

为了无法计算的价值 | []阿里云

快速入门

创建Trail

进入阿里云 (www.aliyun.com),可以在产品列表中找到操作审计(ActionTrail)产品,然后申请开通。

首先选择您想创建Trail的区域,该区域将成为Trail的Home Region。



接着对Trail做具体的配置。由于ActionTrail会将日志保存到您的OSS存储中,所以创建Trail时,您需要开通OSS服务,并且授权ActionTrail服务能操作您的OSS存储空间。

ActionTrail控制台	创建跟踪 🔹 返回	
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

授权ActionTrail服务操作您的OSS存储空间

当首次创建ActionTrail时,如果您没有给ActionTrail服务授权操作OSS,那么会要求您授权。

云资源访问授权								
温馨提示:如图修改角色权限,请前往RAM控制台 角色管理 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。 ×							
AstionTesthint分割你二次流动的你问								
ACTION I Fail 语 水 获 联 切 问 認 云 資 源 的 化 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								
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								
权限描述:用于ActionTral服务默认角色的授权策略,包括OSS的对象列出及写入权限								

您需要单击 同意授权, 否则ActionTrail没有操作您OSS的权限。

修改ActionTrail的配置

创建ActionTrail之后,您仍然可以通过ActionTrail控制台来修改OSS Bucket名称。修改Bucket之后,新的操作记录将写入新的OSS Bucket。

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。





打开ActionTrail控制台,进入"历史事件查询",将可以看到最近7天的操作记录。

ActionTrail控制台		历史事件查询								€ 刷新				
历史事件查询		查找过去7天内您的云账户中与创建、修改和删除资源相关的操作。												
设置		过滤器:	用户名	\$		B	时间: 20	15-12-30	3	至	2016-01-05	搜索		
			事件时间		用户名	事件名称	欲		资源类型		资源名称		错误码	
		•	2016-01-05 1	4:07:08	zhangsan	AttachP	PolicyToUs	er	Policy 等 2 个		AdministratorAccess 等 2 1	`	NoPermission	
		•	2016-01-05 1	4:06:49	zhangsan	DetachP	PolicyFron	nUser	Policy 等 2 个		AliyunRAMFullAccess 等 2	ŕ		
	-	•	2016-01-05 1	4:05:59	zhangsan	AddUse	erToGroup		Group 等 2 个		grp2 等 2 个			
		•	2016-01-05 1	4:05:35	zhangsan	CreateU	Jser		User		lisi			
		•	2016-01-05 1	4:04:56	root	CreateU	Jser		User		zhangsan		EntityAlreadyExis	ts.User
		•	2016-01-05 1	4:04:33	root	CreateU	Jser		User		admin			
		•	2016-01-05 1	4:04:47	root	DeleteU:	lser		User		admin			
		•	2016-01-05 1	4:04:15	root	AttachP	olicyToGr	oup	Group 等 2 个		grp2 等 2 个			
		•	2016-01-05 1	4:03:58	root	CreateG	Group		Group		grp2			

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。

有一点值得注意,全局服务的事件将会冗余到所有区域的历史事件中,便于分析和排查问题。