参数。[\(BZ#1813707\)](#)
- 在 **Topology** 视图中，当命名空间具有 Operator 支持的服务时，应用程序过滤节点会返回一个错误。此程序错误修复添加了根据所选应用程序组过滤 Operator 支持的服务节点的逻辑。[\(BZ#1810532\)](#)
- **Developer Catalog** 直到选择了 **Clear All Filters** 选项后才会显示目录结果。在这个版本中，所有目录项都会默认显示，您不需要清除所有过滤器。[\(BZ#1835548\)](#)
- 在以前的版本中，用户无法为 **knative** 服务添加环境变量。因此，需要 **envVariables** 的应用程序可能无法正常工作。现在，增加了对环境变量的支持。[\(BZ#1839114\)](#)
- **Developer Console Navigation** 菜单现在可用，并与最新的 UX 设计一致。[\(BZ#1801278\)](#)
- 在开发者视角的 **Monitoring** dashboard 标签页里添加了 **Time Range** 和 **Refresh Interval** 下拉菜单。[\(BZ#1807210\)](#)
- 虽然 **Start Pipeline** 模式需要，但在命名空间中不会创建 Pipeline 资源。用户会看到上面的字段

上禁用且为空的下拉菜单，从而无法了解与这些字段相关的上下文。在这个版本中，**Create Pipeline Resource** 在 **Start Pipeline** 模式中提供了相关的上下文信息。现在，当命名空间中没有创建的 Pipeline 资源时，用户从启动模式中启动 Pipeline 也会有很好的体验。(BZ#1826526)

- 标题会与 **Close** 按钮重叠。如果与 **Close** 按钮重叠，则很难点击。现在，这个问题已解决，标题不会和 **Close** 按钮重叠。(BZ#1796516)
- Pipeline Builder 错误地认为空字符串 ("") 代表没有默认值。一些由 Operator 提供的任务需要空字符串作为默认值，所有可能无法正常工作。检查默认属性，且不假定值的有效性。现在，OpenShift Pipeline Operator 确认为有效默认值的任何值都会被遵守。(BZ#1829567)
- Pipeline Builder 会读取 **Task/ClusterTask** 定义，并错误地假设所有参数都是字符串类型。当遇到类型为数组的 **Task** 参数时，它会将数组转换为字符串，从而丢失了它的原始类型。它会以字符串形式为 **Task** 参数生成一个值，从而破坏与 **Task** 对象的合约。现在，web 控制台中支持数组类型，它会被正确处理。管理这两个类型可让 Pipeline Builder 按预期工作。(BZ#1813707)
- Pipeline 页面与其他页面不一致。**Create Pipeline** 按钮总是被启用，而没有考虑没有项目的情况。现在，当启用 Getting Started 指南时，**Create Pipeline** 按钮将不会出现。(BZ#1792693)
- 对 **Dashboard & Metrics** 标签页的指标查询在设计文档中被更新。就查询而言，代码需要同步。现在，查询已被更新，指标查询的顺序及其标签与设计同步。(BZ#1806518)
- tile description 变量被错误地设置为 CRD 描述附加上 CSV 描述。这会导致标题描述错误。标题描述现在回退到原始值，以前附加的值被移到自己的变量中。(BZ#1814639)
- **eventSources** API Group 被更新到最新支持的 API Group **sources.knative.dev**。在这个版本中，允许由新的 API Group 生成的源在 web 控制台的 **Topology** 视图中被识别。(BZ#1836805)
- 自 Red Hat OpenShift Serverless 1 Serverless Operator 版本 1.7.1 发行版本中，Operator 已正式发布。web 控制台的 **Developer** 视角中的技术预览徽标已被删除。(BZ#1827042)

DNS

- 在以前的版本中，CoreDNS 指标可以通过集群中的不安全频道公开。现在，正确的 TLS 组件和 **kube-rbac-proxy sidecar** 已被添加来保护 CoreDNS 指标端点，并通过安全频道提供 CoreDNS 指标。(BZ#1809197)
- 在以前的版本中，将任意的污点添加到节点可能会导致与 DNS Operator 操作数相关的问题。现在，DNS 操作对象可以容忍添加到节点的任何污点。这个操作对象在所有 Linux 节点主机上运行并更新 **/etc/hosts**。当操作对象在仍然进行初始化的节点上启动时，可能会出现 **Missing CNI default network** 事件，但这种错误是瞬时的并可被忽略。(BZ#1813479)
- 在以前的版本中，需要依赖 master 节点的特定 DNS 名称。现在，所有有效的主机名都可用于 master 节点。(BZ#1807234)
- 在以前的版本中，当 **dnses.operator.openshift.io/default** 对象存在，其对应的守护进程集不可用时，**clusteroperators/dns** 会报告 **Available** 条件并带有不正确的 **NoDNS** 原因和 **No DNS resource exists** 信息。现在，在这种情况下会显示正确的原因和信息。(BZ#1835725)

etcd

- 在以前的版本中，etcd peer 证书不包括 IPv6 localhost 地址，无法连接到 **https://[::1]:2379** 信息。现在这个问题已被修复，它包括了 **::1** 作为对等证书中的一个主机。现在不再显示使用 **https://[::1]:2379** 的重复失败尝试的连接。(BZ#1810997)
- 在以前的版本中，CVO 每 10 分钟会覆盖配置映射中的证书。这会导致大量运行成本，并会影响集群的性能和稳定性。现在，证书只在配置映射中创建一次以提高性能和稳定性。(BZ#1819472)

- 在以前的版本中，集群 etcd Operator 健康状态报告不容易理解。这是因为日志消息构建不正确，对集群状态造成不确定的问题。这可以通过在独立函数中正确地分析 Operator 状态来建立正确的日志消息和 etcd 状态的事件来解决这个问题。现在，所有 master 节点上的 etcd pod 的状态更为明确。(BZ#1821286)
- 在以前的版本中，TLS 证书被错误地签名了十年，而文档中说它们被签名三年。现在，证书只会签名三年。(BZ#1837594)
- gRPC-go 1.23.0 有客户端负载均衡器的错误。这个错误可能会导致死锁。gRPC-go 已经升级到了 1.23.1 版，在此版本中修复了这个错误。(BZ#1823993)
- 停止所有 pod 后，恢复过程只能重启 **etcd**、**api-server**、**api-scheduler** 和 **controller-manager**。它没有重启网络 pod。因此，kubelet 无法进行通讯，裸机集群无法工作。现在，恢复服务不再停止它无法重启的 pod。集群在恢复过程运行后可以工作进行。(BZ#1835146)

Etcd Operator

- 在以前的版本中，etcd spec 中缺少属性，导致 **oc explain etcd** 命令错误地列出从 spec 引用的属性。相关的 CRD 已更新，以描述缺失的属性。现在，**oc explain etcd** 命令可以完全描述 etcd 的属性。(BZ#1809282)
- Etcd Operator 在执行不正确的健康检查时，导致事件报告不正确，并会误导日志消息。现在，通过改进的消息，可以正确地检测到健康状况，从而提供准确的健康状况。(BZ#1832986)

Image

- 以前，只有在 registry 被设置为 **managed** 时才会创建 Nodeca 守护进程。删除 registry 时，不会创建 Nodeca 守护进程。在这个版本中，Nodeca 守护进程总是被创建，即使 registry 已被删除也会创建 Nodeca 守护进程。(BZ#1807471)

镜像 registry

- 以前，如果在没有正确存储配置的情况下删除 registry 配置，因为缺少存储配置资源永远不会最终完成，Operator 无法删除存储，因为它不知道该存储。此程序错误修复使得存储配置是可选的，这样就可以完全完成资源。(BZ#1798618)
- 以前，Image Registry Operator 不会在 Image Registry 创建的资源上设置 **nodeSelector** 标签。这可能会导致以后的问题，因为没有指定可以运行哪些节点资源，并最终在不支持的平台上运行 registry。在这个版本中，为创建的资源添加了缺少的标签。现在，您可在创建的资源上看到该标签。(BZ#1809005)
- 以前，将镜像推送到不存在的命名空间会导致 Image Registry 返回一个 **500** 错误代码。在这个版本中修正了这个错误，现在返回的代码明确表明缺少权限的问题。现在，当将镜像推送到不存在的命名空间时，会返回一个权限拒绝的错误。(BZ#1804160)
- Azure 基础架构名称用于生成的 Azure 容器和存储帐户。因此，如果 Azure 基础架构名称包含大写字母，则容器会成功创建，但存储帐户创建会失败。在这个版本中，调整了容器名称创建逻辑，以丢弃无效字符，允许镜像 registry 在名称中包含无效字符的基础架构上部署。(BZ#1827807)
- 当删除使用 GCP 存储的非空镜像 registry 时，镜像重配置主机名不会从镜像配置文件中删除。这导致您无法创建新的镜像 registry。现在相关代码已修改，在删除镜像 registry 时从镜像配置文件中删除镜像 registry 主机名。因此，您可以正确删除并创建镜像 registry。(BZ#1827075)
- 由于镜像 registry 在删除存储桶前没有从存储桶中删除对象，所以无法删除带有镜像的存储桶。现在，代码已修改，在删除存储桶前会删除镜像。您可以如预期删除非空存储桶。(BZ#1827075)

- 因为镜像 registry 中的镜像没有清除其 yum 缓存，所以镜像的大小会较大。镜像 registry **Dockerfile** 被修改为包含 **yum clean all** 命令。镜像的大小会较小。(BZ#1804493)
- 镜像修剪自定义资源中的 **keepYoungerThan** 参数使用纳秒，且无法配置为使用较长的时间。纳秒并不适合于镜像修剪器。在镜像修剪自定义资源中添加新参数，**keepYoungerThanDuration** 替换并覆盖 **keepYoungerThan** 参数。(BZ#1835004)
- 当用户将 Operator 更改为 **Removed** 状态时，Image Registry Operator 没有正确清理存储状态。因此，当用户将 Operator 改回为 **Managed** 时，Operator 无法创建新的存储 pod。Operator 被修改来正确清理存储状态，Operator 可以创建新的存储 pod。(BZ#1785534)
- 因为 Image Registry Operator 没有清理日志，所以您可能会在日志中看到不正确的消息。代码已被修改来清理日志，以删除这些不正确的信息。现在，日志会显示正确的信息。(BZ#1797840)
- 因为默认 Image Registry Operator 被配置为有 0 个副本，所以可能会出现这个问题，除非手动更改了值。Operator 已更新为使用一个安装。(BZ#1811846)
- 特定命名空间无法使用在集群安装过程中使用的 registry 凭证，用户需要创建新凭证的。相关代码已被修改，如果在安装过程中提供了 registry 的凭证，用户就可以使用这些凭证导入镜像。(BZ#1816534)
- 因为 Image Registry Operator 只安装一个 pod，所以它不满足要求。Operator 现安装两个 pod 以实现高可用性。(BZ#1810317)

安装程序

- 在 Azure 平台上，需要 **cifs-utils** 软件包来为 pod 创建卷挂载。在这个版本中，在安装 OpenShift Container Platform 时，**cifs-utils** 会被包括在为 RHEL 7 主机安装的软件包中。(BZ#1827982)
- 当从已过期的 control plane 证书中恢复时，集群无法通过端口 7443 连接到恢复 API 服务器。这是因为恢复 API 服务器的端口与 OpenStack、oVirt、裸机和 vSphere 使用的 HAProxy 端口冲突。这会导致 **Unable to connect to the server: x509: certificate signed by unknown authority** 错误。现在，HAProxy 侦听端口 9443，允许恢复 API 服务器使用端口 7443 处理已过期 control plane 证书的恢复过程。(BZ#1821720)
- 在以前的版本中，RHOSP 安装程序使用 **remote_group_id** 创建安全组来允许流量来源。在安全规则中使用 **remote_group_id** 是非常低效的，它会使 OVS 代理触发大量的计算来生成流量。这个过程有时会超过为生成流量分配的时间。在这种情况下，特别是已经处于压力状况的环境中，master 节点可能无法与 worker 节点进行通信，从而导致部署失败。现在，使用白名单流量来源的 IP 前缀，而不再使用 **remote_group_id**。这会减少 Neutron 资源中的负载，从而减少超时问题的发生。(BZ#1825286)
- 在以前的版本中，安装程序要求用户手动创建虚拟机模板，然后才能在 Red Hat Virtualization (RHV) 上创建 OpenShift Container Platform 集群。这是因为安装程序没有满足 RHV 版本 4.3.9 中的以下要求：
 - 安装程序必须把 ignition 传递给虚拟机。
 - 模板必须将其 OS 类型指定为 Red Hat CoreOS (RHCOS)。

安装程序现在会创建一个模板，该模板将 RHCOS 指定为 OS 类型，并将 ignition 传递给虚拟机。用户不再需要创建虚拟机模板。(BZ#1821151)

- 在以前的版本中，Keepalive 进程（用于在裸机安装程序置备的基础架构集群中为 API-VIP 和 INGRESS-VIP 地址提供故障切换功能）会使用用来监控本地组件状态以确定哪些节点应拥有 VIP 的脚本中的一个 IPv4 本地地址，即使它使用 IPv6 部署。因此，在 IPv6 部署中，Keepalived 有

时会收到不正确的组件状态。现在，Keepalived 脚本使用 localhost，它会在 V4 部署中解析为 127.0.0.1，在 V6 部署中解析为 ::1。因此，它总是使用正确的本地 IP 地址。(BZ#1800969)

