ALIBABA CLOUD

阿里云

云服务器ECS
动态与公告

文档版本：20220701

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.新功能发布记录 05
2.产品公告 28
2.1. 【停售公告】停止售卖阿里云共享块存储（公测） 28
3.安全公告 29
3.1. 漏洞公告 | Linux 内核本地权限提升漏洞（CVE-2022-0847） 29
3.2. 漏洞公告 | Linux Polkit权限提升漏洞风险（CVE-2021-4034） 30
3.3. 漏洞公告 | NSS内存损坏漏洞（CVE-2021-43527） 31
3.4. 漏洞公告 | Linux Netfilter本地权限提升漏洞（CVE-2021-22555... 32
3.5. 漏洞公告 | Windows Print Spooler 0day漏洞预警（CVE-2021-... 33
3.6. 漏洞公告 | Windows Print Spooler权限提升漏洞预警（CVE-202... 34
3.7. 漏洞公告 | Windows HTTP协议远程代码执行漏洞预警（CVE-202... 34
3.8. 漏洞公告 | Windows多个严重高危漏洞预警（CVE-2021-24074、... 35
3.9. 漏洞公告 | Linux sudo权限漏洞（CVE-2021-3156） 36
3.10. 漏洞公告 | Windows TCP/IP远程执行代码漏洞（CVE-2020-168... 37
3.11. 漏洞公告 | Linux内核漏洞（CVE-2020-14386） 39
3.12. 漏洞公告 | 虚拟化逃逸0day漏洞 40
3.13. 漏洞公告 | Windows SMBv3远程执行代码漏洞（CVE-2020-079... 40
3.14. 漏洞公告 | Windows加密库漏洞（CVE-2020-0601） 41

1.新功能发布记录

本章节介绍了云服务器ECS的产品功能和对应的文档动态。

- 镜像版本更新信息请参见公共镜像发布记录、Alibaba Cloud Linux 2发布记录及Alibaba Cloud Linux 3发布记录。
- 服务器迁移中心SMC功能更新信息请参见SMC新功能发布记录。

更多有关阿里云最新产品动态，请订阅云产品动态。

2022年

2022年06月

功能名称	功能概述	发布时间	发布地域	相关文档
新增操作系统迁移	操作系统迁移通过保留系统盘数据，减少业务中断时长，支持以下迁移场景： • CentOS 7操作系统迁移为Alibaba Cloud Linux 2/Anolis OS 7操作系统。 • CentOS 8操作系统迁移为Alibaba Cloud Linux 3/Anolis OS 8操作系统。	2022-06-17	全部	操作系统迁移
云助手支持定时执行命令	云助手支持创建并执行定时命令，可定时触发任务的执行，适用于周期性执行、日常维护、或在某时刻需要完成的单次任务等场景。	2022-06-02	全部	• 立即执行命令 • 创建命令 • 执行命令 • 查看执行结果及修复常见问题

2022年05月

功能名称	功能概述	发布时间	发布地域	相关文档
一致性复制组	一致性复制组能够实现业务系统跨多块云盘的容灾场景下，对多块云盘的异步复制做统一管理和操作，同时可以确保同一复制组内的多块云盘数据能够恢复到同一个时间点，以便实现容灾场景下实例级别或者多实例级别的容灾保护。	2022-05-27	全部	一致性复制组概述
托管弹性网卡	为部分云产品（例如容器服务ACK、NAT网关等）创建弹性网卡时，您可以将弹性网卡托管给云产品系统管理，该模式的弹性网卡称为托管弹性网卡。	2022-05-20	全部	托管弹性网卡

功能名称	功能概述	发布时间	发布地域	相关文档
支持在控制台对云盘分区	在控制台将云盘挂载至ECS实例后，支持直接对云盘分区和创建文件系统。	2022-05-17	部分	挂载数据盘

2022年04月

功能名称	功能概述	发布时间	发布地域	相关文档
实例无法启动的解决方案	ECS支持在系统盘卸载的情况下，对实例进行诊断。	2022-04-29	部分	实例无法启动诊断结果操作指引
实例规格族	发布本地SSD型实例规格族i4g。	2022-04-12	部分	实例规格族
实例规格族	发布本地SSD型实例规格族i4r。	2022-04-12	部分	实例规格族

2022年03月

功能名称	功能概述	发布时间	发布地域	相关文档
社区镜像	社区镜像是一种完全公开的镜像。您可以将制作好的自定义镜像发布为社区镜像供他人使用，也可以获取并使用他人发布的社区镜像。	2022-03-25	全部	• 社区镜像概述 • 发布社区镜像 • 查找社区镜像 • 使用社区镜像 • 下架社区镜像
实例规格族	发布GPU计算型实例规格族gn7e。	2022-03-22	部分	实例规格族
ESSD PL-X云盘	发布新云盘类型ESSD PL-X云盘。ESSD PL-X云盘具备超高IOPS、超高吞吐量和超低时延等多维度的超高性能。	2022-03-18	部分	ESSD PL-X云盘
实例规格族	发布视觉计算型实例规格族ebmgi6s。	2022-03-10	部分	实例规格族
ESSD AutoPL云盘	发布新云盘类型ESSD AutoPL云盘。ESSD AutoPL云盘基于ESSD云盘，在保持ESSD云盘原有功能与性能的同时，实现了云盘容量与云盘性能的解耦。	2022-03-04	部分	ESSD AutoPL云盘

2022年02月

功能名称	功能概述	发布时间	发布地域	相关文档
实例规格族	发布通用型实例规格族g8m。	2022-02-25	部分	实例规格族
实例规格族	GPU计算型实例规格族gn7i新增实例规格。	2022-02-09	部分	实例规格族

功能名称	功能概述	发布时间	发布地域	相关文档

2022年01月

功能名称	功能概述	发布时间	发布地域	相关文档
实例规格族	发布大数据计算密集型实例规格族d3c。	2022-01-27	部分	实例规格族

2021年

2021年12月

功能名称	功能概述	发布时间	发布地域	相关文档
实例规格族	发布GPU计算型超级计算集群实例规格族sccgn7ex。	2021-12-22	全部	实例规格族
块存储	云盘异步复制是一种基于块存储数据复制能力实现跨地域数据保护的功能。	2021-12-01	部分	云盘异步复制概述
块存储	块存储数据洞察（EBS Lens）是阿里云针对块存储资源提供的数据分析、性能监控的一种功能。	2021-12-01	部分	什么是块存储数据洞察

2021年11月

功能名称	功能概述	发布时间	发布地域	相关文档
快照	原实例快照功能更新为快照一致性组。	2021-11-30	全部	创建快照一致性组
实例规格族	发布GPU计算型弹性裸金属服务器实例规格族ebmgn6ia。	2021-11-24	全部	实例规格族
实例规格族	发布通用型弹性裸金属服务器实例规格族ebmg7a、计算型弹性裸金属服务器实例规格族ebmc7a、内存型弹性裸金属服务器实例规格族ebmr7a。	2021-11-16	全部	实例规格族
实例规格族	发布通用型弹性裸金属服务器实例规格族ebmg7、计算型弹性裸金属服务器实例规格族ebmc7、内存型弹性裸金属服务器实例规格族ebmr7。	2021-11-16	全部	实例规格族
实例规格族	发布GPU计算型弹性裸金属服务器实例规格族ebmgn7e。	2021-11-15	全部	实例规格族

功能名称	功能概述	发布时间	发布地域	相关文档
实例规格族	发布GPU虚拟化型实例规格族sgn7i-vws（共享CPU）。	2021-11-15	全部	实例规格族

2021年10月

功能名称	功能概述	发布时间	发布地域	相关文档
实例规格族	发布存储增强通用型实例规格族g7se、存储增强计算型实例规格族c7se、存储增强内存型实例规格族r7se。	2021-11-02	部分	实例规格族
实例规格族	发布RDMA增强型实例规格族c7re。	2021-10-25	部分	实例规格族
实例规格族	发布内存型实例规格族r7p、内存增强型实例规格族re7p、性能增强本地SSD型实例规格族i4p。	2021-10-15	部分	实例规格族

2021年09月

功能名称	功能概述	发布时间	发布地域	相关文档
云助手	云助手的运维任务执行记录投递功能，可以将运维任务执行记录投递到对象存储OSS和日志服务SLS中，进行持久化存储。	2021-09-28	全部	运维任务执行记录投递
实例规格族	发布GPU虚拟化型实例规格族vgn7i-vws，该规格族已包含NVIDIA GRID vWS的软件License。	2021-09-15	全部	实例规格族
专属块存储集群	专属块存储集群具备物理资源隔离、集群内资源独享的特点。使用专属块存储集群，您可以提升业务数据存储的安全性及运维效率。	2021-09-13	部分	什么是专属块存储集群

