ALIBABA CLOUD

阿里云

操作审计

产品简介

文档版本：20220628

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

1.什么是操作审计 ---------- 05
2.基本概念 ---------- 07
3.使用限制 ---------- 09
4.支持的云服务 ---------- 10
5.支持的地域 ---------- 26
6.单账号跟踪、多账号跟踪和平台事件跟踪的差异 ---------- 28

1.什么是操作审计

操作审计（ActionTrail）帮助您监控并记录阿里云账号的活动，包括通过阿里云控制台、OpenAPI、开发者工具对云上产品和服务的访问和使用行为。您可以将这些行为事件下载或保存到日志服务SLS或对象存储OSS，然后进行行为分析、安全分析、资源变更行为追踪和行为合规性审计等操作。

操作审计的实现原理如下图所示。

功能特性

- 开箱即用：无需配置，操作审计默认为您追踪并记录最近90天的事件，支持在线查阅事件。
- 自主管理：通过创建跟踪，操作审计可以将事件保存到日志服务SLS（日志的形式）或对象存储OSS（文件的形式）。您可以利用日志服务的检索能力、分析功能或进一步转存到大数据产品来管理这些数据，例如：授权、开启生命周期管理、归档管理、检索、分析和报警等。
- 多维度查询：操作审计支持从操作时段、用户名、资源类型、资源名称或操作名称等维度查询事件。

应用场景

- 等保合规：根据等保2.0条例要求，云上租户必须记录账户活动并至少保存180天。通过操作审计可以将账号活动记录投递到日志服务或OSS存储空间并长久保存。
- 安全分析：操作审计会对用户操作进行详细的记录，通过这些事件您可以判断您的账号是否存在安全问题。

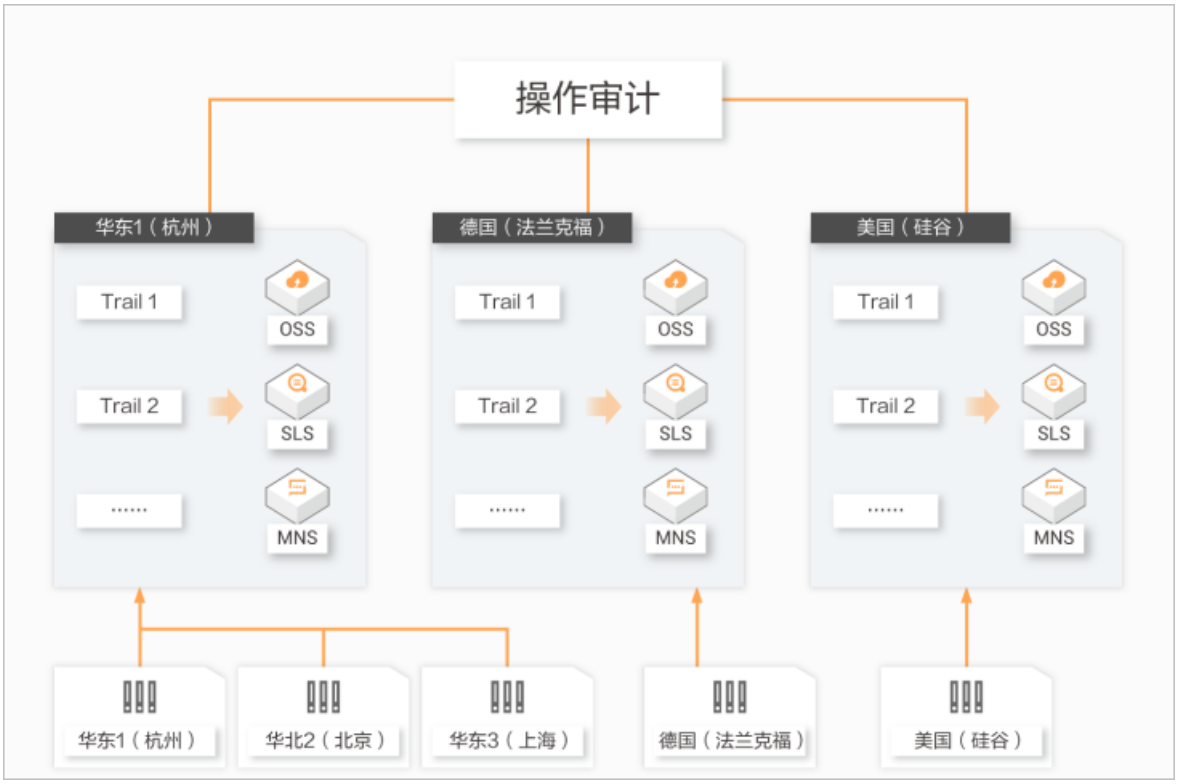
  例如：您可在跟踪中设置将操作事件投递到日志服务SLS的Logstore，进行更长时间地保存和SQL分析。

