云容器引擎
Autopilot
服务公告

文档版本 01

发布日期 2025-01-14

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 最新公告

以下为CCE Autopilot集群发布的最新公告，请您关注。

序号	公告标题	公告类型	发布时间
1	华为云容器服务CCE Autopilot数据面账单变更公告	产品变更公告	2024/09/14
2	华为云容器服务CCE Autopilot于2024年9月30日00:00（北京时间）转商	产品变更公告	2024/08/29
3	Kubernetes安全漏洞公告（CVE-2024-10220）	漏洞公告	2024/12/04
4	NGINX Ingress控制器验证绕过漏洞公告（CVE-2024-7646）	漏洞公告	2024/08/26
5	Fluent Bit内存崩溃漏洞公告（CVE-2024-4323）	漏洞公告	2024/05/23

更多历史公告请详见**产品变更公告**和**漏洞公告**。

2 产品变更公告

2.1 华为云容器服务 CCE Autopilot 数据面账单变更公告

发布时间：2024/09/14

华为云计划于2024/09/18 22:00:00（北京时间）对CCE Autopilot数据面CPU、内存资源账单进行调整，调整后CCE Autopilot数据面资源账单的产品类型将从云容器引擎CCE调整为云容器实例CCI，此次调整资源单价保持不变，已出历史账单不变，不会对您的业务使用造成影响，具体调整如下：

表 2-1 调整前

产品类型	产品	计费模式	使用类型	单价单位	规格
云容器引擎 CCE	CCE Autopilot	按需	时长	元/秒	CCE 内存资源
云容器引擎 CCE	CCE Autopilot	按需	时长	元/秒	CCE CPU资源

表 2-2 调整后

产品类型	产品	计费模式	使用类型	单价单位	规格
云容器实例 CCI	云容器实例 - Autopilot Resources	按需	时长	元/秒	Autopilot通用型内存资源
云容器实例 CCI	云容器实例 - Autopilot Resources	按需	时长	元/秒	Autopilot通用型CPU资源

如您有任何问题，可随时通过工单或者服务热线（4000-955-988或950808）与我们联系。

感谢您对华为云的支持！

2.2 华为云容器服务 CCE Autopilot 于 2024 年 9 月 30 日 00:00（北京时间）转商

发布时间：2024/08/29

华为云计划于2024年9月30日00:00（北京时间）将容器服务CCE Autopilot正式转商用。

服务正式商用后将收取集群管理费用，其余费用与公测期间保持一致，更多收费说明请参见**按需计费区域单价**。

关于CCE Autopilot的更多介绍，请参见**什么是CCE Autopilot集群**。

如您有任何问题，可随时通过**工单**与我们联系。

感谢您对华为云的支持！

公告原文请参考**华为云产品转商通知：华为云容器服务CCE Autopilot于2024年9月30日00:00（北京时间）转商**。

3 漏洞公告

3.1 漏洞修复策略

集群漏洞修复周期

- 高危漏洞：
  - Kubernetes社区发现漏洞并发布修复方案后，CCE Autopilot集群一般在1个月内进行修复，修复策略与社区保持一致。
  - 操作系统紧急漏洞按照操作系统修复策略和流程对外发布，一般在1个月内提供修复方案，用户自行修复。
- 其他漏洞：

  按照版本正常升级流程解决。

修复声明

为了防止客户遭遇不当风险，除漏洞背景信息、漏洞详情、漏洞原理分析、影响范围/版本/场景、解决方案以及参考信息等内容外，CCE Autopilot集群不提供有关漏洞细节的其他信息。

此外，CCE Autopilot集群为所有客户提供相同的信息，以平等地保护所有客户。CCE Autopilot集群不会向个别客户提供事先通知。

最后，CCE Autopilot集群不会针对产品中的漏洞开发或发布可利用的入侵代码（或“验证性代码”）。

3.2 Kubernetes 安全漏洞公告（CVE-2024-10220）

Kubernetes社区近日公布了一个安全漏洞（CVE-2024-10220），该漏洞使得具有创建Pod权限的攻击者能够通过部署配置了gitRepo卷的Pod来执行容器外的任意命令。攻击者可以利用目标Git仓库中的钩子（hooks）目录，实现容器逃逸并执行攻击命令。

漏洞详情

表 3-1 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
容器逃逸	CVE-2024-10220	高	2024-11-22

漏洞影响

受影响的CCE Autopilot集群版本如下：

- v1.27.0-r0-v1.27.8-r0
- v1.28.0-r0-v1.28.6-r0

判断方法

登录CCE控制台，单击集群名称进入集群总览页面，查看集群版本。

图 3-1 集群版本

- 如果集群版本不在上述范围内则不受漏洞影响。
- 如果集群版本在受影响范围内，您可以通过以下命令，检查集群中是否存在该漏洞被利用的情况。

  该命令会列举所有挂载使用了gitRepo类型的存储卷，并将仓库克隆到.git子目录的Pod中。

  ```
  kubectl get pods --all-namespaces -o yaml | grep gitRepo -A 2
  ```

  ```
  [root@j~]# kubectl get pods --all-namespaces -o yaml | grep gitRepo -A 2
      - gitRepo:
          repository: git@so...tory.git
          revision: 22f...c253775
  ```

  如果返回中不存在gitRepo配置则不受漏洞影响。

漏洞修复方案

- 当前CCE Autopilot集群已修复该漏洞，请及时将集群升级至漏洞修复版本。已EOS集群版本请升级到在维版本进行修复。

  已修复集群版本：v1.27.9-r0，v1.28.7-r0及以上版本。
- 由于**gitRepo存储卷**已被弃用，社区建议的解决方案是使用initContainers容器执行Git克隆操作，然后将目录挂载至Pod容器中，请参见**社区示例**。

相关链接

https://github.com/kubernetes/kubernetes/issues/128885

3.3 NGINX Ingress 控制器验证绕过漏洞公告（CVE-2024-7646）

漏洞详情

表 3-2 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
验证绕过、命令注入	**CVE-2024-7646**	严重	2024-08-19

漏洞影响

在社区ingress-nginx控制器v1.11.2之前的版本中，攻击者若具备在Kubernetes集群中创建Ingress对象（属于networking.k8s.io或extensions API 组）的权限，可能绕过注解验证并注入任意命令，从而获取ingress-nginx控制器的凭证，并访问集群中的所有敏感信息。

CCE Autopilot集群中安装NGINX Ingress控制器插件，且版本低于2.4.14时涉及该漏洞。

判断方法

1. 使用kubectl查找与cceaddon-nginx-ingress相关的Pod：

   kubectl get po -A | grep cceaddon-nginx-ingress

   ```
   [root@192-168-53-14 paas]# kubectl get po -A|grep cceaddon-nginx-ingress
   kube-system   cceaddon-nginx-ingress-controller-67bff65f66-h8xlt        1/1     Running
   kube-system   cceaddon-nginx-ingress-default-backend-699d6f4578-nqqqr   1/1     Running
   ```

   若返回如上图，则代表集群中安装了NGINX Ingress控制器插件。
2. 检查NGINX Ingress控制器插件使用的nginx-ingress镜像版本：

   kubectl get deploy cceaddon-nginx-ingress-controller -nkube-system -oyaml|grep -w image

   ```
   [root@192-168-53-14 paas]# kubectl get deploy cceaddon-nginx-ingress-controller -nkube-system -oyaml|grep -w image
         image: [redacted]hwofficial/nginx-ingres:v1.11.2
         image: [redacted]hwofficial/nginx-ingres:v1.11.2
   ```

   如上图，若当前安装的NGINX Ingress控制器插件对应的社区nginx-ingress版本低于v1.11.2，则涉及该漏洞。

漏洞修复方案

当前CCE Autopilot集群的NGINX Ingress控制器插件已修复该漏洞，请及时将插件升级至漏洞修复版本。

已修复插件版本：2.4.14及以上版本。

相关链接

社区已经发布版本修复：**https://github.com/kubernetes/ingress-nginx/releases/tag/controller-v1.11.2**。

