

云容器引擎

服务公告

文档版本 01
发布日期 2024-05-30



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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	1
2 产品变更公告	3
2.1 集群网络、存储功能可靠性加固说明	3
2.2 关于 CCE 集群 Docker 支持策略公告	4
2.3 ServiceAccount Token 安全性提升说明	4
2.4 Helm V2 升级 Helm V3 公告	4
2.5 CCE 集群 IPVS 转发模式下 conn_reuse_mode 问题说明	4
2.6 Everest 插件优化密钥认证功能公告	5
3 集群版本公告	6
3.1 1.23 版本集群停止维护公告	6
3.2 1.21 版本集群停止维护公告	6
3.3 1.19 版本集群停止维护公告	6
3.4 1.17 版本集群停止维护公告	6
3.5 1.15 版本集群停止维护公告	7
3.6 1.13 版本集群停止维护公告	7
3.7 CCE 不再支持 1.13 及之前版本集群的创建公告	7
3.8 Kubernetes 1.9 的集群版本升级公告	7
4 漏洞公告	8
4.1 漏洞修复策略	8
4.2 Fluent Bit 内存崩溃漏洞公告 (CVE-2024-4323)	8
4.3 runc systemd 属性注入漏洞公告 (CVE-2024-3154)	10
4.4 runc 漏洞 (CVE-2024-21626) 对 CCE 服务的影响说明	11
4.5 Kubernetes 安全漏洞公告 (CVE-2022-3172)	13
4.6 Linux Kernel openvswitch 模块权限提升漏洞预警 (CVE-2022-2639)	14
4.7 nginx-ingress 插件安全漏洞预警公告 (CVE-2021-25748)	15
4.8 nginx-ingress 插件安全漏洞预警公告 (CVE-2021-25745, CVE-2021-25746)	16
4.9 containerd 容器进程权限提升漏洞公告 (CVE-2022-24769)	17
4.10 CRI-O 容器运行时引擎任意代码执行漏洞 (CVE-2022-0811)	18
4.11 linux 内核导致的容器逃逸漏洞公告 (CVE-2022-0492)	18
4.12 containerd 镜像 Volume 非安全处理漏洞公告 (CVE-2022-23648)	19
4.13 Linux 内核整数溢出漏洞 (CVE-2022-0185)	20
4.14 Linux Polkit 权限提升漏洞预警 (CVE-2021-4034)	21

4.15 Kubernetes subpath 符号链接交换安全漏洞 (CVE-2021- 25741)	22
4.16 runc 符号链接挂载与容器逃逸漏洞预警公告 (CVE-2021-30465)	25
4.17 Docker 资源管理错误漏洞公告 (CVE-2021-21285)	26
4.18 NVIDIA GPU 驱动漏洞公告 (CVE-2021-1056)	27
4.19 Sudo 缓冲区错误漏洞公告 (CVE-2021-3156)	29
4.20 Kubernetes 安全漏洞公告 (CVE-2020-8554)	30
4.21 Apache containerd 安全漏洞公告 (CVE-2020-15257)	31
4.22 Docker Engine 输入验证错误漏洞公告 (CVE-2020-13401)	31
4.23 Kubernetes kube-apiserver 输入验证错误漏洞公告 (CVE-2020-8559)	32
4.24 Kubernetes kubelet 资源管理错误漏洞公告 (CVE-2020-8557)	33
4.25 Kubernetes kubelet 和 kube-proxy 授权问题漏洞公告 (CVE-2020-8558)	34
4.26 修复 Kubernetes HTTP/2 漏洞公告	36
4.27 修复 Linux 内核 SACK 漏洞公告	37
4.28 修复 Docker 操作系统命令注入漏洞公告 (CVE-2019-5736)	39
4.29 全面修复 Kubernetes 权限许可和访问控制漏洞公告 (CVE-2018-1002105)	40
4.30 修复 Kubernetes Dashboard 安全漏洞公告 (CVE-2018-18264)	41
5 产品发布记录	43
5.1 集群版本发布记录	43
5.1.1 Kubernetes 版本策略	43
5.1.2 Kubernetes 版本发布记录	45
5.1.2.1 Kubernetes 1.29 版本说明	45
5.1.2.2 Kubernetes 1.28 版本说明	49
5.1.2.3 Kubernetes 1.27 版本说明	54
5.1.2.4 Kubernetes 1.25 版本说明	59
5.1.2.5 Kubernetes 1.23 版本说明	63
5.1.2.6 (停止维护) Kubernetes 1.21 版本说明	64
5.1.2.7 (停止维护) Kubernetes 1.19 版本说明	65
5.1.2.8 (停止维护) Kubernetes 1.17 版本说明	67
5.1.2.9 (停止维护) Kubernetes 1.15 版本说明	68
5.1.2.10 (停止维护) Kubernetes 1.13 版本说明	69
5.1.2.11 (停止维护) Kubernetes 1.11 版本说明	70
5.1.2.12 (停止维护) Kubernetes 1.9 及之前版本说明	71
5.1.3 补丁版本发布记录	75
5.2 操作系统镜像发布记录	96
5.2.1 操作系统版本支持机制	96
5.2.2 操作系统镜像版本说明	104
5.3 插件版本发布记录	108
5.3.1 CoreDNS 域名解析插件版本发布记录	108
5.3.2 CCE 容器存储插件 (Everest) 版本发布记录	110
5.3.3 CCE 节点故障检测插件版本发布记录	114
5.3.4 Kubernetes Dashboard 插件版本发布记录	118
5.3.5 CCE 集群弹性引擎版本发布记录	119

5.3.6 NGINX Ingress 控制器插件版本发布记录.....	126
5.3.7 Kubernetes Metrics Server 插件版本发布记录.....	129
5.3.8 CCE 容器弹性引擎插件版本发布记录.....	131
5.3.9 CCE 突发弹性引擎（对接 CCI）插件版本发布记录.....	133
5.3.10 CCE AI 套件（NVIDIA GPU）版本发布记录.....	134
5.3.11 CCE AI 套件（Ascend NPU）版本发布记录.....	136
5.3.12 Volcano 调度器版本发布记录.....	139
5.3.13 CCE 密钥管理（对接 DEW）插件版本发布记录.....	142
5.3.14 CCE 容器网络扩展指标插件版本发布记录.....	143
5.3.15 节点本地域名解析加速插件版本发布记录.....	144
5.3.16 云原生监控插件版本发布记录.....	146
5.3.17 云原生日志采集插件版本发布记录.....	147
5.3.18 Grafana 插件版本发布记录.....	148
5.3.19 CCE 集群备份恢复插件版本发布记录（停止维护）.....	149
5.3.20 Kubernetes Web 终端版本发布记录（停止维护）.....	149
5.3.21 Prometheus 插件版本发布记录（停止维护）.....	150

1 最新公告

以下为CCE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	Fluent Bit内存崩溃漏洞公告 (CVE-2024-4323)	漏洞公告	2024/05/23
2	runc systemd属性注入漏洞公告 (CVE-2024-3154)	漏洞公告	2024/04/29
3	集群网络、存储功能可靠性加固说明	产品变更公告	2024/04/26
4	1.23版本集群停止维护公告	集群版本公告	2024/04/25
5	关于CCE集群Docker支持策略公告	产品变更公告	2024/02/19
6	runc漏洞 (CVE-2024-21626) 对CCE服务的影响说明	漏洞公告	2024/02/01
7	1.21版本集群停止维护公告	集群版本公告	2024/01/22
8	1.19版本集群停止维护公告	集群版本公告	2023/08/02
9	1.17版本集群停止维护公告	集群版本公告	2022/11/29
10	ServiceAccount Token安全性提升说明	产品变更公告	2022/11/24
11	Kubernetes安全漏洞公告 (CVE-2022-3172)	漏洞公告	2022/09/23
12	Linux Kernel openvswitch 模块权限提升漏洞预警 (CVE-2022-2639)	漏洞公告	2022/09/16
13	Helm V2 升级Helm V3 公告	产品变更公告	2022/08/30
14	1.15版本集群停止维护公告	集群版本公告	2022/06/22
15	nginx-ingress插件安全漏洞预警公告 (CVE-2021-25748)	漏洞公告	2022/06/14

序号	公告标题	公告类型	发布时间
16	nginx-ingress插件安全漏洞预警公告 (CVE-2021-25745, CVE-2021-25746)	漏洞公告	2022/04/29
17	containerd容器进程权限提升漏洞公告 (CVE-2022-24769)	漏洞公告	2022/03/25
18	CRI-O容器运行时引擎任意代码执行漏洞 (CVE-2022-0811)	漏洞公告	2022/03/23
19	1.13版本集群停止维护公告	集群版本公告	2022/03/11
20	containerd镜像Volume非安全处理漏洞公告 (CVE-2022-23648)	漏洞公告	2022/03/03
21	linux内核导致的容器逃逸漏洞公告 (CVE-2022-0492)	漏洞公告	2022/02/10

更多历史公告请详见[产品变更公告](#)、[集群版本公告](#)及[漏洞公告](#)。

2 产品变更公告

2.1 集群网络、存储功能可靠性加固说明

发布时间：2024/04/26

当IAM服务发生区域性故障时，存在低概率触发鉴权异常，从而影响集群内工作负载存储卷挂载、负载均衡对接等功能。最新的集群版本针对该类故障场景进行了优化和加固，为确保您的业务稳定运行，建议您尽快将账号下的集群升级至目标版本。

触发条件

同时满足以下条件：

1. 集群版本范围：
 - 已EOS版本：v1.19及以下所有版本
 - 1.21版本（于2024/04/30 00:00（北京时间）正式停止维护）：v1.21.1-r0 - v1.21.11-r40
 - 1.23版本：v1.23.1-r0 - v1.23.10-r20
 - 1.25版本：v1.25.1-r0 - v1.25.5-r20
 - 1.27版本：v1.27.1-r0 - v1.27.2-r20
2. IAM服务出现区域性故障，且故障期间集群中的IAM临时访问密钥发生过期。
3. 集群内工作负载新建或更新等涉及Pod启动，且需要对接存储卷挂载、负载均衡等功能。

修复方案

请您关注补丁版本发布记录，及时将集群升级至目标版本。已EOS集群版本请升级到在维版本进行修复。

目标集群版本：

- 1.21版本（于2024/04/30 00:00（北京时间）正式停止维护）：v1.21.12-r0及以上
- 1.23版本：v1.23.11-r0及以上
- 1.25版本：v1.25.6-r0及以上

- 1.27版本: v1.27.3-r0及以上
- 1.28版本: v1.28.1.0及以上

2.2 关于 CCE 集群 Docker 支持策略公告

发布时间: 2024/02/19

Kubernetes社区已在v1.24版本移除dockershim, 默认不再支持Docker运行时。考虑到当前仍然有部分用户使用Docker, CCE将继续支持创建Docker节点。

建议您在新建节点时选择更加轻量、安全的Containerd运行时, 同时将存量节点的容器运行时逐步迁移至Containerd, 具体操作请参见[将节点容器引擎从Docker迁移到Containerd](#)。

Containerd和Docker的对比请参见[容器引擎Containerd和Docker](#)。

2.3 ServiceAccount Token 安全性提升说明

发布时间: 2022/11/24

Kubernetes 1.21及以上版本的集群中, Pod将不再自动挂载永久Token, 默认使用[TokenRequest](#) API获得Token, 并使用投射卷 (Projected Volume) 挂载到Pod中。

使用这种方法获得的Token具有固定的生命周期 (默认有效期为1小时), 在到达有效期之前, Kubelet会刷新该Token, 保证Pod始终拥有有效的Token, Kubernetes 1.21及以上版本的集群中会默认开启该特性。如果用户使用版本过低的K8s客户端 (Client), 由于低版本Client并不具备证书轮转能力, 会存在证书轮转失效的风险。

详情请参见[ServiceAccount Token安全性提升说明](#)。

2.4 Helm V2 升级 Helm V3 公告

发布时间: 2022/08/30

因控制台“模板管理”功能所依赖的开源软件Helm已从 V2 演进至 V3 版本, 即日起平台会自动将集群中 Helm V2 格式实例转换为 Helm V3 格式。部分 Helm V2 功能在 Helm V3 上有了更好的解决方案, 但可能存在与原有方式不兼容的情况, 需要您根据[Helm V3 与 Helm V2 的差异及适配方案](#)进行排查并做相应的适配验证。

如您短期内切换到 Helm V3 存在困难, 可通过后台 Helm 客户端方式继续管理并部署 Helm V2 实例, 操作方法请参见[通过 Helm V2 客户端部署应用](#)。为了更好地维护您的权益以及更好地获取运维支撑, 请您在2022年12月30日前彻底切换至 Helm V3 管理方式。

2.5 CCE 集群 IPVS 转发模式下 conn_reuse_mode 问题说明

发布时间: 2022/01/27

CCE集群在IPVS模式下, 通过Service方式访问集群内部服务, 偶现1秒延时的情况, 引起该问题的主要原因为社区IPVS连接复用Bug。

详情请参见[CCE集群IPVS转发模式下conn_reuse_mode问题说明](#)。

2.6 Everest 插件优化密钥认证功能公告

发布时间：2021/02/02

Everest插件在1.2.0版本优化了使用OBS存储时的密钥认证功能，请在Everest插件升级完成后（从低于1.2.0的版本升级到1.2.0及以上版本），重启集群中使用OBS的全部工作负载，否则工作负载使用OBS存储能力将受影响！

3 集群版本公告

3.1 1.23 版本集群停止维护公告

发布时间：2024/04/25

华为云CCE集群1.23版本即将于2024/09/30 00:00（北京时间）正式停止维护，届时针对CCE集群1.23以及之前的版本，华为云将不再支持新集群创建。若您账号下存在1.23及之前的集群版本，为了保证您的服务权益，建议尽快升级到最新的商用版本。关于如何升级集群，请参见CCE[集群升级](#)指导。关于CCE集群的版本机制，请参见[Kubernetes版本策略](#)。

3.2 1.21 版本集群停止维护公告

发布时间：2024/01/22

华为云CCE集群1.21版本即将于2024/04/30 00:00（北京时间）正式停止维护，届时针对CCE集群1.21以及之前的版本，华为云将不再支持新集群创建。若您账号下存在1.21及之前的集群版本，为了保证您的服务权益，建议尽快升级到最新的商用版本。关于如何升级集群，请参见CCE[集群升级](#)指导。关于CCE集群的版本机制，请参见[Kubernetes版本策略](#)。

3.3 1.19 版本集群停止维护公告

发布时间：2023/08/02

华为云CCE集群1.19版本即将于2023/09/30 00:00（北京时间）正式停止维护，届时针对CCE集群1.19以及之前的版本，华为云将不再支持新集群创建。若您账号下存在1.19及之前的集群版本，为了保证您的服务权益，建议尽快升级到最新的商用版本。关于如何升级集群，请参见CCE[集群升级](#)指导。关于CCE集群的版本机制，请参见[Kubernetes版本策略](#)。

3.4 1.17 版本集群停止维护公告

发布时间：2022/11/29

根据CCE发布的[Kubernetes版本策略](#)中的版本策略，计划从**2023年1月31日**起，CCE将对1.17版本集群停止维护。在此之后，您仍可以使用您的1.17版本集群，但CCE将不再提供对该版本的技术支持，包含支持新的功能、社区bugfix回合、漏洞修复、升级等。建议您在版本停止维护前及时将集群升级到最新版本，升级操作请参见[集群升级](#)。

3.5 1.15 版本集群停止维护公告

发布时间：2022/06/22

根据CCE发布的[Kubernetes版本策略](#)中的版本策略，计划从**2022年9月30日**起，CCE将对1.15版本集群停止维护。建议您将集群升级到最新版本，升级操作请参见[集群升级](#)。

3.6 1.13 版本集群停止维护公告

发布时间：2022/03/11

根据CCE发布的[Kubernetes版本策略](#)中的版本策略，从**2022年3月11日**起，CCE将对1.13版本集群停止维护。建议您将集群升级到最新版本，升级操作请参见[集群升级](#)。

3.7 CCE 不再支持 1.13 及之前版本集群的创建公告

发布时间：2020/12/08

根据CCE发布的[Kubernetes版本策略](#)中的版本策略，从**2021年3月1日**之后，CCE将不再支持1.13及之前版本集群的创建及维护。

3.8 Kubernetes 1.9 的集群版本升级公告

发布时间：2020/12/07

根据CCE发布的[Kubernetes版本策略](#)中的版本策略，CCE将在近期停止Kubernetes 1.9的集群版本的维护，为了能够更好地方便您使用云容器引擎服务，确保您使用稳定又可靠的Kubernetes版本，如果您仍在使用1.9.7或1.9.10版本集群，请尽快升级到较新版本集群，CCE预计将在**2021年4月30日**后关闭对应升级通道，请您务必在此之前升级您的Kubernetes集群。

升级方法请参见[集群版本升级说明](#)。

4 漏洞公告

4.1 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，一般在一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不提供有关漏洞细节的其他信息。

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

最后，CCE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”）。

4.2 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 4-1 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

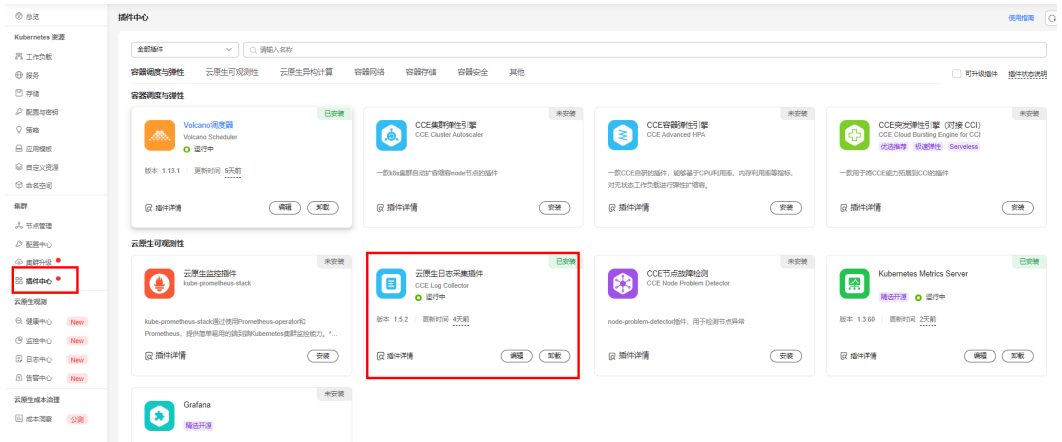
Fluent Bit 版本2.0.7 - 3.0.3中存在堆缓冲区溢出漏洞，该漏洞存在于Fluent Bit的嵌入式http服务器对跟踪请求的解析中，由于在解析/api/v1/traces 端点的传入请求时，在解析之前未正确验证input_name的数据类型，可通过在请求的“inputs”数组中传递非字符串值（如整数值），可能导致内存崩溃，成功利用该漏洞可能导致拒绝服务、信息泄露或远程代码执行。

CCE集群中安装了云原生日志采集插件，且版本为1.3.4-1.5.1时则涉及该漏洞。

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以及插件版本。

图 4-1 查看已安装插件版本



2. 若插件版本在1.3.2-1.5.1范围内，则涉及该漏洞。

漏洞消减方案

CCE将在云原生日志采集插件1.5.2版本中修复该漏洞，在修复前建议通过关闭指标上报接口消减该漏洞影响：

1. 节点上执行以下命令：

```
kubectl edit cm -n monitoring log-agent-fluent-bit-config-service
```
2. 将配置项中HTTP_Server On改为HTTP_Server Off，并保存。

```
service.conf: |-
  [SERVICE]
    Flush          1
    Daemon         Off
    Log_Level      warn
    Parsers_File   /fluent-bit/etc/parsers.conf
    plugins_file   /fluent-bit/etc/plugins/plugins.conf
    HTTP_Server    Off
    HTTP_Listen    ${POD_IP}
    HTTP_Port      2020
    scheduler.cap  180
    scheduler.base 2
```

3. 重启monitoring命名空间下的log-agent-log-operator组件。

4.3 runc systemd 属性注入漏洞公告 (CVE-2024-3154)

业界安全研究人员披露runc systemd属性注入漏洞 (CVE-024-3154)，攻击者可将恶意的systemd属性 (如: ExecStartPre、ExecStart、ExecReload) 注入Pod注解中，进而在宿主机中执行任意操作。

漏洞详情

表 4-2 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
代码执行	CVE-2024-3154	严重	2024-04-26

漏洞影响

攻击者利用runc的systemd cgroup特性进行攻击，可通过在Pod注解中注入恶意的systemd属性 (如: ExecStartPre、ExecStart、ExecReload)，进而在宿主机中执行任意操作。

CCE集群未使用runc的systemd cgroup特性，因此不受此漏洞影响。

判断方法

您可以在节点上执行命令查看容器引擎使用的cgroup。

- 容器引擎为containerd的节点，执行以下命令：

```
cricctl info |grep -i systemdCgroup
```

显示如下：

```
"systemdCgroup": false
```

- 容器引擎为docker的节点，执行以下命令：

```
docker info |grep "Cgroup"
```

显示如下：

```
Cgroup Driver: cgroupfs
```

表明容器引擎使用的cgroup系统为cgroupfs，并未使用systemd cgroup，不受此漏洞影响。

漏洞修复方案

华为云CCE集群未开启runc的systemd cgroup特性，不受runc漏洞CVE-2024-3154影响，请放心使用。

相关链接

runc systemd cgroup特性：<https://github.com/opencontainers/runc/blob/main/docs/systemd.md#auxiliary-properties>

4.4 runc 漏洞（CVE-2024-21626）对 CCE 服务的影响说明

漏洞详情

runc是一个基于OCI标准实现的一个轻量级容器运行工具，是Docker、Containerd、Kubernetes等容器软件的核心基础组件。近日，runc社区发布最新版本，修复了一处高危级别的容器逃逸漏洞（[CVE-2024-21626](#)）。由于内部文件描述符泄漏，攻击者可通过控制容器进程的工作目录，或命令路径，将其设置为文件描述符的父级目录下的路径，读写主机任意文件，实现容器逃逸。

详细信息请参见：[runc容器逃逸漏洞预警（CVE-2024-21626）](#)

漏洞利用条件

CCE服务的正常使用场景不受此漏洞影响。

仅当攻击者具备以下条件之一时，可利用该漏洞：

1. 攻击者具有集群工作负载的创建或更新权限。
2. 集群中工作负载的容器镜像来源不可信，攻击者拥有修改源镜像权限。

典型漏洞利用场景：

- 攻击者具有集群工作负载的创建或更新权限，创建工作负载时设置容器进程的WORKDIR为/proc/self/fd/<num>，以实现在容器运行后访问节点文件系统。
- 工作负载的容器镜像来源不可信，攻击者拥有修改源镜像权限，将镜像中WORKDIR设置为/proc/self/fd/<num>，以实现在容器运行后访问节点文件系统。

漏洞影响

满足上述漏洞利用条件时，容器进程可能逃逸到节点，导致节点信息泄露或执行恶意命令。

判断方法

集群版本范围为v1.21.1-r0 - v1.21.12-r2，v1.23.1-r0 - v1.23.11-r2，v1.25.1-r0 - v1.25.6-r2，v1.27.1-r0 - v1.27.3-r10，v1.28.1-r0 - v1.28.1-r10，同时集群中工作负载配置或容器镜像具备如下特征时，可能存在风险：

- 工作负载中容器进程的WORKDIR为 /proc/self/fd/<num>。

图 4-2 有安全风险的工作负载配置示例

```
spec:
  containers:
  - env:
    - name: PAAS_APP_NAME
      value: test-aatack-2
    - name: PAAS_NAMESPACE
      value: default
    image: nginx:latest
    imagePullPolicy: IfNotPresent
    name: container-1
    workingDir: /proc/self/fd/🗑️
```

- 工作负载的容器镜像中默认WORKDIR或启动命令包含 /proc/self/fd/<num>。
可通过以下命令查看容器镜像元数据：
 - docker运行时执行：**docker inspect <镜像ID>**
 - containerd运行时执行：**crictl inspecti <镜像ID>**

图 4-3 有安全风险的镜像配置示例

```
"ContainerConfig": {
  "Hostname": "9311f7e9fbf6",
  "Env": [
    "PATH=/usr/local/sbin:/usr/local/bin:/usr/sb
  ],
  "Cmd": [
    "/bin/sh",
    "-c",
    "#(nop) ",
    "ENTRYPOINT [\"/var/paas/start.sh\"]"
  ],
  "WorkingDir": "/proc/self/fd/🗑️",
  "Entrypoint": [
    ""
  ],
  "OnBuild": null,
  "Annotations": {
    "native.umask": "normal"
  }
}
```

漏洞修复方案

规避措施：

- 配置工作负载的WORKDIR为固定目录。
- 若未设置工作负载WORKDIR目录，需确保工作负载使用的容器镜像来源可信。

📖 说明

执行以上规避措施前请评估对业务的影响，并进行充分测试。

修复方案：

当前CCE团队已修复该漏洞，请您关注[补丁版本发布记录](#)，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：v1.21.12-r4、v1.23.11-r4、v1.25.6-r4、v1.27.3-r4、v1.28.1-r4及以上版本。

📖 说明

集群升级至漏洞修复版本后，新启动的容器不存在漏洞风险，对于已运行的容器需要进一步排查，详情请参见[判断方法](#)。

- 已运行的容器中，如果启动容器进程时设置WORKDIR为/proc/self/fd/<num>，仍存在风险，需要删除该配置后重新部署容器。
- 已运行的容器中，使用的镜像中WORKDIR设置为/proc/self/fd/<num>，仍存在风险，需要使用可信的镜像，重新部署容器。
- 已运行的容器中，容器WORKDIR未设置为/proc/self/fd/<num>，无风险。

4.5 Kubernetes 安全漏洞公告（CVE-2022-3172）

漏洞详情

Kubernetes社区在 kube-apiserver 中发现了一个安全问题，该问题允许聚合 API Server将客户端流量重定向到任意 URL，这可能导致客户端执行意外操作以及将客户端的 API 服务器凭据转发给第三方。

表 4-3 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
SSRF	CVE-2022-3172	中	2022-09-09

漏洞影响

CCE受影响的版本：

- kube-apiserver <= v1.23.10

符合上述范围的CCE集群，且配置了聚合API Server的均受影响，尤其是将CCE集群在逻辑多租场景下使用风险较高。

判断方法

对于1.23及以下版本的CCE集群、CCE Turbo集群，使用[web-terminal](#)或者配置[kubectl](#)连接集群，运行以下命令，确认是否运行聚合API Server：

```
kubectl get apiservices.apiregistration.k8s.io -o=jsonpath='{range .items[?(@.spec.service)]}{.metadata.name}{\n}{end}'
```

若返回值非空，说明存在聚合API Server。

漏洞修复方案

除了升级之外，当前没有直接可用的缓解措施。集群管理员应注意控制权限，防止非受信人员通过APIService接口部署和控制聚合API Server。

该漏洞已在v1.23.5-r0、v1.21.7-r0、v1.19.16-r4版本的CCE集群中修复。

相关链接

<https://github.com/kubernetes/kubernetes/issues/112513>

4.6 Linux Kernel openvswitch 模块权限提升漏洞预警 (CVE-2022-2639)

漏洞详情

业界披露了Linux Kernel openvswitch模块权限提升漏洞（CVE-2022-2639）的漏洞细节。由于 openvswitch模块中reserve_sfa_size()函数在使用过程中存在缺陷，导致本地经过身份认证的攻击者可以利用漏洞提升至root权限。目前漏洞poc已公开，风险较高。

表 4-4 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
权限提升	CVE-2022-2639	高	2022-09-01

漏洞影响

1. 采用容器隧道网络的CCE集群，节点OS镜像使用了EulerOS 2.8（ARM场景）或EulerOS 2.9。

2. 节点OS镜像使用了Ubuntu。

EulerOS 2.5 和CentOS 7.6的集群节点不受该漏洞影响。

漏洞修复方案

1. 容器内进程使用非root用户启动的进程可以通过为工作负载配置安全计算模式seccomp，建议配置RuntimeDefault模式或者禁用unshare等系统调用。具体配置方法可参考社区官方资料[使用 Seccomp 限制容器的系统调用](#)。