- 在以前的版本中，在使用安装程序置备的基础架构的裸机集群中，VIP 有时不会切换到具有健康负载均衡器的 control plane 机器中。因此，control plane 机器仍然拥有 API-VIP IP 地址，即使本地负载均衡器不健康，OpenShift Container Platform API 会有大约 10 秒无法访问。现在，API-VIP 脚本的 Keepalived 检查也会监控自承载的负载均衡器健康状况，API-VIP 会切换到具有正常工作的负载均衡器的 control plane 节点，并防止 OpenShift Container Platform API 的服务出现无法工作的情况。(BZ#1835974)
- 在以前的版本中，安装程序没有显式检查 **machineCIDR** 和 **provisioningNetworkCIDR** 范围之间的重叠。因此，当网络范围重叠时的错误信息不明确。现在，安装程序会显式地检查这些网络范围间的重叠，并在有重叠时给出一个清晰的错误信息。(BZ#1813422)
- 因为 control plane 中的 Operator 可在 bootstrap 过程完成前启动，裸机置备基础架构可能同时在 bootstrap 和 control plane 上活跃。在以前的版本中，在这两个系统中都可能会置备计算机器，机器并不都使用相同的基础架构。现在，bootstrap 置备基础架构只置备 control plane 机器，因此两个置备基础架构可以同时在线。(BZ#1800746)
- 在以前的版本中，当阻止到 IPv6 bootstrap 节点的 DHCP 流量时，使用了错误的端口号。因此，有时当 control plane 机器错误地从 bootstrap 节点获取 DHCP 租期时会出现竞争条件。现在，在阻止 DHCPv6 时使用了正确地端口，control plane 机器只能从集群中运行的裸机基础架构中置备 (BZ#1809691)
- 在以前的版本中，如果一个使用安装程序置备的基础架构的裸机集群，使用 VRRP 管理 OpenShift Container Platform 集群的虚拟 IP 地址意味着，如果运行多个集群，虚拟路由器 ID 可能已在广播域中使用。因此，节点可能会被分配已在使用中的虚拟 IP 地址。现在，在部署集群前，可以使用一个工具来检查哪个虚拟路由器 ID 将用于所选集群名称。(BZ#1821667)
- OpenShift Container Platform 版本 4.1 集群没有使用 **infrastructure.status.infraPlatform** 参数。因此，Operator 必须检查并使用最初在版本 4.1 中安装的集群的旧字段，这会在升级过程中出现错误。现在，迁移控制器通过使用集群中可用的信息，在升级过程中为所有集群设置新字段。因此 Operator 可使用所有新参数，并减少升级错误。(BZ#1814332)
- 由于用于为集群获取资源的 AWS API 对以前删除资源的响应非常慢，因此如果尝试多次销毁集群，则会因为尝试删除已删除的托管区而导致失败。因此，destroy 命令会一直执行循环，直到 AWS API 从其响应中删除了托管区。现在，安装程序会跳过托管区的 **notfound** 错误，destroy 命令可以更快地完成。(BZ#1817201)
- 在以前的版本中，bootstrap 服务器端点使用 **api** 端点，它会经过外部负载均衡器。因此，需要打开另一个端口来向集群添加 RHEL 节点。现在，bootstrap 服务器端点使用内部的 **api-int** 端点，您不再需要在外部负载均衡器上打开另一个端口。(BZ#1792822)
- 在以前的版本中，对于裸机集群，为了支持节点 DNS 解析，节点的 **/etc/resolv.conf** 文件通过将节点的 control plane IP 地址添加到节点的 **/etc/resolv.conf** 文件前来指向基础架构 CoreDNS 的本地实例。因此，当一个主机已有三个域名解析服务器在 **/etc/resolv.conf** 文件中列出时，pod 会生成一个 "nameserver limits was exceeded" 警报。现在，只有前三个域名解析服务器会包括在 **/etc/resolv.conf** 文件中，因此 pod 不再生成警报。(BZ#1825909)
- 在以前的版本中，运行的 ironic 容器中没有 **ipxe.efi** 文件，因此在需要 **ipxe.efi** 时引导 UEFI 会失败。现在，**ipxe.efi** 文件在运行时被复制到 **/shared** 目录中，因此 UEFI 引导不再受到影响。(BZ#1810071)
- 在以前的版本中，AWS 对速率的限制有时会导致无法为集群创建记录。现在，安装程序允许较长的等待超时，从而会减少因为速率限制而失败的问题。(BZ#1766691)

- 在以前的版本中，AWS 对速率的限制有时会导致集群无法获取区域，这会阻止集群安装。现在，安装程序允许较长的等待超时，从而会减少因为速率限制而失败的问题。(BZ#1779312)
- 在以前的版本中，安装程序在决定到配置文件的相对路径时不会检查符号链接。因此如果安装程序从符号链接中运行时安装程序会失败。现在，安装程序会检查符号链接。您可以从符号链接的目录中运行安装程序。(BZ#1767066)
- 在以前的版本中，安装程序使用的 AWS Terraform 供应商偶尔会导致 S3 存储桶的竞争条件，集群安装会失败，并显示以下错误：

```
When applying changes to module.bootstrap.aws_s3_bucket.ignition, provider level=error
msg="aws\ produced an unexpected new value for was present, but now absent.
```

现在，安装程序使用不同的 AWS Terraform 供应商代码，该代码现在可以更好地处理 S3，安装程序置备的 AWS 集群安装不会因为这个错误而失败。(BZ#1745196)

- 在以前的版本中，CoreDNS 转发插件默认使用随机服务器选择策略。因此，如果有多个外部 DNS 解析器，集群将无法解析 OpenStack API 主机名。该插件现在按照提供地顺序使用 DNS 服务器。(BZ#1809611)
- 由于安装 OpenShift Container Platform 的 RHOSP 云的性能不同，安装时间会有所不同。因此，安装程序可以在安装成功前超时。作为临时解决方案，在安装程序显示失败时检查集群状态。集群可能处于健康状态。(BZ#1819746)
- 在 RHOSP 中，control plane 和计算节点将 IP 地址注入 `/etc/resolv.conf` 文件作为首选名称解析服务器。因此，在文件中已有三个名称解析服务器的主机生成了名称解析限制警告。现在，只有 `/etc/resolv.conf` 文件中的前三个命名服务器会被保留。因此，pod 不再生成名称解析服务器警告。(BZ#1791008)
- 在以前的版本中，没有中继端口的 RHOSP 云可能会返回一个错误，安装程序错误会把它错误地解析为失败。因此，在超时前集群销毁操纵会被循环执行。在这个版本中，安装程序可以正确地解释错误，允许在不支持中继端口的云中成功进行集群销毁。(BZ#1814593)
- 不能删除共享名称的 RHOSP 资源。在以前的版本中，如果共享名称的安全组存在，使用 Ansible playbook 的集群销毁操纵会在 RHOSP 云上失败。现在，在销毁集群时，`down-security-groups.yaml` playbook 使用组 ID 而不是名称。如果 playbook 成功完成，则所有安全组都会被删除。(BZ#1841072)
- 有些 RHOSP 环境可能会强制实施一个策略来禁止虚拟机使用临时磁盘引导。因此，当 bootstrap 机器试图从临时磁盘引导时，集群安装会失败。现在，bootstrap 机器会遵循 control plane 机器池的 `rootVolume` 设置，允许集群在禁止使用临时磁盘引导的环境中安装成功。(BZ#1820434)
- 在以前的版本中，当浮动 IP 地址 (FIP) 在与 RHOSP 上运行的集群关联之前，并不总会执行一个需要的 Terraform 步骤。因此，可能会出现导致安装失败的竞争条件。现在，Terraform 步骤总会在 FIP 关联之前进行。(BZ#1846297)
- 因为一个 RHOSP 用户置备的安装脚本与某些 Ansible 版本不兼容，安装可能会失败。这个脚本已被更新以保证更广泛的兼容性。现在，无论您的 Ansible 版本是什么，安装都可以成功。(BZ#1810916)
- 目前，RHOSP 用户置备的基础架构 playbook 不会删除在集群生命周期中创建的 Cinder 卷。因此，销毁的集群可能会泄漏 Cinder 卷的内容。作为临时解决方案，在销毁集群后手动删除 Cinder 卷。(BZ#1814651)
- 在以前的版本中，RHOSP 上的集群不会处理在证书认证机构 (CA) 文件捆绑包中传递给它的所有证书。因此，无法使用非默认信任授权签名的中间证书安装集群。CA 文件现在被分割并单独处理，允许使用非默认可信机构签名的中间证书的安装。(BZ#1809780)

kube-apiserver

- 在以前的版本中，因为上游程序错误导致混合使用 Kubernetes 1.14 和 1.16 组件的集群无法运行，这会使一些用户无法从 4.2 升级到 4.3。在这个版本中包括了一个来自上游的代码合并。现在，在升级时 OpenShift Container Platform 4.3 与 OpenShift Container Platform 4.2 兼容。[\(BZ#1816302\)](#)
- 在以前的版本中，当创建一个 Operator 的新版本时，可能需要几分钟锁定才可以被被释，Operator 的新版本才可以继续运行。这是因为领导选举设置在 Operator 收到 UNIX 的关闭信号时没有释放锁定。在这个版本中，Operator 推出部署时间有很大改进。因为 control plane Operator 现在要遵守恰当终止期限，且无需在启动前等待锁定被释放。[\(BZ#1775224\)](#)
- 在以前的升级过程中，OpenShift Container Platform API 服务器有时会添加回 GCP 负载均衡器中，尽管因为节点上的路由被错误配置还无法提供流量服务。这是因为在节点和 GCP 负载均衡器间的一个竞争条件所致。这可以通过将路由配置移至 iptables 并区分本地和非本地流量来解决。现在非本地流量总是可以被接受。现在，在 API 服务器升级过程中，连接可以安全地被终止，新的连接只会在运行 API 服务器时进行负载均衡。[\(BZ#1802534\)](#)

kube-scheduler

- 在以前的版本中，位于特定节点中的可驱逐的 pod 可能不会被驱逐。这是因为 Descheduler 会在检查节点是否可以被驱逐的循环代码中错误地提早退出，如果 pod 在 **NodeAffinity** 策略中是可驱逐的。现在，节点检查循环的 break 条件已被修复，在检查是否可驱逐时会考虑所有节点。[\(BZ#1820253\)](#)

日志记录

- 在以前的版本中，Fluentd 缓冲队列没有限制，如果传入了大量日志可能会破坏节点的文件系统，并导致节点崩溃。因此，应用程序会被重新调度。为防止这个问题，现在 Fluentd 缓冲队列限制了每个输出的固定块数量（默认值为 **32**）。[\(BZ#1780698\)](#)
- 在 IPv6 裸机部署中，Elasticsearch 被绑定到 IPv4 回送地址上，而不是集群的 IPv6 地址。因此，Elasticsearch 集群启动会失败。下游 API 被改变来为 Elasticsearch 设置绑定并发布主机。Elasticsearch 可以绑定到网络接口，并按预期启动。[\(BZ#1811867\)](#)
- 由于集群日志记录型服务版本（CSV）使用不正确的路径获取一些集群日志记录组件的状态，所以不会报告这个状态。因此，集群日志记录无法正常工作。现在，路径已被修正，集群日志记录可根据预期工作。[\(BZ#1840888\)](#)
- 因为当配置了 3 个以上的 Elasticsearch 节点时，Elasticsearch Operator 会创建第二个部署，所以 Cluster Logging Operator 没有读取正确的 Elasticsearch 节点数量。因此，集群日志记录自定义资源总是报告与一个部署关联的节点数。Cluster Logging Operator 被更改为可重复计算 Elasticsearch 节点的数量。[\(BZ#1732698\)](#)

Machine Config Operator

- Worker 节点上有多个可用网络使得在 control plane 上为 CRI-O 选择一个地址变得困难。这会导致 CRI-O 经常绑定到非 control plane 接口。在这个版本中，更新了 CRI-O systemd 服务，它依赖于一个可以正确选择接口并配置 CRI-O 服务的服务。因此，CRI-O 会如预期绑定到一个 control plane 中的地址。[\(BZ#1808018\)](#)
- 在以前的版本中，当在 IPv6 裸机部署中为受限网络配置 OperatorHub 时，多个接口可能会出现 OpenShift Container Platform（OCP），而没有由 DHCP 提供的名称，也不会反向解析域名。这会导致多播 DNS 发布服务以默认的 **localhost** 名称开头。在这个版本中，确保 Machine Config Operator 只配置非默认名称并等待那些名称可用。因此，正确的主机名会发布到多播 DNS。[\(BZ#1810333\)](#)

- Ingress Virtual IP 管理配置在其密码中使用固定字符串。如果有两个 VRRP keepalived 实例分别位于不同的集群中，它们具有相同的 Virtual Router ID，则它们将有相同的密码，并可能属于同一个虚拟路由器。在这个版本中，密码会根据集群的配置进行改变。因此，不同的集群 Ingress Virtual IP 现在有不同的密码。(BZ#1803232)
- 在以前的版本中，在配置任何 control plane IP 地址前，会运行 systemd 服务为 control plane IP 检测并配置 Kubelet 和 CRI-O。这会产生 Kubelet 和 CRI-O 失败的信息 (**nodeip-configuration 'Failed to find suitable node ip'**)。现在，系统会重试直到接口配置了 control plane IP。(BZ#1819484)
- 在以前的版本中，当 CoreDNS 可将 DNS 请求转发到 **/etc/resolv.conf** 文件中的服务器列表时，如果文件被改变，则变化不会反映在 CoreDNS Corefile 中。在这个版本中，CoreDNS-monitor pod 会验证 CoreDNS 转发列表是否与 **/etc/resolv.conf** 同步，从而使服务器列表出现在文件中。(BZ#1790819)
- 在以前的版本中，当 keepalived 使用的接口是桥接的时，用户可能会动态将接口放置在绑定或桥接中，这可能会阻止 keepalived 恢复操作，从而破坏虚拟 IP 管理。在这个版本中，监控器接口会更改并重新载入 keepalived，因此它会读取新的配置，虚拟 IP 管理受的影响很小。(BZ#1751978)
- 因为有些路由包含 **expires** 字段，所以 IPv6 (**non_virtual_ip** 脚本) 无法处理路由。因此，需要使用 **non_virtual_ip** 配置的服务会失败。现在，**non_virtual_ip** 脚本已更新。路由可以被解析，服务会被正确配置。(BZ#1817236)

Web 控制台 (管理员视角)

