ALIBABA CLOUD

Alibaba Cloud

容器服务Kubernetes版

相关协议

文档版本：20220214

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会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，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	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。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	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。	`switch {active|stand}`

目录

1.阿里云容器服务Kubernetes版服务等级协议说明

详细信息，请参见阿里云容器服务Kubernetes版服务等级协议。

2.使用前必读

阿里云容器服务Kubernetes版（简称容器服务ACK）提供容器服务相关的技术架构以及核心组件的托管服务，对于非托管组件以及运行在ACK集群中的应用，不当操作可能会导致业务故障。为了更好地预估和避免相关的操作风险，在使用容器服务ACK前，请认真阅读本文中的建议与注意事项。

使用须知

数据面组件相关

数据面组件指运行在客户ECS服务器上的系统组件，例如CoreDNS、Ingress、kube-proxy、terway、kubelet等。由于数据面组件运行在客户ECS服务器上，因此数据面组件运行的稳定性需要阿里云容器服务与客户共同维护。

阿里云容器服务ACK对数据面组件提供以下支持：

- 提供组件的参数化设置管理、定期功能优化、BugFix、CVE补丁等功能，并给出相应的指导文档。
- 提供组件的监控与报警等可观测能力的建设，部分核心组件会提供组件日志，并通过SLS透出给客户。
- 提供配置最佳实践和建议，容器服务将根据集群规模大小给出组件配置建议。
- 提供组件的定期巡检能力和一定的报警通知能力，检查项包括但不限定于：组件版本、组件配置、组件负载、组件部署分布拓扑、组件实例数等。

您在使用数据面组件时，请遵循以下建议：

- 使用最新的组件版本。组件经常会发布新版本以修复BUG或提供新特性。您需要在新版本的组件发布后，在保证业务稳定的前提下选择合适的时机，遵循组件升级指导文档中的说明进行升级操作。更多信息，请参见组件概述。
- 请在容器服务ACK的报警中心中设置联系人的邮箱地址、手机号码，并设置相应的报警信息接收方式，阿里云将通过这些渠道推送容器服务的报警信息、产品公告等。更多信息，请参见容器服务报警管理。
- 在您收到组件稳定性风险报告后，请及时按照相关指引进行处理，消除安全隐患。
- 当您在使用数据面组件时，请通过容器服务管理控制台**运维管理 > 组件管理**的方式或者OpenAPI的方式配置组件的自定义参数。通过其他渠道修改组件配置可能会导致组件功能异常。更多信息，请参见管理组件。
- 请勿直接使用IaaS层产品的OpenAPI来变更组件的运行环境，包括但不限定于使用ECS的OpenAPI更改ECS运行状态、修改Worker节点的安全组配置、更改Worker节点的网络配置以及通过负载均衡的OpenAPI修改SLB配置等，擅自改动IaaS层资源可能会导致数据面组件异常。
- 部分数据面组件受上游社区版组件影响，可能存在有Bug或漏洞，请注意及时升级组件，以避免开源组件Bug或漏洞导致您的业务受损。

集群升级相关

请务必通过容器服务ACK的集群升级功能升级集群的K8s版本，自行升级K8s版本可能导致ACK集群的稳定性和兼容性问题。详细操作，请参见升级ACK集群K8s版本。

阿里云容器服务ACK对集群升级提供以下支持：

- 提供集群K8s新版本的升级功能。
- 提供K8s新版本升级的前置检查功能，确保集群当前状态支持升级。
- 提供K8s新版本的版本说明文档，包括相较于前版本的变化。
- 提示升级到K8s新版本时因资源变化可能会发生的风险。

您在使用集群升级功能时，请遵循以下建议：

- 在集群升级前运行前置检查，并根据前置检查结果逐一修复集群升级的阻塞点。
- 详细阅读K8s新版本的版本说明文档，并根据ACK所提示的升级风险确认集群和业务的状态，自行判断升级风险。详细信息，请参见Kubernetes版本发布概览。
- 由于集群升级不提供回滚功能，请做好充分的升级计划和预后备案。
- 根据容器服务ACK的版本支持机制，在当前版本的支持周期内及时升级集群K8s版本。更多信息，请参见版本机制。

Kubernetes原生配置相关

- 请勿擅自修改Kubernetes的关键配置，例如以下文件的路径、链接和内容：
  - */var/lib/kubelet*
  - */var/lib/docker*
  - */etc/kubernetes*
  - */etc/kubeadm*
  - */var/lib/containerd*
- 在YAML模板中请勿使用Kubernetes集群预留的Annotation，否则会造成资源不可用、申请失败、异常等问题。以 `kubernetes.io/` 和 `k8s.io/` 开头的标签为核心组件预留标签。违规示例：pv.kubernetes.io/bind-completed: "yes"。