3.4 Fluent Bit 内存崩溃漏洞公告（CVE-2024-4323）

Fluent Bit是一个功能强大、灵活且易于使用的日志处理和转发工具，适用于各种规模和类型的应用和系统（如Linux、Windows、嵌入式Linux、MacOS等）。Fluent Bit是众多云提供商和企业使用的流行日志记录实用程序，目前下载和部署次数已超过130亿次。

漏洞详情

表 3-3 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
缓冲区溢出	CVE-2024-4323	严重	2024-05-20

漏洞影响

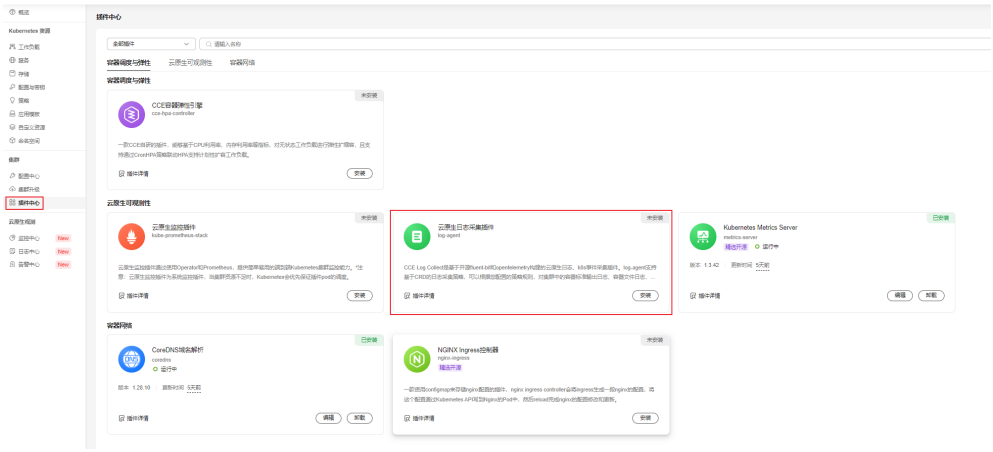
Fluent Bit版本2.0.7-3.0.3中存在堆缓冲区溢出漏洞，该漏洞存在于Fluent Bit的嵌入式http服务器对跟踪请求的解析中，由于在解析/api/v1/traces 端点的传入请求时，在解析之前未正确验证input_name的数据类型，可通过在请求的“inputs”数组中传递非字符串值（如整数值），可能导致内存崩溃，成功利用该漏洞可能导致拒绝服务、信息泄露或远程代码执行。

CCE Autopilot集群中安装云原生日志采集插件，且版本低于1.7.0时涉及该漏洞。

判断方法

1. 前往插件中心，查看是否已安装云原生日志采集插件。

图 3-2 查看已安装插件版本



2. 单击云原生日志采集插件的插件详情，查看当前插件版本。若插件版本在1.7.0以下，则涉及该漏洞。

图 3-3 插件详情

漏洞修复方案

当前CCE Autopilot集群的云原生日志采集插件已修复该漏洞，请及时将插件升级至漏洞修复版本。

已修复插件版本：1.7.0及以上版本。

4 产品发布记录

4.1 集群版本发布记录

4.1.1 Kubernetes 版本策略

云容器引擎（Cloud Container Engine，简称CCE）提供高度可扩展的、高性能的企业级Kubernetes集群。由于社区定期发布Kubernetes版本，CCE Autopilot集群会随之发布相应的集群公测和商用版本。本文将为您介绍CCE Autopilot集群的Kubernetes版本策略。

CCE Autopilot 集群版本生命周期表

Kubernetes版本号	当前状态	社区发布时间	集群版本公测时间	集群版本商用时间	CCE集群版本EOS（停止服务）时间
v1.31	公测	2024年8月	2024年12月	-	-
v1.28	已商用	2023年8月	2024年4月	2024年9月	2026年2月
v1.27	已商用	2023年04月	2024年2月	2024年9月	2025年10月

CCE Autopilot 集群版本阶段说明

- 版本公测阶段：您可以通过CCE Autopilot集群公测版本体验最新的Kubernetes版本特性，但需要注意该版本的稳定性未得到完全的验证，不适用于CCE服务SLA。
- 版本商用阶段：CCE Autopilot集群商用版本经过充分验证，稳定可靠。您可以将该版本用于生产环境，享受CCE服务SLA保障。
- 版本EOS（停止服务）阶段：CCE Autopilot集群版本EOS之后，CCE将不再支持对该版本的集群创建，同时不提供相应的技术支持，包含新特性更新、漏洞/问题修

复、补丁升级以及工单指导、在线排查等客户支持，不再适用于CCE服务SLA保障。

CCE Autopilot 集群版本号说明

CCE Autopilot集群基于社区Kubernetes版本迭代演进，因此集群版本号由社区Kubernetes版本和CCE Autopilot集群补丁版本两部分共同构成，格式为vX.Y.Z-rN（例如v1.28.2-r0）：

- Kubernetes版本：格式为**X.Y.Z**，继承社区版本策略，其中**X**对应社区Kubernetes的主要版本，**Y**对应社区Kubernetes的次要版本，**Z**对应社区Kubernetes的补丁版本，详情请参见**社区Kubernetes版本策略**。关于CCE Autopilot集群支持的Kubernetes版本详情，请参见**Kubernetes版本发布记录**。
- CCE Autopilot集群补丁版本：格式形如v1.30.**4-rN**，处于维护期的Kubernetes版本会不定期地发布新的补丁版本。当新的补丁版本较上一版本提供了新的特性、Bugfix、漏洞修复或场景优化时，**N**版本号增加。关于CCE Autopilot集群补丁版本详情，请参见**Autopilot集群补丁版本发布记录**。

集群升级

为了方便您体验新特性、规避已知漏洞/问题，使用安全、稳定、可靠的Kubernetes版本，建议您定期升级CCE Autopilot集群。CCE Autopilot集群版本EOS之后，您将无法获得相应的技术支持以及CCE服务SLA保障，请及时升级CCE Autopilot集群。

您可以通过CCE Autopilot集群控制台，轻松实现对Kubernetes版本的可视化升级，提升集群业务的稳定性和可靠性，详情请参见**升级概述**。

4.1.2 Kubernetes 版本发布记录

4.1.2.1 Kubernetes 1.31 版本说明（公测）

CCE Autopilot集群严格遵循社区一致性认证，现已支持创建Kubernetes 1.31集群。本文介绍Kubernetes 1.31版本的变更说明。

索引

新增特性及特性增强

Kubernetes 1.31版本

- StatefulSet起始序号（GA）

  在Kubernetes 1.31中，StatefulSetStartOrdinal特性进阶至GA。默认情况下，StatefulSet中Pod的序号是从0开始，该特性引入后允许用户自定义Pod的起始序号。详细使用方式请参考**起始序号**。

- 弹性索引Job（GA）

  在Kubernetes 1.31中，ElasticIndexedJob特性进阶至GA。该特性允许用户在索引Job创建后修改其.spec.completions和.spec.parallelism字段，使之具备弹性伸缩能力。详细使用方式请参考**弹性索引Job**。

- Pod失效策略（GA）

  在Kubernetes 1.31中，JobPodFailurePolicy特性进阶至GA。该特性允许用户根据Pod失效的原因来分别指定处理方式（重试或者忽略），以优化避免不必要的Pod重启带来的运行成本。详细使用方式请参考**Pod失效策略**。

- Pod干扰状况（GA）

  在Kubernetes 1.31中，PodDisruptionConditions特性进阶至GA。该特性在Pod的Condition中新增了DisruptionTarget类型，表示Pod失效的原因，例如被高优先级的Pod抢占、因节点删除而被清理、被kubelet终止等。若Pod是Job或者CronJob控制器创建的，可以与**Pod失效策略**一起使用，通过该Condition定义失效时的行为。更多关于本特性的详细信息请参考**Pod干扰状况**。

- 定制资源的可选择字段（Beta）

  在Kubernetes 1.31中，CustomResourceFieldSelectors特性进阶至Beta。该特性支持对CRD配置selectableFields，并支持使用Field Selectors过滤List、Watch和DeleteCollection请求，方便用户定位或管理符合特定条件的CRD资源。详细使用方式请参考**定制资源的可选择字段**。