- 在启动控制台时，因为监控指标查询页面中缺少 Prometheus 链接，会设置无效的监控标记。现在，设置了正确的标记，Prometheus 监控可以在指标查询页面中找到。(BZ#1811481)
- 当用户试图安装到不支持的命名空间时，不会提交该表单，因为用户不知道哪个安装模式受 Operator 组支持。现在，添加了一个提示信息以提供支持的 Operator 的安装模式。该提示信息明确说明了所选命名空间可以被安装 Operator 使用的原因。(BZ#1821407)
- **Machine Health Check** 和 **Machine Config** 在显示中没有被适当隔开，从而给用户造成混乱。现在，**Machine Health check** 和 **Machine Config** 被明显分隔。(BZ#1817879)
- 在浏览器的控制台中因为缺少了响应组件的属性而会出现错误信息。现在，这个属性已为响应组件添加，不会再出现错误信息。(BZ#1800769)
- 多个警报接收器可以使用相同的名称创建。如果删除了使用同一个名称的多个警报中的一个，它们都将被删除。现在，在 **Create Receiver** 表单中，如果名称已存在，用户会被提示显示出错信息，同时 **Create** 按钮会被禁用。用户不能创建两个具有相同名称的接收方。(BZ#1805133)
- PVC 过去按字母顺序排序，现在按数字排序。(BZ#1806875)
- 以前，服务按字母顺序列出，因此 **oc** 不是第一个选项。现在，**oc** 选项会被附加到列表的前面。(BZ#1802429)
- 警报变为静默状态后，**Status** 卡和 notification drawer 将继续显示静默的警报。现在，仪表板和 notification drawer 不会显示静默的警报。(BZ#1802034)
- 警报变为静默状态后，**Status** 卡和 notification drawer 将继续显示静默的警报。现在，仪表板和 notification drawer 不会显示静默的警报。(BZ#1808059)
- 排序不是基于该列中的数据，从而导致错误的排序。现在，数据根据正确的操作状态值进行排序。(BZ#1812076)

- 状态描述符可能比 donut chart 中为其分配的空间要长。状态描述符可能比较长，影响到用户看到实际的值。现在，状态描述符在 donut chart 的下面，因此可以根据需要换行，从而使每行可以有多个状态描述符。较长的状态描述符现在完全可见，在查看状态描述符时减少了对页面进行滚动的情况。(BZ#1823870)
- 当版本没有出现在更新频道中时，web 控制台会显示一个不准确的 **Error Retrieving** 更新状态。这代表版本可用，但实际并不可用。现在，当版本没有出现在更新频道中时，web 控制台会显示 **Version not found**。(BZ#1819892)
- 所安装的 Operator 列表只能按照 **Name** 栏进行排序，这限制了用户的排序选项。现在，用户可以名称和其他字段对列表进行排序。(BZ#1797931)
- pod 详情页面不包含条件。没有条件，很难知道 pod 的状态。pod 详情页面中有一个条件部分，可以轻松地识别 pod 的状态。(BZ#1804869)
- 查询浏览器的结果使用硬编码排序进行显示。硬编码的排序可能会覆盖查询中指定的排序，从而给出一个与请求不同的结果。现在，硬编码的排序已被删除，因此查询中指定的排序会被保留。(BZ#1808394)
- 在以前的版本中，web 控制台在某些情况下因为 ts-loader 使用不正确的 **tsconfig.json**，从而导致在特定页面中会出现运行时错误。现在，这个 ts-loader 的问题已解决，所有 Web 控制台页面都可以正确加载。(BZ#1811886)
- 从 web 控制台的 **Developer** 视角导航到 **Advanced** → **Project Details** → **Inventory** 部分时，**DeploymentConfig** 对象不会被列出。现在会跟踪 **DeploymentConfig** 对象，并包含在仪表板的 **Inventory** 部分。(BZ#1825228)
- 在以前的版本中，当用户名包含特殊字符（如 #）时，web 控制台不会显示用户详情。现在，无论用户名中的特殊字符是什么，web 控制台都会显示用户详情。(BZ#1835460)
- 在以前的版本中，在 YAML 编辑器中编辑对象时它不会验证是否存在所需的 **metadata** 字段。如果对象保存时缺少了字段，则在浏览器的 JavaScript 控制台中会记录一个错误，但没有提供可见的反馈信息。现在，如果缺少所需的 **metadata** 字段，Web 控制台会显示一个可操作的错误消息。(BZ#1787503)
- 在以前的版本中，当使用表单视图编辑对象时，切换到对象的 YAML 编辑器不会同步所有现有的数据。现在，所有数据都会在表单视图和 YAML 编辑器间进行正常同步。(BZ#1796539)
- 在以前的版本中，当使用 tab 键导航时，可能会触发 notification drawer 并被扩展。在这个版本中，当使用 tab 键导航时，不再会触发 notification drawer。(BZ#1810568)
- 在以前的版本中，当列出自定义资源定义（CRD）的现有实例时，会使用错误的 API 来填充列表。现在，会使用正确的 API 来填充列表。(BZ#1819028)
- 在 **Operators** → **Installed Operators** 页面中，当查看所选 Operator 的可用自定义资源（CR）列表时，**Version** 列会显示 **Unknown** 值。因为 CR 没有可用的版本信息，所以此字段现已从 UI 中删除。(BZ#1829052)
- 在以前的版本中，当完成 **Create Operator Subscription** 表单时，如果 **Update Channel** 字段有变化，订阅的目标命名空间会错误地被重置，且无法提交表单。现在，在调整 **Update Channel** 时，目标命名空间值会被保留，表单可以被成功提交。(BZ#1798851)
- 在以前的版本中，**metric openshift_console_operator_build_info** 没有被正确公开。在这个版本中，指标数据包括在 Prometheus 中。(BZ#1806787)

- 以前，在管理视角中，当在侧面面板中查看 **Workloads** 标签页时，notification drawer 在扩展时会隐藏在侧面板下面。在这个版本中，对 CSS **z-index** 进行了调整，以便可看到 notification drawer。(BZ#1813052)
- 在以前的版本中，OperatorHub 在 web 控制台中只对集群管理员可见。在这个版本中，web 控制台会为分配了 **aggregate-olm-view** 和 **aggregate-olm-edit** 集群角色绑定的用户显示 OperatorHub。(BZ#1819938)
- 在 web 控制台的 **Administrator** 视角的 **Home → Events** 页面中，几个节点事件没有显示节点名称。在这个版本中，所有事件都正确链接到相应节点。(BZ#1809813)
- 在以前的版本中，web 控制台的 **Administrator** 视角中的 **Home → Overview** 菜单项对于无法列出命名空间但具有查看集群指标的权限的用户是不可见的。在这个版本中，所有有权查看集群指标的用户都可以看到 **Overview** 项。(BZ#1811757)
- 以前，在 **Installed Operators** 页面的 OperatorHub 中，用来查看已安装 Operator 的更多 API 的链接不会打开正确的标签页。在这个版本中，**Provided API** 下的 **View x more** 链接到 Installed Operator 的 **Details** 选项卡。(BZ#1824254)
- 以前，在 OperatorHub 中，容器背景溢出在移动视图中不会被隐藏。这个版本解决了灰色背景问题并隐藏了溢出。(BZ#1809812)
- 在以前的版本中，**fieldDependency specDescriptor** 无法按预期工作。因此，Control 字段无法控制 Dependent 字段的可见性。现在，通过 Control 字段可用正确地启用或禁用 Dependent 字段的可见性。(BZ#1826074)
- 在以前的版本中，默认的 CA 证书在控制台 pod 中使用。现在，控制台被配置为使用 **default-ingress-cert** 配置映射（如果 ConfigMap 存在）；或控制台将配置默认 CA 证书（如果不存在）。这允许使用默认 Ingress 证书来验证 Ingress Controller 创建的路由的访问权限。(BZ#1824934)
- 在以前的版本中，当创建新的 Alert Receiver 时，web 控制台没有指定路由标签是必需的。现在，添加了一个红色星号来代表路由标签是必需的。(BZ#1803614)
- 在以前的版本中，web 控制台 **ClusterRole** 详情页面中的 **Role Bindings** 选项卡可能会显示具有相同名称的命名空间角色的绑定。这个标签现在会正确地只显示 **ClusterRole** 的绑定。(BZ#1624328)
- 以前，当 OLM Operator 的标记表有很多内容时，其显示的速度会下降。web 控制台改进了这些表的显示，并在需要时添加了一个水平滚动条。(BZ#1831315)
- 以前，当在 web 控制台中检查所有 PVC 时，很难区分 PVC 所属的存储类。在 web 控制台中添加了 PVC Storage Classes 列，以便更轻松地查找 PVC 的存储类信息。(BZ#1800459)
- 以前，使用控制台的 **Compute → Machine Config Pools → Create Machine ConfigPool** 按钮创建新的机器配置池会导致机器配置池不匹配该节点。这是因为模板使用 **spec.machineSelector** 键来选择要匹配的节点。但是，这个键值不被 API 识别；选择节点的正确值是 **spec.nodeSelector**。选择节点的键已更新，允许 web 控制台显示与正确节点匹配的 Machine Selector。(BZ#1813369)
- 在以前的版本中，在 CLI 下载页面中不首先列出 **oc**，因为 CLI 下载按字母顺序列出。因为 **oc** 是 OpenShift Container Platform 的主要 CLI，现在它列在 CLI 下载页面的顶部。(BZ#1824934)
- 以前，**Explorer** 视图会向没有所需权限的用户显示 **Access Review** 标签页。没有这个授权的用户会看到出错信息以及尝试重新载入标签页的说明，但重试不会改变结果。在这个版本里，没有权限查看标签页内容的用户隐藏了 **Access Review** 标签页。(BZ#1786251)

- 在以前的版本中，**Cluster Utilization** 卡视图和顶端用户的弹出视图中的内存消耗数据不一致，因为这两种视图使用了不同的方法来计算内存用量。在这个版本中，两个视图使用相同的方法计算内存用量，因此它们提供的数据是一致的。(BZ#1812096)
- 在以前的版本中，用户可以为单个警报接收器创建两个路由标签。当两个路由标签具有相同的键时，列表页只会显示最新创建的一个。但是，如果其中一个路由标签使用了正则表达式，则详情页面将其分为两个不同的路由标签。在这个版本中，用户无法为一个警报接收器创建两个路由标签。(BZ#1804049)
- 在这个版本中，web 控制台使用的一个库被更新来解决一些视图中的性能和显示问题。(BZ#1796658)
- mast 标头中的选择链接具有 href 值 #，它带有包括目标目的地的 OnClick handler。因此，这些链接可在新标签页中打开，但 # 会解析为仪表盘，而不是预期的目标目的地。现在，所有带 href # 的链接都会被更新到一个按钮元素中，因此 **Open Link In New Tab** 选项不可用。带有 **Open Link In New Tab** 选项的链接可以显示正确的 URL。(BZ#1703757)

监控

- 在以前的版本中，错误处理与 Prometheus PVC 名称相关的元数据可能会导致升级到或从版本 4.4.0-4.4.8 升级失败。现在，数据被从旧的物理卷复制到新的物理卷以便保留统计数据，从而使升级可以完成。(BZ#1832124)
- 在以前的版本中，Thanos Querier 可以调度到 master 和 worker 节点上，但它只应该调度到 worker 节点上。现在删除了允许在 master 节点上调度 Thanos Querier 的容限，Thanos Querier 只会部署在 worker 节点上。(BZ#1812834)
- 在以前的版本中，对一些 Prometheus 记录规则的评测偶尔会失败，并导致规则产生的指标丢失。现在，这个与记录规则相关的问题已被修复。(BZ#1802941)
- 在以前的版本中，CPU 使用率显示不正确的结果，这是由于统计数据平滑处理造成的。现在，计算 CPU 使用率的方法已被更新，**oc adm top** 显示的结果与 Linux 的 **top** 程序显示的结果非常接近。(BZ#1812004)
- 在以前的版本中，集群监控的自定义配置会丢失。这是因为 **cluster-monitoring-config** 映射无效，并且集群监控操作员默认使用默认配置。现在，当集群监控操作员无法对 **cluster-monitoring-config** 配置映射进行解码时，它将不会使用默认配置，而是发出一个警告信息。(BZ#1807430)

网络

- kube-proxy 指标实现中的更改会在 Kubernetes 1.17 重基的过程中消失。在这个版本中，改变了在 SDN 中发布指标的方式，使其不会丢失。(BZ#1811739)
- 在以前的版本中，当安装程序引入 **machineNetwork** 时，Cluster Network Operator 不会被修改来将其添加到 **proxy.status.noProxy** 中。在这个版本中，设置 **proxy.status.noProxy** 使其包含预期的字段，包括 **machineNetwork**。(BZ#1797894)
- 在以前的版本中，节点会错误地检测到它自己的 IP 地址，阻止它拥有它所分配的 egressIP。在这个版本中，会从 Kubernetes API 中分配节点 IP。(BZ#1802557)
- 一个代码更改意外停止了为第三方插件设置状态，这意味着 Cluster Network Operator 状态不会显示其正在正常工作。在这个版本中，添加了代码来设置使用第三方插件时的状态。现在，在使用第三方插件时，Cluster Network Operator 会正确报告状态。(BZ#1807611)
- 在以前的版本中，Kuryr bootstrapping 上的 Cluster Network Operator 在被新规则替代时没有删除过时的安全组规则的逻辑。在 OpenShift Container Platform 升级过程中，旧的安全组规则保

留在安全组中。这意味着在从 4.3 升级到 4.4 的环境中后没有对它们进行强化以增强安全性。在这个版本中，Cluster Network Operator 删除了旧的安全组规则。因此在把 4.3 升级到 4.4 时安全组规则会被删除，pod 能够正确获得对主机虚拟机的受限访问权限。(BZ#1832305)