2. Ubuntu镜像自带openvswitch内核模块，可以通过将禁止加载openvswitch 内核模块来规避。操作如下：

```
echo "blacklist openvswitch" >>/etc/modprobe.d/blacklist.conf
```

然后重启节点，使上述设置生效。

相关链接

<https://github.com/torvalds/linux/commit/cefa91b2332d7009bc0be5d951d6cbbf349f90f8>

4.7 nginx-ingress 插件安全漏洞预警公告 (CVE-2021-25748)

漏洞详情

Kubernetes开源社区中披露了1个ingress-nginx漏洞，用户通过Ingress 对象的“spec.rules[].http.paths[].path”字段可以获取ingress-controller使用的credentials。这个credentials可以获取集群中所有namespace的secrets。该漏洞被收录为CVE-2021-25748。

表 4-5 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
权限提升	CVE-2021-25748	中	2022-6-10

漏洞影响

有权限可以创建/更新ingress 中`spec.rules[].http.paths[].path`字段的用户，可以使用换行符绕过对Ingress 对象的“spec.rules[].http.paths[].path”字段的处理，通过这种方式获取ingress-controller使用的credentials，进而可以获取集群中所有namespace的secrets。

判断方法

1.23及以下版本的CCE集群、CCE Turbo集群中：

1. 客户自行安装nginx-ingress的场景，判断nginx-ingress应用的镜像版本是否小于1.2.1
2. 使用CCE提供的nginx-ingress插件，判断插件版本号是否小于等于2.1.0

漏洞修复方案

1. 升级ingress-nginx版本至1.2.1；
2. 如果您正在运行 v1.2.0 (gcr.io/k8s-staging-ingress-nginx/controller-chroot) 中引入的“chrooted” ingress-nginx 控制器，则不会受到影响。

相关链接

1. CVE-2021-25748社区漏洞issue: <https://github.com/kubernetes/ingress-nginx/issues/8686>
2. 社区已经发布版本修复: <https://github.com/kubernetes/ingress-nginx/releases/tag/controller-v1.2.1>

4.8 nginx-ingress 插件安全漏洞预警公告 (CVE-2021-25745, CVE-2021-25746)

漏洞详情

Kubernetes开源社区中披露了2个nginx-ingress漏洞：

1. 漏洞CVE-2021-25745：用户有权限可以在创建/更新ingress时，利用‘spec.rules[].http.paths[].path’字段，获取到ingress-controller使用的凭证，这个凭证可以获取集群中所有命名空间的密钥。
2. 漏洞CVE-2021-25746：用户有权限可以在创建/更新ingress时，利用‘.metadata.annotations’字段，获取到ingress-controller使用的凭证，这个凭证可以获取集群中所有命名空间的密钥。

表 4-6 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
权限提升	CVE-2021-25745	中	2022-4-16
权限提升	CVE-2021-25746	中	2022-4-16

漏洞影响

该漏洞主要影响以逻辑多租的方式使用CCE集群并且普通用户拥有创建Ingress对象的场景。

判断方法

1.23及以下版本的CCE集群、CCE Turbo集群中：

1. 客户自行安装nginx-ingress的场景，判断nginx-ingress应用的镜像版本是否小于1.2.0
2. 使用CCE提供的nginx-ingress插件，判断插件版本号是否小于2.1.0

漏洞修复方案

1. 漏洞CVE-2021-25745消减措施：通过实施准入策略，将'networking.k8s.io/Ingress'中的'spec.rules[].http.paths[].path'限制在已知安全字符中（参考社区最新[规则](#)，或者采用[annotation-value-word-blocklist](#)中的建议值）。
2. 漏洞CVE-2021-25746消减措施：通过实施准入策略，将'metadata.annotations'的值限制在已知的安全字符中（参考社区最新[规则](#)，或者采用[annotation-value-word-blocklist](#)中的建议值）。

相关链接

1. CVE-2021-25745社区漏洞issue：<https://github.com/kubernetes/ingress-nginx/issues/8502>

2. CVE-2021-25746社区漏洞issue: <https://github.com/kubernetes/ingress-nginx/issues/8503>
3. 社区已经发布版本修复: <https://github.com/kubernetes/ingress-nginx/releases/tag/controller-v1.2.0>

4.9 containerd 容器进程权限提升漏洞公告 (CVE-2022-24769)

漏洞详情

containerd开源社区中披露了一个安全漏洞，在containerd创建容器的场景，非root容器进程的初始inheritable capability不为空，可能会造成在execve执行可执行文件时提升到允许的cap集合。该问题已被收录为CVE-2022-24769。

表 4-7 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
权限提升	CVE-2022-24769	低	2022-3-24

漏洞影响

containerd创建容器时默认把 Linux Process capabilities配置到 Inheritable 集合上，这会导致在容器内的进程在以 Non-Root 用户 execve() 执行可执行文件时Inheritable 和文件的Inheritable集合的交集被添加到执行完execve后的进程的Permitted集合中，出现非预期的“越权”行为。需要说明的是，这个越权并没有突破 execve 前的进程权限，仅仅是继承之前的 capabilities。

该漏洞的影响范围如下：

1. CCE Turbo集群，使用了低于1.4.1-98版本的containerd作为kuberentes CRI运行时。
2. CCE集群containerd版本低于1.5.11以下的集群。

判断方法

在node节点上使用root用户执行containerd --version查看containerd版本。

新Console上的“节点管理”处也可以查看运行时版本。

漏洞修复方案

容器 entrypoint 使用 capsh工具去除自身的 Inheritable Capabilities。

相关链接

社区公告: <https://github.com/containerd/containerd/security/advisories/GHSA-c9cp-9c75-9v8c>

4.10 CRI-O 容器运行时引擎任意代码执行漏洞 (CVE-2022-0811)

漏洞详情

crowdstrike安全团队披露CRI-O 1.19版本中存在一个安全漏洞，攻击者可以利用该漏洞绕过保护措施并在主机上设置任意内核参数。这将导致任何有权在使用CRI-O的Kubernetes集群上部署Pod的用户都可以滥用kernel.core_pattern内核参数，在集群中的任何节点上以root身份实现容器逃逸和执行任意代码。

该问题已被收录为CVE-2022-0811。

表 4-8 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-2022-0811	高	2021-03-16

漏洞影响

该漏洞影响范围为使用了CRI-O的Kubernetes集群，CRI-O的版本大于1.19，涉及的补丁版本包括1.19.6、1.20.7、1.21.6、1.22.3、1.23.2、1.24.0。

CCE集群未使用CRI-O，因此不受此漏洞影响。

漏洞修复方案

- 1.19、1.20版本CRI-O，将manage_ns_lifecycle设置为false，由OCI运行时配置sysctl。
- 创建PodSecurityPolicy，将所有sysctl指定为false。
- 及时升级CRI-O版本。

相关链接

- Red Hat社区漏洞公告：<https://access.redhat.com/security/cve/cve-2022-0811>
- cr8escape: New Vulnerability in CRI-O Container Engine Discovered by CrowdStrike：<https://www.crowdstrike.com/blog/cr8escape-new-vulnerability-discovered-in-cri-o-container-engine-cve-2022-0811/>

4.11 linux 内核导致的容器逃逸漏洞公告 (CVE-2022-0492)

漏洞详情

在某些场景下linux内核cgroup v1的release_agent特性存在可以被利用在容器内逃逸到OS上的安全问题，该问题已被收录为CVE-2022-0492。

表 4-9 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-2022-0492	高	2021-02-07

漏洞影响

该漏洞为Linux内核权限校验漏洞，根因为没有针对性的检查设置release_agent文件的进程是否具有正确的权限。在受影响的OS节点上，工作负载使用了root用户运行进程（或者具有CAP_SYS_ADMIN权限），并且未配置seccomp时将受到漏洞影响。

CCE集群受该漏洞影响的范围如下：

1. x86场景EulerOS 2.5和CentOS镜像不受该漏洞影响。
2. 内核版本小于4.19.36-vhulk1907.1.0.h962.eulerosv2r8.aarch64的EulerOS arm版本。
3. 内核版本小于4.18.0-147.5.1.6.h541.eulerosv2r9.x86_64的EulerOS x86版本。
4. 内核版本为4.15.0-136-generic以及以下内核版本的Ubuntu节点。

漏洞修复方案

1. EulerOS 2.9 版本镜像已提供修复版本，请尽快迁移到4.18.0-147.5.1.6.h541.eulerosv2r9.x86_64版本节点。
2. 为工作负载配置seccomp，限制unshare系统调用，详情请参考Kubernetes [社区文档](#)。
3. 限制容器内进程权限，最小化容器内的进程权限，如使用非root启动进程、通过capability机制细化进程权限等。

相关链接

1. 内核修复commit: <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=24f6008564183aa120d07c03d9289519c2fe02af>
2. Red Hat社区漏洞公告: <https://access.redhat.com/security/cve/cve-2022-0492>

4.12 containerd 镜像 Volume 非安全处理漏洞公告 (CVE-2022-23648)

漏洞详情

containerd开源社区中披露了一个漏洞，如果镜像具有恶意的属性，在容器内的进程可能会访问主机上任意文件和目录的只读副本，从而造成宿主机上敏感信息泄露。

表 4-10 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-2022-23648	中	2022-02-28

漏洞影响

用户在使用了恶意构造的镜像时，会导致容器内可获取主机上的任意文件的只读副本，从而泄露敏感信息。

该漏洞影响范围如下：

1. 使用containerd作为Kubernetes CRI运行时，且使用了未知来源的恶意镜像。使用docker作为CRI时不涉及该漏洞。
2. containerd版本号小于1.4.1-96。

判断方法

在CCE新Console上的CCE Turbo集群的集群信息下的“节点管理”处，查看“运行时版本”，若运行时为containerd且版本号小于 1.4.1-96则涉及该漏洞。

漏洞修复方案

1. 使用可信的镜像，避免使用来源不明的第三方镜像，推荐使用容器镜像服务SWR。
2. CCE已提供大于1.4.1-96的containerd版本，请迁移至符合要求的节点。

相关链接

社区已经发布补丁，相关信息：<https://github.com/containerd/containerd/security/advisories/GHSA-crp2-qrr5-8pq7>

4.13 Linux 内核整数溢出漏洞（CVE-2022-0185）

漏洞详情

国外安全研究人员William Liu和Jamie Hill-Daniel发现Linux内核中包含一个整数溢出漏洞，可导致写操作越界。本地攻击者可以使用这一点导致拒绝服务(系统崩溃)或执行任意代码，在容器场景下拥有CAP_SYS_ADMIN权限的用户可导致容器逃逸到宿主机。目前已存在poc，但尚未发现已公开的利用代码。

表 4-11 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
资源管理错误	CVE-2022-0185	高	2022-01-27

漏洞影响

容器内用户拥有CAP_SYS_ADMIN权限，并且内核版本在5.1以及以上。在标准的docker环境下，由于使用了Docker seccomp filter，默认情况下不受该漏洞影响。在Kubernetes场景下，默认禁用了seccomp filter，在内核以及权限满足时受该漏洞影响。

CCE当前不受影响

判断方法

uname -a查看内核版本号

规避和消减措施

CCE集群节点不受该漏洞影响。对于自建的K8s集群，建议用户对工作负载：

1. 最小权限运行容器
2. 根据社区提供的配置方法配置[seccomp](#)

相关链接

<https://blog.aquasec.com/cve-2022-0185-linux-kernel-container-escape-in-kubernetes>

<https://ubuntu.com/security/CVE-2022-0185>

<https://access.redhat.com/security/cve/CVE-2022-0185>

<https://www.openwall.com/lists/oss-security/2022/01/18/7>

4.14 Linux Polkit 权限提升漏洞预警（CVE-2021-4034）

漏洞详情

国外安全研究团队披露在polkit的pkexec程序中存在一处权限提升漏洞（CVE-2021-4034，亦称PwnKit），攻击者通过在其默认配置中利用此漏洞实现用任何非特权用户获取易受攻击主机的完全root权限，目前漏洞POC/EXP已公开，风险较高。

Polkit（PolicyKit）是一个用于在类Unix操作系统中控制系统范围权限的组件。pkexec是Polkit框架中的一部分，执行具有提升权限的命令，是sudo的替代方案。请使用Polkit的用户及时安排自检并做好安全加固。

参考链接：<https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt>

表 4-12 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
权限提升	CVE-2021-4034	高	2022-01-28

漏洞影响

影响版本：所有目前主流的Linux版本

安全版本：查看各Linux厂商安全公告

漏洞处理方案

1. 目前RedHat、Ubuntu、Debian、SUSE等各大Linux厂商均已发布补丁版本修复了该漏洞，请受影响的用户升级到安全版本，若无法及时升级，可参考厂商官方提供的建议进行缓解。

[RedHat](#)；Ubuntu： [USN-5252-1](#)、[USN-5252-2](#)；[Debian](#)、[SUSE](#)

2. EulerOS已发布补丁，升级polkit rpm包即可。

升级方法如下

- a. yum clean all
- b. yum makecache
- c. yum update polkit
- d. rpm -qa | grep polkit

检查是否已经修复为对应版本

- EulerOS 2.10 修复版本为polkit-0.116-6.h4
- EulerOS 2.9 修复版本为polkit-0.116-5.h7
- EulerOS 2.8 修复版本为polkit-0.115-2.h14
- EulerOS 2.5 修复版本为polkit-0.112-14.h15

3. 若系统没有可用的补丁，可通过将pkexec中的SUID-bit删除进行临时规避，命令如：`# chmod 0755 /usr/bin/pkexec`

注：修复漏洞前请将资料备份，并进行充分测试。

4.15 Kubernetes subpath 符号链接交换安全漏洞 (CVE-2021- 25741)

漏洞详情

社区在 Kubernetes 中发现了一个安全问题，用户可以创建一个带有subPath volume 挂载的容器，访问卷外的文件和目录，包括主机文件系统上的文件和目录。

容器使用subPath去挂载一些文件或者目录时，攻击者可能利用Symlink Exchange 访问除挂载目录之外的目录或者主机上的文件，造成越权。

表 4-13 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
资源管理错误	CVE-2021-25741	中	2021-09-15

漏洞影响

该漏洞涉及VolumeSubpath特性开关开启场景（默认开启），可能造成以下影响：

- 若恶意用户可以创建一个带有子路径卷挂载的容器，则可以访问卷外的文件和目录，包括主机文件系统上的文件和目录。
- 集群管理员已限制创建 hostPath 挂载的能力的集群受到的影响最严重。利用该漏洞可以在不使用 hostPath 功能的情况下进行类似 hostPath 的访问，从而绕过限制。
- 在默认的 Kubernetes 环境中，漏洞利用可用于掩盖对已授予特权的滥用。

判断方法

涉及所有集群（新建的1.19.10及以上版本集群不受该漏洞影响）。

登录节点，执行命令，查看BuildDate，如果查看BuildDate是在2021-08-20之后的时间，则表示已经修复，不受该漏洞影响。

```
[root@prometheus-38892-wsb84 ~]# kubelet --version=raw
version.Info{Major:"1", Minor:"19+", GitVersion:"v1.19.10-r1.0.0-source-121-gb9675686c54267", GitCommit:"b9675686c54267276a35579d4921c91be3d226f2", GitTreeState:"clean", BuildDate:"2021-09-03T09:35:06Z", GoVersion:"go1.15.7", Compiler:"gc", Platform:"linux/amd64"}
```

漏洞处理方案

您可以禁用 kubelet 上的VolumeSubpath feature gate，并删除任何使用subPath功能的现有 Pod。

步骤1 以root用户登录CCE Node节点。

步骤2 修改kubelet配置参数，关闭VolumeSubpath特性。

vi /opt/cloud/cce/kubernetes/kubelet/kubelet_config.yaml

添加VolumeSubpath: false字段

```
featureGates:
  DevicePlugins: true
  MultiGPUScheduling: true
  CSIDriverRegistry: true
  CSINodeInfo: true
  ExpandCSIVolumes: true
  CSIInlineVolume: true
  CSIMigrationFlexVolumeFuxi: true
  CSIMigrationFlexVolumeFuxiComplete: true
  CSIMigration: true
  IPv6DualStack: false
  SupportSubENI: false
  ReserveMemoryCgroupForPageCache: false
  SizeMemoryBackedVolumes: true
  VolumeSubpath: false
```

步骤3 重启kubelet。

```
systemctl restart kubelet
```

步骤4 确认kubelet新进程已启动，且已关闭VolumeSubpath。

```
vi /var/paas/sys/log/kubernetes/kubelet.log
```

搜索VolumeSubpath=false，如果能搜到说明关闭成功。

```
FuxiComplete:true CSINodeInfo:true DevicePlugins:true ExpandCSIVolumes:true IPv6DualStack:false Multi
upportSubENI:false VolumeSubpath:false}]
W0923 14:58:45.371347 18693 feature_gate.go:235] Setting GA feature gate VolumeSubpath=false. It wi
W0923 14:58:45.371352 18693 feature_gate.go:235] Setting GA feature gate CSIDriverRegistry=true. It
W0923 14:58:45.371357 18693 feature_gate.go:235] Setting GA feature gate CSINodeInfo=true. It will
I0923 14:58:45.371362 18693 feature_gate.go:243] feature gates: &{map[CSIDriverRegistry:true CSINo
FuxiComplete:true CSINodeInfo:true DevicePlugins:true ExpandCSIVolumes:true IPv6DualStack:false Multi
upportSubENI:false VolumeSubpath:false}]
I0923 14:58:45.371464 18693 server.go:842] Client rotation is on, will bootstrap in background
I0923 14:58:45.384429 18693 bootstrap.go:84] Current kubeconfig file contents are still valid, no b
I0923 14:58:45.384482 18693 certificate_store.go:133] Loading cert/key pair from "/opt/cloud/cce/ku
I0923 14:58:45.384754 18693 server.go:886] Starting client certificate rotation.
I0923 14:58:45.384763 18693 certificate_manager.go:282] Certificate rotation is enabled.
I0923 14:58:45.384893 18693 certificate_manager.go:556] Certificate expiration is 2031-08-13 21:33:
I0923 14:58:45.384922 18693 certificate_manager.go:288] Waiting 76594h44m10.622152411s for next cer
I0923 14:58:45.385540 18693 dynamic_cafile_content.go:129] Loaded a new CA Bundle and Verifier for
I0923 14:58:45.385695 18693 dynamic_cafile_content.go:167] Starting client-ca-bundle::/opt/cloud/cc
I0923 14:58:45.385791 18693 manager.go:171] cAdvisor running in container: "/sys/fs/cgroup/cpu,cpuq
I0923 14:58:45.405886 18693 fs.go:130] Filesystem UUIDs: map[8b3744cc-15d9-434c-a9af-66a2c214b55c:/
f854b8:/dev/dm-1 c89eca08-5da4-43de-add0-4bb58e820d78:/dev/vda1]
@
@
@
@
@
?VolumeSubpath=false?
```

步骤5 删除任何使用subPath功能的Pod。

----结束

VolumeSubpath 特性开启或回退

步骤1 修改kubelet配置文件，删除VolumeSubpath相关字段。

```
vi /opt/cloud/cce/kubernetes/kubelet/kubelet_config.yaml
```

步骤2 重启kubelet。

```
systemctl restart kubelet
```

步骤3 确认kubelet新进程已启动，且重启后的kubelet.log日志中无VolumeSubpath=false相关字段。

----结束

相关链接

<https://github.com/kubernetes/kubernetes/issues/104980>

4.16 runc 符号链接挂载与容器逃逸漏洞预警公告 (CVE-2021-30465)

漏洞详情

业界安全研究人员披露runc符号链接挂载与容器逃逸漏洞 (CVE-2021-30465)，攻击者可通过创建恶意Pod，利用符号链接以及条件竞争漏洞，可挂载宿主机目录至容器中，最终可能会导致容器逃逸。目前漏洞细节、POC已公开，风险高。

表 4-14 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-2021-30465	高	2021-05-31

漏洞影响

攻击者可通过创建恶意Pod，挂载宿主机目录至容器中，利用runc的符号链接以及条件竞争漏洞，最终可能会导致容器逃逸，使攻击者能够访问宿主机的文件系统。

CCE v1.17之前版本的集群（不含1.17）涉及该漏洞，存量的CCE v1.17、v1.19、v1.21版本集群，需检查节点上runc版本。

漏洞处理方案

- 限制不受信任的用户拥有创建工作负载权限，尤其是拥有配置卷挂载参数的权限。
- 限制容器所拥有的权限。
 - 以非root用户运行
 - 通过capability限制容器拥有的特权，如CAP_DAC_OVERRIDE、CAP_DAC_READ_SEARCH、CAP_SYS_ADMIN等
 - 通过seccomp限制攻击者对宿主机内核的系统调用权限，具体请参见[使用Seccomp限制容器的系统调用](#)。

CCE新创建节点已经解决该漏洞。

您可以先创建新的节点，然后将老节点设置为不可调度，待老节点上应用都调度到新节点上后，删掉老节点或重置老节点。

相关链接

<https://github.com/opencontainers/runc/security/advisories/GHSA-c3xm-pvg7-gh7r>

4.17 Docker 资源管理错误漏洞公告 (CVE-2021-21285)

漏洞详情

Docker是一款开源的应用容器引擎，支持在Linux系统上创建一个容器（轻量级虚拟机）并部署和运行应用程序，以及通过配置文件实现应用程序的自动化安装、部署和升级。Docker 19.03.15和20.10.3之前的版本存在资源管理错误漏洞，攻击者可以利用该漏洞导致dockerd守护进程崩溃。

表 4-15 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
资源管理错误	CVE-2021-21285	中	2021-02-02

漏洞影响

docker daemon组件在拉取镜像的过程中没有对镜像层digest进行有效性校验，拉取一个被恶意损坏的镜像可能会导致docker daemon崩溃。

该漏洞可能在以下场景触发：

- 在集群内的节点上手动docker pull一个被恶意损坏的镜像。
- 部署工作负载时负载模板中定义了一个被恶意损坏的镜像，kubelet自动拉取镜像时触发。

该漏洞的影响范围如下：

- 若镜像被恶意损坏，拉取镜像时可能会导致docker daemon崩溃。
- 使用容器镜像服务（SWR）时，如果您的镜像是通过在SWR获取的，上传到镜像仓库的镜像会进行digest校验，此场景不受影响。
- 该漏洞不会影响运行中的容器。

判断方法

1. 如果节点是EulerOS和CentOS，可以用如需命令查看安全包版本：

```
rpm -qa |grep docker
```
2. 使用EulerOS或者CentOS的节点，docker版本低于**18.09.0.100.51.h10.51.h3-1.h15.eulerosv2r7**的docker包涉及该CVE漏洞。
3. 使用其它非EulerOS和CentOS的镜像（如Ubuntu），可以使用docker version查看docker版本。若版本低于19.03.15、20.10.3，则涉及该漏洞。

漏洞修复方案

不使用未知来源的镜像，推荐使用容器镜像服务SWR。

相关链接

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：<https://github.com/moby/moby/commit/8d3179546e79065adefa67cc697c09d0ab137d30>

4.18 NVIDIA GPU 驱动漏洞公告（CVE-2021-1056）

漏洞详情

NVIDIA公布了关于NVIDIA GPU驱动的一个漏洞CVE-2021-1056，该漏洞是存在于NVIDIA GPU驱动程序中与设备隔离相关的安全漏洞。当容器以非特权模式启动，攻击者利用这个漏洞，通过在容器中创建特殊的字符设备文件后，能够获取宿主机上所有GPU设备的访问权限。

关于漏洞的详细信息，请参见[CVE-2021-1056](#)。

如果您的CCE集群中存在GPU（ECS）节点，并使用了CCE推荐的NVIDIA GPU驱动版本（Tesla 396.37），按照目前NVIDIA官方公告判断暂不受影响；如果您自行安装或更新过节点上的NVIDIA GPU驱动，则可能存在该漏洞。

表 4-16 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
权限提升	CVE-2021-1056	中	2021-01-07

漏洞影响

按照NVIDIA官方给出的漏洞公告信息，目前受影响的NVIDIA GPU驱动版本如下图所示：

CVE IDs Addressed	Software Product	Operating System	Driver Branch	Affected Versions	Updated Driver Version
CVE-2021-1052 CVE-2021-1053	GeForce	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
	NVIDIA RTX/Quadro, NVS	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
	Tesla	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
CVE-2021-1056	GeForce	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
	NVIDIA RTX/Quadro, NVS	Linux	R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
	Tesla	Linux	R390	All version prior to 390.141	390.141
			R460	All versions prior to 460.32.03	460.32.03
			R450	All versions prior to 450.102.04	450.102.04
			R418	All versions prior to 418.181.07	418.181.07

更多信息，请参见[NVIDIA官网](#)。

影响说明：

- 云容器引擎CCE集群和gpu-beta插件推荐安装的NVIDIA GPU驱动，尚未出现在NVIDIA官方信息中。如果将来有新的官方信息变化，我们将及时跟进帮助您升级修复。
- 如果您是自行选择安装的NVIDIA GPU驱动或更新过节点上的GPU驱动，请参考上图确认您安装的GPU驱动是否受该漏洞影响。

如何确认 GPU 节点的 NVIDIA 驱动版本

登录到您的GPU节点，执行如下命令，即可查看驱动版本。

```
[root@XXX36 bin]# ./nvidia-smi
Fri Apr 16 10:28:28 2021

+-----+
| NVIDIA-SMI 460.32.03   Driver Version: 460.32.03   CUDA Version: 11.2   |
+-----+
| GPU  Name      Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|  Memory-Usage | GPU-Util  Compute M. |
|                               |              MIG M. |
+-----+-----+
| 0  Tesla T4           Off | 00000000:21:01.0 Off |   0 |
| N/A   68C    P0   31W / 70W |  0MiB / 15109MiB |  0%   Default |
|                               |              N/A |
+-----+-----+

+-----+
| Processes:
| GPU  GI  CI       PID   Type   Process name          GPU Memory |
|   ID  ID             |           |         Usage         |
+-----+-----+
| No running processes found
+-----+-----+
```

从上述输出的信息中，可以看到该节点的GPU驱动版本为460.32.03。

漏洞修复方案

请您根据**漏洞影响**范围，将节点升级到对应驱动版本进行漏洞修复：

📖 说明

若您升级了NVIDIA GPU驱动，需重启GPU节点，重启节点将会短暂影响您的业务。

- 如果节点驱动版本为418系列，请升级驱动至418.181.07版本。
- 如果节点驱动版本为450系列，请升级驱动至450.102.04版本。
- 如果节点驱动版本为460系列，请升级驱动至460.32.03版本。

如果您升级CCE集群节点的GPU驱动，可以升级gpu-beta插件或重装插件，并在安装插件时填写修复后的NVIDIA GPU驱动的下地址即可。

相关链接

- 英伟达安全公告：https://nvidia.custhelp.com/app/answers/detail/a_id/5142
- Ubuntu安全公告：<https://ubuntu.com/security/CVE-2021-1056>
- CVE收录信息：<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1056>
- NVD收录信息：<https://nvd.nist.gov/vuln/detail/CVE-2021-1056>
- CVE PoC：<https://github.com/pokerfaceSad/CVE-2021-1056>
- GPUMounter：<https://github.com/pokerfaceSad/GPUMounter>

4.19 Sudo 缓冲区错误漏洞公告 (CVE-2021-3156)

漏洞详情

外部安全研究人员披露sudo中的堆溢出漏洞 (CVE-2021-3156)，该漏洞在类似Unix的主要操作系统上都可以使用。在其默认配置下会影响从1.8.2到1.8.31p2的所有旧版本以及从1.9.0到1.9.5p1的所有稳定版本。成功利用此漏洞，任何没有特权的用户都可以在易受攻击的主机上获得root特权。

sudo是一个功能强大的实用程序，大多数基于Unix和Linux的操作系统都包含sudo。它允许用户使用其他用户的安全特权运行程序。

表 4-17 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
权限提升	CVE-2021-3156	高	2021-01-26

漏洞影响

- sudo 1.8.2到1.8.31p2所有旧版本 (默认配置)
- sudo 1.9.0到1.9.5p1所有稳定版 (默认配置)

