ALIBABA CLOUD

Alibaba Cloud

操作审计

产品简介

文档版本：20200821

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

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或OSS存储空间，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天的操作记录，支持您在线查阅。
- 自主管理：通过创建跟踪，操作审计可以将操作记录保存到日志服务（日志的形式）或OSS存储空间（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历史操作事件。

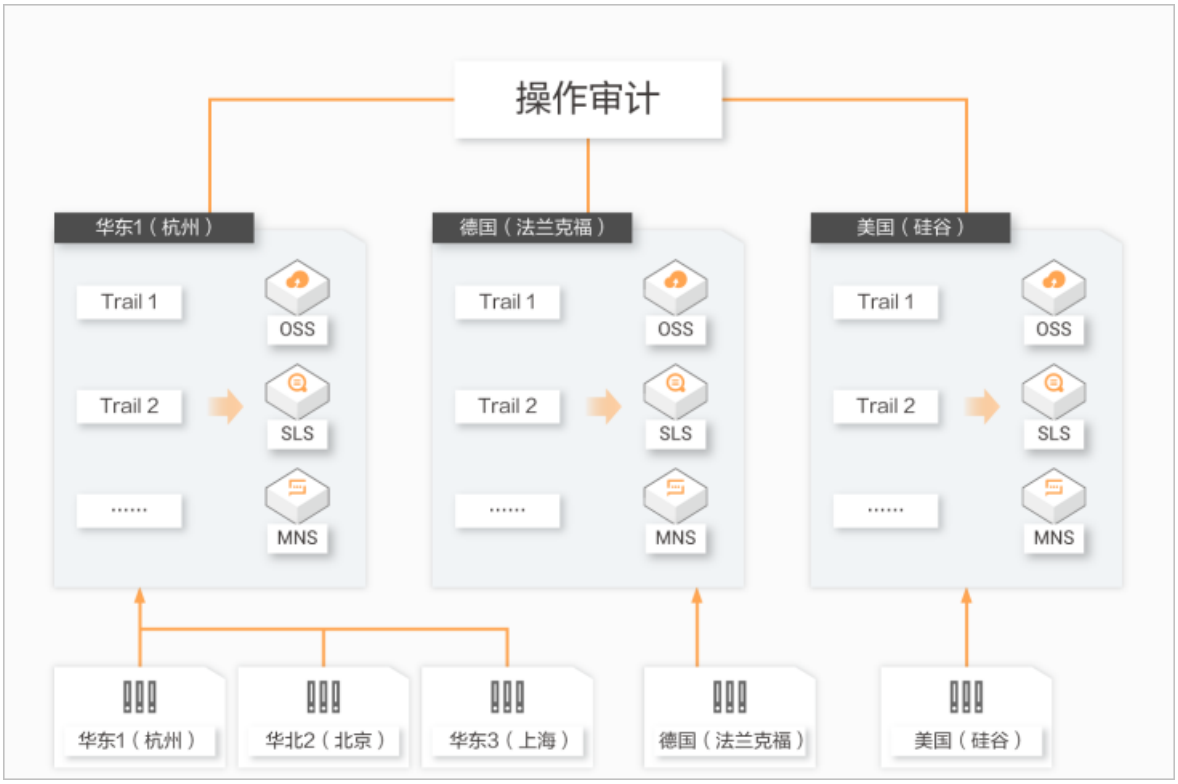
应用场景

- 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，通过这些操作记录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SLS Logstore，做更长时间的保存和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，而且您已经使用了阿里云访问控制（RAM）服务来管理这些成员，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操作记录。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操作记录（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）。操作记录会在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天的操作记录。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：操作审计支持将操作记录投递到阿里云对象存储（OSS）或日志服务（Log Service）等存储产品中，这些存储产品具有极高的可用性，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：您最多可以在每个区域创建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
阿里云账号	阿里云账号是主账号，在操作事件中记录为 `root-account` 。
RAM用户	RAM用户是子账号，在操作事件中记录为 `ram-user` 。
企业管理账号	企业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账号拥有完全控制权限。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企业管理账号。
成员账号	成员账号是阿里云账号在资源目录中的一种称呼。在资源目录内，成员账号作为资源容器，是一种资源分组单位。成员账号通常用于指代一个项目或应用，每个成员账号中的资源相对其他成员账号中的资源是物理隔离的。 成员账号被企业管理账号邀请进入资源目录，或由企业管理账号在资源目录内直接创建。
操作事件	操作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。操作事件包含时间、人员、资源、操作类型、操作结果、来源IP等信息。
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操作事件。在操作审计控制台的**历史事件查询**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 Bucket时，全局事件与跟踪的HomeRegion事件放在同一个目录下。
跟踪	通过设置跟踪将日志保存到指定的OSS Bucket和SLS Logstore下，便于进一步分析和归档。根据创建者和作用范围的不同分为单账号跟踪和多账号跟踪。
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操作日志的跟踪。
多账号跟踪	多账号跟踪是企业管理账号创建的用于记录所有成员账号操作日志的跟踪。多账号跟踪会把所有成员账号的操作日志投递到多账号跟踪设置的OSS Bucket或SLS Logstore中。
Home地域	Home地域是发起创建跟踪操作的地区或区域。