- 在以前的版本中，要强制执行一个禁用任何流量的 Network Policy，与该策略匹配的服务应该具有相应的负载均衡器来阻断流量。由 Octavia 提供的方法是使用 ACL，并在负载均衡器监听器上设置 admin 状态。因此，OpenShift Container Platform 端点上的安全组与 OpenShift Container Platform 端点上的安全组不匹配。pod 的实际安全组会导致一些负载均衡器被考虑进行网络策略更新，从而禁用了 admin 状态的流量。在这个版本中，Kuryr 注解上的端点安全组字段与所选 pod 的现有安全组匹配。现在，如果没有网络策略阻断它，则所有负载均衡器的监听程序都会启用 admin 状态。(BZ#1824258)
- 之前，iptables 可能会遇到锁定问题。在个别情况下，pod 可能无法启动，`oc describe pod` 命令会显示一个事件，"Failed create pod sandbox ... could not set up pod iptables rules: Another app is currently holding the xtables lock." 在这个版本中，在相关代码中将 `-w` 传递给 iptables。这样，iptables 会等待锁定从而避免了意外失败的发生。(BZ#1810505)
- 在以前的版本中，在删除节点时，节点的 chassis 记录不会从更低级别组件 (south-bound) 的数据库中删除。过时的 chassis 记录会导致 chassis 的过时的逻辑流程，而且永远不会被删除。现在，在 `ovnkube-master` 中添加了节点同步机制用于清除已删除节点的 chassis 记录。因此，在更低级别组件的数据库中不会有与已删除节点相对应的过时的 chassis 记录或过时的逻辑流程。(BZ#1809747)
- 当 etcd 运行缓慢时，`openshift-sdn` 可能会因为争用条件而丢失命名空间创建事件。这可能会导致命名空间中的 pod 无法连接。在这个版本中，争用条件已被删除。因此，pod 最终具有可连接性。(BZ#1825355)

节点

- 在以前的版本中，`kubepods.slice` 内存 cgroup 没有被设置为最大限制减去保留值。这会导致节点因为缺少内存而超载，而不是驱除工作负载。现在，`kubepods.slice` 内存保留已被正确设置。(BZ#1800319)
- 在以前的版本中，设备的设备映射程序缺少指标数据，因此如果系统要为 root 设备使用设备映射程序时，没有可用的指标。cadvisor 已被修复。现在，无论设备映射程序是否用于 root 设备，指标都可用。(BZ#1849269)

Node Tuning Operator

- Node Tuning Operator 没有包括针对 tuned 守护进程问题 (BZ#1702724) 和 (BZ#1774645) 的修复。因此，当用户指定无效的配置集时，操作对象功能会发生一个 DoS 问题。另外，修正配置集并不会恢复操作对象的功能。在这个版本中，应用了针对上述程序错误的修复。现在，tuned 守护可以正常处理并设置新的修正的配置集。(BZ#1823941)
- 在以前的版本中，tuned pod 没有从主机挂载 `/etc/sysctl.{conf,d/}`。因此，主机提供的设置可以被 tuned 配置集覆盖。现在，tuned Pod 会从主机挂载 `/etc/sysctl.{conf,d/}`，这样可防止 tuned 配置集覆盖 `/etc/sysctl.{conf,d/}` 中的主机 sysctl 设置。(BZ#1825322)

oc

- 在以前的版本中，打印机标志不正确，`oc adm group sync` 命令缺少输出选项。现在，这个标志可以正常工作，所有输出选项都可以正常工作。(BZ#1828194)
- 在以前的版本中，格式结果函数带有硬编码大小，因此当数组被少于硬编码限制的数据填充后会出现 panic 的问题。现在，LDAP 项的数量会更加实际的数组容量来限制，函数可以正确地对结果进行格式处理。(BZ#1806876)

- 在以前的版本中，如果只指定了 `--from-dir` 选项，`oc image mirror` 命令会出错，即使它应该覆盖 `--dir` 选项。现在，`--from-dir` 可以正确地覆盖 `--dir`，命令可以成功运行。(BZ#1807807)
- 在以前的版本中，`oc adm release` 命令的帮助示例没有被正确显示。现在，它们已经被更新，现在可以正确显示。(BZ#1810310)

OLM

- Operator Lifecycle Manager (OLM) 安装的自定义资源会把 **OwnerReference** 对象授予它们所应用的 **InstallPlan** 对象。删除 **InstallPlan** 对象会删除从中应用的自定义资源。在这个版本中，更新了 OLM 将自定义资源的 **OwnerReferences** 对象指向为其安装的 CSV。因此，删除 **InstallPlan** 对象不会删除应用的自定义资源。(BZ#1808113)
- 在以前的版本中，垃圾回收事件队列没有被正确配置。这会导致在 Operator Lifecycle Manager (OLM) 管理的 Operator 被卸载时，不会清理集群范围内的资源。在这个版本中，更新了 OLM，为引用任何命名空间的所有者标签重新配置垃圾回收队列。因此，在卸载 Operator 时，由 OLM 管理的 Operator 生成的集群范围资源会被正确清理。(BZ#1834136)
- 如果一个 Operator 被升级，它提供了一个需要的 API，而这个 API 的组、版本和 kind (GVK) 自 Operator 的前一个版本以来还没有改变，而且依赖于 API 的 Operator 使用 **skipRange** 项而没有使用 **spec.Replaces** 项，Operator Lifecycle Manager (OLM) 将无法生成带有正确的 **replaces** 项的“升级的 CSV”。特别是，OLM 会：
 1. 将新 Operator 添加到生成中，并将它所提供的 API 标记为 **present**。
 2. 从生成中删除旧 Operator，并将其提供的 API 标记为 **absent**，尽管 Operator 的新版本提供了该 Operator。
 3. 尝试解决缺少 API 的问题，使用没有设置 **spec.Replaces** 字段的副本来覆盖 Operator 的新版本。
这会导致某些 Operator 无法升级到新版本。在这个版本中更新了 OLM，以便在向生成新 Operator 添加新 Operator 之前，从当前生成中删除旧的 Operator。因此，升级可以如预期成功。(BZ#1818788)
- 无效的 **CatalogSource** 对象配置会导致 nil-pointer 异常和 panic。当每次协调无效的 **CatalogSource** 对象时，**catalog-operator** pod 都会崩溃。在这个版本中，增加了运行时的 nil 检查和 **CatalogSource** 对象验证。因此，无效的 **CatalogSources** 对象会被赋予一个相应的条件，**catalog-operator** pod 不会崩溃。(BZ#1817833)
- Operator Lifecycle Manager (OLM) 允许用户使用 **Subscription** 对象的 **subscriptionConfig** 字段来指定卷和卷挂载。使用此功能更新 **ClusterServiceVersion** 资源 (CSV) 中定义的 **Deployment** 资源。偶尔，OLM 无法为缓存中的 CSV 创建 **Subscription** 对象，CSV 会被放在“安装阶段”中，而不创建在 **Subscription** 对象中定义的卷或卷挂载的 **Deployment** 资源。然后，OLM 将无法进入“succeeded 阶段”，因为计算的 **Deployment** 资源哈希值与 **Deployment** 资源上的实际 **Deployment** 资源哈希不匹配。这个错误不会被解决，因为 OLM 不会在“安装阶段”更新或重新创建 **Deployment** 资源，这个问题会持续 5 分钟直到 OLM 与 CSV 重新同步。因此，OLM 在安装 CSV 时偶尔会出现延迟。在这个版本中，如果 OLM 在安装 CSV 时遇到 **Deployment** 资源哈希错误，OLM 现在会重新创建 **Deployment** 资源。因此，OLM 不再会因为不正确的 **Deployment** 资源哈希而延迟。(BZ#1826443)
- 在以前的版本中，Operator Lifecycle Manager (OLM) 不期望在单个 **Deployment** 资源上运行多个 **APIService** 资源，仅挂载与 OLM 创建的最后一个 **APIService** 资源关联的 CA。这会导致 OLM 无法在单个 **Deployment** 资源中运行多个 **APIService** 资源。在这个版本中，OLM 对单个 **Deployment** 资源中的所有 **APIService** 资源都使用相同的 CA。因此，OLM 现在可在单个 **Deployment** 资源中运行多个 **APIService** 资源。(BZ#1805412)
- 在以前的版本中，Operator Lifecycle Manager (OLM) 在引入一个结构性 schema 时无法正确

地弃用 v1alpha2 本地 **OperatorGroup** 自定义资源定义 (CRD)。这会导致 v1alpha2 **OperatorGroup** CRD 不再被支持且无法创建它们。在这个版本中，重新使用了 v1alpha2 **OperatorGroup** CRD，因此 OLM 会再次支持 v1alpha2 **OperatorGroup** CRD。(BZ#1798051)

- 当之前解析的 **InstallPlans** 对象不再包含对应的清单集合时，一组新的、非绝对解析的依赖应用程序会被触发。如果 Operator 存在多个有效的依赖项，则有时会出现应用一个对等的但不同解析的依赖关系而不是使用一个存在的依赖关系。在这个版本中，为 **InstallPlan** 对象 API 的状态添加了一个 **generation** 字段，并在每次解析时增加它，只应用最新状态的 **InstallPlan** 对象。因此，在一个特定时间点上，集群中只有一组 Operator 依赖关系。(BZ#1784024)
- **OperatorHub** 类型定义缺少了生成 Kubernetes 客户端所需的额外的 **+genclient** 标记注释。这会导致生成的客户端没有包括在 **openshift/client-go** 中。在这个版本中，为 **OperatorHub** 配置类型添加了缺失的 **+genclient** 标记注释，因此生成的客户端现在可以按预期可用。(BZ#1816483)

openshift-apiserver

- 在以前的版本中，OpenShift API 服务器在升级过程中对于客户端是不可用的，这会导致操纵失败。现在，OpenShift API 服务器在升级过程中仍然可以被客户端使用。(BZ#1791162)

openshift-controller-manager

- 在以前的版本中，用于为 OpenShift Container Platform 内部 registry 创建 pull secret 的客户端的速率限制较低。如果在短时间内创建了大量命名空间，则需要很长时间才能创建镜像 registry pull secret。现在，客户端的速率限制已提高，因此可以快速创建内部 registry pull secret，即使在流量高的情况下也是如此。(BZ#1785023)
- 在以前的版本中，Prometheus 指标中没有 **workqueue_depth** 等指标。在这个版本中，提供了缺少的指标。(BZ#1825324)
- 如果 **openshift-controller-manager** pod 失败，不会提供终止信息。现在，如果 pod 终止，会提供一个终止信息。(BZ#1804432)
- 在以前的版本中，没有正确注册 OpenShift Container Platform control plane 的指标。在这个版本中，提供了 control plane 的指标。(BZ#1809699)
- 在以前的版本中，当删除了关联的令牌时，内部 registry 的 pull secret 可能会被孤立。在这个版本中，在 pull secret 和令牌之间创建了一个引用，在删除关联的令牌时 pull secret 不会被孤立。(BZ#1765294)
- 在以前的版本中，如果 OpenShift Container Platform 配置为使用全局代理服务器，则该代理不会在连接到外部镜像 registry 时使用。现在，当从外部 registry 拉取镜像时，OpenShift Container Platform 会使用集群范围的代理服务器配置。(BZ#1805168)
- 在以前的版本中，在部署滚动更新过程中，控制器可能会长时间不可用。在这个版本中，允许控制器在部署中的 pod 被终止时主动释放其租期，从而减少了延迟时间。(BZ#1809719)
- 在以前的版本中，**openshift-controller-manager-operator** 可能会以提升的 SELinux 的权限运行。在这个版本中，会使用正确的安全上下文对其进行约束。(BZ#1806913)
- 在以前的版本中，在升级 **openshift-controller-manager** 的过程中会错误地报告 Operator 已升级并可用。现在，Operator 会正确地报告其状态。(BZ#1804434)
- 在安装或升级过程中，**openshift-controller-manager** 没有正确报告其进度条件。因此，安装或升级可能会失败。现在，Operator 在成功安装或升级时会正确报告其进度。(BZ#1814446)
- 在以前的版本中，如果在资源创建后添加了 **alpha.image.policy.openshift.io/resolve-names** 注解，则 **image-resolve-plugin** 不会解析镜像。这个问题现在已解决。即使在资源创建后添加了

alpha.image.policy.openshift.io/resolve-names 注解, **image-resolve-plugin** 也会解析镜像。(BZ#1805155)

- 在以前的版本中, 在 IPv6 集群上, Controller Manager Operator 不会公开其指标数据。因此, 指标不会被正确抓取, 从而导致用户无法以图形方式显示性能数据或查询性能数据。现在, Controller Manager Operator 可以正确地绑定到 IPv6 接口, 这样指标数据就可以被正确地抓取并提供给用户。(BZ#1813233)