- Job成功策略（Beta）

  在Kubernetes 1.31中，JobSuccessPolicy特性进阶至Beta。该特性允许用户基于成功的Pod个数为Job配置成功策略。详细使用方式请参考**成功策略**。

- podAffinity中的matchLabelKeys（Beta）

  在Kubernetes 1.31中，MatchLabelKeysInPodAffinity特性进阶至Beta。该特性在podAffinity和podAntiAffinity中引入了更为精细的配置字段matchLabelKeys和mismatchLabelKeys，以解决调度器在Deployment滚动更新期间无法区分新老Pod，继而导致调度结果不符合亲和性和反亲和性预期的问题。详细使用方式请参考**matchLabelKeys**。

- ServiceAccountTokenNodeBinding（Beta）

  在Kubernetes 1.31中，ServiceAccountTokenNodeBinding特性进阶至Beta。该特性支持创建绑定到节点的ServiceAccount Token：在Token中包含节点信息的声明，并在使用Token时验证节点的存在，若节点被删除，则Token将会失效。详细使用方式请参考**手动为 ServiceAccount 创建 API 令牌**。

Kubernetes 1.30版本

- Webhook匹配表达式（GA）

  在Kubernetes1.30版本中，Webhook匹配表达式特性进阶至GA。此特性允许对准入Webhook支持根据特定的条件进行匹配，更细粒度地控制Webhook的触发条件。详细使用方式请参考**动态准入控制**。

- 验证准入策略（GA）

  在Kubernetes1.30版本中，验证准入策略（ValidatingAdmissionPolicy）特性进阶至GA。该特性支持通过CEL表达式声明资源的验证准入策略。详细使用方式请参考**验证准入策略**。

- 基于ContainerResource指标的Pod水平自动扩缩容（GA）

  在Kubernetes1.30版本中，基于ContainerResource指标的Pod水平自动扩缩容特性进阶至GA。该特性允许HPA根据Pod中各个容器的资源使用情况来配置自动伸缩，而不仅是Pod的整体资源使用情况，便于为Pod中最重要的容器配置扩缩容阈值。详细使用方式请参考**容器资源指标**。

- 传统ServiceAccount令牌清理器（GA）

  在Kubernetes1.30版本中，传统ServiceAccount令牌清理器特性进阶至GA。其作为kube-controller-manager的一部分运行，每24小时检查一次，查看是否有任何

自动生成的传统ServiceAccount令牌在特定时间段内（默认为一年，通过--legacy-service-account-token-clean-up-period指定）未被使用。如果有的话，清理器会将这些令牌标记为无效，并添加kubernetes.io/legacy-token-invalid-since标签，其值为当前日期。如果一个无效的令牌在特定时间段（默认为1年，通过--legacy-service-account-token-clean-up-period指定）内未被使用，清理器将会删除它。更多使用细节请参考**传统ServiceAccount令牌清理器**。

Kubernetes 1.29版本

- Service的负载均衡IP模式（Alpha）

  在Kubernetes1.29版本，Service的负载均衡IP模式以Alpha版本正式发布。其在Service的status中新增字段ipMode，用于配置集群内Service到Pod的流量转发模式。当设置为VIP时，目的地址为负载均衡IP和端口的流量将由kube-proxy重定向到目标节点，当设置为Proxy时，流量将被发送到负载均衡器，然后由负载均衡器转发到目标节点。这项特性将有助于解决流量绕过负载均衡器缩导致的负载均衡器功能缺失问题。更多使用细节请参考**Service的负载均衡IP模式**。

- NFTables代理模式（Alpha）

  在Kubernetes1.29版本，NFTables代理模式以Alpha版本正式发布。该特性允许kube-proxy运行在NFTables模式，在该模式下，kube-proxy使用内核netfilters子系统的nftables API来配置数据包转发规则。更多使用细节请参考**NFTables代理模式**。

- 未使用容器镜像的垃圾收集（Alpha）

  在Kubernetes1.29版本，未使用容器镜像的垃圾收集以Alpha版本正式发布。该特性允许用户为每个节点配置本地镜像未被使用的最长时间，超过这个时间镜像将被垃圾回收。配置方法为使用kubelet配置文件中的ImageMaximumGCAge字段。更多使用细节请参考**未使用容器镜像的垃圾收集**。

- PodLifecycleSleepAction（Alpha）

  在Kubernetes1.29版本，PodLifecycleSleepAction以Alpha版本正式发布。该特性在容器生命周期回调中引入了Sleep回调程序，可以配置让容器在启动后和停止前暂停一段指定的时间。更多使用细节请参考**PodLifecycleSleepAction**。

- KubeletSeparateDiskGC（Alpha）

  在Kubernetes1.29版本，KubeletSeparateDiskGC以Alpha版本正式发布。该特性启用后，即使在容器镜像和容器位于独立文件系统的情况下，也能进行垃圾回收。

- matchLabelKeys/mismatchLabelKeys（Alpha）

  在Kubernetes1.29版本，matchLabelKeys/mismatchLabelKeys以Alpha版本正式发布。该特性启用后，在Pod的亲和/反亲和配置中新增了matchLabelKeys/mismatchLabelKeys字段，可配置更丰富的Pod间亲和/反亲和策略。更多使用细节请参考**matchLabelKeys/mismatchLabelKeys**。

- clusterTrustBundle投射卷（Alpha）

  在Kubernetes1.29版本，clusterTrustBundle投射卷以Alpha版本正式发布。该特性启用后，支持将ClusterTrustBundle对象以自动更新的文件的形式注入卷。更多使用细节请参考**clusterTrustBundle投射卷**。

- 基于运行时类的镜像拉取（Alpha）

  在Kubernetes1.29版本中，基于运行时类的镜像拉取以Alpha版本正式发布。该特性启用后， kubelet 会通过一个元组（镜像名称，运行时处理程序）而不仅仅是镜像名称或镜像摘要来引用容器镜像。 您的容器运行时可能会根据选定的运行时处理程序调整其行为。基于运行时类来拉取镜像对于基于VM的容器会有帮助。更多使用细节请参考**基于运行时类的镜像拉取**。

- PodReadyToStartContainers状况达到Beta

  在Kubernetes1.29版本，PodReadyToStartContainers状况特性达到Beta版本。其在Pod的status中新增了一个名为PodReadyToStartContainers的Condition，该Condition为true表示Pod的沙箱已就绪，可以开始创建业务容器。该特性使得集群管理员可以更清晰和全面地查看 Pod 沙箱的创建完成和容器的就绪状态，增强了指标监控和故障排查能力。更多使用细节请参考**PodReadyToStartContainersCondition**。

- Job相关特性
  - Pod更换策略达到Beta

    在Kubernetes1.29版本，Pod更换策略特性达到Beta版本。该特性确保只有Pod达到Failed阶段（ status.phase: Failed ）才会被替换，而不是当删除时间戳不为空时，Pod仍处于删除过程中就重建Pod，以此避免出现2个Pod同时占用索引和节点资源。
  - 逐索引的回退限制达到Beta

    在Kubernetes1.29版本，逐索引的回退限制特性达到Beta版本。默认情况下，带索引的 Job（ Indexed Job ）的 Pod 失败情况会被统计下来，受 .spec.backoffLimit 字段所设置的全局重试次数限制。这意味着，如果存在某个索引值的 Pod 一直持续失败，则会 Pod 会被重新启动，直到重试次数达到限制值。 一旦达到限制值，整个 Job 将被标记为失败，并且对应某些索引的 Pod 甚至可能从不曾被启动。该特性可以在某些索引值的 Pod 失败的情况下，仍完成执行所有索引值的 Pod，并且通过避免对持续失败的、特定索引值的Pod进行不必要的重试，更好地利用计算资源。

- 原生边车容器达到Beta

  在Kubernetes1.29版本，原生边车容器特性达到Beta版本。其在initContainers中新增了restartPolicy字段，当配置为Always时表示启用边车容器。边车容器和业务容器部署在同一个Pod中，但并不会延长Pod的生命周期。边车容器常用于网络代理、日志收集等场景。更多使用细节请参考**边车容器**。

