



OpenShift Container Platform 4.4

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 4.4 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 4.4 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	10
1.4. 弃用和删除的功能	10
1.5. 程序错误修复	19
1.6. 技术预览功能	27
1.7. 已知问题	30
1.8. 异步勘误更新	33
第 2 章 OPENSIFT CONTAINER PLATFORM 版本政策	58

第 1 章 OPENSIFT CONTAINER PLATFORM 4.4 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 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-2020:0581) 现已发布。此发行版本使用 [Kubernetes 1.17](#) 和 CRI-O 运行时。OpenShift Container Platform 4.4 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 4.4.0，而是直接发布了 OpenShift Container Platform 4.4.3 作为正式发行版本 (GA)。

OpenShift Container Platform 4.4 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 Container Platform 集群。

OpenShift Container Platform 4.4 需要运行在 Red Hat Enterprise Linux 7.6 及更新的版本，或 Red Hat Enterprise Linux CoreOS 4.4 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 Red Hat Enterprise Linux 7.6 及更新的版本。



重要

因为当前只支持使用 Red Hat Enterprise Linux 7.6 或更新的次版本作为 compute 系统，所以不能把使用 Red Hat Enterprise Linux 的 compute 系统升级到版本 8。

随着 OpenShift Container Platform 4.4 的发布，版本 4.1 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. 使用用户置备的基础架构在 Microsoft Azure 上安装集群

OpenShift Container Platform 4.4 支持使用用户置备的基础架构在 Azure 上安装集群。在 Azure 上运行用户置备的基础架构可让您自定义您的环境，如规范、安全以及操作控制。

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

详情请参阅[在使用 ARM 模板的 Azure 上安装集群](#)。

1.2.1.2. 使用安装程序置备的基础架构在 Red Hat Virtualization 上安装集群

OpenShift Container Platform 4.4 支持使用安装程序置备的基础架构在 Red Hat Virtualization (RHV) 上安装集群。

如需更多信息，请参阅 [在 RHV 上快速安装集群](#)。

1.2.1.3. 使用用户置备的基础架构在 OpenStack 上安装集群

OpenShift Container Platform 4.4 支持在您自己提供的基础架构中运行的 Red Hat OpenStack Platform (RHOSP) 上安装集群。通过利用您自己的基础架构，您可以将集群与现有的基础架构进行集成。例如，您需要创建所有 RHOSP 资源，如 Nova 服务器、Neutron 端口和安全组。红帽提供了 Ansible playbook 来帮助您完成部署过程。

您还可以使用自己的基础架构在带有 Kuryr 的 RHOSP 上安装集群。

如需更多信息，请参阅 [在您自己的基础架构的 OpenStack 上安装集群](#) 或 [在您自己的基础架构的带有 Kuryr 的 OpenStack 上安装集群](#)。

1.2.1.4. 在 OpenStack 上安装集群不再需要 Swift 对象存储服务

从版本 4.4 开始，OpenShift Container Platform 不再需要 RHOSP 云中存在 Swift 对象存储服务。如果 OpenShift Container Platform 中没有包括 Swift，安装程序将使用 Cinder 块存储和 Glance 镜像 registry 服务。

如需更多信息，请参阅 [使用您自己的基础架构在 OpenStack 上安装集群](#)。

1.2.1.5. 在 OpenStack 中安装的集群支持自签名证书

OpenShift Container Platform 4.4 现在可以在使用自签名证书进行授权的 RHOSP 云中安装。

如需更多信息，请参阅 [使用您自己的基础架构在 OpenStack 上安装集群](#)。

1.2.1.6. OpenStack 通过检查 sha256 checksum 来验证 RHCOS 镜像

现在，在 RHOSP 上安装程序会对 Red Hat Enterprise Linux CoreOS (RHCOS) 镜像执行自动 checksum 验证。

1.2.1.7. 支持在带有 Kuryr 的 OpenStack 上使用 OVN 负载均衡的 east-west 流量

在 RHOSP 16 上使用 Kuryr 的 OpenShift Container Platform 安装现在可以使用 OVN 负载均衡供应商驱动程序而不是 Amphora 驱动程序。如果在环境中存在 OVN 和 OVN Octavia 驱动程序，则会自动使用 OVN。这样，可以提高负载均衡器的性能和资源使用率。另外，每个服务都需要一个负载均衡器虚拟机的要求也已被取消。

1.2.1.8. 4.4 发行版本的升级频道

对于已切换到 **fast-4.4** 频道的集群，在 GA 时将可以将最新的 OpenShift Container Platform 4.3.z 升级到 4.4。来自 **fast-4.4** 频道的早期适配器的 Telemetry 数据会被监测以决定在什么时候把升级推广到 **stable-4.4** 频道。这种监测过程需要进行广泛的企业级测试，因此可能需要几周时间。

1.2.2. 安全性

1.2.2.1. 绑定服务帐户令牌的支持

OpenShift Container Platform 4.4 支持绑定服务帐户令牌，它可以提高与云供应商身份访问管理 (IAM) 服务（如 AWS IAM）集成的能力。

如需更多信息，请参阅 [使用绑定服务帐户令牌](#)。

1.2.2.2. **oauth-proxy** 镜像流现在可用

OpenShift Container Platform 4.4 为第三方身份验证集成引入了 **oauth-proxy** 镜像流。您不应该再使用 Red Hat Registry 中的 **oauth-proxy** 镜像。如果您以 OpenShift Container Platform 4.4 或更高版本的集群为目标，则应使用 **openshift/oauth-proxy:v4.4** 镜像流。这可以保证后向兼容，并允许您添加镜像流触发器来获得重要的修复。**v4.4** 标签至少可用于后续的 3 个 OpenShift Container Platform 次要发行版本。每个次要发行版本还会生成自己的标签。

1.2.2.3. **kube-apiserver** 会在检查令牌前先检查客户端证书

在以前的 OpenShift Container Platform 版本中，**kube-apiserver** 在检查客户端证书前会先检查令牌。现在，**kube-apiserver** 会在检查令牌前先检查客户端证书。

例如，如果您在以前的 OpenShift Container Platform 版本中有 **system:admin** kubeconfig 并运行 **oc --token=foo get pod** 命令，它将被验证为以带有令牌 **foo** 的用户。现在，它被验证为 **system:admin**。以前的版本建议使用参数 **--as** 来模拟用户，而不是在使用客户端证书时覆盖令牌；这已不再需要。

1.2.3. 节点

1.2.3.1. 使用 **descheduler** 驱除 pod（技术预览）

Descheduler 提供了驱除正在运行的 pod 的功能，以便可将 pod 重新调度到更合适的节点上。

在以下情况下，适用于取消调度（deschedule）pod：

- 节点使用不足或过度使用。
- Pod 和节点关联性要求（如污点或标签）已更改，并且原始的调度不再适合于某些节点。
- 节点失败需要移动 pod。
- 集群中添加了新节点。

如需更多信息，请参阅 [使用 descheduler 来驱除 pod](#)。

1.2.3.2. 在节点上控制过量使用和管理容器密度

OpenShift Container Platform 管理员现在可以控制过量使用的程度，并管理节点上的容器密度。您可以使用 Cluster Resource Override Operator 配置集群一级的过量使用，以覆盖开发人员容器上设置的请求和限制之间的比例。

如需更多信息，请参阅 [配置集群以将 pod 放置到过量使用的节点上](#)。

1.2.4. 集群监控

1.2.4.1. 在 web 控制台中监控 Dashboard

现在，web 控制台中的 **Monitoring** 部分包括了 **Dashboards** 视图。这样，您可以方便地查看 OpenShift Container Platform 集群及其依赖组件的相关指标数据。

1.2.4.2. node-exporter 中禁用了 hwmon 收集器

在 node-exporter 监控组件中禁用了 **hwmon** 收集器，因为它已不再用于收集集群指标数据。

1.2.4.3. cluster-reader 可以读取节点指标数据

现在，在默认情况下，**cluster-reader** 角色可以读取节点指标数据。

1.2.4.4. 当多个容器被终止时会有集群警报

当因为内存问题导致多个容器在 15 分钟内被终止时，您会接收到一个 **MultipleContainersOOMKilled** 警报信息。

1.2.4.5. 新的 API 服务器警报

OpenShift Container Platform 4.4 有两个新的 API 服务器警报：

- **ErrorBudgetBurn**: 当 API 服务器有 **5xx** 请求响应时触发。
- **AggregatedAPIErrors**: 当聚合 API 服务器的错误数增加时触发。

1.2.4.6. Prometheus Operator 的权限更新

由 Prometheus Operator 管理的自定义资源定义 (CRD) 现在具有更严格的权限。

Prometheus Operator 所管理的自定义资源 (CR) 包括：

- **Prometheus**
- **ServiceMonitor**
- **PodMonitor**
- **Alertmanager**
- **PrometheusRule**

1.2.4.7. Cluster 监控 (monitoring) 组件版本更新

以下监控组件已升级：

- Prometheus: 从 2.14.0 升级到 2.15.2
- Alertmanager: 从 0.19.0 升级到 0.20.0
- Prometheus Operator: 从 0.34.0 升级到 0.35.1
- kube-state-metrics: 从 1.8.0 升级到 1.9.5
- Grafana: 从 6.4.3 升级到 6.5.3

1.2.5. Web 控制台

1.2.5.1. OperatorHub 中的 IBM Marketplace 集成

IBM Marketplace 现在与 OperatorHub 集成，该 OperatorHub 位于 OpenShift Container Platform Web 控制台中。此集成功能允许您在 OperatorHub 接口的 IBM Marketplace 上安装和管理托管的 Operator。

1.2.5.2. 在 Topology 视图中编辑应用程序

现在，您可以使用 Topology 视图从 Developer 视角编辑应用程序。

1.2.5.3. 创建 Helm 发行版本

您现在可以通过 Helm chart 来创建 Helm 发行版本，Helm chart 由 Developer Catalog 提供。

1.2.6. 网络

1.2.6.1. OpenShift Container Platform 上的流控制传输协议 (SCTP)

SCTP 是基于信息的可靠协议，可在 IP 网络之上运行。启用后，您可以使用 SCTP 作为带有 pod 和服务的协议。如需更多信息，请参阅 [使用 SCTP](#)。

1.2.6.2. 使用 DNS 转发

您可以针对一个区 (zone)，使用 DNS 转发来覆盖转发默认配置，方法是每个区中指定需要使用的域名解析服务器。

如需更多信息，请参阅 [使用 DNS 转发](#)。

1.2.6.3. HAProxy 升级至版本 2.0

用于入口的 HAProxy 从 1.8.17 更新至 2.0.13。此升级没有为 OpenShift Container Platform 引入新的 API 或支持的用户支持功能。这个升级提供了显著的性能改进，并对一些程序错误进行了修复。HAProxy 2.0 还添加了原生 Prometheus 指标数据，并在配置了其他 OpenShift Container Platform 组件来支持它时提供完整的 IPv6 支持。

1.2.6.4. Ingress 增强

OpenShift Container Platform 4.4 中对 **Ingress** 对象引入了两个值得注意的改进：

- **Ingress** 对象获取了 [Route 准入策略 API](#)：允许您在具有相同域名的多个命名空间中运行应用程序。
- **Ingress** 对象可以被 [NodePort 服务公开](#)：有助于集成现有的负载均衡器，以便对您的负载均衡解决方案拥有精细的控制。

1.2.7. 存储

1.2.7.1. 使用 CSI 快照的持久性存储（技术预览）

现在，您可以使用 Container Storage Interface (CSI) 来创建、恢复和删除卷快照。在技术预览中默认启用这个功能。

如需更多信息，请参阅 [使用 CSI 卷快照](#)。

1.2.7.2. 使用 CSI 克隆的持久性存储（技术预览）

现在，您可以在存储卷被创建后，使用 Container Storage Interface (CSI) 来克隆它们。在技术预览中默认启用这个功能。

如需更多信息，请参阅[使用 CSI 卷克隆](#)。

1.2.8. 扩展

1.2.8.1. 集群最大限制

针对 OpenShift Container Platform 4.4 的[集群最大限制](#)指导信息已更新。

4.4 测试的每个节点上最多的 pod 数量为 500。

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

1.2.9. 开发者体验

1.2.9.1. 自动镜像修剪

现在，您可以启用自动镜像修剪。这个功能在默认情况下不启用。在安装或升级到 OpenShift Container Platform 4.4 后会收到启用这个功能的选项通知。这由 Image Registry Operator 管理，它创建一个 CronJob 来运行定期镜像修剪。

1.2.9.2. 构建对象报告状态条件

每个现有的 OpenShift Container Platform 构建阶段均添加了构建条件。这些条件包含构建期间构建的信息。您可以使用 `oc wait` 命令来等待到达特定构建阶段。

1.2.9.3. 为镜像 registry 重新创建推出部署 (rollout)

现在，在部署镜像 registry 时可以使用 **Recreate** rollout 策略。这样，您就可以使用 **ReadWriteOnce** 持久性卷，如 AWS Elastic Block Store。在使用这些存储类型时，您必须使用 **Recreate** rollout 策略来成功升级 OpenShift Container Platform 集群。