路由

- 在以前的版本中, 服务负载均衡器不能包括 Azure master 节点, 这会在 worker 节点也是 master 节点的紧凑集群中使 ingress 无法正常工作。Azure 仅允许节点的网卡 (NIC) 在一个时间点上与一个负载均衡器关联。在这个版本中, 安装程序被修改为创建一个统一的负载均衡器和网络安全组, **LoadBalancer** 类型的 API 和服务都使用它。现在, 在 Azure 上服务负载均衡器可以包括 master 节点, 在紧凑型的集群 ingress 可以正常工作。(BZ#1794839)
- 在以前的版本中, 如果 secret 无效, openshift-router 不会建立对默认证书 Secret 内容的监控。启动后, openshift-router 无法读取无效的 secret。该 secret 必须存在路由器 pod 才能启动。因此, 用户需要更新无效的 secret 并删除当前的路由器 pod。在这个版本中, 路由器会监控默认证书 secret 而无需删除路由器 pod。如果 secret 无效, 路由器将使用并提供默认路由器证书。如果 secret 有效, 路由器从该 secret 中提供默认证书。(BZ#1820400)
- 在以前的版本中, 在 AWS 中国区域运行时, ingress operator 无法配置 DNS。在这个版本中, ingress Operator 会检测到何时在 AWS 中国区域运行, 并可以在 Route 53 API 端点中配置 DNS。(BZ#1805224)
- 在以前的版本中, Ingress Operator 持续覆盖它在 Azure 和 Google Cloud Provider (GCP) 上管理的 DNS 记录。在这个版本中, Ingress Operator 会在记录已发布且记录和 DNS 区配置没有改变后避免更新 DNS 记录。Ingress Operator 现在会向云供应商 API 发出较少的调用, 这可以防止在 **openshift-ingress** 命名空间中出现 **cloud provider rate limited** 事件。另外, ingress operator 日志现在显示较少的 **upserted DNS record** 日志信息。(BZ#1809354)
- 在以前的版本中, ingress-to-route 控制器使用 **extensions/v1beta1** API 组中的入站 (ingresses) 资源, 它已在 Kubernetes 1.18 中被弃用。在这个版本中, ingress-to-route 控制器会使用来自 **networking.k8s.io/v1beta1** API 组中的 **ingresses** 资源。(BZ#1801415)
- 在以前的版本中, 当删除冲突路由时, 路由器不会推广不活跃的路由。现在, 当删除路由时, 路由器会重新处理所有不活跃的路由并激活不再与删除的路由冲突的路由。(BZ#1821095)
- 在以前的版本中, 当删除类型为 **LoadBalancer** 或带有 **LoadBalancerService** 端点发布策略类型的 IngressController 时, 服务会始终存在并处于 **pending** 状态。在 OpenShift Container Platform 3.10 中更改了服务控制器, 在创建或删除非 **LoadBalancer** 服务时防止不必要的 **GetLoadBalancer** cloud-provider API 调用。在 Kubernetes 1.15 中的一个后续变化将以不同的方式来防止调用非必需的 API。因此, 这两种更改之间的交互会破坏服务控制器对类型为 **LoadBalancer** 的服务的清理逻辑。在这个版本中, OpenShift Container Platform 3.10 里添加的更改已被删除。现在, 可以成功删除类型为 **LoadBalancer** 的服务和类型为 **LoadBalancerService** 的 Ingress Controller。(BZ#1798282)
- 在以前的版本中, 当端点公布的策略没有包括对于负载均衡器的管理时, Ingress Operator 会设置一个令人混淆的 **LoadBalancerManager** 状态原因。当 **IngressController** 资源配置为使用 **LoadBalancerService** 以外的端点发布策略类型时, Ingress Operator 不会为 Ingress Controller 管理负载均衡器。在这个版本中, **LoadBalancerManager** 状态条件更为明确地说明 Operator 未为 IngressController 管理负载均衡器的原因。现在, 在信息中不再包括如 **unsupported** 或 **does not support** 等不明确的说明。(BZ#1826113)
- 在以前的版本中, 当入口控制器将 HTTP 请求转发到应用程序时, 会添加带有非标准 **proto-version** 参数的 Forwarded HTTP 标头。因此, Forwarded 的标头与标准不兼容。当应用程序尝

试解析标头值时可能会造成问题。在这个版本中，Forwarded 标头符合标准，口控制器不会在 Forwarded 标头中指定 **proto-version** 参数。(BZ#1803001)

- 在以前的版本中，显示活跃会话数量的 Prometheus 计数器会在路由器重启后保留并无限期增加。在这个版本中，**haproxy_frontend_current_session** 和 **haproxy_server_current_session** 可以准确反映活跃会话的数目。现在，在路由器重启时会重置这些计数器的值。(BZ#1832539)
- 如果通过路由公开的服务后端的 pod 不可用时（如 crashlooping、已删除等情况），路由器会返回 **503** 错误。在以前的版本中，不再为这个路由器提供 **haproxy_server_http_responses_total** 指标，因此无法再对路由进行监控。在这个版本中，所有后端指标都会被报告，用户可以在没有 pod 时跟踪相关的数据。(BZ#1835845)

Samples

- Samples Operator 的早期版本在 s390x 和 ppc64le 架构中没有在 bootstrap 后删除，虽然样本内容还没有在那些架构中提供。这会导致在 s390x 和 ppc64le 构架中进行集群升级的失败，因为它们会期望一些样本内容，而它们并没有被提供。现在，Samples Operator 被强制升级，即使它不包含必要的样本内容。这解决了因为 s390x 和 ppc64le 架构中不可用的内容示例导致的集群升级失败的问题。(BZ#1835112)
- 如果在后续发行版本中移除了之前 OpenShift Container Platform 发行版本中的示例镜像流，则在升级到后续版本时，会错误跟踪移除的镜像流，因为需要完成镜像流导入。因为没有发生镜像流导入，样本不会报告升级已完成。这会导致集群升级失败。Samples Operator 已更新，忽略了跟踪上一个版本中存在的、在升级到的版本中不再存在的镜像流的过程。现在，在发行版本间移除的镜像流在升级过程中不再导致 Samples Operator 失败。(BZ#1811143)
- 在以前的版本中，Samples Operator 会发送有关无效配置或缺少镜像 pull secret 的警报。这会导致错误地向用户发送警报，因为如果删除了 Samples Operator，则不能由 Samples Operator 发送无效的配置和丢失的镜像 pull secret。Samples Operator 已更新，在进行引导时不会发送与导入示例相关的警报。(BZ#1813175)
- 在以前的版本中，在之前的发行版本中但在后续版本中删除的样本模板可能会被标记为需要更新。尝试更新模板会导致各种错误和失败状态。这些模板已更新，在移除后不会再接收更新。因此，删除的样本模板不会再产生错误或失败。(BZ#1828065)

存储

- 在以前的版本中，在某些 Azure 区域中，卷可能无法置备，而且这些区域在没有正确可用区支持的情况下创建。在这个版本中，可在置备过程中检测到可用域的支持，从而可以在所有 Azure 区域中启用卷置备。(BZ#1828174)
- 在以前的版本中，当在关联 **VolumeSnapshot** 资源之前删除 **VolumeSnapshotClass** 时，因为无法删除关联的资源，命名空间会卡在 **Terminating** 状态，**VolumeSnpshts** 会存在于集群中。在这个版本中，**VolumeSnapshot** 资源功能会检查相关的 **VolumeSnapshotClass** 资源是否已被删除，从而可以在没有对应的 **VolumeSnapshotClass** 资源时成功删除 **VolumeSnapshot** 资源。(BZ#1808123)
- 在以前的版本中，当 **VolumeSnapshotContents** 资源为 nil 时，CSI Snapshot Controller 可能会崩溃。现在，系统会在使用 **VolumeSnapshotContent** 资源前检查 **VolumeSnapshotContent** 资源是否为 nil。(BZ#1814280)
- 在以前的版本中，升级 Local Storage Operator 时，关联的 **diskmaker** 和 **provisioner pod** 可能都已过时，除非也修改了 **LocalVolume** 资源。在这个版本中，守护进程集的 hash 包含在注解中。如果 hash 不匹配，pod 被部署以便在更新 Local Storage Operator 时成功更新 **diskmaker** 和 **provisioner pod**。(BZ#1822213)

- 在以前的版本中, `oc get volumesnapshot` 只会显示资源的名称和创建时间, 而不会显示状态。在这个版本中, `oc get volumesnapshot` 现在会包括额外的信息, 如关联的 `VolumeSnapshotContent` 资源、`VolumeSnapshot` 资源和其他相关信息。(BZ#1800437)
- 在以前的版本中, `oc get volumesnapshotclass` 只会显示资源的名称和创建时间, 而不显示删除策略或驱动程序信息。在这个版本中, `oc get volumesnapshotclass` 包括了其他的信息, 如相关的 CSI Driver 和删除策略。(BZ#1800470)
- 在以前的版本中, `oc get volumesnapshotcontent` 只会显示资源的名称和创建时间, 而不会显示其他相关信息。在这个版本中, `oc get volumesnapshotcontent` 现在会包括额外的信息, 如关联的 `VolumeSnapshot` 资源、`VolumeSnapshotClass` 资源和其他相关信息。(BZ#1800477)

1.6. 技术预览功能

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

技术预览功能支持范围

在下表中, 功能被标记为以下状态：

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

表 1.2. 技术预览

功能	OCP 4.3	OCP 4.4	OCP 4.5
精度时间协议 (PTP)	TP	TP	TP
oc CLI Plug-ins	TP	TP	TP
experimental-qos-reserved	TP	TP	TP
Pod Unidler	TP	TP	GA
为临时存储设置 Limit/Requests	TP	TP	TP
Descheduler	-	TP	TP
Podman	TP	TP	TP
PID 命名空间的共享控制	TP	TP	GA
OVN-Kubernetes Pod network provider	TP	TP	TP
基于 Prometheus 的 HPA 定制 metrics adapter	TP	TP	TP

功能	OCP 4.3	OCP 4.4	OCP 4.5
HPA 用于内存使用	TP	TP	TP
机器健康状态检查	TP	GA	GA
三节点裸机部署	TP	TP	GA
Helm CLI	TP	GA	GA
服务绑定	TP	TP	TP
日志转发	TP	TP	TP
用户工作负载监控	TP	TP	TP
OpenShift Serverless	TP	GA	GA
Compute Node Topology Manager	TP	TP	GA
使用 Cinder 的原始块	TP	TP	TP
CSI 卷快照	-	TP	TP
CSI 卷克隆	-	TP	GA
CSI 卷扩展	TP	TP	TP
CSI AWS EBS Driver Operator	-	-	TP
OpenStack Manila CSI Driver Operator	-	-	GA
CSI inline 临时卷	-	-	TP
OpenShift Pipelines	-	TP	TP
Vertical Pod Autoscaler	-	-	TP
Operator API	-	-	TP
OpenShift virtualization	TP	TP	GA

1.7. 已知问题

- 当使用用户置备的基础架构在 vSphere 上打开虚拟机时,扩展节点的过程可能无法正常工作。虚拟机监控程序配置中的一个已知问题会导致在虚拟机监控程序中创建机器,但不打开电源。如果在扩展机器集后某个节点可能处于 **Provisioning** 状态,您可以调查 vSphere 实例本身中的虚拟机状

态。使用 VMware 命令 **govc** 任务和 **govc** 事件 来确定虚拟机的状态。检查类似以下内容的错误消息：

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

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

- 如果您的内部 Elasticsearch 实例使用持久性卷声明 (PVC)，PVC 必须包含 **logging-cluster:elasticsearch** 标签。如果没有标签，在升级垃圾回收过程中会删除这些 PVC，Elasticsearch Operator 会创建新的 PVC。如果您要从版本 4.4.30 之前的 OpenShift Container Platform 版本更新，则必须手动将该标签添加到 Elasticsearch PVC。在 OpenShift Container Platform 4.4.30 后，Elasticsearch Operator 会自动将该标签添加到 PVC 中。
- 当升级到新的 OpenShift Container Platform z-stream 发行版本时，当节点升级后，与 API 服务器的连接可能会中断，这会导致 API 请求失败。(BZ#1845411)
- 当升级到新的 OpenShift Container Platform z-stream 版本时，路由器的连接可能会在路由器 Pod 被更新后中断。在升级期间，一些应用程序可能无法被稳定访问。(BZ#1809665)
- 当使用默认 CNI 网络供应商设置为 OVN-Kubernetes 升级到新的 OpenShift Container Platform 版本时，升级会失败且集群处于不可用状态。(BZ#1854175)
- 由于镜像 registry pull-through 的 **ImageContentSourcePolicy** 尚不受支持，因此如果镜像流启用了 pull-through 策略，则部署 pod 无法使用摘要 ID 来对镜像进行镜像 (mirror)。在这种情况下，会显示 **ImagePullBackOff** 错误。(BZ#1787112)
- 当在使用用户置备的基础架构 RHOSP 中运行集群时使用 RHEL worker 扩展，如果入口端口 VIP 在 RHEL worker 上则无法访问所有路由。作为临时解决方案，您必须将路由器 pod 重新调度到 RHCOS 节点，并将 Ingress VIP 迁移至 RHCOS 节点。要做到这一点，请在升级前将 **node.openshift.io/os_id: rhcos** 标签添加到 Ingress Controller:

```
$ oc -n openshift-ingress-operator edit ingresscontroller/default -o yaml
spec:
  nodePlacement:
    nodeSelector:
      matchLabels:
        kubernetes.io/os: linux
        node-role.kubernetes.io/worker: ""
        node.openshift.io/os_id: rhcos
```

(BZ#1848945)

- Che Workspace Operator 更新为使用 **DevWorkspace** 自定义资源，而不是 **Workspace** 自定义资源。但是，OpenShift web 终端继续使用 **Workspace** 自定义资源。因此，OpenShift web 终端无法使用最新版本的 Che Workspace Operator。(BZ#1846969)
- 在 **Developer** 视角中，一个 **basic-user** 无法查看 **Monitoring** 界面中的 **Dashboard** 和 **Metrics** 标签页。(BZ#1846409)
- 在 **Topology** 视图中，当右键点击 Knative 服务时，**Edit Application Grouping** 选项会在上下文菜单中会显示两次。(BZ#1849107)