判断方法

1. 以非root用户身份登录系统。
2. 执行命令`sudedit -s /`进行漏洞排查。
 - 如果系统容易受到攻击，它将以“`sudedit:` ”开头的错误作为响应。
 - 如果对系统进行了修补，它将以“`usage:` ”开头的错误作为响应。

漏洞修复方案

受影响的用户请及时将sudo升级到安全版本，并在升级前做好自验：

- CentOS：更新到sudo 1.9.5p2及以上版本。
sudo版本下载请参见<https://www.sudo.ws/download.html>。
- EulerOS：sudo补丁包获取链接。
 - EulerOS 2.2：https://mirrors.huaweicloud.com/euler/2.2/os/x86_64/updates/sudo-1.8.6p7-23.h9.x86_64.rpm
 - EulerOS 2.5：https://mirrors.huaweicloud.com/euler/2.5/os/x86_64/updates/sudo-1.8.19p2-14.h9.eulerov2r7.x86_64.rpm
 - EulerOS 2.8：<https://mirrors.huaweicloud.com/euler/2.8/os/aarch64/updates/sudo-1.8.23-3.h18.eulerov2r8.aarch64.rpm>

相关链接

<https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit>

4.20 Kubernetes 安全漏洞公告（CVE-2020-8554）

漏洞详情

CVE-2020-8554是Kubernetes社区发现的关于集群内网络流量劫持的安全问题。具有创建和更新Service和Pod对象权限的潜在攻击者，能够劫持集群内来自其他Pod或者节点的流量。潜在攻击者通过设置Service对象的spec.externalIPs字段，能够劫持集群内其他Pod或者节点访问该externalIP（如某公网知名IP）的流量，并将其转发到攻击者创建的恶意Pod中，造成中间人攻击。同理，攻击者通过修改Service对象的状态status.loadBalancer.ingress.ip也能达到此目的。

表 4-18 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
流量劫持	CVE-2020-8554	中	2020-12-07

漏洞影响

对于单集群内多个用户共享使用的场景，如果将Pod和Service的创建和更新权限授予不信任的用户易受此漏洞的影响。

涉及所有Kubernetes版本。

漏洞修复方案

建议您检查所有使用externalIP和loadBalancerIP的Service，确认是否有可疑的Service。

该问题由Kubernetes软件的设计缺陷导致，当前用户可以采取如下措施进行防范：

- **限制externalIP的使用**
 - **方法一：**通过Admission Webhook容器（k8s.gcr.io/multitenancy/externalip-webhook:v1.0.0）限制externalIP的使用。源代码和部署说明发布在：<https://github.com/kubernetes-sigs/externalip-webhook>。
 - **方法二：**使用开源软件OPA Gatekeeper限制externalIP的使用。示例说明ConstraintTemplate和Constraint发布在：<https://github.com/open-policy-agent/gatekeeper-library/tree/master/library/general/externalip>。
- **限制LoadBalancerIP的使用**

由于社区不建议集群管理员向集群内的用户授予service/status对象的patch权限，因此社区没有为LoadBalancerIP提供规避措施。如果您需要对LoadBalancerIP进行限制，则可以参考externalIP的规避措施。

相关链接

<https://github.com/kubernetes/kubernetes/issues/97076>

4.21 Apache containerd 安全漏洞公告 (CVE-2020-15257)

漏洞详情

CVE-2020-15257是containerd官方发布的一处Docker容器逃逸漏洞。containerd是一个支持Docker和常见Kubernetes配置的容器运行时管理组件，它处理与容器化有关的抽象，并提供API以管理容器的生命周期。在特定的条件下，可以通过访问containerd-shim API，来实现Docker容器逃逸。

表 4-19 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
Docker容器逃逸	CVE-2020-15257	中	2020-11-30

漏洞影响

CCE集群版本：v1.9-v1.17.9。

如果没有使用主机网络并且容器内进程不以root用户（UID为0）运行，则不涉及该漏洞。

漏洞修复方案

建议使用最小权限运行容器，对于不信任的容器进行如下限制：

1. 禁止使用主机网络；
2. 禁止容器内的进程以root用户运行。

相关链接

[containerd-shim API exposed to host network containers](#)

4.22 Docker Engine 输入验证错误漏洞公告 (CVE-2020-13401)

漏洞详情

CVE-2020-13401漏洞源于IPv6动态分配除提供了IPv6的DHCP技术外，还支持Router Advertisement技术。路由器会定期向节点通告网络状态，包括路由记录。客户端会通过NDP进行自身网络配置。本文介绍该漏洞的影响。

表 4-20 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
输入验证错误	CVE-2020-13401	中	2020-06-01

漏洞影响

对操作系统中启用了IPv6并且容器网络的CNI Plugins小于V0.8.6版本的节点有影响。

恶意攻击者可以篡改主机上其他容器或主机本身的IPv6路由记录，实现中间人攻击。即使现在系统或者服务上没有直接使用IPv6地址进行网络请求通知，但是如果DNS返回了A(IPv4)和AAAA(IPv6)记录，许多HTTP库都会尝试IPv6进行连接，如果再回退到IPv4，这为攻击者提供了响应的机会。该漏洞为中危漏洞，CVSS评分为6.0。

Kubernetes本身不受该漏洞影响，但Kubernetes所使用的CNI插件（请参阅<https://github.com/containernetworking/plugins/pull/484>）会受影响，以下kubelet版本都包含了受影响的CNI插件服务：

- kubelet v1.18.0~v1.18.3
- kubelet v1.17.0~v1.17.6
- kubelet<v1.16.11

漏洞修复方案

- 修改主机内核参数配置net.ipv6.conf.all.accept_ra值为0，以拒绝接收IPv6路由发布。
- 业务容器结合使用TLS和适当的证书验证，防止中间人欺骗。
- 禁止在Pod中设置CAP_NET_RAW能力，防止恶意容器篡改IPv6路由：

```
securityContext:  
  capabilities:  
    drop: ["NET_RAW"]
```

4.23 Kubernetes kube-apiserver 输入验证错误漏洞公告 (CVE-2020-8559)

漏洞详情

Kubernetes官方披露了kube-apiserver组件的安全漏洞，攻击者可以通过截取某些发送至节点kubelet的升级请求，通过请求中原有的访问凭据转发请求至其它目标节点，攻击者可利用该漏洞提升权限。本文介绍该漏洞的影响范围、漏洞影响和防范措施。

表 4-21 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
其它	CVE-2020-8559	中	2020-07-15

漏洞影响

由于kube-apiserver中在升级请求的代理后端中允许将请求传播回源客户端，攻击者可以通过截取某些发送至节点kubelet的升级请求，通过请求中原有的访问凭据转发请求至其他目标节点，从而造成被攻击节点的权限提升漏洞。该漏洞为中危漏洞，CVSS评分为6.4。

如果有多个集群共享使用了相同的CA和认证凭证，攻击者可以利用此漏洞攻击其他集群，这种情况下该漏洞为高危漏洞。

对于此次漏洞的跨集群攻击场景，CCE集群使用了独立签发的CA，同时不同集群间认证凭据完全隔离，跨集群场景不受影响。

从v1.6.0之后到下列修复版本的所有kube-apiserver组件均包含漏洞代码：

- kube-apiserver v1.18.6
- kube-apiserver v1.17.9
- kube-apiserver v1.16.13

下列应用场景在此次漏洞的影响范围内：

- 如果集群运行业务中存在多租户场景，且以节点作为不同租户间隔离的安全边界。
- 不同集群间共享使用了相同的集群CA和认证凭据。

漏洞修复方案

对于集群内跨节点的攻击，建议您采取以下安全防范措施：

- 请妥善保管认证凭据。
- 授权子账号遵循权限最小化原则，通过设置RBAC权限，限制不必要的pods/exec、pods/attach、pods/portforward和proxy类型的资源访问。

4.24 Kubernetes kubelet 资源管理错误漏洞公告 (CVE-2020-8557)

漏洞详情

kubelet的驱逐管理器（eviction manager）中没有包含对Pod中挂载的/etc/hosts文件的临时存储占用管理，因此在特定的攻击场景下，一个挂载了/etc/hosts的Pod可以通过对该文件的大量数据写入占满节点的存储空间，从而造成节点的拒绝访问（Denial of Service）。

表 4-22 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
资源管理错误	CVE-2020-8557	中	2020-07-15

漏洞影响

kubelet的驱逐管理器（eviction manager）中没有包含对Pod中挂载的/etc/hosts文件的临时存储占用管理，因此在特定的攻击场景下，一个挂载了/etc/hosts的Pod可以通过对该文件的大量数据写入占满节点的存储空间，从而造成节点的拒绝访问（Denial of Service）。该漏洞为中危漏洞，CVSS评分为5.5。

具备以下特权的Pod拥有节点上/etc/hosts文件的写入权限：

- Pod中的容器具备CAP_DAC_OVERRIDE系统权限（默认具备）。
- Pod以root（UID为0）用户启动或者Pod Security Context中的allowPrivilegeEscalation设置为true（当以特权容器或者加了CAP_SYS_ADMIN权限运行时默认为true）。

下列版本的kubelet组件均在此CVE的影响范围内：

- kubelet v1.18.0~v1.18.5
- kubelet v1.17.0~v1.17.8
- kubelet<v1.16.13

漏洞修复方案

建议您采取以下安全防范措施：

- 通过设置集群Pod安全策略或admission准入机制强制Pod删除CAP_DAC_OVERRIDE系统权限：

```
securityContext:  
  capabilities:  
    drop: ["DAC_OVERRIDE"]
```

- 通过使用集群Pod安全策略或其他admission准入机制限制以root用户启动容器，或设置参数allowPrivilegeEscalation为false：

```
securityContext:  
  allowPrivilegeEscalation: false
```

- 通过以下命令对容器内的/etc/hosts文件进行监控，如果该文件的大小异常，请采取相应告警或容器隔离措施。

```
find /var/lib/kubelet/pods/*/etc-hosts -size +1M
```

4.25 Kubernetes kubelet 和 kube-proxy 授权问题漏洞公告（CVE-2020-8558）

漏洞详情

Kubernetes官方发布安全公告，其核心组件kube-proxy存在主机边界绕过漏洞（CVE-2020-8558）。利用漏洞攻击者可能通过同一局域网下的容器，或在集群节点上访问同一个二层域下的相邻节点上绑定监听了本地127.0.0.1端口的TCP/UDP服务，从而获取接口信息。如果绑定在端口上的服务没有设置身份验证，则会导致该服务容易受到攻击。例如，如果集群管理员运行监听了127.0.0.1:1234的TCP服务，由于这个bug，该服务将有可能被与该节点在同一局域网中的其他主机，或与该服务运行在同一节点上的容器所访问。如果端口1234上的服务不需要额外的认证（因为假设只有其他localhost进程可以），那么很容易受到利用此bug进行攻击。

华为云提醒使用kube-proxy的用户及时安排自检并做好安全加固。

详情请参考链接：<https://github.com/kubernetes/kubernetes/issues/92315>

表 4-23 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
代码注入	CVE-2020-8558	高	2020-07-08

漏洞影响

当攻击者拥有主机网络配置能力或运行在一个具备了CAP_NET_RAW能力的容器实例时，就可以获取在目标节点上监听了127.0.0.1的服务socket信息。如果在目标主机上存在127.0.0.1可以访问到且不需要任何认证鉴权的暴露服务，那么该服务信息就能被攻击者获取。问题详情请参见[Placeholder issue](#)。

可能的攻击者：

- 同一交换机内的其他共享主机实例。
- 本机的运行容器。

在下列版本的kube-proxy组件均在此CVE的影响范围内：

- kube-proxy v1.18.0~v1.18.3
- kube-proxy v1.17.0~v1.17.6
- kube-proxy <v1.16.10

CCE集群控制面已经通过安全组进行防护，只允许从租户节点或者相邻节点访问安全端口，默认安全。

集群node节点上系统组件监听在127.0.0.1的端口只涉及健康检查、监控信息查询等请求，不会有信息泄露风险。

综上，该CVE对CCE集群影响不大。

漏洞修复方案

目前官方已提供安全版本修复了该漏洞，请受影响的用户升级至以下安全版本。

- kubelet/kube-proxy v1.18.4+
- kubelet/kube-proxy v1.17.7+
- kubelet/kube-proxy v1.16.11+

建议您采取以下安全防范措施：

- 如果业务容器需使用主机网络模式且又监听在非安全端口上，可以通过在节点上手动添加iptables规则来缓解此漏洞。

执行以下命令，在集群中配置iptables规则，用于拒绝非本地对127.0.0.1的访问流量：

```
iptables -I INPUT --dst 127.0.0.0/8 ! --src 127.0.0.0/8 -m conntrack ! --ctstate RELATED,ESTABLISHED,DNAT -j DROP
```

如果集群不需要开启API Server不安全端口，可以将--insecure-port=0添加到kubernetes API服务器命令行来禁用端口。

- 如集群内运行有不受信的容器，需要manifest文件中关闭CAP_NET_RAW能力，可执行如下命令：


```
securityContext:  
  capabilities:  
    drop: ["NET_RAW"]
```

⚠ 注意

修复漏洞前请将资料备份，并进行充分测试。

4.26 修复 Kubernetes HTTP/2 漏洞公告

漏洞详情

近期Kubernetes社区发布了与Go相关的安全漏洞CVE-2019-9512和CVE-2019-9514。具体的安全问题出现在Go语言的net/http库中，它会影响Kubernetes的所有版本和所有组件。这些漏洞可能导致所有处理HTTP或HTTPS Listener的进程受到DoS攻击。

由于此问题影响范围很广，Go官方及时针对此问题发布了Go 1.12.9和Go 1.11.13版本。

Kubernetes也在v1.13.10 - go1.11.13版本中完成了Go版本的更新。

CCE已发布最新Kubernetes 1.13.10版本对漏洞进行修复，对于已经创建的Kubernetes 1.13版本，2019年9月底将提供补丁进行修复。针对低于Kubernetes 1.13集群版本将提供升级能力。

表 4-24 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间
拒绝服务攻击	CVE-2019-9512	高	2019-08-13
资源管理错误	CVE-2019-9514	高	2019-08-13

漏洞影响

默认集群在VPC和安全组内保护下不受影响。

如果用户通过互联网访问方式开放集群API，集群控制面可能会受影响。

漏洞修复方案

- CCE已发布最新Kubernetes 1.13.10版本对漏洞进行修复。
- 针对低于Kubernetes 1.13集群版本请升级集群版本。

参考链接

Netflix报告链接：

<https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-002.md>

Go版本发布链接：

<https://golang.org/doc/devel/release.html#go1.12>

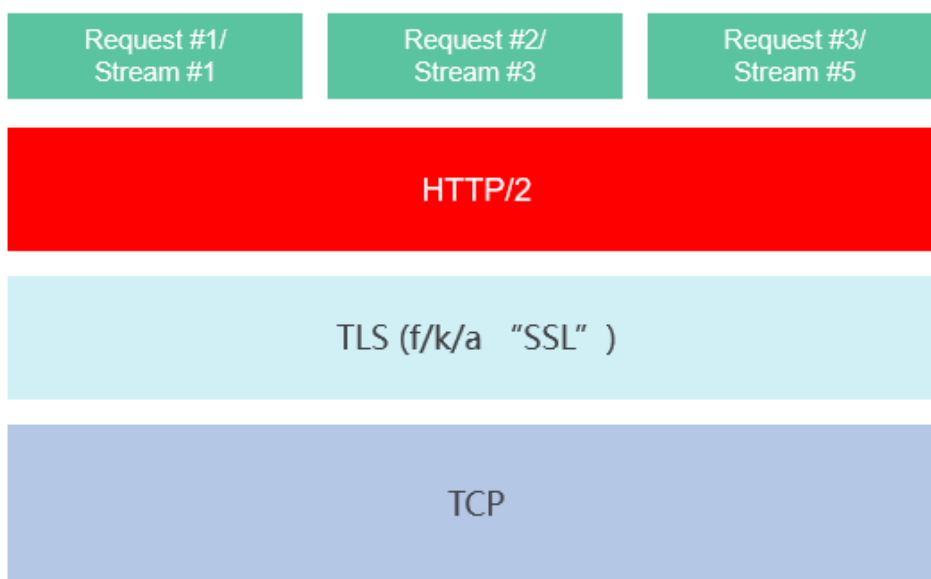
Kubernetes社区PR链接:

<https://github.com/kubernetes/kubernetes/pull/81520>

<https://github.com/kubernetes/kubernetes/pull/81522>

附：为何影响？

这些攻击大多在HTTP/2传输层进行。如下图所示，该层位于TLS传输之上，但在请求概念之下。事实上，许多攻击都涉及0或1个请求。



从早期的超文本传输协议开始，中间件服务就以请求为导向：日志以请求为分割(而不是连接)；速率限制发生在请求级别；并且流量控制也由请求触发。

相比之下，没有多少工具可以根据客户端在HTTP/2连接层的行为来执行记录、速率限制和修正。因此，中间件服务可能会发现更难发现和阻止恶意的HTTP/2连接，并且可能需要添加额外的工具来处理这些情况。

这些攻击媒介允许远程攻击者消耗过多的系统资源。有些攻击足够高效，单个终端系统可能会对多台服务器造成严重破坏（服务器停机/核心进程崩溃/卡死）。其他攻击效率较低的情况则产生了一些更棘手的问题，只会使服务器的运行变得缓慢，可能是间歇性的，这样的攻击会更难以检测和阻止。

4.27 修复 Linux 内核 SACK 漏洞公告

漏洞详情

2019年6月18日，Redhat发布安全公告，Linux内核处理器TCP SACK模块存在3个安全漏洞(CVE-2019-11477、CVE-2019-11478、CVE-2019-11479)，这些漏洞与最大分段大小（MSS）和TCP选择性确认（SACK）功能相关，攻击者可远程发送特殊构造的攻击包造成拒绝服务攻击，导致服务器不可用或崩溃。

华为云CCE团队已经紧急修复Linux内核SACK漏洞，并已发布解决方案。

参考链接：

<https://www.suse.com/support/kb/doc/?id=7023928>

<https://access.redhat.com/security/vulnerabilities/tcpsack>

<https://www.debian.org/lts/security/2019/dla-1823>

<https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SACKPanic?>

<https://lists.centos.org/pipermail/centos-announce/2019-June/023332.html>

<https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md>

表 4-25 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间	华为云修复时间
输入验证错误	CVE-2019-11477	高	2019-06-17	2019-07-06
资源管理错误	CVE-2019-11478	高	2019-06-17	2019-07-06
资源管理错误	CVE-2019-11479	高	2019-06-17	2019-07-06

漏洞影响

影响Linux内核2.6.29及以上版本。

漏洞修复方案

此问题已在稳定内核版本4.4.182、4.9.182、4.14.127、4.19.52、5.1.11中修复，用户通过滚动升级节点即可。

附：TCP SACK 介绍

TCP是面向连接的协议。当双方希望通过TCP连接进行通信时，他们通过TCP握手交换某些信息建立连接，例如发起一个TCP请求，通过SYN发送初始序列ID，确认ID，连接使用的最大数据包段大小（MSS），认证信息和处理选择性确认（SACK）等。整体TCP连接通过我们熟知的三次握手最终建立。

TCP通过一个数据段单元发送和接收用户数据包。TCP数据段由TCP头，选项和用户数据组成。每个TCP段都有序列号（SEQ）和确认号（ACK）。

接收方通过SEQ号和ACK号来跟踪成功接收了哪些段。ACK号下一个预期接受的段。

示例：



上图中用户A通过13个100字节的段发送1k字节的数据，每个段具有20字节的TCP头，总计是13个段。在接收端，用户B接收了段1,2,4,6,8-13，而段3,5和7丢失，B没有接收到。

通过使用ACK号，用户B告诉A，他需要段3，用户A收到B接收到2，而没有收到3，A将重新发送全部段，尽管B已经收到了4,6和8-13段。所以导致大量重复传输，性能低下。

4.28 修复 Docker 操作系统命令注入漏洞公告 (CVE-2019-5736)

漏洞详情

Docker、containerd或者其他基于runc的容器运行时存在安全漏洞，攻击者可以通过特定的容器镜像或者exec操作可以获取到宿主机的runc执行时的文件句柄并修改掉runc的二进制文件，从而获取到宿主机的root执行权限。

华为云容器引擎已修复runc漏洞CVE-2019-5736。

表 4-26 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间	华为云修复时间
代码执行	CVE-2019-5736	高	2019-02-11	2019-02-12

漏洞CVE-2019-5736的详细信息，请参见：<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5736>

漏洞影响

本次漏洞典型的攻击方式是通过恶意镜像：在恶意镜像中，将攻击函数隐藏在恶意动态库如（libseccomp.so.2）中，并使执行命令指向/proc/self/exe。

当runc动态编译时，会从容器镜像中载入动态链接库，导致加载恶意动态库；当打开/prco/self/exe即runc时，会执行恶意动态链接库中的恶意程序，由于恶意程序继承runc打开的文件句柄，可以通过该文件句柄替换host上的runc。

此后，再次执行runc相关的命令，则会产生逃逸。

该漏洞影响范围如下：

- 本次漏洞对所有采用runc的容器引擎均生效，runc是Docker容器的核心组件，因此对绝大部分容器均会产生影响。其中主要影响的是多用户共享节点的场景，可导致某用户通过渗透进而控制节点并攻击整集群。
- **华为云CCE容器服务：**
CCE容器服务创建的Kubernetes集群属于单租户专属，不存在跨租户共享，影响范围较小，对于多用户场景需要关注。
当前CCE采用华为优化的Docker容器，其中RUNC采用静态编译，目前公开披露的攻击方法无法成功入侵。

- **华为云CCI容器实例服务：**
CCI引擎采用华为Kata容器引擎，提供单节点上多容器高安全的hypervisor级别的隔离能力，并没有采用runc容器，因此本次漏洞将不会对CCI产生影响。

漏洞修复方案

- 华为云CCE容器服务：
华为云容器引擎已修复runc漏洞CVE-2019-5736。
- 自建Kubernetes或使用开源容器引擎：
 - 升级Docker到18.09.2版本，由于开源Docker在17.06之后的版本做了较大变更，涉及架构解耦重构，该办法可能会导致用户容器业务中断，建议做好充分验证，并按节点逐步滚动升级。
 - 仅升级runc，对于17.06等Docker版本，可以不中断已运行业务，当前runc官方尚未发布包含漏洞修复补丁的新版本，如果要单独升级runc，用户可自行编译。
 - 另特别提醒，本次Docker官方补丁使用了高版本Linux内核的系统调用，在低版本内核部分版本上可能会失效，若补丁失效时，建议升级至3.17以上内核。华为云CCE容器服务提供的补丁针对官方补丁进行了优化适配，已验证在多版本内核上均可生效。

4.29 全面修复 Kubernetes 权限许可和访问控制漏洞公告 (CVE-2018-1002105)

漏洞详情

近日，Kubernetes社区发现安全漏洞CVE-2018-1002105。通过伪造请求，Kubernetes用户可以在已建立的API Server连接上提权访问后端服务，华为云容器服务已在第一时间完成全面修复。

表 4-27 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间	华为云修复时间
权限提升	CVE-2018-1002105	严重	2018-12-05	2018-12-05

漏洞详细介绍：<https://github.com/kubernetes/kubernetes/issues/71411>。

漏洞影响

集群使用了聚合API，只要kube-apiserver与聚合API server的网络直接连通，攻击者就可以利用这个漏洞向聚合API服务器发送任何API请求；

如果集群开启了匿名用户访问的权限，则匿名用户也利用这个漏洞。不幸的是Kubernetes默认允许匿名访问，即kube-apiserver的启动参数“--anonymous-auth=true”；给予用户Pod的exec/attach/portforward的权限，用户也可以利用这个漏洞升级为集群管理员，可以对任意Pod做破坏操作。

该漏洞的更详细讨论，可见社区Issue：<https://github.com/kubernetes/kubernetes/issues/71411>

该漏洞的影响范围如下：

- 集群启用了扩展API server，并且kube-apiserver与扩展API server的网络直接连通。
- 集群对攻击者可见，即攻击者可以访问到kube-apiserver的接口，如果您的集群是部署在安全的私网内，那么不会有影响。
- 集群开放了pod exec/attach/portforward接口，则攻击者可以利用该漏洞获得所有的kubelet API访问权限。

具体影响的集群版本如下：

- Kubernetes v1.0.x-1.9.x
- Kubernetes v1.10.0-1.10.10 (fixed in v1.10.11)
- Kubernetes v1.11.0-1.11.4 (fixed in v1.11.5)
- Kubernetes v1.12.0-1.12.2 (fixed in v1.12.3)

漏洞修复方案

综合以上分析，使用华为云CCE服务时不必过于担心，因为：

- CCE服务创建的集群默认关闭匿名用户访问权限。
- CCE服务创建的集群没有使用聚合API。

华为云容器引擎已完成1.11以上版本Kubernetes集群的在线补丁修复，针对低于v1.10的集群（社区已不对其进行修复），已提供补丁版本进行修复，请关注升级公告，及时修复漏洞。

📖 说明

如果您是自行搭建Kubernetes集群，为提高集群的安全系数，建议如下，一定要关闭匿名用户访问权限。

尽快升级到社区漏洞修复版本。合理配置RBAC，只给可信用户Pod的exec/attach/portforward权限。

如果您当前使用的Kubernetes版本低于v1.10，不在官方补丁支持范围内，建议自行回滚补丁代码：<https://github.com/kubernetes/kubernetes/pull/71412>。

4.30 修复 Kubernetes Dashboard 安全漏洞公告 (CVE-2018-18264)

漏洞详情

Kubernetes社区发现Kubernetes Dashboard安全漏洞CVE-2018-18264：使用Kubernetes Dashboard v1.10及以前的版本有跳过用户身份认证，及使用Dashboard登录账号读取集群密钥信息的风险。

华为云CCE提供的Dashboard插件已将对应镜像升级到v1.10.1版本，不受Kubernetes Dashboard漏洞CVE-2018-18264影响。

表 4-28 漏洞信息

漏洞类型	CVE-ID	漏洞级别	披露/发现时间	华为云修复时间
Access Validation Error	CVE-2018-18264	高	2019-01-03	2019-01-05

安全漏洞CVE-2018-18264的详细信息，请参考：

- <https://github.com/kubernetes/dashboard/pull/3289>
- <https://github.com/kubernetes/dashboard/pull/3400>
- <https://github.com/kubernetes/dashboard/releases/tag/v1.10.1>

漏洞影响

如果您的Kubernetes集群中独立部署了Kubernetes Dashboard v1.10及之前版本（v1.7.0-v1.10.0），同时支持登录功能且使用了自定义证书。

漏洞修复方案

华为云CCE提供的Dashboard插件已将对应镜像升级到v1.10.1版本，不受Kubernetes Dashboard漏洞CVE-2018-18264影响，请放心使用。

5 产品发布记录

5.1 集群版本发布记录

5.1.1 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集群的Kubernetes版本策略。

CCE 集群版本生命周期表

Kubernete s版本号	当前状态	社区发布时间	CCE集群版 本公测时间	CCE集群版 本商用时间	CCE集群版 本EOS（停 止服务）时 间
v1.29	公测	2023年11 月	2024年4月	2024年6月	2026年6月
v1.28	已商用 ^a	2023年8月	2023年12 月	2024年2月	2026年2月
v1.27	已商用 ^a	2023年04 月	2023年08 月	2023年10 月	2025年10 月
v1.25	已商用 ^b	2022年08 月	2022年11 月	2023年03 月	2025年03 月
v1.23	已商用 ^b	2021年12 月	2022年04 月	2022年09 月	2024年09 月
v1.21	EOS	2021年04 月	2021年12 月	2022年04 月	2024年04 月
v1.19	EOS	2020年08 月	2020年12 月	2021年03 月	2023年09 月

Kubernetes版本号	当前状态	社区发布时间	CCE集群版本公测时间	CCE集群版本商用时间	CCE集群版本EOS（停止服务）时间
v1.17	EOS	2019年12月	/	2020年07月	2023年01月
v1.15	EOS	2019年06月	/	2019年12月	2022年09月
v1.13	EOS	2018年12月	/	2019年06月	2022年03月
v1.11	EOS	2018年08月	/	2018年10月	2021年03月
v1.9	EOS	2017年12月	/	2018年03月	2020年12月

