



OpenShift Container Platform 4.3

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 4.3 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 © 2020 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 4.3 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	9
1.4. 程序错误修复	11
1.5. 技术预览功能	17
1.6. 已知问题	20
1.7. 异步勘误更新	24
第 2 章 OPENSIFT CONTAINER PLATFORM 版本政策	47

第 1 章 OPENSIFT CONTAINER PLATFORM 4.3 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-2020:0062) 现已发布。此发行版本使用 [Kubernetes 1.16](#) 和 CRI-O 运行时。OpenShift Container Platform 4.3 的新功能、改变以及已知的问题包括在此文档中。



注意

它比 OpenShift Container Platform 4.2 使用的 Kubernetes (Kubernetes 1.14) 提高了两个版本。

OpenShift Container Platform 4.3 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 4.3 需要运行在 Red Hat Enterprise Linux 7.6 及更新的版本，或 Red Hat Enterprise Linux CoreOS 4.3 上。

您必须使用 Red Hat Enterprise Linux CoreOS (RHCOS) 作为 control plane (或 master) 的系统，而 compute (或 worker) 系统可以使用 RHCOS，或 Red Hat Enterprise Linux 7.6 及更新的次版本。



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。

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. OpenShift Container Platform 升级分阶段部署

在 OpenShift Container Platform 4.1 中，红帽引进了升级频道的概念，用于为集群推荐适当的升级版本。升级频道分离升级策略，并可用来控制更新的节奏。频道与 OpenShift Container Platform 的次要版本关联。例如，OpenShift Container Platform 4.3 频道永远不会包括到版本 4.4 的升级。这可确保管理员明确决定升级到下一个 OpenShift Container Platform 次要版本。频道只控制更新，且不会影响到安装的集群版本；指定补丁级别的 OpenShift Container Platform 中的 **openshift-install** 二进制文件始终会安装该补丁级别。

您必须选择与计划升级到的 OpenShift Container Platform 版本相对应的升级频道版本。OpenShift Container Platform 4.3 包括从之前的 4.2 版本的升级。

有关更新类型和升级频道的更多信息，请参阅 [OpenShift 4.x 升级分阶段部署](#)。

因为把升级发布到频道的过程是根据 Red Hat Service Reliability engineering (SRE) 团队的数据向客户逐渐推出的，所以您可能不会在 web 控制台中马上看到从 4.2.z 升级到 4.3 的更新信息。

1.2.1.2. 支持 FIPS 加密

现在，您可以安装一个使用经 FIPS 验证的/IUT (Implementation Under Test) 加密库的 OpenShift Container Platform 集群。OpenShift Container Platform 在 Red Hat Enterprise Linux (RHEL) 和 Red Hat CoreOS (RHCOS) 中使用特定的 FIPS 验证的/IUT (Implementation Under Test) 模块用于使用它们的操作系统组件。如需更多信息，请参阅 [FIPS 加密的支持](#)。

1.2.1.3. 在 AWS、Azure 或 GCP 上部署私有集群

您可以将私有集群安装到

- Amazon Web Services (AWS) 上的现有 VPC。
- Google Cloud Platform (GCP) 上的现有 VPC。
- Microsoft Azure 上的现有 Azure Virtual Network (VNet)。

要在这些云平台上创建私有集群，您必须提供一个现有的专用 VPC/VNet 和子网来托管集群。安装程序将 Ingress Operator 和 API 服务器配置为只可以从私有网络访问。

如需有关将私有集群部署到支持的云平台的更多信息，请参阅 [AWS](#)、[Azure](#) 和 [GCP](#) 的安装指南。

1.2.2. 安全性

1.2.2.1. 服务证书 CA 自动化轮转

对于此发行版本，未来的 z-stream 更新中会提供自动服务 CA 轮转功能。在以前的版本中，服务 CA 不会自动续订，从而造成服务中断并需要手动干预进行修复。服务 CA 和签名密钥现在会在过期前自动轮转。这可让管理员预先规划其环境，避免服务中断。

1.2.2.2. 加密存储在 etcd 中的数据

现在，您可以[对存储在 etcd 中的数据进行加密](#)。在集群中启用对 etcd 进行加密的功能可为数据的安全性提供额外的保护层。

启用 etcd 加密时，以下 OpenShift API 服务器和 Kubernetes API 服务器资源将被加密：

- Secrets
- ConfigMaps
- Routes
- OAuth 访问令牌
- OAuth 授权令牌

1.2.3. 集群监控

1.2.3.1. web 控制台中的 PromQL 查询浏览器的改进

现在，OpenShift Container Platform Web 控制台中使用的 PromQL 查询浏览器的性能已有所改进。

1.2.3.2. 为 KubeletTooManyPods 警报使用 Pod 容量指标

KubeletTooManyPods 警报现在使用 Pod 容量指标作为阈值而不是固定数字。

1.2.3.3. 监控您自己的服务（技术预览）

现有的监控堆栈可以扩展，您可以为自己的服务配置监控功能。

1.2.3.4. 在 web 控制台中查询指标（技术预览）

现在可以通过 OpenShift Container Platform Web 控制台中的 Developer 视角来查询指标。

1.2.4. 机器 API

1.2.4.1. 使用机器健康检查自动修复损坏的机器

一个被删除的机器实例不再会尝试重新创建新实例。相反，机器会进入一个失败阶段。您可以通过配置和部署机器健康检查，在一个机器池中自动修复损坏的机器。

监控 MachineHealthCheck 资源的控制器将检查您定义的状态。如果机器不能通过健康检查，会自动被删除并创建新的机器来代替它。删除机器之后，您会看到“机器被删除”事件。为限制删除机器造成的破坏性影响，控制器一次仅清空并删除一个节点。

若要停止检查，请删除其资源。

1.2.5. 日志记录

1.2.5.1. 日志转发（技术预览）

Log Forwarding API 能提供将容器和节点日志发送到目的地的方法，而目的地不一定由 OpenShift Container Platform 集群日志记录基础架构管理。目标端点可以在您的 OpenShift Container Platform 集群中，也可以在集群以外。日志转发提供了比使用 Fluentd 插件更容易的转发日志的方法，而无需将集群设置为非受管状态。请参阅[使用 Log Forwarding API 转发日志](#)来获得更详细的信息。

1.2.6. 开发者体验

1.2.6.1. OpenShift Do 的改进

OpenShift Do (odo) 有几个改进，主要针对应用程序部署的用户体验：

- **PushTimeout** 已添加为可配置的 wait 参数。
- 通过更多输出和信息提示，服务目录和组件的创建有所改进。
- 构架支持增加了对 IBM Z 和 Power 平台的支持，提供可用于安装的二进制文件。

1.2.6.2. Helm（技术预览）

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。

1.2.7. Web 控制台

1.2.7.1. 新的项目仪表盘

新的**Project (项目)** 仪表盘现在可从管理员和开发者视角访问。此仪表盘提供以下有关项目的信息：

- status/health
- 外部链接
- inventory
- 使用率
- 资源配额
- 活动及主要消耗者

1.2.7.2. ConsoleLink 自定义资源定义中的新 NamespaceDashboard 选项

在 ConsoleLink 自定义资源定义中新增加了位置选项 **NamespaceDashboard**，可让您向项目仪表盘添加特定于项目的链接。

1.2.7.3. 提供集群范围的第三方用户界面

现在，您可以集成集群范围的第三方用户界面，以便使用 ConsoleLink 自定义资源定义来开发、管理并配置 Operator 支持的服务。

1.2.7.4. 新的 ConsoleYAMLSample 自定义资源定义

新的 **ConsoleYAMLSample** 自定义资源定义可随时动态地将 YAML 示例添加到任何 Kubernetes 资源中。

如需更多信息，请参阅[自定义 Web 控制台](#)。

1.2.7.5. 从 web 控制台访问支持问题单

现在，您可以在 web 控制台的帮助菜单中访问红帽支持问题单。

1.2.7.6. 查看安全漏洞

现在，您可以从 Web 控制台仪表盘查看容器漏洞。这会利用 Quay Operator，支持内部和外部 Quay registry。只有 Quay 管理的镜像才会报告安全漏洞。

1.2.7.7. 新用户管理部分

现在，可以通过 **User Resource** 来访问所有用户管理资源。

另外还添加了模拟用户的功能，这样您就可以查看用户使用控制台时可以看到什么信息。

1.2.7.8. 创建警报接收器

现在，您可以创建警报接收器来获得与集群状态相关的警报信息。您可以创建 PagerDuty 和 Webhook 警报类型。

1.2.7.9. Developer Perspective (开发者视角)

现在，您可以使用开发者视角来：

- 创建无服务器应用程序及修订版本，并在修订版本间分割流量。
- 删除应用程序及其所有组件。
- 为项目中的用户分配 RBAC 权限。
- 使用绑定连接器将应用程序与 Service 绑定。

1.2.7.10. CSI 置备程序现在在存储类创建页面中显示

现在，存储类创建页面中会显示容器存储接口 (CSI) 置备程序。存储类在用户界面中是硬编码的；基于 CSI 的存储类是动态的，且没有静态名称。现在，用户可以在存储类创建页面中列出基于 CSI 的置备程序，也可以创建它。

1.2.8. 网络

1.2.8.1. 配置网络策略

OpenShift Container Platform 中提供了 Kubernetes **v1** NetworkPolicy 功能，但 Egress 策略类型和 IPBlock 除外。

NetworkPolicy 对 IPBlock 的支持有一定限制，它支持没有 **except** 的 IPBlock。如果创建的策略带有一个有 **except** 的 **ipBlock** 项，SDN Pods 的日志中会出现警告，策略中的整个 **ipBlock** 项都会被忽略。