2021年8月

功能名称	功能概述	发布时间	发布地域	相关文档
网络连通性诊断	网络连通性诊断功能用于诊断专有网络中两个对象（实例或弹性网卡）间的网络连通性，方便您了解网络连通情况和定位网络不通的原因。	2021-08-30	全部	诊断网络连通性

功能名称	功能概述	发布时间	发布地域	相关文档
镜像	Alibaba Cloud Linux 3支持内核热补丁功能，无需重启服务器即可对操作系统内核更新补丁。	2021-08-10	全部	内核热补丁概述
节省停机模式	停机不收费功能改名为节省停机模式。	2021-08-09	全部	按量付费实例节省停机模式

2021年07月

功能名称	功能描述	发布时间	发布地域	相关文档
部署集	部署集内可创建的ECS实例数量由7台提升至20台。	2021-07-29	全部	部署集概述
安全组	针对安全组规则做专项检测，判断安全组允许和拒绝访问的情况是否符合预期。	2021-07-28	全部	安全组规则检测
实例规格族	发布通用型超级计算集群实例规格族sccg7、计算型超级计算集群实例规格族sccc7。	2021-07-22	部分	实例规格族
资源保障	支持标签匹配，用于精细化使用开放私有池，将使用私有池和您已有的标签设计无缝对接。	2021-07-19	全部	资源保障概述
实例规格族	发布通用型实例规格族g6r、计算型实例规格族c6r。	2021-07-10	部分	实例规格族
前缀列表	发布前缀列表功能，便于管理维护CIDR地址块。	2021-07-02	部分	前缀列表概述
实例规格族	发布GPU计算型实例规格族gn7i。	2021-07-01	全部	实例规格族

2021年6月

功能名称	功能描述	发布时间	发布地域	相关文档
镜像	Alibaba Cloud Linux 2支持内核热补丁功能，无需重启服务器即可对操作系统内核更新补丁。	2021-06-30	全部	内核热补丁概述
自动重开机	结清欠费账单后系统自动重开机。如果自动重开机失败，请及时手动重开机（即手动启动实例）。	2021-06-22	全部	启动实例
实例健康诊断	健康诊断新增实例无法启动问题场景。	2021-06-09	部分	诊断实例的健康状态

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布GPU计算型弹性裸金属服务器实例规格族ebmgn7i。	2021-06-08	全部	实例规格族

2021年5月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布计算型弹性裸金属服务器实例规格族ebmc6me。	2021-05-28	部分	实例规格族
实例规格族	发布通用型实例规格族g7a、计算型实例规格族c7a、内存型实例规格族r7a。	2021-05-28	部分	实例规格族

2021年4月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布通用型实例规格族g7、计算型实例规格族c7、内存型实例规格族r7。	2021-04-19	部分	实例规格族
镜像	发布公共镜像Alibaba Cloud Linux 3。	2021-04-16	全部	Alibaba Cloud Linux概述
预留实例券	预留实例券支持抵扣更多规格族。	2021-04-15	全部	预留实例券概述
实例健康诊断	• 实例健康诊断支持选择问题场景。 • 操作系统内相关配置诊断支持更多诊断项。	2021-04-15	全部	诊断实例的健康状态
实例休眠	发布实例休眠功能，休眠实例后再次启动实例，ECS实例会自动恢复至休眠前的应用程序状态。	2021-04-06	部分	休眠实例
快照	发布实例快照功能，您可以为一台ECS实例中的多个云盘同时创建快照，保证数据写入时序上的一致性。	2021-04-06	部分	创建快照一致性组
快照	发布应用一致性快照功能，您使用应用一致性快照进行回滚时，可确保应用处于一致性的启动状态。	2021-04-06	部分	通过控制台创建应用一致性快照

2021年3月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布安全增强通用型实例规格族g7t、安全增强计算型实例规格族c7t、安全增强内存型实例规格族r7t。	2021-03-31	部分	• 实例规格族 • 安全增强型实例概述
实例规格族	发布异构服务型实例规格族video-enhance。	2021-03-25	部分	实例规格族
实例规格族	发布本地SSD型弹性裸金属服务器实例规格族ebmi2g。	2021-03-03	部分	实例规格族
实例规格族	发布高主频通用型弹性裸金属服务器实例规格族ebmhfg7、高主频计算型弹性裸金属服务器实例规格族ebmhfc7、高主频内存型弹性裸金属服务器实例规格族ebmhfr7。	2021-03-03	部分	实例规格族

2021年2月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布本地SSD型实例规格族i3g。	2021-02-26	全部	实例规格族
实例规格族	发布网络增强型实例规格族g7ne。	2021-02-09	部分	实例规格族

2021年1月

功能名称	功能描述	发布时间	发布地域	相关文档
网络	部分实例规格支持设置网卡的MTU值和开启Jumbo Frame特性。	2021-01-29	部分	设置网卡MTU值
Workbench	Workbench已接入特权访问管理中心（PAM），通过PAM凭据认证登录实例更加方便快捷。	2021-01-26	全部	通过凭据认证登录实例
云助手	云助手支持托管非阿里云服务器。托管后，您可以通过云助手向服务器远程下发命令和文件。	2021-01-22	部分	混合云托管服务器
实例规格族	发布GPU计算型实例规格族gn7。	2021-01-12	部分	实例规格族
镜像构建	镜像构建服务（Image Builder）是云服务器ECS为您提供的一站式镜像定制服务，并支持跨地域跨账号定制镜像。	2021-01-11	全部	镜像构建服务（ImageBuilder）概述

历史年份

2020年12月

功能名称	功能描述	发布时间	发布地域	相关文档
资源保障	资源保障是包括资源供应量化感知、资源的确定性预定、私有池规划使用的全链路资源确定性服务。	2020-12-14	部分	资源保障概述
faasutil	faasutil是阿里云FPGA云服务器提供的新一代命令行工具，进一步提高FPGA云服务器的易用性、稳定性、安全性和可扩展性。	2020-12-08	部分	• 获取faasutil • 使用faasutil
快照	快照极速可用功能在华北5（呼和浩特）上线公测。	2020-12-03	部分	开启或关闭快照极速可用功能

2020年11月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布持久内存型实例规格族re6p。	2020-11-04	部分	实例规格族
实例规格族	发布本地SSD型实例规格族i3。	2020-11-03	部分	实例规格族

2020年10月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布GPU计算型弹性裸金属服务器实例规格族ebmgn7。	2020-10-26	部分	实例规格族
实例规格族	发布存储增强型实例规格族g6se。	2020-10-23	部分	实例规格族
块存储	变更云盘类型功能上线公测。	2020-10-12	部分	变更云盘类型

2020年9月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布异构服务型实例规格族video-trans。	2020-09-30	部分	实例规格族
抢占式实例	调用OpenAPI创建抢占式实例时，支持设置为无保护周期。	2020-09-25	全部	• 抢占式实例概述 • RunInstances • 抢占式实例开放无保护期新模式
云助手	支持直接发送本地文件到ECS实例，方便您运维和管理ECS实例。	2020-09-22	全部	发送本地文件到ECS实例

功能名称	功能描述	发布时间	发布地域	相关文档
节省计划	一种折扣权益计划，可以抵扣按量付费实例（不含抢占式实例）的账单。	2020-09-18	全部	• 节省计划概述 • 节省计划 • 购买和使用节省计划
实例规格族	发布安全增强通用型实例规格族g6t、安全增强计算型实例规格族c6t。	2020-09-08	部分	• 实例规格族 • 安全增强型实例概述
实例规格族	发布通用型实例规格族g6a、计算型实例规格族c6a、内存型实例规格族r6a。	2020-09-07	部分	实例规格族
实例规格族	发布通用型弹性裸金属服务器实例规格族ebmg6a、计算型弹性裸金属服务器实例规格族ebmc6a、内存型弹性裸金属服务器实例规格族ebmr6a。	2020-09-07	部分	实例规格族

2020年8月

功能名称	功能描述	发布时间	发布地域	相关文档
标签	标签支持绑定预留实例券等更多资源。	2020-08-18	全部	标签概述
快照	支持跨地域复制快照，提高业务可靠性与可用性。	2020-08-14	部分	复制快照