📖 说明

CCE控制台支持最新两个商用版本的集群：

- a：支持通过控制台、API方式创建。
- b：仅支持API方式创建。

CCE 集群版本阶段说明

- 版本公测阶段：您可以通过CCE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 集群版本号说明

CCE 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，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，详情请参见[社区Kubernetes版本策略](#)。关于CCE支持的Kubernetes版本详情，请参见[Kubernetes版本发布记录](#)。
- CCE补丁版本：格式形如v1.28.Z-rN，处于维护期的Kubernetes版本会不定期的发布新的补丁版本。当新的补丁版本较上一版本提供了新的特性时，Z版本号增加；当新的补丁版本较上一版本提供了Bugfix、漏洞修复或场景优化时，N版本号增加。关于CCE补丁版本详情，请参见[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集群。CCE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，请您务必及时升级CCE集群。

您可以通过云容器引擎管理控制台，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。

5.1.2 Kubernetes 版本发布记录

5.1.2.1 Kubernetes 1.29 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 1.29集群。本文介绍Kubernetes 1.29版本的变更说明。

索引

- [新增特性及特性增强](#)
- [API变更与弃用](#)
- [CCE对Kubernetes 1.29版本的增强](#)
- [参考链接](#)

新增特性及特性增强

- 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/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。你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，更好的利用计算资源。

- 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。
- **ServiceNodePortStaticSubrange达到GA**
在Kubernetes1.29版本，ServiceNodePortStaticSubrange特性达到GA版本。该特性kubelet会根据Nodeport范围计算出预留地址大小，并将Nodeport划分为静态段和动态段。在Nodeport自动分配时，优先分配在动态段，这有助于减小指定静态段分配时的端口冲突。更多使用细节请参考[ServiceNodePortStaticSubrange](#)
- **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

- 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，移除了selectorSpread调度器插件，使用podTopologySpread替代。
- 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。
- 在Kubernetes1.29版本中，kubelet可通过--node-ips来设置双栈IP（kubelet设置--cloud-provider=external，此时可以使用--node-ips参数来设置节点地址（IPv4/IPv6）），使用该特性需开启特性门控CloudDualStackNodeIPs。

CCE 对 Kubernetes 1.29 版本的增强

在版本维护周期中，CCE会对Kubernetes 1.29版本进行定期的更新，并提供功能增强。

关于CCE集群版本的更新说明，请参见[补丁版本发布说明](#)。

参考链接

关于Kubernetes 1.29与其他版本的性能对比和功能演进的更多信息，请参考：[Kubernetes v1.29 Release Notes](#)

5.1.2.2 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](#)
- [新增特性及特性增强](#)
- [API变更与弃用](#)
- [特性门禁及命令行参数](#)
- [CCE对Kubernetes 1.28版本的增强](#)
- [参考链接](#)

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，但仍然存在一些问题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[索引的回退限制](#)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，你可以检查 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。

- 逐索引的回退限制

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。此时逐索引的回退限制就显得有用。

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[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达到次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[逐索引的回退限制](#)。
- 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`。

CCE 对 Kubernetes 1.28 版本的增强

在版本维护周期中，CCE会对Kubernetes 1.28版本进行定期的更新，并提供功能增强。

关于CCE集群版本的更新说明，请参见[CCE集群版本发布说明](#)。

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](#)

5.1.2.3 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版本相对于1.25版本所做的变更说明。

索引

- [主要特性](#)
- [弃用和移除](#)
- [CCE对Kubernetes 1.27版本的增强](#)
- [参考链接](#)

主要特性

Kubernetes 1.27版本

- **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。如果你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，序号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](#)。

Kubernetes 1.26版本

- 移除CRI v1alpha2

Kubernetes 1.26版本不再支持CRI v1alpha2，请使用v1（要求containerd版本 \geq 1.5.0）。这意味着Kubernetes 1.26将不支持containerd 1.5.x 及更早的版本；需要升级到containerd 1.6.x或更高版本后，才能将该节点的kubelet升级到1.26。

📖 说明

CCE目前使用的containerd版本为1.6.14，已满足要求。如存量的节点不满足containerd版本要求，请将节点重置为最新版本。

- 动态资源分配 Alpha API

在Kubernetes 1.26版本，新增[动态资源分配](#)功能，用于Pod之间和Pod内部容器之间请求和共享资源，支持用户提供参数初始化资源。该功能尚处于alpha阶段，需要启用DynamicResourceAllocation特性门禁和resource.k8s.io/v1alpha1 API组，需要为要管理的特定资源安装驱动程序。更多信息，请参见[Kubernetes 1.26: 动态资源分配 Alpha API](#)。

- 节点非体面关闭进入Beta阶段

在Kubernetes 1.26 中，节点非体面关闭特性是Beta版，默认被启用。当kubelet的节点关闭管理器可以检测到即将到来的节点关闭操作时，节点关闭才被认为是体面的。详情请参见[处理节点非体面关闭](#)。

- 支持在挂载时将Pod fsGroup传递给CSI驱动程序

将fsGroup委托给CSI驱动程序管理首先在Kubernetes 1.22中作为Alpha特性引入，并在Kubernetes 1.25中进阶至Beta状态。该特性在Kubernetes 1.26已进入正式发布阶段，详情请参见[将卷权限和所有权更改委派给CSI驱动程序](#)。

- Pod调度就绪态

Kubernetes 1.26引入了一个新的Pod特性schedulingGates，可以让调度器感知到何时可以进行Pod调度。详情请参见[Pod调度就绪态](#)。

- CPU Manager正式发布

CPU管理器是kubelet的一部分，从Kubernetes 1.10[进阶至 Beta](#)，能够将独占CPU分配给容器。该特性在Kubernetes 1.26已进入稳定阶段，详情请参见[控制节点上的CPU管理策略](#)。

- Kubernetes中流量工程的进步

[优化内部节点本地流量](#)和[支持EndpointSlice终止状况](#)升级为正式发布版本，[ProxyTerminatingEndpoints](#)功能升级为Beta版本。

- 支持跨命名空间存储数据源

Kubernetes 1.26允许在源数据属于不同的命名空间时为PersistentVolumeClaim指定数据源。当前该特性处于Alpha阶段，详情请参见[跨命名空间数据源](#)。

- 可追溯的默认StorageClass进入Beta阶段

Kubernetes 1.25引入了一个Alpha特性来更改默认StorageClass被分配到PersistentVolumeClaim (PVC) 的方式。启用此特性后，您不再需要先创建默认

StorageClass，再创建PVC来分配类。此外，任何未分配StorageClass的PVC都可以在后续被更新。此特性在Kubernetes 1.26 中已进入Beta阶段，详情请参见[可追溯的默认StorageClass赋值](#)。

- PodDisruptionBudget支持指定不健康Pod的驱逐策略
Kubernetes 1.26允许针对[PodDisruptionBudget](#) (PDB) 指定不健康Pod驱逐策略，这有助于在节点执行管理操作期间保持可用性。当前该特性处于Beta阶段，详情请参见[不健康的Pod驱逐策略](#)。
- 支持设置水平伸缩Pod控制器的数量
kube-controller-manager支持flag `--concurrent-horizontal-pod-autoscaler-syncks`设置水平伸缩Pod控制器的worker数量。详情请参见[集群配置管理](#)。

弃用和移除

Kubernetes 1.27版本

- 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 CSI Migration 特性门禁将在 v1.27 中被移除。
- 在Kubernetes 1.27版本，移除 [CSInlineVolume](#) 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 [CSInlineVolume](#) 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，你可以为 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。

Kubernetes 1.26版本

- 移除v2beta2版本的HorizontalPodAutoscaler API
HorizontalPodAutoscaler的autoscaling/v2beta2 API版本将不再在1.26版本中提供，详情请参见[各发行版本中移除的API](#)。用户应迁移至autoscaling/v2版本的API。
- 移除v1beta1版本的流量控制API组
在Kubernetes 1.26版本后，开始不再提供flowcontrol.apiserver.k8s.io/v1beta1 API版本的FlowSchema和PriorityLevelConfiguration，详情请参见[各发行版本中移除的API](#)。但此API从Kubernetes 1.23版本开始，可以使用flowcontrol.apiserver.k8s.io/v1beta2；从Kubernetes 1.26版本开始，可以使用flowcontrol.apiserver.k8s.io/v1beta3。
- 存储驱动的弃用和移除，移除云服务厂商的in-tree卷驱动。
- 移除kube-proxy userspace模式
在Kubernetes 1.26版本，Userspace代理模式已被移除，已弃用的Userspace代理模式不再受Linux或Windows支持。Linux用户应使用Iptables或IPVS，Windows用户应使用Kernelspace，现在使用--mode userspace会失败。
 - Windows winkernel kube-proxy不再支持Windows HNS v1 APIs。
- 弃用--prune-whitelist标志
在Kubernetes 1.26版本，为了支持[Inclusive Naming Initiative](#)，--prune-whitelist标志将被**弃用**，并替换为--prune-allowlist，该标志在未来将彻底移除。
- 移除动态Kubelet配置
DynamicKubeletConfig特性门禁移除，通过API动态更新节点上的Kubelet配置。在Kubernetes 1.24版本中从Kubelet移除相关代码，在Kubernetes 1.26版本从APIServer移除相关代码，移除该逻辑有助于简化代码提升可靠性，推荐方式是修改Kubelet配置文件然后重启Kubelet。更多信息，请参见[在Kubernetes 1.26版本从APIServer移除相关代码](#)。
- 弃用kube-apiserver命令行参数
在Kubernetes 1.26版本，正式标记**弃用 --master-service-namespace** 命令行参数，它对APIServer没有任何效果。

- 弃用kubectl run命令行参数
在Kubernetes 1.26版本，kubectl run未使用的几个子命令将被标记为**弃用**，并在未来某个版本移除，包括--cascade、--filename、--force、--grace-period、--kustomize、--recursive、--timeout、--wait等这些子命令。
- 移除与日志相关的原有命令行参数
在Kubernetes 1.26版本，将**移除**一些与日志相关的命令行参数，这些参数在之前的版本已被**弃用**。

CCE 对 Kubernetes 1.27 版本的增强

在版本维护周期中，CCE会对Kubernetes 1.27版本进行定期的更新，并提供功能增强。

关于CCE集群版本的更新说明，请参见[CCE集群版本发布说明](#)。

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](#)
- [Kubernetes v1.26 Release Notes](#)

5.1.2.4 Kubernetes 1.25 版本说明

云容器引擎（CCE）严格遵循社区一致性认证。本文介绍Kubernetes 1.25版本相对于1.23版本所做的变更说明。

索引

- [主要特性](#)
- [弃用和移除](#)
- [CCE对Kubernetes 1.25版本的增强](#)
- [参考链接](#)

主要特性

Kubernetes 1.25版本

- Pod Security Admission进入稳定阶段，并移除PodSecurityPolicy
PodSecurityPolicy被废弃，并提供Pod Security Admission取代，具体的迁移方法可参见[从PodSecurityPolicy迁移到内置的PodSecurity准入控制器](#)。
- Ephemeral Containers进入稳定阶段
临时容器是在现有的Pod中存在有限时间的容器。它对故障排除特别有用，特别是当需要检查另一个容器，但因为该容器已经崩溃或其镜像缺乏调试工具不能使用kubectl exec时。
- 对cgroups v2的支持进入稳定阶段
Kubernetes支持cgroups v2，与cgroups v1相比提供了一些改进，详情请参见[cgroups v2](#)。
- SeccompDefault提升到Beta状态

如果要开启该特性，需要给kubelet增加启动参数为--seccomp-default=true，这样会默认开启seccomp为RuntimeDefault，提升整个系统的安全。1.25集群将不再支持使用注解“seccomp.security.alpha.kubernetes.io/pod”和“container.seccomp.security.alpha.kubernetes.io/annotation”来使用seccomp，请使用pod或container中“securityContext.seccompProfile”字段替代，详情请参见[为Pod或容器配置安全上下文](#)。

📖 说明

特性开启后可能应用所需的系统调用会被runtime限制，所以开启后应确保在测试环境调试，不会对应用造成影响。

- 网络策略中的EndPort进入稳定阶段
Network Policy中的EndPort已进入稳定状态，该特性于1.21版本合入。主要是在NetworkPolicy新增EndPort，可以指定一个Port范围，避免声明每一个Port。
- 本地临时容器存储容量隔离进入稳定阶段
本地临时存储容量隔离功能提供了对Pod之间本地临时存储容量隔离的支持，如EmptyDir。因此，如果一个Pod对本地临时存储容量的消耗超过该限制，就可以通过驱逐Pod来硬性限制其对共享资源的消耗。
- CRD验证表达式语言升级为Beta阶段
CRD验证表达式语言已升级为 beta 版本，这使得声明如何使用[通用表达式语言 \(CEL\)](#) 验证自定义资源成为可能。请参考[验证规则](#)指导。
- 引入KMS v2 API
在Kubernetes 1.25版本，引入KMS v2 alpha1 API以提升性能，实现轮替与可观察性改进。此API使用AES-GCM替代了AES-CBC，通过DEK实现静态数据加密（Kubernetes Secrets），此过程中无需您额外操作，且支持通过AES-GCM和AES-CBC进行读取。更多信息，请参考[使用 KMS provider进行数据加密指南](#)。
- Pod新增网络就绪状况
Kubernetes 1.25引入了对kubelet所管理的新的Pod状况PodHasNetwork的Alpha支持，该状况位于Pod的status字段中。详情请参见[Pod网络就绪](#)。
- 应用滚动上线所用的两个特性进入稳定阶段
 - 在Kubernetes 1.25版本，StatefulSet的minReadySeconds进入稳定阶段，允许每个Pod等待一段预期时间来减缓StatefulSet的滚动上线。更多信息，请参见[最短就绪秒数](#)。
 - 在Kubernetes 1.25版本，DaemonSet的maxSurge进入稳定阶段，允许DaemonSet工作负载在滚动上线期间在一个节点上运行同一 Pod的多个实例，有助于将DaemonSet的停机时间降到最低。DaemonSet不允许maxSurge和hostPort同时使用，因为两个活跃的Pod无法共享同一节点的相同端口。更多信息，请参见[DaemonSet工作负载滚动上线](#)。
- 对使用用户命名空间运行Pod提供Alpha支持
对使用user namespace运行Pod提供alpha支持，将Pod内的root用户映射到容器外的非零ID，使得从容器角度看是root身份运行，而从主机角度看是常规的非特权用户。目前尚处于内测阶段，需要开启特性门控UserNamespacesStatelessPodsSupport，且要求容器运行时必须能够支持此功能。更多信息，请参见[对使用user namespace运行Pod提供alpha支持](#)。

Kubernetes 1.24版本

- 从kubelet中删除 Dockershim

Dockershim自1.20版本被标废弃以来，在1.24版本正式从Kubelet代码中移除。如果还想使用Docker作为容器运行时的话，需要切换到cri-dockerd，或者使用其他支持CRI的运行时比如Containerd/CRI-O等。

从Docker Engine 切换到Containerd的流程请参见[将节点容器引擎从Docker迁移到Containerd](#)。

📖 说明

您需要注意排查是否有agent或者应用强依赖Docker Engine的，比如在代码中使用docker ps, docker run, docker inspect等，需要注意兼容多种runtime，以及切换到标准cri接口。

- Beta APIs默认关闭

在社区移除一些长期Beta API的过程中发现，90%的集群管理员并没有关心Beta API默认开始，其实Beta特性是不推荐在生产环境中使用，但是因为默认的打开策略，导致这些API在生产环境中都被默认开启，这样会因为Beta特性的bug带来一些风险，以及升级的迁移的风险。所以在1.24版本开始，Beta API默认关闭，之前已经默认开启的Beta API会保持默认开启。

- 支持OpenAPI v3

在Kubernetes 1.24版本后，OpenAPI V3默认开启。

- 存储容量跟踪特性进入稳定阶段

在Kubernetes 1.24版本后，CSIStorageCapacity API支持显示当前可用的存储大小，确保Pod调度到足够存储容量的节点上，减少Volumes创建和挂载失败导致的Pod调度延迟，详细信息请参见[存储容量](#)。

- gRPC 探针升级到Beta阶段

在Kubernetes 1.24版本后，gRPC探针进入Beta，默认可用特性门控参数GRPCContainerProbe，使用方式请参见[配置探针](#)。

- 特性门控LegacyServiceAccountTokenNoAutoGeneration默认启用

LegacyServiceAccountTokenNoAutoGeneration特性门控进入beta状态，默认为开启状态，开启后将不再为Service Account自动生成Secret Token。如果需要长期使用永不过期的Token，需要自己新建Secrets并挂载，详情请参见[服务账号令牌Secret](#)。

- 避免 IP 分配给服务的冲突

Kubernetes 1.24引入了一项新功能，允许[为服务的静态IP地址分配软保留范围](#)。通过手动启用此功能，集群将从服务IP地址池中自动分配IP，从而降低冲突风险。

- 基于Go 1.18编译

在Kubernetes 1.24版本后，Kubernetes基于Go 1.18编译，默认不再支持SHA-1哈希算法验证证书签名，例如SHA1WithRSA、ECDSAWithSHA1算法，推荐使用SHA256算法生成的证书进行认证。

- StatefulSet支持设置最大不可用副本数

在Kubernetes 1.24版本后，StatefulSets支持可配置maxUnavailable参数，使得滚动更新时可以更快地停止Pods。

- 节点非体面关闭进入Alpha阶段

在Kubernetes 1.24中，节点非体面关闭特性是Alpha版。当kubelet的节点关闭管理器可以检测到即将到来的节点关闭操作时，节点关闭才被认为是体面的。详情请参见[处理节点非体面关闭](#)。

弃用和移除

Kubernetes 1.25版本

- 清理iptables链的所有权

Kubernetes通常创建iptables链来确保这些网络数据包到达，这些iptables链及其名称属于Kubernetes内部实现的细节，仅供内部使用场景，目前有些组件依赖于这些内部实现细节，Kubernetes总体上不希望支持某些工具依赖这些内部实现细节。详细信息，请参见[Kubernetes的iptables链不是API](#)。

在Kubernetes 1.25版本后，Kubelet通过IPTablesCleanup特性门控分阶段完成迁移，是为了不在NAT表中创建iptables链，例如KUBE-MARK-DROP、KUBE-MARK-MASQ、KUBE-POSTROUTING。关于清理iptables链所有权的信息，请参见[清理IPTables链的所有权](#)。

- 存储驱动的弃用和移除，移除云服务厂商的in-tree卷驱动。

Kubernetes 1.24版本

- 在Kubernetes 1.24版本后，Service.Spec.LoadBalancerIP被弃用，因为它无法用于双栈协议。请使用自定义annotation。
- 在Kubernetes 1.24版本后，kube-apiserver移除参数--address、--insecure-bind-address、--port、--insecure-port=0。
- 在Kubernetes 1.24版本后，kube-controller-manager和kube-scheduler移除启动参数--port=0和--address。
- 在Kubernetes 1.24版本后，kube-apiserver --audit-log-version和--audit-webhook-version仅支持audit.k8s.io/v1，Kubernetes 1.24移除audit.k8s.io/v1[alpha|beta]1，只能使用audit.k8s.io/v1。
- 在Kubernetes 1.24版本后，kubelet移除启动参数--network-plugin，仅当容器运行环境设置为Docker时，此特定于Docker的参数才有效，并会随着Dockershim一起删除。
- 在Kubernetes 1.24版本后，动态日志清理功能已经被废弃，并在Kubernetes 1.24版本移除。该功能引入了一个日志过滤器，可以应用于所有Kubernetes系统组件的日志，以防止各种类型的敏感信息通过日志泄漏。此功能可能导致日志阻塞，所以废弃，更多信息请参见[Dynamic log sanitization](#)和 [KEP-1753](#)。
- VolumeSnapshot v1beta1 CRD在Kubernetes 1.20版本中被废弃，在Kubernetes 1.24版本中移除，需改用v1版本。
- 在Kubernetes 1.24版本后，移除自1.11版本就废弃的service annotation tolerate-unready-endpoints，使用Service.spec.publishNotReadyAddresses代替。
- 在Kubernetes 1.24版本后，废弃metadata.clusterName字段，并将在下一个版本中删除。
- Kubernetes 1.24及以后的版本，去除了kube-proxy监听NodePort的逻辑，在NodePort与内核net.ipv4.ip_local_port_range范围有冲突的情况下，可能会导致偶发的TCP无法连接的情况，导致健康检查失败、业务异常等问题。升级前，请确保集群没有NodePort端口与任意节点net.ipv4.ip_local_port_range范围存在冲突。更多信息，请参见[Kubernetes社区PR](#)。

CCE 对 Kubernetes 1.25 版本的增强

在版本维护周期中，CCE会对Kubernetes 1.25版本进行定期的更新，并提供功能增强。

关于CCE集群版本的更新说明，请参见[CCE集群版本发布说明](#)。

参考链接

关于Kubernetes 1.25与其他版本的性能对比和功能演进的更多信息，请参考：

- [Kubernetes v1.25 Release Notes](#)
- [Kubernetes v1.24 Release Notes](#)

5.1.2.5 Kubernetes 1.23 版本说明

云容器引擎（CCE）严格遵循社区一致性认证。本文介绍CCE发布Kubernetes 1.23版本所做的变更说明。

资源变更与弃用

社区1.23 ReleaseNotes

- FlexVolume废弃，建议使用CSI。
- HorizontalPodAutoscaler v2版本GA，HorizontalPodAutoscaler API v2在1.23版本中逐渐稳定。不建议使用HorizontalPodAutoscaler v2beta2 API，建议使用新的v2版本API。
- [PodSecurity](#)支持beta，PodSecurity替代废弃的PodSecurityPolicy，PodSecurity是一个准入控制器，它根据设置实施级别的特定命名空间标签在命名空间中的Pod上实施Pod安全标准。在1.23中PodSecurity默认启用。

社区1.22 ReleaseNotes

- Ingress资源不再支持networking.k8s.io/v1beta1和extensions/v1beta1 API。如果使用旧版本API管理Ingress，会影响应用对外暴露服务，请尽快使用networking.k8s.io/v1替代。
- CustomResourceDefinition资源不再支持apiextensions.k8s.io/v1beta1 API。如果使用旧版本API创建自定义资源定义，会导致定义创建失败，进而影响调和（reconcile）该自定义资源的控制器，请尽快使用apiextensions.k8s.io/v1替代。
- ClusterRole、ClusterRoleBinding、Role和RoleBinding资源不再支持rbac.authorization.k8s.io/v1beta1 API。如果使用旧版本API管理RBAC资源，会影响应用的权限服务，甚至无法在集群内正常使用，请尽快使用rbac.authorization.k8s.io/v1替代。
- Kubernetes版本发布周期由一年4个版本变为一年3个版本。
- StatefulSets 支持minReadySeconds。
- 缩容时默认根据Pod uid排序随机选择删除Pod（LogarithmicScaleDown）。基于该特性，可以增强Pod被缩容的随机性，缓解由于Pod拓扑分布约束带来的问题。更多信息，请参见[KEP-2185](#)和[issues 96748](#)。
- [BoundServiceAccountTokenVolume](#)特性已稳定，该特性能够提升服务账号（ServiceAccount）Token的安全性，改变了Pod挂载Token的方式，Kubernetes 1.21及以上版本的集群中会默认开启。

参考链接

关于Kubernetes 1.23与其他版本的性能对比和功能演进的更多信息，请参考：

- [Kubernetes v1.23 Release Notes](#)
- [Kubernetes v1.22 Release Notes](#)

5.1.2.6（停止维护）Kubernetes 1.21 版本说明

云容器引擎（CCE）严格遵循社区一致性认证。本文介绍CCE发布Kubernetes 1.21版本所做的变更说明。

资源变更与弃用

社区1.21 ReleaseNotes

- CronJob现在已毕业到稳定状态，版本号变为batch/v1。
- 不可变的Secret和ConfigMap现在已升级到稳定状态。向这些对象添加了一个新的不可变字段，以拒绝更改。此拒绝可保护集群免受可能无意中中断应用程序的更新。因为这些资源是不可变的，kubelet不会监视或轮询更改。这减少了kube-apiserver的负载，提高了可扩展性和性能。更多信息，请参见[Immutable ConfigMaps](#)。
- 优雅节点关闭现在已升级到测试状态。通过此更新，kubelet可以感知节点关闭，并可以优雅地终止该节点的Pod。在此更新之前，当节点关闭时，其Pod没有遵循预期的终止生命周期，这导致了工作负载问题。现在kubelet可以通过systemd检测即将关闭的系统，并通知正在运行的Pod，使它们优雅地终止。
- 具有多个容器的Pod现在可以使用kubectl.kubernetes.io/默认容器注释为kubectl命令预选容器。
- PodSecurityPolicy废弃，详情请参见<https://kubernetes.io/blog/2021/04/06/podsecuritypolicy-deprecation-past-present-and-future/>。
- [BoundServiceAccountTokenVolume](#)特性进入Beta，该特性能够提升服务账号（ServiceAccount）Token的安全性，改变了Pod挂载Token的方式，Kubernetes 1.21及以上版本的集群中会默认开启。

社区1.20 ReleaseNotes

- API优先级和公平性已达到测试状态，默认启用。这允许kube-apiserver按优先级对传入请求进行分类。更多信息，请参见[API Priority and Fairness](#)。
- 修复 exec probe timeouts不生效的BUG，在此修复之前，exec 探测器不考虑timeoutSeconds 字段。相反，探测将无限期运行，甚至超过其配置的截止日期，直到返回结果。通过此更改，如果未指定值，将使用默认值，默认值为1秒。如果探测时间超过一秒，可能会导致应用健康检查失败。请再升级时确定使用该特性的应用更新timeoutSeconds字段。新引入的 ExecProbeTimeout 特性门控所提供的修复使集群操作员能够恢复到以前的行为，但这种行为将在后续版本中锁定并删除。
- RuntimeClass已达到稳定状态。RuntimeClass资源提供了一种机制，用于支持集群中的多个运行时，并将有关该容器运行时的信息公开到控制平面。
- kubectl调试已达到测试状态。kubectl调试直接从kubectl提供对常见调试 workflow 的支持。
- Dockershim在1.20被标记为废弃，目前您可以继续在集群中使用Docker。该变动与集群所使用的容器镜像（Image）无关。您依然可以使用Docker构建您的镜像。更多信息，请参见[Dockershim Deprecation FAQ](#)。

参考链接

关于Kubernetes 1.21与其他版本的性能对比和功能演进的更多信息，请参考：

- [Kubernetes v1.21 Release Notes](#)
- [Kubernetes v1.20 Release Notes](#)

5.1.2.7（停止维护）Kubernetes 1.19 版本说明

云容器引擎（CCE）严格遵循社区一致性认证。本文介绍CCE发布Kubernetes 1.19版本所做的变更说明。

资源变更与弃用

社区1.19 ReleaseNotes

- 增加对vSphere in-tree卷迁移至vSphere CSI驱动的支持。in-tree vSphere Volume插件将不再使用，并在将来的版本中删除。
- `apiextensions.k8s.io/v1beta1`已弃用，推荐使用`apiextensions.k8s.io/v1`。
- `apiregistration.k8s.io/v1beta1`已弃用，推荐使用`apiregistration.k8s.io/v1`。
- `authentication.k8s.io/v1beta1`、`authorization.k8s.io/v1beta1`已弃用，1.22将移除，推荐使用`authentication.k8s.io/v1`、`authorization.k8s.io/v1`。
- `autoscaling/v2beta1`已弃用，推荐使用`autoscaling/v2beta2`。
- `coordination.k8s.io/v1beta1`在1.19中已弃用，1.22将移除，推荐使用`v1`。
- Kube-apiserver: `componentstatus` API已弃用。
- Kubeadm: `kubeadm config view`命令已被弃用，并将在未来版本中删除，请使用`kubectrl get cm -o yaml -n kube-system kubeadm-config`来直接获取kubeadm配置。
- Kubeadm: 弃用`kubeadm alpha kubelet config enable-dynamic`命令。
- Kubeadm: `kubeadm alpha certs renew`命令`--use-api`参数已弃用。
- Kubernetes不再支持构建hyperkube镜像。
- Remove `--export` flag from `kubectrl get` command - `kubectrl get`中移除 `--export` 参数。
- alpha特性“ResourceLimitsPriorityFunction”已完全删除。
- `storage.k8s.io/v1beta1`已弃用，推荐使用`storage.k8s.io/v1`。

