操作审计

产品简介

产品简介

产品概述

操作审计(ActionTrail)会记录您的云账户资源操作，提供操作记录查询，并可以将审计事件保存到您指定的日志服务Logstore或者OSS存储空间。通过ActionTrail保存的所有操作记录，您可以实现安全分析、资源变更追踪以及合规性审计。

ActionTrail收集云服务的API调用记录（包括用户通过控制台触发的API调用记录），规格化处理后将操作记录以日志的形式保存到指定的日志服务Logstore中，或者以文件形式保存到指定的OSS存储空间。用户可以使用存储产品丰富的管理功能来管理这些审计数据，比如授权、开启生命周期管理、归档管理、检索、分析、报警等。

一般情况下，当用户通过控制台或SDK发起操作调用之后，ActionTrail会在十分钟内传送操作记录到用户指定的存储产品中。用户可以通过ActionTrail控制台或API来查看最近30天的操作记录，也可以投递到存储产品中，以便审计数据保存更长时间和做更丰富的数据分析。

功能描述

开箱即用

“历史事件”功能无需配置即可收集最近三十天的操作记录，并且支持从操作时段、用户名、资源类型、资源名称、操作名称等维度来查询操作事件。

自主管理事件

通过创建“跟踪”，ActionTrail可以持续将操作记录投递到您指定的存储产品中。您可以通过存储产品自身的分析功能来分析数据，也可以通过阿里云丰富的大数据产品来分析数据。

多维查询事件

ActionTrail支持将操作记录投递到日志服务中，利用日志服务强大的检索能力，您可以方便地分析审计数据。通过设置报警，您可以监控自己关注的操作。

关于费用

使用ActionTrail不需要用户付费，但用户需要为ActionTrail所使用的日志服务和OSS存储付费。

名词解释

术语	中文	说明
Account	云账户	这里是指主账户，有时称为root-account
RAM-User	RAM用户	这里是指RAM中的一个用户
AK (Access Key)	访问密钥	访问密钥由AccessKeyID和AccessKeySecret组成，用于云服务API请求的身份认证
Event	操作事件	用户通过阿里云控制台或SDK发起的API操作都可能触发一个事件
Global Service	全局服务	并不做区域化部署的服务，比如RAM。全局服务会产出全局服务事件。
Trail	跟踪	Trail帮助用户将审计数据保存到指定的OSS桶中
Home Region	家区域	发起创建Trail操作的区域
Shadow Trail	影子跟踪	创建跟踪时，会同时在支持的区域创建的跟踪。

产品优势

快速推送

ActionTrail 利用高可用数据处理管道进行事件收集、处理和传送。ActionTrail 一般会在用户操作发生后10分钟内完成事件处理。

高清记录

ActionTrail 会清晰记录用户操作上下文信息。比如，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？这些都会有详细的记录。

稳定可靠

ActionTrail 支持使用OSS来保存操作记录，经济可靠。您可以使用 OSS 生命周期配置规则降低存储成本，也可以使用 OSS 授权机制将记录文件授权他人访问。

使用场景

安全分析

当您的云账号或资源存在安全问题时，ActionTrail所记录的日志将能帮助您分析原因。比如，ActionTrail会记录您的所有账号登录操作，何时、从哪个IP、是否使用多因素认证登录，这些都有详细记录，通过这些记录您可以判断您的账号是否存在安全问题。

资源变更追踪

当您的资源出现异常变更时，ActionTrail所记录的操作日志将能帮助您找到原因。比如，当您发现一台ECS实例停机了，您可以通过ActionTrail找到是谁、何时、从哪个IP发起的停机操作。

合规性审计

如果您的组织有多个成员，而且您已经使用阿里云的RAM服务来管理这些成员的身份，那么为了满足您所在组织的合规性审计需要，您需要获取每个成员的详细操作记录。ActionTrail所记录的操作事件将能满足这种合规性审计需求。