- 传统ServiceAccount令牌清理器达到Beta

  在Kubernetes1.29版本，传统ServiceAccount令牌清理器特性达到Beta版本。其作为kube-controller-manager的一部分运行，每24小时检查一次，查看是否有任何自动生成的传统ServiceAccount令牌在特定时间段内（ 默认为一年，通过--legacy-service-account-token-clean-up-period指定 ）未被使用。如果有的话，清理器会将这些令牌标记为无效，并添加kubernetes.io/legacy-token-invalid-since标签，其值为当前日期。如果一个无效的令牌在特定时间段（ 默认为1年，通过--legacy-service-account-token-clean-up-period指定 ）内未被使用，清理器将会删除它。更多使用细节请参考**传统ServiceAccount令牌清理器**。

- DevicePluginCDIDevices达到Beta

  在Kubernetes1.29版本，DevicePluginCDIDevices特性达到Beta版本。该特性在DeviceRunContainerOptions增加CDIDevices字段，使得设备插件开发者可以直接将CDI设备名称传递给支持CDI的容器运行时。

- PodHostIPs达到Beta

  在Kubernetes1.29版本中，PodHostIPs特性达到Beta版本。该特性在Pod和downward API的Status中增加hostIPs字段，用于将节点IP地址暴露给工作负载。该字段是hostIP的双栈协议版本，第一个IP始终与hostIP相同。

- API优先级和公平性达到GA

  在Kubernetes1.29版本，API优先级和公平性（ APF ）特性达到GA版本。APF以更细粒度的方式对请求进行分类和隔离，提升最大并发限制，并且它还引入了空间有限的排队机制，因此在非常短暂的突发情况下，API 服务器不会拒绝任何请

求。 通过使用公平排队技术从队列中分发请求，这样，一个行为不佳的控制器就不会导致其他控制器异常（即使优先级相同）。更多使用细节请参考**API优先级和公平性**。

- APIListChunking达到GA

  在Kubernetes1.29版本，APIListChunking特性达到GA版本。该特性允许客户端在List请求中进行分页，避免一次性返回过多数据而导致的性能问题。

- PersistentVolume的阶段转换时间戳达到Beta

  在Kubernetes1.29版本，PersistentVolume的阶段转换时间戳特性达到Beta版本。该特性在PV的status中添加了一个lastPhaseTransitionTime字段，表示PV上一次phase变化的时间。通过该字段，集群管理员可以跟踪PV上次转换到不同阶段的时间，从而实现更高效、更明智的资源管理。更多使用细节请参考**PersistentVolume的阶段转换时间戳**。

- ReadWriteOncePod达到GA

  在Kubernetes1.29版本中，ReadWriteOncePod特性达到GA版本。该特性允许用户在PVC中配置访问模式为ReadWriteOncePod，确保同时只有一个 Pod能够修改存储中的数据，以防止数据冲突或损坏。更多使用细节请参考**ReadWriteOncePod**。

- CSINodeExpandSecret达到GA

  在Kubernetes1.29版本中，CSINodeExpandSecret特性达到GA版本。该特性允许在添加节点时将Secret身份验证数据传递到CSI驱动以供后者使用。

- CRD验证表达式语言达到GA

  在Kubernetes1.29版本中，CRD验证表达式语言特性达到GA版本。该特性允许用户在CRD中使用通用表达式语言（CEL）定义校验规则，相比webhook更加高效。更多使用细节请参考**CRD校验规则**。

API 变更与弃用

Kubernetes 1.31版本

在Kubernetes1.31版本中，在CustomResourceDefinition（CRD）中指定caBundle字段时，如果caBundle非空，但内容无效或不包含任何CA证书，那么该CRD将不会提供服务。CRD的caBundle设置为有效状态后，将不再允许通过更新操作将其变为无效或内容为空的状态（直接更新将报错invalid field value），以避免中断CRD的正常服务。

Kubernetes 1.30版本

- 在Kubernetes1.30版本中，kubectl移除了apply命令的prune-whitelist参数，使用prune-allowlist替代。
- 在Kubernetes1.30版本中，移除了在1.27版本已废弃的准入插件SecurityContextDeny，使用**Pod安全性准入插件**（PodSecurity）替代。

Kubernetes 1.29版本

- 在Kubernetes1.29版本中，新创建的CronJob不再支持在.spec.schedule中通过TZ或者CRON_TZ配置时区，请使用.spec.timeZone替代。已经创建的CronJob不受此影响。
- 在Kubernetes1.29版本中，移除了alpha API ClusterCIDR。
- 在Kubernetes1.29版本中，kube-apiserver新增启动参数--authentication-config，用于指定AuthenticationConfiguration文件地址，该启动参数与--oidc-*启动参数互斥。

- 在Kubernetes1.29版本中，移除了KubeSchedulerConfiguration的API版本kubescheduler.config.k8s.io/v1beta3，请迁移至kubescheduler.config.k8s.io/v1。
- 在Kubernetes1.29版本中，将CEL表达式添加到v1alpha1 AuthenticationConfiguration中。
- 在Kubernetes1.29版本中，新增对象ServiceCIDR，允许用户动态配置集群分配Service的ClusterIP时所使用的地址范围。
- 在Kubernetes1.29版本中，kube-proxy新增启动参数--conntrack-udp-timeout、--conntrack-udp-timeout-stream，可对nf_conntrack_udp_timeout和nf_conntrack_udp_timeout_stream内核参数进行设置 。
- 在Kubernetes1.29版本中，将CEL表达式的支持添加到v1alpha1 AuthenticationConfiguration的WebhookMatchCondition中。
- 在Kubernetes1.29版本中，PVC.spec.Resource的类型由原先的ResourceRequirements替换为VolumeResourceRequirements。
- 在Kubernetes1.29版本中，将PodFailurePolicyRule中的OnPodConditions转变为可选字段。
- 在Kubernetes1.29版本中，FlowSchema与PriorityLevelConfiguration的API版本flowcontrol.apiserver.k8s.io/v1beta3已升级至flowcontrol.apiserver.k8s.io/v1，并进行了以下更改
  - PriorityLevelConfiguration：.spec.limited.nominalConcurrencyShares字段在省略时自动设为默认值30，并且为了确保与1.28兼容，在1.29中v1版本该字段不允许显示指定为0。在1.30中，将允许v1版本该字段显示指定为0。flowcontrol.apiserver.k8s.io/v1beta3已废弃，并在1.32中不再支持。
- 在Kubernetes1.29版本中， 优化了kube-proxy的命令行文档，kube-proxy实际上不会将任何socket绑定到由--bind-address启动参数指定的IP。
- 在Kubernetes1.29版本中，当CSI-Node-Driver没有在运行时，NodeStageVolume操作会重试。
- 在Kubernetes1.29版本中，ValidatingAdmissionPolicy支持对CRD资源进行校验。使用该特性需开启特性门控ValidatingAdmissionPolicy。
- 在Kubernetes1.29版本中，kube-proxy新增启动参数--nf-conntrack-tcp-be-liberal，可对内核参数nf_conntrack_tcp_be_liberal进行配置。
- 在Kubernetes1.29版本中，kube-proxy新增启动参数--init-only，设置后使kube-proxy的init容器在特权模式下运行，进行一些初始化配置，然后退出。
- 在Kubernetes1.29版本中，CRI的返回体中新增容器的fileSystem字段，表示容器的fileSystem使用信息，而原先只包含镜像的fileSystem。
- 在Kubernetes1.29版本中，所有内置的CloudProvider全部默认设置为关闭，如果仍需使用，可通过配置DisableCloudProviders和DisableKubeletCloudCredentialProvider特性门控来选择性关闭或者打开。

参考链接

关于Kubernetes 1.31与其他版本的性能对比和功能演进的更多信息，请参考：

- **Kubernetes v1.31 Release Notes**
- **Kubernetes v1.30 Release Notes**
- **Kubernetes v1.29 Release Notes**