社区1.18 ReleaseNotes

- kube-apiserver
 - `apps/v1beta1` and `apps/v1beta2`下所有资源不再提供服务，使用`apps/v1`替代。
 - `extensions/v1beta1`下`daemonsets`，`deployments`，`replicasets`不再提供服务，使用`apps/v1`替代。
 - `extensions/v1beta1`下`networkpolicies`不再提供服务，使用`networking.k8s.io/v1`替代。
 - `extensions/v1beta1`下`podsecuritypolicies`不再提供服务，使用`policy/v1beta1`替代。

- kubelet
 - --redirect-container-streaming不推荐使用，v1.20会正式废弃。
 - 资源度量端点 /metrics/resource/v1alpha1以及此端点下的所有度量标准均已弃用。请转换为端点 /metrics/resource下的度量标准：
 - scrape_error --> scrape_error
 - node_cpu_usage_seconds_total --> node_cpu_usage_seconds
 - node_memory_working_set_bytes --> node_memory_working_set_bytes
 - container_cpu_usage_seconds_total --> container_cpu_usage_seconds
 - container_memory_working_set_bytes --> container_memory_working_set_bytes
 - scrape_error --> scrape_error
 - 在将来的发行版中，kubelet将不再根据CSI规范创建CSI NodePublishVolume目标目录。可能需要相应地更新CSI驱动程序，以正确创建和处理目标路径。
 - kube-proxy
 - --healthz-port和--metrics-port参数不建议使用，请使用--healthz-bind-address和--metrics-bind-address。
 - 增加EndpointSliceProxying功能选项以控制kube-proxy中EndpointSlices的使用，默认情况下已禁用此功能。
 - kubeadm
 - kubeadm upgrade node的--kubelet-version参数已弃用，将在后续版本中删除。
 - kubeadm alpha certs renew命令中--use-api参数已弃用。
 - kube-dns已弃用，在将来的版本中将不再受支持。
 - kubeadm-config ConfigMap中存在的ClusterStatus结构体已废弃，将在后续版本中删除。
 - kubectl
 - --dry-run不建议使用boolean和unset values，新版本中server|client|none会被使用。
 - kubectl apply --server-dry-run已弃用，替换为--dry-run=server。
 - add-ons
- 删除cluster-monitoring插件。
- kube-scheduler
 - scheduling_duration_seconds指标已弃用。
 - scheduling_algorithm_predicate_evaluation_seconds和scheduling_algorithm_priority_evaluation_seconds指标已弃用，使用framework_extension_point_duration_seconds[extension_point="Filter"]和framework_extension_point_duration_seconds[extension_point="Score"]替代。
 - 调度器策略AlwaysCheckAllPredicates已弃用。

- 其他变化
 - k8s.io/node-api组件不再更新。作为替代，可以使用位于k8s.io/api中的RuntimeClass类型和位于k8s.io/client-go中的generated clients。
 - 已从apiserver_request_total中删除“client”标签。

参考链接

关于Kubernetes 1.19与其他版本的性能对比和功能演进的更多信息，请参考：

- [Kubernetes v1.19.0 Release Notes](#)
- [Kubernetes v1.18.0 Release Notes](#)

5.1.2.8（停止维护）Kubernetes 1.17 版本说明

云容器引擎（CCE）严格遵循社区一致性认证。本文介绍CCE发布Kubernetes 1.17版本所做的变更说明。

资源变更与弃用

- apps/v1beta1和apps/v1beta2下所有资源不再提供服务，使用apps/v1替代。
- extensions/v1beta1下daemonsets、deployments、replicasets不再提供服务，使用apps/v1替代。
- extensions/v1beta1下networkpolicies不再提供服务，使用networking.k8s.io/v1替代。
- extensions/v1beta1下podsecuritypolicies不再提供服务，使用policy/v1beta1替代。
- extensions/v1beta1 ingress v1.20版本不再提供服务，当前可使用networking.k8s.io/v1beta1。
- scheduling.k8s.io/v1beta1 and scheduling.k8s.io/v1alpha1下的PriorityClass计划在1.17不再提供服务，迁移至scheduling.k8s.io/v1。
- events.k8s.io/v1beta1中event series.state字段已废弃，将在1.18版本中移除。
- apiextensions.k8s.io/v1beta1下CustomResourceDefinition已废弃，将在1.19不在提供服务，使用apiextensions.k8s.io/v1。
- admissionregistration.k8s.io/v1beta1 MutatingWebhookConfiguration和ValidatingWebhookConfiguration已废弃，将在1.19不在提供服务，使用admissionregistration.k8s.io/v1替换。
- rbac.authorization.k8s.io/v1alpha1 and rbac.authorization.k8s.io/v1beta1被废弃，使用rbac.authorization.k8s.io/v1替代，v1.20会正式停止服务。
- storage.k8s.io/v1beta1 CSINode object废弃并会在未来版本中移除。

其他废弃和移除

- 移除OutOfDisk node condition，改为使用DiskPressure。
- scheduler.alpha.kubernetes.io/critical-pod annotation已被移除，如需要改为设置priorityClassName。
- beta.kubernetes.io/os和beta.kubernetes.io/arch在1.14版本中已经废弃，计划在1.18版本中移除。

- 禁止通过--node-labels设置kubernetes.io和k8s.io为前缀的标签，老版本中kubernetes.io/availablezone该label在1.17中移除，整改为failure-domain.beta.kubernetes.io/zone获取AZ信息。
- beta.kubernetes.io/instance-type被废弃，使用node.kubernetes.io/instance-type替代。
- 移除{kubelet_root_dir}/plugins路径。
- 移除内置集群角色system:csi-external-provisioner和system:csi-external-attacher。

参考链接

关于Kubernetes 1.17与其他版本的性能对比和功能演进的更多信息，请参考：

- [Kubernetes v1.17.0 Release Notes](#)
- [Kubernetes v1.16.0 Release Notes](#)

5.1.2.9（停止维护）Kubernetes 1.15 版本说明

云容器引擎（CCE）严格遵循社区一致性认证。本文介绍CCE发布Kubernetes 1.15版本所做的变更说明。

为了能够更好地方便您使用容器服务，确保您使用稳定又可靠的Kubernetes版本，请您务必在维护周期结束之前升级您的Kubernetes集群。

版本说明

CCE针对Kubernetes v1.15版本提供了全链路的组件优化和升级，v1.15版本包含两个小版本，即v1.15.11和v1.15.6-r1。

资源变更与弃用

- extensions/v1beta1中Ingress已弃用，1.19正式暂停使用，迁移到networking.k8s.io/v1beta1
- extensions/v1beta1中NetworkPolicy 1.16正式暂停使用，迁移到networking.k8s.io/v1
- extensions/v1beta1中PodSecurityPolicy 1.16正式暂停使用，迁移到policy/v1beta1
- extensions/v1beta1、apps/v1beta1或apps/v1beta2的DaemonSet、Deployment、和ReplicaSet，迁移至apps/v1，1.16版本暂停使用
- PriorityClass升级到scheduling.k8s.io/v1，scheduling.k8s.io/v1beta1和scheduling.k8s.io/v1alpha1 1.17正式废弃
- events.k8s.io/v1beta1 Event API中series.state字段废弃，将在1.18版本中移除

参考链接

社区v1.13与v1.15版本之间的CHANGELOG

- v1.14到v1.15的变化：
<https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.15.md>

- v1.13到v1.14的变化：
<https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.14.md>

5.1.2.10（停止维护）Kubernetes 1.13 版本说明

云容器引擎（CCE）严格遵循社区一致性认证。本文介绍CCE发布Kubernetes 1.13版本所做的变更说明。

表 5-1 v1.13 版本集群说明

Kubernetes版本 (CCE增强版)	版本说明
v1.13.10-r0	主要特性: <ul style="list-style-type: none">• CCE集群支持添加ARM节点• 负载均衡支持设置名称• 4层负载均衡支持健康检查，7层负载均衡支持健康检查/分配策略/会话保持• CCE集群支持创建裸金属节点（容器隧道网络）• 支持AI加速型节点（搭载海思Ascend 310 AI处理器），适用于图像识别、视频处理、推理计算以及机器学习等场景• 支持配置docker baseSize• 支持命名空间亲和调度• 支持节点数据盘划分用户空间• 支持集群cpu管理策略• 支持集群下的节点跨子网（容器隧道网络）
v1.13.7-r0	主要特性: <ul style="list-style-type: none">• Kubernetes同步社区1.13.7版本• 支持网络平面（NetworkAttachmentDefinition）

参考链接

社区v1.11与v1.13版本之间的CHANGELOG

- v1.12到v1.13的变化：
<https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.13.md>
- v1.11到v1.12的变化：
<https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.12.md>

5.1.2.11（停止维护）Kubernetes 1.11 版本说明

云容器引擎（CCE）严格遵循社区一致性认证。本文介绍CCE发布Kubernetes 1.11版本所做的变更说明。

表 5-2 v1.11 版本集群说明

Kubernetes版本 (CCE增强版)	版本说明
v1.11.7-r2	主要特性: <ul style="list-style-type: none">GPU支持V100类型集群支持权限管理
v1.11.7-r0	主要特性: <ul style="list-style-type: none">Kubernetes同步社区1.11.7版本支持创建节点池（nodepool），虚拟机/鲲鹏ARM集群均支持CCE集群支持创建裸金属节点（VPC网络），支持裸金属和虚机混合部署GPU支持V100类型1.11集群对接AOM告警通知机制Service支持访问类型切换支持服务网段集群支持自定义每个节点分配的IP数（IP分配）
v1.11.3-r2	主要特性: <ul style="list-style-type: none">集群支持IPv6双栈ELB负载均衡支持源IP跟后端服务会话保持
v1.11.3-r1	主要特性: <ul style="list-style-type: none">Ingress的URL匹配支持Perl语法的正则表达式
v1.11.3-r0	主要特性: <ul style="list-style-type: none">Kubernetes同步社区1.11.3版本集群控制节点支持多可用区容器存储支持对接SFS Turbo极速文件存储

参考链接

社区v1.9与v1.11版本之间的CHANGELOG

- v1.10到v1.11的变化：
<https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.11.md>
- v1.9到v1.10的变化：

<https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.10.md>

5.1.2.12（停止维护）Kubernetes 1.9 及之前版本说明

云容器引擎（CCE）严格遵循社区一致性认证。本文介绍CCE发布Kubernetes 1.9及之前版本所做的变更说明。

表 5-3 v1.9 及之前版本集群说明

Kubernetes版本 (CCE增强版)	版本说明
v1.9.10-r2	主要特性: <ul style="list-style-type: none">ELB负载均衡支持源IP跟后端服务会话保持
v1.9.10-r1	主要特性: <ul style="list-style-type: none">支持对接SFS存储支持Service自动创建二代ELB支持公网二代ELB透传源IP支持设置节点最大实例数maxPods
v1.9.10-r0	主要特性: <ul style="list-style-type: none">kubernetes对接ELB/Ingress, 新增流控机制Kubernetes同步社区1.9.10版本支持Kubernetes RBAC能力授权 问题修复: <ul style="list-style-type: none">修复操作系统cgroup内核BUG导致概率出现的节点内存泄漏问题
v1.9.7-r1	主要特性: <ul style="list-style-type: none">增强PVC和PV事件的上报机制, PVC详情页支持查看事件支持对接第三方认证系统集群支持纳管EulerOS2.3的物理机数据盘支持用户自定义分配比例裸金属场景支持对接EVS云硬盘存储裸金属场景下支持IB网卡裸金属场景支持通过CM-v3接口创建节点

Kubernetes版本 (CCE增强版)	版本说明
v1.9.7-r0	<p>主要特性:</p> <ul style="list-style-type: none"> ● 新建集群的Docker版本升级到1706 ● 支持DNS级联 ● 支持插件化管理 ● Kubernetes同步社区1.9.7版本 ● 支持7层ingress的https功能 ● 有状态工作负载支持迁移调度更新升级
v1.9.2-r3	<p>主要特性:</p> <ul style="list-style-type: none"> ● 集群支持创建/纳管CentOS7.4操作系统的节点 ● kubernetes的Service支持对接DNAT网关服务 ● NetworkPolicy能力开放 ● 增强型ELB支持Service配置多个端口 <p>问题修复:</p> <ul style="list-style-type: none"> ● 修复kubernetes资源回收过程中连不上kube-apiserver导致pod残留的问题 ● 修复节点弹性扩容数据不准确的问题
v1.9.2-r2	<p>主要特性:</p> <ul style="list-style-type: none"> ● 经典型ELB支持自定义健康检查端口 ● 经典型ELB性能优化 ● ELB四层负载均衡支持修改Service的端口 <p>问题修复:</p> <ul style="list-style-type: none"> ● 修复网络插件防止健康检查概率死锁问题 ● 修复高可用集群haproxy连接数限制问题
v1.9.2-r1	<p>主要特性:</p> <ul style="list-style-type: none"> ● Kubernetes同步社区1.9.2版本 ● 集群节点支持CentOS 7.1操作系统 ● 支持GPU节点, 支持GPU资源限制 ● 支持web-terminal插件
v1.7.3-r13	<p>主要特性:</p> <ul style="list-style-type: none"> ● 新建集群的Docker版本升级到1706 ● 支持DNS级联 ● 支持插件化管理 ● 增强PVC和PV事件的上报机制 ● 裸金属场景支持对接OBS对象存储

Kubernetes版本 (CCE增强版)	版本说明
v1.7.3-r12	<p>主要特性:</p> <ul style="list-style-type: none"> ● 集群支持创建/纳管CentOS7.4操作系统的节点 ● kubernetes的Service支持对接DNAT网关服务 ● NetworkPolicy能力开放 ● 增强型ELB支持Service配置多个端口 <p>问题修复:</p> <ul style="list-style-type: none"> ● 修复kubernetes资源回收过程中连不上kube-apiserver导致pod残留的问题 ● 修复节点弹性扩容数据不准确的问题 ● 事件老化周期提示修正: 集群老化周期为1小时
v1.7.3-r11	<p>主要特性:</p> <ul style="list-style-type: none"> ● 经典型ELB支持自定义健康检查端口 ● 经典型ELB性能优化 ● ELB四层负载均衡支持修改Service的端口 ● 支持删除命名空间 ● 支持EVS云硬盘存储解绑 ● 支持配置迁移策略 <p>问题修复:</p> <ul style="list-style-type: none"> ● 修复网络插件防止健康检查概率死锁问题 ● 修复高可用集群haproxy连接数限制问题
v1.7.3-r10	<p>主要特性:</p> <ul style="list-style-type: none"> ● 容器网络支持Overlay L2模式 ● 集群节点支持GPU类型虚拟机 ● 集群节点支持CentOS 7.1操作系统, 支持操作系统选择 ● Windows集群支持对接二代ELB ● 支持弹性文件服务SFS导入 ● 裸金属场景支持对接SFS文件存储
v1.7.3-r9	<p>主要特性:</p> <ul style="list-style-type: none"> ● 工作负载支持跨AZ部署 ● 容器存储支持OBS对象存储服务 ● 支持ELB L7负载均衡 ● Windows集群支持EVS存储 ● 裸金属场景支持devicemapper direct-lvm模式

Kubernetes版本 (CCE增强版)	版本说明
v1.7.3-r8	主要特性: <ul style="list-style-type: none"> ● 集群支持节点弹性扩容 ● 支持纳管ARM节点
v1.7.3-r7	主要特性: <ul style="list-style-type: none"> ● 容器隧道网络集群支持纳管SUSE 12sp2节点 ● docker支持direct-lvm模式挂载devicemapper ● 集群支持安装dashboard ● 支持创建Windows集群
v1.7.3-r6	主要特性: <ul style="list-style-type: none"> ● 集群存储对接原生EVS接口
v1.7.3-r5	主要特性: <ul style="list-style-type: none"> ● 支持创建HA高可靠集群 问题修复: <ul style="list-style-type: none"> ● 节点重启后容器网络不通
v1.7.3-r4	主要特性: <ul style="list-style-type: none"> ● 集群性能优化 ● 裸金属场景支持对接ELB
v1.7.3-r3	主要特性: <ul style="list-style-type: none"> ● 容器存储支持KVM虚拟机挂载
v1.7.3-r2	主要特性: <ul style="list-style-type: none"> ● 容器存储支持SFS文件存储 ● 工作负载支持自定义应用日志 ● 开放工作负载优雅缩容 问题修复: <ul style="list-style-type: none"> ● 修复容器存储AK/SK会过期的问题
v1.7.3-r1	主要特性: <ul style="list-style-type: none"> ● kube-dns支持外部域名解析
v1.7.3-r0	主要特性: <ul style="list-style-type: none"> ● Kubernetes同步社区1.7.3版本 ● 支持ELB负载均衡 ● 容器存储支持XEN虚拟机挂载 ● 容器存储支持EVS云硬盘存储

5.1.3 补丁版本发布记录

索引

- [v1.29版本](#)
- [v1.28版本](#)
- [v1.27版本](#)
- [v1.25版本](#)
- [v1.23版本](#)
- [v1.21版本](#)
- [v1.19版本](#)

v1.29 版本

表 5-4 v1.29 补丁版本发布说明

CCE 集群补丁版本号	Kubernetes社区版本号	特性更新	优化增强	安全漏洞修复
v1.29.1-r0	v1.29.1	首次发布CCE v1.29集群，有关更多信息请参见 Kubernetes 1.29版本说明 。	-	-

v1.28 版本

表 5-5 v1.28 补丁版本发布说明

CCE 集群补丁版本号	Kubernetes社区版本号	特性更新	优化增强	安全漏洞修复
v1.28.4-r0	v1.28.5	<ul style="list-style-type: none">• 创建节点支持选择 Docker 容器引擎。• 支持使用通用性 SSD v2 类型的云硬盘。• ELB Ingress 支持配置灰度发布。• ELB Ingress 支持配置 URL 重定向、Rewrite 重写、HTTP 重定向到 HTTPS 能力。	开放高频使用的集群参数、节点池参数配置。	修复部分安全问题。

CCE 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
v1.28.3-r0	v1.28.3	<p>负载均衡类型的Service和ELB Ingress能力新增：</p> <ul style="list-style-type: none"> 支持配置SNI。 支持开启HTTP/2。 支持配置空闲超时时间、请求超时时间、响应超时时间。 支持从HTTP报文的请求头中获取监听器端口号、客户端请求端口号、重写X-Forwarded-Host。 	-	修复部分安全问题。
v1.28.2-r0	v1.28.3	<ul style="list-style-type: none"> 创建Service或Ingress支持设置ELB黑/白名单访问控制。 CCE的节点镜像支持安全加固（满足等保三级基线要求）。 	-	修复部分安全问题。
v1.28.1-r4	v1.28.3	-	-	修复 CVE-2024-21626 安全漏洞。
v1.28.1-r2	v1.28.3	-	修复Ingress配置SNI证书并同时开启HTTP/2的场景下偶现配置冲突的问题。	-

CCE 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
v1.28.1-r0	v1.28.3	<p>首次发布CCE v1.28集群，有关更多信息请参见Kubernetes 1.28版本说明。</p> <ul style="list-style-type: none">节点池支持节点的自定义前缀和后缀命名CCE Turbo集群中，支持创建工作负载类型的容器网络配置，可指定Pod子网。ELB Ingress支持GRPC协议。负载均衡类型的服务在通过YAML创建时支持指定ELB私有IP。	<ul style="list-style-type: none">优化CCE Turbo集群中大批量创建安全容器的启动速度。提升CCE Turbo集群中反复创建删除安全容器时的稳定性。	-

v1.27 版本

须知

Kubernetes在1.24版本中移除了Dockershim，并从此不再默认支持Docker容器引擎，建议您使用Containerd容器引擎。如果您需要将Docker节点迁移至Containerd节点，详情请参见[将节点容器引擎从Docker迁移到Containerd](#)。

表 5-6 v1.27 补丁版本发布说明

CCE 集群补丁版本号	Kubernetes社区版本号	特性更新	优化增强	安全漏洞修复
v1.27.6-r0	v1.27.9	<ul style="list-style-type: none"> 创建节点支持选择 Docker 容器引擎。 支持使用通用性 SSD v2 类型的云硬盘。 ELB Ingress 支持配置灰度发布。 ELB Ingress 支持配置 URL 重定向、Rewrite 重写、HTTP 重定向到 HTTPS 能力。 	开放高频使用的集群参数、节点池参数配置。	修复部分安全问题。
v1.27.5-r0	v1.27.4	负载均衡类型的 Service 和 ELB Ingress 能力新增： <ul style="list-style-type: none"> 支持配置 SNI。 支持开启 HTTP/2。 支持配置空闲超时时间、请求超时时间、响应超时时间。 支持从 HTTP 报文的请求头中获取监听器端口号、客户端请求端口号、重写 X-Forwarded-Host。 	-	修复部分安全问题。
v1.27.4-r0	v1.27.4	<ul style="list-style-type: none"> 创建 Service 或 Ingress 支持设置 ELB 黑/白名单访问控制。 CCE 的节点镜像支持安全加固（满足等保三级基线要求）。 	-	修复部分安全问题。
v1.27.3-r4	v1.27.4	-	-	修复 CVE-2024-21626 安全漏洞。
v1.27.3-r2	v1.27.4	-	修复 Ingress 配置 SNI 证书并同时开启 HTTP/2 的场景下偶现配置冲突的问题。	-

CCE 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
v1.27.3-r0	v1.27.4	<ul style="list-style-type: none"> 节点池支持节点的自定义前缀和后缀命名 CCE Turbo集群中，支持创建工作负载类型的容器网络配置，可指定Pod子网。 ELB Ingress支持GRPC协议。 负载均衡类型的服务在通过YAML创建时支持指定ELB私有IP。 	<ul style="list-style-type: none"> 优化CCE Turbo集群中大批量创建安全容器的启动速度。 提升CCE Turbo集群中反复创建删除安全容器时的稳定性。 创建Ingress对象时增加配置证书校验，避免对ELB侧已存在的Ingress证书进行覆盖。 优化autoscaler扩容节点池时的事件上报逻辑，去除规格售罄的重复事件。 增加Service与Ingress端口占用的相互校验逻辑；增加同集群下Ingress的路径冲突的校验逻辑。 	修复部分安全问题。
v1.27.2-r0	v1.27.2	<ul style="list-style-type: none"> Volcano支持节点池亲和和调度。 Volcano支持负载重调度能力。 	-	修复部分安全问题。
v1.27.1-r10	v1.27.2	-	优化节点池伸缩时的事件信息。	修复部分安全问题。
v1.27.1-r0	v1.27.2	<p>首次发布CCE v1.27集群，有关更多信息请参见Kubernetes 1.27版本说明。</p> <ul style="list-style-type: none"> 节点池配置管理支持软驱逐和硬驱逐的设置。 支持为自动创建的EVS块存储添加TMS资源标签，以便于成本管理。 	由于 社区安全加固 ，v1.27及以上版本的集群中ClusterIP地址无法ping通。	-

v1.25 版本

须知

除EulerOS 2.5操作系统外，CCE v1.25集群的节点均默认采用Containerd容器引擎。

表 5-7 v1.25 补丁版本发布说明

CCE 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
v1.25.9-r0	v1.25.16	<ul style="list-style-type: none">支持使用通用性SSD v2类型的云硬盘。ELB Ingress支持配置灰度发布。ELB Ingress支持配置URL重定向、Rewrite重写、HTTP重定向到HTTPS能力。	开放高频使用的集群参数、节点池参数配置。	修复部分安全问题。
v1.25.8-r0	v1.25.10	负载均衡类型的Service和ELB Ingress能力新增： <ul style="list-style-type: none">支持配置SNI。支持开启HTTP/2。支持配置空闲超时时间、请求超时时间、响应超时时间。支持从HTTP报文的请求头中获取监听器端口号、客户端请求端口号、重写X-Forwarded-Host。	-	修复部分安全问题。
v1.25.7-r0	v1.25.10	<ul style="list-style-type: none">创建Service或Ingress支持设置ELB黑/白名单访问控制。CCE的节点镜像支持安全加固（满足等保三级基线要求）。	-	修复部分安全问题。
v1.25.6-r4	v1.25.10	-	-	修复 CVE-2024-21626 安全漏洞。

CCE 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
v1.25.6-r2	v1.25.10	-	修复Ingress配置SNI证书并同时开启HTTP/2的场景下偶现配置冲突的问题。	-
v1.25.6-r0	v1.25.10	<ul style="list-style-type: none"> 节点池支持节点的自定义前缀和后缀命名 CCE Turbo集群中，支持创建工作负载类型的容器网络配置，可指定Pod子网。 ELB Ingress支持GRPC协议。 负载均衡类型的服务在通过YAML创建时支持指定ELB私有IP。 	<ul style="list-style-type: none"> 优化CCE Turbo集群中大批量创建安全容器的启动速度。 提升CCE Turbo集群中反复创建删除安全容器时的稳定性。 修复kubelet在特定场景下偶现启动卡死的问题。 优化autoscaler扩容节点池时的事件上报逻辑，去除规格售罄的重复事件。 修复特定场景下kubelet重启，出现Succeed状态的Pod变为Failed的问题。 	修复部分安全问题。
v1.25.5-r0	v1.25.5	<ul style="list-style-type: none"> Volcano支持节点池亲和调度。 Volcano支持负载重调度能力。 	-	修复部分安全问题。
v1.25.4-r10	v1.25.5	-	优化节点池伸缩时的事件信息。	修复部分安全问题。
v1.25.4-r0	v1.25.5	<ul style="list-style-type: none"> 节点池配置管理支持软驱逐和硬驱逐的设置。 支持为自动创建的EVS块存储添加TMS资源标签，以便于成本管理。 	-	修复部分安全问题。
v1.25.3-r10	v1.25.5	<ul style="list-style-type: none"> CCE集群支持对接使用弹性规格的独享型ELB。 负载均衡支持设置超时时间。 	kube-apiserver高频参数支持配置。	修复部分安全问题。

CCE 集群 补丁 版本号	Kube netes 社区 版本	特性更新	优化增强	安全漏洞 修复
v1.25.3-r0	v1.25.5	<ul style="list-style-type: none"> ● CCE Turbo容器网卡支持固定IP。详情请参见Pod配置固定IP。 ● CCE Turbo容器网卡支持自动创建和自动绑定EIP。详情请参见Pod配置固定EIP。 ● CCE Turbo集群在离线混部增强：支持Pod网络优先级限制。详情请参见出口网络带宽保障。 ● CCE Turbo集群支持命名空间关联容器网段。详情请参见网络配置（NetworkAttachmentDefinition）。 ● 集群支持CPU Burst特性，避免CPU限流影响时延敏感型容器业务。详情请参见CPU Burst弹性限流。 	增强CCE Turbo集群在规格变更场景时网络的稳定性。	修复部分安全问题。
v1.25.1-r0	v1.25.5	首次发布CCE v1.25集群，有关更多信息请参见 Kubernetes 1.25版本说明 。	-	-

v1.23 版本

表 5-8 v1.23 补丁版本发布说明

CCE 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
v1.23.14-r0	v1.23.17	<ul style="list-style-type: none"> 支持使用通用性SSD v2类型的云硬盘。 ELB Ingress支持配置灰度发布。 ELB Ingress支持配置URL重定向、Rewrite重写、HTTP重定向到HTTPS能力。 	开放高频使用的集群参数、节点池参数配置。	修复部分安全问题。
v1.23.13-r0	v1.23.17	负载均衡类型的Service和ELB Ingress能力新增： <ul style="list-style-type: none"> 支持配置SNI。 支持开启HTTP/2。 支持配置空闲超时时间、请求超时时间、响应超时时间。 支持从HTTP报文的请求头中获取监听器端口号、客户端请求端口号、重写X-Forwarded-Host。 	-	修复部分安全问题。
v1.23.12-r0	v1.23.17	<ul style="list-style-type: none"> 创建Service或Ingress支持设置ELB黑/白名单访问控制。 CCE的节点镜像支持安全加固（满足等保三级基线要求）。 	-	修复部分安全问题。
v1.23.11-r4	v1.23.17	-	-	修复 CVE-2024-21626 安全漏洞。
v1.23.11-r2	v1.23.17	-	修复Ingress配置SNI证书并同时开启HTTP/2的场景下偶现配置冲突的问题。	-