2020年7月

功能名称	功能描述	发布时间	发布地域	相关文档
云助手	提供云助手插件功能，帮助您运维和管理ECS实例。	2020-07-31	全部	使用云助手插件
镜像族系	提供镜像族系（ImageFamily）功能，帮助您实现镜像平滑更新与回滚。	2020-07-02	全部	镜像族系概述

2020年6月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布大数据计算密集型实例规格族d2c。	2020-06-23	部分	实例规格族

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布高主频计算型超级计算集群实例规格族scchfc6、高主频通用型超级计算集群实例规格族scchfg6、高主频内存型超级计算集群实例规格族scchfr6。	2020-06-23	全部	实例规格族
实例规格族	发布计算型（平衡增强）弹性裸金属服务器实例规格族ebmc6e、通用型（平衡增强）弹性裸金属服务器实例规格族ebmg6e、内存型（平衡增强）弹性裸金属服务器实例规格族ebmr6e。	2020-06-23	全部	实例规格族
存储容量单位包	支持抵扣多存储产品的按量付费账单，例如云盘、OSS、NAS、快照等。	2020-06-23	全部	• 存储容量单位包概述 • 存储容量单位包 • 存储容量单位包抵扣规则
块存储	支持在ECS实例中查询磁盘的序列号。	2020-06-16	全部	查看磁盘序列号
网络	支持在控制台上切换ECS实例的VPC，此功能正在邀测中。	2020-06-10	部分	更换ECS实例的VPC
ESSD云盘	ESSD PL0云盘在华东1（杭州）和华北2（北京）地域上线公测。	2020-06-10	部分	• ESSD云盘 • 块存储性能
本地盘系统事件	支持在控制台上查看本地盘损坏事件，并支持在控制台上隔离损坏的本地盘。	2020-06-09	全部	隔离损坏的本地盘（控制台）
实例规格族	发布高主频通用型实例规格族hfg7、高主频计算型实例规格族hfc7和高主频内存型实例规格族hfr7。	2020-06-09	部分	实例规格族
实例规格族	发布通用平衡增强型实例规格族g6e、计算平衡增强型实例规格族c6e和内存平衡增强型实例规格族r6e。	2020-06-09	全部	实例规格族
实例规格族	发布非易失性内存增强型弹性裸金属服务器实例规格族ebmre6p。	2020-06-09	部分	实例规格族
实例规格族	发布NPU计算型实例规格族ebman1。	2020-06-04	部分	实例规格族

2020年5月

功能名称	功能描述	发布时间	发布地域	相关文档
镜像	停止对CoreOS Container Linux公共镜像提供技术协助。由于该操作系统已经结束生命周期，不会继续提供安全补丁。出于安全因素的考虑，不推荐您继续使用CoreOS Container Linux镜像。阿里云也将在近期上线Fedora CoreOS公共镜像以替代CoreOS Container Linux。	2020-05-26	全部	公共镜像发布记录
预留实例券	支持查看实例规格计算力因子，方便理解拆分合并预留实例券时的计算力要求和地域级预留实例券的实例大小灵活性。	2020-05-14	全部	• 预留实例券概述 • 查看计算力因子
安全组	支持一站式配置和管理安全组，支持批量维护安全组规则。	2020-05-08	全部	• 安全组概述 • 创建安全组 • 添加安全组规则

2020年4月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布内存增强型弹性裸金属服务器实例规格族ebmre6-6t。	2020-04-28	全部	实例规格族
实例规格族	发布内存增强型实例规格族re6。	2020-04-20	部分	实例规格族

2020年3月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布网络增强型实例规格族g5ne。	2020-03-24	部分	实例规格族
操作审计	支持查看最近90天的ECS实例相关操作记录。	2020-03-19	全部	查看ECS实例的操作记录
安全组	ECS实例支持切换安全组，包括企业安全组和普通安全组之间切换。	2020-03-11	全部	替换ECS实例的安全组
实例规格族	发布本地SSD型实例规格族i2ne和i2gne。	2020-03-11	全部	实例规格族

2020年1月

功能名称	功能描述	发布时间	发布地域	相关文档

功能名称	功能描述	发布时间	发布地域	相关文档
标签	丰富标签功能，支持通过标签对RAM用户进行权限控制，支持通过OOS批量绑定和修改标签。	2020-01-03	全部	• 使用标签控制资源的访问 • 创建带特定标签的资源 • 使用OOS批量绑定标签 • 使用OOS批量修改标签值
实例规格族	发布大数据存储密集型实例规格族d2s。	2020-01-17	部分	实例规格族
实例规格族	发布轻量级GPU计算型实例规格族vgn6i。	2020-01-16	部分	实例规格族
实例规格族	发布共享标准型实例规格族s6。	2020-01-16	部分	实例规格族
镜像	停止对Windows Server 2008和Windows Server 2008 R2公共镜像提供技术支持，建议您尽快更新至Windows Server 2012或以上版本。	2020-01-14	全部	公共镜像概述
ESSD云盘	支持通过API降低ESSD云盘性能级别。	2020-01-14	全部	ModifyDiskSpec

2019年12月

功能名称	功能描述	发布时间	发布地域	相关文档
Workbench	支持通过Workbench远程连接Linux实例和Windows实例，更加高效便捷。	2019-12-26	部分	• 通过密码或密钥认证登录Linux实例 • 通过密码或密钥认证登录Windows实例
存储容量单位包	新增40GiB、100GiB以及500GiB的容量规格。	2019-12-05	部分	存储容量单位包概述

2019年11月

功能名称	功能描述	发布时间	发布地域	相关文档
标签	标签编辑器功能上线，支持跨产品和跨地域查询5000条资源信息，能够编辑资源的标签以及导出资源信息。	2019-11-28	全部	使用标签编辑器管理资源标签
企业安全组	企业安全组能容纳的私网IP数量提升至65536。	2019-11-22	全部	企业安全组

功能名称	功能描述	发布时间	发布地域	相关文档
快照	自动快照的额度提升至1000份。	2019-11-15	全部	快照概述
实例规格族	发布GPU计算型实例规格族gn6e。	2019-11-14	部分	实例规格族
实例规格族	发布GPU计算型弹性裸金属服务器实例规格族ebmgn6e。	2019-11-14	部分	实例规格族

2019年10月

功能名称	功能描述	发布时间	发布地域	相关文档
存储容量单位包	存储容量单位包结束公测。	2019-10-23	部分	存储容量单位包概述
实例规格族	发布高主频实例规格族hfc6、hfg6、hfr6。	2019-10-15	部分	实例规格族
实例规格族	发布弹性裸金属服务器实例规格族ebmhfc6、ebmhfg6、ebmhfr6。	2019-10-10	全部	实例规格族

2019年9月

功能名称	功能描述	发布时间	发布地域	相关文档
存储容量单位包	存储容量单位包公测开放，可以抵扣按量付费云盘的每小时计费账单。	2019-09-26	部分	存储容量单位包概述
扩容云盘	• SSD云盘和高效云盘最高支持扩容至32TiB。 • ESSD云盘支持在线扩容。	2019-09-26	全部	• 扩容概述 • 在线扩容云盘（Linux系统）
实例规格族	发布弹性裸金属服务器实例规格族ebmc6、ebmg6、ebmr6。	2019-09-24	全部	实例规格族
经典网络公网IP	手动释放经典网络类型ECS实例时，支持将公网IP转换为弹性公网IP（Elastic IP，简称EIP）。	2019-09-20	部分	经典网络类型ECS公网IP转为弹性公网IP
实例规格族	发布突发性能实例规格族t6。	2019-09-12	部分	实例规格族
安全组	安全组规则上限提升到200条。	2019-09-03	全部	使用限制
快照	手动快照与自动快照的快照额度分别提升至256份。	2019-09-02	全部	快照概述

2019年8月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布GPU计算型弹性裸金属服务器实例规格族ebmgn6v。	2019-08-26	部分	实例规格族
实例规格族	发布GPU计算型弹性裸金属服务器实例规格族ebmgn6i。	2019-08-26	部分	实例规格族
镜像	导出镜像功能全网开放。	2019-08-21	全部	导出镜像
企业安全组	企业安全组结束邀测阶段，所有地域均支持使用企业安全组管理ECS实例。	2019-08-07	全部	企业安全组
快照	支持在创建云盘或者ECS实例时启用自动快照策略。	2019-08-01	全部	执行或取消自动快照策略