4.1.2.2 Kubernetes 1.28 版本说明

云容器引擎（CCE）严格遵循社区一致性认证，现已支持创建Kubernetes 1.28集群。本文介绍Kubernetes 1.28版本的变更说明。

索引

重要说明

- 在Kubernetes 1.28版本，调度框架发生变化，减少无用的重试，从而提高调度程序的整体性能。如果开发人员在集群中使用了自定义调度程序插件，请参见**调度框架变化**进行适配升级。
- 在Kubernetes 1.28版本，Ceph FS树内插件已在v1.28中弃用，并计划在v1.31中删除（社区没有计划进行CSI迁移）。建议使用**Ceph CSI**第三方存储驱动程序作为替代方案。
- 在Kubernetes 1.28版本，Ceph RBD树内插件已在v1.28中弃用，并计划在v1.31中删除（社区没有计划进行CSI迁移）。建议使用RBD模式的**Ceph CSI**第三方存储驱动程序作为替代方案。

新增特性及特性增强

社区特性的Alpha阶段默认禁用、Beta阶段一般默认启用、GA阶段将一直默认启用，且不能禁用（会在后续版本中删除这个开关功能）。CCE对新特性的策略与社区保持一致。

- 版本偏差策略扩展至3个版本

  从1.28控制平面/1.25工作节点开始，Kubernetes版本偏差策略将支持的控制平面/工作节点偏差扩展到3个版本。 这使得节点的年度次要版本升级成为可能，同时保持受支持的次要版本。更多细节请参考**版本偏差策略**。

- 可追溯的默认StorageClass进阶至GA

  在Kubernetes 1.28版本，可追溯默认StorageClass赋值现已进阶至GA。 这项增强特性极大地改进了默认的StorageClasses为PersistentVolumeClaim（PVC）赋值的方式。

  PersistentVolume（PV）控制器已修改为：当未设置storageClassName时，自动向任何未绑定的PersistentVolumeClaim分配一个默认的StorageClass。此外，API服务器中的PersistentVolumeClaim准入验证机制也已调整为允许将值从未设置状态更改为实际的StorageClass名称。更多使用细节请参考**默认StorageClass赋值**。

- 原生边车容器（Alpha）

  在Kubernetes 1.28版本，原生边车容器以Alpha版本正式发布。其在Init容器中添加了一个新的restartPolicy字段， 该字段在SidecarContainers特性门控启用时可用。需要注意的是，原生边车容器目前仍有些问题需要解决，因此K8S社区建议仅在Alpha阶段的**短期测试集群**中使用边车功能。 更多使用细节请参考**原生边车容器**。

- 混合版本代理（Alpha）

  在Kubernetes 1.28版本，发布了用于改进集群安全升级的新机制（混合版本代理）。该特性为Alpha特性。当集群进行升级时，集群中不同版本的kube-apiserver为不同的内置资源集（组、版本、资源）提供服务。在这种情况下资源请求如果由任一可用的apiserver提供服务，请求可能会到达无法解析此请求资源的apiserver中，导致请求失败。该特性能解决该问题。（主要注意的是，CCE本身提供的升级能力即可做到无损升级，因此不存在该特性涉及的场景）。更多使用细节请参考**混合版本代理**。

- 节点非体面关闭特性达到GA

  在Kubernetes 1.28版本，节点非体面关闭特性达到GA阶段。当一个节点被关闭但没有被Kubelet的Node Shutdown Manager检测到时，StatefulSet的Pod将会停留在终止状态，并且不能移动到新运行的节点上。当用户确认该节点已经处于不可恢复的情况下，可以手动为Node打上out-of-service的污点，以使得该节点上的StatefulSet的Pod和VolumeAttachments被强制删除，并在健康的Node上创建相应的Pod。更多使用细节请参考**节点非体面关闭**。

- NodeSwap特性达到Beta

  在Kubernetes 1.28版本，NodeSwap能力进阶至Beta版本。目前仍然处于默认关闭状态，需要使用NodeSwap门控打开。该特性可以为Linux节点上运行的Kubernetes工作负载逐个节点地配置内存交换。需要注意的是，该特性虽然进阶至Beta特性，但仍然存在一些需要增强的问题和安全风险。更多使用细节请参考**NodeSwap特性**。

- Job相关特性

  在Kubernetes 1.28版本，增加了**Pod更换策略**和基于**带索引Job的回退限制**两个alpha特性。

  - Pod更换策略

    默认情况下，当Pod进入终止（Terminating）状态（例如由于抢占或驱逐机制）时，Kubernetes会立即创建一个替换的Pod，因此这时会有两个Pod同时运行。

    在Kubernetes 1.28版本中可以使用JobPodReplacementPolicy 来启用该特性。可以在Job的Spec中定义podReplacementPolicy，目前仅可设置为Failed。在设置为Failed之后，Pod仅在达到Failed阶段时才会被替换，而不是在它们处于终止过程中（Terminating）时被替换。此外，您可以检查Job的.status.termination字段。该字段的值表示终止过程中的Job所关联的Pod数量。

  - 带索引Job的回退限制

    默认情况下，带索引的Job（Indexed Job）的 Pod 失败情况会被记录下来，受.spec.backoffLimit字段所设置的全局重试次数限制。这意味着，如果存在某个索引值的Pod一直持续失败，则Pod会被重新启动，直到重试次数达到限制值。一旦达到限制值，整个Job将被标记为失败，并且对应某些索引的Pod甚至可能从不曾被启动。

    在Kubernetes 1.28版本中，可以通过启用集群的JobBackoffLimitPerIndex特性门控来启用此特性。开启之后，允许在创建带索引的Job（Indexed Job）时指定.spec.backoffLimitPerIndex字段。当某个Job的失败次数超过设定的上限时，将不再进行重试。

- CEL相关特性

  在Kubernetes 1.28版本，CEL能力进行了相应的增强。

  - CRD使用CEL进行Validate的特性进阶至Beta

该特性在v1.25版本就已经升级为Beta版本。通过将CEL表达式直接集成在CRD中，可以使开发者在不使用Webhook的情况下解决大部分对CR实例进行验证的用例。在未来的版本，将继续扩展CEL表达式的功能，以支持默认值和CRD转换。

- 基于CEL的准入控制进阶至Beta

  基于通用表达式语言 (CEL) 的准入控制是可定制的，对于kube-apiserver接受到的请求，可以使用CEL表达式来决定是否接受或拒绝请求，可作为Webhook准入控制的一种替代方案。在 v1.28 中，CEL准入控制被升级为Beta，同时添加了一些新功能，包括但不限于：

  - ValidatingAdmissionPolicy类型检查现在可以正确处理CEL表达式中的“authorizer”变量。
  - ValidatingAdmissionPolicy支持对messageExpression字段进行类型检查。
  - kube-controller-manager组件新增ValidatingAdmissionPolicy控制器，用来对ValidatingAdmissionPolicy中的CEL表达式做类型检查，并将原因保存在状态字段中。
  - 支持变量组合，可以在ValidatingAdmissionPolicy中定义变量，然后在定义其他变量时使用它。
  - 新增CEL库函数支持对Kubernetes的resource.Quantity类型进行解析。

- 其它特性说明
  - 在Kubernetes 1.28版本，ServiceNodePortStaticSubrange 特性为beta，允许保留静态端口范围，避免与动态分配端口冲突。具体细节请参考**为NodePort Service分配端口时避免冲突**。
  - 在Kubernetes 1.28版本，增加了alpha特性ConsistentListFromCache，允许kube-apiserver从缓存中提供一致性列表，Get和List请求可以从缓存中读取数据，而不需要从etcd中获取。
  - 在Kubernetes 1.28版本，kubelet能够配置drop-in目录（alpha特性）。该特性允许向kubelet添加对“--config-dir”标志的支持，以允许用户指定一个插入目录，该目录将覆盖位于/etc/kubernetes/kubelet.conf位置的Kubelet的配置。
  - 在Kubernetes 1.28版本，ExpandedDNSConfig升级至GA，默认会被打开。该参数用于允许扩展DNS的配置。
  - 在Kubernetes 1.28版本，提供Alpha特性CRD Validation Ratcheting。该特性允许Patch或者Update请求没有更改任何不合法的字段，将允许CR验证失败。
  - 在Kubernetes 1.28版本，kube-controller-manager添加了--concurrent-cron-job-syncs flag用来设置cron job controller的workers数。