1.2.8.2. Kuryr CNI 支持 Red Hat OpenStack Platform (RHOSP)

您可在使用 Kuryr SDN 的 RHOSP 13 和 16 上安装自定义集群。请参阅[在带有 Kuryr 的 OpenStack 上安装集群指南](#)。

1.2.9. 扩展

1.2.9.1. 集群最大限制

针对 OpenShift Container Platform 4.3 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. 存储

1.2.10.1. OpenShift Container Storage 4.2

现在，您可以部署、管理、监控和迁移 Red Hat OpenShift Container Storage 4.2 集群。如需更多信息，请参阅 [Red Hat OpenShift Container Storage 4.2 发行注记](#)。

1.2.10.2. 使用 iSCSI 的持久性存储

现在，OpenShift Container Platform 4.3 已完全支持使用 iSCSI 的持久性卷（以前为技术预览功能）。

1.2.10.3. 原始块卷支持

iSCSI 原始块卷现在被 OpenShift Container Platform 4.3 完全支持（以前为技术预览）。

使用 Cinder 的原始块卷现在还是一个技术预览功能。

1.2.10.4. CSI 卷扩展

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

1.2.10.5. 在 Local Storage Operator 中使用容忍功能

Local Storage Operator 现在可以容忍节点污点，您可以从污点节点置备本地卷。

1.2.11. Operator

1.2.11.1. Samples Operator

Samples Operator 在安装过程中自动识别集群架构，且不会在 Power 和 Z 架构中安装不兼容的 x86_64 内容。

Samples Operator 还使用 Prometheus metrics 收集有关哪个镜像流导入失败的信息，以及 Samples Operator 是否有无效配置。如果镜像流无法导入，或 Samples Operator 具有无效的配置，则会发送警报。

1.2.11.2. Image Registry Operator

Image Registry Operator 有以下改进：

- registry 管理状态在 Baremetal、vSphere 和 Red Hat Virtualization 平台上被设置为 **Removed**，这样就可以配置其他存储供应商。在置备存储之外，新安装必须将 registry 状态设置为 **Managed**。
- 当 registry 存储有变化时会发送警报，因为这可能导致数据丢失。

1.2.11.3. 简化的 OperatorHub 的镜像 (mirror)

假设在一个与网络断开连接的环境中运行一个对断开连接的集群和运行 **oc adm** 命令的工作站都可用的 registry，您现在可以通过以下三个步骤来对 OperatorHub 进行镜像：

1. 将 Operator 目录镜像 (mirror) 到容器镜像中，使用 **oc adm catalog build** 推送到断开连接的 registry 中。
2. 解析引用的 Operator 和应用镜像，并使用 **oc adm catalog mirror** 推送到断开连接的 registry 中。
3. 使用 **oc apply -f ./manifests** 在断开连接的集群中启用镜像的 (mirror) 目录。

详情请参阅[在受限网络中使用 Operator Lifecycle Manager](#)。

1.2.11.4. Operator 遥测和警报

Lifecycle Operator Manager (OLM) 现在会报告已安装的 Operator 信息。例如，OLM 会发送有关 Operator 转换到失败状态的警报。

1.3. 主要的技术变化

OpenShift Container Platform 4.3 包括以下显著的技术更改。

Operator SDK v0.12.0

OpenShift Container Platform 4.3 支持 Operator SDK v0.12.0 或更高版本。

Operator 测试工具 (scorecard v2) 现在包括以下改进：

- 将 Operator 测试分类为 required 和 optional。
- 配置测试选择以及 pass/fail 的行为。
- 提供自定义测试。

基于 Helm 的 Operator 的改进包括

- helm v3 支持，从 Operator SDK 0.14.0 开始。
- 基于角色的访问控制 (RBAC) 生成。

基于 Ansible 的 Operator 的增强包括

- 支持 Prometheus 指标。
- Red Hat Universal Base Image (UBI) 的使用。
- 基于 Molecule 的端到端的测试。

基于 Golang 的 Operator 的改进包括：

- OpenAPI spec 生成。
- Kubernetes 1.14 支持。
- 删除基于 **dep** 的项目。现在，所有 Go 项目都被构建为使用 Go 模块。删除 **operator-sdk new** 命令的 **--dep-manager** 标记。
- 所需的 Go 版本从 v1.10 更新到 v1.13。
- 支持 Prometheus 指标。

集群日志 Fluent 的 forward 配置改变

从 OpenShift Container Platform 4.3 开始，由新的 [Log Forwarding API](#) 功能所引入的变化改变了对 Fluentd **forward** 插件的支持。对于 4.3，您仍然可以使用 [Fluentd forward 协议](#)，而无需使用新的属于技术预览的日志转发功能。

要使用 Fluentd **forward** 协议，您必须创建一个 ConfigMap 对象来配置 **out_forward**，而不是编辑 **fluentd** ConfigMap 中的 **secure-forward.conf** 部分。另外，您还可以将配置所需的证书添加到挂载到 Fluentd Pod 的 Secret 中。请参阅 [使用 Fluentd Forward 插件将日志发送到外部设备](#)。

在 4.3 中，Fluentd **forward** 方法被弃用，并将在以后的版本中删除。

当您升级到 OpenShift Container Platform 4.3 时，所有现存的对 **fluentd** ConfigMap 的 **secure-forward.conf** 部分的修改都会被删除。在创建 **secure-forward** ConfigMap 对象时，可以在更新前复制您当前的 **secure-forward.conf** 内容。

1.3.1. 不支持的功能

集群日志记录不再允许通过编辑 Fluentd Daemonset 来转发日志

由于新的 Log Forwarding API 引入的变化，您无法通过编辑 Fluentd DaemonSet 将日志转发到一个外部的 Elasticsearch 实例。

在以前的版本中，可以使用 **ES_HOST** 和 **OPS_HOST** 环境变量，或通过 **fluentd** Daemonset 配置 **fluent-plugin-remote-syslog** 插件。

您可以使用新的 [Log Forwarding API](#) 功能，或 [Fluentd forward](#) 协议来把日志转发到一个外部的 Elasticsearch 实例中。相关文档已更新了相关内容。

1.3.1.1. 本地存储置备程序

以前已弃用的技术预览 **ose-local-storage-provisioner** 容器已被删除。建议您使用基于 OLM 的 Local Storage Operator (**ose-local-storage-operator**)。

1.3.1.2. 持久性卷快照

OpenShift Container Platform 4.2 中已弃用了持久性卷快照，并已在 OpenShift Container Platform 4.3 中删除。

1.3.2. 已弃用的功能

1.3.2.1. pipelines 构建策略

pipelines 构建策略现已弃用。使用 OpenShift Pipelines 代替。

1.3.2.2. beta 工作负载警告

随着 Kubernetes 1.16 的推出，**apps/v1beta1**、**apps/v1beta2** 和 **extensions/v1beta1** 工作负载现已弃用。

当使用已弃用的 API 时，会出现 **UsingDeprecatedAPIExtensionsV1Beta1** 警告信息。这些已弃用的 API 将在 OpenShift Container Platform 的下一版本中移除，因此请迁移至支持的 API。

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

Service Catalog、Template Service Broker、Ansible Service Broker 及其关联的 Operator 在 OpenShift Container Platform 4.2 中已弃用，并将在以后的 OpenShift Container Platform 版本中删除。如果在 4.3 中启用了这些功能，Web 控制台现在会警告用户这些功能仍处于启用状态。

以下警报可以在 [Monitoring → Alerts](#) 页面中查看，其严重性级别为 **Warning**：

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

- **AnsibleServiceBrokerEnabled**

以后的发行版本会删除以下相关的 API :

- **.servicecatalog.k8s.io/v1beta1**
- **.automationbroker.io/v1alpha1**
- **.osb.openshift.io/v1**

1.3.2.4. 弃用 OperatorSources 和 CatalogSourceConfig

OperatorSources 和 CatalogSourceConfig 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**

1.3.2.5. 对 CodeReady Containers 的 VirtualBox 支持

现在已弃用了在 CodeReady Containers (paramsReady Containers) 中使用 VirtualBox 的支持。

1.4. 程序错误修复

身份验证

- Authentication Operator 报告使用静态的 "available" 字符串作为不可用条件的原因, 这个信息并不明确。此程序错误修复给出了更明确的不可用条件的原因, 因此更容易找出造成 Operator 不可用的原因。(BZ#1740357)
- **oauth-proxy** 进程为每个请求重新载入 CA 证书, 并存储在内存中。这会造成高内存消耗导致 **oauth-proxy** 容器被终止运行。在这个版本中, CA 证书会被缓存, 除非它们有变化。因此, 在有多个针对它的请求时, **oauth-proxy** 进程的内存消耗会显著下降。(BZ#1759169)
- 在以前的版本中, 在使用 OAuth 服务器的 TLS 握手期间, 为 RequestHeader 身份提供程序 (IdP) 配置的客户端 CA 证书不会在其它证书中声明。当 **login-proxies** 尝试连接到 OAuth 服务器时, 它们将不会使用其客户端证书, 从而导致其请求未经身份验证, 从而导致 IdP 的用户无法登录到集群。此程序错误修复在 TLS 配置的其余部分中添加了配置的客户端 CA, 因此, 使用 RequestHeader IdP 的身份验证可以正常工作。(BZ#1764558)
- OpenShift Container Platform 4.1 中引入的 bootstrap 用户内部使得 CLI 日志流始终可用。如果只配置了 web 控制台流, 当从 CLI 进行登陆时, 有关如何获取验证令牌的信息将不会被显示。这些信息在 OCP 3.x 中会显示。在这个版本中, 当用户禁用 bootstrap 用户身份提供程序 (IdP) 时, 它不会再被配置。因此, 在按照 OCP 文档中的步骤禁用 bootstrap IdP 后, 现在当只配置了 web 时仍会显示有关如何获取身份验证令牌的信息。(BZ#1781083)
- 在以前的版本中, 到 **oauth-server** 的路由不会响应 Ingress 域的更改, 这会影响到 Authentication Operator, 并导致 **oauth-server** 无法正确验证。现在, 当检测到 Ingress 域更改时, **oauth-server** 路由会做出相应的更新, 从而使身份验证可以正常进行。(BZ#1707905)