- 资源变更追踪：当您的资源出现异常变更时，操作审计记录的操作可以帮您定位问题。例如：当您发现一

台ECS实例停机了，您可以通过操作审计定位停机的操作者、操作时间以及操作IP地址。

- 合规性审计：如果您的组织有多个成员，而且您已经使用了访问控制RAM来管理这些成员，操作审计可以满足您所在组织的合规性审计要求，帮您获取每个成员的详细事件。您还可以根据审计人员的职责不同，创建多个跟踪追踪不同区域的不同事件类型并投递到不同的存储空间。

  例如：如果您在阿里云中国站和国际站均部署了资源，考虑到各国家数据安全要求不同，您可以创建多个追踪分别追踪不同国家、地域的操作事件，分别投递到当地的存储空间。



产品优势

- 快速推送：操作审计收集用户使用阿里云服务的事件（包括用户通过控制台触发的操作、调用阿里云API进行的操作以及云服务通过服务角色进行的操作等）。事件通常会在10分钟内被操作审计追踪并记录。
- 详细记录：操作审计会详细记录用户操作上下文信息，并可以通过操作审计控制台或调用API来查看最近90天的事件。例如：您可以获知是谁在什么时刻、从哪个源IP发起对哪个对象的什么操作？该操作来自于API还是控制台？操作结果是成功还是失败？失败原因是什么？
- 稳定可靠：操作审计支持将事件投递到日志服务SLS或对象存储OSS等存储产品中，这些存储产品具有高可用性，并且可以通过加密和权限控制，保证审计数据安全。当投递发生时，操作审计还将向您发送通知。
- 定制跟踪：您最多可以在每个地域创建5个跟踪，分别追踪不同的事件类型、区域范围，并可分别投递到不同的存储空间，以满足您为不同职责员工备份不同范围行为数据的要求。

  > **说明** 应避免同一个区域的相同事件类型重复投递到同一个地址。

- 平台运维透明：操作审计可以近实时地记录并存储阿里云平台的操作日志，基于日志服务提供查询、分析、告警、报表等下游计算能力，为用户打开平台运维的黑盒，满足您对平台操作的分析和审计需求。

2.基本概念

本文解释了操作审计的基本概念，帮助您正确理解和使用操作审计。

概念	说明
管理账号	管理账号是资源目录的超级管理员，也是开通资源目录的初始账号，对其创建的资源目录和成员拥有完全控制权限。只有通过企业实名认证的阿里云账号才能开通资源目录，每个资源目录有且只有一个管理账号。
成员	在资源目录内，成员作为资源容器，是一种资源分组单位。成员通常用于指代一个项目或应用，每个成员中的资源相对其他成员中的资源是物理隔离的。您可以通过管理账号授予RAM用户、RAM用户组或RAM角色对成员内资源的访问权限。 成员被管理账号邀请进入资源目录，或由管理账号在资源目录内直接创建。
事件	事件是用户通过阿里云控制台、OpenAPI、开发者工具访问和管控云上服务所产生的事件记录。事件包含时间、人员、资源、操作类型、操作结果、来源IP等信息。根据事件来源的不同分为管控事件和Insight事件。
管控事件	管控事件是用户管理云上资源时，管控平面的操作记录（例如：RDS实例、OSS存储空间的创建、删除），但不包括数据平面的操作记录（例如：RDS实例内的表操作、OSS对象的操作）。
Insight事件	Insight事件是帮助用户从管控事件中发现异常行为的事件。基于管控事件的分析结果，Insight事件呈现了一种异常情况的发生。目前仅支持IPInsight事件。您在跟踪中启用IPInsight事件功能后，操作审计会基于过去已有的管控操作事件分析出常规的来访IP特征，然后判断新的来访IP是否为异常IP。当发现一个异常IP，将生成一个IPInsight事件向您通报异常IP的情况。
全局服务	全局服务是不区分地域的服务，例如：RAM。全局服务会产出全局事件。
全局事件	全局事件是全局服务的事件。在操作审计控制台的**事件查询**页面，选择任意地域均可看到全量的全局事件。但当事件被投递到用户设置的OSS存储空间时，全局事件与跟踪的Home地域事件放在同一个目录下。
Home地域	Home地域是发起创建跟踪操作的地域。
跟踪	跟踪是一种配置，用于将事件保存到指定的OSS存储空间或SLS Logstore，以便进一步分析和存储。根据创建者、作用范围和投递内容的不同分为单账号跟踪、多账号跟踪和平台事件跟踪。
单账号跟踪	单账号跟踪是阿里云账号创建的用于记录当前账号事件的跟踪。
多账号跟踪	多账号跟踪是管理账号创建的用于记录所有成员事件的跟踪。多账号跟踪会把所有成员的事件投递到多账号跟踪设置的OSS存储空间或SLS Logstore。
平台事件	平台事件是阿里云运维团队针对用户服务的维护操作所产生的事件。您可以通过平台操作审计创建跟踪，记录此类事件。
平台事件跟踪	平台事件跟踪是阿里云账号创建的用于记录平台事件的跟踪。