API 变更与弃用

- 在Kubernetes 1.28版本，移除特性NetworkPolicyStatus，因此Network Policy不再有status属性。
- 在Kubernetes 1.28版本，Job对象中增加了新的annotationbatch.kubernetes.io/cronJob-scheduled-timestamp，表示Job的创建时间。
- 在Kubernetes 1.28版本，Job API中添加podReplacementPolicy和terminating字段，当前一旦先前创建的pod终止，Job就会立即启动替换pod。添加字段允许用

户指定是在先前的Pod终止后立即更换Pod（原行为），还是在现有的Pod完全终止后才替换Pod（新行为）。这是一项Alpha级别特性，您可以通过在集群中启用 **JobPodReplacementPolicy** 来启用该特性。

- 在Kubernetes 1.28版本，Job支持BackoffLimitPerIndex字段。当前使用的运行Job的策略是Job中的整个Pod共享一个Backoff机制，当Job达到Backoff的限制时，整个Job都会被标记为失败，并清理资源，包括尚未运行的index。此字段允许对单个的index设置Backoff。更多信息请参见**带索引Job的Backoff限制**。
- 在Kubernetes 1.28版本，添加ServedVersions字段到 StorageVersion API中。该变化由混合代理版本特性引入。该增加字段ServedVersions用于表明API服务器可以提供的版本。
- 在Kubernetes 1.28版本，SelfSubjectReview 添加到authentication.k8s.io/v1中，并且kubectl auth whoami走向GA。
- 在Kubernetes 1.28版本，PersistentVolume有了一个新的字段 LastPhaseTransitionTime，用来保存最近一次volume转变Phase的时间。
- 在Kubernetes 1.28版本，PVC.Status中移除resizeStatus，使用 AllocatedResourceStatus替代。resizeStatus表示调整存储大小操作的状态，默认为空字符串。
- 在Kubernetes 1.28版本，设置了hostNetwork: true并且定义了ports的Pods，自动设置hostport字段。
- 在Kubernetes 1.28版本，StatefulSet的Pod索引设置为Pod的标签 statefulset.kubernetes.io/pod-index。
- 在Kubernetes 1.28版本，Pod的Condition字段中的PodHasNetwork重命名为 PodReadyToStartContainers，用来表明网络、卷等已成功创建，sandbox pod已经创建完成，可以启动容器。
- 在Kubernetes 1.28版本，在KubeSchedulerConfiguration中添加了新的配置选项 delayCacheUntilActive， 该参数为true时，非master节点的kube-scheduler不会缓存调度信息。这为非主节点的内存减缓了压力，但会导致主节点发生故障时，减慢故障转移的速度。
- 在Kubernetes 1.28版本，在admissionregistration.k8s.io/ v1alpha1.ValidatingAdmissionPolicy中添加namespaceParamRef字段。
- 在Kubernetes 1.28版本，在CRD validation rules中添加reason和fieldPath，允许用户指定验证失败的原因和字段路径。
- 在Kubernetes 1.28版本，ValidatingAdmissionPolicy的CEL表达式通过 namespaceObject支持namespace访问。
- 在Kubernetes 1.28版本，将API groups ValidatingAdmissionPolicy 和 ValidatingAdmissionPolicyBinding提升到betav1。
- 在Kubernetes 1.28版本，ValidatingAdmissionPolicy 扩展了messageExpression 字段，用来检查已解析类型。

特性门禁及命令行参数

- 在Kubernetes 1.28版本，kubelet移除了flag –short。因此kubectl version 默认输出与kubectl version –short相同。
- 在Kubernetes 1.28版本，kube-controller-manager废弃flag--volume-host-cidr-denylist和--volume-host-allow-local-loopback。--volume-host-cidr-denylist是用逗号分隔的一个CIDR范围列表，禁止使用这些地址上的卷插件。--volume-host-allow-local-loopback为false时，禁止本地回路IP地址和--volume-host-cidr-denylist中所指定的CIDR范围。

- 在Kubernetes 1.28版本，kubelet --azure-container-registry-config被弃用并在未来的版本中会被删除。 请使用--image-credential-provider-config和--image-credential-provider-bin-dir来设置。
- 在Kubernetes 1.28版本，kube-scheduler: 删除了--lock-object-namespace和--lock-object-name。 请使用--leader-elect-resource-namespace和--leader-elect-resource-name或ComponentConfig来配置这些参数。（ --lock-object-namespace用来定义锁对象的命名空间，--lock-object-name用来定义锁对象的名称）
- 在Kubernetes 1.28版本，KMSv1已弃用，以后只会接收安全更新。请改用KMSv2。在未来版本中，设置--feature-gates=KMSv1=true以使用已弃用的KMSv1功能。
- 在Kubernetes 1.28版本，移除了如下特性门禁：DelegateFSGroupToCSIDriver、DevicePlugins、KubeletCredentialProviders、MixedProtocolLBService、ServiceInternalTrafficPolicy、ServiceIPStaticSubrange、EndpointSliceTerminatingCondition。

参考链接

关于Kubernetes 1.28与其他版本的性能对比和功能演进的更多信息，请参考：**Kubernetes v1.28 Release Notes**

4.1.2.3 Kubernetes 1.27 版本说明

云容器引擎（CCE）严格遵循社区一致性认证，现已支持创建Kubernetes 1.27集群。本文介绍Kubernetes 1.27版本的变更说明。

索引

主要特性

- SeccompDefault特性已进入稳定阶段

  如需使用SeccompDefault特性，您需要为每个节点的kubelet启用--seccomp-default**命令行标志**。如果启用该特性，kubelet将为所有工作负载默认使用RuntimeDefault seccomp配置文件，该配置文件由容器运行时定义，而不是使用Unconfined（禁用seccomp）模式。

- Job可变调度指令

  该特性在Kubernetes 1.22版本中引入，当前已进入稳定阶段。在大多数情况下，并行作业Pod希望在一定的约束下运行，例如希望所有Pod在同一可用区。该特性允许在Job开始前修改调度指令。您可以使用suspend字段挂起Job，在Job挂起阶段，Pod模板中的调度部分（例如节点选择器、节点亲和性、反亲和性、容忍度）允许修改。详情请参见**可变调度指令**。

- Downward API HugePages已进入稳定阶段

  在Kubernetes 1.20版本中，**Downward API**引入了*requests.hugepages-<pagesize>*和*limits.hugepages-<pagesize>*，HugePage可以和其他资源一样设置资源配额。

- Pod调度就绪态进入Beta阶段

  Pod创建后，Kubernetes调度程序会负责选择合适的节点运行pending状态的Pod。在实际使用时，一些Pod可能会由于资源不足长时间处于pending状态。这些Pod可能会影响集群中的其他组件运行（如Cluster Autoscaler）。通过指定/删除Pod的.spec.schedulingGates，您可以控制Pod何时准备好进行调度。详情请参见**Pod调度就绪态**。

- 通过Kubernetes API访问节点日志

  此功能当前处于Alpha阶段。集群管理员可以直接查询节点上的服务日志，可以帮助调试节点上运行的服务问题。如需使用此功能，请确保在该节点上启用了NodeLogQuery**特性门控**，并且kubelet配置选项enableSystemLogHandler和enableSystemLogQuery都设置为true。

- ReadWriteOncePod访问模式进入Beta阶段

  在Kubernetes 1.22版本中，PV和PVC提供了一种新的访问模式ReadWriteOncePod，该功能当前进入Beta阶段。卷可以被单个Pod以读写方式挂载。如果您想确保整个集群中只有一个Pod可以读取或写入该PVC，请使用ReadWriteOncePod访问模式，详情请参见**访问模式**。

- Pod拓扑分布约束中matchLabelKeys字段进入Beta阶段

  matchLabelKeys是一个Pod标签键的列表，用于选择需要计算分布方式的Pod集合。使用matchLabelKeys字段，您无需在变更Pod修订版本时更新pod.spec。控制器或Operator只需要将不同修订版的标签键设为不同的值。调度器将根据matchLabelKeys自动确定取值。详情请参见**Pod拓扑分布约束**。