Builds

- 在一个镜像流被创建后很快启动的构建可能不会利用指定的本地 pullthrough 镜像流标签。构建尝

试从外部镜像 registry 拉取镜像，如果构建没有使用该 registry 所需的授权和证书设置，构建将失败。现在构建控制器已被更新，当检测到其镜像流缓存不包括所需的信息时，允许利用本地的 pullthrough 镜像流标签并通过其他方法检索这些信息。构建过程现在可以成功利用本地镜像流标签 pullthrough。(BZ#1753731)

- 在以前的版本中，构建控制器有时会错误地认为一个构建是由构建配置端点实例化的，而实际上构建是由构建端点实例化的。因此，当用户直接实例化 OpenShift 构建，而不是通过向构建配置 API 端点启动一个构建请求时，构建控制器日志中会出现不存在的构建配置信息，这个日志信息可能会造成混淆。现在构建控制器已被更新，它可以更好地检查构建是否从构建配置端点实例化，从而避免了在日志中记录不必要的错误信息。构建控制器日志已不再出现上面提到的易混淆的错误消息。(BZ#1767218), (BZ#1767219)

Cluster Version Operator

- 在以前的版本中，更新协议 Cincinnati (为利用自动更新而设计) 使用标签 (tag) 来指代实际数据。当在不同点应用同一图形的同一版本时，可能会产生不同的结果。现在，如果容器 registry 提供了 **manifestref**，则会使用镜像 SHA 来指代实际数据。这保证了集群会使用特定的发行版本。(BZ#1686589)

控制台 Kubevirt 插件

- 在以前的版本中，指定的 **volumeMode** 没有被传递给新创建的磁盘，因此 PVC 可能无法正确绑定。现在，**volumeMode** 可以被正确传递给新创建的磁盘。(BZ#1753688)
- 在以前的版本中，当通过 URL 直接访问时，虚拟机详情页面不会被正确加载。现在，该页面可以被正确加载。(BZ#1731480)
- 在以前的版本中，**kubevirt-storage-class-defaults** ConfigMap 设置没有正确地反映 VMware VM 的导入。因此，**blockMode** PVC 不能用于 VMware VM 导入。现在，在请求 VMware 导入磁盘时，存储类默认会被正确使用。(BZ#1762217)
- 在以前的版本中，Import VM 向导的标题不正确，可能会导致混淆。现在，这个向导的标题已被改为 **Import Virtual Machine**。(BZ#1768442)
- 在以前的版本中，VM 迁移向导中的存储和网络配置确认按钮位于错误的地方。现在，这些确认按钮位于正确的位置。(BZ#1778783)
- 在以前的版本中，**创建虚拟机** 向导不会在创建虚拟机前提示确认，这意味着用户可能会意外地创建一个虚拟机。在这个版本中，在创建虚拟机前，用户必须在复查页面中点击 "Create Virtual Machine"。(BZ#1674407)
- 在以前的版本中，**Create Virtual Machine** 向导在导入 VM 时需要输入的字段不太直观。**Create Virtual Machine** 向导现已被重新设计，以按预期工作。(BZ#1710939)
- 在以前的版本中，验证虚拟机名称的出错信息不明确。这些出错信息已被改进以提供更准确的描述。(BZ#1743938)

容器

- 在以前的版本中，当进行一个回复操作时，CRI-O 没有正确过滤 Podman 容器。因为在开始时，Podman 容器没有特定于 CRI-O 的元数据，所以 CRI-O 会将 Podman 容器认为是错误创建的 CRI-O 容器。因此，它会要求存储库删除容器。现在，在 CRI-O 恢复过程中可以正确地过滤 Podman 容器，它们在启动时不再会被从存储中删除。(BZ#1758500)

Etcd

- etcd 会因为大量对象造成超载，从而导致在 etcd 失败时集群停止工作。现在，etcd 客户端均衡器会在客户端连接超时进行端点故障切换。(BZ#1706103)
- etcd 在升级过程中会失败，并导致灾难恢复补救步骤。现在，已更新 etcd 来解决 gRPC 软件包问题，以防止出现灾难性的集群失败。(BZ#1733594)

镜像 Registry

- 在更改了镜像 registry Operator 配置中的存储类型后，旧的和新的存储类型都会出现在 Operator 的状态中。由于此行为，在删除其配置后，镜像 registry Operator 不会被删除。现在只显示新存储类型，因此在更改镜像使用的存储类型后，镜像 registry Operator 会被删除。(BZ#1722878)
- 由于旧镜像流可能具有无效的名称，因此当镜像流标签的 spec 无效时镜像修剪操作会失败。现在，镜像修剪程序总会修剪镜像，即使关联的镜像流具有无效名称。(BZ#1749256)
- 当镜像 registry Operator 的管理状态为 **Removed** 时，它不会报告自己为 Available 状态或正确版本号。由于这个问题，当镜像 registry Operator 被设置为 **Removed** 时，升级会失败。现在，当将镜像 registry Operator 的状态设置为 **Removed** 时，它会报告自己为 Available 状态，并报告正确的版本。即使从集群中移除了镜像 registry，您也可以完成升级。(BZ#1753778)
- 在以前的版本中，可以使用无效的 Azure 容器名称配置镜像 registry Operator，因为名称无效，镜像 registry 将不会部署到 Azure 上。现在，镜像 registry Operator 的 API 模式可确保您输入的 Azure 容器名称符合 Azure API 的要求且有效，从而确保 Operator 可以部署。(BZ#1750675)

kube-apiserver

- 在以前的版本中，会为以下每个控制器创建一个不需要的服务监控对象: kube-apiserver、kube-controller-manager 和 kube-scheduler。现在，不需要的服务监控对象不再会被创建。(BZ#1735509)
- 在以前的版本中，当因为启用了技术预览功能或自定义功能而使集群处于不可升级状态时，不会发送警报。现在，如果在处于不可升级状态的集群中尝试升级时，集群会通过 Prometheus 发送一个 **TechPreviewNoUpgrade** 警报。(BZ#1731228)

kube-controller-manager

- 在以前的版本中，在定义 StatefulSet 资源对象时，通过 **volumeClaimTemplates** 参数指定的模板创建 PersistentVolumeClaim 资源对象时，不会应用自定义标签。现在，自定义标签可以正确地应用到通过 StatefulSet 资源定义的 **volumeClaimTemplates** 对象创建的 PersistentVolumeClaim 对象。(BZ#1753467)
- 在以前的版本中，如果删除了 Kubernetes Controller Manager (KCM) 的租期 ConfigMap，KCM 便没有权限重新创建 ConfigMap，且无法这样做。现在，如果已删除，KCM 可以重新创建租期 ConfigMap。(BZ#1780843)

日志记录

- 在以前的版本中，集群版本和 ClusterLogging 版本之间的不匹配会导致 ClusterLogging 无法部署。现在，kubeverion 会被确认支持部署的 ClusterLogging 版本。(BZ#1765261)
- 在以前的版本中，日志中关于工具值的数据没有被隔离，其值不正确，从而导致 fluentd 在错误的级别上释放错误信息。现在，在 debug 级别上 luentd 的日志被正确记录。(BZ#1753936,BZ#1766187)
- 在以前的版本中，oauth-proxy 被错误配置，用户无法在登出后再登录。现在，重新配置了 oauth-proxy，用户可以在登出后再重新登录。(BZ#1725517)

- 在以前的版本中，Eventrouter 无法处理未知事件类型，这会导致 Eventrouter 崩溃。现在，Eventrouter 可以正确处理未知事件类型。(BZ#1753568)

管理控制台

- 在以前的版本中，Management Console 面板详情页不必要地监视基础架构资源。因此，可能会出现有关早期 web 套接字连接终止的错误。现在，详情页不会监视基础架构资源，仅获取资源数据一次。在应用此程序修复后不会再报告错误。(BZ#1765083)
- 在以前的版本中，在路由器有机会提供主机名前，控制台 Operator 将控制台 URL 记录为初始的空字符串值。现在，Operator 会进行等待直到主机名被填充，从而不会出现空字符串的问题。(BZ#1768684)

Metering Operator

- 在以前的版本中，**metering-operator** CSV 中的 **containerImage** 项引用了一个镜像标签，该标签没有列在 ART 用于替换目的的 **image-references** 文件中。这意味着 ART 无法将 **containerImage** 字段中列出的原始镜像正确替换为关联的 **image-registry** 存储仓库和 **sha256** 标签。在这个版本中，镜像标签 **latest** 被 **image-references** 文件中定义的 **release-4.3** 替换。因此，ART 现在可以成功替换 **metering-operator** 容器镜像。(BZ#1782237)
- 在以前的版本中，Hadoop **Dockerfile.rhel** 将 **gcs-connector** JAR 文件复制到容器的错误位置。现在，路径已被修正，指向正确的位置。(BZ#1767629)