概念	说明
影子跟踪	如果您创建跟踪的同时追踪了多个地域的事件，则操作审计会在相关地域创建相同配置的跟踪来收集这些地域的事件，这种跟踪叫做影子跟踪。

3.使用限制

本文列举了操作审计的使用限制。

限制项	最大值
一个阿里云账号允许创建的跟踪数目	• 单账号跟踪：每个地域5个 • 多账号跟踪：所有地域1个 • 平台事件跟踪：所有地域1个
一个跟踪允许配置的OSS存储空间（Bucket）数目	1个
用户操作后多久才能通过控制台查询数据	10分钟
用户操作多久才能在OSS存储空间中访问数据	10分钟
用户通过控制台或API能查询多久的操作事件 **说明** 操作审计默认为每个阿里云账号记录最近90天的操作事件，如果不创建跟踪，您将无法追溯90天以前的操作事件。	90天
单账号跟踪的历史事件通过操作审计控制台或LookupEvents接口查询时，每秒最多查询次数	2次

说明

- RAM用户、用户组或RAM角色可以绑定的策略个数与授权范围无关，即单个资源组内授权与整个云账号内授权的策略额度是相同的，彼此独立，不会互相占用。
- 本文仅展示了各限制项的默认配额。对于可以调整配额的限制项，您可以前往配额中心申请提升配额。配额中心现已支持多个云产品，请参见配额中心支持的云产品。

4.支持的云服务

本文介绍操作审计支持的云服务及其相关事件。

弹性计算

云服务	云服务代码	支持时间	云服务事件支持情况说明
云服务器ECS	Ecs	2020年前	无
弹性伸缩	Ess	2020年前	无
容器服务	CS	2020年前	无
容器镜像服务	cr	2020年前	无
轻量应用服务器	SWAS	2020年前	无
批量计算	BatchCompute	2020年前	无
弹性高性能计算E-HPC	EHPC	2020年前	无
Web应用托管服务	WebPlus	2020年前	无
弹性容器实例ECI	Eci	2020年前	无
运维编排服务	oos	2020年前	无
函数计算	FC	2020-11-27	无
弹性云桌面	ECD	2020-12-21	无
云桌面	Gws	2021-04-28	无
Serverless应用引擎	SAE	2021-08-03	无
云盒	CloudBox	2021-07-29	无
计算巢服务	ComputeNest	2021-07-12	无
VMware服务	ACVS	2022-01-05	无
弹性云手机	ECP	2021-10-22	无
块存储	EBS	2021-12-23	无
Serverless工作流	FnF	2021-09-16	无
弹性加速计算实例	EAIS	2021-09-01	无
分布式云容器平台	AckOne	2022-03-30	分布式云容器平台事件说明

存储

云服务	云服务代码	支持时间	云服务事件支持情况说明
文件存储	NAS	2020年前	无
智能云相册	CloudPhoto	2020年前	无
对象存储OSS	Oss	2020年前	仅OSS Bucket管控事件可以通过操作审计控制台查询。OSS Bucket管控事件列表，请参见事件。 当您通过角色扮演或跨账号授权的方式管控OSS时，身份信息可能不准确。当OSS记录完整的OSS Bucket管控事件后可以明确身份信息，我们将尽快推动OSS服务团队解决此问题。
智能媒体管理	IMM	2020-07-21	无
云存储网关	CloudStorageGateway	2020-11-27	无
数据库文件存储	DBFS	2020-12-21	数据库文件存储支持被审计的事件说明
文件存储HDFS	DFS	2021-01-13	文件存储HDFS事件说明
混合云备份服务	HBR	2021-07-20	无
混合云容灾服务	HDR	2021-07-20	无
闪电立方	HcsMgw	2021-07-12	无
相册与网盘服务	PDS	2021-09-08	无
日志服务	SLS	2021-10-11	无

数据库

云服务	云服务代码	支持时间	云服务事件支持情况说明
云数据库RDS版	Rds	2020年前	无
数据传输服务DTS	Dts	2020年前	无
HybridDBforMySQL	PetaData	2020年前	无