2019年7月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布通用型实例规格族g6。	2019-07-30	部分	实例规格族
实例规格族	发布计算型实例规格族c6。	2019-07-30	部分	实例规格族
实例规格族	发布内存型实例规格族r6。	2019-07-30	部分	实例规格族
实例规格族	发布计算网络增强型弹性裸金属服务器ebmc5s。	2019-07-30	部分	实例规格族
实例规格族	发布通用网络增强型弹性裸金属服务器ebmg5s。	2019-07-30	部分	实例规格族
实例规格族	发布内存网络增强型弹性裸金属服务器ebmr5s。	2019-07-30	部分	实例规格族

2019年6月

功能名称	功能描述	发布时间	发布地域	相关文档
弹性供应	弹性供应以供应组为载体调度和维护计算资源，支持一键部署跨计费方式、跨可用区、跨实例规格族的实例集群。	2019-06-28	全部	弹性供应概述
ESSD云盘	ESSD产品结束公测，正式商用，全新发布三种性能等级的ESSD云盘规格。	2019-06-28	部分地域，详情请参见块存储FAQ	ESSD云盘

功能名称	功能描述	发布时间	发布地域	相关文档
轻量级GPU计算型实例规格族vgn5i	提供适用于vgn5i实例的GRID驱动资源。	2019-06-19	全部	• 创建配备GRID驱动的GPU实例（Windows） • 在GPU虚拟化型实例中安装GRID驱动（Linux）
实例重部署	当ECS实例收到系统事件通知时，您可以调用RedeployInstance接口重新部署这台实例。	2019-06-12	全部	RedeployInstance
镜像	Aliyun Linux 2镜像支持在本地环境（基于KVM技术的虚拟化环境）使用。	2019-06-11	全部	在本地使用Alibaba Cloud Linux 2镜像

2019年5月

功能名称	功能描述	发布时间	发布地域	相关文档
云助手	支持通过控制台以及API在创建云助手命令时设置自定义参数，调用命令时再动态传入取值。	2019-05-15	全部	• 创建命令 • 执行命令
块存储	支持调用API创建包年包月磁盘。	2019-05-15	全部	CreateDisk
事件通知	支持为手动创建的快照设置云监控事件通知。	2019-05-10	全部	事件通知概述

2019年4月

功能名称	功能描述	发布时间	发布地域	相关文档
弹性网卡	弹性网卡支持分配多个私有IP。	2019-04-28	全部	分配辅助私网IP地址
块存储	支持在线扩容数据盘，即扩容过程中无需重启ECS实例就能完成扩容。	2019-04-24	全部	在线扩容云盘（Linux系统）
块存储	支持扩容系统盘容量。	2019-04-24	全部	离线扩容云盘（Linux系统）
快照	支持对已过期的云盘创建快照。	2019-04-20	全部	• 创建快照 • CreateSnapshot

2019年3月

功能名称	功能描述	发布时间	发布地域	相关文档
公共镜像	发布公共镜像Aliyun Linux 2。	2019-03-27	全部	Alibaba Cloud Linux概述

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布GPU计算型实例规格族gn6i。	2019-03-21	全部	实例规格族
实例规格族	发布GPU计算型超级计算集群实例规格族sccgn6。	2019-03-20	全部	实例规格族
实例规格族	发布轻量级GPU计算型实例规格族vgn5i。	2019-03-19	全部	实例规格族
预留实例券	启动预留实例券功能邀测。	2019-03-18	全部	预留实例券概述
云助手	支持经典网络类型ECS实例使用云助手。	2019-03-01	全部	安装云助手客户端

2019年1月

功能名称	功能描述	发布时间	发布地域	相关文档
事件通知	ECS实例新提供状态变化事件以及抢占式实例回收告警事件。	2019-01-29	全部	系统事件

2018年12月

功能名称	功能描述	发布时间	发布地域	相关文档
云助手	云助手支持英国（伦敦）地域。	2018-12-31	全部	云助手概述
抢占式实例	抢占式实例按秒计费。	2018-12-17	全部	抢占式实例
实例	支持实例释放保护功能。	2018-12-14	全部	实例释放保护
IPv6	ECS支持IPv6。	2018-12-06	部分	IPv6地址
弹性网卡	DescribeNetworkInterfaces支持输出网卡绑定的公网IP。	2018-12-04	全部	DescribeNetworkInterfaces

2018年11月

功能名称	功能描述	发布时间	发布地域	相关文档
自定义镜像	支持使用Packer快速创建自定义镜像。	2018-11-30	全部	使用Packer创建自定义镜像
实例规格族	发布re4e内存增强型实例。	2018-11-30	全部	实例规格族
块存储	支持单独创建包年包月云盘，并挂载到包年包月实例。	2018-11-29	全部	创建包年包月云盘

功能名称	功能描述	发布时间	发布地域	相关文档
全局标签	支持全局标签功能，ECS控制台云资源实现分组管理。	2018-11-23	全部	全局标签
部署集	阿里云部署集（Deployment Set）上线。	2018-11-16	全部	部署集概述

2018年10月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布全新一代FaaS平台f3（VU9P）实例。	2018-10-31	全部	实例规格族
API最佳实践	控制台发布常用的核心功能API的最佳实践。	2018-10-19	全部	使用向导创建实例

2018年9月

功能名称	功能描述	发布时间	发布地域	相关文档
突发性能实例（t5）	突发性能实例支持无性能约束模式。	2018-09-30	全部	无性能约束模式
实例元数据Metadata	实例元数据metadata支持实例运维相关系统事件信息。	2018-09-14	全部	实例元数据
实例健康状态	ECS实例详情页面提供实例健康状态。	2018-09-14	全部	查看实例健康状况
实例规格族	最新一代GPU云主机gn6v（V100机型）正式售卖。	2018-09-12	全部	实例规格族
实例购买	支持批量续费实例以及购买历史实例。	2018-09-07	全部	手动续费实例
系统事件	支持创建和取消模拟事件的接口。	2018-09-03	全部	• CreateSimulatedSystemEvents • CancelSimulatedSystemEvents
计费方式	支持包年包月实例转按量付费实例。	2018-09-01	全部	包年包月转按量付费

2018年8月

功能名称	功能描述	发布时间	发布地域	相关文档
本地盘	本地盘实例运维体验提升。	2018-08-31	全部	本地盘
云助手	控制台支持云助手功能。	2018-08-17	全部	云助手

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布超级计算集群实例规格族。	2018-08-16	全部	实例规格族

2018年7月

功能名称	功能描述	发布时间	发布地域	相关文档
自定义镜像	支持导入qcow2格式的镜像。	2018-07-30	全部	• 导入自定义镜像 • ImportImage
安全组	支持修改安全组规则。	2018-07-25	全部	修改安全组规则
标签	创建资源时支持绑定标签。	2018-07-20	全部	绑定标签
实例规格族	发布计算型弹性裸金属服务器实例规格族ebmc4。	2018-07-18	全部	实例规格族
快照	显示快照创建剩余时长。	2018-07-17	全部	创建一个云盘快照
账号与用户特权	管理配额。	2018-07-15	全部	查看配额（旧版）
ESSD云盘	ESSD云盘在华北2（北京）可用区G（公测）发布。	2018-07-14	华北2（北京）可用区G	云盘概述
实例故障排查	查看系统日志和屏幕截图。	2018-07-13	全部	查看实例的系统日志和屏幕截图
安全组	安全组内添加的实例数和安全组规则数量可提交工单调整。	2018-07-10	全部	使用限制
实例规格族	发布密集计算型实例规格族ic5。	2018-07-09	全部	实例规格族

2018年6月

功能名称	功能描述	发布时间	发布地域	相关文档
公共镜像	创建ECS实例时公共镜像支持选择Red Hat及其他操作系统。	2018-06-29	全部	使用向导创建实例
安全组	查看潜在高危安全组概览。	2018-06-22	全部	查看潜在高危安全组
配置升级	按量付费实例变配与实时降配支持跨系列。	2018-06-15	全部	变配规格
计费方式	包年包月实例支持按周续费。	2018-06-12	全部	手动续费实例
安全组	一键克隆经典网络安全组到专有网络。	2018-06-06	全部	克隆安全组
主动运维	主动运维二期上线。	2018-06-01	全部	ECS系统事件概述