- 快速标记SELinux卷标签功能进入Beta阶段

  默认情况下，容器运行时递归地将SELinux标签赋予所有Pod卷上的所有文件。 为了加快该过程，Kubernetes使用挂载可选项*-o context=<label>*可以立即改变卷的SELinux标签。详情请参见**快速标记SELinux卷标签**。

- VolumeManager重构进入Beta阶段

  重构的VolumeManager后，如果启用NewVolumeManagerReconstruction**特性门控**，将会在kubelet启动期间使用更有效的方式来获取已挂载卷。

- 服务器端字段校验和OpenAPI V3已进入稳定阶段

  Kubernetes 1.23中添加了对OpenAPI v3的支持，1.24版本中已进入Beta阶段，1.27已进入稳定阶段。

- 控制StatefulSet启动序号

  Kubernetes 1.26为StatefulSet引入了一个新的Alpha级别特性，可以控制Pod副本的序号。 从Kubernetes 1.27开始，此特性进入Beta阶段，序数可以从任意非负数开始。详情请参见**Kubernetes 1.27: StatefulSet启动序号简化了迁移**。

- HorizontalPodAutoscaler ContainerResource类型指标进入Beta阶段

  Kubernetes 1.20在HorizontalPodAutoscaler (HPA) 中引入了**ContainerResource类型指标**。在Kubernetes 1.27中，此特性进阶至Beta，相应的特性门控 (HPAContainerMetrics) 默认被启用。

- StatefulSet PVC自动删除进入Beta阶段

  Kubernetes v1.27提供一种新的策略机制，用于控制StatefulSets的PersistentVolumeClaims（PVCs）的生命周期。这种新的PVC保留策略允许用户指定当删除StatefulSet或者缩减StatefulSet中的副本时，是自动删除还是保留从StatefulSet规约模板生成的PVC。详情请参见**PersistentVolumeClaim保留**。

- 磁盘卷组快照

  磁盘卷组快照在Kubernetes 1.27中作为Alpha特性被引入。此特性允许用户对多个卷进行快照，以保证在发生故障时数据的一致性。 它使用标签选择器来将多个

PersistentVolumeClaims分组以进行快照。 这个新特性仅支持CSI卷驱动器。详情请参见**Kubernetes 1.27：介绍用于磁盘卷组快照的新API**。

- kubectl apply裁剪更安全、更高效

  在Kubernetes 1.5版本中，kubectl apply引入了--prune标志来删除不再需要的资源，允许kubectl apply自动清理从当前配置中删除的资源。然而，现有的--prune实现存在设计缺陷，会降低性能并导致意外行为。Kubernetes 1.27中，kubectl apply提供基于ApplySet的剪裁方式，当前处于Alpha阶段，详情请参见**使用配置文件对Kubernetes对象进行声明式管理**。

- 为NodePort Service分配端口时避免冲突

  在Kubernetes 1.27中，您可以启用新的**特性门控** ServiceNodePortStaticSubrange，为NodePort Service使用不同的端口分配策略，减少冲突的风险。当前该特性处于Alpha阶段。

- 原地调整Pod资源

  在Kubernetes 1.27中，允许用户调整分配给Pod的CPU和内存资源大小，而无需重新启动容器。当前该特性处于Alpha阶段，详情请参见**纵向弹性伸缩**。

- 加快Pod启动

  在Kubernetes 1.27中进行了一系列的参数调整，以提高Pod的启动速度，例如并行镜像拉取、提高Kubelet默认API每秒查询限值等。详情请参见**Kubernetes 1.27：关于加快Pod启动的进展**。

- KMS V2进入Beta阶段

  Kubernetes中的密钥管理KMS v2 API进入Beta阶段，对KMS加密提供程序的性能进行了重大改进。详情请参见**使用KMS驱动进行数据加密**。

弃用和移除

- 在Kubernetes 1.27版本，针对卷扩展GA特性的以下特性门禁将被移除，且不得再在--feature-gates标志中引用。（**ExpandCSIVolumes，ExpandInUsePersistentVolumes，ExpandPersistentVolumes**）
- 在Kubernetes 1.27版本，移除--master-service-namespace 命令行参数。该参数支持指定在何处创建名为kubernetes的Service来表示API服务器。自v1.26版本已被弃用，1.27版本正式移除。
- 在Kubernetes 1.27版本，移除ControllerManagerLeaderMigration特性门禁。**Leader Migration**提供了一种机制，让HA集群在升级多副本的控制平面时通过在kube-controller-manager和cloud-controller-manager这两个组件之间共享的资源锁，安全地迁移“特定于云平台”的控制器。特性自v1.24正式发布，被无条件启用， 在v1.27版本中此特性门禁选项将被移除。
- 在Kubernetes 1.27版本，移除--enable-taint-manager命令行参数。该参数支持的特性基于污点的驱逐已被默认启用，且在标志被移除时也将继续被隐式启用。
- 在Kubernetes 1.27版本，移除--pod-eviction-timeout 命令行参数。弃用的命令行参数--pod-eviction-timeout将被从kube-controller-manager中移除。
- 在Kubernetes 1.27版本，移除CSI Migration特性门禁。**CSI migration**程序允许从树内卷插件移动到树外CSI驱动程序。CSI迁移自Kubernetes v1.16起正式发布，关联的CSIMigration特性门禁将在v1.27中被移除。
- 在Kubernetes 1.27版本，移除CSIInlineVolume特性门禁。**CSI Ephemeral Volume**特性允许在Pod规约中直接指定CSI卷作为临时使用场景。这些CSI卷可用于使用挂载的卷直接在Pod内注入任意状态，例如配置、Secret、身份、变量或类似信息。 此特性在v1.25中进阶至正式发布。因此，此特性门禁CSIInlineVolume将在v1.27版本中移除。

- 在Kubernetes 1.27版本，移除EphemeralContainers特性门禁。对于Kubernetes v1.27，临时容器的API支持被无条件启用；EphemeralContainers特性门禁将被移除。
- 在Kubernetes 1.27版本，移除LocalStorageCapacityIsolation特性门禁。**Local Ephemeral Storage Capacity Isolation**特性在 v1.25 中进阶至正式发布。此特性支持emptyDir卷这类Pod之间本地临时存储的容量隔离，因此可以硬性限制Pod对共享资源的消耗。如果本地临时存储的消耗超过了配置的限制，kubelet将驱逐Pod。特性门禁LocalStorageCapacityIsolation将在v1.27版本中被移除。
- 在Kubernetes 1.27版本，移除NetworkPolicyEndPort特性门禁。Kubernetes v1.25版本将NetworkPolicy中的endPort进阶至正式发布。支持endPort字段的NetworkPolicy提供程序可用于指定一系列端口以应用NetworkPolicy。
- 在Kubernetes 1.27版本，移除StatefulSetMinReadySeconds特性门禁。对于作为StatefulSet一部分的Pod，只有当Pod至少在**minReadySeconds**中指定的持续期内可用（并通过检查）时，Kubernetes才会将此Pod标记为只读。 该特性在Kubernetes v1.25中正式发布，StatefulSetMinReadySeconds特性门禁将锁定为true，并在v1.27版本中被移除。
- 在Kubernetes 1.27版本，移除IdentifyPodOS特性门禁。启用该特性门禁，您可以为Pod指定操作系统，此项特性支持自v1.25版本进入稳定。IdentifyPodOS特性门禁将在Kubernetes v1.27中被移除。
- 在Kubernetes 1.27版本，移除DaemonSetUpdateSurge特性门禁。Kubernetes v1.25版本还稳定了对DaemonSet Pod的浪涌支持，其实现是为了最大限度地减少部署期间DaemonSet的停机时间。DaemonSetUpdateSurge特性门禁将在Kubernetes v1.27中被移除。
- 在Kubernetes 1.27版本，移除--container-runtime 命令行参数。kubelet 接受一个已弃用的命令行参数--container-runtime， 并且在移除dockershim代码后，唯一有效的值将是remote。 Kubernetes v1.27将移除该参数，该参数自v1.24版本以来已被弃用。