云服务	云服务代码	支持时间	云服务事件支持情况说明
HybridDBforPostgreSQL	gpdb	2020年前	无
云数据库Redis版	R-kvstore	2020年前	无
云数据库PolarDB	polardb	2020年前	无
分布式关系型数据库服务	Drds	2020年前	无
云数据库MongoDB版	Dds	2020年前	无
表格存储	OTS	2020-02-27	无
云原生数据仓库AnalyticDB MySQL版2.0	ADS	2020-02-27	无
云原生数据仓库AnalyticDB MySQL版3.0	ADB	2021-08-27	无
数据库自治服务DAS	DAS	2020-02-26	无
数据管理DMS	DMSEnterprise	2020-05-18	无
云数据库HBase	HBase	2020-02-27	无
时序数据库	TSDB	2020-12-29	时序数据库事件说明
云数据库Cassandra版	Cassandra	2021-01-08	云数据库Cassandra版事件说明
云数据库OceanBase版	OceanBase	2021-03-19	无
图数据库	GraphDatabase	2021-06-25	无
数据库和应用迁移	ADAM	2021-06-15	无
云数据库ClickHouse版	ClickHouse	2021-06-10	云数据库ClickHouse版事件说明
云数据库专属集群	CDDC	2021-07-27	无
可信账本数据库	LedgerDB	2021-06-02	无
数据库备份	DBS	2021-08-16	无
数据湖分析	DataLakeAnalytics	2021-07-28	无

网络

云服务	云服务代码	支持时间	云服务事件支持情况说明
专有网络VPC	Vpc	2020年前	无
NAT网关	Vpc	2020年前	无
弹性公网IP	Vpc	2020年前	无
高速通道	Vpc	2020年前	无
全球加速	Vpc	2020年前	无
共享流量包	flowbag	2020年前	无
共享带宽	Vpc	2020年前	无
云企业网	Cen	2020年前	无
传统型负载均衡	Slb	2020年前	无
应用型负载均衡	ALB	2021-08-24	无
智能接入网关	Smartag	2020年前	无
PrivateLink	Privatelink	2020年前	无
云解析PrivateZone	PrivateZone	2021-01-13	云解析PrivateZone事件说明
全球加速	Ga	2021-03-16	无
云网管	CMN	2021-02-23	云网管事件说明
任播弹性公网IP	Eipanycast	2022-04-18	无

视频与CDN

云服务	云服务代码	支持时间	云服务事件支持情况说明
CDN	Cdn	2020年前	无
视频点播	vod	2020年前	无
视频直播	live	2020年前	无
媒体处理	Mts	2020年前	无
音视频通信	RTC	2020-08-26	无
云视频会议	Aliyuncvc	2020-09-21	无

云服务	云服务代码	支持时间	云服务事件支持情况说明
PCDN	Pcdn	2020年前	无
全站加速	DCDN	2020-02-13	无
边缘节点服务ENS	ENS	2020-02-27	无
视频监控	VideoSurveillanceSystem	2021-06-10	无
智能媒体中台	IMP	2021-08-12	无
智能媒体生产	ICE	2021-08-04	无
智能视觉	IVisionVCS	2021-05-10	无
安全加速SCDN	SCDN	2021-07-06	无

域名与网站（万网）

云服务	云服务代码	支持时间	云服务事件支持情况说明
域名	Domain/Domain-intl	2020年前	无
云解析DNS	Alidns	2020年前	无

应用服务

云服务	云服务代码	支持时间	云服务事件支持情况说明
API网关	CloudAPI	2020年前	无
云AP	cloudwf	2020年前	无
云桌面	CloudDesktop	2020年前	无
区块链服务	Baas	2020年前	无
开放搜索	OpenSearch	2020-08-17	无

互联网中间件

云服务	云服务代码	支持时间	云服务事件支持情况说明
消息队列RocketMQ	Ons	2020年前	无

云服务	云服务代码	支持时间	云服务事件支持情况说明
消息队列Kafka版	AliKafka	2020-02-27	消息队列Kafka版支持被审计的事件说明
应用配置管理ACM	ACM	2020-07-31	无
性能测试PTS	PTS	2020-08-06	无
微服务引擎MSE	MSE	2020-09-16	无
事件总线EventBridge	EventBridge	2020-11-18	无

云通信

云服务	云服务代码	支持时间	云服务事件支持情况说明
短信服务	Dysms	2020年前	无
短信服务API	Dysmsapi	2020年前	无
语音服务	Dyvms	2020年前	无
语音服务API	Dyvmsapi	2020年前	无
流量服务	Dycdp	2020年前	无
流量服务API	Dycdpapi	2020年前	无
号码隐私保护	Dypls	2020-07-21	无
号码认证服务	Dypns	2020-06-04	无

云游戏

云服务	云服务代码	支持时间	云服务事件支持情况说明
云游戏平台	CloudGamingPlatform	2020-07-30	无

安全

云服务	云服务代码	支持时间	云服务事件支持情况说明
DDoS原生防护（防护包）	ddosbgp	2020年前	无
DDoS高防（新BGP）	ddoscoo	2020年前	无