网络

- 在以前的版本中，在修改 CNO 时不会删除所有相关对象，这会留下过时的网络附加定义。在 OpenShift Container Platform 4.3 中，已重构了代码，以更通用的方式进行此操作，以便正确清理相关的对象。(BZ#1755586)
- 在以前的版本中，一些更新被丢弃，造成事件丢失。现在，不再会丢弃事件。(BZ#1747532)
- 在以前的版本中，当具有带有数据包丢失的大量网络数据的集群中，已成功连接到服务的连接可能会出现 **Connection reset by peer** 错误。因此，客户端需要重新连接并重新传输数据。现在，已更新了 iptables 规则以便正确处理 TCP 重新传输。已建立的连接将会保持打开，直到关闭为止。(BZ#1762298)
- 在以前的版本中，NetworkPolicy 在具有多个命名空间、命名空间更改以及选择命名空间的 NetworkPolicies 的集群中，对新命名空间的应用可能会慢慢。新的命名空间可能需要等待大量时间才可以被其他命名空间访问。现在，Namespace 和 NetworkPolicy 的代码已更新，NetworkPolicies 会马上应用到新的命名空间。(BZ#1752636)
- 在以前的版本中，SDN Pod 在重启节点时不会清理 Egress IP 地址，从而导致 IP 地址冲突。现在，SDN pod 会在启动时清除过时的 Egress IP 地址，以防止发生冲突。(链接: BZ#1753216)
- 在以前的版本中，每次在 EgressNetworkPolicy 中查询 DNS 名称时都会查询 DNS 名称。无论前面的查询是否刷新了特定的 DNS 记录，都会查询记录，从而降低网络性能。现在，DNS 记录根据唯一的名称而不是每个 EgressNetworkPolicy 进行查询。因此，DNS 查询性能显著提高。(BZ#1684079)
- 在以前的版本中，控制台无法在多个服务端点间创建路由。现在，GUI 已被更新，可以添加或删除三个替代服务端点。(BZ#1725006)

节点

- 在以前的版本中，当容器具有高（或 >1）的重启数时，kubelet 会将重复的容器指标数据注入 metrics 流，从而导致 kubelet 上的 **/metrics** 端点抛出一个 500 错误。在这个版本中，仅包含大

多数当前容器（运行或停止）的指标。因此，`/metrics` 端点现在允许指标流到 Prometheus，而不会造成 500 错误。(BZ#1779285)

- 对长路径名测试进行了上游更改。以前，名称大于 255 个字符的 Pod 没有被记录，且不会发出警告。现在，名称长度超过 255 个字符的 Pod 会如预期在日志中被记录。(BZ#1711544)
- 在以前的版本中，`LocalStorageCapacityIsolation` 功能被禁用，用户无法使用 `Statefulset.emptyDir.sizeLimit` 参数。现在，`LocalStorageCapacityIsolation` 功能已被启用，并且可以设置 `Statefulset.emptyDir.sizeLimit` 参数。(BZ#1758434)

oc

- 在以前的版本中，使用服务器端打印时，在监视时会忽略 wide 输出选项（`oc get clusteroperators -o wide`）。现在，在使用服务器端打印时，可以正确地识别所有可能的选项。(BZ#1685189)
- `oc explain` 命令到上游文档的链接过期。这些链接已经更新，现在有效。(BZ#1727781)
- 完整用法菜单信息会和错误标志错误信息一起输出，导致错误信息被忽略。现在，当运行 `oc command --help` 时，标志错误是唯一显示的信息。(BZ#1748777)
- 因为缺少状态代码信息，`oc status` 命令没有以一致的格式显示 DaemonSet。现在，在 `oc status` 命令的输出中会正确输出 Daemonset、Deployment 和 Deployment Configuration。(BZ#1540560)
- 因为设置了不正确的标记，`oc version` 和 `openshift-install version` 会显示为 Dirty。这些标志已经更新，命令将不再显示 Dirty GitTreeState 或 GitVersion。(BZ#1715001)
- `oc status` 命令建议 `oc set probe pod` 验证 pod 仍在运行，包括控制器可能拥有的 pod。现在，探测建议会忽略控制器拥有的 pod。(BZ#1712697)
- 在以前的版本中，`oc new-build help` 命令没有正确过滤标志。这会导致在调用 `oc new-build --help` 时打印不相关的标志。这已被解决，现在 help 命令只输出相关的信息。(BZ#1737392)

openshift-apiserver

- 4.2 和 4.3 中的 `ClusterResourceQuota` 不允许使用非字符串作为限制值，因为 OpenAPI 模式错误。因此，虽然之前在 4.1 中可能这样做，但无法在 `ClusterResourceQuota` 对象中设置整数配额值。`ClusterResourceQuota` 的 OpenAPI 模式已被修复，它允许整数，从而可以在 `ClusterResourceQuota` 中再次使用整数作为配额值。(BZ#1756417)
- 在升级过程中，`openshift-apiserver` 会报告 `degraded`。造成降级的原因为 `MultipleAvailable`，但这对于用户无法理解。现在，这个程序错误修复会列出造成降级的原因，因此不会向用户隐藏任何信息。(BZ#1767156)

Web 控制台

- 如果安装了 knative serverless TP1 Operator 且以非 admin 用户身份登录，控制台工作负载会显示一个限制的访问错误。在这个版本中，对于普通的部署或特定于 knative 的部署，Overview 侧边栏资源都可以正常工作。非管理员用户现在可以查看工作负载。(BZ#1758628)
- 拓扑视图数据模型最初是项目 Workloads 页的一个子集。当 Workloads 页增加了新的功能时，虽然拓扑视图会以相似的形式进行改变，但它们并没有共享相同的代码。随着用例变得复杂，新的代码可能会忽略掉一些边缘用例。在某些情况下，拓扑视图中的 Pod 列表不正确。在这个版本中，拓扑视图和项目 Workloads 页共享了相同的代码逻辑。因此，现在无论从拓扑视图还是项目 Workloads 页中查看 Pod 列表，Pod 详情信息都是相同的。(BZ#1760827)

- 在以前的版本中，当创建 Route 对象时，会设置可用端口列表中的第一个端口，而不是设置在目标端口下拉菜单中选则的端口。因此，用户无法选择所需的目标端口。现在，在创建 Route 对象时，目标端口下拉菜单中选择的端口会被设置。如果没有选择端口，则设置列表里的第一个端口。(BZ#1760836)
- 在以前的版本中，对于 Edge 浏览器中，Topology 视图中无法呈现某些特征，如应用程序名称和构建状态。在这个版本中，Edge 浏览器会正常显示应用程序名称和构建状态。(BZ#1760858)
- 以前，当安装了 Knative Operator 时，一个非 admin 用户无法在 web 控制台的 Overview 页中查看工作负载，即使选择了非 Knative 工作负载的部署。在这个版本中增加了一个是否有相关配置的检查，如果没有相关的配置，系统就不会在 Overview 页中添加特定于 Knative 的资源。这可以让非 admin 用户按预期查看工作负载。(BZ#1760810)
- 在以前的版本中，当 Topology 上下文菜单打开时，相关的节点不容易被识别。这会给用户造成混乱，因为用户不知道上下文菜单指向的节点。现在，当右键单击节点以打开上下文菜单时，一个明显的鼠标光标或影子会出现在节点上以便更容易地识别。(BZ#1776401)
- 在以前的版本中，web 控制台中的 Import from Git 表单使用的用来验证 Git URL 的正则表达式太严格，从而使一些有效的 URL 无法通过验证。现在，正则表达式已被更新，可以接受所有有效的 Git URL。(BZ#1766350), (BZ#1771851)
- 开发人员控制台的错误消息被重复。这个系统已经更新，以正确反映客户端里的值。现在，错误消息非常简洁清晰。(BZ#1688613)
- 在以前的版本中，当访问 OLM 操作数资源的 Resources 标签卡时，web 控制台可能会出现运行时错误。当尝试为 OLM 操作资源排序 Resources 选项卡时，web 控制台也可能停滞。现在这个问题已解决。(BZ#1756319)
- 在以前的版本中，当使用 Microsoft Edge 访问 OpenShift web 控制台的 pod 详情页面时，可能会导致运行时错误，从而无法显示该页面。这个问题现已解决，pod 详情页面现在可以正确显示。(BZ#1768654)
- 在以前的版本中，如果一个 dashboard card 监视了 Prometheus 结果，则 dashboard 页面的性能会因为旧警报和新警报的比较不正确而降低。现在，这个问题已解决。(BZ#1781053)
- 在以前的版本中，Network Policy 页面中的文档链接不正确。现在，这些文档链接已被修正。(BZ#1692227)
- 在以前的版本中，Prometheus 查询包含一个范围选择器，它会阻止 Prometheus UI 的默认页面上的图表正确显示。现在，查询已不再包含范围选择器，因此查询现在可以正确运行。(BZ#1746979)
- **Recycle** 是持久性卷重新声明策略的默认值，即使该选项已弃用。默认情况下，持久性卷包含了已弃用的值。现在，默认的 Persistent Volume Reclaim 策略已被改为 **Retain**，因此新的持久性卷不包含已弃用的值。(BZ#1751647)
- 在以前的版本中，在升级集群后，web 控制台可以使用缓存的 CSS 风格表，这可能会导致加载控制台时出现一些问题。这个问题已被解决，网页控制台现在在升级后使用了正确的风格表。(BZ#1772687)
- 在以前的版本中，当在一些情况下在选项菜单中使用 web 控制台时，页面里的其他元素被隐藏。现在，选项菜单不再出现在其他页面元素后面，并可根据需要页中正确地展开，以确保整个菜单始终可见。(BZ#1723254)
- 以前，长节点名称可能会使 OpenShift 控制台 Pod 表中的表字段溢出。在这个版本中，它们可以被正确地换行。(BZ#1713193)