参考链接

关于Kubernetes 1.27与其他版本的性能对比和功能演进的更多信息，请参考：**Kubernetes v1.27 Release Notes**

4.1.3 Autopilot 集群补丁版本发布记录

索引

v1.31 版本（公测）

表 4-1 v1.31 补丁版本发布说明

Autopilot集群补丁版本号	Kubernetes社区版本	特性更新	优化增强	安全漏洞修复
v1.31.1-r0	v1.31.1	CCE Autopilot支持创建1.31集群版本，有关更多信息请参见**Kubernetes 1.31版本说明**。	-	修复部分安全问题。

v1.28 版本

表 4-2 v1.28 补丁版本发布说明

Autopilot集群补丁版本号	Kubernetes社区版本	特性更新	优化增强	安全漏洞修复
v1.28.7-r0	**v1.28.3**	• 支持命名空间/工作负载绑定子网及安全组。 • 支持在SFS Turbo文件系统中创建子目录。	-	修复部分安全问题。
v1.28.6-r0	**v1.28.3**	• 支持工作负载实例挂载EVS存储。 • 支持命名空间/工作负载绑定子网及安全组。 • 支持自定义磁盘空间。	• 增强集群运维监控能力。 • 持续优化Pod启动时间。 • 优化autopilot大规模集群性能。	修复部分安全问题。
v1.28.5-r0	**v1.28.3**	• 支持创建工作负载时配置APM探针。 • 支持使用内网IP访问kube-apiserver。	-	修复部分安全问题。
v1.28.4-r0	**v1.28.3**	• 支持使用网络、磁盘等自定义指标创建弹性伸缩策略。 • 支持公网访问kube-apiserver。	使用YAML创建应用时自动忽略Autopilot不支持且不影响业务功能的配置参数。	修复部分安全问题。
v1.28.3-r0	**v1.28.3**	• Everest存储插件后台托管。 • 支持使用OBS存储卷。	-	修复部分安全问题。

Autopilot集群补丁版本号	Kubernetes社区版本	特性更新	优化增强	安全漏洞修复
v1.28.2-r0	v1.28.3	• 支持CronHPA定时扩缩容策略。 • 支持实例配置Security Context。	-	修复部分安全问题。
v1.28.1-r10	v1.28.3	CCE Autopilot支持创建1.28集群版本，有关更多信息请参见Kubernetes 1.28版本说明。	-	-

v1.27 版本

表 4-3 v1.27 补丁版本发布说明

Autopilot集群补丁版本号	Kubernetes社区版本	特性更新	优化增强	安全漏洞修复
v1.27.9-r0	v1.27.4	• 支持命名空间/工作负载绑定子网及安全组。 • 支持在SFS Turbo文件系统中创建子目录。	-	修复部分安全问题。
v1.27.8-r0	v1.27.4	• 支持工作负载实例挂载EVS存储。 • 支持命名空间/工作负载绑定子网及安全组。 • 支持自定义磁盘空间。	• 增强集群运维监控能力。 • 持续优化Pod启动时间。 • 优化autopilot大规模集群性能。	修复部分安全问题。
v1.27.7-r0	v1.27.4	• 支持创建工作负载时配置APM探针。 • 支持使用内网IP访问kube-apiserver。	-	修复部分安全问题。
v1.27.6-r0	v1.27.4	• 支持使用网络、磁盘等自定义指标创建弹性伸缩策略。 • 支持公网访问kube-apiserver。	使用YAML创建应用时自动忽略Autopilot不支持且不影响业务功能的配置参数。	修复部分安全问题。

Autopilot集群补丁版本号	Kubernetes社区版本	特性更新	优化增强	安全漏洞修复
v1.27.5-r0	v1.27.4	• Everest存储插件后台托管。 • 支持使用OBS存储卷。	-	修复部分安全问题。
v1.27.4-r0	v1.27.4	• 支持CronHPA定时扩缩容策略。 • 支持实例配置Security Context。	-	修复部分安全问题。
v1.27.3-r30	v1.27.4	-	支持一键配置监控告警。	修复部分安全问题。
v1.27.3-r20	v1.27.4	• 支持安装NGINX Ingress控制器插件。 • 支持安装云原生监控插件以及云原生日志插件，实现对应用指标的监控以及应用日志采集。 • 支持应用模板市场。 • 支持自定义资源(CRD)的使用。 • 支持对接Cloudshell。	优化集群创建时默认创建NAT网关以便于应用访问公网。	修复部分安全问题。
v1.27.3-r10	v1.27.4	CCE Autopilot支持创建1.27集群版本，有关更多信息请参见**Kubernetes 1.27版本说明**。	-	-

4.2 插件版本发布记录

4.2.1 CoreDNS 域名解析插件版本发布记录

表 4-4 CoreDNS 域名解析插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.28.10	• v1.31 • v1.28 • v1.27	适配CCE Autopilot v1.31集群	1.10.1

插件版本	支持的集群版本	更新特性	社区版本
1.28.9	• v1.28 • v1.27	修复部分问题	1.10.1
1.28.8	• v1.28 • v1.27	插件依赖例行升级	1.10.1
1.28.7	• v1.28 • v1.27	插件依赖例行升级	1.10.1
1.28.6	• v1.28 • v1.27	修复部分问题	1.10.1

4.2.2 NGINX Ingress 控制器插件版本发布记录

表 4-5 NGINX Ingress 控制器插件 2.4.x 版本发布记录

插件版本	支持的集群版本	更新特性	社区版本
2.4.14	• v1.31 • v1.28 • v1.27	• 适配CCE Autopilot v1.31集群 • 解决CVE-2024-7646漏洞	1.11.2
2.4.13	• v1.28 • v1.27	基于社区版本v1.9.6	1.9.6
2.4.12	• v1.28 • v1.27	修复部分问题	1.9.3
2.4.11	• v1.28 • v1.27	修复部分问题	1.9.3
2.4.10	• v1.28 • v1.27	修复部分问题	1.9.3

4.2.3 Kubernetes Metrics Server 插件版本发布记录

表 4-6 Kubernetes Metrics Server 插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.3.42	• v1.31 • v1.28 • v1.27	适配CCE Autopilot v1.31集群	0.6.2

插件版本	支持的集群版本	更新特性	社区版本
1.3.41	• v1.28 • v1.27	修复部分问题	**0.6.2**
1.3.40	• v1.28 • v1.27	修复部分问题	**0.6.2**
1.3.39	• v1.28 • v1.27	修复部分问题	**0.6.2**
1.3.38	• v1.28 • v1.27	• 支持插件实例AZ反亲和配置 • 默认污点容忍时长修改为60s • 插件挂载节点时区	**0.6.2**

4.2.4 CCE 容器弹性引擎插件版本发布记录

表 4-7 CCE 容器弹性引擎插件版本记录

插件版本	支持的集群版本	更新特性
1.3.48	• v1.31 • v1.28 • v1.27	适配CCE Autopilot v1.31集群
1.3.47	• v1.28 • v1.27	修复部分问题
1.3.46	• v1.28 • v1.27	插件依赖例行升级
1.3.45	• v1.28 • v1.27	修复部分问题
1.3.44	• v1.28 • v1.27	支持CronHPA策略

4.2.5 云原生监控插件版本发布记录

表 4-8 云原生监控插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
3.12.0	• v1.31 • v1.28 • v1.27	适配CCE Autopilot v1.31集群	2.53.2
3.9.6	• v1.28 • v1.27	升级Prometheus版本，移除node-exporter组件	2.53.2
3.9.5	• v1.28 • v1.27	支持自定义指标	2.37.8
3.9.3	• v1.28 • v1.27	修复部分问题	2.37.8

4.2.6 云原生日志采集插件版本发布记录

表 4-9 云原生日志采集插件版本记录

插件版本	支持的集群版本	更新特性
1.7.0	• v1.31 • v1.28 • v1.27	适配CCE Autopilot v1.31集群
1.4.5	• v1.28 • v1.27	资源配置优化
1.4.4	• v1.28 • v1.27	修复部分问题
1.4.3	• v1.28 • v1.27	修复部分问题
1.2.25	• v1.28 • v1.27	修复部分问题