1.2.9.4. odo 增强

`odo` 有几个与用户体验相关的改进和增强：

- 现在，可以使用 `odo debug info` 命令。
- 现在，`odo url` 命令带有一个 `--secure` 标记用来指定 HTTPS URL。
- 现在，`odo create`、`odo url` 和 `odo config` 命令都有一个 `--now` 标记来马上在集群中应用改变。
- 现在，如果默认端口被占用，`odo debug port-forward` 命令会自动选择一个端口。
- 现在，`odo storage` 和 `odo push` 命令的输出已被重新安排，以使用户阅读。
- 现在，提供了一个实验模式，您可以在其中使用技术预览功能，比如使用 `devfile` 创建应用程序。
- 技术预览功能 - 现在提供对 `devfile` 的支持。如需了解更多相关信息，请参阅 [odo 发行注记](#)。

1.2.9.5. OpenShift Pipelines (技术预览)

OpenShift Pipelines 使用 Tekton 自定义资源 (CR) 为自动化部署创建可扩展的 CI/CD 解决方案。这些 CR 充当编译 Pipeline 的构建块。OpenShift Pipelines 提供了一个可重复使用的任务目录，用于轻松构建 Pipelines。每个 Pipeline 在隔离容器中运行，无需维护 CI 服务器，且可移植到多个平台。

1.2.9.6. Helm 3 GA 支持

helm 是 Kubernetes 和 OpenShift Container Platform 应用程序的软件包管理器。它使用名为 Helm charts 的打包格式来简化应用程序和服务的定义、安装和升级。

Helm CLI 由 OpenShift Container Platform 构建并提供，可在 Web 控制台的 CLI 菜单中下载。

1.2.10. Operator

1.2.10.1. etcd 集群 Operator

OpenShift Container Platform 4.4 引入了 etcd 集群 Operator，它处理 etcd 扩展和置备 etcd 依赖项（如 TLS 证书）。etcd 集群 Operator 可简化灾难恢复流程，以便恢复到以前的集群状态，自动添加 etcd 成员，提供更准确的 etcd 成员健康报告，以及报告事件，以帮助调试 etcd 集群。

在这个版本中，以下灾难恢复脚本的名称已改变：

- **etcd-snapshot-backup.sh** 现在是 **cluster-backup.sh**。
- **etcd-snapshot-restore.sh** 现在是 **cluster-restore.sh**。

如需更多信息，请参阅[关于灾难恢复](#)。

1.2.10.2. Insights Operator 现在收集匿名 CSR

在这个版本中，Insights Operator 会定期收集匿名证书签名请求 (CSR) 来识别没有在 Kubernetes 中验证或未批准的 CSR。另外，Insights Operator 会在证书有效时收集数据。这有助于改进 OpenShift Container Platform 客户支持体验。

1.2.10.3. 如果无法连接到 registry.redhat.io，则删除 Samples Operator

如果 Samples Operator 在安装过程中无法连接到 **registry.redhat.io**，则不会创建示例镜像流。这可确保示例内容安装不会导致 OpenShift Container Platform 集群安装失败。

如果集群安装过程中出现这个问题，您可以[配置备用或镜像 registry](#)。

1.2.11. 文档更新及惯例

1.2.11.1. OpenShift Container Platform 文档使用 Apache 许可证 2.0

OpenShift Container Platform 文档现在根据 [Apache 许可证 2.0](#) 被授权。之前，它使用 Creative Commons Attribution-ShareAlike 3.0 Unported 许可证授权。

1.2.11.2. docs.openshift.com 站点的复制按钮

docs.openshift.com 上的所有代码块现在都提供了一个复制按钮，可让您将代码块中的所有文本复制到您机器的剪贴板中。客户门户网站版本的 OpenShift Container Platform 文档不提供此功能。

1.2.11.3. OpenShift Container Engine 重命名为 OpenShift Kubernetes Engine

红帽已决定把 Red Hat OpenShift Container Engine 重命名为 Red Hat OpenShift Kubernetes Engine，以便更好地沟通所提供的产品价值。如需更多信息，请参阅 [关于 OpenShift Kubernetes Engine](#)。

1.2.11.4. 现在，针对 Azure Red Hat OpenShift 的 4.3 版本提供了相关文档

这个新版本由红帽和 Microsoft 共同管理、支持和记录：

- [Microsoft 文档](#)
- [红帽文档](#)

1.3. 主要的技术变化

OpenShift Container Platform 4.4 包括以下显著的技术更改。

使用 Fluentd syslog 插件 (RFC 3164) 发送集群日志

由于 OpenShift Container Platform 4.3 中使用 Log Forwarding 功能进行了更改，您无法再使用 Fluentd syslog 插件将日志转发到外部 syslog 服务器。在 OpenShift Container Platform 4.4 中，这个功能已被恢复，您可以使用 syslog 插件。配置插件的步骤在 OpenShift Container Platform 版本 4.4 和版本 4.2 中有所不同。如需更多信息，请参阅使用 [Fluentd syslog 插件 \(RFC 3164\) 发送日志](#)。

Operator SDK v0.15.0

OpenShift Container Platform 4.4 支持 Operator SDK v0.15.0，它包括以下显著的技术改变：

- `olm-catalog gen-csv` 子命令现已改为 `generate csv` 子命令。
- `up local` 子命令现已改为 `run --local` 子命令。

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 4.4 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
- **-:** 已删除

表 1.1. 过时和删除的功能

功能	OCP 4.2	OCP 4.3	OCP 4.4
Service Catalog	DEP	DEP	DEP
Template Service Broker	DEP	DEP	DEP
OpenShift Ansible Service Broker	DEP	DEP	-
OperatorSources	DEP	DEP	DEP
CatalogSourceConfigs	DEP	DEP	DEP
Operator Framework 的软件包清单格式	GA	GA	DEP
System Containers for Docker, CRI-O	-	-	-
Hawkular 代理	-	-	-
Pod 预设置	-	-	-
Audit 策略	-	-	-
集群的 MongoDB 模板	-	-	-
集群的 MySQL 模板	-	-	-
CephFS 置备程序	-	-	-
Manila 置备程序	-	-	-

1.4.1. 已弃用的功能

1.4.1.1. OpenShift CLI config 标志

在 `oc` 命令中使用 `--config` 标志已被弃用。现在需要使用 `--kubeconfig` 标志。

1.4.1.2. OpenShift CLI timeout 标志

在 `oc rsh` 命令中使用 `--timeout` 标志已被弃用。现在需要使用 `--request-timeout` 标志。

1.4.1.3. OpenShift 编辑器

`OS_EDITOR` 已弃用。现在需要使用 `KUBE_EDITOR` 或 `EDITOR`。

1.4.1.4. machineCIDR 网络参数

在 `install-config.yaml` 文件中使用 `machineCIDR` 网络参数现已弃用。您应该使用 `machineNetwork.cidr`。

1.4.1.5. Service Catalog、Template Service Broker、Ansible Service Broker 以及它们的 Operator



注意

默认情况下，OpenShift Container Platform 4 不安装 Service Catalog。

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。

Ansible Service Broker、Ansible Service Broker Operator 和以下 APB 现已从 OpenShift Container Platform 4.4 中删除：

- APN 基础镜像
- APB 工具容器
- PostgreSQL APB
- MySQL APB
- MariaDB APB

以下相关的 API 也被删除：

- **.automationbroker.io/v1alpha1**
- **.osb.openshift.io/v1**

Service Catalog、Template Service Broker 以及以下相关的 API 将在以后的 OpenShift Container Platform 发行版本中移除。

- **.servicecatalog.k8s.io/v1beta1**

如果在 4.4 中启用了这些功能，Web 控制台会警告集群管理员这些功能仍处于启用状态。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**

现在，**service-catalog-controller-manager** 和 **service-catalog-apiserver** 集群 Operator 还会在 4.4 中被设置为 **Upgradeable=false**。这意味着，如果集群将来仍被安装，它们将阻断升级到下一个次版本，如 4.5。但是，升级到 z-stream 发行本版本（如 4.4.z）仍被允许。

如果安装了 Service Catalog，集群管理员可在发布下一个 OpenShift Container Platform 次要版本前看到 [Uninstalling Service Catalog](#) 来卸载它。

1.4.1.6. OperatorSources、CatalogSourceConfig 和打包格式已弃用。

OperatorSources 和 **CatalogSourceConfigs** 对象已从 OperatorHub 中弃用。以后的发行版本会删除以下相关的 API：

- **operatorsources.operators.coreos.com/v1**

- `catalogsourceconfigs.operators.coreos.com/v2`
- `catalogsourceconfigs.operators.coreos.com/v1`

Operator Framework 的当前打包格式 *Package Manifest Format* 在此版本中已被弃用，在以后的版本中它将被新的 *捆绑格式 (Bundle Format)* 替代。因此，`oc adm catalog build` 命令也被弃用，它使用较老的、已弃用的 *Package Manifest Format* 构建目录。

如需有关即将推出的 Bundle Format 和 `opm` CLI 的更多信息，请参阅 [上游社区的 OKD 文档](#)。

1.4.1.6.1. 转换自定义 `OperatorSources` 和 `CatalogSourceConfigs` 对象

如果 OpenShift Container Platform 4.4 集群中存在任何自定义 `OperatorSources` 或 `CatalogSourceConfigs` 对象，则 `marketplace` 集群 Operator 现在会设置一个 `Upgradeable=false` 条件并发出一个 `Warning` 警报。这意味着，如果集群将来仍被安装，它将阻断升级到下一个次版本，如 4.5。然而，升级到 z-stream 发行本，如 4.4.z，仍被允许。

集群管理员可以转换自定义 `OperatorSource` 或 `CatalogSourceConfigs` 对象，以直接使用 `CatalogSource` 对象清除此警报：

流程

1. 删除您的自定义 `OperatorSource` 或 `CatalogSourceConfigs` 对象。
 - a. 在所有命名空间中搜索 `OperatorSource` 或 `CatalogSourceConfigs` 对象：

```
$ oc get opsrc --all-namespaces
$ oc get csc --all-namespaces
```

- b. 从所有相关命名空间中删除所有自定义对象：

```
$ oc delete opsrc <custom_opsrc_name> -n <namespace>
$ oc delete csc <custom_csc_name> -n <namespace>
```



重要

不要删除 `openshift-marketplace` 命名空间中的默认 `OperatorSources` 对象：`redhat-operators`、`community-operators`、`certified-operators` 和 `redhat-marketplace`。但它们如果被意外删除就会启动。

2. 使用受限网络文档中 [构建 Operator 目录镜像](#) 的步骤来创建和推送新的目录镜像，并在 `oc adm catalog build` 命令步骤中进行以下更改：
 - 将 `--appregistry-org` 更改为 App Registry 实例上的命名空间，例如在 [Quay.io](#) 上。
 - 将 `--to` 改为您的镜像存储库标签，该标签应用于构建的目录镜像并推送。

例如：

```
$ oc adm catalog build \
  --appregistry-org <namespace> \
  --from=registry.redhat.io/openshift4/ose-operator-registry:v4.4 \
  --to=quay.io/<namespace>/<catalog_name>:<tag> \
  [-a ${REG_CREDS}]
```



注意

oc adm catalog build 命令已弃用，但弃用的功能仍被支持。

3. 将 **CatalogSource** 对象应用到集群以引用新目录镜像：

```
cat <<EOF | oc apply -f -
apiVersion: operators.coreos.com/v1alpha1
kind: CatalogSource
metadata:
  name: my-operator-catalog
  namespace: openshift-marketplace
spec:
  sourceType: grpc
  image: quay.io/<namespace>/<catalog_name>:<tag> ❶
  displayName: My Operator Catalog
  updateStrategy:
    registryPoll: ❷
    interval: 30m
EOF
```

- ❶ 指定您的自定义 Operator 目录镜像。
- ❷ **CatalogSource** 对象现在可以自动检查新版本以保持最新。

1.4.2. 删除的功能

1.4.2.1. OpenShift CLI secrets 子命令

OpenShift Container Platform 3.9 中弃用的以下 **oc secrets** 子命令不再可用：

- **new**
- **new-basicauth**
- **new-dockercfg**
- **new-sshauth**

您必须使用 **oc create secret** 命令替代。

1.4.2.2. OpenShift CLI build-logs 命令

oc build-logs 命令在 OpenShift Container Platform 3.11 中已弃用，现已被删除。您必须使用 **oc logs** 替代。

1.4.2.3. 已删除过时的上游 Kubernetes 指标

已删除所有过时的上游 Kubernetes 指标。删除指标的完整列表如下。

Kubelet 指标

- **kubelet_pod_worker_latency_microseconds**

- **kubelet_pod_start_latency_microseconds**
- **kubelet_cgroup_manager_latency_microseconds**
- **kubelet_pod_worker_start_latency_microseconds**
- **kubelet_pleg_relist_latency_microseconds**
- **kubelet_pleg_relist_interval_microseconds**
- **kubelet_runtime_operations**
- **kubelet_runtime_operations_latency_microseconds**
- **kubelet_runtime_operations_errors**
- **kubelet_eviction_stats_age_microseconds**
- **kubelet_device_plugin_registration_count**
- **kubelet_device_plugin_alloc_latency_microseconds**
- **kubelet_network_plugin_operations_latency_microseconds**

调度程序指标

- **scheduler_e2e_scheduling_latency_microseconds**
- **scheduler_scheduling_algorithm_predicate_evaluation**
- **scheduler_scheduling_algorithm_priority_evaluation**
- **scheduler_scheduling_algorithm_preemption_evaluation**
- **scheduler_scheduling_algorithm_latency_microseconds**
- **scheduler_binding_latency_microseconds**
- **scheduler_scheduling_latency_seconds**