注册集群相关

- 通过容器服务管理控制台的注册集群功能接入外部Kubernetes集群时，请确保外部集群与阿里云之间的网络稳定性。
- 容器服务ACK提供外部Kubernetes集群的注册接入，但无法管控外部集群自身的稳定性以及不当操作。因此当您通过注册集群配置外部集群节点的Label、Annotation、Tag等信息时，可能导致应用运行异常，请谨慎操作。

应用目录相关

为了丰富Kubernetes应用，容器服务ACK的应用市场提供了应用目录，它们是基于开源软件做了适配和二次开发的应用。ACK无法管控开源软件本身产生的缺陷，请知晓此风险。更多信息，请参见应用市场。

高危操作

在使用容器服务ACK过程中相关功能模块存在高危操作，可能会对业务稳定性造成较大影响。在使用前请认真了解以下高危操作及其影响。

- 集群相关高危操作
- 节点池相关高危操作
- 网络与负载均衡相关高危操作
- 存储相关高危操作
- 日志相关高危操作

集群相关高危操作

分类	高危操作	影响	恢复方案
API Server	删除API Server所使用的SLB。	导致集群不可操作。	不可恢复，请重新创建集群。

分类	高危操作	影响	恢复方案
Worker节点	修改集群内节点安全组。	可能导致节点不可用。	将节点重新添加到集群自动创建的节点安全组中，请参见ECS实例加入安全组。
	节点到期或被销毁。	该节点不可用。	不可恢复。
	重装操作系统。	节点上组件被删除。	节点移出再加入集群。
	自行升级节点组件版本。	可能导致节点无法使用。	回退到原始版本。
	更改节点IP。	节点不可用。	改回原IP。
	自行修改核心组件（kubelet、docker、containerd 等）参数。	可能导致节点不可用。	按照官网推荐配置参数。
	修改操作系统配置。	可能导致节点不可用。	尝试还原配置项或删除节点重新购买。
Master节点（ACK专有版集群）	修改集群内节点安全组。	可能导致Master节点不可用。	将节点重新添加到集群自动创建的节点安全组中，请参见ECS实例加入安全组。
	节点到期或被销毁。	该Master节点不可用。	不可恢复。
	重装操作系统。	Master节点上组件被删除。	不可恢复。
	自行升级Master或者etcd组件版本。	可能导致集群无法使用。	回退到原始版本。
	删除或格式化节点*/etc/kubernetes*等核心目录数据。	该Master节点不可用。	不可恢复。
	更改节点IP。	该Master节点不可用。	改回原IP。
	自行修改核心组件（etcd、kube-apiserver、docker等）参数。	可能导致Master节点不可用。	按照官网推荐配置参数。
	自行更换Master或etcd 证书	可能导致集群无法使用。	不可恢复。
	自行增加或减少Master节点。	可能导致集群无法使用。	不可恢复。
其他	通过RAM执行权限变更或修改操作。	集群部分资源如负载均衡可能无法创建成功。	恢复原先权限。

节点池相关高危操作

高危操作	影响	恢复方案
删除伸缩组。	导致节点池异常。	不可恢复，只能重建节点池。

高危操作	影响	恢复方案
通过kubectl移除节点。	节点池节点数显示和实际不符。	通过节点池重新添加节点，请参见手动添加节点。移除节点的正确做法是通过容器服务管理控制台或者节点池相关API修改节点池的期望节点数缩容（参见调整期望节点数）或移除指定节点（参见移除节点）。
直接释放ECS实例。	可能导致节点池详情页面显示异常。	不可恢复。正确做法是通过容器服务管理控制台或者节点池相关API修改节点池的期望节点数缩容（参见调整期望节点数）或移除指定节点（参见移除节点）。
对开启自动伸缩的节点池手动扩容或缩容。	自动伸缩组件会根据策略自动调整节点数，导致结果与期望不符。	不可恢复。自动伸缩节点池无需手动干预。
修改ESS伸缩组的最大或最小实例数。	可能导致扩缩容异常。	• 对于未开启自动伸缩组的节点池，ESS伸缩组最大和最小实例数改为默认值2000和0。 • 对于开启自动伸缩的节点池，将ESS伸缩组最大和最小实例数修改为与节点池最大和最小节点数一致。
添加已有节点前不做数据备份。	添加前实例上的数据丢失。	不可恢复。 • 手动添加已有节点前必须对要保留的所有数据做提前备份。 • 自动添加节点时会执行系统盘替盘操作，需要您提前备份保存在系统盘中的有用数据。
在节点系统盘中保存重要数据。	节点池的自愈操作可能通过重置节点配置的方式修复节点，因此可能导致系统盘数据丢失。	不可恢复。正确做法是将重要数据存放于额外的数据盘或者云盘、NAS、OSS。