2018年5月

功能名称	功能描述	发布时间	发布地域	相关文档
自定义镜像	发布镜像规范检测工具。	2018-05-28	全部	使用工具检测镜像规范
系统事件	ECS系统事件接入云监控，并支持历史记录查询功能。	2018-05-25	全部	ECS系统事件概述
实例启动模板	发布ECS实例启动模板。	2018-05-11	全部	实例启动模板

2018年4月

功能名称	功能描述	发布时间	发布地域	相关文档
计费方式	按量付费实例转包年包月实例。	2018-04-23	全部	按量付费转包年包月
配置降级	到期的包年包月ECS实例支持续费降配。	2018-04-13	全部	续费降配
控制台体验优化	控制台提供实例和存储资源概览大盘视图。	2018-04-01	全部	资源概览

2018年3月

功能名称	功能描述	发布时间	发布地域	相关文档
GPU实例	支持NGC GPU加速容器。	2018-03-28	全部	在gn5实例上部署NGC环境
系统事件	发布系统事件功能。	2018-03-26	全部	ECS系统事件概述
弹性裸金属服务器	发布弹性裸金属服务器。	2018-03-14	全部	弹性裸金属服务器概述
实例标识	发布实例标识功能。	2018-03-01	全部	使用实例标识

2018年2月

功能名称	功能描述	发布时间	发布地域	相关文档
ECS API	开放资源变配能力查询接口。	2018-02-10	全部	DescribeResourcesModification
包年包月实例	包年包月实例到期释放时长从7天延长到15天。	2018-02-07	全部	包年包月
ECS API	开放资源创建查询接口。	2018-02-02	全部	DescribeAvailableResource

2018年1月

功能名称	功能描述	发布时间	发布地域	相关文档
公网带宽	ECS带宽支持按小时临时升级。	2018-01-30	全部	临时升级带宽（连续时间段）
资源组	创建ECS实例时支持选择资源组。	2018-01-26	全部	资源组

2017年12月

功能名称	功能描述	发布时间	发布地域	相关文档
网络类型	控制台发布预约迁移升级，支持经典网络迁移到VPC网络。	2017-12-20	全部	经典网络迁移至专有网络
停机不收费	按量付费实例支持停机不收费。	2017-12-14	全部	按量付费实例节省停机模式
弹性网卡	发布弹性网卡功能。	2017-12-08	全部	弹性网卡
FPGA实例规格	FPGA云服务器f1正式售卖。	2017-12-02	全部	实例规格族
ECS API	开放批量创建实例接口。	2017-12-01	全部	RunInstances
实例故障排查	控制台支持实时诊断功能。	2017-12-01	全部	操作异常诊断

2017年11月

功能名称	功能描述	发布时间	发布地域	相关文档
包年包月实例	支持包年包月ECS资源统一到期日。	2017-11-30	全部	统一包年包月实例的到期日
迁云工具	发布迁云工具。	2017-11-27	全部	什么是服务器迁移中心
安全组规则	支持导入与导出安全组规则。	2017-11-23	全部	管理安全组规则
包年包月实例	包年包月实例到期支持设置不续费。	2017-11-23	全部	ModifyInstanceAutoRenewAttribute
计费方式	API支持按周付费实例的创建和续费。	2017-11-03	全部	CreateInstance
实例RAM角色	支持实例RAM角色功能。	2017-11-01	全部	概述

2017年10月

功能名称	功能描述	发布时间	发布地域	相关文档
弹性公网IP	支持VPC实例公网IP转弹性公网IP功能。	2017-10-31	全部	公网IP转EIP
抢占式实例	抢占式实例正式上线。	2017-10-18	全部	抢占式实例概述

功能名称	功能描述	发布时间	发布地域	相关文档
突发性能实例（t5）	发布突发性能实例t5。	2017-10-09	全部	突发性能实例概述

2017年9月

功能名称	功能描述	发布时间	发布地域	相关文档
计费方式	按量付费实例和云盘实行按秒计费、小时结算。	2017-09-29	全部	按量付费
gn5i实例规格族	ECS面向深度学习在线推理场景的gn5i规格族发布上线。	2017-09-23	全部	实例规格族
云盘加密	支持云盘加密。	2017-09-05	全部	ECS云盘加密

2017年8月

功能名称	功能描述	发布时间	发布地域	相关文档
安全组规则	安全组规则支持五元组方式配置。	2017-08-31	全部	安全组五元组规则
ClassicLink	经典网络实例与专有网络实例支持通过ClassicLink连接。	2017-08-25	全部	网络类型
实例规格族	发布基于Skylake处理器 +25G网络的最新一代高主频实例及本地SSD型实例。	2017-08-22	全部	实例规格族
ECS API	支持通过API变配实例的带宽。	2017-08-17	全部	ModifyInstanceNetworkSpec
自定义镜像	支持导入自定义镜像。	2017-08-10	全部	导入自定义镜像

2017年7月

功能名称	功能描述	发布时间	发布地域	相关文档
镜像	停止对Windows Server 2003系列公共镜像提供技术支持，建议您尽快更新至Windows Server 2012或以上版本。	2017-07-20	全部	公共镜像概述
资源组	ECS支持资源组创建和管理。	2017-07-18	全部	资源组
安全组	支持设置规则使同一安全组内网络不互通。	2017-07-07	全部	普通安全组内网络隔离
快照	快照正式商用。	2017-07-03	全部	快照计费

2017年6月

功能名称	功能描述	发布时间	发布地域	相关文档
经典网络	从17:00（UTC+8）时刻以后第一次创建ECS实例的用户，不能选择经典网络，建议您使用专有网络VPC。	2017-06-14	全部	什么是专有网络

2017年5月

功能名称	功能描述	发布时间	发布地域	相关文档
实例RAM角色	实例RAM角色API发布。	2017-05-26	全部	通过API使用实例RAM角色
实例规格族	网络优化型实例上线。	2017-05-23	全部	实例规格族
实例规格族	发布存储密集型d1规格族。	2017-05-12	全部	实例规格族
安全组	调整默认安全组安全策略，仅暴漏ICMP、TCP（22）和TCP（3389）。	2017-05-11	全部	默认安全组的默认规则
安全组	支持备份、覆盖及还原安全组。	2017-05-10	全部	还原安全组规则

2017年4月

功能名称	功能描述	发布时间	发布地域	相关文档
SSH密钥对	上线SSH密钥对功能。	2017-04-25	全部	SSH密钥对概述

2017年2月

功能名称	功能描述	发布时间	发布地域	相关文档
自定义镜像	cloud-init支持部分自定义镜像。	2017-02-24	全部	安装cloud-init
实例规格族	发布高IO型本地盘存储实例i1规格族。	2017-02-17	全部	实例规格族
快照	支持系统盘快照创建数据盘。	2017-02-15	全部	使用快照创建云盘
实例规格族	发布GPU计算实例gn4规格族。	2017-02-14	全部	实例规格族

2017年1月

功能名称	功能描述	发布时间	发布地域	相关文档
实例规格族	发布GPU可视化实例ga1规格族。	2017-01-24	全部	实例规格族
实例规格族	发布独享型实例se1规格族。	2017-01-21	全部	实例规格族

2016年

功能名称	功能描述	发布时间	发布地域	相关文档
快照	发布快照2.0。	2016-03-15	全部	快照概述
云盘扩容	发布系统盘扩容功能。	2016-01-15	全部	离线扩容云盘（Linux系统）

2015年

功能名称	功能描述	发布时间	发布地域	相关文档
自定义镜像	发布镜像导入功能。	2015-12-15	全部	导入镜像必读
安全组	控制台支持安全组功能。	2015-11-02	全部	创建安全组
镜像市场	镜像市场正式商用。	2015-09-02	全部	镜像市场
标签	发布标签功能。	2015-08-20	全部	标签概述
系统盘	按量付费实例支持更换操作系统功能开放。	2015-08-13	全部	更换操作系统（公共镜像）
自定义镜像	支持共享镜像给其他用户。	2015-05-15	全部	共享镜像
云盘扩容	磁盘离线扩容功能。	2015-04-20	全部	扩容概述
自定义镜像	发布镜像复制功能。	2015-01-26	全部	复制镜像

2014年

功能名称	功能描述	发布时间	发布地域	相关文档
块存储	发布独立云盘。	2014-08-22	全部	块存储介绍

2.产品公告

2.1. 【停售公告】停止售卖阿里云共享块存储（公测）

尊敬的阿里云用户，阿里云将于2022年06月30日起停止售卖共享块存储（公测）。块存储的共享挂载能力将通过多重挂载功能实现，多重挂载功能现已商业化发布，ESSD全系列均可支持，欢迎使用。