API 服务器指标

- **apiserver_request_count**
- **apiserver_request_latencies**
- **apiserver_request_latencies_summary**
- **apiserver_dropped_requests**
- **apiserver_storage_data_key_generation_latencies_microseconds**
- **apiserver_storage_transformation_failures_total**
- **apiserver_storage_transformation_latencies_microseconds**
- **apiserver_proxy_tunnel_sync_latency_secs**

Docker 指标

- **kubelet_docker_operations**
- **kubelet_docker_operations_latency_microseconds**
- **kubelet_docker_operations_errors**
- **kubelet_docker_operations_timeout**

Reflector 指标

- **reflector_items_per_list**
- **reflector_items_per_watch**
- **reflector_list_duration_seconds**
- **reflector_lists_total**
- **reflector_short_watches_total**
- **reflector_watch_duration_seconds**
- **reflector_watches_total**

etcd 指标

- **etcd_helper_cache_hit_count**
- **etcd_helper_cache_miss_count**
- **etcd_helper_cache_entry_count**
- **etcd_request_cache_get_latencies_summary**
- **etcd_request_cache_add_latencies_summary**
- **etcd_request_latencies_summary**

Transformation 指标

- **transformation_latencies_microseconds**
- **transformation_failures_total**

其他指标

- **admission_quota_controller_adds**
- **crd_autoregistration_controller_work_duration**
- **APIServiceOpenAPIAggregationControllerQueue1_adds**
- **AvailableConditionController_retries**
- **crd_openapi_controller_unfinished_work_seconds**
- **APIServiceRegistrationController_retries**

- `admission_quota_controller_longest_running_processor_microseconds`
- `crdEstablishing_longest_running_processor_microseconds`
- `crdEstablishing_unfinished_work_seconds`
- `crd_openapi_controller_adds`
- `crd_autoregistration_controller_retries`
- `crd_finalizer_queue_latency`
- `AvailableConditionController_work_duration`
- `non_structural_schema_condition_controller_depth`
- `crd_autoregistration_controller_unfinished_work_seconds`
- `AvailableConditionController_adds`
- `DiscoveryController_longest_running_processor_microseconds`
- `autoregister_queue_latency`
- `crd_autoregistration_controller_adds`
- `non_structural_schema_condition_controller_work_duration`
- `APIServiceRegistrationController_adds`
- `crd_finalizer_work_duration`
- `crd_naming_condition_controller_unfinished_work_seconds`
- `crd_openapi_controller_longest_running_processor_microseconds`
- `DiscoveryController_adds`
- `crd_autoregistration_controller_longest_running_processor_microseconds`
- `autoregister_unfinished_work_seconds`
- `crd_naming_condition_controller_queue_latency`
- `crd_naming_condition_controller_retries`
- `non_structural_schema_condition_controller_queue_latency`
- `crd_naming_condition_controller_depth`
- `AvailableConditionController_longest_running_processor_microseconds`
- `crdEstablishing_depth`
- `crd_finalizer_longest_running_processor_microseconds`
- `crd_naming_condition_controller_adds`

- **APIServiceOpenAPIAggregationControllerQueue1_longest_running_processor_microseconds**
- **DiscoveryController_queue_latency**
- **DiscoveryController_unfinished_work_seconds**
- **crd_openapi_controller_depth**
- **APIServiceOpenAPIAggregationControllerQueue1_queue_latency**
- **APIServiceOpenAPIAggregationControllerQueue1_unfinished_work_seconds**
- **DiscoveryController_work_duration**
- **autoregister_adds**
- **crd_autoregistration_controller_queue_latency**
- **crd_finalizer_retries**
- **AvailableConditionController_unfinished_work_seconds**
- **autoregister_longest_running_processor_microseconds**
- **non_structural_schema_condition_controller_unfinished_work_seconds**
- **APIServiceOpenAPIAggregationControllerQueue1_depth**
- **AvailableConditionController_depth**
- **DiscoveryController_retries**
- **admission_quota_controller_depth**
- **crdEstablishing_adds**
- **APIServiceOpenAPIAggregationControllerQueue1_retries**
- **crdEstablishing_queue_latency**
- **non_structural_schema_condition_controller_longest_running_processor_microseconds**
- **autoregister_work_duration**
- **crd_openapi_controller_retries**
- **APIServiceRegistrationController_work_duration**
- **crdEstablishing_work_duration**
- **crd_finalizer_adds**
- **crd_finalizer_depth**
- **crd_openapi_controller_queue_latency**
- **APIServiceOpenAPIAggregationControllerQueue1_work_duration**

- `APIServiceRegistrationController_queue_latency`
- `crd_autoregistration_controller_depth`
- `AvailableConditionController_queue_latency`
- `admission_quota_controller_queue_latency`
- `crd_naming_condition_controller_work_duration`
- `crd_openapi_controller_work_duration`
- `DiscoveryController_depth`
- `crd_naming_condition_controller_longest_running_processor_microseconds`
- `APIServiceRegistrationController_depth`
- `APIServiceRegistrationController_longest_running_processor_microseconds`
- `crd_finalizer_unfinished_work_seconds`
- `crdEstablishing_retries`
- `admission_quota_controller_unfinished_work_seconds`
- `non_structural_schema_condition_controller_adds`
- `APIServiceRegistrationController_unfinished_work_seconds`
- `admission_quota_controller_work_duration`
- `autoregister_depth`
- `autoregister_retries`
- `kubeproxy_sync_proxy_rules_latency_microseconds`
- `rest_client_request_latency_seconds`
- `non_structural_schema_condition_controller_retries`

1.4.2.4. Prometheus 中的高粒度请求期间存储桶

Prometheus 中丢弃了高粒度请求期间存储桶，它使用 `apiserver_request_duration_seconds_bucket` 进行跟踪。这样可让其他监控组件有足够的存储桶来提供有意义的警告，但会极大降低数据建模基数。

1.5. 程序错误修复

apiserver-auth

- 在以前的版本中，如果用户在只配置了基于浏览器的登录的情况下试图通过 CLI 登录，则系统会提示他们输入用户名和密码。现在，如果用户只在配置基于浏览器的登录时尝试从 CLI 登录，则会显示一条信息，提示用户如何获取登录令牌。(BZ#1671604)

- 在以前的版本中，因为一个竞争条件，当加载的服务证书发生变化时将不会被注意，因此 HTTPS 端点中指标抓取程序将无法信任该服务证书。竞争条件已被删除，基于 **library-go** 的 Operator 现在可以正确地重新加载服务证书。(BZ#1779438)
- 在以前的版本中，如果使用 IPv6 地址，Kubernetes API 服务器服务网络地址不会被正确处理。现在，OAuth 代理可以正确地连接到使用 IPv6 地址的 Kubernetes API 服务器。(BZ#1789462)

Build

- 在开始构建前，OpenShift Container Platform 构建器将解析提供的 Dockerfile 并重新构建用于构建的修改版本，以添加标签并处理 **FROM** 说明中指定的镜像替换。生成的 Dockerfile 有时不会正确重建 **ENV** 和 **LABEL** 指令。生成的 Dockerfile 有时会包含原始文件中没有包括的 **=** 字符，构建会失败并显示语法错误。在这个版本中，在生成修改的 Dockerfile 时，现在使用了原始文件中的 **ENV** 和 **LABEL** 指令。因此，构建过程不再会出现 **ENV** 和 **LABEL** 指令中的语法错误。(BZ#1821860)
- **JenkinsPipeline** 构建策略在 OpenShift Container Platform 4.3.0 中弃用。在 Jenkins 或 OpenShift Pipelines 上直接使用 **Jenkinsfile** 对象。(BZ#1804976)
- 构建标签生成和验证未完全符合 Kubernetes 的预期。构建可能会因为某些 **BuildConfig** 对象名称具有无效的标签错误而失败。此程序错误修复更新了构建控制器和构建 API 服务器，现在使用完整的 Kubernetes 验证过程，以确保添加的任何构建标签均符合 Kubernetes 标签标准。因此，具有任何有效 **BuildConfig** 对象名称的构建不会因为构建标签值无效而失败。(BZ#1804934)
- 在以前的版本中，如果 Samples Operator 的 **samplesRegistry** 字段已更改，仍然会造成镜像流导入错误。这是因为 Samples Operator 在查看镜像流状态时没有应用配置更改。现在，如果对 Samples Operator 的 **samplesRegistry** 字段的更改仍然会导致镜像流导入错误，则镜像流状态中会显示正确的故障原因。(BZ#1795705)
- 在以前的版本中，在 **RUN** 指令后，OpenShift Container Platform 构建器会尝试卸载创建的每个绑定挂载，并记录在此过程中遇到的任何错误。现在，构建器只卸载顶层目录，且内核卸载了绑定挂载。错误将不会再出现，因此也不会再报告。(BZ#1772179)
- 在以前的版本中，将构建策略上的 **incremental** 和 **forcePull** 标志设置为 **true** 可能会导致使用推送镜像凭证来拉取镜像的构建。因此，从私有 registry 拉取镜像会失败。现在，在 **incremental** 和 **forcePull** 都被设置为 **true** 时，构建镜像可以正确地管理 registry push 和 pull 操作的凭证。(BZ#1774492)
- **oc new-build** 命令中没有包括 **oc new-app** 命令中的 **--insecure-registries** 标记。这个标记允许使用不安全的镜像引用 URL 作为源。因此，**oc new-build** 调用会在尝试使用基于 HTTP 的镜像引用作为构建的基本镜像进行 HTTPS 连接时出现错误。现在，**--insecure-registries** 选项被添加到 **oc new-build** 命令中，用户现在可以创建引用不安全 registry 的构建，将其作为其基础镜像。(BZ#1780714)

Cloud Credential Operator

- Cloud Credential Operator (CCO) 会报告 **CredentialsRequests** CR 带有条件，即使 CCO 已被禁用。以前，即使 Operator 已被配置为禁用，仍然会出现警报。在这个版本中，当 CCO 被设置为禁用时，不会再报告条件。(BZ#1794536)
- 协调 **CredentialsRequest** CR 会尝试创建已经存在的角色分配，Microsoft Azure 日志会显示 **create role assignment** 错误。此程序错误修复会检查是否存在角色分配，以避免创建已存在的角色。因此，Azure 日志中显示的错误消息会减少。(BZ#1776079)

控制台 Kubevirt 插件

- 以前，当在没有注解的情况下选择 VM 模板时，VM 向导会意外关闭。VM 向导现在可以与没有注解的模板一起工作。(BZ#1776190)
- 在以前的版本中，当创建一个使用 URL 作为磁盘镜像源的 VM 模板时，不会为使用该模板创建的虚拟机创建一个持久性卷声明 (PVC)。现在，在从这类模板创建新虚拟机时，PVC 被克隆并用于磁盘镜像。(BZ#1779116)
- 在以前的版本中，在解释模板中的内存值和存储值时会使用不同的单位，从而导致请求创建 VM 有时会失败。现在，在 VM 模板中内存和存储的值都使用 Gi 作为单位。(BZ#1792101)
- 在以前的版本中，VM 向导会忽略 VM 模板中的任何磁盘配置。现在，如果磁盘配置在模板中指定，则 VM 向导会使用它。(BZ#1782434)
- 以前，UI 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，UI 可以正确地报告。(BZ#1785344)
- 在以前的版本中，如果虚拟机定义了多个 CD-ROM 驱动器，在没有保存然后再重新打开 CD-ROM 对话框的情况下，不能删除多个 CD-ROM 光盘驱动器。现在，无需保存并重新打开对话框就可以删除多个光盘驱动器。(BZ#1786070)
- 在以前的版本中，无法使用虚拟机向导使用的默认 YAML 创建虚拟机，因为 YAML 无效。现在，在创建带有向导的虚拟机时可以使用默认虚拟机模板。(BZ#1808304)
- 在以前的版本中，无法使用可视编辑器修改引导顺序，因为模板 YAML 中的引导顺序没有识别。现在，在使用可视编辑器时可以修改引导顺序。(BZ#1789269)

Image

- 当 **ImageStreamTag** 对象无法访问时，**oc tag** 命令不会更新镜像流。该命令会报告新标签已创建，但实际并没有创建。此程序错误修复更新了 **oc tag** 命令，以便在 **ImageStreamTag** API 没有权限时也会实际创建标签。(BZ#1746149)
- 解码器会依赖于字符串长度来决定 base64 是否被 padded 或 unpadded。这使得解码器无法处理包含空格信息的 pull secret。此程序错误修复现在会检查这个字符串是否带有 trailing padding 符号。因此，可以使用带有空格的 pull secret 来拉取镜像。(BZ#1776599)

镜像 Registry

- 在以前的版本中，如果 Image Registry Operator 处于非受管状态，则不会报告新的版本，这会导致无法进行升级。在这个版本中，如果 Image Registry Operator 处于非受管状态，它会准确的报告版本状态，从而可以成功升级。(BZ#1791934)
- 在以前的版本中，**nodeca** 守护进程集不会宽容 **NoSchedule** 污点，这会导致在节点上缺少 pod 的情况。此程序错误修复添加了相应的容限，带有污点的节点现在可以接收来自 **nodeca** 守护进程集的更新。(BZ#1785115)
- Image Registry Operator 使用与 RWO 卷不兼容的滚动更新策略，这意味着无法使用 RWO 卷。此程序错误修复支持 Image Registry Operator 获取滚动更新策略，现在可以使用非高可用性配置（例如，只有一个副本的配置）中的 RWO 卷进行部署。(BZ#1798759)
- 在以前的版本中，当镜像 Registry Operator 移除存储时，它不会清理存储状态。当 registry 切换回 **Managed** 状态时，将无法检测到引导所需的存储。在这个版本中，Image Registry Operator 会清理存储状态，允许 Operator 在切换到 **Managed** 状态时创建存储。(BZ#1787488)

