

为了无法计算的价值 | []阿里云

快速入门

创建跟踪

前提条件

目前操作审计仍处于公测阶段,您需要打开操作审计产品页面,点击获取使用资格,才可以在阿里云控制台上使用操作审计。

创建跟踪

登录ActionTrail控制台。

在左侧导航栏中,点击跟踪列表。

选择您想创建	跟踪的区域,	,点击 创建跟踪 。ù	亥区域将成为这条跟踪的	Home	Region.
ActionTrail控制台	跟踪列表 华东1 亚	友东北 1 (东京)		♀刷新	创建跟踪
历史事件查询	操作日志将会存储在您的OSS中,您可以在此设置文件存储位置及文件名称前缀等信息。				
跟踪列表		COME I MANO			
	跟踪名称	OSS Bucket名称	跟踪状态	操作	
Ξ		① 没有:	查询到符合条件的记录		■ 答询,
					建议

输入**跟踪名称**。

选择**是否创建新的OSS Bucket**。

- i. 选择是,在OSS Bucket文本框,输入一个名称。
- ii. 选择否,点击OSS Bucket,会出现可供选择的Bucket列表。

ActionTrail控制台	创建跟踪 💿	
历史事件查询	* 跟踪名称	default
跟踪列表	是否创建新的OSS Bucket?	● 是 ○ 否
	* OSS Bucket	secloud
	日志文件前缀	trail1
-	是否开启日志记录	
		提交 清除

滑动滑块以开启日志记录。

如果这是您首次创建跟踪,点击提交后,会提示授权ActionTrail访问OSS的权限。

云资源访问授权					
昌馨提示:如需修改角色权限,请前往RAM控制台 <mark>角色管理</mark> 中设置,需要注意的是,错误的配置可能导致ActionTrail无法获取到必要的权限。	×				
ActionTrail请求获取访问您云资源的权限 下方是系统创建的可供 ActionTrail 使用的角色,授权后,ActionTrail 拥有对您云资源相应的访问权限。					
AliyunActionTrailDefaultRole					
描述: ActionTrail默认使用此角色来访问您在其他云产品中的资源					
权限描述:用于ActionTrail服务默认角色的授权策略,包括OSS的对象列出及写入权限					

点击 **同意授权**。

创建ActionTrail之后,您仍然可以通过ActionTrail控制台来修改OSS Bucket。修改Bucket之后的操作记录将保存在新的OSS Bucket。

(•)	管理控制台 产品与服务	-				
	ActionTrail控制台	★ 返回				
	历史事件查询					
	跟踪列表	關時名称 at0312				
4		是否创建新的OSS Bucket ? 🛛 🔘 是 🖲 否				
Ø		* OSS Burket tastualuma				
۲						
*		日志文件前缀 at0312				
₿						
co		保存修改				
-	=					

说明: OSS存储路径格式

oss://<bucket>/<日志文件前缀>/AliyunLogs/Actiontrail/<region>/<年>/<月>/<日>/<日志数据文件 >

比如,保存在oss的一个存储文件路径如下。

oss://mybucket/auditing/AliyunLogs/ActionTrail/cn-hangzhou/2015/12/16/xxx.gz

操作日志是以压缩格式保存到OSS Bucket中。一个压缩文件的大小不超过2KB,它是一个 json格式的操作记录列表。 您可以通过E-MapReduce服务来分析保存在OSS中的操作记录,也可以自行授权第三方日志分

析服务来进行操作记录的分析。



您可以使用ActionTrail控制台更新跟踪。

登录ActionTrail控制台。

在左侧导航窗格中,单击跟踪列表,然后单击要更新的跟踪的名称。

在刷新的页面上,更新此跟踪的参数设置。

单击保存修改。

关闭跟踪的日志记录

本文介绍如何关闭跟踪的日志记录。

登录 ActionTrail 控制台。

在左侧导航窗格中,选择跟踪列表,然后选择要配置的跟踪。

在配置页面右上角,向左移动滑块关闭该跟踪的日志记录。

单击**保存修改**。

历史事件查询

登录ActionTrail控制台。

点击左侧导航栏中的历史事件查询,将可以看到最近30天的操作记录。

单击每行操作记录,可以展开该记录的详细信息。

您还可以使用过滤器来查询操作日志。过滤器支持对"用户名"、"事件名称"、"资源类型"、 "资源名称",以及"时间范围"进行条件过滤查询。

说明: 全局服务的事件可在所有区域的历史事件中查询。