停售内容

阿里云将于2022年06月30日起停止售卖阿里云共享块存储（公测）。多重挂载功能的更多信息，请参见开启多重挂载功能。

停售时间

2022年06月30日

停售影响

- 自2022年06月30日起，您将无法新购阿里云共享块存储（公测）。
- 存量阿里云共享块存储云盘可以进行云盘扩容，服务不受影响。

3.安全公告

3.1. 漏洞公告 | Linux 内核本地权限提升漏洞（CVE-2022-0847）

2022年03月07日，国外安全研究员披露了一个Linux内核本地权限提升漏洞CVE-2022-0847。攻击者通过利用此漏洞可进行任意可读文件重写，将普通权限用户提升到root权限。漏洞作者将此漏洞命名为“Dirty Pipe”。目前网上已有公开的漏洞利用工具PoC。

漏洞信息

- 漏洞编号：CVE-2022-0847
- 漏洞评级：高危
- 影响范围：Linux内核版本大于等于5.8，或小于等于5.16.11/5.15.25/5.10.102

修复建议

阿里云强烈建议您关注该漏洞相关应用和系统的更新，及时更新组件至最新版本，或使用相关应用、系统的自动更新机制。

阿里云Alibaba Cloud Linux 3操作系统的内核版本已修复至安全版本。具体修复版本信息为Alibaba Cloud Linux 3：kernel-5.10.84-10.3.al8。

其他版本，请参考发行版本官方公告，将Linux内核升级至安全版本：

- Ubuntu公告
- Redhat公告
- Debian公告

部分操作系统的升级命令如下：

> **说明** 此过程需要重新启动您的机器，请您在升级之前做好各项数据保存。

如果您的操作系统为CentOS，可以采用如下命令进行内核升级：

```
sudo yum update -y kernel
```

重启之后，您可以使用如下命令查看您的内核是否升级到安全版本：

```
sudo uname -r
```

相关链接

The Dirty Pipe Vulnerability

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.2. 漏洞公告 | Linux Polkit权限提升漏洞风险（CVE-2021-4034）

近日，国外安全团队发布安全公告称，在Polkit的pkexec程序中发现一个本地权限提升漏洞。pkexec程序对命令行参数处理有误，造成通过参数注入能够导致本地提权的风险。

漏洞信息

- 漏洞编号：CVE-2021-4034
- 漏洞评级：高
- 影响范围：所有主流Linux发行版本均受影响

详细描述

本次漏洞具体是指存在于Polkit的pkexec程序中的内存损坏漏洞。这是一个安装在所有主要Linux发行版上的SUID-root程序，旨在允许非特权用户根据预定义的策略以特权用户身份运行命令。由于当前版本的pkexec程序对命令行参数处理有误，攻击者可以通过控制环境变量诱导pkexec程序执行任意代码。成功利用该漏洞后，可导致非特权用户获得管理员权限。

修复建议

阿里云的Anolis OS以及Alibaba Cloud Linux操作系统内的Polkit版本已修复至安全版本。具体版本信息如下：

- Anolis OS 7：polkit-0.112-26.an7.1
- Anolis OS 8：polkit-0.115-13.an8_5.1
- Alibaba Cloud Linux 2：polkit-0.112-26.3.al7.1
- Alibaba Cloud Linux 3：polkit-0.115-13.al8.1

其他各Linux发行版官方均已提供安全补丁，建议您尽快升级Polkit至安全版本。Ubuntu、Red Hat、CentOS及Debian官方漏洞公告，请参见：

- Ubuntu漏洞修复帮助文档
- Red Hat（含CentOS）漏洞修复帮助文档
- Debian漏洞修复帮助文档

部分操作系统升级命令说明如下：

- 如果您的操作系统为CentOS，可采用以下命令升级Polkit至安全版本。

  ```
  yum clean all && yum makecache && yum update polkit -y
  ```

  成功升级后，您可以运行以下命令查看Polkit的版本信息，检查是否为安全版本。

  ```
  rpm -qa polkit
  ```

- 如果您的操作系统为Ubuntu，可采用以下命令升级Polkit至安全版本。

  ```
  sudo apt-get updatesudo apt-get install policykit-1
  ```

  成功升级后，您可以运行以下命令查看Polkit的版本信息，检查是否为安全版本。

  ```
  dpkg -l policykit-1
  ```

相关链接

- pwnkit: Local Privilege Escalation in polkit's pkexec (CVE-2021-4034)
- pkexec: local privilege escalation (CVE-2021-4034)
- pwnkit: Local Privilege Escalation in polkit's pkexec (CVE-2021-4034)

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.3. 漏洞公告 | NSS内存损坏漏洞（CVE-2021-43527）

近日，Mozilla发布了Mozilla NSS（Network Security Services）缓冲区堆溢出的风险通告。NSS验证证书的方式中存在一个远程代码执行缺陷，该缺陷允许冒充TLS/SSL服务器的攻击者对使用NSS编译的客户端触发堆溢出的问题，此外，在使用NSS编译的服务器应用程序中处理客户端证书时也会触发堆溢出的问题。

漏洞信息

- 漏洞编号：CVE-2021-43527
- 漏洞评级：高
- 影响范围：NSS版本小于3.73或小于3.68.1 ESR

详细描述

NSS（Network Security Services）是一组支持跨平台开发安全客户端与服务器应用程序的程序库，提供了服务器侧硬件TLS/SSL加速和客户端侧智能卡的可选支持。

版本小于3.73或小于3.68.1 ESR的NSS，在处理DER编码的DSA或RSA-PSS签名时易发生堆溢出。影响项：

- 使用NSS处理CMS、S/MIME、pkcs# 7或pkcs# 12中编码签名的应用程序可能会受到影响。
- 使用NSS进行证书验证或其他功能（TLS、X.509、OCSP或CRL功能）的应用程序可能会受到影响。

> **说明** 您可以通过curl -V命令查看系统中默认使用的NSS版本信息。

安全建议

通过curl -V命令查看并排查NSS版本是否小于3.73或小于3.68.1 ESR。如果小于请尽快将NSS升级到安全版本。修复命令如下：

```
yum clean all & yum install -y nss
```

相关链接

Bug 1737470 - Ensure DER encoded signatures are within size limits.

公告方

阿里云计算有限公司

3.4. 漏洞公告 | Linux Netfilter本地权限提升漏洞（CVE-2021-22555）

近日，海外研究团队披露出Linux Netfilter本地权限提升漏洞，漏洞编号CVE-2021-22555。该漏洞在kCTF中被用于攻击Kubernetes Pod容器，实现容器逃逸。此漏洞影响较大，阿里云建议您及时自查并修复漏洞。

漏洞信息

- 漏洞编号：CVE-2021-22555
- 漏洞评级：高
- 影响范围：Linux内核版本大于等于 `2.6.19(9fa492cdc160cd27ce1046cb36f47d3b2b1efa21)`
- ECS受影响的镜像版本包括：
  - Alibaba Cloud Linux 2/3
  - CentOS 7/8
  - RedHat 7/8
  - Ubuntu 14/16/18/20
  - Debian 8/9/10
  - SUSE Linux Enterprise Server 12/15
  - OpenSUSE 42.3/15

详细描述

Linux Netfilter模块在实现IPT_SO_SET_REPLACE（或IP6T_SO_SET_REPLACE）setsockopt时，存在堆越界写入漏洞。该漏洞将允许本地用户通过用户名空间获取权限提升，在kCTF中被用于攻击Kubernetes Pod容器，实现容器逃逸。该漏洞已在Linux内核代码中存在15年。

安全建议

如果您的ECS实例操作系统为Alibaba Cloud Linux 2，具体修复方案，请参见Alibaba Cloud Linux 2系统的CVE-2021-22555安全漏洞内核热补丁修复方案。

其他发行版的操作系统，请您尽快将Linux内核版本升级到如下所示的安全版本。

- `5.12(b29c457a6511435960115c0f548c4360d5f4801d)`
- `5.10.31`
- `5.4.113`
- `4.19.188`
- `4.14.231`
- `4.9.267`
- `4.4.267`

RedHat提供的临时修补建议：

您可以通过运行以下命令禁止非特权用户执行CLONE_NEWUSER与CLONE_NEWNET，以缓解该漏洞产生的影响。

```
echo 0 > /proc/sys/user/max_user_namespaces
```