安装程序

- 使用安装程序置备的基础架构在 AWS 上置备的早期版本的集群不包括允许从 control plane 主机到 worker 的 TCP 端口和 UDP 端口 30000-32767 的流量的安全组规则。因此，新的 OVN 网络

组件无法象预期一样工作。现在，所需的安全组规则将被添加到集群中，以便 control plane 和 worker 系统可以通过 TCP 和 UDP 端口 30000-32767 进行通信，OVN 网络组件可以正常工作。(BZ#1763936)

- 之前，Red Hat Enterprise Linux (RHEL) 节点上的升级可能无法正常进行。当无法从代理的后面拉取镜像时，一个不需要的机器配置应用步骤会导致失败。现在，这个不必要的步骤已被删除，代理后面的 RHEL 节点升级可以成功进行。(BZ#1786297)
- 在以前的版本中，当您将 RHEL 7 节点从版本 4.2.12 升级时，机器配置没有被 MCO 正确更新。因为软件包会在本地磁盘中安装更新的文件，所以 MCO 不会处理 RHEL 节点上的配置更新。现在，机器配置应用步骤已被恢复，镜像拉取过程可以在代理后完成。当 RHEL 7 节点中的软件包被更新和升级后，机器配置会被正确应用。(BZ#1792139)

kube-apiserver

- 虽然已存在用于聚合 API 服务器状态的指标，但不会出现为其发出的警报。现在，当一个聚合的 API 在一个较短的时间段内报告太多错误时，会显示错误，因为这意味着服务的可用性状态变化太频繁。(BZ#1772564)

kube-controller-manager

- 在以前的版本中，证书不会被正确传播，因此云供应商无法在 man-in-the-middle 代理后进行实例化。现在，证书会被正确传播到 **kube-controller-manager**，云供应商与 man-in-the-middle 代理可以正常工作。(BZ#1772756)

Logging

- 在以前的版本中，您可以通过 Fluentd 插件使用 syslog 协议 (RFC 3164) 将日志转发到外部系统。添加到 OpenShift Container Platform 4.3 中的日志转发 API 更改了使用 syslog 配置日志转发的过程。因此，您无法使用与 OpenShift Container Platform 4.2 相同的方法来转发日志。为了解决这个问题，采用了新的过程来允许使用 syslog 协议进行日志转发。此更改被后向移植到 OpenShift Container Platform 4.3.7。因此，您可以继续将日志转发到外部 syslog 服务器。(BZ#1799024)

Machine Config Operator

- 因为 HAProxy 超时值对于某些应用程序（如 Kuryr）来说过于敏感，所以过去 API LB 的超时值被设置为 24 小时。如果在一个较短的时间段内触发了多次 HAProxy 重新加载操作，则可能会累积很多 HAProxy 进程。此程序错误修复会强制在默认超时时间 120 秒后向旧的 HAProxy 进程（这些进程可能还没有被终止）发送 **SIGTERM**。因此，已存在较长时间的重复的 HAProxy 进程数量会减少。(BZ#1771566)

Metering Operator

- Metering 不会管理或删除任何 S3 存储桶数据。在删除一个报告时，用于存储 metering 数据的 S3 存储桶需要被手动清理。如果没有手动清理 S3 存储桶中保存的数据并重新创建了同一报告，则原始报告数据仍会存在，从而导致出现重复的行条目。(BZ#1728350)

监控

- 由于 OAuth 代理容器就绪探针配置不正确，因此容器日志每 10 秒就会产生错误信息。现在，就绪探针已被正确配置。因此，错误信息不会出现在日志中。(BZ#1658899)
- 因为 **cluster-reader** 角色没有权限查看节点或 pod 指标，所以绑定到该角色的用户无法使用 **oc top node** 等命令访问指标。更新了 **cluster-reader** 角色，使其包含允许查看指标的权限。(BZ#1723662)

- 上游社区引入了一种新的实验性 Prometheus 用户界面。对于这个新的实验性界面，还没有进行充分测试且不稳定。因此，从实验接口切换到默认接口会返回一个空页面。为了防止出现这个问题，现在隐藏了实验 UI 的链接。因此，现在无法再访问实验性 Prometheus 界面。(BZ#1781415)
- OpenShift Container Platform 会错误地评估一些记录规则，因此会缺少一些由记录规则生成的指标。这个与记录规则相关的问题已被修复。现在，所有记录规则都可以被成功评估。(BZ#1807843, BZ#1779324)

网络

- 在以前的版本中的一个 Egress IP 程序错误修复在删除 Egress IP 后没有进行完全清理，从而可能会导致节点上存在不必要的（但也没有什么伤害）的额外 iptables 规则。在这个版本中，如果不再使用这些额外的规则，它们会被删除。(BZ#1787488)
- 在以前的版本中，使用带大写字母的 **httpProxy** 或 **httpsProxy** 主机名会导致 CNO 错误，它违反了 RFC 3986 的规定。因此，CNO 不能正常工作。此程序错误修复使用 **golang url.ParseRequestURI** 对它进行解析，它正确实现了 RFC 3986 以及一些更多 RFC。因此，**httpProxy** 和 **httpsProxy** 中现在允许使用大写字母。(BZ#1802606)
- 在以前的版本中，kubelet 使用的 kubeconfig（用于 SDN），改变其路径会导致 SDN 有一个 null deference 尝试来解析空文件。在这个版本中，SDN 可以同时处理旧路径和新路径。(BZ#1781707)

节点

- 在以前的版本中，当 kubelet 证书过期时不会发出警报。这会导致在管理员没有注意到之前，kubelets 就停止了工作。在这个版本中，添加了 **server_expiration_renew_errors** 指标来报告过期的证书。(BZ#1767523)
- Conmon 会在 kubelet exec 存活度探测中超时。这会导致一些 exec 探测失败，强制容器被终止并重启。现在，exec 存活度探测可以正常工作。(BZ#1817568)
- 在节点重新引导时，当 pod 无法恢复时，CRI-O 没有正确清理 IP 地址。这会导致节点 IP 耗尽，从而导致 pod 无法启动。现在，如果重启后 pod 无法恢复，pod 网络就会被销毁，释放 IP 地址以备未来使用。(BZ#1781824)
- RHEL 7 无法添加到 OpenShift Container Platform 集群，因为 CRI-O 不会启动。这是由于 Conmon 软件包中的问题造成的。现在，这个 Conmon 的程序错误已被修复，RHEL 7 现在可以加入 OpenShift Container Platform 集群。(BZ#1809906)
- Pod 横向自动扩展 (HPA) 没有从退出的初始容器中获取指标数据。这个问题已通过为退出的初始容器提交零指标来解决，从而允许 HPA 对带有初始容器的 pod 执行分析。(BZ#1814283)
- Kubelet 指标端点定期返回 **500** 状态代码，阻止 Prometheus 为 kubelet 端点和节点收集指标。**500** 代码是由将死容器混合到指标流中导致的，从而导致了重复的指标被注入。此程序错误已被修复，现在可以从 kubelet 正确报告指标数据。(BZ#1748073)

oc

- 因为 OpenShift CLI 的内部代码没有考虑新版本 API，所以 **oc logs** 命令会从某些资源返回错误。OpenShift CLI 现在支持所有已知的 API 类型和版本，允许 **oc logs** 为所有资源工作。(BZ#1774366)
- 使用 **--since** 参数运行 **oc adm node-logs** 命令时出现错误。这是由于预期时间戳格式的拼写错误所引起的。这个拼写错误已被修正，**oc adm node-logs** 现在可以和 **--since** 参数一起正常使用。(BZ#1779563)

openshift-apiserver

- 在以前的版本中，Helm 3.0.0+ 无法用于 OpenShift Container Platform 对象。这会导致在尝试部署有效 Helm Chart 时出现错误。在这个版本中，可以使用 OpenShift Container Platform 对象部署 Helm chart。([BZ#1773682](#))

openshift-controller-manager

- 在以前的版本中，**openshift-controller-manager** 的 metrics 没有与 1.16 Kubernetes Prometheus registry 正确注册。这会导致 OpenShift Container Platform control plane 缺少指标。在这个版本中，**openshift-controller-manager** 的 metrics 已被正确注册，缺少的 OpenShift Container Platform control plane 指标已被恢复。([BZ#1810304](#))
- 在以前的版本中，当相关令牌被删除时，pull secret 有时不会被删除。这会导致 pull secret 与 Kubernetes 服务帐户保持关联。在这个版本中，pull secret 的所有者被引用，相关令牌 secret 已被创建。现在，当 pull secret 被删除时，相关的令牌也会被删除。([BZ#1806792](#))
- 在以前的版本中，在内部 registry 中创建 pull secret 的速率限制较低。这会导致短时间内创建大量命名空间的等待时间。在这个版本中，内部 registry 中创建 pull secret 的速率限制被增加。现在，即使在负载很重时也可以快速创建 pull secret。([BZ#1819849](#))

RHCOS

- Red Hat Enterprise Linux CoreOS (RHCOS) 现在支持网络团队 (network teaming)。在 RHCOS 中添加了 **teamd** 和 **NetworkManager-team** RPM，启用团队网络设备的设置和管理。([BZ#1758162](#))

Samples

- registry.redhat.io** 不支持 IPv6，这意味着 Samples Operator 不会尝试安装镜像流，因为所有红帽样本都托管在 **registry.redhat.io**。因为 IPv6 是红帽和 OpenShift Container Platform 的一个关键技术，所以 Samples Operator 将不会影响在 IPv6 上的 OpenShift Container Platform 安装。([BZ#1788676](#))
- Samples Operator 以前在 s390x 或 ppc64le 上运行时无法报告其版本，因此在那些架构上安装将无法成功完成。在这个版本中，Samples Operator 会正确报告其版本，因此可以在 s390x 或 ppc64le 上正确安装。([BZ#1779933](#))
- 在以前的版本中，最新的 Java 11 镜像流标签无法正确链接到镜像流详情页面上的版本，这意味着无法从 Web 控制台检查 **ImageStreamTag** 对象。在这个版本中，可以通过 web 控制台正确检查 Java 11 的正确的 **ImageStreamTag** 规格。([BZ#1778613](#))
- 在以前的版本中，如果控制器管理器在启动后不久但更新镜像流元数据之前访问了镜像流，则镜像流的本地引用设置可能会被忽略。这会导致对由私有容器镜像仓库 (registry) 支持的镜像流的请求失败。在这个版本中，控制器管理器会在元数据初始化完成后刷新其镜像流缓存。这会在启动后马上产生准确的本地引用镜像流策略。([BZ#1775973](#))

存储

- 如果在 Local Storage Operator 上使用了 **storage-class** 注解而不是 **storeClassName**，则无法调度 Pod，并且 PVC 会一直处于待处理状态。在这个版本中，Kubernetes 调度程序在评估 Pod 和它的 PVC 时，会检查 **volume.beta.kubernetes.io/storage-class** 和 **PVC.Spec.StorageClassName**。现在，可以调度并运行使用 beta 注解指向 StorageClass 的 Pod。([BZ#1791786](#))
- 在以前的版本中，如果卷挂载在最终由 CSI 驱动程序完成前发生超时而 pod 被删除，则 Kubernetes 不会卸载 CSI 卷。这会导致在 Kubernetes 不知情的情况下将卷挂载到节点上。因

此，这个卷无法在其它任何位置被挂载。在这个版本中，Kubernetes 会等待操作最终成功完成，或 CSI 驱动返回一个超时或其他类似的瞬时错误。现在，Kubernetes 知道一个卷是否被挂载或卸载，并会在 pod 被删除时清除相关的挂载。(BZ#1745776)

模板

- 在将 `--param-file` 选项与模板处理命令（如 `oc new-app` 或 `oc process`）一起使用时，如果该文件大小大于 64K，则不会被完全读取。这会导致带有 `--param-file` 的基于 `oc` 的模板进程失败。OpenShift Container Platform 现在检查由 `--process-file` 指定的文件的大小，并增强用于读取整个文件的参数。基于 `oc` 的模板处理中的 `--param-file` 所指向的文件如果大于 64K 现在也可以正常工作。(BZ#1748061)
- 在以前的版本中，用于创建项目的 `new-app/new-build` 示例之一会在 FIPS 环境中出现错误，因为示例不兼容 FIPS。现在，在创建新的项目时，只有 FIPS 兼容的 `new-app/new-build` 示例显示，用户可以使用 FIPS 环境中的任何示例。(BZ#1774318)