CCE 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
v1.23.11-r0	v1.23.17	<ul style="list-style-type: none"> 节点池支持节点的自定义前缀和后缀命名 CCE Turbo集群中，支持创建工作负载类型的容器网络配置，可指定Pod子网。 ELB Ingress支持GRPC协议。 负载均衡类型的服务在通过YAML创建时支持指定ELB私有IP。 	<ul style="list-style-type: none"> 优化CCE Turbo集群中大批量创建安全容器的启动速度。 提升CCE Turbo集群中反复创建删除安全容器时的稳定性。 修复Docker在journald异常退出场景下导致容器无法被结束的问题。 修复Everest插件卸载时，调度器未能在创建Pod时拦截自动挂载SFS3.0存储卷的问题。 修复v1.23版本集群中，EulerOS 2.9系统的containerd节点上/var/lib/contained磁盘目录使用率虚高的问题。 	修复部分安全问题。
v1.23.10-r0	v1.23.11	<ul style="list-style-type: none"> Volcano支持节点池亲和和调度。 Volcano支持负载重调度能力。 	-	修复部分安全问题。
v1.23.9-r10	v1.23.11	-	优化节点池伸缩时的事件信息。	修复部分安全问题。
v1.23.9-r0	v1.23.11	<ul style="list-style-type: none"> 节点池配置管理支持软驱逐和硬驱逐的设置。 支持为自动创建的EVS块存储添加TMS资源标签，以便于成本管理。 	-	修复部分安全问题。
v1.23.8-r10	v1.23.11	<ul style="list-style-type: none"> CCE集群支持对接使用弹性规格的独享型ELB。 负载均衡支持设置超时时间。 	kube-apiserver高频参数支持配置。	修复部分安全问题。

CCE 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
v1.23.8-r0	v1.23.11	<ul style="list-style-type: none"> ● CCE Turbo容器网卡支持固定IP。详情请参见Pod配置固定IP。 ● CCE Turbo容器网卡支持自动创建和自动绑定EIP。详情请参见Pod配置固定EIP。 ● CCE Turbo集群在离线混部增强：支持Pod网络优先级限制。详情请参见出口网络带宽保障。 ● CCE Turbo集群支持命名空间关联容器网段。详情请参见网络配置（NetworkAttachmentDefinition）。 ● 集群支持CPU Burst特性，避免CPU限流影响时延敏感型容器业务。详情请参见CPU Burst弹性限流。 	<ul style="list-style-type: none"> ● 增强docker版本升级时的可靠性。 ● 优化集群节点时间同步能力。 	修复部分安全问题。
v1.23.7-r20	v1.23.11	-	<ul style="list-style-type: none"> ● 增强Service/Ingress对接ELB特性稳定性。 ● 增强节点挂载多块数据盘场景可靠性。 	修复部分安全问题。
v1.23.7-r10	v1.23.11	-	<ul style="list-style-type: none"> ● 增强docker版本升级时的可靠性。 ● 增强containerd运行时在异常断链场景下的可靠性。 ● 内核参数调优异常场景下加固。 	修复部分安全问题。

CCE 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
v1.23.7-r0	v1.23.11		<ul style="list-style-type: none"> 优化CCE Turbo集群在规格变更场景时网络的稳定性。 增强集群升级场景，nginx-ingress-controller的网络稳定性。 优化集群节点时间同步能力。 	修复部分安全问题。
v1.23.6-r0	v1.23.11	<ul style="list-style-type: none"> 支持LB类型的Service同时配置TCP/UDP端口 支持Pod readiness gate 	<ul style="list-style-type: none"> 增强底层网络异常时的流表可靠性。 增强高版本内核的OS异常掉电等重启场景的稳定性。 cadvisor GPU/NPU相关指标优化。 	修复部分安全问题。
v1.23.5-r0	v1.23.11	<ul style="list-style-type: none"> 容器存储支持对接SFS 3.0文件存储服务。 支持GPU节点的设备故障检测和隔离能力。 支持配置集群维度的自定义安全组。 CCE Turbo集群支持节点级别的网卡预热参数配置。 支持集群控制面组件的日志信息开放。 集群支持华为云自研的Huawei Cloud EulerOS 2.0操作系统。 CCE集群支持选择Containerd容器运行时。 CCE Turbo集群在离线混部增强：支持CPU潮汐亲和性。 	<ul style="list-style-type: none"> 优化升级控制节点ETCD版本至社区版本3.5.6。 优化EulerOS 2.8节点上Service的访问性能。 优化调度均衡性，工作负载实例数缩容时仍保持跨AZ分布均衡。 优化kube-apiserver在频繁更新CRD场景下的内存使用。 	修复部分安全问题及以下CVE漏洞： <ul style="list-style-type: none"> CVE-2022-3294 CVE-2022-3162 CVE-2022-3172 CVE-2021-25749

CCE 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
v1.23.4-r10	v1.23.4	-	优化kube-apiserver在频繁更新crd场景下的内存使用。	修复部分安全问题。
v1.23.4-r0	v1.23.4	支持ARM节点创建。	-	修复部分安全问题。
v1.23.3-r0	v1.23.4	<ul style="list-style-type: none">• CCE集群支持对租户开放master节点组件监控指标。• 通过预热机制优化CCE Turbo集群SubENI网卡启动速度。• 支持ELB类型service配置后端服务器权重。• CCE集群支持跨集群部署服务。• CCE Turbo集群使用虚拟机节点场景下支持在离线混部功能。	增强安全容器在反复创删场景下的可靠性。	修复部分安全问题。
v1.23.1-r1	v1.23.4	优化节点的资源预留参数，支持资源耗尽检测，提升节点的稳定性。	提升节点的安装兼容性。	修复部分安全问题。
v1.23.1-r0	v1.23.4	首次发布CCE v1.23集群，有关更多信息请参见 Kubernetes 1.23版本说明 。	-	-

v1.21 版本

表 5-9 v1.21 补丁版本发布说明

CCE 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
v1.21.15-r0	v1.21.14	<ul style="list-style-type: none">支持使用通用性SSD v2类型的云硬盘。ELB Ingress支持配置灰度发布。ELB Ingress支持配置URL重定向、Rewrite重写、HTTP重定向到HTTPS能力。	开放高频使用的集群参数、节点池参数配置。	修复部分安全问题。
v1.21.14-r0	v1.21.14	支持使用PVC动态创建SFS Turbo子目录并挂载。	-	修复部分安全问题。
v1.21.13-r0	v1.21.14	<ul style="list-style-type: none">创建Service或Ingress支持设置ELB黑/白名单访问控制。CCE的节点镜像支持安全加固（满足等保三级基线要求）。	-	修复部分安全问题。
v1.21.12-r4	v1.21.14	-	-	修复 CVE-2024-21626 安全漏洞。
v1.21.12-r2	v1.21.14	-	修复Ingress配置SNI证书并同时开启HTTP/2的场景下偶现配置冲突的问题。	-

CCE 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
v1.21.12-r0	v1.21.14	<ul style="list-style-type: none"> 节点池支持节点的自定义前缀和后缀命名 CCE Turbo集群中，支持创建工作负载类型的容器网络配置，可指定Pod子网。 ELB Ingress支持GRPC协议。 负载均衡类型的服务在通过YAML创建时支持指定ELB私有IP。 	<ul style="list-style-type: none"> 优化健康检查配置，避免出现keepalived反复重启的问题。 优化securityPolicy缓存及Ingress重试风暴。 修复cloud-controller-manager组件主进程所在Master节点出现卡IO，组件切主失败的问题。 修复Service设置权重后，会错误计算terminating状态的Pod数，导致Pod权重不准确的问题。 	修复部分安全问题。
v1.21.11-r20	v1.21.14	<ul style="list-style-type: none"> Volcano支持节点池亲和调度。 Volcano支持负载重调度能力。 	-	修复部分安全问题。
v1.21.11-r10	v1.21.14	-	优化节点池伸缩时的事件信息。	修复部分安全问题。
v1.21.11-r0	v1.21.14	<ul style="list-style-type: none"> 节点池配置管理支持软驱逐和硬驱逐的设置。 支持为自动创建的EVS块存储添加TMS资源标签，以便于成本管理。 	-	修复部分安全问题。
v1.21.10-r10	v1.21.14	<ul style="list-style-type: none"> CCE集群支持对接使用弹性规格的独享型ELB。 负载均衡支持设置超时时间。 	kube-apiserver高频参数支持配置。	修复部分安全问题。

CCE 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
v1.21.10-r0	v1.21.14	<ul style="list-style-type: none"> CCE Turbo容器网卡支持固定IP。详情请参见Pod配置固定IP。 CCE Turbo容器网卡支持自动创建和自动绑定EIP。详情请参见Pod配置固定EIP。 	<ul style="list-style-type: none"> 增强docker版本升级时的可靠性。 优化集群节点时间同步能力。 优化节点重启后，docker运行时拉取镜像的稳定性。 	修复部分安全问题。
v1.21.9-r0	v1.21.14		优化CCE Turbo集群在规格变更场景时网络的稳定性。	修复部分安全问题。
v1.21.8-r0	v1.21.14	<ul style="list-style-type: none"> 支持LB类型的Service同时配置TCP/UDP端口 支持Pod readiness gate 	<ul style="list-style-type: none"> 增强底层网络异常时的流表可靠性。 增强高版本内核的OS异常掉电等重启场景的稳定性。 cadvisor GPU/NPU相关指标优化。 	修复部分安全问题。
v1.21.7-r0	v1.21.14	<ul style="list-style-type: none"> 容器存储支持对接SFS 3.0文件存储服务。 支持GPU节点的设备故障检测和隔离能力。 支持配置集群维度的自定义安全组。 CCE Turbo集群支持节点级别的网卡预热参数配置。 支持集群控制面组件的日志信息开放。 	优化ELB Service/Ingress在大量连接场景下的稳定性。	修复部分安全问题及以下CVE漏洞： <ul style="list-style-type: none"> CVE-2022-3294 CVE-2022-3162 CVE-2022-3172
v1.21.6-r0	v1.21.7	支持ARM节点创建。	-	修复部分安全问题。
v1.21.5-r10	v1.21.7	-	<ul style="list-style-type: none"> 优化隧道网络在控制面节点间网络闪断场景下导网络分配的稳定性。 ovs漏洞加固。 	修复部分安全问题。

CCE 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
v1.21.5-r0	v1.21.7	-	<ul style="list-style-type: none"> 增强集群升级下容器隧道网络模式的稳定性。 增强pod拓扑分布约束能力。 增强集群控制面节点掉电时链接释放的稳定性。 增强节点上pod并发挂载存储卷的稳定性。 	修复部分安全问题。
v1.21.4-r10	v1.21.7	-	增强EulerOS 2.9操作系统NetworkManager的稳定性。	修复部分安全问题。
v1.21.4-r0	v1.21.7	-	<ul style="list-style-type: none"> 增强安全容器场景下容器网卡驱动切换的稳定性。 增强升级工作负载且处于节点伸缩时，访问负载均衡服务的稳定性。 	修复部分安全问题。
v1.21.3-r10	v1.21.7	-	增强安全容器场景下容器网卡驱动切换的稳定性。	修复部分安全问题。
v1.21.3-r0	v1.21.7	-	CCE Turbo集群容器内的SNAT网段支持可配置。	修复部分安全问题。
v1.21.2-r10	v1.21.7	-	增强Service对接负载均衡场景的稳定性。	修复部分安全问题。
v1.21.2-r0	v1.21.7	优化节点的资源预留参数，支持资源耗尽检测，提升节点的稳定性。	<ul style="list-style-type: none"> 提升集群升级能力，增强升级可靠性。 优化容器本地存储功能，提升稳定性。 	修复部分安全问题。

CCE 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
v1.21.1-r2	v1.21.7	<ul style="list-style-type: none"> 容器存储支持本地持久卷。 支持管理EulerOS 2.9鲲鹏计算实例。 容器隧道网络模式和VPC网络模式支持OS内核版本宽匹配。 	<ul style="list-style-type: none"> 优化节点安装流程，增强节点创建的可靠性。 优化CentOS和EulerOS 2.5的内核参数，提升OS性能。 	修复部分安全问题。
v1.21.1-r1	v1.21.7	-	容器网络支持内核宽匹配。	修复部分安全问题。
v1.21.1-r0	v1.21.7	首次发布CCE v1.21集群，有关更多信息请参见 Kubernetes 1.21版本说明 。	-	-

v1.19 版本

表 5-10 v1.19 补丁版本发布说明

CCE 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
v1.19.16-r84	v1.19.16	-	-	修复 CVE-2024-21626 安全漏洞。
v1.19.16-r82	v1.19.16	-	修复Ingress配置SNI证书并同时开启HTTP/2的场景下偶现配置冲突的问题。	-

CCE 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
v1.19.16-r80	v1.19.16	<ul style="list-style-type: none"> 节点池支持节点的自定义前缀和后缀命名 CCE Turbo集群中，支持创建工作负载类型的容器网络配置，可指定Pod子网。 ELB Ingress支持GRPC协议。 负载均衡类型的服务在通过YAML创建时支持指定ELB私有IP。 	<ul style="list-style-type: none"> 修复BMS节点重启后显示节点不可用的问题。 优化VIP路由清理逻辑，先清理残留VIP路由，避免出现NetworkManager重启后重新添加路由的问题。 修复CCE Turbo集群使用独享型ELB场景，Pod滚动升级复用IP可能导致ELB后端服务器无法添加的问题。 修复创建负载均衡类型Service时加入healthcheck队列后，如果Service被删除，会导致缓存残留的问题。 修复Master节点所在的物理机或者交换机网络设备掉线之后，内存持续上涨，docker占用内存持续上涨的问题。 	修复部分安全问题。
v1.19.16-r60	v1.19.16	<ul style="list-style-type: none"> Volcano支持节点池亲和和调度。 Volcano支持负载重调度能力。 	-	修复部分安全问题。
v1.19.16-r50	v1.19.16	-	优化节点池伸缩时的事件信息。	修复部分安全问题。
v1.19.16-r40	v1.19.16	<ul style="list-style-type: none"> 节点池配置管理支持软驱逐和硬驱逐的设置。 支持为自动创建的EVS块存储添加TMS资源标签，以便于成本管理。 	-	修复部分安全问题。

CCE 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
v1.19.16-r30	v1.19.16	<ul style="list-style-type: none"> CCE集群支持对接使用弹性规格的独享型ELB。 负载均衡支持设置超时时间。 	kube-apiserver高频参数支持配置。	修复部分安全问题。
v1.19.16-r20	v1.19.16	<ul style="list-style-type: none"> CCE Turbo容器网卡支持固定IP。详情请参见Pod配置固定IP。 CCE Turbo容器网卡支持自动创建和自动绑定EIP。详情请参见Pod配置固定EIP。 	<ul style="list-style-type: none"> 云原生2.0网络支持命名空间指定子网。 增强节点重启后，docker运行时拉取镜像的稳定性。 优化CCE Turbo集群在非全预热场景分配网卡的性能。 	修复部分安全问题。
v1.19.16-r10	v1.19.16	-	提升Service/Ingress对接ELB特性稳定性。	修复部分安全问题。
v1.19.16-r7	v1.19.16	-	<ul style="list-style-type: none"> 增强Docker版本升级时的可靠性。 优化集群节点时间同步能力。 增强CCE Turbo集群预热场景可靠性。 	修复部分安全问题。
v1.19.16-r6	v1.19.16		<ul style="list-style-type: none"> 增强配置了QoS的containerd容器运行的稳定性。 Ingress支持对url重写策略配置和修改。 优化kube-controller-manager在频繁更新CRD场景下的内存使用。 	修复部分安全问题。
v1.19.16-r5	v1.19.16	<ul style="list-style-type: none"> 支持LB类型的Service同时配置TCP/UDP端口 支持Pod readiness gate 	<ul style="list-style-type: none"> 增强底层网络异常时的流表可靠性。 增强高版本内核的OS异常掉电等重启场景的稳定性。 	修复部分安全问题。

CCE 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
v1.19.16-r4	v1.19.16	<ul style="list-style-type: none"> 容器存储支持对接SFS 3.0文件存储服务。 支持GPU节点的设备故障检测和隔离能力。 支持配置集群维度的自定义安全组。 CCE Turbo集群支持节点级别的网卡预热参数配置。 	<ul style="list-style-type: none"> 优化节点污点场景下负载调度的性能。 增强Containerd运行时绑核场景下长时间运行的稳定性。 优化ELB Service/ Ingress在大量连接场景下的稳定性。 优化kube-apiserver在频繁更新crd场景下的内存使用。 	修复部分安全问题及以下CVE漏洞： <ul style="list-style-type: none"> CVE-2022-3294 CVE-2022-3162 CVE-2022-3172
v1.19.16-r3	v1.19.16	-	<ul style="list-style-type: none"> 支持image-pull-progress-deadline启动参数升级保留。 CCE Turbo支持节点自定义网卡动态预热配置。 解决隧道网络在master节点间网络闪断场景下导致的网络分配不一致问题。 优化容器隧道网络模式集群在控制面节点网络闪断场景下的稳定性。 	修复部分安全问题。
v1.19.16-r2	v1.19.16	-	<ul style="list-style-type: none"> 增强集群控制面节点掉电时链接释放的稳定性。 增强节点上Pod并发挂载存储卷的稳定性。 	修复部分安全问题。
v1.19.16-r1	v1.19.16	-	增强EulerOS 2.9操作系统NetworkManager的稳定性。	修复部分安全问题。

CCE 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
v1.19.16-r0	v1.19.16	-	增强工作负载升级且节点伸缩状态下，负载均衡服务更新的稳定性。	修复部分安全问题及以下CVE漏洞： <ul style="list-style-type: none">• CVE-2021-25741• CVE-2021-25737
v1.19.10-r0	v1.19.10	首次发布CCE v1.19集群，有关更多信息请参见 Kubernetes 1.19版本说明 。	-	-

5.2 操作系统镜像发布记录

5.2.1 操作系统版本支持机制

同步机制

云容器引擎CCE发布的集群节点组件会随CCE集群版本发布定期更新。

操作系统重大漏洞修复：跟随集群补丁升级策略发布。

集群版本与操作系统对应关系

如下为当前已经发布的集群版本与操作系统版本的对应关系，请参考：

表 5-11 弹性云服务器-虚拟机节点操作系统

操作系统	集群版本	CCE Standard集群		CCE Turbo集群	最新内核信息
		VPC网络模型	容器隧道网络模型	云原生网络2.0	
Huawei Cloud EulerOS 2.0	v1.29	√	√	√	5.10.0-60.18.0.50.r1083_58.hce2.x86_64
	v1.28	√	√	√	5.10.0-60.18.0.50.r1083_58.hce2.x86_64
	v1.27	√	v1.27.3-r0及以上版本支持	√	5.10.0-60.18.0.50.r1083_58.hce2.x86_64
	v1.25	√	v1.25.6-r0及以上版本支持	√	5.10.0-60.18.0.50.r1083_58.hce2.x86_64
	v1.23	√	v1.23.11-r0及以上版本支持	√	5.10.0-60.18.0.50.r1083_58.hce2.x86_64
Huawei Cloud EulerOS 2.0 (ARM)	v1.29	√	√	√	5.10.0-60.18.0.50.r1083_58.hce2.aarch64
	v1.28	√	√	√	5.10.0-60.18.0.50.r1083_58.hce2.aarch64
	v1.27	√	v1.27.3-r0及以上版本支持	√	5.10.0-60.18.0.50.r1083_58.hce2.aarch64
	v1.25	√	v1.25.6-r0及以上版本支持	√	5.10.0-60.18.0.50.r1083_58.hce2.aarch64
	v1.23	√	v1.23.11-r0及以上版本支持	√	5.10.0-60.18.0.50.r1083_58.hce2.aarch64
Ubuntu 22.04	v1.29	√	×	√	5.15.0-92-generic
	v1.28	√	×	√	5.15.0-92-generic
	v1.27	√	×	√	5.15.0-92-generic
	v1.25	√	×	√	5.15.0-92-generic
	v1.23	√	×	√	5.15.0-92-generic

操作系统	集群版本	CCE Standard集群		CCE Turbo集群	最新内核信息
		VPC网络模型	容器隧道网络模型	云原生网络2.0	
Huawei Cloud EulerOS 1.1	v1.29	√	√	√	3.10.0-1160.76.2.hce1c.x86_64
	v1.28	√	√	√	3.10.0-1160.76.2.hce1c.x86_64
	v1.27	√	√	√	3.10.0-1160.76.2.hce1c.x86_64
	v1.25	√	√	√	3.10.0-1160.76.2.hce1c.x86_64
	v1.23	√	√	√	3.10.0-1160.76.2.hce1c.x86_64
	v1.21	√	√	√	3.10.0-1160.76.2.hce1c.x86_64
CentOS Linux release 7.6	v1.29	√	√	√	3.10.0-1160.108.1.el7.x86_64
	v1.28	√	√	√	3.10.0-1160.108.1.el7.x86_64
	v1.27	√	√	√	3.10.0-1160.108.1.el7.x86_64
	v1.25	√	√	√	3.10.0-1160.108.1.el7.x86_64
	v1.23	√	√	√	3.10.0-1160.108.1.el7.x86_64
	v1.21 (停止维护)	√	√	√	3.10.0-1160.108.1.el7.x86_64
	v1.19 (停止维护)	√	√	√	3.10.0-1160.108.1.el7.x86_64
	v1.17.17 (停止维护)	√	√	√	3.10.0-1160.15.2.el7.x86_64
	v1.17.9 (停止维护)	√	√	√	3.10.0-1062.12.1.el7.x86_64
	v1.15.11 (停止维护)	√	√	√	3.10.0-1062.12.1.el7.x86_64

操作系统	集群版本	CCE Standard集群		CCE Turbo集群	最新内核信息
		VPC网络模型	容器隧道网络模型	云原生网络2.0	
	v1.15.6-r1 (停止维护)	√	√	√	3.10.0-1062.1.1.el7.x86_64
	v1.13.10-r1 (停止维护)	√	√	√	3.10.0-957.21.3.el7.x86_64
	v1.13.7-r0 (停止维护)	√	√	√	3.10.0-957.21.3.el7.x86_64
EulerOS release 2.9	v1.29	√	√	√	4.18.0-147.5.1.6.h1152.eulerosv2r9.x86_64
	v1.28	√	√	√	4.18.0-147.5.1.6.h1152.eulerosv2r9.x86_64
	v1.27	√	√	√	4.18.0-147.5.1.6.h1152.eulerosv2r9.x86_64
	v1.25	√	√	√	4.18.0-147.5.1.6.h1152.eulerosv2r9.x86_64
	v1.23	√	√	√	4.18.0-147.5.1.6.h1152.eulerosv2r9.x86_64
	v1.21 (停止维护)	√	√	√	4.18.0-147.5.1.6.h1152.eulerosv2r9.x86_64
	v1.19 (停止维护)	√	√	√	4.18.0-147.5.1.6.h1152.eulerosv2r9.x86_64
EulerOS release 2.9 (ARM)	v1.29	√	√	√	4.19.90-vhulk2103.1.0.h1144.eulerosv2r9.aarch64
	v1.28	√	√	√	4.19.90-vhulk2103.1.0.h1144.eulerosv2r9.aarch64

操作系统	集群版本	CCE Standard集群		CCE Turbo集群	最新内核信息
		VPC网络模型	容器隧道网络模型	云原生网络2.0	
	v1.27	√	√	√	4.19.90-vhulk2103.1.0.h1144.eulerosv2r9.aarch64
	v1.25	√	√	√	4.19.90-vhulk2103.1.0.h1144.eulerosv2r9.aarch64
	v1.23	√	√	√	4.19.90-vhulk2103.1.0.h1144.eulerosv2r9.aarch64
	v1.21 (停止维护)	√	√	√	4.19.90-vhulk2103.1.0.h1144.eulerosv2r9.aarch64
	v1.19 (停止维护)	√	√	√	4.19.90-vhulk2103.1.0.h1144.eulerosv2r9.aarch64
EulerOS release 2.8 (ARM) (停止维护)	v1.27及以上	×	×	×	-
	v1.25 (停止维护)	√	√	√	4.19.36-vhulk1907.1.0.h1350.eulerosv2r8.aarch64
	v1.23 (停止维护)	√	√	√	4.19.36-vhulk1907.1.0.h1350.eulerosv2r8.aarch64
	v1.21 (停止维护)	√	√	√	4.19.36-vhulk1907.1.0.h1350.eulerosv2r8.aarch64
	v1.19.16 (停止维护)	√	√	√	4.19.36-vhulk1907.1.0.h1350.eulerosv2r8.aarch64

操作系统	集群版本	CCE Standard集群		CCE Turbo集群	最新内核信息
		VPC网络模型	容器隧道网络模型	云原生网络2.0	
	v1.19.10 (停止维护)	√	√	√	4.19.36- vhulk1907.1.0.h96 2.eulerosv2r8.aarc h64
	v1.17.17 (停止维护)	√	√	√	4.19.36- vhulk1907.1.0.h96 2.eulerosv2r8.aarc h64
	v1.15.11 (停止维护)	√	√	√	4.19.36- vhulk1907.1.0.h70 2.eulerosv2r8.aarc h64
EulerOS release 2.5 (停止 维护)	v1.27及以上	×	×	×	-
	v1.25 (停止维护)	√	√	√	3.10.0-862.14.1.5. h687.eulerosv2r7. x86_64
	v1.23 (停止维护)	√	√	√	3.10.0-862.14.1.5. h687.eulerosv2r7. x86_64
	v1.21 (停止维护)	√	√	√	3.10.0-862.14.1.5. h687.eulerosv2r7. x86_64
	v1.19.16 (停止维护)	√	√	√	3.10.0-862.14.1.5. h687.eulerosv2r7. x86_64
	v1.19.10 (停止维护)	√	√	√	3.10.0-862.14.1.5. h520.eulerosv2r7. x86_64
	v1.19.8 (停止维护)	√	√	√	3.10.0-862.14.1.5. h520.eulerosv2r7. x86_64
	v1.17.17 (停止维护)	√	√	√	3.10.0-862.14.1.5. h470.eulerosv2r7. x86_64
	v1.17.9 (停止维护)	√	√	√	3.10.0-862.14.1.5. h428.eulerosv2r7. x86_64

操作系统	集群版本	CCE Standard集群		CCE Turbo集群	最新内核信息
		VPC网络模型	容器隧道网络模型	云原生网络2.0	
	v1.15.11 (停止维护)	√	√	√	3.10.0-862.14.1.5. h428.eulerosv2r7. x86_64
	v1.15.6-r1 (停止维护)	√	√	√	3.10.0-862.14.1.5. h328.eulerosv2r7. x86_64
	v1.13.10-r1 (停止维护)	√	√	√	3.10.0-862.14.1.2. h249.eulerosv2r7. x86_64
	v1.13.7-r0 (停止维护)	√	√	√	3.10.0-862.14.1.0. h197.eulerosv2r7. x86_64
Ubuntu 18.04 server 64bit (停止维护)	v1.27及以上	×	×	×	-
	v1.25 (停止维护)	√	×	√	4.15.0-171- generic
	v1.23 (停止维护)	√	×	√	4.15.0-171- generic
	v1.21 (停止维护)	√	×	√	4.15.0-171- generic
	v1.19.16 (停止维护)	√	×	√	4.15.0-171- generic
	v1.19.8 (停止维护)	√	×	√	4.15.0-136- generic
	v1.17.17 (停止维护)	√	×	√	4.15.0-136- generic

表 5-12 弹性云服务器-物理机节点操作系统

操作系统	集群版本	CCE Standard集群		CCE Turbo集群	最新内核信息
		VPC网络模型	容器隧道网络模型	云原生网络2.0	
EulerOS release 2.10	v1.29	√	√	√	4.18.0-147.5.2.15.h1109.eulerosv2r10.x86_64
	v1.28	√	√	√	4.18.0-147.5.2.15.h1109.eulerosv2r10.x86_64
	v1.27	√	√	√	4.18.0-147.5.2.15.h1109.eulerosv2r10.x86_64
	v1.25	√	√	√	4.18.0-147.5.2.15.h1109.eulerosv2r10.x86_64
	v1.23	√	√	√	4.18.0-147.5.2.15.h1109.eulerosv2r10.x86_64
	v1.21 (停止维护)	√	√	√	4.18.0-147.5.2.15.h1109.eulerosv2r10.x86_64
	v1.19.16 (停止维护)	√	√	√	4.18.0-147.5.2.15.h1109.eulerosv2r10.x86_64