相关链接

- Linux: Heap Out-Of-Bounds Write in xt_compat_target_from_user
- CVE-2021-22555 Detail
- 如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.5. 漏洞公告 | Windows Print Spooler 0day漏洞预警（CVE-2021-34527）

微软官方于2021年07月01日发布Windows Print Spooler远程代码执行漏洞，漏洞编号为CVE-2021-34527。成功利用该漏洞的攻击者可以使用SYSTEM权限运行任意代码。阿里云建议您及时更新漏洞补丁，并做好安全防护工作。

漏洞信息

- 漏洞编号：CVE-2021-34527
- 漏洞评级：严重
- 影响范围：
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2008 R2
  - Windows Server, version 2004 (Server Core installation)
  - Windows Server, version 1909 (Server Core installation)

详细描述

微软官方在2021年06月发布的更新补丁中，已经解决了Windows Print Spooler权限提升漏洞（CVE-2021-1675）。本次微软官方发布的Windows Print Spooler远程代码执行漏洞（CVE-2021-34527）与CVE-2021-1675漏洞相似，但不完全相同。当Windows Print Spooler服务不正确地执行特权文件的相关操作时，存在远程执行代码漏洞风险，攻击者会攻击必须调用 `RpcAddPrinterDriverEx()` 且经过身份验证的用户。

成功利用该漏洞的攻击者可以使用SYSTEM权限运行任意代码，进而完成安装程序、管理（查看、更改或删除）数据或创建具有完全用户权限的新账户等操作。

安全建议

及时更新官方补丁。

解决方案

前往微软官方下载相应的补丁进行更新。具体操作，请参见CVE-2021-34527。

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.6. 漏洞公告 | Windows Print Spooler权限提升漏洞预警（CVE-2021-1675）

2021年06月08日，微软官方发布了06月更新补丁，其中包括一个Windows Print Spooler权限提升漏洞，漏洞CVE编号为CVE-2021-1675。未经身份验证的远程攻击者可以利用该漏洞以SYSTEM权限在域控制器上执行任意代码，从而获得整个域的控制权。阿里云建议您及时更新漏洞补丁，并做好安全防护工作。

漏洞信息

- 漏洞编号：CVE-2021-1675
- 漏洞评级：严重
- 影响范围：
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2008 R2
  - Windows Server, version 2004 (Server Core installation)
  - Windows Server, version 1909 (Server Core installation)

详细描述

Print Spooler是Windows系统中用于管理打印相关事务的服务。在域环境中，如果存在合适的条件，未经身份验证的远程攻击者无需进行任何交互，即可利用该漏洞以SYSTEM权限在域控制器上执行任意代码，从而获得整个域的控制权。

安全建议

及时更新官方补丁。

解决方法

前往微软官方下载相应的补丁进行更新。具体操作，请参见CVE-2021-1675。

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.7. 漏洞公告 | Windows HTTP协议远程代码执行漏洞预警（CVE-2021-31166）

2021年05月11日，微软官方发布补丁，修复了Windows HTTP协议远程代码执行问题导致的高危严重漏洞。微软官方将其标记为可造成蠕虫攻击及易被攻击，攻击者可以利用该漏洞造成大范围蠕虫攻击。

漏洞信息

- 漏洞编号：CVE-2021-31166

- 漏洞评级：严重
- 影响范围：Windows Server, version 2004 (Server Core installation)

  具体包含以下操作系统版本：

  - Windows Server Version 2004 数据中心版 64位中文版
  - Windows Server Version 2004 数据中心版 64位英文版
  - Windows Server Version 2004 with Container 数据中心版 64位中文版
  - Windows Server Version 2004 with Container 数据中心版 64位英文版

详细描述

该漏洞存在于Windows 10和Windows Server中的HTTP协议栈（`http.sys`）处理程序中，该程序广泛的用于应用之间或设备之间的通信，常见的组件（例如`Internet Information Services（IIS）`）便使用该程序进行通信处理。未授权的攻击者可以构造恶意请求包攻击目标服务器，成功利用该漏洞的攻击者可以在目标服务器执行任意代码。

安全建议

及时更新官方补丁。

解决方法

前往微软官方下载相应的补丁进行更新。具体操作，请参见CVE-2021-31166。

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.8. 漏洞公告 | Windows多个严重高危漏洞预警（CVE-2021-24074、CVE-2021-24078等）

2021年2月10日，微软官方发布补丁，修复了包含TCP/IP远程执行代码漏洞（CVE-2021-24074）、Windows DNS Server远程代码执行漏洞（CVE-2021-24078）在内的多个高危严重漏洞。目前微软官方已提供相应的月度安全补丁以修复该漏洞。

漏洞信息

- 漏洞编号：CVE-2021-24074、CVE-2021-24078
- 漏洞评级：严重
- 影响范围：
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2008 R2
  - Windows Server, version 2004 (Server Core installation)

- Windows Server, version 1909 (Server Core installation)

详细描述

微软官方于2021年2月10日发布安全更新，其中修复了多个高危严重漏洞。在CVE-2021-24074 TCP/IP远程执行代码漏洞中，攻击者通过构造并发送恶意的IPv4/IPv6数据包，从而控制目标主机。在CVE-2021-24078 Windows DNS Server远程代码执行漏洞中，攻击者通过构造并发送恶意的DNS请求，可以在开启了DNS服务的Windows Server上执行任意代码。同时微软2月补丁中还涉及其他多个高危漏洞，建议您尽快安装补丁阻止漏洞攻击。

安全建议

及时更新官方补丁。

解决方法

您可以使用以下任一解决方法：

- 前往微软官方下载相应的补丁进行更新。具体操作，请参见CVE-2021-24074和CVE-2021-24078。
- 阿里云云安全中心Windows系统漏洞模块已支持对该漏洞补丁一键检测和修复。更多信息，请登录云安全中心控制台。
- 针对CVE-2021-24074 TCP/IP远程执行代码漏洞，您可以将 `sourceroutingbehavior` 设置为 `drop` 来缓解风险。

```
netsh int ipv4 set global sourceroutingbehavior=drop
```

相关链接

Microsoft安全更新程序指南

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.9. 漏洞公告 | Linux sudo权限漏洞（CVE-2021-3156）

2021年1月26日，Linux sudo堆漏洞被公开。利用此漏洞，攻击者可以在默认配置的sudo主机上获取root权限。

漏洞信息

- 漏洞编号：CVE-2021-3156
- 漏洞评级：高
- sudo受影响的版本包括：
  - 1.8.2到1.8.31p2的版本
  - 1.9.0到1.9.5p1的稳定版本
- ECS受影响的镜像版本包括：
  - Alibaba Cloud Linux 2

- CentOS 6/7/8
- Red Hat Enterprise Linux 6/7/8
- Ubuntu 14/16/18/20
- Debian 8/9/10
- SUSE Linux Enterprise Server 12/15
- OpenSUSE 42.3/15
- FreeBSD 11/12

详细描述

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。利用sudo堆溢出漏洞CVE-2021-3156，普通用户可以在易受攻击的主机上获得root特权。

安全建议

及时更新官方补丁。

截至目前，大部分系统已经修复对应的sudo漏洞，对应的更新包已经推出，请及时更新官方补丁。

检测方法

检测方法如下：

- 方法一：执行 `sudo --version` 查看sudo版本号是不是在受影响版本范围。
- 方法二：以非root账户登录系统运行命令 `sudoedit -s /` 。

结果如下：

- 如果错误信息以 `sudoedit:` 开头，表示受影响，您需要修复。
- 如果错误信息以 `usage:` 开头，表示已安装补丁，您无需修复。

解决方法

更新sudo版本至1.9.5p2或更新版本。

相关链接

- Alibaba Cloud Linux漏洞修复帮助文档
- Debian漏洞修复帮助文档
- Red Hat漏洞修复帮助文档
- Ubuntu漏洞修复帮助文档
- SUSE漏洞修复帮助文档

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.10. 漏洞公告 | Windows TCP/IP远程执行代码漏洞（CVE-2020-16898）

2020年10月13日，微软发布预警，Windows TCP/IP堆栈不正确的处理ICMPv6 Router Advertisement（路由通告）数据包时，存在一个远程执行代码漏洞。成功利用此漏洞的攻击者可以获得在目标服务器或客户端上执行代码的能力。该漏洞（CVE-2020-16898）官方评级严重，目前微软官方已提供相应的月度安全补丁以修复该漏洞。