- 在以前的版本中，使用 YAML 示例创建报告查询会导致错误。现在，为报告查询添加了一个新的 YAML 示例，该查询包含所有必填字段，因此不会发生错误。(BZ#1753124)
- 在之前的 Install Plan Details 页面中，相关目录源的命名空间被错误地设置。这会导致链接无法正常工作，因为命名空间不存在。此程序错误修复使用 InstallPlan 资源的 **status.plan** 字段将目录源与正确的命名空间关联。因此，目录源链接可以正常工作。(BZ#1767072)
- 在以前的版本中，未知的自定义资源会被自动分成单词来估计用户应该看到的内容。然而，有些资源被不正确地分割。在这个版本中，自定义资源使用自定义资源定义中定义的名称，而不是将其分隔为不同的单词。(BZ#1722811)

1.5. 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，标记为 **TP** 的功能代表 *技术预览*，标记为 **GA** 的功能代表 *正式发布 (General Availability)*。使用 - 标记的功能代表该功能已从发行版本中删除或已弃用。

表 1.1. 技术预览

功能	OCP 4.1	OCP 4.2	OCP 4.3
Prometheus Cluster Monitoring	GA	GA	GA
精度时间协议 (PTP)	-	-	TP
CRI-O for runtime pods	GA	GA	GA
oc CLI Plug-ins	TP	TP	TP
Service Catalog	GA	-	-
Template Service Broker	GA	-	-
OpenShift Ansible Service Broker	GA	-	-
Network Policy	GA	GA	GA
Multus	GA	GA	GA
New Add Project Flow	GA	GA	GA
Search Catalog	GA	GA	GA
Cron Jobs	GA	GA	GA

功能	OCP 4.1	OCP 4.2	OCP 4.3
Kubernetes Deployments	GA	GA	GA
StatefulSets	GA	GA	GA
Explicit Quota	GA	GA	GA
Mount Options	GA	GA	GA
System Containers for Docker, CRI-O	-	-	-
Hawkular Agent	-	-	-
Pod PreSets	-	-	-
experimental-qos-reserved	TP	TP	TP
Pod sysctls	GA	GA	GA
中央审计	-	-	-
外部项目网络通讯的静态 IP	GA	GA	GA
模板完整性检测	GA	GA	GA
replicaSet	GA	GA	GA
集群的 MongoDB 模板	-	-	-
集群的 MySQL 模板	-	-	-
Kubernetes 资源的镜像流 (image stream)	GA	GA	GA
设备管理器	GA	GA	GA
重新调整持久性卷的大小	GA	GA	GA
大内存页	GA	GA	GA
CPU 固定 (CPU pinning)	GA	GA	GA

功能	OCP 4.1	OCP 4.2	OCP 4.3
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
CephFS Provisioner	-	-	-
Podman	TP	TP	TP
Kuryr CNI 插件	-	TP	GA
PID 命名空间的共享控制	TP	TP	TP
Manila Provisioner	-	-	-
Cluster Administrator 控制台	GA	GA	GA
Cluster Autoscaling	GA	GA	GA
Container Storage Interface (CSI)	TP	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 network provider	TP	TP	TP

功能	OCP 4.1	OCP 4.2	OCP 4.3
基于 Prometheus 的 HPA 定制 metrics adapter	TP	TP	TP
机器健康状态检查	TP	TP	GA
使用 iSCSI 的持久性存储	TP	TP	GA
使用 iSCSI 原始块	-	TP	GA
使用 Cinder 的原始块			TP
OperatorHub		GA	GA
三节点裸机部署		TP	TP
Cluster Network Operator		TP	GA
Helm CLI			TP
服务绑定			TP
日志转发			TP
用户工作负载监控			TP
OpenShift Serverless	TP	TP	TP
Compute Node Topology Manager			TP
Metering	TP	GA	GA
成本管理	TP	TP	GA

1.6. 已知问题

- 如果您安装了 Service Mesh，请在升级 OpenShift Container Platform 前升级 Service Mesh。如需临时解决方案，请参阅 [Updating OpenShift Service Mesh from 1.0.1 to 1.0.2](#)。
- 在部署失败时，Topology 视图中认定的活动 Pod 可能会不正确。(BZ#1760828)
- 当具有有限集群范围权限的用户使用 Add 页面中的 Container Image 选项创建应用程序，并选择 Image name from internal registry 选项时，即使镜像流存在，在项目中也无法检测到镜像流。(BZ#1784264)

- 发布时 registry 不支持 **ImageContentSourcePolicy** ([BZ#1787112](#))。在断开网络连接的环境中，可以默认启用 Jenkins 来拉取。在断开网络连接的环境中，使用以下命令来使用 Jenkins 作为一个临时解决方案：

```
$ oc tag <jenkins_source_image> jenkins:2 --reference-policy=source -n openshift
```

- OpenShift Cluster Version Operator (CVO) 无法正确挂载来自主机的 SSL 证书，这会阻止在使用 MITM 代理检查时进行集群版本更新。([BZ#1773419](#))
- 在 [builds.config.openshift.io](#) 中添加 **defaultProxy** 和 **gitProxy** 时，Jenkins 的 pipeline 构建无法获得代理配置。([BZ#1753562](#))
- 当在 Red Hat OpenStack Platform 13 或 16 上安装时，使用自签名 TLS 证书配置 OpenStack 端点会导致安装失败。([BZ#1786314](#),[BZ#1769879](#),[BZ#1735192](#))
- 当 OpenStack Neutron 负载非常重时，OpenStack 上的安装程序部署的基础架构会失败，错误为 **Security group rule already exists**。([BZ#1788062](#))
- 在 **etcd** 加密迁移过程中，集群会在 **etcd** 备份或恢复功能后显示错误和异常状态。([BZ#1776811](#))
- 当从 4.2.12 升级到 4.3.0 时，RHCOS master 和 worker 节点可能会进入 **NotReady, SchedulingDisabled** 状态。([BZ#1786993](#))
- 如果启用了 FIPS 模式，则无法直接使用 RHEL 的公共云访问镜像。这是因为公共云镜像不允许内核完整性检查。为了解决这个问题，需要上传自己的镜像。([BZ#1788051](#))
- 当启用 Kuryr SDN 时，Operator Lifecycle Manager (OLM) 在 OpenShift Container Platform 中无法工作。([BZ#1786217](#))
- 对于受限制的集群，**oc adm catalog build** 和 **oc adm catalog mirror** 命令无法正常工作。([BZ#1773821](#))
- 当将 OpenShift Container Platform 集群从 4.1 升级到 4.2 时，使用 Node Tuning Operator 调整的 Pod 可能会处于 **ContainerCreating** 状态。
要确认这个问题，请运行：

```
$ oc get pods -n openshift-cluster-node-tuning-operator
```

一个或多个调整的 Pod 处于 **ContainerCreating** 状态。

要解决这个问题，请应用以下临时解决方案。运行：

```
$ oc delete daemonset/tuned -n openshift-cluster-node-tuning-operator
$ oc get daemonset/tuned -n openshift-cluster-node-tuning-operator
$ oc get pods -n openshift-cluster-node-tuning-operator
```

验证 Pod 是否现在处于 **Running** 状态。([BZ#1791916](#))

- Node Feature Discovery (NFD) Operator 版本 4.3 无法从 OperatorHub 部署到 OpenShift Container Platform Web 控制台。作为临时解决方案，为您的操作系统下载 **oc** 客户端，并将 **kubeconfig** 文件放在 `~/.kube/config` 中。运行这些命令从 CLI 和 GitHub 部署 NFD Operator：

```
$ cd $GOPATH/src/openshift
$ git clone https://github.com/openshift/cluster-nfd-operator.git
$ cd cluster-nfd-operator
```

```
$ git checkout release-4.3
$ PULLPOLICY=Always make deploy
$ oc get pods -n openshift-nfd
```

输出示例：

```
$ oc get pods -n openshift-nfd
NAME READY STATUS RESTARTS AGE
nfd-master-gj4bh 1/1 Running 0 9m46s
nfd-master-hngrm 1/1 Running 0 9m46s
nfd-master-shwg5 1/1 Running 0 9m46s
nfd-operator-b74cbdc66-jsgqq 1/1 Running 0 10m
nfd-worker-87wpm 1/1 Running 2 9m47s
nfd-worker-d7kj8 1/1 Running 1 9m47s
nfd-worker-n4g7g 1/1 Running 1 9m47s
```

([BZ#1793535](#))

- 如果配置了集群范围的出口（egress）代理且之后又取消了设置，则之前由 OLM 管理的 Operator 部署的应用程序的 Pod 可能会进入 **CrashLoopBackOff** 状态。这是因为所部署的 Operator 仍会被配置为依赖于代理。



注意

这个问题会出现在集群范围出口代理创建的环境变量、卷和 VolumeMount 中。在使用 SubscriptionsConfig 对象设置环境变量、卷和 VolumeMounts 时也会出现这个问题。

这个问题计划在 OpenShift Container Platform 以后的发行版本被修复，现在，您可以通过使用 CLI 或 Web 控制台删除 Deployment 来解决这个问题。这会触发 OLM 来重新生成部署并使用正确的网络配置启动 Pod。

集群管理员可以通过运行以下命令，获取所有受影响的 OLM 管理的 Deployment 的列表：

```
$ oc get deployments --all-namespaces \
  -l olm.owner,olm.owner!=packageserver 1
```

- 1** **packageserver** 除外，它不受影响。

([BZ#1751903](#))

- 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 ConfigMap 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](#))

- 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)
- 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 4.3 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)

1.7. 异步勘误更新

OpenShift Container Platform 4.3 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 4.3 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 4.3 相关的异步勘误信息。异步子版本（例如，OpenShift Container Platform 4.3.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 [updating your cluster](#) 中的内容。

1.7.1. RHBA-2020:0062 - OpenShift Container Platform 4.3 镜像和程序错误公告

发布日期：2020 年 1 月 23 日

OpenShift Container Platform release 4.3 现已正式发布。容器镜像列表和程序错误修正信息包括在 [RHBA-2020:0062](#) 公告中。此更新中包括的 RPM 软件包由 [RHBA-2019:0063](#) 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 4.3.0 容器镜像列表](#)