Web 控制台（管理员视角）

- 在以前的版本中，对于没有 `cluster-admin` 权限的用户，OpenShift 控制台中的构建页中的 **Rebuild** 操作会被错误地禁用。现在，这个问题已被解决，一般用户如果具有克隆构建的权限，则可以使用这个操作。(BZ#1774842)
- 在以前的版本中，只有集群管理员才能在控制台 YAML 编辑器中看到使用 **ConsoleYAMLSample** 资源创建的 YAML 模板示例。现在，所有用户都可以看到这些模板。(BZ#1783163)
- 在 CronJobs 列表页中，根据 **Starting Deadlines Seconds** 或 **Concurrency Policy** 字段进行的排序不会被正确排序。现在，`sortField` 已被更新，您可以正确排序 cron 任务。(BZ#1787096)
- 由于有创建重复内容的条件，**Local Volumes** 页面会显示重复的内容。现在，这个条件已从状态描述项中删除，因此内容不会重复。(BZ#1776131)
- **Role Bindings** 页面为没有项目的用户有一个不可点击的 **Create Binding** 按钮。现在，对于没有项目的用户来说，**Create Binding** 按钮是隐藏的。(BZ#1785487)
- 在以前的版本中，在 web 控制台 **Create Operand** 表单中，一些带有 OLM 描述符的必填字段缺少了所需的红色星号。现在，所有必填字段都被正确标注。(BZ#1779858)
- 在以前的版本中，您可以在 web 控制台中为机器或副本数设置一个负值。现在，不能设置小于 0 的值。(BZ#1780367)
- 在以前的版本中，**PodRing** GUI 组件没有在 **Deployment Config Page** 上更新 `count` 时反映正确的 Pod 数量，然后再点 **Actions => Edit Count** 时会在同一个页面上再次更新。例如，如果使用 **Deployment Config** 页上的 **Edit Count** 把 Pod 的数量从 5 增加到 10，然后用户再使用 `up` 箭头增加 **PodRing** 组件的计数，则 **PodRing** 计数从 5 增加到 6 个 Pod，而不是从 10 增加到 11。在这个版本中，当使用 **Deployment Config** 页上的 **Edit Count** 进行修改时，**PodRing** 组件现在会显示正确的、已更新的 pod 计数。另外，当用户在 **PodRing** 组件上点击 `up` 或 `down` 箭头时，Pod 计数会准确更新。(BZ#1787210)
- 在以前的版本中，用户无法在 web 控制台的 **Installed Operators** 页面中编辑集群范围的操作对象。操作对象 YAML 编辑器会导致浏览器中出现 **HTTP 404 Not Found** 客户端错误响应代码。在这个版本中，Web 控制台可以正确地操作对象 YAML 编辑器打开一个新的 Web 浏览器，用户可以在此更新集群范围的操作对象。(BZ#1781246)
- 在以前的版本中，当在 **ConsoleExternalLogLink** URL 模板中多次出现变量时，web 控制台不会替换所有实例。相反，只有变量的第一个表达式会被替换。在这个版本中，控制台可以把模板中的每个变量实例替换为正确的值。(BZ#1781827)

- 在以前的版本中，在 Web 控制台的 **Operator Details** 页面中，**Subscription Overview** 中的 **InstallPlan** 资源链接无法正常工作。这使得用户很难在 web 控制台中批准 **InstallPlan** 资源。批准 **InstallPlan** 资源的链接（例如，1 需要批准的链接）现在可以正常工作。(BZ#1783651)
- 在以前的版本中，当用户在 Web 控制台的 **OperatorHub Details** 页面中的 **Source** 标签页中根据源名称过滤时会出现一个错误。该过滤器已被修复，用户输入源名称时可正常工作。(BZ#1786418)
- 在以前的版本中，Web 控制台的 **Explore** 页面中的 **Endpoints** 资源缺少 API 文档。现在，**Endpoints** 资源提供了 API 文档，如描述和模式信息。(BZ#1794754)
- 在以前的版本中，如果 Operator 设置了无效的 OLM 描述符，web 控制台将无法显示操作对象。因此，在预期的 web 控制台页面中出现错误。在这个版本中，可以容忍无效的 OLM 描述符，控制台可以正确地显示操作对象详情。(BZ#1797727)
- 在以前的版本中，一些状态值没有与它们关联的图标。因此，一些值会出现在图标中，其他值则没有。现在，所有状态值都定义了相应的图标并可以正确显示。(BZ#1780629)
- 在以前的版本中，控制台没有在路由标签中检查特殊字符，这会导致以下错误：

```
AlertmanagerFailedReload Alert:
Reloading Alertmanager's configuration has failed for openshift-monitoring/alertmanager-main-x.
```

Create Receiver 表单现在将标签名称仅限为只能使用有效字符。(BZ#1784725)

- 在以前的版本中，如果 Operator 声明了一个无效的 **K8sResourceLink** OLM 描述符，web 控制台会显示一个空白页面。控制台现在容许不正确的 **K8sResourceLink** 描述符，这可以防止出现空白页面。(BZ#1795407)
- 在以前的版本中，从 Web UI 修改所需的 Operator 资源不会更新 Operator 的 YAML 文件。YAML 文件现在可按预期更新。(BZ#1797769)
- 以前，警报被静默后会保留在通知抽屉中。现在，静默的警报不再保留在通知抽屉中。(BZ#1808062)
- Web 控制台中的一个错误偶尔会在特定页面中造成运行时错误。这个错误已被修复。(BZ#1818978)
- 查询浏览器的结果在 web 控制台中以一个硬代码的形式进行排序，因此自定义的排序结果可能与期望的结果不同。已删除了硬编码的排序，允许查询结果反映任何自定义的排序。(BZ#1808437)
- 使用控制台的 **Compute → Machine Config Pools → Create Machine Config Pool** 按钮创建新的 **MachineConfigPool** 会导致 **MachineConfigPool** 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 GUI 显示与正确节点匹配的 **Machine Selector**。(BZ#1818944)
- 在以前的版本中，web 控制台 pod 终端无法正确处理 Unicode 字符。这个问题已被解决，Unicode 字符现在可以被正确显示。(BZ#1821285)
- 在以前的版本中，在滚动页面时，web 控制台工作负载页面中的卷表可能会部分消失。这个程序错误已被解决。(BZ#1822195)

- 在以前的版本中，用于创建报告和报告查询的默认模板使用 **apiVersion v1alpha** 而不是 **v1**。虽然 alpha 版本的模板仍可工作，但对它的支持可能会随时取消。模板已更新为使用 **apiVersion: metering.openshift.io/v1**。(BZ#1772694)
- 当点击 web 控制台的 **Dashboard** 并在 **Dashboard** 中选择一个导航项时，所选择的两个导航项目仍会突出显示。此程序错误修复应用新的 CSS 规则，以消除同时突出显示的多个导航项目，确保只突出显示活跃导航项。(BZ#1774702)

Web 控制台 (开发者视角)

- Microsoft Edge 浏览器不识别滚动时所使用的功能。日志屏幕无法加载，并会产生错误。屏幕阅读器支持被启用，日志现在可以被正确显示。(BZ#1777980)
- Serverless 资源（如 **Service** YAML 文件）列为 **v1beta1** 而不是 **v1**。但是 **v1beta1** 已被弃用。在这个版本中，**apiVersion** 被更新为 **v1**。(BZ#1796421)
- 拓扑 (**Topology**) 视图中的服务绑定请求 (SBR) 与 修订版本 (**revision**) 关联。因此，没有新修订版本会获取相关的 **secret**。SBR 应该通过 Knative 服务注入 **secret** 并创建新的修订版本。(BZ#1798288)
- **KnativeServing** 资源的 **service.knative.dev** API 组已弃用，它在 Serverless Operator 版本 1.4 中已被改为 **operator.knative.dev**。在 Serverless Operator 的下一发行版本中，**service.knative.dev** 将被弃用。(BZ#1800598)
- 在容器镜像部署中，如果为 Knative 选择了内部镜像流，那么 Knative 会尝试创建新的镜像流，这可能会失败。您无法将内部镜像流部署为一个 Knative 服务。不要为内部镜像选择创建新镜像流，它已存在。(BZ#1808280)
- 在 Kubernetes 部署中，如果来自外部镜像 registry 的镜像带有标签，如 **openshift/hello-world:1.0**，标签不会被应用。用户无法使用标签导入外部镜像。在这个版本中，用于部署的标签会被正确应用。(BZ#1801736)
- 在以前的版本中，当两个连续的 rollout 失败时，**Topology** 视图会显示失败的 pod，而不是显示最后一个活跃的修订版本。在这个版本中，当一个 rollout 失败时，会显示最后一个活跃的修订版本。(BZ#1760828)
- 在以前的版本中，创建应用程序时不会检测到命名空间中的现有镜像流。当具有有限集群范围权限的用户在 **Add** 页面的内部 registry* 选项中使用 **Container Image** → **Image** 名称时会出现这种情况。现在，镜像流获取逻辑已从集群级别移到命名空间级别，这使得拥有命名空间权限的用户能够查看该命名空间中的镜像流。(BZ#1784264)
- Knative 服务及修订资源没有 **Topology** 视图中的绑定或可视连接程序，因此 Knative 工作负载无法连接到其他工作负载。这些资源现在在 **Topology** 视图中有连接器，并可连接到其他工作负载。(BZ#1779201)
- 当安装并配置 Eclipse Che Operator 时，**Topology** 视图会显示 Git 图标而不是 Che 图标。因此，用户可能不会知道点这个图标可以访问 Che 工作区。现在，**Topology** 视图在配置 Che 时正确显示 Che 图标，方便用户访问 Che 工作区。(BZ#1780338)
- 在使用 CLI 创建 Knative 服务时打开 **Topology** 视图会导致 GUI 错误。现在，为处理这个工作负载添加了相应的检查，因此不会再出现 GUI 错误。(BZ#1781188)
- 当出现服务器端错误时，内部 registry 功能会出现一个不清楚的错误消息。这个错误信息现已被改进，以便帮助用户找出造成问题的原因。(BZ#1787492)

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 4.2	OCP 4.3	OCP 4.4
Prometheus Cluster Monitoring	GA	GA	GA
精度时间协议 (PTP)	-	TP	TP
CRI-O for runtime pods	GA	GA	GA
oc CLI 插件	TP	TP	TP
Network Policy	GA	GA	GA
Multus	GA	GA	GA
New Add Project Flow	GA	GA	GA
Search Catalog	GA	GA	GA
Cron 作业	GA	GA	GA
Kubernetes 部署	GA	GA	GA
有状态的集合	GA	GA	GA
显式配额	GA	GA	GA
挂载选项	GA	GA	GA
experimental-qos-reserved	TP	TP	TP
Pod sysctls	GA	GA	GA
用于外部项目流量的静态 IP	GA	GA	GA
模板完整性检测	GA	GA	GA

功能	OCP 4.2	OCP 4.3	OCP 4.4
replicaSet	GA	GA	GA
Kubernetes 资源的镜像流	GA	GA	GA
设备管理器	GA	GA	GA
持久性卷重新调整大小	GA	GA	GA
巨页	GA	GA	GA
CPU 固定	GA	GA	GA
准入 (Admission) webhooks	GA	GA	GA
AWS EFS 的外部置备程序	TP	TP	TP
Pod Unidler	TP	TP	TP
为临时存储设置 Limit/Requests	TP	TP	TP
Descheduler	-	-	TP
Podman	TP	TP	TP
Kuryr CNI 插件	TP	GA	GA
共享 PID 命名空间的控制	TP	TP	TP
Cluster Administrator 控制台	GA	GA	GA
集群自动扩展	GA	GA	GA
Container Storage Interface (CSI)	GA	GA	GA
Operator Lifecycle Manager	GA	GA	GA
Red Hat OpenShift Service Mesh	GA	GA	GA
"完全自动的" Egress IP	GA	GA	GA
Pod 优先级和抢占功能	GA	GA	GA
Dockerfiles 的多阶段构建	GA	GA	GA
OVN-Kubernetes pod 网络供应商	TP	TP	TP

功能	OCP 4.2	OCP 4.3	OCP 4.4
基于 Prometheus 的 HPA 定制 metrics adapter	TP	TP	TP
机器健康状态检查	TP	GA	GA
使用 iSCSI 的持久性存储	TP	GA	GA
使用 iSCSI 的原始块	TP	GA	GA
使用 Cinder 的原始块	-	TP	TP
OperatorHub	GA	GA	GA
三节点裸机部署	TP	TP	TP
Cluster Network Operator	TP	GA	GA
Helm CLI	-	TP	GA
服务绑定	-	TP	TP
日志转发	-	TP	TP
用户工作负载监控	-	TP	TP
OpenShift Serverless	TP	TP	GA
Compute Node Topology Manager	-	TP	TP
CSI 卷快照	-	-	TP
CSI 卷克隆	-	-	TP
CSI 卷扩展	-	-	TP
OpenShift Pipelines	-	-	TP
成本管理	TP	GA	GA

1.7. 已知问题

- Machine Config Operator (MCO) 支持第 2 天代理支持时存在一个问题，它出现在重新配置现有非代理集群以使用代理时。MCO 应该对 RHCOS 信任捆绑包在配置映射中应用新配置的代理 CA 证书。当前这无法正常工作。作为临时解决方案，您必须手动将代理 CA 证书添加到信任捆绑包中，然后更新信任捆绑包：

```
$ cp /opt/registry/certs/<my_root_ca>.cert /etc/pki/ca-trust/source/anchors/
$ update-ca-trust extract
$ oc adm drain <node>
$ systemctl reboot
```

([BZ#1784201](#))

- 使用自签名的 Red Hat OpenStack Platform (RHOSP) 16 集群时，您无法从内部镜像 registry 拉取镜像，或把镜像推送到内部镜像 registry。作为临时解决方案，您必须在 **configs.imageregistry/cluster** 资源中把 **spec.disableRedirects** 设为 **true**。这样，客户端可以从镜像 registry 中拉取镜像层，而不是直接从 Swift 链接拉取。(BZ#1810461)
- 集群代理配置 **HTTP_PROXY** 仅适用于 OpenShift Container Platform 组件，不适用于用户应用程序。这个问题的一个解决方案是，您必须运行以下命令为用户应用程序启用集群代理配置：

```
$ oc set env dc/jenkins \
  http_proxy=$(oc get proxy cluster -o jsonpath='{.status.httpProxy}') \
  https_proxy=$(oc get proxy cluster -o jsonpath='{.status.httpsProxy}') \
  no_proxy=$(oc get proxy cluster -o jsonpath='{.status.noProxy}')
```