云服务	云服务代码	支持时间	云服务事件支持情况说明
Web应用防火墙	waf-openapi	2020年前	无
安骑士	aegis	2020年前	无
堡垒机	Yundun-bastionhost	2020年前	无
数据库审计	DBAudit	2020-02-27	无
云防火墙	Cloudfw	2020年前	无
数据风控	afs	2020年前	无
网站威胁扫描系统	avds	2020年前	无
SSL证书	cas	2020年前	无
云安全中心	Sas	2020年前	无
内容安全	Green	2020年前	无
数据安全中心	Sddp	2020年前	无
风险识别	SAF	2020-02-27	无
游戏盾	Gameshield	2021-08-24	无
安全管家	Mssp	2021-08-24	无
应用身份服务（IDaaS）	IDaaS	2021-07-23	无
终端访问控制系统	UEM	2021-07-20	无
实人认证	Cloudauth	2021-07-13	无
云安全访问服务	CloudSecurityAccessService	2021-07-07	无
DDoS基础防护	DdosBasic	2022-05-09	无

大数据

云服务	云服务代码	支持时间	云服务事件支持情况说明
E-MapReduce	Emr	2020年前	无
Quick BI	quickbi	2020年前	无

云服务	云服务代码	支持时间	云服务事件支持情况说明
MaxCompute	MaxCompute	2020年前	MaxCompute支持被审计的事件说明
交互式分析	Hologram	2020年前	无
DataWorks	DataWorks	2020-07-21	无
阿里云Elasticsearch	ElasticSearch	2020-06-12	无
智能推荐	AIRec	2020-02-27	无
Databricks数据洞察	DDI	2020-09-22	无
实时计算Flink版	RealtimeCompute	2020-12-14	仅Flink全托管的管控事件可以通过操作审计控制台查询。 更多信息，请参见实时计算Flink版事件说明。
DataV数据可视化	DataV	2021-01-21	无
智能用户增长	QuickAudience	2021-06-22	无
数据湖构建	DataLake	2021-04-22	无
数据总线	DataHub	2021-07-29	无
数据资源平台	DRP	2021-12-10	无
图计算服务	IGraph	2022-02-22	无
个性化算法开发平台	TPP	2022-03-22	无

人工智能

云服务	云服务代码	支持时间	云服务事件支持情况说明
智能语音交互	nls-slp/nls-cloud-measure	2020年前	无
城市视觉智能引擎	CityVisual	2020-06-04	无
三维空间重建	TDSR	2021-03-30	三维空间重建事件说明
多媒体AI	MultimediaAI	2021-02-07	多媒体AI事件说明
智能视觉生产	IVPD	2021-06-22	无

云服务	云服务代码	支持时间	云服务事件支持情况说明
卫星及无人机遥感影像分析产品	Rsimganalys	2021-06-16	无
机器学习	PAI	2021-05-21	仅云原生深度学习训练PAI-DLC的管控事件可以通过操作审计控制台查询。
视觉计算服务	VCS	2021-05-10	无
视觉智能开放平台	VisualIntelligenceAPI	2021-04-28	仅人脸人体、目标检测的事件可以通过操作审计控制台查询。
图像搜索	ImageSearch	2020-10-13	无
基因分析平台	Genomics	2021-08-19	无
印刷文字识别	OCR	2021-08-19	无
优化求解器	OPT	2021-08-16	无
直播一体机	MindLive	2021-08-11	无
全息空间	Holowatcher	2021-08-04	无
交通云控平台	ETtraffic	2021-07-13	无
机器翻译	Alimt	2021-07-08	无
智能语义理解	IntelligentSemanticUnderstanding	2021-06-07	无
自然语言处理1.0	NLP	2021-09-09	无
自然语言处理2.0	AliNLP	2021-09-09	无

容器和中间件

云服务	云服务代码	支持时间	云服务事件支持情况说明
全局事务服务	GTS	2021-06-15	仅全局事务服务GTS的售卖事件可以通过操作审计控制台查询。
消息服务	MNS	2021-05-20	无
服务网格	ServiceMesh	2021-04-28	无
企业级分布式应用服务	EDAS	2021-08-16	无
云服务总线CSB	CSB	2021-07-07	无

云服务	云服务代码	支持时间	云服务事件支持情况说明
云原生应用交付平台	ADP	2021-09-28	无

物联网

云服务	云服务代码	支持时间	云服务事件支持情况说明
阿里云物联网平台	Iot	2020年前	无
视频边缘智能服务	LinkVisual	2020-09-02	无
物联网络管理平台	LinkWAN	2021-06-17	无
智联车管理云平台	IoVCommandCenter	2021-06-07	无
IoT设备身份认证	Iotid	2021-08-16	无
物联网无线连接服务	Dyiot	2021-07-22	无