- 在 OpenShift Container Platform 4.5 中无法成功部署 Special Resources Operator (SRO)。这会防止部署 NVIDIA 驱动程序，集群需要这些驱动程序来运行需要 GPU 资源的负载。另外，因为同样的问题，Topology Manager 功能无法使用 GPU 资源测试。(BZ#1847805)
- web 控制台包含使用 SLIRP 绑定创建虚拟机 vNIC 的选项，但这并不被支持。尝试使用这个选项将导致 VM 无法引导。不要选择这个选项。(BZ#1828744)
- pod 在节点中使用 OpenShift SDN 默认 CNI 网络供应商时，可能会丢失网络通讯，从而导致 pod 崩溃。在升级集群时有时会发生这个问题。作为临时解决方案，您可以删除并重新创建 pod。(BZ#1855118)
- 存在一个在 master 节点上不支持自定义池的问题。**oc label node** 将新的自定义角色应用到目标 master 节点，但 Machine Config Operator 不应用针对于自定义池的更改。这会产生一个错误，它会被记录在 Machine Config Controller pod 日志中。为了确保 control plane 节点保持稳定，建议不要对 master 应用多个角色。(BZ#1797687)
- 与过去的 OpenShift Container Platform 版本相比，集群的日志记录性能会降级。这个问题正在被积极调查，并将在以后的 OpenShift Container Platform 版本中更新。(BZ#1833486)
- 当卷包含大量文件时，您可能会收到系统无法挂载卷的信息。当 pod 挂载一个设置了 **FSGroup SecurityContext** 的卷时，可能会发生这种情况。因为文件的 GID 所有权必须为卷上的所有文件递归更新。用户应该预计，使用具有大量文件并带有 **FSGroup SecurityContext** 设置的卷的 pod，会需要花费较长时间才能启动。(BZ#1515907)
- 运行带有频繁探测的 pod 可能会导致 common 进程的数量迅速增长。common 进程是一个从其父进程 CRI-O 中分离的程序，用来执行容器运行时。如果这个探测的频率足够频繁，systemd 会在恢复所有新子进程时遇到问题，一些 common 进程就可能成为僵尸进程。(BZ#1852064)
- 在 Microsoft Azure 中，当从 4.4 升级到 4.5 时，Ingress Operator 可能会因为刷新令牌错误而无法确保 DNSRecord。重启 Ingress Operator 可以解决这个问题。(BZ#1854383)
- 在带有安装程序置备的基础架构的 Azure 中运行 OpenShift Container Platform 时，存在一个已知问题：**oc** 命令有时会出现 TLS 握手超时的错误。(BZ#1851549)
- 对于使用安装程序置备的基础架构的 VMware vSphere 实例上的集群，bootstrap worker 会失败。默认资源池解析为多个实例。(BZ#1852545)
- 存在一个在安装 OpenShift Container Platform 集群时 Machine Config Operator (MCO) 被降级的问题。这是因为 bootstrap 过程中的机器配置排序问题导致。作为临时解决方案，您必须为任何自定义机器配置文件添加前缀，不同的地方是优先级为 **98-** 而不是 **99-**。(BZ#1826150)
- 通过 HTTPS 代理的 git clone 操作会失败。使用非 TLS (HTTP) 代理不会出现这个问题。(BZ#1750650)
- 如果源 URI 使用 **git://** 或 **ssh://**，则需要通过代理进行的构建的 git clone 操作都会失败。(BZ#1751738)
- 在 s390x 和 ppc64le 架构中存在一个问题，在强制重启或关机后，工作负载可能没有可用的节点。不要强制重新引导或关闭节点。
如果必须要重启或关机，且重新运行后的节点对于工作负载不可用：
 1. SSH 到该节点。
 2. 停止 CRI-O 和 kubelet 服务。
 3. 运行 **rm -rf /var/lib/containers** 命令。

4. 重启 CRI-O 和 kubelet 服务。

(BZ#1858411)

- 如果 AWS 帐户被配置为使用 AWS 机构服务控制策略 (SCP)，使用全局条件拒绝所有操作或需要特定权限，OpenShift Container Platform AWS 安装也会失败，即使提供的凭证有安装所需的权限。

OpenShift Container Platform 4.5.8 中引入了一个临时解决方案。(BZ#1829101)

- 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 4.5 的集群的集群管理员，您可以撤销或继续允许未经身份验证的访问。建议取消未经身份验证的访问，除非有特殊需要。如果您继续允许未经身份验证的访问，请注意相关的风险。

**警告**

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

使用以下脚本撤销对发现端点的未经身份验证的访问：

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

此脚本从以下集群角色绑定中删除未经身份验证的对象：

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

(BZ#1821771)

1.8. 异步勘误更新

OpenShift Container Platform 4.5 的安全更新、程序错误修正、功能增强更新将会通过红帽网络以异步勘误的形式发布。所有的 OpenShift Container Platform 4.5 勘误都可以通过[红帽客户门户网站](#)获得。[OpenShift Container Platform 生命周期](#) 包括了详细的与异步勘误相关的内容。

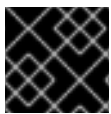
红帽客户门户网站的用户可以在红帽订阅管理 (RHSM) 帐户设置中启用勘误通知功能。当勘误通知被启用后，用户会在有与其注册的系统相关的勘误发行时接收到电子邮件通知。



注意

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

本节的内容将会持续更新，以提供以后发行的与 OpenShift Container Platform 4.5 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.5.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[更新集群](#)中的内容。

1.8.1. RHBA-2020:2409 - OpenShift Container Platform 4.5 镜像和程序错误公告

发布日期：2020 年 7 月 13 日

OpenShift Container Platform release 4.5 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:2409](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2408](#) 公告提供。

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

[OpenShift Container Platform 4.5.1 容器镜像列表](#)

1.8.2. RHSA-2020:2412 - Moderate: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 7 月 13 日

现在，OpenShift Container Platform 4.5 提供了容器镜像更新。有关更新的详情请查看 [RHSA-2020:2412](#) 公告。

1.8.3. RHSA-2020:2413 - Moderate: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 7 月 13 日

现在有一个 OpenShift Container Platform 4.5 的软件包更新。有关更新的详情请查看 [RHSA-2020:2413](#) 公告。

1.8.4. RHBA-2020:2909 - OpenShift Container Platform 4.5.2 程序错误修正更新

发布日期：2020 年 7 月 16 日

OpenShift Container Platform release 4.5.2 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:2909](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2908](#) 公告提供。

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

OpenShift Container Platform 4.5.2 容器镜像列表

1.8.4.1. 程序错误修复

- 在配置了安全引导（Secure Boot）的节点中，升级到 OpenShift Container Platform 4.5.1 会失败。对于配置了 Secure Boot 的集群，来自 control plane 和计算 Machine Config Pools 的一个节点无法重启，从而导致 Machine Config Operator（MCO）被降级。这会造成集群升级失败。这个版本不存在这个问题。（[BZ#1856501](#)）

1.8.5. RHBA-2020:2956 - OpenShift Container Platform 4.5.3 程序错误修正更新

发布日期：2020 年 7 月 22 日

OpenShift Container Platform release 4.5.3 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:2956](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2955](#) 公告提供。

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

OpenShift Container Platform 4.5.3 容器镜像列表

1.8.5.1. 程序错误修复

- 在以前的版本中存在一个问题，在强制重启或停机后导致节点无法用于工作负载。这个问题已被解决。（[BZ#1857224](#)）
- 在以前的版本中，web 控制台会返回软件包中声明的第一个频道中的图标，从而在 OperatorHub 中显示 Operator 图标。这有时会导致显示的图标与在软件包中发布的最新图标不同。这可以通过从默认频道中选择图标来确定最新的图标被显示。（[BZ#1844588](#)）
- 在以前的版本中，OpenShift Container Platform 构建中使用的容器镜像签名策略不包含任何本地镜像的配置。当只允许来自特定 registry 的镜像时，构建中的 **postCommit** 脚本会失败，因为不允许使用本地镜像。容器镜像签名策略已更新，始终允许直接引用本地存储层的镜像。现在，如果构建包含 **postCommit** hook，则可以成功完成。（[BZ#1849173](#)）

1.8.6. RHBA-2020:3028 - OpenShift Container Platform 4.5.4 程序错误修复更新

发布日期：2020 年 7 月 30 日

OpenShift Container Platform release 4.5.4 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3028](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3027](#) 和 [RHEA-2020:3208](#) 公告提供。

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

OpenShift Container Platform 4.5.4 容器镜像列表

1.8.6.1. 功能

1.8.6.1.1. IBM Z 和 LinuxONE

在这个版本中，IBM Z 和 LinuxONE 与 OpenShift Container Platform 4.5 兼容。如需了解安装步骤，请参阅[在 IBM Z 和 LinuxONE 上安装集群](#)。

限制

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

- 用于 IBM Z 的 OpenShift Container Platform 不包括以下技术预览功能：
 - OpenShift virtualization
 - 日志转发
 - 精度时间协议 (PTP) 硬件
 - CSI 卷快照
 - OpenShift Pipelines
- 以下 OpenShift Container Platform 功能不被支持：
 - Red Hat OpenShift Service Mesh
 - OpenShift Do (odo)
 - CodeReady Containers (CRC)
 - OpenShift Container Platform Metering
 - Multus CNI 插件
 - OpenShift Container Platform 升级分阶段部署
 - FIPS 加密
 - 加密数据存储存储在 etcd 中
 - 使用机器健康检查功能自动修复损坏的机器
 - 在 OpenShift Container Platform 部署过程中启用 Tang 模式磁盘加密。
 - OpenShift Serverless
 - Helm 命令行界面 (CLI) 工具
 - 在节点上控制过量使用和管理容器密度
 - CSI 卷克隆
- worker 节点必须运行 Red Hat Enterprise Linux CoreOS (RHCOS)。
- 持久性共享存储必须是 Filesystem: NFS 类型。
- 以下功能适用于 IBM Z 上的 OpenShift Container Platform 4.5，但不适用于 x86 上的 OpenShift Container Platform 4.5:
 - 在 IBM System Z 上为附加了 ficon 的 ECKD 存储的虚拟机启用了 HyperPAV。

1.8.6.1.2. IBM Power 系统

在这个版本中，IBM Power Systems 与 OpenShift Container Platform 4.5 兼容。请参阅 [在 IBM Power 上安装集群](#) 或 [在受限网络中在 IBM Power 上安装集群](#)。

限制

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

- 用于 IBM Power 系统的 OpenShift Container Platform 不包括以下技术预览功能：
 - 容器原生虚拟化 (CNV)
 - OpenShift Serverless
- 以下 OpenShift Container Platform 功能不被支持：
 - Red Hat OpenShift Service Mesh
 - OpenShift Do (odo)
 - CodeReady Containers (CRC)
 - 基于 Tekton 的 OpenShift Pipelines
 - OpenShift Container Platform Metering
 - SR-IOV CNI 插件
- worker 节点必须运行 Red Hat Enterprise Linux CoreOS (RHCOS)。
- 持久性存储必须是使用本地卷、网络文件系统 (NFS)、OpenStack Cinder 或容器存储接口 (CSI) 的 **Filesystem** 模式。
- 网络必须使用 DHCP 或 Red Hat OpenShift SDN 的静态地址。

支持的功能

- 目前，支持三个 Operator：
 - Cluster-Logging-Operator
 - Cluster-NDF-Operator
 - Elastic Search-Operator

1.8.6.2. 程序错误修复

- 在以前的版本中，操作符列表上的操作符菜单会在打开后马上关闭。当在 **Installed Operators** → **Operator Details** 页中点击 Operator 提供的 API 选项卡时会看到这个问题。这个菜单现在可以正常工作。(BZ#1842717)
- 在以前的版本中，当在 web 控制台中过滤 OperatorHub 目录时，一些 Operator 图标直到用户在页面上滚动时才会出现。在这个版本中，当过滤后图标会立即出现。(BZ#1844503)
- 在以前的版本中，web 控制台的 **Resource Quota Details** 页面中的配额图表显示的宽度为零，且不可见。这个版本已经解决了这个问题。(BZ#1845125)
- 在以前的版本中，点 **EtcdRestores** 页面中的 **Create EtcdRestores** 会导致 web 控制台停止响应。在这个版本中，**Create EtcdRestore** 表单会正确加载工作流。(BZ#1847277)

- 在以前的版本中，在 OpenShift Serverless Operator 的 **Create Knative Serving** 表单视图工作流程中，一些字段应该只接受数字字符的项会接受非数字字符。这个版本已经解决了这个问题。
([BZ#1847283](#))
- 在以前的版本中，点 **Create ManilaDriver** 表单查看 Manila CSI Driver Operator 的工作流不会创建 **ManilaDriver** 实例，或在 web 控制台出现任何响应。这个版本已经解决了这个问题。
([BZ#1853274](#))

1.8.6.3. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.7. RHSA-2020:3207 - Moderate: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 7 月 30 日

OpenShift Container Platform 4.5 现在提供了对 **jenkins-2-plugins** 的更新。有关更新的详情请查看 [RHSA-2020:3207](#) 公告。

1.8.8. RHBA-2020:3188 - OpenShift Container Platform 4.5.5 程序错误修复更新

发布日期：2020 年 8 月 10 日

OpenShift Container Platform release 4.5.5 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3188](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3189](#) 公告提供。

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

[OpenShift Container Platform 4.5.5 容器镜像列表](#)

1.8.8.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.9. RHBA-2020:3330 - OpenShift Container Platform 4.5.6 程序错误修复更新

发布日期：2020 年 8 月 17 日

OpenShift Container Platform release 4.5.6 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3330](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3331](#) 公告提供。

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

[OpenShift Container Platform 4.5.6 容器镜像列表](#)

1.8.9.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.10. RHSA-2020:3453 - Important: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 8 月 17 日

OpenShift Container Platform 4.5 提供了 **jenkins-2-plugins** 和 **python-rsa** 的更新。有关更新的详情，请查看 [RHSA-2020:3453](#) 公告。

1.8.11. RHBA-2020:3436 - OpenShift Container Platform 4.5.7 程序错误修复更新

发布日期：2020 年 8 月 24 日

OpenShift Container Platform release 4.5.7 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3436](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3437](#) 公告提供。

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

[OpenShift Container Platform 4.5.7 容器镜像列表](#)

1.8.11.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.12. RHSA-2020:3519 - Important: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 8 月 24 日

OpenShift Container Platform 4.5 提供了 **jenkins** 和 **openshift** 的更新。有关更新的详情，请查看 [RHSA-2020:3519](#) 公告。

1.8.13. RHSA-2020:3520 - Moderate: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 8 月 24 日

OpenShift Container Platform 4.5 提供了 **openshift-enterprise-hyperkube-container** 更新。有关更新的详情，请查看 [RHSA-2020:3520](#) 公告。

1.8.14. RHBA-2020:3510 - OpenShift Container Platform 4.5.8 程序错误修复更新

发布日期：2020 年 9 月 8 日

OpenShift Container Platform release 4.5.8 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3510](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3511](#) 公告提供。

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

[OpenShift Container Platform 4.5.8 容器镜像列表](#)