([BZ#1780125](#))

- 所有通过 HTTPS 代理的 **git clone** 操作将失败。使用 HTTP 代理不会出现这个问题。(BZ#1750650)
- 如果源 URI 使用 **git://** 或 **ssh://**，则所有对代理后面的构建的 **git clone** 操作都会失败。(BZ#1751738)
- 使用镜像 (mirror) 构建镜像时，当 mirror registry 的 pull secret 仅链接到构建器服务帐户时，构建会失败。pull secret 还必须链接到构建配置对象。(BZ#1810904)
- 在带有 Kuryr 的 Red Hat OpenStack Platform (RHOSP) 13 中，如果 FIPS 被禁用，则无法启用服务目录。Service Catalog 控制器管理器和 API 服务器组件的 Pod 显示 **CrashLoopBackOff** 状态。这是因为 **https://etcd.openshift-etcd.svc.cluster.local:2379** URL 并不总是被解析。在 OpenShift Container Platform 4 中使用了一个新方法来获取 etcd 集群 URL。(BZ#1821589)
- 因为 **ovn_controller** 在初始设置后崩溃，安装使用 Kuryr 的 RHOSP 16 无法正常工作。(BZ#1812009, BZ#1818844)
- Red Hat Virtualization (RHV) 机器的 **instance-state** 注解和 **providerStatus.instanceState** 状态并不总是匹配。不匹配会导致客户端失败或者错误地对 RHV 机器状态进行补丁。(BZ#1815394)
- 当扩展 RHV 上设置的机器时，新机器无法退出 **Provisioned** 阶段。这会导致机器不能运行。(BZ#1815435, BZ#1817853)
- OpenShift Container Platform 集群的自动扩展因为集群资源计算错误而失败。(BZ#1822118)
- 当使用 Firefox 浏览器来选择 **Topology** 视图中的节点或节点组时，所有相关标签和节点的背景变得透明。(BZ#1822337)
- 在 **Topology** 视图中，当用户选择节点或工作负载，然后点击侧面面板上的 **Monitoring → View monitoring dashboard** 时，用户会看到该特定工作负载的监控仪表盘。此过滤出的工作负载面板视图没有被明确命名，这会导致与显示所有工作负载指标的通用仪表盘产生混乱。(BZ#1822331)

- 当从 **Developer** 视角在无服务器流量分布标签中输入无效字符，比如句点 (.) 时，流量分布功能将停止工作。然而，它并没有显示任何错误消息来防止在标签中输入无效字符。(BZ#1822344)
- 如果身份提供者(IDP)需要超过 60 秒的时间来验证用户，在尝试其他 IDP 前验证可能会失败。这个问题的一个解决方案是，从 IDP 列表中删除有问题的 IDP，以使用户可以使用其他 IDP 进行身份验证。(BZ#1826484)
- 当将集群日志记录从版本 4.3 更新至版本 4.4 时，Elasticsearch Pod 可能会停留在 **CrashLoopBackOff** 状态中。您可以通过按顺序删除 Elasticsearch 部署来解决这个问题。(BZ#1824006)
- OpenShift Container Platform 4.4 不附带 v.4.4 Metering Operator。用户可以在 OpenShift Container Platform 4.4 集群中安装或继续运行 v4.3 Metering Operator。(BZ#1829035)
- 当把 OpenShift Container Platform 集群从版本 4.3 更新至版本 4.4 时，etcd Operator 有时可能会因为处于降级状态而无法升级，这是因为 **InstallerPod** 失败所致。这个问题的一个解决方案是，您必须在 etcd 上强制一个新修订版本来修复 **InstallerPod** 故障，这样可以让 etcd Operator 恢复：
 1. 在 etcd 上强制一个新的修订版本：


```
$ oc patch etcd cluster -p='{ "spec": { "forceRedeploymentReason": "recovery-"$( date --rfc-3339=ns )"' } }' --type=merge
```
 2. 验证节点是否处于最新的修订版本：


```
$ oc get etcd '-o=jsonpath={range .items[0].status.conditions[? (@.type=="NodeInstallerProgressing")].reason}{ "\n" }{.message}{ "\n" }
```

 (BZ#1830789)
- web 控制台下载部署在配置了 **ipv6.disable=1** 的节点上会失败。(BZ1795325)
- **Topology Manager** 中存在一个问题，如果在同一节点上同时创建保证 QoS pod，可能会导致 NUMA 资源无法与同一 NUMA 节点一致。因此，pod 规格中请求的资源可能会 MUMA 不一致。为了避免在 4.4 中出现这个问题，请不要同时在节点上启动带有 Guaranteed QoS 的多个 pod。如果您遇到这个问题，请先删除然后再重新创建 pod。(BZ#1834979)
- **runStrategy** 属性设置为 **Manual** 的虚拟机并不表示它们在运行或停止，web 控制台会错误地假设它们正在运行。要避免这个问题，在通过 web 控制台处理虚拟机时，不要将 **runStrategy** 设置为 **Manual**。使用 **running** 属性，或将 **runStrategy** 设置为 **Always RerunOnFailure**、或 **Halted**。(BZ#1834717)
- 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#1791162)
- 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)
- 由于与过期 OAuth 令牌相关的问题，您可能在 Kibana 控制台中收到 **security_exception** 错误，并无法访问 Kibana 索引。如果您看到这个错误，请登出 Kibana 控制台后再重新登录。这会刷新 OAuth 令牌，您应该能够访问索引。(BZ#1791837)
- 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 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 4.4 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：

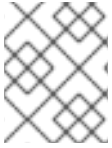
- **cluster-status-binding**
- **discovery**
- **system:basic-user**
- **system:discovery**
- **system:openshift:discovery**

([BZ#1821771](#))

1.8. 异步勘误更新

OpenShift Container Platform 4.4 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 4.4 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。

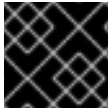
红帽客户门户网站的用户可以在红帽订阅管理（RHSM）帐户设置中启用勘误通知功能。当勘误通知被启用后，用户会在有与其注册的系统相关的勘误发行时接收到电子邮件通知。



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 4.4 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.4.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-2020:0581 - OpenShift Container Platform 4.4 镜像和程序错误公告

发布日期：2020 年 5 月 4 日

OpenShift Container Platform release 4.4 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:0581](#) 公告中。此更新包括的 RPM 软件包由 [RHBA-2020:0582](#) 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 4.4.3 容器镜像列表](#)

1.8.2. RHSA-2020:1936 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 5 月 4 日

现在，OpenShift Container Platform 4.4 提供了对 **haproxy** 的更新。有关更新的详情，请查看 [RHSA-2020:1936](#) 公告。

1.8.3. RHSA-2020:1937 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 5 月 4 日

OpenShift Container Platform 4.4 现在提供了对 **cri-o** 的更新。有关更新的详情，请查看 [RHSA-2020:1937](#) 公告。

1.8.4. RHSA-2020:1938 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 5 月 4 日

OpenShift Container Platform 4.4 现在提供了对 **hadoop-container** 的更新。有关更新的详情，请查看 [RHSA-2020:1938](#) 公告。

1.8.5. RHSA-2020:1939 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 5 月 4 日

OpenShift Container Platform 4.4 现在提供了 **ose-machine-config-operator-container** 的更新。有关更新的详情，请查看 [RHSA-2020:1939](#) 公告。

1.8.6. RHSA-2020:1940 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 5 月 4 日

OpenShift Container Platform 4.4 现在提供了 **ose-cluster-policy-controller-container** 的更新。有关更新的详情，请查看 [RHSA-2020:1940](#) 公告。

1.8.7. RHSA-2020:1942 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 5 月 4 日

OpenShift Container Platform 4.4 现在提供了 **presto-container** 的更新。有关更新的详情请查看 [RHSA-2020:1942](#) 公告。

1.8.8. RHBA-2020:2133 - OpenShift Container Platform 4.4.4 程序错误修复更新

发布日期：2020 年 5 月 18 日

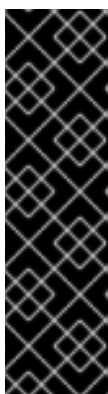
OpenShift Container Platform release 4.4.4 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:2133](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2132](#) 公告提供。

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 4.4.4 容器镜像列表](#)

1.8.8.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.9. RHSA-2020:2136 - Important: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 5 月 18 日

OpenShift Container Platform 4.4 现在提供了 **cluster-image-registry-operator** 的更新。有关更新的详情请查看 [RHSA-2020:2136](#) 公告。

1.8.10. RHBA-2020:2180 - OpenShift Container Platform 4.4.5 程序错误修复更新

发布日期：2020 年 5 月 26 日

OpenShift Container Platform release 4.4.5 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:2180](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2179](#) 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 4.4.5 容器镜像列表

1.8.10.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅 [使用 web 控制台更新集群](#) 以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.11. RHBA-2020:2310 - OpenShift Container Platform 4.4.6 程序错误修复更新

发布日期：2020 年 6 月 1 日

OpenShift Container Platform release 4.4.6 现已正式发布。此程序错误修正列表包括在 [RHBA-2020:2310](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2309](#) 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 4.4.6 容器镜像列表

1.8.11.1. 程序错误修复

- 在以前的版本中，对 Samples Operator 实现断开连接的支持会给一些用户造成问题。**samplesRegistry** 覆盖可以应用到基于 CVO 的 Jenkins 镜像流，这些镜像流在其它场景中使用 **samplesRegistry** 覆盖。在这个版本中，不再需要 **samplesRegistry** 覆盖，避免出现之前版本中的相关问题。(BZ#1824280)
- 在以前的版本中，**Installed Operators** 页面中的操作对象列表可能会显示来自自定义资源 **status.conditions** 的状态，其中没有 **status: true**，这代表显示的状态可能不正确。Web 控制台现在只显示 **status: true** 的状态。(BZ#1829591)
- 在以前的版本中，如果后续版本中删除了较早版本的示例模板，因为需要更新缺少的模板被错误跟踪，则后续版本的升级会失败。在这个版本中，升级过程不再更新之前版本中存在但还没有升级到的模板。(BZ#1832344)

- 在以前的版本中，当 Cluster Version Operator 试图通过 HTTPS 提供指标数据，但无法找到 TLS 密钥和证书时，操作会失败。在这个版本中，monitoring Operator 会创建一个 TLS 密钥和证书，以便 Cluster Version Operator 能够通过 HTTPS 提供指标服务。(BZ#1835483)
- 在以前的版本中，自定义 worker 或 master VM 规格的唯一方法是在安装前自定义 RHV 或 oVirt 模板，然后配置环境变量来让安装程序使用该模板。在这个版本中，MachinePool 对象已对这个平台实现，并在 `install-config.yaml` 文件中公开。现在，可以成功使用 MachinePool 配置中包含的规格创建 worker 和 master 虚拟机实例。由于现在支持不同的磁盘大小，所以默认的磁盘大小更新为 120 GB。(BZ#1835795)
- 在以前的版本中，不正确的配额行为可能会导致部署或构建 pod 失败。在这个版本中，构建控制器会被更新，从而可以正确地处理构建的配额。(BZ#1835913)
- 在以前的版本中，当用户使用 CLI 或 YAML 创建 PipelineRun 对象时，web 控制台会停止响应。在这个版本中，增加了相应的检查来避免 web 控制台错误。(BZ#1838792)

1.8.11.2. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.12. RHBA-2020:2445 - OpenShift Container Platform 4.4.8 程序错误更新

发布日期：2020 年 6 月 15 日

OpenShift Container Platform release 4.4.8 现已正式发布。此程序错误修正列表包括在 [RHBA-2020:2445](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2444](#) 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 4.4.8 容器镜像列表](#)

1.8.12.1. 功能

1.8.12.1.1. 自动 control plane 证书恢复

OpenShift Container Platform 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](#)。

1.8.12.2. 程序错误修复

- 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 Enterprise Linux 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#1821638)