管理与监控

云服务	云服务代码	支持时间	云服务事件支持情况说明
云监控	Cms	2020年前	无
访问控制	Ram	2020年前	无
身份管理服务	Ims	2020年前	无
云账号登录服务	AasCustomer	2020年前	无
RAM用户登录服务	AasSub	2020年前	无
安全令牌	Sts	2020年前	无
资源管理	ResourceManager	2020年前	无
操作审计	Actiontrail	2020年前	操作审计支持被审计的事件说明
配置审计	Config	2020-07-21	无
资源编排	ROS	2020年前	资源编排事件说明
密钥管理服务	Kms	2020年前	无

会员服务

云服务	云服务代码	支持时间	云服务事件支持情况说明
费用中心API	BssOpenApi	2020年前	无

ET大脑

云服务	云服务代码	支持时间	云服务事件支持情况说明
工业大脑开放平台	BrainIndustrial	2020-09-16	无

数字金融

云服务	云服务代码	支持时间	云服务事件支持情况说明
移动开发平台mPaaS	MobilePaaS	2020-12-18	移动开发平台mPaaS事件说明
金融分布式架构	SOFA	2021-08-24	仅金融分布式架构的售卖事件可以通过操作审计控制台查询。
蚂蚁隐私计算服务平台	ANTPPC	2021-12-16	无

开发与运维

云服务	云服务代码	支持时间	云服务事件支持情况说明
应用高可用服务	AHAS	2021-03-29	无
移动研发平台-移动推送	Push	2021-06-25	无
移动研发平台-HTTPDNS	HTTPDNS	2021-05-06	操作审计日志
移动研发平台-移动监控	AppMonitor	2021-12-15	无
移动研发平台	EMAS	2021-06-13	移动研发平台事件说明
链路追踪	Tracing	2021-06-10	无
逻辑编排	LC	2021-06-03	无
异地多活	MSHA	2021-04-07	无
小程序云	MiniProgramCloud	2021-08-30	无
GOC应急管控平台	GEMP	2021-08-27	无
云SSO	CloudSSO	2021-08-19	无
应用实时监控服务	ARMS	2021-08-19	无
移动数据分析	QuickAnalyticsPlus	2021-07-30	仅移动数据分析的售卖事件可以通过操作审计控制台查询。
移动研发平台-移动热修复	MobileHotfix	2021-07-30	无

云服务	云服务代码	支持时间	云服务事件支持情况说明
云速搭	BPStudio	2021-08-04	无
智能顾问	Advisor	2021-07-21	无
云效	RDC	2021-07-14	无
移动研发平台-移动测试	MQC	2022-02-24	无
云治理中心	Governance	2021-05-31	无
服务目录	ServiceCatalog	2022-05-18	无

企业应用与服务

云服务	云服务代码	支持时间	云服务事件支持情况说明
智能外呼机器人	OutboundBot	2021-03-25	智能外呼机器人事件说明
云呼叫中心	CloudCallCenter	2021-01-26	云呼叫中心事件说明
智能联络中心	AICCS	2021-06-25	无
货架商品识别与管理	RetailImageRecognition	2021-06-24	无
云价签	CloudESL	2021-06-15	无
智能双录质检	Idrsservice	2021-06-08	无
Teambition	Teambition	2021-08-19	无
智能数据助理	Databot	2021-08-16	无
客服工作台	CCS	2021-08-19	无
云通信网络加速	Snsu	2021-08-16	无
云投屏	CD	2021-07-30	仅云投屏的售卖事件可以通过操作审计控制台查询。
新零售智能助理	Retailbot	2021-08-12	无
云行情	Assettech	2021-08-04	无
BizWorks	BizWorks	2021-07-29	无
邮件推送	DirectMail	2021-07-27	无
地址标准化	AddressPurification	2021-07-27	地址标准化支持被审计的事件说明

云服务	云服务代码	支持时间	云服务事件支持情况说明
号码百科	DYTNS	2021-07-20	无
智能对话机器人	Chatbot	2021-07-13	无
智能对话分析	SmartConversationAnalysis	2021-07-07	无
阿里邮箱	Alimail	2021-06-24	无
GTS专家服务	HealthCheckService	2021-10-09	无
Linkedmall企业商城	Linkedmall	2021-12-25	无
阿里云消息中心订阅管理	MscSub	2022-05-12	无
5G互联平台	XGIP	2022-06-21	无

工商财税与知识产权

云服务	云服务代码	支持时间	云服务事件支持情况说明
工商财税	CompanyReg	2021-08-16	无
商标服务	Trademark	2021-08-16	无
图片与设计	Premiumpics	2021-07-23	无
智能设计	AIDesign	2021-07-22	无
版权与专利服务	Copyright	2021-08-04	无