1.8.14.1. 功能

1.8.14.1.1. 为网络接口添加了 **projectID** 字段

新的 `projectID` 字段现在可以在 `.spec.template.spec.providerSpec.networkInterfaces` 下的 `MachineSet` 自定义资源中配置。此字段允许在共享 VPC 中引导机器。

```
...
providerSpec:
  ...
  networkInterfaces:
    - network: <infrastructureID>-network
      subnet: <infrastructureID>-<role>-subnet
      projectID: <projectID>
  ...
```

如需更多信息，请参阅 [BZ#1868751](#)。

1.8.14.1.2. 添加了 `credentialsMode` 参数以绕过不正确的 AWS 权限验证

对于 AWS 安装，OpenShift Container Platform 依赖于 AWS 策略模拟器 API 来验证权限。如果 AWS 帐户被配置为使用 AWS 机构服务控制策略（SCP），则会根据 SCP 中设置的策略检查权限。当 SCP 包含使用全局条件拒绝所有操作或需要特定权限的策略时，策略模拟器 API 无法正确验证权限。例如，带有条件的策略，比如 `us-east-1` 和 `us-west-2` 以外的所有区域，或者 `role-xyz` 以外的所有角色，都会导致 AWS API 返回 `false` 负数。当无法验证权限时，OpenShift Container Platform AWS 安装会失败，即使提供的凭证具有安装 OpenShift Container Platform 所需的权限。

在这个版本中，您可以通过在 `install-config.yaml` 配置文件中为 `credentialsMode` 参数设置值来绕过策略模拟器权限检查。

示例 `install-config.yaml` 配置文件

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

1 这一行被添加来将 `credentialsMode` 参数设置为 `Mint`。

为 `credentialsMode` 设置值会绕过配置为使用 SCP 的 AWS 帐户的权限检查，并允许安装继续进行。绕过此检查时，请确保您提供的凭证具有指定模式所需的权限。

`credentialsMode` 的值会更改 Cloud Credential Operator (CCO) 的行为，如下所示：

- **Mint** - CCO 使用提供的管理员级云凭证来运行安装程序。如果凭证在安装后没有被删除，它将被 CCO 存储并使用来处理集群中的 `CredentialsRequest` 自定义资源，并为每个用户创建新用户，每个用户具有特定的所需权限。
- **Passthrough** - CCO 使用提供的非管理员云凭证，这些凭证有足够的权限来执行安装来运行安装程序。有关查找正在安装的 OpenShift Container Platform 版本的 `CredentialsRequest` 自定义资源中指定的权限的更多信息，请参阅 [AWS 手动创建 IAM](#)。

1.8.14.2. 程序错误修复

- 在以前的版本中，会根据 Samples Operator 配置对象的 `ImageChangesInProgress` 条件而不是

Samples Operator 配置对象的 **SamplesExists** 条件报告间 API 服务器错误。当 API 服务器报告已安装所有样本时，Samples Operator 无法将 **Progressing** 条件切换为 **false**，因为 **ImageChangesInProgress** 条件中存在意外数据。这会导致升级被标记为不完整。此程序错误修复更新了 **SamplesExists** 条件，在 API 服务器上报告错误，因此如果 Samples Operator 升级时出现间隔 API 服务器错误，升级将不会阻断。(BZ#1857201)

- 在以前的版本中，**ironic-image** 容器配置缺少了设置来启用 **idrac-redfish-virtual-media** 引导驱动。因此，用户无法选择 Metal3 的 **idrac-virtual-media** 引导 URL。现在包括了缺少的 **ironic-image** 容器配置，因此用户可以选择 Metal3 的 **idrac-virtual-media** URL。(BZ#1859488)
- 在以前的版本中，Operand 表单数组和对象字段没有逻辑来检索和显示表单上的字段描述。因此，数组或对象类型字段的描述不会被呈现。现在，这个程序错误修复添加了在 Operand 创建表单上显示阵列和对象字段描述的逻辑。(BZ#1861433)
- 在以前的版本中，Buildah 会清除镜像上的镜像架构和 OS 字段。这会导致通用容器工具失败，因为生成的镜像无法识别其架构和操作系统。此程序错误修复可防止 Buildah 覆盖镜像和架构，除非有显式覆盖。这样可确保镜像始终具有架构和操作系统字段，且不会出现镜像不匹配警告。(BZ#1868401)
- 在以前的版本中，会发生重复的无效内存地址或 nil pointer 解引用错误，在运行 CoreDNS 1.6.6 时会包括 Kube API 访问超时。现在，这个问题可以通过正确处理 Endpoint Tombstones 错误来解决。现在，CoreDNS 的行为是不会重复的 panics。(BZ#1869309)
- 在以前的版本中，**BareMetalHost** 对象的控制器将状态数据镜像为注解，包括最新状态更新的时间戳。集群不需要这个设置。这可能会导致 **BareMetalHost** 对象进入一个连续流状态，受影响的 **BareMetalHost** 对象在协调之间可能存在较长的后退状态，以防止控制器解析 Kubernetes API。造成此问题的注解不再写入，这样就解决了这个问题。(BZ#1851531)
- 在以前的版本中，Cluster Version Operator (CVO) 没有同步 pod spec 中的 **shareProcessNamespace** 参数，这会导致 Registry Operator 不会更新 **shareProcessNamespace** 设置。CVO 现在同步 **shareProcessNamespace**、**DNSPolicy** 和 **TerminationGracePeriodSeconds**，修正 Registry Operator 更新问题。(BZ#1868478)

1.8.14.3. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.15. RHSA-2020:3578 - Moderate: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 9 月 8 日

OpenShift Container Platform 4.5 现在提供了 **cluster-network-operator-container**、**cluster-version-operator-container**、**elasticsearch-operator-container**、**logging-kibana6-container** 和 **ose-cluster-svc-cat-controller-manager-operator-container** 的更新。有关更新的详情请查看 [RHSA-2020:3578](#) 公告。

1.8.16. RHBA-2020:3618 - OpenShift Container Platform 4.5.9 程序错误修复更新

发布日期：2020 年 9 月 14 日

OpenShift Container Platform release 4.5.9 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3618](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3619](#) 公告提供。

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

OpenShift Container Platform 4.5.9 容器镜像列表

1.8.16.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.17. RHBA-2020:3719 - OpenShift Container Platform 4.5.11 程序错误修复更新

发布日期：2020 年 9 月 21 日

OpenShift Container Platform release 4.5.11 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3719](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3720](#) 公告提供。

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

OpenShift Container Platform 4.5.11 容器镜像列表

1.8.17.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.18. RHSA-2020:3780 - Moderate: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 9 月 21 日

OpenShift Container Platform 4.5 现在提供了 **ose-cluster-svcat-apiserver-operator-container** 的更新。有关更新的详情请查看 [RHSA-2020:3780](#) 公告。

1.8.19. RHBA-2020:3760 - OpenShift Container Platform 4.5.13 程序错误修复更新

发布日期：2020 年 9 月 30 日

OpenShift Container Platform release 4.5.13 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3760](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3761](#) 公告提供。

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

OpenShift Container Platform 4.5.13 容器镜像列表

1.8.19.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.20. RHSA-2020:3841 - Important: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 9 月 30 日

OpenShift Container Platform 4.5 现在提供了对 **jenkins** 的更新。有关更新的详情请查看 [RHSA-2020:3841](#) 公告。

1.8.21. RHSA-2020:3842 - Moderate: OpenShift Container Platform 4.5 安全更新

发布日期：2020 年 9 月 30 日

OpenShift Container Platform 4.5 现在提供了 **openshift-enterprise-console-container** 的更新。有关更新的详情请查看 [RHSA-2020:3842](#) 公告。

1.8.22. RHBA-2020:3843 - OpenShift Container Platform 4.5.14 程序错误修复更新

发布日期：2020 年 10 月 12 日

OpenShift Container Platform release 4.5.14 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3843](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3844](#) 公告提供。

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

OpenShift Container Platform 4.5.14 容器镜像列表

1.8.22.1. 程序错误修复

- 在这个版本中，每个日志记录级别的值都会包括在 **imageregistry** API 的 logging 字段中。
([BZ#1843244](#))
- 在以前的版本中，当从最新镜像恢复 pod 时，版本与数据库之间的不匹配有时会导致问题。在这个版本中，pod 的配置 YAML 文件被复制并带有备份，以避免造成不匹配的问题。
([BZ#1877930](#))
- 在以前的版本中，如果 pod 指向无效的镜像引用，修剪器作业会导致 Image Registry Operator 进入降级状态，这会阻止升级。要进行升级，用户需要删除导致此问题的 pod，并等待下一次修剪发生，或挂起修剪器作业。在这个版本中，添加了指标和警报来指示修剪器作业何时失败，修剪器状态不再影响 Operator 状态。
([BZ#1879176](#))
- 在以前的版本中，OpenShift Container Platform 4.5 分支中 Cluster DNS Operator 的 Kubernetes 依赖项已过时。在这个版本中，Cluster DNS Operator 的依赖项从 Kubernetes 0.18.0-rc2 更新至 v0.18.9。
([BZ#1880311](#))
- 在以前的版本中，OpenShift Container Platform 4.5 分支中 Cluster Ingress Operator 的 Kubernetes 依赖项已过时。在这个版本中，Cluster Ingress Operator 的依赖项从 Kubernetes 0.18.3 更新至 v0.18.9。
([BZ#1880315](#))
- 在以前的版本中，Kubernetes API 中的监视缓存是从全局修订版本 (**etcd**) 初始化的，并在没有更改时保留未定义的时间段。这个行为有时会导致客户端从发现较新的 RV 的服务器获取资源版本 (RV)，并因为网络错误而断开连接，并重新连接到后面的服务器，从而导致 "Too large resource version" 错误。在这个版本中，reflector 被修复，以便它可以从这些错误中恢复，使用 **client-go** 库从服务器获取通知的 Operator 可以在接收错误时恢复并进行操作。
这个问题已解决：**cluster-kube-apiserver-operator** ([BZ#1880322](#)) **cluster-kube-storage-version-migrator-operator** ([BZ#1880327](#))** **cluster-openshift-apiserver-operator** ([BZ#1880353](#))
- 在以前的版本中，无法创建新管道触发器，因为 Web 控制台与最新的 OpenShift Pipelines Operator 1.1 不兼容。此发行版本支持最新版本，并允许创建管道触发器。
([BZ#1880376](#))
- 在以前的版本中，Kubernetes 程序错误阻止 API 客户端在从 TCP 重置恢复后迅速恢复。当重新发生连接丢失时，客户端日志可能会出现 "Timeout: Too large resource version" 错误。这可能会导致维护到 API 服务器的客户端连接的控制台或 Operator 出现问题。在这个版本中，对

Kubernetes 程序错误的修复应用到 Samples Operator, Operator 不再容易受到这个错误消息循环的影响。(BZ#1881068)

- 在以前的版本中，不必要的 API VIP 移动会导致客户端连接错误。在这个版本中，API VIP 健康检查会限制其移动次数，从而减少错误。(BZ#1881147)

1.8.22.2. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.23. RHBA-2020:4228 - OpenShift Container Platform 4.5.15 程序错误修复更新

发布日期：2020 年 10 月 19 日

OpenShift Container Platform release 4.5.15 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:4228](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:4229](#) 公告提供。

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

[OpenShift Container Platform 4.5.15 容器镜像列表](#)

1.8.23.1. 程序错误修复

- 以后的 OpenShift Container Platform 版本中引入了一个新的 CSR API 版本，因此，旧的版本无法在升级过程中批准或拒绝证书。在这个版本中，旧版本的 `oc` 会容许 CSR 版本，以便可以针对将来的版本拒绝或批准 `oc` 4.5 的证书。(BZ#1860789)
- 在裸机环境中，`infra-dns` 容器在每个主机上运行，以支持节点名称解析和其他内部 DNS 记录。`NetworkManager` 脚本还会更新主机上的 `/etc/resolv.conf` 使其指向 `infra-dns` 容器。另外，当创建 pod 时，会从它们的主机接收 DNS 配置文件 (`/etc/resolv.conf` 文件)。如果在 `NetworkManager` 脚本更新主机上的 `/etc/resolv.conf` 文件前创建了 HAProxy pod，则该 pod 可能会重复失败，因为无法解析 `api-int` 内部 DNS 记录。在这个版本中更新了 Machine Config Operator (MCO)，它会验证 HAProxy pod 的 `/etc/resolv.conf` 文件是否与主机 `/etc/resolv.conf` 文件一致。因此，HAProxy Pod 不再会遇到这些错误。(BZ#1862874)
- 在以前的版本中，如果无法访问 control plane kubelet，但 pod 仍在运行，则在该节点上运行的机器 API pod 会重新调度到另一个节点上。这会创建多个 Machine API pod，它们与控制集群中的机器 API 资源有关。这可能导致创建太多的实例，以及 Machine API 控制器可能会泄漏实例，需要手动干预。在这个版本中，所有 Machine API 控制器都添加了领导选举机制，确保只有单个控制器实例可以管理机器 API 资源。如果每个控制器只有一个领导，过量实例将不再创建或泄漏。(BZ#1864352)
- 在以前的版本中，资源名称在编辑流中被更新，编辑应用程序用户无法更改 Git 存储库或更新应用程序。在这个版本中，编辑流中不再更新应用程序名称，编辑流程用户可以更改 Git 存储库并更新应用程序。(BZ#1877290)
- 在以前的版本中，Kubernetes API 中的监视缓存是从全局修订版本 (`etcd`) 初始化的，并在没有更改时保留未定义的时间段。这个行为可能会导致客户端从观察到较新的 RV 的服务器获取资源版本 (RV) 资源版本 (RV)，并因为网络错误与它断开连接，并重新连接到后面的服务器，从而导致 "Too large resource version" 错误。在这个版本中，reflector 被修复，它可以从 "Too large resource version" 错误中恢复，使用 `client-go` 库从服务器获取通知的 Operator 可以在接收 "Too large resource version" 错误时恢复并进行操作。(BZ#1877346)
- 在以前的版本中，当 Authentication Operator 从忽略 `Accept: application/json` 标头的 OpenID