表 5-13 裸金属服务器节点操作系统

操作系统	集群版本	CCE Standard集群		CCE Turbo集群	最新内核信息
		VPC网络模型	容器隧道网络模型	云原生网络2.0	
EulerOS release 2.9 (受限使用, 请提交工单申请)	v1.29	√	√	×	4.18.0-147.5.1.6.h841.eulerosv2r9.x86_64
	v1.28	√	√	×	4.18.0-147.5.1.6.h841.eulerosv2r9.x86_64

操作系统	集群版本	CCE Standard集群		CCE Turbo集群	最新内核信息
		VPC网络模型	容器隧道网络模型	云原生网络2.0	
	v1.27	√	√	×	4.18.0-147.5.1.6.h841.eulerosv2r9.x86_64
	v1.25	√	√	×	4.18.0-147.5.1.6.h841.eulerosv2r9.x86_64
	v1.23	√	√	×	4.18.0-147.5.1.6.h841.eulerosv2r9.x86_64
	v1.21 (停止维护)	√	√	×	4.18.0-147.5.1.6.h841.eulerosv2r9.x86_64
	v1.19 (停止维护)	√	√	×	4.18.0-147.5.1.6.h841.eulerosv2r9.x86_64
EulerOS release 2.3 (停止维护)	v1.27及以上	×	×	×	-
	v1.25 (停止维护)	√	√	×	3.10.0-514.41.4.28.h62.x86_64
	v1.23 (停止维护)	√	√	×	3.10.0-514.41.4.28.h62.x86_64
	v1.21 (停止维护)	√	√	×	3.10.0-514.41.4.28.h62.x86_64
	v1.19 (停止维护)	√	√	×	3.10.0-514.41.4.28.h62.x86_64
	v1.17 (停止维护)	√	√	×	3.10.0-514.41.4.28.h62.x86_64
	v1.15.11 (停止维护)	√	√	×	3.10.0-514.41.4.28.h62.x86_64

5.2.2 操作系统镜像版本说明

本文为您提供CCE集群操作系统版本相关的最新发布动态。

如需获取最新的集群版本与操作系统版本对应表，请参见[集群版本与操作系统对应关系](#)。

Huawei Cloud EulerOS 2.0

内核版本	发布时间	发布说明
5.10.0-60.18.0.50.r1083_58.hce2.x86_64	2024年4月	更新系统内核，修复安全漏洞。
5.10.0-60.18.0.50.r1002_48.hce2.x86_64	2023年12月	更新系统内核，修复安全漏洞。
5.10.0-60.18.0.50.r865_35.hce2.x86_64	2023年4月	更新系统内核，修复安全漏洞。
5.10.0-60.18.0.50.r509_2.hce2.x86_64	2023年1月	更新系统内核，修复安全漏洞。
5.10.0-60.18.0.50.h322_1.hce2.x86_64	2022年11月	CCE支持Huawei Cloud EulerOS 2.0操作系统。

Huawei Cloud EulerOS 2.0 (ARM)

内核版本	发布时间	发布说明
5.10.0-60.18.0.50.r1083_58.hce2.aarch64	2024年4月	更新系统内核，修复安全漏洞。
5.10.0-60.18.0.50.r1002_48.hce2.aarch64	2023年12月	更新系统内核，修复安全漏洞。
5.10.0-60.18.0.50.r865_35.hce2.aarch64	2023年4月	ARM架构节点支持Huawei Cloud EulerOS 2.0操作系统。

Huawei Cloud EulerOS 1.1

内核版本	发布时间	发布说明
3.10.0-1160.76.2.hce1c.x86_64	2023年1月	CCE支持Huawei Cloud EulerOS 1.1操作系统。 支持的集群版本如下： <ul style="list-style-type: none">• v1.19.16-r4及以上• v1.21.7-r0及以上• v1.23.5-r0及以上• v1.25.1-r0及以上

Ubuntu 22.04

内核版本	发布时间	发布说明
5.15.0-92-generic	2024年4月	更新系统内核，修复安全漏洞。
5.15.0-86-generic	2023年12月	更新系统内核，修复安全漏洞。
5.15.0-60-generic	2023年4月	更新系统内核，修复安全漏洞。
5.15.0-53-generic	2023年1月	CCE支持Ubuntu 22.04操作系统。

EulerOS 2.9

内核版本	发布时间	发布说明
4.18.0-147.5.1.6.h1152.eulerosv2r9.x86_64	2024年4月	更新系统内核，修复安全漏洞。
4.18.0-147.5.1.6.h1071.eulerosv2r9.x86_64	2023年12月	更新系统内核，修复安全漏洞。
4.18.0-147.5.1.6.h1017.eulerosv2r9.x86_64	2023年6月	<ul style="list-style-type: none">更新系统内核，修复安全漏洞。修复IPVS模式下，EulerOS 2.9节点上升级CoreDNS后出现概率性解析超时的问题。
4.18.0-147.5.1.6.h841.eulerosv2r9.x86_64	2023年1月	更新系统内核，修复安全漏洞。
4.18.0-147.5.1.6.h766.eulerosv2r9.x86_64	2022年12月	更新系统内核，修复安全漏洞。

EulerOS 2.9 (ARM)

内核版本	发布时间	发布说明
4.19.90-vhulk2103.1.0.h1144.eulerosv2r9.aarch64	2024年4月	更新系统内核，修复安全漏洞。
4.19.90-vhulk2103.1.0.h1060.eulerosv2r9.aarch64	2023年12月	更新系统内核，修复安全漏洞。

内核版本	发布时间	发布说明
4.19.90-vhulk2103.1.0.h990.eulerosv2r9.aarch64	2023年6月	<ul style="list-style-type: none">更新系统内核，修复安全漏洞。修复IPVS模式下，EulerOS 2.9节点上升级CoreDNS后出现概率性解析超时的问题。
4.19.90-vhulk2103.1.0.h848.eulerosv2r9.aarch64	2023年1月	更新系统内核，修复安全漏洞。

CentOS 7.6

内核版本	发布时间	发布说明
3.10.0-1160.108.1.el7.x86_64	2024年4月	更新系统内核，修复安全漏洞。
3.10.0-1160.92.1.el7.x86_64	2023年12月	更新系统内核，修复安全漏洞。
3.10.0-1160.90.1.el7.x86_64	2023年8月	更新系统内核，修复安全漏洞。
3.10.0-1160.66.1.el7.x86_64	2023年1月	<ul style="list-style-type: none">更新系统内核，修复安全漏洞。修复CentOS节点出现容器OOM时，偶现ext4文件系统卡死问题。

EulerOS 2.8 (ARM) (停止维护)

内核版本	发布时间	发布说明
4.19.36-vhulk1907.1.0.h1350.eulerosv2r8.aarch64	2022年12月	更新系统内核，修复安全漏洞。

EulerOS 2.5 (停止维护)

内核版本	发布时间	发布说明
3.10.0-862.14.1.5.h687.eulerosv2r7.x86_64	2022年12月	更新系统内核，修复安全漏洞。

EulerOS 2.3 (停止维护)

内核版本	发布时间	发布说明
3.10.0-514.41.4.28.h62.x86_64	2022年12月	更新系统内核，修复安全漏洞。

Ubuntu 18.04 (停止维护)

内核版本	发布时间	发布说明
4.15.0-171-generic	2023年1月	更新系统内核，修复安全漏洞。

5.3 插件版本发布记录

5.3.1 CoreDNS 域名解析插件版本发布记录

表 5-14 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
1.29.4	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	适配CCE v1.29集群	1.10.1
1.28.7	v1.21 v1.23 v1.25 v1.27 v1.28	支持插件热更新配置，无需滚动升级	1.10.1
1.28.5	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题	1.10.1

插件版本	支持的集群版本	更新特性	社区版本
1.28.4	v1.21 v1.23 v1.25 v1.27 v1.28	适配CCE v1.28集群	1.10.1
1.27.4	v1.19 v1.21 v1.23 v1.25 v1.27	-	1.10.1
1.25.14	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">支持插件规格与集群规格联动插件与节点时区一致	1.10.1
1.25.11	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">支持插件实例AZ反亲和配置升级至社区版本 1.10.1	1.10.1
1.25.1	v1.19 v1.21 v1.23 v1.25	适配CCE v1.25集群	1.8.4
1.23.3	v1.15 v1.17 v1.19 v1.21 v1.23	插件依赖例行升级	1.8.4
1.23.2	v1.15 v1.17 v1.19 v1.21 v1.23	插件依赖例行升级	1.8.4

插件版本	支持的集群版本	更新特性	社区版本
1.23.1	v1.15 v1.17 v1.19 v1.21 v1.23	适配CCE v1.23集群	1.8.4
1.17.15	v1.15 v1.17 v1.19 v1.21	适配CCE v1.21集群	1.8.4
1.17.9	v1.15 v1.17 v1.19	插件依赖例行升级	1.8.4
1.17.7	v1.15 v1.17 v1.19	同步至社区v1.8.4版本	1.8.4
1.17.4	v1.17 v1.19	适配CCE v1.19集群	1.6.5
1.17.3	v1.17	支持v1.17集群，修复存根域配置问题	1.6.5
1.17.1	v1.17	支持v1.17集群	1.6.5

5.3.2 CCE 容器存储插件（Everest）版本发布记录

表 5-15 CCE 容器存储插件（Everest）版本记录

插件版本	支持的集群版本	更新特性
2.4.8	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	<ul style="list-style-type: none">• 适配CCE v1.29集群• 支持GPSSD2类型磁盘• 支持DSS专属分布式存储

插件版本	支持的集群版本	更新特性
2.3.23	v1.21 v1.23 v1.25 v1.27 v1.28	支持在SFS Turbo文件系统中创建子目录
2.3.21	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题
2.3.14	v1.21 v1.23 v1.25 v1.27 v1.28	适配CCE v1.28版本
2.1.51	v1.19 v1.21 v1.23 v1.25 v1.27	支持HCE OS 2.0系统
2.1.30	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">支持插件实例AZ反亲和配置obsfs包适配Ubuntu 22.04
2.1.13	v1.19 v1.21 v1.23 v1.25	SFS Turbo存储卷subpath PVC批创性能优化
2.1.9	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">支持controller优雅退出适配CCE v1.25版本
2.0.9	v1.19 v1.21 v1.23	<ul style="list-style-type: none">对 everest 部分代码及架构进行重构，改善代码架构，提高插件的可扩展性和稳定性支持优雅退出支持OBS进程监控

插件版本	支持的集群版本	更新特性
1.3.28	v1.19 v1.21 v1.23	<ul style="list-style-type: none">支持优雅退出支持OBS进程监控
1.3.22	v1.19 v1.21 v1.23	修复重复挂盘偶现挂载后读写失败的问题
1.3.20	v1.19 v1.21 v1.23	修复重复挂盘偶现挂载后读写失败的问题
1.3.17	v1.19 v1.21 v1.23	<ul style="list-style-type: none">调整everest-csi-driver滚动更新的最大不可用数：从10更新到10%自定义规格支持Pod反亲和统计节点上可由csi插件管理的scsi卷个数的上限支持Driver自定义资源规格部署
1.3.8	v1.23	适配CCE v1.23集群
1.3.6	v1.23	适配CCE v1.23集群
1.2.78	v1.15 v1.17 v1.19 v1.21	支持插件实例AZ反亲和配置
1.2.70	v1.15 v1.17 v1.19 v1.21	SFS Turbo存储卷subpath PVC批创性能优化
1.2.67	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none">支持controller优雅退出支持OBS进程监控
1.2.61	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none">支持优雅退出支持OBS进程监控

插件版本	支持的集群版本	更新特性
1.2.55	v1.15 v1.17 v1.19 v1.21	修复重复挂盘偶现挂载后读写失败的问题
1.2.53	v1.15 v1.17 v1.19 v1.21	修复重复挂盘偶现挂载后读写失败的问题
1.2.51	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none">● 调整everest-csi-driver滚动更新的最大不可用数：从10更新到10%● 自定义规格支持Pod反亲和● 统计节点上可由csi插件管理的scsi卷个数的上限
1.2.44	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none">● EVS、OBS存储卷支持选择企业项目● OBS对象桶挂载默认不再使用enable_noobj_cache参数
1.2.42	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none">● EVS、OBS存储卷支持选择企业项目● OBS对象桶挂载默认不再使用enable_noobj_cache参数
1.2.30	v1.15 v1.17 v1.19 v1.21	CCE支持EmptyDir
1.2.28	v1.15 v1.17 v1.19 v1.21	适配CCE v1.21集群
1.2.27	v1.15 v1.17 v1.19 v1.21	支持极速型SSD(ESSD)、通用型SSD(GPSSD)类型云硬盘
1.2.13	v1.15 v1.17 v1.19	支持EulerOS 2.10系统。

插件版本	支持的集群版本	更新特性
1.2.9	v1.15 v1.17 v1.19	<ul style="list-style-type: none"> 增强PV资源生命周期维护的可靠性 支持1.19.10版本集群使用Attach/Detach Controller挂卸卷能力 提高SFS挂载稳定性 新建集群EVS默认创建类型调整为SAS
1.2.5	v1.15 v1.17 v1.19	<ul style="list-style-type: none"> 提升挂载相关能力可靠性 优化了使用OBS存储时的认证功能，需要用户上传密钥 提高everest插件对flexvolume卷的兼容能力 提高插件运行稳定性
1.1.12	v1.15 v1.17	优化和增强everest-csi-controller组件可靠性
1.1.11	v1.15 v1.17	<ul style="list-style-type: none"> 配置安全加固 支持挂载三方OBS存储 切换更优性能的EVS查询接口 默认快照以clone模式创建磁盘 优化和增强Attach和Detach磁盘状态检测和日志输出 增加认证过期判断可靠性
1.1.8	v1.15 v1.17	支持CCE v1.17, v1.13升级到v1.15场景支持接管Flexvolume
1.1.7	v1.15 v1.17	支持CCE v1.17, v1.13升级到v1.15场景支持接管Flexvolume

5.3.3 CCE 节点故障检测插件版本发布记录

表 5-16 CCE 节点故障检测插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.19.1	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	修复部分问题	0.8.10

插件版本	支持的集群版本	更新特性	社区版本
1.19.0	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题	0.8.10
1.18.48	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题	0.8.10
1.18.46	v1.21 v1.23 v1.25 v1.27 v1.28	适配CCE v1.28版本	0.8.10
1.18.22	v1.19 v1.21 v1.23 v1.25 v1.27	-	0.8.10
1.18.14	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none"> 支持插件实例AZ反亲和配置 支持在竞价实例被释放前给节点加污点，驱逐节点上的pod 插件挂载节点时区 	0.8.10
1.18.10	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none"> 配置界面优化 优化DiskSlow检查项，支持阈值配置 优化NTPProblem检查项，支持阈值配置 支持插件实例AZ反亲和配置 支持竞价实例中断检测，中断前驱逐节点上的pod 	0.8.10

插件版本	支持的集群版本	更新特性	社区版本
1.17.4	v1.17 v1.19 v1.21 v1.23 v1.25	优化DiskHung检查项	0.8.10
1.17.3	v1.17 v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">• NPC最大可打污点节点数支持百分比配置• 新增进程Z状态检查项 ProcessZ• 优化NTPProblem检查项，支持检测时间偏差• 修复BMS节点场景存在常驻D状态进程，干扰 ProcessD检查项	0.8.10
1.17.2	v1.17 v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">• 新增磁盘卡IO检查项 DiskHung• 新增磁盘慢IO检查项 DiskSlow• 新增进程D状态检查项 ProcessD• 新增挂载点健康检查 MountPointProblem• 避免与Service端口范围冲突，默认健康检查监听端口修改为19900，默认 Prometheus指标暴露端口修改为19901。• 新增支持1.25集群版本	0.8.10
1.16.4	v1.17 v1.19 v1.21 v1.23	<ul style="list-style-type: none">• 新增beta检查项 ScheduledEvent，支持通过metadata接口检测宿主机异常导致虚拟机进行冷热迁移事件。该检查项默认不开启。	0.8.10
1.16.3	v1.17 v1.19 v1.21 v1.23	新增ResolvConf配置文件检查。	0.8.10

插件版本	支持的集群版本	更新特性	社区版本
1.16.1	v1.17 v1.19 v1.21 v1.23	<ul style="list-style-type: none">新增node-problem-controller。支持基本故障隔离能力。新增PID、FD、磁盘、内存、临时卷存储池、持久卷存储池检查项。	0.8.10
1.15.0	v1.17 v1.19 v1.21 v1.23	<ul style="list-style-type: none">检测项全面加固，避免误报。支持内核巡检。支持OOMKilling事件，TaskHung事件上报。	0.8.10
1.14.11	v1.17 v1.19 v1.21	适配CCE v1.21集群	0.7.1
1.14.5	v1.17 v1.19	修复监控指标无法被获取的问题	0.7.1
1.14.4	v1.17 v1.19	<ul style="list-style-type: none">适配containerd运行时节点	0.7.1
1.14.2	v1.17 v1.19	<ul style="list-style-type: none">适配CCE v1.19集群新增支持Ubuntu操作系统和安全容器场景	0.7.1
1.13.8	v1.15.11 v1.17	<ul style="list-style-type: none">修复容器隧道网络下CNI健康检查问题调整资源配额	0.7.1
1.13.6	v1.15.11 v1.17	修复僵尸进程未被回收的问题	0.7.1
1.13.5	v1.15.11 v1.17	增加污点容忍配置	0.7.1
1.13.2	v1.15.11 v1.17	增加资源限制，增强cni插件的检测能力	0.7.1

5.3.4 Kubernetes Dashboard 插件版本发布记录

表 5-17 Kubernetes Dashboard 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
2.2.27	v1.21 v1.23 v1.25	修复部分问题	2.7.0
2.2.7	v1.21 v1.23 v1.25	-	2.7.0
2.2.5	v1.21 v1.23 v1.25	插件与节点时区一致	2.7.0
2.2.3	v1.21 v1.23 v1.25	-	2.7.0
2.1.1	v1.19 v1.21 v1.23	<ul style="list-style-type: none">• 适配CCE v1.23集群• 更新至社区v2.5.0版本	2.5.0
2.0.10	v1.15 v1.17 v1.19 v1.21	适配CCE v1.21集群	2.0.0
2.0.4	v1.15 v1.17 v1.19	配置seccomp默认规则	2.0.0
2.0.3	v1.15 v1.17 v1.19	兼容CCE v1.15集群	2.0.0
2.0.2	v1.17 v1.19	适配CCE v1.19集群	2.0.0
2.0.1	v1.15 v1.17	-	2.0.0
2.0.0	v1.17	支持对接CCE v1.17	2.0.0

5.3.5 CCE 集群弹性引擎版本发布记录

表 5-18 v1.29 集群配套插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.29.13	v1.29	支持v1.29集群	1.29.1

表 5-19 v1.28 集群配套插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.28.51	v1.28	优化节点池资源售罄告警逻辑	1.28.1
1.28.22	v1.28	修复部分问题	1.28.1
1.28.20	v1.28	修复部分问题	1.28.1
1.28.17	v1.28	解决存在自定义控制器类型的Pod时无法扩容的问题	1.28.1

表 5-20 v1.27 集群配套插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.27.84	v1.27	优化节点池资源售罄告警逻辑	1.27.1
1.27.55	v1.27	修复部分问题	1.27.1
1.27.53	v1.27	修复部分问题	1.27.1
1.27.51	v1.27	修复部分问题	1.27.1
1.27.14	v1.27	修复多规格情况下无法扩容和非预期PreferNoSchedule污点问题	1.27.1

表 5-21 v1.25 集群配套插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.25.116	v1.25	优化节点池资源售罄告警逻辑	1.25.0
1.25.88	v1.25	修复部分问题	1.25.0
1.25.86	v1.25	修复部分问题	1.25.0
1.25.84	v1.25	修复部分问题	1.25.0

插件版本	支持的集群版本	更新特性	社区版本
1.25.46	v1.25	修复多规格情况下无法缩容和非预期PreferNoSchedule污点问题	1.25.0
1.25.34	v1.25	<ul style="list-style-type: none"> • 优化异构设备(GPU/NPU)识别方法 • 扩容节点数量超过集群规模时,使用集群支持的剩余节点数量进行扩容 	1.25.0
1.25.21	v1.25	<ul style="list-style-type: none"> • 修复autoscaler伸缩策略least-waste默认未启用的问题 • 修复节点池扩容失败后无法未切换到其他节点池扩容且插件有重启动作的问题 • 默认污点容忍时长修改为60s • 扩容规则禁用后仍然触发扩容 	1.25.0
1.25.11	v1.25	<ul style="list-style-type: none"> • 支持插件实例AZ反亲和配置 • 对创建临时存储卷的POD添加不可调度容忍时间 • 修复伸缩组资源不足时无法正常修复节点池数量问题 	1.25.0
1.25.7	v1.25	<ul style="list-style-type: none"> • 适配CCE v1.25集群 • 修改自定义规格的内存申请与限制 • 当没有开启弹性伸缩的节点池时上报无法伸缩的事件 • 修复NPU节点在扩容过程中会再次触发扩容的问题 	1.25.0

表 5-22 v1.23 集群配套插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.23.121	v1.23	优化节点池资源售罄告警逻辑	1.23.0
1.23.95	v1.23	修复部分问题	1.23.0
1.23.93	v1.23	修复部分问题	1.23.0
1.23.91	v1.23	修复部分问题	1.23.0
1.23.54	v1.23	修复多规格情况下无法缩容和非预期PreferNoSchedule污点问题	1.23.0

插件版本	支持的集群版本	更新特性	社区版本
1.23.44	v1.23	<ul style="list-style-type: none"> • 优化异构设备(GPU/NPU)识别方法 • 扩容节点数量超过集群规模时，使用集群支持的剩余节点数量进行扩容 	1.23.0
1.23.31	v1.23	<ul style="list-style-type: none"> • 修复autoscaler伸缩策略least-waste默认未启用的问题 • 修复节点池扩容失败后无法切换到其他节点池扩容且插件有重启动作的问题 • 默认污点容忍时长修改为60s • 扩容规则禁用后仍然触发扩容 	1.23.0
1.23.21	v1.23	<ul style="list-style-type: none"> • 支持插件实例AZ反亲和配置 • 对创建临时存储卷的POD添加不可调度容忍时间 • 修复伸缩组资源不足时无法正常修复节点池数量问题 	1.23.0
1.23.17	v1.23	<ul style="list-style-type: none"> • 适配NPU和安全容器 • 节点伸缩策略支持不设置步长 • bug修复，自动移除已删除的节点池 • 设置优先调度 • 注册EmptyDir调度策略 • 修复停用节点伸缩策略时，低于缩容阈值的节点未触发缩容的问题 • 修改自定义规格的内存申请与限制 • 当没有开启弹性伸缩的节点池时上报无法伸缩的事件 • 修复NPU节点在扩容过程中会再次触发扩容的问题 	1.23.0
1.23.10	v1.23	<ul style="list-style-type: none"> • 日志优化 • 支持缩容等待，等待用户在节点删除前完成数据转储等操作 	1.23.0
1.23.9	v1.23	新增 nodenetworkconfigs.crd.yangtse.cn i资源对象权限。	1.23.0

插件版本	支持的集群版本	更新特性	社区版本
1.23.8	v1.23	修复周期性扩容场景下，单次扩容数量超过节点池上限，扩容失败问题。	1.23.0
1.23.7	v1.23	-	1.23.0
1.23.3	v1.23	适配CCE v1.23集群	1.23.0

表 5-23 v1.21 集群配套插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.21.114	v1.21	优化节点池资源售罄告警逻辑	1.21.0
1.21.89	v1.21	修复部分问题	1.21.0
1.21.87	v1.21	修复部分问题	1.21.0
1.21.86	v1.21	修复配置节点AZ拓扑约束时，节点池弹性扩容后不符合预期问题	1.21.0
1.21.51	v1.21	修复多规格情况下无法缩容和非预期PreferNoSchedule污点问题	1.21.0
1.21.43	v1.21	<ul style="list-style-type: none">优化异构设备(GPU/NPU)识别方法扩容节点数量超过集群规模时，使用集群支持的剩余节点数量进行扩容	1.21.0
1.21.29	v1.21	<ul style="list-style-type: none">支持插件实例AZ反亲和配置对创建临时存储卷的POD添加不可调度容忍时间修复伸缩组资源不足时无法正常修复节点池数量问题修复节点池扩容失败后无法未切换到其他节点池扩容且插件有重启动作的问题默认污点容忍时长修改为60s扩容规则禁用后仍然触发扩容	1.21.0
1.21.20	v1.21	<ul style="list-style-type: none">支持插件实例AZ反亲和配置对创建临时存储卷的POD添加不可调度容忍时间修复伸缩组资源不足时无法正常修复节点池数量问题	1.21.0

插件版本	支持的集群版本	更新特性	社区版本
1.21.16	v1.21	<ul style="list-style-type: none"> • 适配NPU和安全容器 • 节点伸缩策略支持不设置步长 • bug修复，自动移除已删除的节点池 • 设置优先调度 • 注册EmptyDir调度策略 • 修复停用节点伸缩策略时，低于扩容阈值的节点未触发扩容的问题 • 修改自定义规格的内存申请与限制 • 当没有开启弹性伸缩的节点池时上报无法伸缩的事件 • 修复NPU节点在扩容过程中会再次触发扩容的问题 	1.21.0
1.21.9	v1.21	<ul style="list-style-type: none"> • 日志优化 • 支持扩容等待，等待用户在节点删除前完成数据转储等操作 	1.21.0
1.21.8	v1.21	新增 nodenetworkconfigs.crd.yangtse.cn i资源对象权限	1.21.0
1.21.6	v1.21	修复插件请求重试场景下签名错误导致鉴权失败的问题	1.21.0
1.21.4	v1.21	修复插件请求重试场景下签名错误导致鉴权失败的问题	1.21.0
1.21.2	v1.21	修复未注册节点删除失败可能阻塞弹性伸缩的问题	1.21.0
1.21.1	v1.21	修复在已有的周期弹性伸缩规则里节点池修改不生效的问题。	1.21.0

表 5-24 v1.19 集群配套插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.19.76	v1.19	<ul style="list-style-type: none"> • 优化异构设备(GPU/NPU)识别方法 • 扩容节点数量超过集群规模时，使用集群支持的剩余节点数量进行扩容 	1.19.0

插件版本	支持的集群版本	更新特性	社区版本
1.19.56	v1.19	修复多规格情况下无法缩容和非预期PreferNoSchedule污点问题	1.19.0
1.19.48	v1.19	<ul style="list-style-type: none"> • 优化异构设备(GPU/NPU)识别方法 • 扩容节点数量超过集群规模时,使用集群支持的剩余节点数量进行扩容 	1.19.0
1.19.35	v1.19	<ul style="list-style-type: none"> • 支持插件实例AZ反亲和配置 • 对创建临时存储卷的POD添加不可调度容忍时间 • 修复伸缩组资源不足时无法正常修复节点池数量问题 • 修复节点池扩容失败后无法未切换到其他节点池扩容且插件有重启动作的问题 • 默认污点容忍时长修改为60s • 扩容规则禁用后仍然触发扩容 	1.19.0
1.19.27	v1.19	<ul style="list-style-type: none"> • 支持插件实例AZ反亲和配置 • 对创建临时存储卷的POD添加不可调度容忍时间 • 修复伸缩组资源不足时无法正常修复节点池数量问题 	1.19.0
1.19.22	v1.19	<ul style="list-style-type: none"> • 适配NPU和安全容器 • 节点伸缩策略支持不设置步长 • bug修复,自动移除已删除的节点池 • 设置优先调度 • 注册EmptyDir调度策略 • 修复停用节点伸缩策略时,低于扩容阈值的节点未触发扩容的问题 • 修改自定义规格的内存申请与限制 • 当没有开启弹性伸缩的节点池时上报无法伸缩的事件 • 修复NPU节点在扩容过程中会再次触发扩容的问题 	1.19.0