- 在以前的版本中，Elasticsearch Operator 和 Cluster Logging Operator 不会协调 Fluentd 注入的 CA Bundle 内容。这会导致 Fluentd 和 Kibana 缺少卷挂载到带有注入的 CA 捆绑包的配置映射中。现在，配置映射的内容会在协调的过程中获取，以确保卷被挂载。这可让 Fluentd 和 Kibana 正确挂载 CA 捆绑包配置映射，且认证可以再次工作。(BZ#1833288)
- 因为 OpenShift Container Platform 代码中存在不正确的条件，`oc adm node drain` 命令在排空节点时没有正确考虑守护进程集和附加到 pod 的本地数据。逻辑已被修复，因此在排空节点时会考虑所有 pod。当尝试排空具有守护进程集的 pod 的节点时，或者在 pod 附加了本地卷数据时，`oc adm node drain` 命令现在会失败，建议使用会忽略这两个情况的标记。(BZ#1835739)
- 在以前的版本中，在 web 控制台中，当尝试编辑 YAML 文件时，Safari 网页浏览器中的 JavaScript 异常会导致 YAML 编辑页面永远无法加载。现在，这个问题已被解决，允许 YAML 文件编辑在 Safari Web 浏览器中正常工作。(BZ#1838815)
- 在以前的版本中，Web 控制台中的 **Installed Operators** 列假定所有已安装的 Operator 都有订阅。因为 Package Server Operator 没有订阅，所以它的状态会被错误地显示为 remove（即使它实际是存在的）。已将 Package Server Operator 状态修复为不依赖于其订阅状态，因此它现在可以在 Installed Operators 页中正确显示。(BZ#1840647)
- 从 web 控制台的 **Developer** 视角导航到 **Advanced** → **Project Details** → **Inventory** 部分时，部署配置不会被列出。部署配置现已被跟踪，并包含在仪表板的 **Inventory** 部分。(BZ#1825975)
- 在以前的版本中，pod 日志页面不包含指示所选容器的查询字符串参数。这会导致带有多个容器的 pod 在刷新页面或访问页面 URL 时报告不正确的容器日志。添加了一个新的查询字符串参数，URL 会显示哪些容器日志要被显示。(BZ#1827197)
- 在以前的版本中，在搜索页面中列出 OLM 订阅时，web 控制台只会显示名称、命名空间和创建日期。Web 控制台现在显示额外的 OLM 订阅详情。(BZ#1827746)
- 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#1831008)
- Cloud Credential Operator (CCO) 对其 **CredentialsRequest** CR 进行了特殊处理，需要存在云根凭证。如果缺少云根凭证，CCO 无法协调其自身只读 **CredentialsRequest** CR。这个问题已通过使用只读 **CredentialsRequest** 凭证来验证只读 **CredentialsRequest** 来解决。现在，当删除云根凭证时，CCO 不会降级。(BZ#1838810)
- 在以前的版本中，当点击 Pipeline Builder 中没有关联任务的 **Task** bubble 时会出现一个空白屏幕。这个问题已通过将节点转换为一个列表节点被解决，您可以对其进行更改。现在，您可以更新不再指向 **Task** 或 **ClusterTask** 资源的任务引用。(BZ#1840954)
- 因为 Cluster Operator reason 字段中的 API 服务器错误被错误报告，Operator 文件系统示例被错误地报告。另外，操作 API 服务器对象时实际 API 服务器错误的详情没有提供具体故障类型的

详情。这会导致报告错误不正确。现在，Sample Operator 文件系统错误会在 degraded reason 字段中作为文件系统错误报告，而 degraded reason 字段中报告的 API 服务器错误会包括特定的错误类型。(BZ#1842560)

- 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#1843732)
- 在以前的版本中，在 Azure 上运行的集群中的 RHEL 8 虚拟机可能会丢失网络连接。这是因为 RHEL 的 Hyper-V netvsc 驱动中的一个缺陷所致。这个程序错误已在 RHEL 中解决，相关更新现在可用于集群中使用的 RHEL VM。因此，在 Azure 上运行的集群不再遇到 netvsc 驱动程序问题导致的网络连接问题。(BZ#1841900)

这个版本还引进了以下改进：

- 为 OpenShift Container Platform 添加了一个功能增强来扩展 `oc adm release mirror` 命令。在没有与互联网有活跃连接的集群中可以完成集群升级。在以前，需要手动步骤来创建包含镜像更新验证所需的签名数据的配置映射。现在，命令会自动创建并应用包含发行镜像签名的配置映射清单，Cluster Version Operator 用来验证已镜像的发行版本。(BZ#1837675)

1.8.12.3. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.13. RHSA-2020:2403 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 6 月 15 日

OpenShift Container Platform 4.4 现在提供了 **containernetworking-plugins** 的更新。有关更新的详情请查看 [RHSA-2020:2403](#) 公告。

1.8.14. RHSA-2020:2448 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 6 月 15 日

OpenShift Container Platform 4.4 现在提供了 **openshift** 的更新。有关更新的详情请查看 [RHSA-2020:2448](#) 公告。

1.8.15. RHSA-2020:2449 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 6 月 15 日

OpenShift Container Platform 4.4 现在提供了 **openshift-enterprise-builder-container** 的更新。有关更新的详情请查看 [RHSA-2020:2449](#) 公告。

1.8.16. RHBA-2020:2580 - OpenShift Container Platform 4.4.9 程序错误修正更新

发布日期：2020 年 6 月 22 日

OpenShift Container Platform release 4.4.9 现已正式发布。此程序错误修正列表包括在 [RHBA-2020:2580](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2579](#) 和 [RHEA-2020:2623](#) 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 4.4.9 容器镜像列表](#)

1.8.16.1. 功能

1.8.16.1.1. 添加了 Node.js Jenkins Agent v10 和 v12

jenkins-agent-nodejs-10-rhel7 和 **jenkins-agent-nodejs-12-rhel7** 镜像现已添加到 OpenShift Container Platform 中。这些新镜像允许 Jenkins Pipelines 升级为使用 Node.js Jenkins Agent 的 v10 或 v12。Node.js v8 Jenkins Agent 现已弃用，但将继续提供。对于现有集群，您必须手动升级 Node.js Jenkins Agent，该功能可针对命名空间执行。按照以下步骤完成手动升级：

1. 选择要升级 Jenkins Pipelines 的项目：

```
$ oc project <project_name>
```

2. 导入新的 Node.js Jenkins Agent 镜像：

```
$ oc import-image nodejs openshift4/jenkins-agent-nodejs-10-rhel7 --  
from=registry.redhat.io/openshift4/jenkins-agent-nodejs-10-rhel7 --confirm
```

此命令导入 v10 镜像。如果您希望使用 v12，相应地更新镜像规格。

3. 使用您导入的新功能覆盖当前 Node.js Jenkins Agent:

```
$ oc label is nodejs role=jenkins-slave --overwrite
```

4. 在 Jenkins 日志中验证是否配置了新的 Jenkins Agent 模板：

```
$ oc logs -f jenkins-1-<pod>
```

如需更多信息，请参阅 [Jenkins 代理](#)。

1.8.16.1.2. IBM Power 系统

在这个版本中，IBM Power Systems 与 OpenShift Container Platform 4.4 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。

1.8.16.1.3. IBM Z 和 LinuxONE

在这个版本中，IBM Z 和 LinuxONE 与 OpenShift Container Platform 4.4 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：
 - 容器原生虚拟化 (CNV)
 - 日志转发
 - 精度时间协议 (PTP) 硬件
 - CSI 卷快照
 - CSI 卷克隆
 - 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
 - etcd 集群 Operator
- 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 4.4, 但不适用于 x86 上的 OpenShift Container Platform 4.4 :
 - 在 IBM System Z 上为附加了 ficon 的 ECKD 存储的虚拟机启用了 HyperPAV。

1.8.16.2. 程序错误修复

- 在虚拟机和虚拟机模板向导中, virtIO 是附加一个 CD-ROM 时的默认接口。但是, virtIO CD-ROM 无法通过虚拟机的验证过程, 因此不能被创建。作为临时解决方案, 在创建虚拟机和虚拟机模板时, 选择 **SATA** 作为 CD-ROM 接口。 ([BZ#1817394](#))
- 在以前的版本中, 当从 Kibana 仪表盘登出时, 仍可以从新浏览器标签页重新登录而无需指定登录凭证。这是因为 signoff 链接指向为 Kibana 提供安全性的 OAuth 代理的错误处理器。现在, 在尝试重新访问 Kibana 仪表盘时, 强制登录凭证已被修复。 ([BZ#1823305](#))
- **Installed Operators** 页面中的 **View more** 链接现在可以链接到正确的页面。 ([BZ#1824255](#))
- 在这个版本中, Web 控制台中操作对象视图中的 **Status** 列已被更新, 以显示 **Details** 和 **YAML** 视图中可用的最新状态。 ([BZ#1831808](#))
- 在这个版本中, **eventSources** API 组被更新到最新支持的 API 组 **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** 视图被识别。 ([BZ#1836807](#))
- 在以前的版本中, 无法通过 web 控制台中的 **Developer** 视角的 **Add** 视图来指定 Knative 服务的环境变量。因此, 需要环境变量的应用程序可能无法按预期工作。在这个发行版本中, 用户可从 **Add** 视图添加环境变量。 ([BZ#1839115](#))
- 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#1840812](#))
- 在将 Octavia 从 OpenStack 13 升级到 16 后, 支持 UDP 侦听程序, 并删除通过 TCP 协议强制使用 DNS 解析策略。这个更改要求将新的监听程序添加到指定 UDP 协议的现有 DNS 服务中。旧

的用于现有 DNS 负载均衡器的 Amphora 镜像不支持新的监听器，并导致监听器创建失败。在这个版本中，需要 UDP 的 DNS 服务被重新创建，从而导致使用新的 Amphora 版本重新创建负载均衡器。重新创建服务和负载均衡器会导致 DNS 解析出现一些停机时间。此过程完成后，会使用所有需要的监听程序创建 DNS 服务的负载均衡器。(BZ#1841029)

- 在以前的版本中，当 `operatorframework.io/cluster-monitoring=true` 注解被设置为 `true` 时，Web 控制台不会创建 OpenShift Monitoring Prometheus Operator 所需的角色绑定来收集 Operator 指标。这个问题已在本发行版本中解决。(BZ#1841149)
- 在以前的版本中，自动扩展需要跨节点和 Machine 对象的供应商 ID 完全匹配，如果机器配置指定了使用混合级干的资源组名称，则该 ID 并不完全匹配。在这种情况下，自动扩展无法识别机器有节点，并在 15 分钟后终止机器。在这个发行版本中，自动扩展会忽略供应商 ID 中的字母问题单，这样它们可以与问题单匹配。(BZ#1841478)
- 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#1845819)
- 在以前的版本中，SELinux 权限阻止了对 Azure 平台上挂载的卷的读/写访问权限。在这个版本中，SELinux 布尔值被更新为与 RHCOS 8.x 匹配，并允许正确的访问权限。(BZ#1845830)

1.8.16.3. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.17. RHSA-2020:2583 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 6 月 22 日

OpenShift Container Platform 4.4 现在提供了对 `python-psutil` 的更新。有关更新的详情请查看 [RHSA-2020:2583](#) 公告。

1.8.18. RHBA-2020:2713 - OpenShift Container Platform 4.4.10 程序错误修正更新

发布日期：2020 年 6 月 29 日

OpenShift Container Platform release 4.4.10 现已正式发布。此程序错误修正列表包括在 [RHBA-2020:2713](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2734](#) 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 4.4.10 容器镜像列表

1.8.18.1. 程序错误修复

- 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。当应用程序试图解析标头值时，这个非标准标头会导致问题。在这个版本中，ingress 控制器不再指定 **Forwarded** 标头中的 **proto-version** 参数。[\(BZ#1816544\)](#)
- 在以前的版本中，MachineHealthCheck 上的 **maxUnhealthy** 字段的值可以接受多个格式，如 **10**、**"10"**、或 **"10%"**。引号中的数值即使不包含百分比符号，也被认为是百分比值。对 **maxUnhealthy** 值的这种解释可能与用户的意向不匹配，如果机器原本不希望被修复或者没有在机器应该被修复时，它们可能已被修复。在这个发行本中，只有包含百分比符号的值才会解释为百分比。例如，**10** 和 **"10"** 现在解释为 10，而不是 10%。[\(BZ#1816606\)](#)
- 在以前的版本中，指标不会在 IPv6 地址上绑定，且无法提取。在这个版本中，指标数据可以在 IPv6 地址中被正确地抓取。[\(BZ#1819770\)](#)
- 在以前的版本中，**Edit ClusterServiceVersion** 出现在 **ClusterServiceVersion** 对象的 **Actions** 菜单中，这可能会错误地让用户编辑 **ClusterServiceVersion** 对象。在这个版本中，**Edit ClusterServiceVersion** 从 **ClusterServiceVersion** 对象的 **Actions** 菜单中删除。[\(BZ#1827306\)](#)
- 在以前的版本中，如果没有资源，某些资源没有空状态 **None**。缺少这个状态与其他资源不一致，这会导致模糊不清。在这个发行版本中，如果没有资源，这些资源现在处于 **None** 空状态。[\(BZ#1827766\)](#)
- 之前，masthead 下拉菜单项目之间的时间间隔会大于应该。这个显示问题已解决。[\(BZ#1829030\)](#)
- 在以前的版本中，Pipeline Builder 错误地认为空字符串 ("") 代表没有默认值。但是，在没有作为默认值为空字符串的情况下，一些由 Operator 提供的任务将无法正常工作。在这个版本中，OpenShift Pipeline Operator 接受的任何值都作为默认值（包括空字符串）被识别为一个有效的默认值。[\(BZ#1829568\)](#)
- 在以前的版本中，OpenShift Controller Manager Operator 中的控制器不会使用命名的工作队列，一些指标（如 **workqueue_depth**）不会出现在 Prometheus 中。在这个版本中，控制器使用命名的工作队列，这些指标会出现在 Prometheus 中。[\(BZ#1832839\)](#)
- 在以前的版本中，如果为 IPv6 配置了用户定义的 **PROV_IFACE** 接口，并使用本地链接（link-local）地址而不是可全局路由的地址，OpenShift Container Platform 中的 Ironic 容器将无法启动。在这个发行版本中，容器启动脚本除全局地址外还接受本地链接寻址。[\(BZ#1838083\)](#)
- 在以前的版本中，OVN 容器请求的 CPU 和 RAM 比需要多，用户工作负载会减少。在这个版本中，OVN 请求会被调整以匹配实际要求。[\(BZ#1844245\)](#)
- 在以前的版本中，Terraform 步骤 **openstack_networking_floatingip_associate_v2** 没有列出它所有的依赖步骤，从而导致独立步骤的缺失有时会导致 Terraform 作业失败，特别是在超载系统中。在这个版本中，依赖 Terraform 步骤列为 **dependent_on** 来强制按正确顺序运行 Terraform 步骤。[\(BZ#1847957\)](#)