Connect Authentication (OIDC) 服务器收到 HTML 有效负载时,OIDC 服务器可能会使用一个 HTML 页面响应,表示身份验证 Operator 无法解析,因为它希望使用 JSON。现在,Operator 会忽略错误,并不允许用于忽略标头的 OIDC 服务器的 CLI 登录。(BZ#1879417)

- 在以前的版本中,当 Image Registry Operator 遇到 "Too large resource version" 错误时,它无法从集群中获取事件。在这个版本中, **client-go** 库已被更新,它修复了反射器 (reflector) 以便 Operator 可以从 "Too large resource version" 错误中恢复。(BZ#1880314)
- Kubernetes 网络代理不支持多个集群 CIDR 来检测本地流量。如果在 OpenShift SDN 中配置了多个 CIDR, Cluster Network Operator (CNO) 会将 **KubeProxyConfiguration.clusterCIDR** 字段设置为空字符串。在 OpenShift Container Platform 4.4 及更早的版本中,空值被忽略,但在 4.5 及之后的版本中,传递一个空值会导致错误。因此,在从 4.4 升级到 4.5 后,如果 **sdn-config ConfigMap** 在 clusterCIDR 字段中有一个空字符串,则无法解析配置,SDN Pod 进入崩溃循环。在这个版本中,空值会被忽略,当配置了多个 CIDR 时 SDN Pod 不会崩溃。(BZ#1881830)

1.8.23.2. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本,请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.24. RHBA-2020:4268 - OpenShift Container Platform 4.5.16 程序错误修复更新

发布日期: 2020 年 10 月 26 日

OpenShift Container Platform release 4.5.16 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:4268](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:4269](#) 公告提供。

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

[OpenShift Container Platform 4.5.16 容器镜像列表](#)

1.8.24.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本,请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.25. RHSA-2020:4320 - Low: OpenShift Container Platform 4.5 安全更新

发布日期: 2020 年 10 月 26 日

OpenShift Container Platform 4.5 现在提供了 **openshift4/ose-machine-config-operator** 的更新。有关更新的详情请查看 [RHSA-2020:4320](#) 公告。

1.8.26. RHBA-2020:4325 - OpenShift Container Platform 4.5.17 程序错误修复更新

发布日期: 2020 年 11 月 5 日

OpenShift Container Platform release 4.5.17 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:4325](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:4326](#) 公告提供。

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

OpenShift Container Platform 4.5.17 容器镜像列表

1.8.26.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.27. RHBA-2020:4425 - OpenShift Container Platform 4.5.18 程序错误修复更新

发布日期：2020 年 11 月 10 日

OpenShift Container Platform release 4.5.18 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:4425](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:4426](#) 公告提供。

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

OpenShift Container Platform 4.5.18 容器镜像列表

1.8.27.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.28. RHBA-2020:5051 - OpenShift Container Platform 4.5.19 程序错误修复更新

发布日期：2020 年 11 月 17 日

OpenShift Container Platform release 4.5.19 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:5051](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:5052](#) 公告提供。

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

OpenShift Container Platform 4.5.19 容器镜像列表

1.8.28.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.29. RHSA-2020:5118 - Moderate: OpenShift Container Platform 4.5.20 程序错误修复和安全更新

发布日期：2020 年 11 月 24 日

OpenShift Container Platform release 4.5.20（包括 **golang** 的安全更新）现已正式发布。其程序错误修正列表包括在 [RHSA-2020:5118](#) 公告中。此更新中包括的 RPM 软件包由 [RHSA-2020:5119](#) 公告提供。

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

OpenShift Container Platform 4.5.20 容器镜像列表

1.8.29.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.30. RHSA-2020:5194 - Moderate: OpenShift Container Platform 4.5.21 程序错误修复和安全更新

发布日期：2020 年 12 月 1 日

OpenShift Container Platform release 4.5.21（包括 **openshift-enterprise-hyperkube** 的安全更新）现已正式发布。其程序错误修正列表包括在 [RHSA-2020:5194](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:5193](#) 公告提供。

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

[OpenShift Container Platform 4.5.21 容器镜像列表](#)

1.8.30.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.31. RHBA-2020:5051 - OpenShift Container Platform 4.5.22 程序错误修复更新

发布日期：2020 年 12 月 8 日

OpenShift Container Platform release 4.5.22 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:5250](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:5251](#) 公告提供。

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

[OpenShift Container Platform 4.5.22 容器镜像列表](#)

1.8.31.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.32. RHSA-2020:5359 - Moderate: OpenShift Container Platform 4.5.23 程序错误修复和安全更新

发布日期：2020 年 12 月 15 日

OpenShift Container Platform release 4.5.23 现已正式发布，其中包括 **kubernetes** 的安全更新。其程序错误修正列表包括在 [RHSA-2020:5359](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:5356](#) 公告提供。

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

[OpenShift Container Platform 4.5.23 容器镜像列表](#)

1.8.32.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.33. RHBA-2020:5468 - Moderate: OpenShift Container Platform 4.5.24 程序错误修复更新

发布日期：2020 年 12 月 21 日

OpenShift Container Platform release 4.5.24 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:5468](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:5469](#) 公告提供。

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

[OpenShift Container Platform 4.5.24 容器镜像列表](#)

1.8.33.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.34. RHBA-2021:0033 - OpenShift Container Platform 4.5.27 程序错误修复更新

发布日期：2021 年 1 月 19 日

OpenShift Container Platform release 4.5.27 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:0033](#) 公告中。此更新中包括的 RPM 软件包由 [RHSA-2021:0034](#) 公告提供。

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

[OpenShift Container Platform 4.5.27 容器镜像列表](#)

1.8.34.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.35. RHBA-2021:0175 - OpenShift Container Platform 4.5.28 程序错误修复更新

发布日期：2021 年 1 月 26 日

OpenShift Container Platform release 4.5.28 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:0175](#) 公告中。这个版本没有 RPM 软件包。

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

[OpenShift Container Platform 4.5.28 容器镜像列表](#)

1.8.35.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.36. RHBA-2021:0231 - OpenShift Container Platform 4.5.30 程序错误修复更新

发布日期：2021 年 2 月 2 日

OpenShift Container Platform release 4.5.30 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:0231](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2021:0232](#) 公告提供。

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

[OpenShift Container Platform 4.5.30 容器镜像列表](#)

1.8.36.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.37. RHSA-2021:0313 - OpenShift Container Platform 4.5.31 程序错误修复和安全更新

发布日期：2021 年 2 月 9 日

OpenShift Container Platform release 4.5.31 现已正式发布。其程序错误修正列表包括在 [RHSA-2021:0313](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2021:0314](#) 公告提供。

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

[OpenShift Container Platform 4.5.31 容器镜像列表](#)

1.8.37.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.38. RHSA-2021:0428 - OpenShift Container Platform 4.5.33 程序漏洞修复和安全更新

发布日期：2021 年 3 月 3 日

OpenShift Container Platform release 4.5.33 现已正式发布。其程序错误修正列表包括在 [RHSA-2021:0428](#) 公告中。此更新中包括的 RPM 软件包由 [RHSA-2021:0429](#) 公告提供。

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

[OpenShift Container Platform 4.5.33 容器镜像列表](#)

1.8.38.1. 功能

1.8.38.1.1. Insights Operator 的改进

在这个版本中，Insights Operator 会从 **MachineConfigPools** 集群收集信息。这个信息对故障排除非常有用。如需更多信息，请参阅 [BZ#1887763](#)。

1.8.38.2. 程序错误修复

- 在以前的版本中，不正确的 OVN-kubernetes 安全规则会阻断某些入站连接。在试图连接到一个 pod 时，在极为罕见的情况下可能会失败。在这个版本中，iptables 会阻止预定的连接，这会导致没有错误的故障。（[BZ#1921283](#)）
- 在以前的版本中，Kubernetes API 中的监视缓存是从全局修订版本（etcd）初始化的，并在没有更改时保留未定义的时间段。这个行为有时会导致客户端从发现较新的 RV 的服务器获取资源版本（RV），并因为网络错误而断开连接，并重新连接到后面的服务器，从而导致 **Timeout: Too large resource version** 错误。在这个版本中，reflector 被修复，以便它可以从这些错误中恢复，使用 **client-go** 库从服务器获取通知的 Operator 可以在接收错误时恢复并进行操作。（[BZ#1877346](#)）
- 在以前的版本中，尝试写入 nil writer 可能会导致 **invalid memory address** 或 **nil pointer dereference** 错误。共享同一写者实例可能也会导致 **index out of range [43] with length 30 and recovered from err index > windowEnd** 错误。在这个版本中，kube-apiserver 的 **SerializeObject** 函数中的数据竞争问题已被修复。（[BZ#1879208](#)）
- 在以前的版本中，当从内存中修剪记录时，会错误地放置阵列索引，从而导致过量内存使用，且无法从归档中删除旧报告。在这个版本中，更改了数组索引键，以便修剪可以成功从内存中删除记录，而不会造成过量内存用量。（[BZ#1894243](#)）
- 在以前的版本中，Red Hat Enterprise Linux CoreOS（RHCOS）在 kernel-rt 软件包中使用 stage repo 位置。因此，kernel-rt 软件包将不会与 vanilla 内核软件包同步。在这个版本中，RHCOS 构建配置更改为使用 production 仓库位置，该位置可正确将 kernel-rt 软件包与 vanilla 内核软件包同步。（[BZ#1922262](#)）

1.8.38.3. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.39. RHBA-2021:0714 - OpenShift Container Platform 4.5.34 程序错误修复和安全更新

发布日期：2021 年 3 月 10 日

OpenShift Container Platform release 4.5.34 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:0714](#) 公告中。此更新中包括的 RPM 软件包由 [RHSA-2021:0713](#) 公告提供。

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

[OpenShift Container Platform 4.5.34 容器镜像列表](#)

1.8.39.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.40. RHSA-2021:0785 - OpenShift Container Platform 4.5.35 程序漏洞修复和安全更新

发布日期：2021年3月17日

OpenShift Container Platform 4.5.35 现已正式发布。其程序错误修正列表包括在 [RHSA-2021:0785](#) 公告中。此更新中包括的 RPM 软件包由 [RHSA-2021:0786](#) 公告提供。

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

[OpenShift Container Platform 4.5.35 容器镜像列表](#)

1.8.40.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.41. RHBA-2021:0840 - OpenShift Container Platform 4.5.36 程序错误修复更新

发布日期：2021年3月24日

OpenShift Container Platform release 4.5.36 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:0840](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2021:0841](#) 公告提供。

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

[OpenShift Container Platform 4.5.36 容器镜像列表](#)

1.8.41.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.42. RHBA-2021:1015 - OpenShift Container Platform 4.5.37 程序错误修复和安全更新

发布日期：2021年4月12日

OpenShift Container Platform release 4.5.37 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:1015](#) 公告中。此更新中包括的 RPM 软件包由 [RHSA-2021:1016](#) 公告提供。

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

[OpenShift Container Platform 4.5.37 容器镜像列表](#)

1.8.42.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.43. RHBA-2021:1300 - OpenShift Container Platform 4.5.38 程序错误修复更新

发布日期：2021年4月28日

OpenShift Container Platform release 4.5.38 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:1300](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2021:1302](#) 公告提供。

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

[OpenShift Container Platform 4.5.38 容器镜像列表](#)

1.8.43.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.44. RHBA-2021:1491 - OpenShift Container Platform 4.5 程序漏洞修复更新

发布日期：2021 年 5 月 13 日

OpenShift Container Platform release 4.5→ 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:1491](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2021:1492](#) 公告提供。

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

[OpenShift Container Platform 4.5→ 容器镜像列表](#)

1.8.44.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

1.8.45. RHBA-2021:2056 - OpenShift Container Platform 4.5.40 程序错误修复和安全更新

发布日期：2021 年 5 月 26 日

OpenShift Container Platform release 4.5.40 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:2056](#) 公告中。此更新中包括的 RPM 软件包由 [RHSA-2021:2057](#) 公告提供。

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

[OpenShift Container Platform 4.5.40 容器镜像列表](#)

1.8.45.1. 升级

要将现有 OpenShift Container Platform 4.5 集群升级到此最新版本，请参阅[使用 CLI 更新集群以获取相关说明](#)。

第 2 章 OPENSIFT CONTAINER PLATFORM 版本政策

OpenShift Container Platform 对所有支持的 API 提供了严格的后向兼容保证，但这不包括 alpha API（这些 API 可能会在不通知的情况下被改变），以及 beta API（这些 API 偶尔可能会被改变且不保证后向兼容）。

红帽没有公开发布 OpenShift Container Platform 4.0，而是在版本 3.11 后直接发布了 OpenShift Container Platform 4.1。

master 主机和节点（node）主机使用的 OpenShift Container Platform 版本必须相互匹配（在集群升级过程中出现的临时不匹配除外）。例如，在一个 4.5 集群中，所有的 master 必需是 4.5，所有节点也必需是 4.5。如果安装了旧版本的 **oc**，则无法使用 OpenShift Container Platform 4.5 中的所有命令。您需要下载并安装新版本的 **oc**。

因为非安全的原因改变 API 将会最少涉及到 2 个次发行版本（例如，4.1 到 4.2 到 4.3）来更新旧的 **oc**。一些新功能可能需要新版本的 **oc**。一个 4.3 版本的服务器可能会带有版本 4.2 的 **oc** 不能使用的功能，而一个版本为 4.3 的 **oc** 也可能会带有不被版本 4.2 服务器支持的功能。

表 2.1. 兼容性列表

	X.Y (oc Client)	X.Y+N footnote:versionpolicyn[其中 N 是一个大于 1 的值。] (oc Client)
X.Y (Server)	1	3
X.Y+N footnote:versionpolicyn[] (Server)	2	1

- 1 完全兼容。
- 2 **oc** 客户端可能无法访问服务器的功能。
- 3 **oc** 客户端可能会包括与要访问的服务器不兼容的选项和功能。