API与工具

云服务	云服务代码	支持时间	云服务事件支持情况说明
工单系统	Workorder	2021-08-05	无

特殊云服务事件说明

操作审计支持的部分云服务比较特殊，例如：账号事件和一些包含数据操作的云服务。下表中主要针对此类云服务给出明确的支持和不支持的事件列表。不支持的事件一般为数据事件，例如：OSS Bucket中的文件上传和下载。

云服务或事件类型	支持的事件	不支持的事件
账号事件	• 阿里云账号（主账号）登录异常 • 阿里云账号（主账号）重置密码	不涉及
	OSS Bucket管控事件，具体如下： • DeleteBucket	

云服务或事件类型	支持的事件	不支持的事件
对象存储OSS	• DeleteBucketCors • DeleteBucketEncryption • DeleteBucketEventNotification • DeleteBucketInventory • DeleteBucketLifecycle • DeleteBucketLog • DeleteBucketNotification • DeleteBucketPolicy • DeleteBucketQoSInfo • DeleteBucketReplication • DeleteBucketTagging • DeleteBucketWebSite • DeleteBucketWebSite • GetBucketAcl • GetBucketCors • GetBucketEncryption • GetBucketEventNotification • GetBucketInfo • GetBucketInventory • GetBucketLifecycle • GetBucketLocation • GetBucketLog • GetBucketMimeType • GetBucketNotification • GetBucketPolicy • GetBucketQoSInfo • GetBucketReferer • GetBucketReplication • GetBucketReplicationLocation • GetBucketReplicationProgress • GetBucketRequestPayment • GetBucketStat • GetBucketTagging • GetBucketTransferAcceleration • GetBucketUserQos • GetBucketVersioning • GetBucketVersions • GetBucketWebSite • GetBucketWorm • PutBucket • PutBucketCors • PutBucketEncryption • PutBucketEventNotification • PutBucketHash	Object和Live Channel相关事件。以下为部分典型事件： • PutObject • GetObject • CopyObject • AppendObject • DeleteObject • DeleteMultipleObjects • PutObjectACL • GetObjectACL • PutObjectTagging • GetObjectTagging • DeleteObjectTagging • PutLiveChannelStatus • PutLiveChannel • GetVodPlaylist • PostVodPlaylist • GetLiveChannelStat • GetLiveChannelInfo • GetLiveChannelHistory • ListLiveChannel • DeleteLiveChannel

云服务或事件类型	支持的事件	不支持的事件
	• PutBucketInventory • PutBucketLifecycle • PutBucketLog • PutBucketNotification • PutBucketPolicy • PutBucketQoSInfo • PutBucketReferer • PutBucketReplication • PutBucketRequestPayment • PutBucketTagging • PutBucketTransferAcceleration • PutBucketUserQos • PutBucketVersioning • PutBucketWebSite	
日志服务SLS	管控事件，支持的地域如下： • 华东1（上海） • 西南1（成都） • 新加坡 • 英国（伦敦） • 德国（法兰克福） • 印度尼西亚（雅加达） • 马来西亚（吉隆坡） • 澳大利亚（悉尼） • 美国（硅谷） • 美国（弗吉尼亚） • 阿联酋（迪拜） • 日本（东京）	以下为部分典型事件： • GetProjectLogs • GetLogs • GetHistograms • GetCursor • ListShards • MergeShards • PutLogs • PullLogs • CreateAlert • UpdateAlert • DeleteAlert • GetAlert • ListAlert
开放搜索OpenSearch	管控事件。 关于管控事件的更多信息，请参见管控API参考。	流量事件。 关于流量事件的更多信息，请参见流量API参考。
消息队列RocketMQ	管控事件。	通过AccessKey调用SDK收发消息。

云服务或事件类型	支持的事件	不支持的事件
表格存储OTS	管控事件。	以下为部分典型事件： • GetRow • PutRow • UpdateRow • DeleteRow • GetRange • BatchGetRow • BatchWriteRow • CreateTable • ListTable • DeleteTable • UpdateTable • DescribeTable • CreateIndex • DeleteIndex
消息服务MNS	管控事件。	以下为部分典型事件： • SendMessage • BatchSendMessage • ReceiveMessage • BatchReceiveMessage • DeleteMessage • BatchDeleteMessage • PeekMessage • BatchPeekMessage • ChangeMessageVisibility • SetSubscriptionAttributes • GetSubscriptionAttributes • PublishMessage
MaxCompute	管控事件和数据事件。	由于MaxCompute审计事件没有记录AccessKey信息，因此无法通过AccessKey搜索事件。