1.8.18.2. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.19. RHSA-2020:2737 - Important: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 6 月 29 日

OpenShift Container Platform 4.4 现在提供了对 **jenkins-2-plugins** 的更新。有关更新的详情请查看 [RHSA-2020:2737](#) 公告。

1.8.20. RHBA-2020:2786 - OpenShift Container Platform 4.4.11 程序错误修复更新

发布日期：2020 年 7 月 6 日

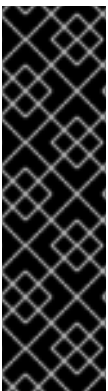
OpenShift Container Platform release 4.4.11 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:2786](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2785](#) 公告提供。

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 4.4.11 容器镜像列表](#)

1.8.20.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.21. RHSA-2020:2789 - Low: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 7 月 6 日

OpenShift Container Platform 4.4 现在提供了 **ose-baremetal-operator-container** 的更新。有关更新的详情请查看 [RHSA-2020:2789](#) 公告。

1.8.22. RHSA-2020:2790 - Low: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 7 月 6 日

OpenShift Container Platform 4.4 现在提供了 **ose-azure-machine-controllers-container** 的更新。有关更新的详情请查看 [RHSA-2020:2790](#) 公告。

1.8.23. RHSA-2020:2792 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 7 月 6 日

OpenShift Container Platform 4.4 现在提供了 **grafana-container** 的更新。有关更新的详情请查看 [RHSA-2020:2792](#) 公告。

1.8.24. RHSA-2020:2793 - Low: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 7 月 6 日

OpenShift Container Platform 4.4 现在提供了 **atomic-openshift-descheduler-container** 的更新。有关更新的详情请查看 [RHSA-2020:2793](#) 公告。

1.8.25. RHBA-2020:2871 - OpenShift Container Platform 4.4.12 程序错误修复更新

发布日期：2020 年 7 月 13 日

OpenShift Container Platform release 4.4.12 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:2871](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2875](#) 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 4.4.12 容器镜像列表](#)

1.8.25.1. 程序错误修复

- 在以前的版本中，不支持在 **ovn-octavia** 驱动的同一直线上使用多个监听程序，并被阻断。在这个版本中，它被支持且不需要阻断它。不同协议的多个监听程序可以在相同的端口公开。这意味着，在使用 **ovn-octavia** 时 DNS 服务可以在 TCP 和 UDP 协议中公开端口 53。([BZ#1847558](#))
- 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顺序使用 DNS 服务器。([BZ#1851267](#))
- 在以前的版本中，如果 Fluentd 是使用 CLO 独立部署，它会因为缺少配置详情而崩溃。在这个版本中，提供了一个空的 Fluentd 配置来启用 pod 的启动，并添加了一个状态来告知用户需要手动干预。([BZ#1851381](#))
- 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#1852249](#))

1.8.25.2. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅 [使用 web 控制台更新集群](#) 以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.26. RHSA-2020:2878 - Low: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 7 月 13 日

OpenShift Container Platform 4.4 现在提供了 **ose-cloud-credential-operator-container** 的更新。有关更新的详情请查看 [RHSA-2020:2878](#) 公告。

1.8.27. RHBA-2020:2913 - OpenShift Container Platform 4.4.13 程序错误修复更新

发布日期：2020 年 7 月 21 日

OpenShift Container Platform release 4.4.13 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:2913](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:2912](#) 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 4.4.13 容器镜像列表](#)

1.8.27.1. 功能

1.8.27.1.1. 升级 Metering Operator

现在，您可以升级 Metering Operator。之前，需要先卸载当前的 metering 安装，然后重新安装 Metering Operator 的新版本。如需更多信息，请参阅[升级 metering](#)。

1.8.27.2. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.28. RHSA-2020:2926 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 7 月 21 日

OpenShift Container Platform 4.4 现在提供了 **openshift-enterprise-builder-container** 的更新。有关更新的详情请查看 [RHSA-2020:2926](#) 公告。

1.8.29. RHSA-2020:2927 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 7 月 21 日

OpenShift Container Platform 4.4 现在提供了 **openshift** 的更新。有关更新的详情请查看 [RHSA-2020:2927](#) 公告。

1.8.30. RHBA-2020:3075 - OpenShift Container Platform 4.4.14 程序错误修复更新

发布日期：2020 年 7 月 28 日

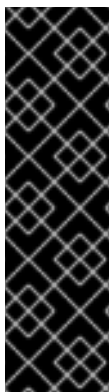
OpenShift Container Platform release 4.4.14 现已正式发布。此程序错误修正列表包括在 [RHBA-2020:3075](#) 和 [RHBA-2020:3288](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3074](#) 公告提供。

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 4.4.14 容器镜像列表](#)

1.8.30.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.31. RHSA-2020:3078 - Low: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 7 月 28 日

OpenShift Container Platform 4.4 现在提供了 **ose-cluster-machine-approver-container** 的更新。有关更新的详情请查看 [RHSA-2020:3078](#) 公告。

1.8.32. RHBA-2020:3128 - OpenShift Container Platform 4.4.15 程序错误修复更新

发布日期：2020 年 8 月 4 日

OpenShift Container Platform release 4.4.15 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3128](#) 公告中。此更新包括的 RPM 软件包由 [RHBA-2020:3127](#) 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 4.4.15 容器镜像列表

1.8.32.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.33. RHBA-2020:3237 - OpenShift Container Platform 4.4.16 程序错误修复更新

发布日期：2020 年 8 月 6 日

OpenShift Container Platform release 4.4.16 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:3237](#) 公告中。此更新包括的 RPM 软件包由 [RHBA-2020:3238](#) 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 4.4.16 容器镜像列表

1.8.33.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.34. RHBA-2020:3334 - OpenShift Container Platform 4.4.17 程序错误修复更新

发布日期：2020 年 8 月 18 日

OpenShift Container Platform release 4.4.17 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:3334](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3335](#) 公告提供。

因篇幅原因，没有在这个公告中包括此版本的所有容器镜像信息。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 4.4.17 容器镜像列表](#)

1.8.34.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.35. RHBA-2020:3440 - OpenShift Container Platform 4.4.18 程序错误修复更新

发布日期：2020 年 8 月 25 日

OpenShift Container Platform release 4.4.18 现已正式发布。。此程序错误修正列表包括在 [RHBA-2020:3440](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3441](#) 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 4.4.18 容器镜像列表](#)

1.8.35.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.36. RHBA-2020:3514 - OpenShift Container Platform 4.4.19 程序错误修复更新

发布日期：2020 年 9 月 1 日

OpenShift Container Platform release 4.4.19 现已正式发布。。此程序错误修正列表包括在 [RHBA-2020:3514](#) 公告中。此更新包括的 RPM 软件包由 [RHBA-2020:3515](#) 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 4.4.19 容器镜像列表](#)

1.8.36.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.37. RHSA-2020:3579 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 9 月 1 日

OpenShift Container Platform 4.4 现在提供了 **openshift** 的更新。有关更新的详情请查看 [RHSA-2020:3579](#) 公告。

1.8.38. RHSA-2020:3580 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 9 月 1 日

OpenShift Container Platform 4.4 现在提供了 **openshift-enterprise-builder-container** 的更新。有关更新的详情请查看 [RHSA-2020:3580](#) 公告。

1.8.39. RHBA-2020:3564 - OpenShift Container Platform 4.4.20 程序错误修复更新

发布日期：2020 年 9 月 8 日

OpenShift Container Platform release 4.4.20 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:3564](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3565](#) 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 4.4.20 容器镜像列表](#)

1.8.39.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.40. RHSA-2020:3625 - Important: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 9 月 8 日

OpenShift Container Platform 4.4 现在提供了对 **jenkins-2-plugins** 的更新。有关更新的详情请查看 [RHSA-2020:3625](#) 公告。

1.8.41. RHBA-2020:3605 - OpenShift Container Platform 4.4.21 程序错误修复更新

发布日期：2020 年 9 月 15 日

OpenShift Container Platform release 4.4.21 现已正式发布。此程序错误修正列表包括在 [RHBA-2020:3605](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3606](#) 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 4.4.21 容器镜像列表](#)

1.8.41.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.42. RHBA-2020:3715 - OpenShift Container Platform 4.4.23 程序错误修复更新

发布日期：2020 年 9 月 22 日

OpenShift Container Platform release 4.4.23 现已正式发布。此程序错误修正列表包括在 [RHBA-2020:3715](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3716](#) 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 4.4.23 容器镜像列表

1.8.42.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.43. RHSA-2020:3783 - Moderate: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 9 月 22 日

OpenShift Container Platform 4.4 现在提供了 [golang.org/x/text](#) 的更新。有关更新的详情请查看 [RHSA-2020:3783](#) 公告。

1.8.44. RHBA-2020:3764 - OpenShift Container Platform 4.4.26 程序错误修复更新

发布日期：2020 年 10 月 1 日

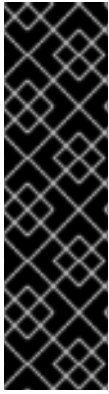
OpenShift Container Platform release 4.4.26 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:3764](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:3765](#) 公告提供。

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 4.4.26 容器镜像列表

1.8.44.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.45. RHBA-2020:4063 - OpenShift Container Platform 4.4.27 程序错误修复更新

发布日期：2020 年 10 月 13 日

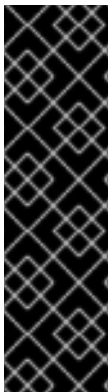
OpenShift Container Platform release 4.4.27 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:4063](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:4064](#) 公告提供。

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 4.4.27 容器镜像列表](#)

1.8.45.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅 [使用 web 控制台更新集群](#) 以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.46. RHSA-2020:4220 - Important: OpenShift Container Platform 4.4 安全更新

发布日期：2020 年 10 月 13 日

OpenShift Container Platform 4.4 现在提供了 [openshift-jenkins-2-container](#) 的更新。有关更新的详情请查看 [RHSA-2020:4220](#) 公告。

1.8.47. RHBA-2020:4224 - OpenShift Container Platform 4.4.29 程序错误修复更新

发布日期：2020 年 10 月 27 日

OpenShift Container Platform release 4.4.29 现已正式发布。此更新包括的程序错误修正列表包括在 [RHBA-2020:4224](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:4225](#) 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 4.4.29 容器镜像列表

1.8.47.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.48. RHBA-2020:4321 - OpenShift Container Platform 4.4.30 程序错误修复更新

发布日期：2020 年 11 月 11 日

OpenShift Container Platform release 4.4.30 现已正式发布。此程序错误修正列表包括在 [RHBA-2020:4321](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:4322](#) 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 4.4.30 容器镜像列表

1.8.48.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.49. RHBA-2020:5122 - OpenShift Container Platform 4.4.31 程序错误修复更新

发布日期：2020 年 12 月 2 日

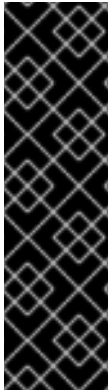
OpenShift Container Platform release 4.4.31 现已正式发布。其程序错误修正列表包括在 [RHBA-2020:5122](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2020:5123](#) 公告提供。

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 4.4.31 容器镜像列表](#)

1.8.49.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.50. RHBA-2021:0029 - OpenShift Container Platform 4.4.32 程序错误修复更新

发布日期：2021 年 1 月 13 日

OpenShift Container Platform release 4.4.32 现已正式发布。其程序错误修正列表包括在 [RHBA-2021:0029](#) 公告中。此更新中包括的 RPM 软件包由 [RHSA-2021:0030](#) 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 4.4.32 容器镜像列表](#)

1.8.50.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

1.8.51. RHSA-2021:0281 - OpenShift Container Platform 4.4.33 程序错误修复和安全更新

发布日期：2021 年 2 月 2 日

OpenShift Container Platform release 4.4.33 现已正式发布,其中包括安全更新。其程序错误修正列表包括在 [RHSA-2021:0281](#) 公告中。此更新中包括的 RPM 软件包由 [RHSA-2021:0282](#) 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 4.4.33 容器镜像列表](#)

1.8.51.1. 升级

要将现有 OpenShift Container Platform 4.4 集群升级到此最新版本，请参阅[使用 web 控制台更新集群](#)以获取相关说明。



重要

如果您要从 OpenShift Container Platform 4.3.3 或更早版本升级到这个版本，则必须在升级完成后重启所有 pod。

这是因为服务 CA 会在 OpenShift Container Platform 4.3.5 中自动轮转。升级过程中会轮转服务 CA，之后需要重启服务以确保所有服务在上一个服务 CA 过期前都使用新的服务 CA。

这个手动重启操作只需要执行一次，后续的升级和轮转将在服务 CA 过期前确保重启，而无需人工干预。

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 4.4 集群中，所有的 master 必需是 4.4，所有节点也必需是 4.4。如果安装了旧版本的 **oc**，则无法使用 OpenShift Container Platform 4.4 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 ^[a] (oc Client)
X.Y (Server)	1	3
X.Y+N ^[a] (Server)	2	1

[a] 其中 N 是一个大于 1 的数值。

- 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。