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操作事件，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日志，这种跟踪叫做影子跟踪。影子跟踪只能查看，不能管理。

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
一个用户允许创建的跟踪数目	每个地域5个
一个跟踪允许配置的OSS 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 Bucket中访问数据	10分钟
用户通过控制台或API能查询多久的操作记录	90天
保存到OSS Bucket中文件对象（压缩后）的大小	2KB

4.支持操作审计的地域

本文介绍支持操作审计的地域。

公共云

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

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。

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。

5.支持操作审计的云服务及事件

本文介绍支持操作审计的云服务及事件。

弹性计算

服务名称	服务代码
云服务器ECS	Ecs
弹性伸缩	Ess
容器服务	CS
容器镜像服务	cr
轻量应用服务器	SWAS
批量计算	BatchCompute
弹性高性能计算E-HPC	EHPC
Web应用托管服务	WebPlus
弹性容器实例ECI	Eci

存储

服务名称	服务代码
文件存储	NAS
对象存储OSS 说明 仅OSS Bucket管控事件支持操作审计。具体事件请参见事件。	Oss
智能媒体管理	IMM

数据库

服务名称	服务代码
云数据库RDS版	Rds
数据传输服务DTS	Dts
HybridDBforPostgreSQL	gpdb
云数据库Redis版	R-kvstore

服务名称	服务代码
分布式关系型数据库服务	Drds
云数据库MongoDB版	Dds
表格存储	Ots
云原生数据仓库AnalyticDB MySQL版	ADS
云数据库HBase	HBase

网络

服务名称	服务代码
专有网络VPC	Vpc
NAT网关	Vpc
弹性公网IP	Vpc
高速通道	Vpc
全球加速	Vpc
云企业网	Cen
负载均衡	Slb
智能接入网关	Smartag
PrivateLink	Privatelink

视频与CDN

服务名称	服务代码
CDN	Cdn
视频点播	vod
视频直播	live
媒体处理	Mts
全站加速	DCDN
边缘节点服务ENS	ENS

域名与网站（万网）

服务名称	服务代码
域名	Domain/Domain-intl
云解析DNS	Alidns

应用服务

服务名称	服务代码
API网关	CloudAPI
区块链服务	Baas

互联网中间件

服务名称	服务代码
消息队列RocketMQ	Ons
消息队列Kafka版	AliKafka
应用配置管理ACM	ACM

云通信

服务名称	服务代码
短信服务	Dysms
短信服务API	Dysmsapi

安全

服务名称	服务代码
DDoS高防（国际）	ddosdip
DDoS高防（新BGP）	ddoscoo
Web应用防火墙	Waf
Web应用防火墙API	waf-openapi
安骑士	aegis
云防火墙	Cloudfw

服务名称	服务代码
网站威胁扫描系统	avds
SSL证书	cas
云安全中心	Sas
内容安全	Green
风险识别	SAF

大数据

服务名称	服务代码
E-MapReduce	Emr
QuickBI	quickbi
DataWorks	DataWorks
阿里云Elasticsearch	ElasticSearch

物联网

服务名称	服务代码
阿里云物联网平台	IoT

管理与监控

服务名称	服务代码
云监控	Cms
访问控制	Ram
身份管理服务	Ims
账号登录服务	Aas
云账号登录服务	AasCustomer
RAM用户登录服务	AasSub
安全令牌	Sts
资源管理	ResourceManager
操作审计	Actiontrail

服务名称	服务代码
配置审计	Config
资源编排	ROS
密钥管理服务	Kms

会员服务

服务名称	服务代码
费用中心API	BssOpenApi

事件

事件类型	事件名称
账号事件	• 主账号登录异常 • 主账号重置密码
	• DeleteBucket • DeleteBucketCors • DeleteBucketEncryption • DeleteBucketEventNotification • DeleteBucketInventory • DeleteBucketLifecycle • DeleteBucketLog • DeleteBucketNotification • DeleteBucketPolicy • DeleteBucketQoSInfo • DeleteBucketReplication • DeleteBucketTagging • DeleteBucketWebSite • DeleteBucketWebSite • GetBucketAcl • GetBucketCors • GetBucketEncryption • GetBucketEventNotification • GetBucketInfo • GetBucketInventory • GetBucketLifecycle • GetBucketLocation • GetBucketLog • GetBucketMimeType

事件类型	事件名称
OSS Bucket管控事件	• GetBucketNotification • GetBucketPolicy • GetBucketQoSInfo • GetBucketReferer • GetBucketReplication • GetBucketReplicationLocation • GetBucketReplicationProgress • GetBucketRequestPayment • GetBucketStat • GetBucketTagging • GetBucketTransferAcceleration • GetBucketUserQos • GetBucketVersioning • GetBucketVersions • GetBucketWebSite • GetBucketWorm • PutBucket • PutBucketCors • PutBucketEncryption • PutBucketEventNotification • PutBucketHash • PutBucketInventory • PutBucketLifecycle • PutBucketLog • PutBucketNotification • PutBucketPolicy • PutBucketQoSInfo • PutBucketReferer • PutBucketReplication • PutBucketRequestPayment • PutBucketTagging • PutBucketTransferAcceleration • PutBucketUserQos • PutBucketVersioning • PutBucketWebSite