1.7.2. RHBA-2020:0390 - OpenShift Container Platform 4.3.1 Bug Fix Update

发布日期：2020 年 2 月 12 日

OpenShift Container Platform release 4.3.1 现已正式发布。其软件包列表包括在 [RHBA-2020:0390](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:0391](#) 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 4.3.1 容器镜像列表](#)

1.7.2.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。

1.7.3. RHBA-2020:0491 - OpenShift Container Platform 4.3.2 Bug Fix Update

发布日期：2020 年 2 月 19 日

OpenShift Container Platform release 4.3.2 现已正式发布。其软件包列表包括在 [RHBA-2020:0491](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:0492](#) 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 4.3.2 容器镜像列表

1.7.3.1. 程序错误修复

- Amazon Web Services (AWS) 安装程序置备的基础架构和 Red Hat OpenStack Platform (RHOSP) 用户置备的基础架构缺少安全组规则来允许在 control plane 主机和 worker 系统之间的 TCP 和 UDP 端口 30000-32767 的双向流量。这会导致新引入的 OVN Networking 组件无法在缺少这些安全组规则的集群中正常工作。现在，安全组规则可以允许上述的双向流量支持。[\(BZ#1779469\)](#)
- 在以前的版本中，当用户试图访问 web 控制台中的 **Installed Operators** 界面时，会出现一个 *Restricted Access* 错误。这是因为控制台试图访问当前命名空间以外的订阅资源来显示订阅详情。现在，用户可以访问 **Installed Operators** 页面。如果用户没有访问订阅资源的权限，订阅标签页会被隐藏。[\(BZ#1791101\)](#)

1.7.3.2. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。

1.7.4. RHBA-2020:0491 - OpenShift Container Platform 4.3.3 程序错误修正更新

发布日期：2020 年 2 月 24 日

OpenShift Container Platform release 4.3.3 现已正式发布。其软件包列表包括在 [RHBA-2020:0527](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:0528](#) 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 4.3.3 容器镜像列表

1.7.4.1. 程序错误修复

- KnativeServing 资源 **servicing.knative.dev** 的 API 组已被弃用，它在 Serverless Operator 1.4 中被改为 **operator.knative.dev**。[\(BZ#1779469\)](#)

1.7.4.2. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。

1.7.5. RHSA-2020:0562 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 2 月 24 日

OpenShift Container Platform 4.3 现在提供了 **jenkins-slave-base-rhel7-container** 的更新。有关更新的详情请查看 [RHSA-2020:0562](#) 公告。

1.7.6. RHBA-2020:0675 - OpenShift Container Platform 4.3.5 程序错误修正更新

发布日期：2020 年 3 月 10 日

OpenShift Container Platform release 4.3.5 现已正式发布。其软件包列表包括在 [RHBA-2020:0675](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:0676](#) 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 4.3.5 容器镜像列表](#)

1.7.6.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.7. RHSA-2020:0679 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 3 月 10 日

OpenShift Container Platform 4.3 现在提供了对 **skopeo** 的更新。有关更新的详情请查看 [RHSA-2020:0679](#) 公告。

1.7.8. RHSA-2020:0680 - Low: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 3 月 10 日

OpenShift Container Platform 4.3 现在提供了对 **podman** 的更新。有关更新的详情请查看 [RHSA-2020:0680](#) 公告。

1.7.9. RHSA-2020:0681 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 3 月 10 日

现在，OpenShift Container Platform 4.3 提供了 **openshift-enterprise-apb-base-container**、**openshift-enterprise-mariadb-apb**、**openshift-enterprise-mysql-apb** 和 **openshift-enterprise-postgresql-apb** 的更新。有关更新的详情请查看 [RHSA-2020:0681](#) 公告。

1.7.10. RHSA-2020:0683 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 3 月 10 日

OpenShift Container Platform 4.3 现在提供了 **openshift-enterprise-ansible-operator-container** 的更新。有关更新的详情请查看 [RHSA-2020:0683](#) 公告。

1.7.11. RHBA-2020:0857 - OpenShift Container Platform 4.3.8 程序错误修正更新

发布日期：2020 年 3 月 24 日

OpenShift Container Platform release 4.3.8 现已正式发布。其软件包列表包括在 [RHBA-2020:0857](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:0858](#) 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 4.3.8 容器镜像列表](#)

1.7.11.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.12. RHSA-2020:0863 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 3 月 24 日

OpenShift Container Platform 4.3 现在提供了 **openshift-enterprise-builder-container** 和 **openshift-enterprise-cli-container** 的更新。有关更新的详情请查看 [RHSA-2020:0863](#) 公告。

1.7.13. RHSA-2020:0866 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 3 月 24 日

OpenShift Container Platform 4.3 现在提供了 **openshift-enterprise-template-service-broker-operator-container** 的更新。有关更新的详情请查看 [RHSA-2020:0866](#) 公告。

1.7.14. RHSA-2020:0928 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 3 月 24 日

OpenShift Container Platform 4.3 现在提供了 **openshift-clients** 的更新。有关更新的详情请查看 [RHSA-2020:0928](#) 公告。

1.7.15. RHBA-2020:0929 - OpenShift Container Platform 4.3.9 程序错误修正更新

发布日期：2020 年 4 月 1 日

OpenShift Container Platform release 4.3.9 现已正式发布。其软件包列表包括在 [RHBA-2020:0929](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:0930](#) 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 4.3.9 容器镜像列表](#)

1.7.15.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.16. RHSA-2020:0933 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 4 月 1 日

OpenShift Container Platform 4.3 现在提供了 **ose-openshift-apiserver-container** 的更新。有关更新的详情请查看 [RHSA-2020:0933](#) 公告。

1.7.17. RHSA-2020:0934 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 4 月 1 日

OpenShift Container Platform 4.3 现在提供了 **ose-openshift-controller-manager-container** 的更新。有关更新的详情请查看 [RHSA-2020:0934](#) 公告。

1.7.18. RHBA-2020:1262 - OpenShift Container Platform 4.3.10 程序错误修正更新

发布日期：2020 年 4 月 8 日

OpenShift Container Platform release 4.3.10 现已正式发布。其软件包列表包括在 [RHBA-2020:1255](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:1262](#) 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 4.3.10 容器镜像列表

1.7.18.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.19. RHSA-2020:1276 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 4 月 8 日

OpenShift Container Platform 4.3 现在提供了 **openshift** 的更新。有关更新的详情请查看 [RHSA-2020:1276](#) 公告。

1.7.20. RHSA-2020:1277 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 4 月 8 日

OpenShift Container Platform 4.3 现在提供了 **openshift-enterprise-builder-container** 的更新。有关更新的详情请查看 [RHSA-2020:1277](#) 公告。

1.7.21. RHBA-2020:1393 - OpenShift Container Platform 4.3.12 程序错误修正更新

发布日期：2020 年 4 月 14 日

OpenShift Container Platform release 4.3.12 现已正式发布。其软件包列表包括在 [RHBA-2020:1392](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:1393](#) 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 4.3.12 容器镜像列表

1.7.21.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.22. RHSA-2020:1396 - Low: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 4 月 14 日

OpenShift Container Platform 4.3 现在提供了对 **podman** 的更新。有关更新的详情请查看 [RHSA-2020:1396](#) 公告。

1.7.23. RHBA-2020:1482 - OpenShift Container Platform 4.3.13 程序错误修正更新

发布日期：2020 年 4 月 20 日

OpenShift Container Platform release 4.3.13 现已正式发布。其软件包列表包括在 [RHBA-2020:1481](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:1482](#) 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 4.3.13 容器镜像列表](#)

1.7.23.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.24. RHSA-2020:1485 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 4 月 20 日

OpenShift Container Platform 4.3 现在提供了对 **runc** 的更新。有关更新的详情请查看 [RHSA-2020:1485](#) 公告。

1.7.25. RHBA-2020:1529 - OpenShift Container Platform 4.3.18 程序错误修正更新

发布日期：2020 年 4 月 29 日

OpenShift Container Platform release 4.3.18 现已正式发布。其软件包列表包括在 [RHBA-2020:1528](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:1529](#) 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 4.3.18 容器镜像列表](#)

1.7.25.1. 功能

1.7.25.1.1. IBM Power 系统

在这个版本中，IBM Power Systems 与 OpenShift Container Platform 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 Container Platform 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 Container Platform Pipelines
 - OpenShift Container Platform Metering
 - Multus CNI 插件
- Worker 节点必须运行 Red Hat Enterprise Linux CoreOS。
- 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。

1.7.25.1.2. IBM Z 和 LinuxONE

在这个版本中，IBM Z 和 LinuxONE 与 OpenShift Container Platform 4.3 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)
 - OpenShift Container Platform Serverless
 - 日志转发
 - Helm 命令行界面 (CLI) 工具
 - 精度时间协议 (PTP) 硬件
- 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 Container Platform Pipelines
 - 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。
- Worker 节点必须运行 Red Hat Enterprise Linux CoreOS。
- 持久性共享存储必须是 Filesystem: NFS 类型。
- 其他第三方存储供应商可能会提供启用了 Container Storage Interface (CSI) 的解决方案，这些解决方案经过认证可与 OpenShift Container Platform 一起工作。如需更多信息，请参阅 OpenShift Container Platform 上的 OperatorHub，或联系您的存储厂商。
- 为 OpenShift Container Platform 安装设置 z/VM 实例时，您可能需要暂时为 worker 节点授予更多虚拟 CPU 容量或添加第三个 worker 节点。(BZ#1822770)
- 以下功能适用于 IBM Z 上的 OpenShift Container Platform 4.3，但不适用于 x86 上的 OpenShift Container Platform 4.3:
 - 在 IBM System Z 上为附加了 ficon 的 ECKD 存储的虚拟机启用了 HyperPAV。