漏洞信息

- 漏洞编号：CVE-2020-16898
- 漏洞评级：严重
- 影响范围：
  - Windows Server 2019
  - Windows Server 2019 (Server Core installation)
  - Windows Server, version 1903 (Server Core installation)
  - Windows Server, version 1909 (Server Core installation)
  - Windows Server, version 2004 (Server Core installation)

详细描述

Windows TCP/IP堆栈不正确的处理ICMPv6 Router Advertisement数据包时，存在一个远程执行代码漏洞（CVE-2020-16898）。如果攻击者要利用此漏洞，必须将特制的ICMPv6 Router Advertisement数据包发送到远程Windows计算机。远程攻击者无需接触目标计算机也无需获取相应权限，只需向目标计算机发送攻击数据包即可能实现RCE（remote command/code execute）。目前尚无EXP（Exploit）公开。

安全建议

及时更新官方补丁。

解决方法

您可以使用以下任一解决方法：

- 前往微软官方下载相应的补丁进行更新。请参见CVE-2020-16898 | Windows TCP/IP Remote Code Execution Vulnerability。
- 阿里云云安全中心Windows系统漏洞模块已支持对该漏洞补丁一键检测和修复，详情请参见Windows系统漏洞。
- 通过禁用ICMPv6 RDNSS，缓解风险。

  通过以下PowerShell命令禁用ICMPv6 RDNSS，以防止攻击者利用此漏洞。此解决方法仅适用于Windows 1709及更高版本。

  ```
  netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable
  ```

  > **说明** 进行更改后，无需重新启动。

  您也可以使用以下PowerShell命令重新开启ICMPv6 RDNSS，但无法再缓解被攻击的风险。

  ```
  netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=enable
  ```

  > **说明** 进行更改后，无需重新启动。

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.11. 漏洞公告 | Linux内核漏洞（CVE-2020-14386）

9月4日，Linux社区公布了编号为CVE-2020-14386的内核漏洞。该漏洞源自Linux内核*net/packet/af_packet.c*，攻击者可以通过该漏洞实现越界写，可能造成提权和容器逃逸等风险。

漏洞信息

- 漏洞编号：CVE-2020-14386
- 漏洞评级：高
- 影响版本：
  - 内核版本高于4.6的不同操作系统的Linux发行版均在此次漏洞的影响范围内。
  - ECS受影响的镜像版本包括：
    - Alibaba Cloud Linux 2.1903（原Aliyun Linux 2.1903）
    - CentOS 8
    - Red Hat Enterprise Linux 8
    - Debian 9/10
    - OpenSUSE 15
    - SUSE Linux Enterprise Server 12/15
    - Ubuntu 18.04/20.04

详细描述

CVE-2020-14386是内核模块中存在的内存溢出漏洞。在高版本Linux系统（内核版本高于4.6）上，非特权用户以及K8s或Docker容器中的用户存在触发该漏洞的可能。该漏洞能够允许攻击者实现越界写，可能实现提权或容器逃逸。

安全建议

及时更新官方补丁。

解决方法

- Alibaba Cloud Linux 2.1903（Aliyun Linux 2.1903）修复和升级方式：
  i. 使用以下任一方式升级内核版本。
     - 运行以下命令升级内核至修复版本。

```
yum -y install kernel-4.19.91-21.2.al7
```

     - 运行以下命令升级至最新内核版本。

```
yum -y update kernel
```

  ii. 运行以下命令重启系统。

```
reboot
```

> **说明** 关于Alibaba Cloud Linux 2.1903安全漏洞的修复信息，请参见Alibaba Cloud Linux 2 CVE更新记录。

- 公共镜像升级方式请参见SUSE Linux Enterprise Server、Ubuntu、Debian。

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.12. 漏洞公告 | 虚拟化逃逸0day漏洞

ISC2020第八届互联网安全大会上，QEMU-KVM虚拟机的0day漏洞（虚拟机逃逸）被公开。该漏洞可越界读写某一个堆之后0xffffffff（4 GB内存）的内容，可实现完整的虚拟机逃逸。阿里云已对该漏洞进行了修复。

漏洞信息

2019年11月17日天府杯国际网络安全大赛，第一次暴露出QEMU-KVM虚拟机的0day安全漏洞。2020年08月13日，ISC2020第八届互联网安全大会上，该漏洞被公开。该漏洞可越界读写某一个堆之后0xffffffff（4 GB内存）的内容，可实现完整的虚拟机逃逸，最终在宿主机中执行任意代码，造成较为严重的信息泄露。截止目前QEMU官方并未提供任何修复补丁。

解决方法

阿里云已于2019年12月完成该漏洞的修复，您无需做修复操作。

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司

3.13. 漏洞公告 | Windows SMBv3远程执行代码漏洞（CVE-2020-0796）

3月12日，微软发布了CVE-2020-0796漏洞更新补丁，用于更新Windows操作系统的SMBv3远程执行代码漏洞。利用此漏洞，攻击者可以获得在目标服务器或客户端上执行代码的能力。阿里云已经同步更新Windows系统更新源，建议您及时更新ECS实例的操作系统到最新补丁。

漏洞信息

- 漏洞编号：CVE-2020-0796
- 漏洞评级：高危，风险极大
- 补丁更新日期：2020年03月12日
- 漏洞位置：Windows 10和Windows Server的服务器消息模块3.1.1（Server Message Block 3.1.1，简称SMBv3）
- 影响版本：
  - Windows 10，Version 1903，1909
  - Windows Server Version 1903

- Windows Server Version 1909

> **说明** 2020年04月01日之后，阿里云Windows Server Version 1909公共镜像已更新安全补丁，如果您在ECS管理控制台使用该公共镜像创建了ECS实例，或者更换实例系统盘，则无需更新补丁。

详细描述

Microsoft SMBv3协议处理某些请求的方式中存在一个已知的远程执行代码漏洞。攻击者利用此漏洞可以在目标服务器或客户端上执行代码。

- 针对服务器的漏洞，未经身份验证的攻击者可以将恶意数据包发送到目标SMBv3服务器。
- 针对客户端的漏洞，未经身份验证的攻击者可以配置恶意的SMBv3服务器，并诱使您连接到该恶意服务器。

安全建议

及时更新官方补丁。

解决方法

您可以选择以下任意方式更新补丁。

- 方式一：从Windows Update更新，并确保安装最新的2020年3月份安全更新或累积更新。
- 方式二：前往微软官方网站，自行下载对应的补丁。
  i. 下载并安装服务堆栈更新KB4541338。
     - 下载地址：KB4541338
     - Windows Server Version 1909直接下载地址：windows10.0-kb4541338-x64
  ii. 下载并安装累积更新KB4551762。
     - 下载地址：KB4551762
     - Windows Server Version 1909直接下载地址：windows10.0-kb4551762-x64
  iii. 重启ECS实例的操作系统。

如果您有相关需求或反馈，请提交工单联系阿里云。

相关链接

- Microsoft官方安全公告
- 微软补丁信息帮助文档

公告方

阿里云计算有限公司

3.14. 漏洞公告 | Windows加密库漏洞（CVE-2020-0601）

1月14日，微软发布了CVE-2020-0601漏洞更新补丁，用于更新Windows操作系统的Windows CryptoAPI验证绕过漏洞。利用此漏洞，攻击者可伪造签名将勒索软件或间谍软件伪装成可信文件的方式，从而发起攻击。阿里云已同步更新Windows系统更新源，建议您及时更新ECS实例的操作系统到最新补丁。

漏洞信息

- 漏洞编号：CVE-2020-0601
- 漏洞评级：高危，风险极大
- 补丁更新日期：2020年01月14日
- 影响版本：
  - Windows 10
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server Version 1809
  - Windows Server Version 1903
  - Windows Server Version 1909

详细描述

CVE-2020-0601漏洞位于验证证书合法性的Windows CryptoAPI（Crypt32.dll）椭圆曲线加密算法，会对以下场景和信任实体造成严重影响。

- HTTPS连接
- 签名文件和签名电子邮件
- 用户模式启动的签名可执行程序

攻击者利用此漏洞可以伪造证书签名恶意文件，或是通过中间人攻击方式解密用户连接，截获受影响软件的机密信息。

安全建议

及时更新官方补丁。

解决方法

您可以选择以下任意方式更新补丁。

- 方式一：从Windows Update更新，并确保安装最新的2020年1月份安全更新或累积更新。
- 方式二：前往微软官方网站，自行下载对应的补丁。

如果您有相关需求或反馈，请提交工单联系阿里云。

公告方

阿里云计算有限公司