5.支持的地域

本文介绍操作审计支持的地域。

公共云

- 华东1（杭州）
- 华东2（上海）
- 华北1（青岛）
- 华北2（北京）
- 华北3（张家口）
- 华北5（呼和浩特）
- 华北6（乌兰察布）
- 华南1（深圳）
- 华南2（河源）
- 华南3（广州）
- 西南1（成都）
- 中国（香港）
- 新加坡
- 澳大利亚（悉尼）
- 韩国（首尔）
- 马来西亚（吉隆坡）
- 印度尼西亚（雅加达）
- 日本（东京）
- 泰国（曼谷）
- 印度（孟买）
- 德国（法兰克福）
- 英国（伦敦）
- 美国（硅谷）
- 美国（弗吉尼亚）
- 阿联酋（迪拜）

> **说明** 韩国（首尔）、泰国（曼谷）暂不支持事件告警和历史事件投递任务功能。

金融云

目前，操作审计只支持部署在“华东2金融云（上海）”，金融云所有地域的审计事件都可以在“华东2金融云（上海）”的控制台查询。

- 华东1金融云（杭州）
- 华东2金融云（上海）
- 华南1金融云（深圳）
- 华北1金融云（青岛）

> **说明** 金融云的所有全局事件都会被默认记录为“华东1金融云（杭州）”的操作事件。

政务云

目前，操作审计只支持部署在“华北2阿里政务云1（北京）”，阿里政务云的审计事件会被投递至“华北2阿里政务云1（北京）”。

- 阿里政务云
- 华北2阿里政务云1（北京）

> **说明** 政务云的所有全局事件都会被默认记录为杭州地域的操作事件。

6.单账号跟踪、多账号跟踪和平台事件跟踪的差异

操作审计支持单账号跟踪、多账号跟踪和平台事件跟踪，您可以根据所需进行选择。

单账号跟踪、多账号跟踪和平台事件跟踪的差异如下表所示。

差异项	单账号跟踪	多账号跟踪	平台事件跟踪
场景	个人用户需要投递事件到日志服务SLS或对象存储OSS时，可以创建单账号跟踪。 通过创建多个单账号跟踪，可以实现以下需求： • 不同角色审计不同范围的事件。 • 合规管理多地域的审计数据。 • 为事件创建多个副本备份。	企业用户（开通了资源目录的企业）需要将资源目录内的所有成员的事件投递到日志服务SLS或对象存储OSS时，可以创建多账号跟踪。	个人用户需要将阿里云运维团队针对用户服务的维护操作所产生的事件投递到日志服务SLS时，可以创建平台事件跟踪。
开通方式	阿里云账号登录即可使用，免开通。	当企业开通了资源目录并在资源目录中创建了组织结构后，管理账号可以在操作审计中创建多账号跟踪。	提交工单或向销售经理申请白名单。
支持的云服务	支持操作审计的云服务	支持操作审计的云服务	密钥管理服务KMS、数据安全中心DSC、对象存储OSS、云服务器ECS、云数据库RDS、容器服务Kubernetes版ACK、容器镜像服务ACR和E-MapReduce。
创建跟踪的账号	阿里云账号	管理账号	阿里云账号
投递的事件	个人用户通过阿里云控制台、OpenAPI、开发者工具访问和管控云上服务所产生的事件。	企业用户通过阿里云控制台、OpenAPI、开发者工具访问和管控云上服务所产生的事件。	阿里云运维团队针对用户服务的维护操作所产生的事件。
投递事件的范围	当前账号的事件	所有成员的事件	当前账号的平台事件
投递事件的存储空间	• 日志服务SLS • 对象存储OSS	• 日志服务SLS • 对象存储OSS	日志服务SLS

差异项	单账号跟踪	多账号跟踪	平台事件跟踪

事件查询方式	• 操作审计控制台
	• `LookupEvents` 接口
	• 对象存储控制台
	• 日志服务控制台
		• 管理账号：
		  ◦ 操作审计控制台
		  ◦ `LookupEvents` 接口
		• 成员：
		  ◦ 对象存储控制台
		  ◦ 日志服务控制台
			• 操作审计控制台
			• 日志服务控制台

创建的最大跟踪数目	每个地域5个	所有地域1个	所有地域1个
OSS存储空间存储路径	• 管控事件：`oss://<bucket>/<日志文件前缀>/AliyunLogs/Actiontrail/<region>/<年>/<月>/<日>/<日志文件>` • Insight事件：`oss://<bucket>/<日志文件前缀>/AliyunLogs/Actiontrail-Insight/<region>/<年>/<月>/<日>/<日志文件>` 说明 Insight事件需要申请才能使用。更多信息，请参见Insight事件概览。	`oss://<bucket>/<日志文件前缀>/AliyunLogs/Actiontrail/rd_id/accountid/regionid/yyyy/mm/dd/日志文件`	不涉及
SLS Logstore默认名称	`actiontrail_单账号跟踪名称`	`actiontrail_多账号跟踪名称`	`innertrail_平台事件跟踪名称`