1.7.25.2. 程序错误修复

- 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。Web 控制台现在容许无效的描述符并显示操作对象详情。(BZ#1798130)

- 在以前的版本中，没有创建项目权限的用户可以在 Web 控制台中看到 **Create Project** 操作选项。因此没有正确权限的用户可能会尝试创建项目，并且出现错误信息（称无法创建项目）。现在，没有创建项目权限的用户将无法看到 **Create Project** 操作选项。(BZ#1804708)
- Service Catalog Operator 没有正确设置 **Upgradeable**。这会在全新 OpenShift Container Platform 集群安装后显示 **Unknown** 的错误升级状态。现在，**Upgradeable** 项可以被正确配置，集群的升级状态将会正确显示。(BZ#1813488)
- 如果 Operator 被设置为 **Unmanaged**，则 Image Registry Operator 不会报告 OpenShift Container Platform 的新版本。这会导致升级到较新集群版本的过程失败。现在，当 Image Registry Operator 被设置为 **Unmanaged** 时，会报告新的集群版本，从而可以成功升级。(BZ#1816656)
- 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#1818980)
- 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#1819850)
- 在以前的版本中，node-ca 守护进程不容许 **NoExecute** 污点。这会导致 node-ca 守护进程忽略应用 **NoExecute** 污点的节点中的证书。此程序错误修复将 **additionalTrustedCA** 同步到具有污点的所有节点，允许容许所有污点。(BZ#1820242)
- 用于刷新 CA 证书的 **oc** 命令缺少了要操作的资源类型。这会导致命令返回错误。现在，以前缺失的 ConfigMap 已被添加，从而解决了这个问题。(BZ#1824921)

1.7.25.3. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.25.4. 已知问题

- 由于 **coreos-installer** 存在问题，所以无法在使用带有 4K 扇区的 NVMe 驱动器的裸机节点上安装 CoreOS。(BZ#1805249)
- IBM Power 系统的 **fw_enabled_large_send** 设置存在问题，导致 VXLAN 数据包丢失，并可能导致部署失败。(BZ#1816254)

- 对于 IBM Power 基础架构上的集群，因为缺少了与热插拔设备相关的软件包，虚拟机可能无法检测动态置备的持久性卷。因此，您需要安装以下软件包和服务：**librtas**、**powerpc-utils** 和 **ppc64-diag**。(BZ#1811537)

1.7.26. RHBA-2020:2006 - OpenShift Container Platform 4.3.19 程序错误修复更新

发布日期：2020 年 5 月 11 日

OpenShift Container Platform release 4.3.19 现已正式发布。其软件包列表包括在 [RHBA-2020:2005](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:2006](#) 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 4.3.19 容器镜像列表

1.7.26.1. 程序错误修复

- 以前，如果镜像流由内部镜像 registry 具有凭证的私有 registry 支持，但消费者没有凭证，则后续镜像拉取 (pull) 将失败。如果在集群启动或 OpenShift 控制器管理器重启后不久发生镜像流访问，则镜像流的本地引用设置会被忽略，因此控制器管理器会将镜像流存储到缓存中的元数据不完整。OpenShift 控制器管理器已被更新，在其元数据初始化不完整时刷新其镜像流缓存。这会保留本地引用镜像流策略，即使在集群启动或 OpenShift 控制器管理器重启后马上发生的时间窗口中。(BZ#1813420)
- 在以前的版本中，OpenShift 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#1821647)
- 一个 Multus 相关的 DaemonSet 错误地使用了已弃用的版本 **extensions/v1beta1**，而不是在 YAML 定义中的 **apps/v1**。这会为启用了已弃用 API 用量警报的集群发送警报。DaemonSet 已更新为使用正确的版本名称，因此不再发送已弃用的 API 用量警报。(BZ#1824866)
- 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 Dockerfile 没有包括它们。这会导致构建失败，并出现语法错误。在这个版本中，在生成修改的 Dockerfile 时使用了原始文件中的 **ENV** 和 **LABEL** 指令。(BZ#1821861)
- 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#1825007)
- 在以前的版本中，OpenStack 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程分配的时间。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#1825973)
- 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#1826167)

1.7.26.2. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.27. RHSA-2020:2009 - Important: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 5 月 11 日

OpenShift Container Platform 4.3 现在提供了 **ose-cluster-image-registry-operator-container** 的更新。有关更新的详情请查看 [RHSA-2020:2009](#) 公告。

1.7.28. RHBA-2020:2129 - OpenShift Container Platform 4.3.21 程序错误修复更新

发布日期：2020 年 5 月 19 日

OpenShift Container Platform release 4.3.21 现已正式发布。其软件包列表包括在 [RHBA-2020:2128](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:2129](#) 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 4.3.21 容器镜像列表](#)

1.7.28.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.29. RHBA-2020:2184 - OpenShift Container Platform 4.3.22 程序错误修复更新

发布日期：2020 年 5 月 26 日

OpenShift Container Platform release 4.3.22 现已正式发布。其软件包列表包括在 [RHBA-2020:2183](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:2184](#) 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 4.3.22 容器镜像列表

1.7.29.1. 程序错误修复

- 在以前的版本中，在 s390x 和 ppc64le 构架中的安装无法成功完成，因为 Samples Operator 在那些架构上运行时无法报告其版本。这个问题已被解决，这些安装现在可以成功完成。
([BZ#1779934](#))
- 在这个版本中，一些涉及 TLS 证书和 ETCDCCTL API 版本的环境变量被写入 `/root/.profile`。因此，当用户执行 `oc rsh` 时，`etcdctl` 命令现在可以正常工作，而无需手动设置这些变量。
([BZ#1801430](#))
- 为了防止其中一个 registry Pod 出现问题影响 registry 的可用性，在默认情况下会尽可能有两个 registry 副本。
([BZ#1810563](#))
- 在以前的版本中，Machine Health Check 和 Machine Config 在视觉上没有被分开。现在在这两个项目间添加了一行以将其分开。
([BZ#1819289](#))
- 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#1824427](#), [BZ#1833226](#))
- 在以前的版本中，如果 Dockerfile 带有 ARG 步骤的 OpenShift Docker 策略构建，在调用 `buildah` 前会失败，因为处理 ARG 步骤所需的映射没有初始化。在这个版本中，映射会被初始化，在调用 `buildah` 之前，带有 ARG 步骤的 Dockerfile OpenShift Docker 策略构建将不会导致 panic。
([BZ#1832975](#))
- 在以前的版本中，已过时的 `ImageStreamImport` 错误消息让用户无法了解当前存在的 `ImageStreamImport` 问题。在这个版本中，更新 `ImageStreamImport` 错误消息的逻辑已被更新，以更好地判断连续错误是否来自不同的根原因，并相应地更新错误信息。因此，用户在连续尝试解决 `ImageStreamImport` 问题失败后，可以获得更好的指导信息。
([BZ#1833019](#))
- 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。因此，在 OCP 在 4.3.z 版本的升级过程中，已弃用的规则被保留。现在，`cluster-network-operator` 已被更新。已弃用的安全组规则会被删除，以便在 4.3.z 升级后 Pod 继续对正确的主机 VM 访问限制。
([BZ#1834858](#))

1.7.29.2. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.30. RHBA-2020:2256 - OpenShift Container Platform 4.3.23 程序错误修复更新

发布日期：2020 年 6 月 2 日

OpenShift Container Platform release 4.3.23 现已正式发布。其软件包列表包括在 [RHBA-2020:2255](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:2256](#) 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 4.3.23 容器镜像列表](#)

1.7.30.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.31. RHBA-2020:2436 - OpenShift Container Platform 4.3.25 程序错误修复更新

发布日期：2020 年 6 月 16 日

OpenShift Container Platform release 4.3.25 现已正式发布。其软件包列表包括在 [RHBA-2020:2435](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:2436](#) 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 4.3.25 容器镜像列表](#)

1.7.31.1. 程序错误修复

- 在以前的版本中，用户可能在错误的 master 节点上运行 `etc-member-add.sh`，从而导致 etcd 丢失仲裁。在这个版本中，如果 etcd 已在指定的 master 节点上运行，额外的检查可防止用户运行该脚本。(BZ#1804067)
- 在以前的版本中，如果后续版本中删除了来自较早版本的示例镜像流，因为需要更新缺少的镜像流被错误跟踪，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镜像流。(BZ#1811206)
- 在本发行版本中，用户可从 **ConfigMap** 对象收集有关配置的数据，以确定证书是否用于集群 CA，并从 **openshift-config** 命名空间中收集其他与集群相关的设置。(BZ#1825758)
- 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#1829046)
- 在这个版本中，用户可以收集有关未批准的证书服务请求的匿名数据，以帮助排除问题。(BZ#1835094)
- 在以前的版本中，Samples operator 无法完成 s390x 架构的升级，因为它无法找到不存在的样本内容，从而导致整个升级失败。在这个版本中，Samples operator 不会在 s390x 升级过程中尝试检索样本内容。
另外，还有一个使 Samples operator 退出降级状态的一个临时解决方案。集群管理员可以运行 `oc delete config.samples cluster` 来重置 Samples Operator。(BZ#1835996)
- 在以前的版本中，在 Azure 上使用 IPI 时无法创建 Image Registry Operator，因为 API 限制不允许引导包含空容器的配置对象。在本发行版本中，API 的限制已被删除。(BZ#1836753)
- 在以前的版本中，处理证书轮转的过程中存在一个错误，会导致 Prometheus 无法从 `/metrics` 端点获取数据。这个版本已经解决了这个问题。(BZ#1836939)
- 在以前的版本中，当用户使用 CLI 或 YAML 创建 PipelineRun 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#1839036)
- 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#1841996)