网络与负载均衡相关高危操作

高危操作	影响	恢复方案
修改内核参数 `net.ipv4.ip_forward=0` 。	网络不通。	修改内核参数为 `net.ipv4.ip_forward=1` 。

高危操作	影响	恢复方案
修改内核参数： • `net.ipv4.conf.all.rp_filter = 1|2` • `net.ipv4.conf.[ethX].rp_filter = 1|2` **说明** `ethX` 代表所有以 `eth` 开头的网卡。	网络不通。	修改内核参数为： • `net.ipv4.conf.all.rp_filter = 0` • `net.ipv4.conf.[ethX].rp_filter = 0`
修改内核参数 `net.ipv4.tcp_tw_reuse = 1` 。	导致Pod健康检查异常。	修改内核参数为 `net.ipv4.tcp_tw_reuse = 0` 。
修改内核参数 `net.ipv4.tcp_tw_recycle = 1` 。	导致NAT异常。	修改内核参数 `net.ipv4.tcp_tw_recycle = 0` 。
修改内核参数 `net.ipv4.ip_local_port_range` 。	导致网络偶发不通。	修改内核参数到默认值 `net.ipv4.ip_local_port_range="32768 60999"` 。
安装防火墙软件，例如Firewalld或者ufw等。	导致容器网络不通。	卸载防火墙软件并重启节点。
节点安全组配置未放通容器 CIDR的53端口UDP。	集群内DNS无法正常工作。	按照官网推荐配置放通安全组。
修改或者删除ACK添加的SLB的标签。	导致SLB异常。	恢复SLB的标签。
通过负载均衡控制台修改ACK管理的SLB的配置，包括SLB、监听及虚拟服务器组。	导致SLB异常。	恢复SLB的配置。
移除Service中复用已有SLB的Annotation，即 `service.beta.kubernetes.io/alibaba-cloud-loadbalancer-id: ${YOUR_LB_ID}` 。	导致SLB异常。	在Service中添加复用已有SLB的Annotation。 **说明** 复用已有SLB的Service无法直接修改为使用自动创建SLB的Service。您需要重新创建Service。
通过负载均衡控制台删除ACK创建的SLB。	可能导致集群网络异常。	通过删除Service的方式删除SLB。

高危操作	影响	恢复方案

在安装Nginx Ingress Controller组件的情况下手动删除 kube-system命名空间下的 `nginx-ingress-lb` Service。	Ingress Controller工作不正常，严重时产生崩溃。	使用以下YAML新建一个同名Service。
		`apiVersion: v1`
		`kind: Service`
		`metadata:`
		`  annotations:`
		`  labels:`
		`  app: nginx-ingress-lb`
		`  name: nginx-ingress-lb`
		`  namespace: kube-system`
		`spec:`
		`  externalTrafficPolicy: Local`
		`  ports:`
		`  - name: http`
		`  port: 80`
		`  protocol: TCP`
		`  targetPort: 80`
		`  - name: https`
		`  port: 443`
		`  protocol: TCP`
		`  targetPort: 443`
		`  selector:`
		`  app: ingress-nginx`
		`  type: LoadBalancer`

存储相关高危操作

高危操作	影响	恢复方案
控制台手动解挂云盘。	Pod写入报IO Error。	重启Pod，手动清理节点挂载残留。
节点上umount磁盘挂载路径	Pod写入本地磁盘。	重启Pod。
节点上直接操作云盘。	Pod写入本地磁盘。	不可恢复。
多个Pod挂载相同云盘。	Pod写入本地磁盘或者报错IO Error。	确保一个云盘给一个Pod使用。
手动删除NAS挂载目录。	Pod写入报IO Error。	重启Pod。
删除在用的NAS盘或挂载点。	Pod出现IO Hang。	重启ECS节点。

日志相关高危操作

高危操作	影响	恢复方案
删除宿主机*/tmp/ccs-log-collector/pos*目录。	日志重复采集。	不可恢复。该目录下的文件记录了日志的采集位置。
删除宿主机*/tmp/ccs-log-collector/buffer*目录。	日志丢失。	不可恢复。该目录是待消费的日志缓存文件。
删除aliyunlogconfig CRD资源。	日志采集失效。	重新创建删除的CRD以及对应的资源，但失效期间日志无法恢复。 删除CRD会关联删除对应所有的实例，即使恢复CRD后还需要手动创建被删除的实例。
删除日志组件。	日志采集失效。	重新安装日志组件并手动恢复aliyunlogconfig CRD实例，删除期间日志无法恢复。 删除日志组件相当于删除aliyunlogconfig CRD以及日志采集器Logtail，期间日志采集能力全部丢失。

相关文档

- Nginx Ingress最佳实践
- DNS最佳实践