目录

产品概述

产品简介

操作审计(Action Trail)提供金山云账号操作的历史记录，这些记录包括通过金山云管理控制台、API服务或其他金山云云服务执行的操作。您可以通过操作审计服务对金山云账号进行监控、合规性检查、操作审核和风险审核。

工作原理

在您创建金山云账号后，操作审计服务将自动开通。当您的金山云账号中发生活动，改活动将被记录在操作审计的事件中。

通过**历史事件查询**，您可以查看、检索金山云账号过去30天内发生的活动。同时您可以创建事件跟踪，以便审计数据保存更长时间和做更丰富的数据分析。事件跟踪是一种配置，可以将事件传输到您指定的KS3存储空间中。

产品优势

安全性分析和故障排除

用户注册金山云账号后，可通过控制台或API登录金山云Action Trail服务查看您账号下的操作事件。借助Action Trail，您可以通过捕捉特定时段内您的金山云账户所发生更改的全面历史记录，发现并解决安全性和操作性问题。

合规性审计

Action Trail可以自动记录和存储金山云账户中已执行操作的事件日志，从而简化合规性的审核过程，也可以更方便地搜索所有日志数据、识别不合规事件、加快事故调查速度并加快响应审核员请求的速度。

用户与资源活动的可见性

Action Trail会清晰记录用户操作上下文信息。比如谁在什么时刻、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。

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。一般会在用户操作发生后10分钟内完成事件处理。

使用场景

安全分析

当您的云账号或资源存在安全问题时，Action Trail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，Action Trail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KEC实例停机了，您可以通过Action Trail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，而且您已经使用金山云的IAM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。Action Trail所记录的操作事件将能满足这种合规性审计需求。