1.7.31.2. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.32. RHSA-2020:2439 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 6 月 16 日

OpenShift Container Platform 4.3 现在提供了 **machine-config-operator-container** 的更新。有关更新的详情请查看 [RHSA-2020:2439](#) 公告。

1.7.33. RHSA-2020:2440 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 6 月 16 日

OpenShift Container Platform 4.3 现在提供了对 Kubernetes 的更新。有关更新的详情请查看 [RHSA-2020:2440](#) 公告。

1.7.34. RHSA-2020:2441 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 6 月 16 日

OpenShift Container Platform 4.3 现在提供了对 Kubernetes 的更新。有关更新的详情请查看 [RHSA-2020:2441](#) 公告。

1.7.35. RHSA-2020:2442 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 6 月 16 日

OpenShift Container Platform 4.3 现在提供了 **openshift-enterprise-apb-tools-container** 的更新。有关更新的详情请查看 [RHSA-2020:2442](#) 公告。

1.7.36. RHSA-2020:2443 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 6 月 16 日

OpenShift Container Platform 4.3 现在提供了 **containernetworking-plugins** 的更新。有关更新的详情请查看 [RHSA-2020:2443](#) 公告。

1.7.37. RHBA-2020:2436 - OpenShift Container Platform 4.3.26 程序错误修复更新

发布日期：2020 年 6 月 23 日

OpenShift Container Platform 版本 4.3.26 现已正式发布。其软件包列表包括在 [RHBA-2020:2435](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:2436](#) 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 4.3.26 容器镜像列表](#)

1.7.37.1. 功能

1.7.37.1.1. 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>
```

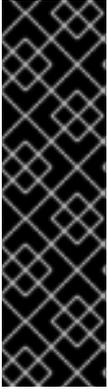
如需更多信息，请参阅 [Jenkins 代理](#)。

1.7.37.2. 程序错误修复

- 由于在 OpenShift Container Platform 4.2 及之后的版本中为示例提供了断开连接的集群支持，Samples Operator 必须允许 samplesRegistry 的应用程序覆盖基于 CVO 安装有效负载镜像的 Jenkins 镜像流。这会导致 samplesRegistry 覆盖更为困难，因为 CVO 有效负载中的 Jenkins 镜像规格与用户可能已决定镜像的 [quay.io](#) 或 [registry.redhat.io](#) 中的类似规格不匹配。另外，这些 registry 上的 Jenkins 镜像违反了红帽为 Jenkins 镜像提供的特殊问题单支持合同，因为它是基本的 OpenShift 安装的一部分。此程序错误修复删除了对 Jenkins 镜像流的 samplesRegistry 覆盖的使用，镜像 registry 现在可在安装镜像时处理 Jenkins 镜像流的导入。现在，当您使用 samplesOverride 将来自 [registry.redhat.io](#) 以外的其他位置的示例镜像流放置到其他示例镜像流时，Jenkins 镜像流会导入。(BZ#1826028)
- 在以前的版本中，在 Home → Search 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订阅详情。(BZ#1827747)
- 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#1832144)
- 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#1844117)

1.7.37.3. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.38. RHSA-2020:2635 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 6 月 23 日

OpenShift Container Platform 4.3 现在提供了对 [python-psutil](#) 的更新。有关更新的详情请查看 [RHSA-2020:2635](#) 公告。

1.7.39. RHBA-2020:2628 - OpenShift Container Platform 4.3.27 程序错误修复更新

发布日期：2020 年 6 月 30 日

OpenShift Container Platform release 4.3.27 现已正式发布。其软件包列表包括在 [RHBA-2020:2627](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:2628](#) 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 4.3.27 容器镜像列表](#)

1.7.39.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.40. RHBA-2020:2805 - OpenShift Container Platform 4.3.28 程序错误修复更新

发布日期：2020 年 7 月 7 日

OpenShift Container Platform release 4.3.28 现已正式发布。其软件包列表包括在 [RHBA-2020:2804](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:2805](#) 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 4.3.28 容器镜像列表

1.7.40.1. 程序错误修复

- 在以前的版本中，触发器无法在 `v1.StatefulSet` 对象上工作，因为触发器控制器无法将 `StatefulSet` 识别为 GA。这个版本已经解决了这个问题。(BZ#1831888)
- 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#1835578)
- 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。这个更改需要将新的监听器添加到指定 UDP 协议的现有 DNS 服务中，但现有 DNS 负载均衡器的旧的 Amphora 镜像不支持新的监听程序，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#1846459)
- 在以前的版本中，Azure 磁盘的 Kubernetes 卷插件无法查找附加的 Azure 卷，因为它需要在主机操作系统上安装新的 `udev` 规则。因此，所有使用卷的 Pod 都无法在 RHEL 7 上启动。在这个版本中，Azure 磁盘的 Kubernetes 卷插件会扫描附加的 Azure 磁盘（即使使用 RHEL 7 的 `udev` 规则），带有 Azure 磁盘卷的 Pod 可在 RHEL 7 上启动。(BZ#1847089)
- 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。在这个发行版本中，依赖 Terraform 步骤列为 `dependent_on` 以强制按正确顺序运行 Terraform 步骤。(BZ#1849171)

1.7.40.2. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.41. RHBA-2020:2872 - OpenShift Container Platform 4.3.29 程序错误修复更新

发布日期：2020 年 7 月 14 日

OpenShift Container Platform release 4.3.29 现已正式发布。其软件包列表包括在 [RHBA-2020:2879](#) 公告中。此更新包括的容器镜像及程序错误修正由 [RHBA-2020:2872](#) 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 4.3.29 容器镜像列表

1.7.41.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.42. RHBA-2020:3180 - OpenShift Container Platform 4.3.31 程序错误修复更新

发布日期：2020 年 8 月 5 日

OpenShift Container Platform release 4.3.31 现已正式发布。其容器镜像及程序错误修正信息包括在[RHBA-2020:3180](#) 公告中。此更新包括的软件包列表由[RHBA-2020:3179](#) 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 4.3.31 容器镜像列表

1.7.42.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.43. RHSA-2020:3183 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 8 月 5 日

OpenShift Container Platform 4.3 现在提供了 **openshift** 的更新。有关更新的详情请查看 [RHSA-2020:3183](#) 公告。

1.7.44. RHSA-2020:3184 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 8 月 5 日

OpenShift Container Platform 4.3 现在提供了 **openshift-enterprise-builder-container** 的更新。有关更新的详情，请查看 [RHSA-2020:3184](#) 公告。

1.7.45. RHBA-2020:3259 - OpenShift Container Platform 4.3.33 程序错误修复更新

发布日期：2020 年 8 月 19 日

OpenShift Container Platform release 4.3.33 现已正式发布。其容器镜像及程序错误修正信息包括在 [RHBA-2020:3259](#) 公告中。其软件包列表由 [RHBA-2020:3258](#) 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 4.3.33 容器镜像列表](#)

1.7.45.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.46. RHBA-2020:3457 - OpenShift Container Platform 4.3.35 程序错误修复更新

发布日期：2020 年 9 月 9 日

OpenShift Container Platform release 4.3.35 现已正式发布。其容器镜像及程序错误修正信息包括在 [RHBA-2020:3457](#) 公告中。其软件包列表由 [RHBA-2020:3458](#) 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 4.3.35 容器镜像列表](#)

1.7.46.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.47. RHSA-2020:3616 - Important: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 9 月 9 日

OpenShift Container Platform 4.3 现在提供了对 **jenkins-2-plugins** 的更新。有关更新的详情请查看 [RHSA-2020:3616](#) 公告。

1.7.48. RHBA-2020:3609 - OpenShift Container Platform 4.3.38 程序错误修复更新

发布日期：2020 年 9 月 23 日

OpenShift Container Platform release 4.3.38 现已正式发布。其容器镜像及程序错误修正信息包括在 [RHBA-2020:3609](#) 公告中。其软件包列表由 [RHBA-2020:3610](#) 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 4.3.38 容器镜像列表](#)

1.7.48.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.49. RHSA-2020:3808 - Important: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 9 月 23 日

OpenShift Container Platform 4.3 现在提供了对 **jenkins** 和 **openshift** 的更新。有关更新的详情请查看 [RHSA-2020:3808](#) 公告。

1.7.50. RHSA-2020:3809 - Moderate: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 9 月 23 日

OpenShift Container Platform 4.3 现在提供了 **openshift-enterprise-hyperkube-container** 和 **sriov-dp-admission-controller-container** 的更新。有关更新的详情请查看 [RHSA-2020:3809](#) 公告。

1.7.51. RHSA-2020:4264 - Low: OpenShift Container Platform 4.3.40 安全和程序错误修复更新

发布日期：2020 年 10 月 20 日

OpenShift Container Platform release 4.3.40（包括 [golang.org/x/crypto](#) 的安全更新）现已正式发布。[RHSA-2020:4264](#) 公告中记录了容器镜像、程序错误修正和 CVE。

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 4.3.40 容器镜像列表](#)

1.7.51.1. 升级

要将现有 OpenShift Container Platform 4.3 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](#)。



重要

如果您要从 OpenShift Container Platform 4.2、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。

1.7.52. RHSA-2020:4265 - Important: OpenShift Container Platform 4.3 安全更新

发布日期：2020 年 10 月 20 日

OpenShift Container Platform 4.3 现在提供了对 **jenkins-2-plugins** 的更新。有关更新的详情请查看 [RHSA-2020:4265](#) 公告。

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 4.3 集群中，所有的 master 必需是 4.3，所有节点也必需是 4.3。如果安装了旧版本的 **oc**，则无法使用 OpenShift Container Platform 4.3 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。