插件版本	支持的集群版本	更新特性	社区版本
1.19.14	v1.19	<ul style="list-style-type: none"> 日志优化 支持缩容等待，等待用户在节点删除前完成数据转储等操作 	1.19.0
1.19.13	v1.19	修复周期性扩容场景下，单次扩容数量超过节点池上限，扩容失败问题	1.19.0
1.19.12	v1.19	修复插件请求重试场景下签名错误导致鉴权失败的问题	1.19.0
1.19.11	v1.19	修复插件请求重试场景下签名错误导致鉴权失败的问题	1.19.0
1.19.9	v1.19	修复未注册节点删除失败可能阻塞弹性伸缩的问题	1.19.0
1.19.8	v1.19	修复在已有的周期弹性伸缩规则里节点池修改不生效的问题。	1.19.0
1.19.7	v1.19	插件依赖例行升级。	1.19.0
1.19.6	v1.19	修复污点异步更新场景触发的重复扩容问题。	1.19.0
1.19.3	v1.19	定时策略中能够根据节点总数，CPU，内存限制进行扩缩容。修复其它功能缺陷。	1.19.0

表 5-25 v1.17 集群配套插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.17.27	v1.17	<ul style="list-style-type: none"> 日志优化 bug修复，自动移除已删除的节点池 设置优先调度 修复刚扩容出的节点打污点会被覆盖的问题 修复停用节点伸缩策略时，低于缩容阈值的节点未触发缩容的问题 修改自定义规格的内存申请与限制 当没有开启弹性伸缩的节点池时上报无法伸缩的事件 	1.17.0

插件版本	支持的集群版本	更新特性	社区版本
1.17.22	v1.17	日志优化	1.17.0
1.17.21	v1.17	修复周期性扩容场景下，单次扩容数量超过节点池上限，扩容失败问题	1.17.0
1.17.19	v1.17	修复插件请求重试场景下签名错误导致鉴权失败的问题	1.17.0
1.17.17	v1.17	修复未注册节点删除失败可能阻塞弹性伸缩的问题	1.17.0
1.17.16	v1.17	修复在已有的周期弹性伸缩规则里节点池修改不生效的问题。	1.17.0
1.17.15	v1.17	资源规格配置单位统一化	1.17.0
1.17.14	v1.17	修复Taints异步更新场景触发的重复扩容问题。	1.17.0
1.17.8	v1.17	Bug修复	1.17.0
1.17.7	v1.17	添加日志内容，Bug修复	1.17.0
1.17.5	v1.17	支持v1.17版本的集群，支持页面显示伸缩事件	1.17.0
1.17.2	v1.17	支持v1.17版本的集群	1.17.0

5.3.6 NGINX Ingress 控制器插件版本发布记录

表 5-26 NGINX Ingress 控制器插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
2.6.4	v1.25 v1.27 v1.28 v1.29	适配CCE v1.29集群	1.9.3
2.5.6	v1.25 v1.27 v1.28	修复部分问题	1.9.3

插件版本	支持的集群版本	更新特性	社区版本
2.5.4	v1.25 v1.27 v1.28	<ul style="list-style-type: none">• 同一集群支持安装多套 NGINX Ingress控制器• 支持通过控制台配置 nginx-ingress默认证书• 支持将NGINX Ingress控制器指标上报至 Prometheus	1.9.3
2.4.6	v1.25 v1.27 v1.28	<ul style="list-style-type: none">• 适配CCE v1.28集群• 支持开启准入校验• 支持优雅退出、无损升级能力• 插件多可用区部署模式支持选择均匀分布• 修复CVE-2023-44487漏洞	1.9.3
2.3.5	v1.27	-	1.8.0
2.2.52	v1.23 v1.25	<ul style="list-style-type: none">• 同一集群支持安装多套 NGINX Ingress控制器• 支持通过控制台配置 nginx-ingress默认证书	1.5.1
2.2.42	v1.23 v1.25	<ul style="list-style-type: none">• 支持优雅退出、无损升级能力• 插件多可用区部署模式支持选择均匀分布	1.5.1
2.2.7	v1.25	<ul style="list-style-type: none">• 插件挂载节点时区• 支持双栈	1.5.1
2.2.3	v1.25	<ul style="list-style-type: none">• 支持插件实例AZ反亲和配置• 对创建临时存储卷的POD添加不可调度容忍时间• 默认污点容忍时长修改为60s	1.5.1
2.2.1	v1.25	<ul style="list-style-type: none">• 适配CCE v1.25集群• 更新至社区v1.5.1版本	1.5.1
2.1.33	v1.19 v1.21 v1.23	<ul style="list-style-type: none">• 支持优雅退出、无损升级能力• 插件多可用区部署模式支持选择均匀分布	1.2.1

插件版本	支持的集群版本	更新特性	社区版本
2.1.9	v1.19 v1.21 v1.23	<ul style="list-style-type: none">支持插件实例AZ反亲和配置默认污点容忍时长修改为60s插件挂载节点时区支持双栈	1.2.1
2.1.5	v1.19 v1.21 v1.23	<ul style="list-style-type: none">支持插件实例AZ反亲和配置默认污点容忍时长修改为60s	1.2.1
2.1.3	v1.19 v1.21 v1.23	nginx-ingress支持开启publishService开关	1.2.1
2.1.1	v1.19 v1.21 v1.23	更新至社区v1.2.1版本	1.2.1
2.1.0	v1.19 v1.21 v1.23	<ul style="list-style-type: none">更新至社区v1.2.0版本修复CVE-2021-25746漏洞，新增规则禁用一些存在越权风险的Anntotations值修复CVE-2021-25745漏洞，新增规则禁用一些存在越权风险的访问路径	1.2.0
2.0.1	v1.19 v1.21 v1.23	<ul style="list-style-type: none">适配CCE v1.23集群更新至社区v1.1.1版本	1.1.1
1.3.2	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none">适配CCE v1.21集群同步至社区v0.49.3版本	0.49.3
1.2.6	v1.15 v1.17 v1.19	配置seccomp默认规则	0.46.0
1.2.5	v1.15 v1.17 v1.19	同步至社区v0.46.0版本	0.46.0

插件版本	支持的集群版本	更新特性	社区版本
1.2.3	v1.15 v1.17 v1.19	适配CCE v1.19集群	0.43.0
1.2.2	v1.15 v1.17	同步至社区v0.43.0版本	0.43.0

5.3.7 Kubernetes Metrics Server 插件版本发布记录

表 5-27 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
1.3.60	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	适配CCE v1.29集群	0.6.2
1.3.39	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题	0.6.2
1.3.37	v1.21 v1.23 v1.25 v1.27 v1.28	适配CCE v1.28集群	0.6.2
1.3.12	v1.19 v1.21 v1.23 v1.25 v1.27	-	0.6.2
1.3.8	v1.19 v1.21 v1.23 v1.25	插件挂载节点时区	0.6.2

插件版本	支持的集群版本	更新特性	社区版本
1.3.6	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">支持插件实例AZ反亲和配置默认污点容忍时长修改为60s	0.6.2
1.3.3	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">适配CCE v1.25集群CronHPA调整Deployment实例数，新增skip场景	0.6.2
1.3.2	v1.19 v1.21 v1.23 v1.25	适配CCE v1.25集群	0.6.2
1.2.1	v1.19 v1.21 v1.23	适配CCE v1.23集群	0.4.4
1.1.10	v1.15 v1.17 v1.19 v1.21	适配CCE v1.21集群	0.4.4
1.1.4	v1.15 v1.17 v1.19	资源规格配置单位统一化	0.4.4
1.1.2	v1.15 v1.17 v1.19	同步至社区v0.4.4版本	0.4.4
1.1.1	v1.13 v1.15 v1.17 v1.19	支持自定义资源规格配置，最大无效实例数改为1	0.3.7
1.1.0	v1.13 v1.15 v1.17 v1.19	适配CCE v1.19集群	0.3.7
1.0.5	v1.13 v1.15 v1.17	更新至社区v0.3.7版本	0.3.7

5.3.8 CCE 容器弹性引擎插件版本发布记录

表 5-28 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
1.4.2	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	适配CCE v1.29集群
1.3.43	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题
1.3.42	v1.21 v1.23 v1.25 v1.27 v1.28	适配CCE v1.28集群
1.3.14	v1.19 v1.21 v1.23 v1.25 v1.27	适配CCE v1.27集群
1.3.10	v1.19 v1.21 v1.23 v1.25	周期规则不受冷却时间影响定时触发
1.3.7	v1.19 v1.21 v1.23 v1.25	支持插件实例AZ反亲和配置

插件版本	支持的集群版本	更新特性
1.3.3	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">• 适配CCE v1.25集群• CronHPA调整Deployment实例数，新增skip场景
1.3.1	v1.19 v1.21 v1.23	适配CCE v1.23集群
1.2.12	v1.15 v1.17 v1.19 v1.21	插件性能优化，降低资源消耗
1.2.11	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none">• 从K8s Metrics API查询资源指标• 计算资源利用率时考虑未就绪的Pod
1.2.10	v1.15 v1.17 v1.19 v1.21	适配CCE v1.21集群
1.2.4	v1.15 v1.17 v1.19	<ul style="list-style-type: none">• 插件依赖例行升级• 支持配置插件资源规格
1.2.3	v1.15 v1.17 v1.19	适配ARM64节点部署
1.2.2	v1.15 v1.17 v1.19	增强健康检查能力
1.2.1	v1.15 v1.17 v1.19	<ul style="list-style-type: none">• 适配CCE v1.19集群• 更新插件为稳定版本
1.1.3	v1.15 v1.17	支持周期扩缩容规则

5.3.9 CCE 突发弹性引擎（对接 CCI）插件版本发布记录

表 5-29 CCE 突发弹性引擎（对接 CCI）插件版本记录

插件版本	支持的集群版本	更新特性
1.3.57	v1.21 v1.23 v1.25 v1.27 v1.28	适配CCE v1.28集群。
1.3.48	v1.21 v1.23 v1.25 v1.27	<ul style="list-style-type: none">• 支持v1.25、v1.27版本集群• 支持JuiceFS类型的存储
1.3.25	v1.17 v1.19 v1.21 v1.23	<ul style="list-style-type: none">• 支持DownwardAPI Volume• 支持Projected Volume• 支持自定义StorageClass
1.3.19	v1.17 v1.19 v1.21 v1.23	支持schedule profile
1.3.7	v1.17 v1.19 v1.21 v1.23	支持v1.21、v1.23版本集群
1.2.12	v1.13 v1.15 v1.17 v1.19	<ul style="list-style-type: none">• 新增了部分metrics指标• 支持HPA与CustomedHPA• 支持将弹性到CCI的Pod中的hostPath转换为其它类型存储• 修复Kubernetes Dashboard无法使用终端问题

插件版本	支持的集群版本	更新特性
1.2.5	v1.13 v1.15 v1.17 v1.19	<ul style="list-style-type: none"> 自动清理CCI中不再被Pod依赖的资源 支持配置Requests与Limits不相等，弹性到CCI时的资源申请量以Limits为准 修复CCI命名空间不存在时插件卸载失败问题 增加对Pod规格超过CCI限制的创建请求的拦截
1.2.0	v1.13 v1.15 v1.17 v1.19	<ul style="list-style-type: none"> 支持v1.19版本集群 支持SFS、SFS Turbo类型存储 支持CronJob 支持配置envFrom 日志文件自动转储 屏蔽TCPSocket类型健康检查 支持配置资源标签（pod-tag） 提升了性能和可靠性 修复了一些已知问题
1.0.5	v1.13 v1.15 v1.17	支持v1.17版本集群

5.3.10 CCE AI 套件（NVIDIA GPU）版本发布记录

表 5-30 CCE AI 套件（NVIDIA GPU）版本记录

插件版本	支持的集群版本	更新特性
2.6.4	v1.28 v1.29	更新GPU卡逻辑隔离逻辑
2.6.1	v1.28 v1.29	升级GPU插件基础镜像
2.5.6	v1.28	修复安装驱动的问题
2.5.4	v1.28	支持v1.28集群

插件版本	支持的集群版本	更新特性
2.0.69	v1.21 v1.23 v1.25 v1.27	升级GPU插件基础镜像
2.0.46	v1.21 v1.23 v1.25 v1.27	<ul style="list-style-type: none"> 支持535版本Nvidia驱动 支持非root用户使用XGPU 优化启动逻辑
2.0.18	v1.21 v1.23 v1.25 v1.27	支持HCE 2.0
1.2.28	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none"> 适配OS Ubuntu22.04 GPU驱动目录自动挂载优化
1.2.24	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none"> 节点池支持配置GPU驱动版本 支持GPU指标采集
1.2.20	v1.19 v1.21 v1.23 v1.25	设置插件别名为gpu
1.2.17	v1.15 v1.17 v1.19 v1.21 v1.23	增加nvidia-driver-install pod limits 配置
1.2.15	v1.15 v1.17 v1.19 v1.21 v1.23	适配CCE v1.23集群

插件版本	支持的集群版本	更新特性
1.2.11	v1.15 v1.17 v1.19 v1.21	支持EulerOS 2.10系统
1.2.10	v1.15 v1.17 v1.19 v1.21	CentOS系统支持新版本GPU驱动
1.2.9	v1.15 v1.17 v1.19 v1.21	适配CCE v1.21集群
1.2.2	v1.15 v1.17 v1.19	适配EulerOS新内核
1.2.1	v1.15 v1.17 v1.19	<ul style="list-style-type: none">• 适配CCE v1.19集群• 插件增加污点容忍
1.1.13	v1.13 v1.15 v1.17	支持Centos7.6 3.10.0-1127.19.1.el7.x86_64内核 系统
1.1.11	v1.15 v1.17	<ul style="list-style-type: none">• 支持用户自定义驱动地址下载 驱动• 支持v1.15、v1.17集群

5.3.11 CCE AI 套件（Ascend NPU）版本发布记录

表 5-31 CCE AI 套件（Ascend NPU）插件版本记录

插件版本	支持的集群版本	更新特性
2.1.5	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	<ul style="list-style-type: none">• 适配CCE v1.29集群• 新增静默故障码

插件版本	支持的集群版本	更新特性
2.0.9	v1.21 v1.23 v1.25 v1.27 v1.28	修复进程级故障恢复和给工作负载添加注解偶现失败问题
2.0.5	v1.21 v1.23 v1.25 v1.27 v1.28	<ul style="list-style-type: none">• 适配CCE v1.28集群• 支持存活探针检查机制
1.2.14	v1.19 v1.21 v1.23 v1.25 v1.27	支持NPU监控
1.2.6	v1.19 v1.21 v1.23 v1.25	支持NPU驱动自动安装
1.2.5	v1.19 v1.21 v1.23 v1.25	支持NPU驱动自动安装
1.2.4	v1.19 v1.21 v1.23 v1.25	适配CCE v1.25集群
1.2.2	v1.19 v1.21 v1.23	适配CCE v1.23集群
1.2.1	v1.19 v1.21 v1.23	适配CCE v1.23集群

插件版本	支持的集群版本	更新特性
1.1.8	v1.15 v1.17 v1.19 v1.21	适配CCE v1.21集群
1.1.2	v1.15 v1.17 v1.19	配置seccomp默认规则
1.1.1	v1.15 v1.17 v1.19	兼容CCE v1.15集群
1.1.0	v1.17 v1.19	适配CCE v1.19集群
1.0.8	v1.13 v1.15 v1.17	适配D310 C75驱动
1.0.6	v1.13 v1.15 v1.17	支持昇腾C75驱动
1.0.5	v1.13 v1.15 v1.17	支持容器里使用huawei NPU设备的管理插件
1.0.3	v1.13 v1.15 v1.17	支持容器里使用huawei NPU设备的管理插件

5.3.12 Volcano 调度器版本发布记录

表 5-32 Volcano 调度器版本记录

插件版本	支持的集群版本	更新特性
1.12.18	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	<ul style="list-style-type: none">• 适配CCE v1.29集群• 默认开启抢占功能
1.12.1	v1.19.16 v1.21 v1.23 v1.25 v1.27 v1.28	应用弹性扩缩容性能优化
1.11.21	v1.19.16 v1.21 v1.23 v1.25 v1.27 v1.28	<ul style="list-style-type: none">• 支持Kubernetes v1.28• 支持负载感知调度• 镜像OS更新为HCE 2.0• 优化CSI资源抢占能力• 优化负载感知重调度能力• 优化混部场景抢占能力
1.11.6	v1.19.16 v1.21 v1.23 v1.25 v1.27	<ul style="list-style-type: none">• 支持Kubernetes v1.27• 支持重调度功能• 支持节点池亲和调度能力• 优化调度性能
1.10.7	v1.19.16 v1.21 v1.23 v1.25	修复本地持久卷插件未计算预绑定到节点的pod的问题

插件版本	支持的集群版本	更新特性
1.10.5	v1.19.16 v1.21 v1.23 v1.25	<ul style="list-style-type: none">• volcano agent支持资源超卖。• 添加针对GPU资源字段的校验 admission: nvidia.com/gpu应小于1或者为正整数, volcano.sh/gpu-core.percentage应小于100并为5的倍数。• 修复存在PVC绑定失败的场景下, 后续提交Pod调度慢的问题。• 修复节点上存在长时间Terminating Pod场景下, 新提交Pod无法运行的问题。• 修复并发创建挂载PVC的Pod的场景下, volcano重启的问题。
1.9.1	v1.19.16 v1.21 v1.23 v1.25	<ul style="list-style-type: none">• 修复networkresource插件计数 pipeline pod占用subeni问题• 修复binpack插件对资源不足节点打分问题• 修复对结束状态未知的Pod的资源处理• 优化事件输出• 默认高可用部署
1.7.2	v1.19.16 v1.21 v1.23 v1.25	<ul style="list-style-type: none">• Volcano支持v1.25集群• 提升Volcano调度性能
1.7.1	v1.19.16 v1.21 v1.23 v1.25	Volcano支持v1.25集群
1.4.7	v1.15 v1.17 v1.19 v1.21	删除Pod状态Undetermined, 以适配集群Autoscaler的弹性能力。
1.4.5	v1.17 v1.19 v1.21	volcano-scheduler的部署方式由StatefulSet调整为Deployment, 修复节点异常时Pod无法自动迁移的问题

插件版本	支持的集群版本	更新特性
1.4.2	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none"> 修复跨GPU分配失败问题 适配更新后的EAS API
1.3.7	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none"> 支持在/离线作业混合部署及资源超卖功能 优化集群调度吞吐性能 修复特定场景下调度器panic的问题 修复CCE v1.15集群中volcano作业volumes.secret校验失败的问题 修复挂载volume，作业调度不成功的问题
1.3.3	v1.15 v1.17 v1.19 v1.21	修复GPU异常导致的调度器崩溃问题；修复特权Init容器准入失败问题
1.3.1	v1.15 v1.17 v1.19	<ul style="list-style-type: none"> 升级Volcano框架到最新版本 支持Kubernetes v1.19版本 添加numa-aware插件 修复多队列场景下Deployment扩缩容的问题 调整默认开启的算法插件
1.2.5	v1.15 v1.17 v1.19	<ul style="list-style-type: none"> 修复某些场景下OutOfcpu的问题 修复queue设置部分capability情况下Pod无法调度问题 支持volcano组件日志时间与系统时间保持一致 修复队列间多抢占问题 修复ioaware插件在某些极端场景下结果不符合预期的问题 支持混合集群

插件版本	支持的集群版本	更新特性
1.2.3	v1.15 v1.17 v1.19	<ul style="list-style-type: none"> 修复因为精度不够引发的训练任务OOM的问题 修复CCE v1.15以上版本GPU调度的问题，暂不支持任务分发时的CCE版本滚动升级 修复特定场景下队列状态不明的问题 修复特定场景下作业挂载PVC panic的问题 修复GPU作业无法配置小数的问题 添加ioaware插件 添加ring controller

5.3.13 CCE 密钥管理（对接 DEW）插件版本发布记录

表 5-33 CCE 密钥管理（对接 DEW）插件版本记录

插件版本	支持的集群版本	更新特性
1.1.2	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	<ul style="list-style-type: none"> 适配CCE v1.29集群 支持同步csms凭据时创建secret
1.0.31	v1.21 v1.23 v1.25 v1.27 v1.28	<ul style="list-style-type: none"> 适配CCE v1.27集群 适配CCE v1.28集群
1.0.9	v1.19 v1.21 v1.23 v1.25	-
1.0.6	v1.19 v1.21 v1.23 v1.25	-

插件版本	支持的集群版本	更新特性
1.0.3	v1.19 v1.21 v1.23 v1.25	适配CCE v1.25集群
1.0.2	v1.19 v1.21 v1.23	适配CCE v1.23集群
1.0.1	v1.19 v1.21	支持主动感知SecretProviderClass对象的变化

5.3.14 CCE 容器网络扩展指标插件版本发布记录

表 5-34 CCE 容器网络扩展指标插件版本记录

插件版本	支持的集群版本	更新特性
1.4.5	v1.23 v1.25 v1.27 v1.28 v1.29	<ul style="list-style-type: none"> 支持普通容器Pod粒度的UDP、TCP drop、TCP connect fail监控 支持普通容器flow粒度的UDP、TCP drop监控 支持HCE 2.0 x86和HCE 2.0 ARM 支持CCE v1.29集群
1.3.10	v1.23 v1.25 v1.27 v1.28	修复部分问题
1.3.8	v1.23 v1.25 v1.27 v1.28	<ul style="list-style-type: none"> 支持普通容器pod粒度的IP和TCP监控 支持普通容器flow粒度的IP和TCP监控 支持CCE v1.27集群 支持CCE v1.28集群
1.2.27	v1.19 v1.21 v1.23 v1.25	-

插件版本	支持的集群版本	更新特性
1.2.4	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">增加不支持EulerOS以外操作系统描述
1.2.2	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">本地Pod VPC网络健康检查
1.1.8	v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">适配CCE v1.25集群
1.1.6	v1.19 v1.21 v1.23	-
1.1.5	v1.19 v1.21 v1.23	<ul style="list-style-type: none">liveness健康检查优化
1.1.2	v1.19 v1.21 v1.23	<ul style="list-style-type: none">支持操作系统类型宽匹配
1.0.1	v1.19 v1.21	<ul style="list-style-type: none">支持流量统计数据持久化和本地socket通信.

5.3.15 节点本地域名解析加速插件版本发布记录

表 5-35 节点本地域名解析加速插件版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.6.2	v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	适配CCE v1.29集群	1.22.20

插件版本	支持的集群版本	更新特性	社区版本
1.5.2	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题	1.22.20
1.5.1	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题	1.22.20
1.5.0	v1.21 v1.23 v1.25 v1.27 v1.28	<ul style="list-style-type: none">• 适配CCE v1.28集群• 插件多可用区部署模式支持选择均匀分布• 插件容器基础镜像切HCE20	1.22.20
1.4.0	v1.19 v1.21 v1.23 v1.25 v1.27	修复插件在CCI场景下pod请求耗时长问题	1.22.20
1.2.7	v1.19 v1.21 v1.23 v1.25	支持插件实例AZ反亲和配置	1.21.1
1.2.4	v1.19 v1.21 v1.23 v1.25	适配CCE v1.25集群	1.21.1
1.2.2	v1.19 v1.21 v1.23	支持自定义NodeLocal DNSCache规格	1.21.1

5.3.16 云原生监控插件版本发布记录

表 5-36 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
3.9.5	v1.21 v1.23 v1.25 v1.27 v1.28	<ul style="list-style-type: none">新增采集自定义指标的开关，默认开启。移除对1.17和1.19版本集群的支持。Grafana从云原生监控插件中移除，拆分为独立的Grafana插件。默认只采集免费指标和服务发现自定义指标。升级开源组件版本	2.37.8
3.8.2	v1.17 v1.19 v1.21 v1.23 v1.25 v1.27	修复部分问题。	2.35.0
3.7.3	v1.17 v1.19 v1.21 v1.23 v1.25	-	2.35.0
3.7.2	v1.17 v1.19 v1.21 v1.23 v1.25	支持采集Virtual-Kubelet Pod指标。	2.35.0
3.7.1	v1.17 v1.19 v1.21 v1.23 v1.25	支持PrometheusAgent模式	2.35.0

插件版本	支持的集群版本	更新特性	社区版本
3.6.6	v1.17 v1.19 v1.21 v1.23 v1.25	<ul style="list-style-type: none">Grafana版本升级至7.5.17支持containerd节点	2.35.0
3.5.1	v1.17 v1.19 v1.21 v1.23	-	2.35.0
3.5.0	v1.17 v1.19 v1.21 v1.23	更新至社区2.35.0版本	2.35.0

5.3.17 云原生日志采集插件版本发布记录

表 5-37 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
1.4.5	v1.21 v1.23 v1.25 v1.27 v1.28	修复部分问题
1.4.2	v1.21 v1.23 v1.25 v1.27 v1.28	<ul style="list-style-type: none">支持v1.28集群支持本地集群日志采集支持GPU事件上报AOM字段特殊处理
1.3.2	v1.17 v1.19 v1.21 v1.23 v1.25	支持Kubernetes事件上报至AOM

插件版本	支持的集群版本	更新特性
1.3.0	v1.17 v1.19 v1.21 v1.23 v1.25	支持v1.25集群
1.2.3	v1.17 v1.19 v1.21 v1.23	-
1.2.2	v1.17 v1.19 v1.21 v1.23	log-agent是基于开源fluent-bit和opentelemetry构建的云原生日志采集插件。log-agent支持基于CRD的日志采集策略，可以根据您配置的策略规则，对集群中的容器标准输出日志、容器文件日志、节点日志及K8s事件日志进行采集与转发。

5.3.18 Grafana 插件版本发布记录

表 5-38 Grafana 插件版本记录

插件版本	支持的集群版本	更新特性
1.2.0	v1.17 v1.19 v1.21 v1.23 v1.25 v1.27 v1.28 v1.29	支持v1.29集群
1.1.0	v1.17 v1.19 v1.21 v1.23 v1.25 v1.27 v1.28	提供Grafana的开源版。

5.3.19 CCE 集群备份恢复插件版本发布记录（停止维护）

表 5-39 CCE 集群备份恢复插件版本记录

插件版本	支持的集群版本	更新特性
1.2.0	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none">支持EulerOS 2.0 (SP5, SP9)配置安全加固功能优化

5.3.20 Kubernetes Web 终端版本发布记录（停止维护）

表 5-40 Kubernetes Web 终端版本记录

插件版本	支持的集群版本	更新特性	社区版本
1.1.12	v1.15 v1.17 v1.19 v1.21	<ul style="list-style-type: none">适配CCE v1.21集群	0.6.6
1.1.6	v1.15 v1.17 v1.19	<ul style="list-style-type: none">配置seccomp默认规则	0.6.6
1.1.5	v1.15 v1.17 v1.19	<ul style="list-style-type: none">兼容CCE v1.15集群	0.6.6
1.1.3	v1.17 v1.19	<ul style="list-style-type: none">适配CCE v1.19集群	0.6.6
1.0.6	v1.15 v1.17	<ul style="list-style-type: none">增加Pod安全策略资源	0.6.6
1.0.5	v1.9 v1.11 v1.13 v1.15 v1.17	<ul style="list-style-type: none">支持v1.17版本集群	0.6.6

5.3.21 Prometheus 插件版本发布记录（停止维护）

表 5-41 Prometheus 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
2.23.32	v1.17 v1.19 v1.21	-	2.10.0
2.23.31	v1.15	<ul style="list-style-type: none">适配CCE v1.15集群	2.10.0
2.23.30	v1.17 v1.19 v1.21	<ul style="list-style-type: none">适配CCE v1.21集群	2.10.0
2.21.14	v1.17 v1.19 v1.21	<ul style="list-style-type: none">适配CCE v1.21集群	2.10.0
2.21.12	v1.15	<ul style="list-style-type: none">适配CCE v1.15集群	2.10.0
2.21.11	v1.17 v1.19	<ul style="list-style-type: none">适配CCE v1.19集群	2.10.0
1.15.1	v1.15 v1.17	<ul style="list-style-type: none">Prometheus是一个监控系统和时间序列库	2.10.0