阿里云
容器服务Kubernetes版

产品公告

文档版本：20190815

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 Kubectl cp相关漏洞修复公告（CVE-2019-11249）

Kubectl cp相关漏洞修复公告（CVE-2019-11249）继前不久刚刚爆出的Kubectl cp相关漏洞CVE-2019-11246，近日Kubernetes官方又公布了一个Kubectl cp相关漏洞CVE-2019-11249，此漏洞可能允许恶意攻击者利用目录遍历（Directory Traversal）的方式将容器tar包中的恶意文件写入或替换至所在主机上目标路径之外的其他位置，该过程仅受本地用户的系统权限限制。 我们建议您尽快升级Kubectl客户端版本。详情请参见修复Kubectl cp漏洞CVE-2019-11249的公告。

2 Kubectl cp相关漏洞修复公告（CVE-2019-11246）

Kubernetes最近公布了另一个kubectl cp 相关漏洞 CVE-2019-11246，此漏洞可能允许攻击者利用kubectl cp命令，采用路径遍历(Path Traversal）的方式将容器tar包中的恶意文件写入所在主机上的任何路径，而该过程仅受本地用户的系统权限限制。 我们建议您尽快升级Kubectl客户端版本。详情请参见修复Kubectl cp漏洞CVE-2019-11246的公告。

3 容器服务即将停止对Swarm的技术支持

容器服务即将于2019年年底停止对Swarm的技术支持，感谢您在过去几年对容器服务的支持，我们将在容器服务Kubernetes版（ACK）继续为您提供稳定、可靠的企业级容器服务。现将Swarm的下线计划向您通知，以助您更好地规划业务的迁移工作。

1. 自2019年7月1日起，停止用户在控制台创建Swarm集群。如您有特别需求，请工单联系我们。
2. 自2019年12月31日起，下线Swarm相关的控制台和文档，并停止对Swarm集群的技术支持。您仍旧可以通过API来运维您的集群。

为了帮助您迁移容器集群至ACK，我们特别发布了Swarm迁移Kubernetes的指南，您可在官网查阅迁移方案概述。如您在使用中遇到任何问题，可与我们取得联系。

4 升级Terway组件的公告

- v1.0.9.15-g3957085-aliyun

  修复了偶发的升级失败的问题。

- v1.0.9.14-ga0346bb-aliyun

  - 修复Terway获取弹性网卡信息时偶发性失败的问题。
  - 修复创建容器时上报failed to move veth to host netns: file exists 的问题。
  - 新增对弹性网卡状态定期扫描，对于异常释放的弹性网卡会定期回收的功能。
  - 优化健康检查：Terway健康检查方式从HTTP路径检查优化成TCP端口检查。

请前往容器服务控制台升级最新的Terway系统组件，此次升级不会对业务造成影响。

5 升级Cloud Controller Manager组件的公告

v1.9.3.105-gfd4e547-aliyun

- 修复了annotation配置不生效的问题。
- 新增支持在控制台上重新命名SLB的功能。如果您是从v1.9.3.10及以前的版本升级上来的，还需要参考旧版本CCM如何支持SLB重命名为之前创建的SLB打上相应的tag以支持重命名。

请前往容器服务控制台，组件升级页面单击 Cloud Controller Manager 组件升级。

6 Kubernetes版本支持的公告

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，我们推出 Kubernetes 版本支持机制，将同时支持四个版本的维保，每个版本的支持周期为一年，请您务必在维保周期结束之前升级您的 Kubernetes 集群。

更多信息请参见版本支持说明。

7 容器服务升级安全策略的公告

容器服务将在一周后升级集群授权管理安全策略，禁止所有未授权的子账号访问集群资源，请您及时参考子账号Kubernetes应用权限配置指导，对管理范围内的集群进行子账号应用权限设置及RAM授权操作。升级后子账号将只拥有授权域内集群的指定访问权限，在授权域外的原有兼容访问模式将被禁止，感谢您的配合。

8 Kubectl cp 相关漏洞公告（CVE-2019-1002101）

Kubectl cp 命令允许用户在容器和用户机器之间拷贝文件，攻击者可能通过在镜像或运行容器中植入带有符号链接（symbolic links）头的恶意 tar 包，在 cp 命令执行解压过程中修改或监控符号链接头同名目录下的任意文件，造成破坏。该漏洞已经在Kubectl工具的 v1.11.9、v1.12.7、v1.13.5 和 v1.14.0 版本中修复，请参考https://kubernetes.io/docs/tasks/tools/install-kubectl/，使用以上版本的 Kubectl 来避免该问题。

9 修复部分集群节点未成功挂载数据盘的公告

我们发现近期有部分多可用区集群节点未能成功挂载数据盘，容器服务现已修复，新创建的集群将不再出现此问题。对于已经创建了的多可用区集群，如果您运行了较多的应用或者拉取镜像的数量不断增加时，可能会导致那些没有为Docker挂载数据盘的节点磁盘空间不足，为此我们也推出了解决方案，请参考集群节点挂载数据盘。如果您对修复有任何问题或者需要支持，请通过钉钉联系容器服务值班答疑。

10 Serverless Kubernetes 底层ECI容器实例即将商用收费的公告

Serverless Kubernetes 底层所调度的ECI容器实例服务即将于2019年1月22日10:00商用收费，详情请参考产品定价，如果您拥有Serverless Kubernetes集群并已创建相应的容器实例，请提前做好预算规划，容器实例在存续时间内会收取您相应的费用。如果您已不再使用容器实例，请提前将其删除，以免扣费。Serverless Kubernetes不会收费，将继续为您提供免费服务。

11 Kubernetes Dashboard漏洞修复公告（CVE-2018-18264）

Kubernetes 社区发现 Kubernetes Dashboard v1.10及之前的版本，存在跳过用户身份认证，直接使用 Dashboard 登录账号并读取集群密钥信息的漏洞，阿里云容器服务已在第一时间发布漏洞修复方案，请您及时采取措施，以避免不必要的损失。修复方案参考修复Kubernetes Dashboard漏洞CVE-2018-18264的公告。