

操作审计

快速入门

快速入门

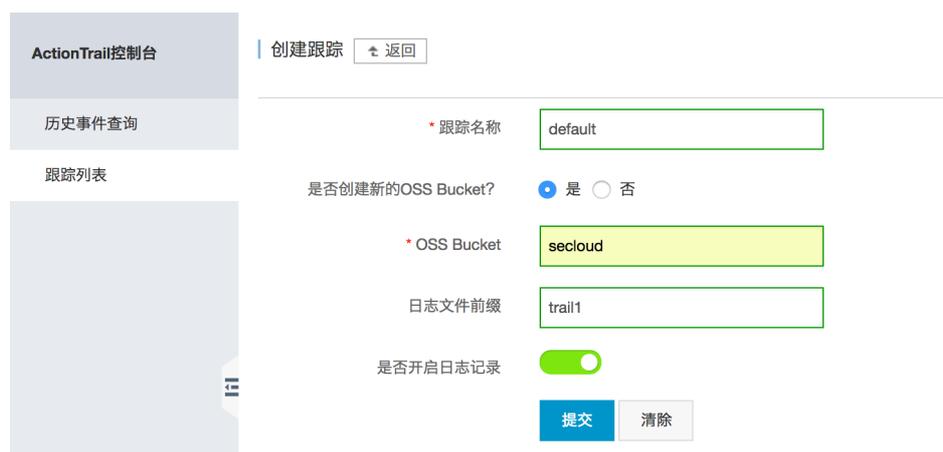
创建Trail

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。



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。



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
```

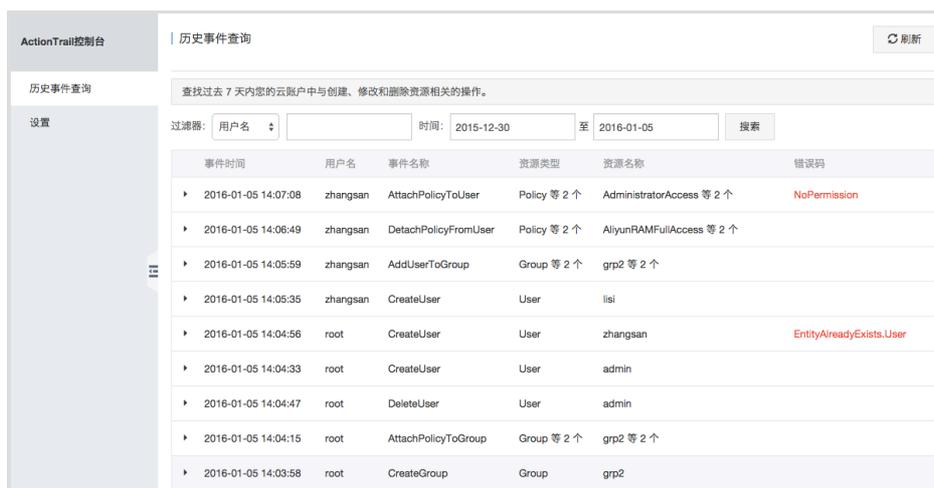
操作日志是以压缩格式保存到OSS Bucket中。一个压缩文件的大小不超过2KB, 它是一个json格式的操作记录列表。

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。

查看操作事件

查看历史操作事件

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。



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。

过滤器: 用户名: [] 时间: 2015-12-30 至 2016-01-05 搜索

事件时间	用户名	事件名称	资源类型	资源名称	错误码
2016-01-05 14:07:08	zhangsan	AttachPolicyToUser	Policy 等 2 个	AdministratorAccess 等 2 个	NoPermission
2016-01-05 14:06:49	zhangsan	DetachPolicyFromUser	Policy 等 2 个	AliyunRAMFullAccess 等 2 个	
2016-01-05 14:05:59	zhangsan	AddUserToGroup	Group 等 2 个	grp2 等 2 个	
2016-01-05 14:05:35	zhangsan	CreateUser	User	lisi	
2016-01-05 14:04:56	root	CreateUser	User	zhangsan	EntityAlreadyExists.User
2016-01-05 14:04:33	root	CreateUser	User	admin	
2016-01-05 14:04:47	root	DeleteUser	User	admin	
2016-01-05 14:04:15	root	AttachPolicyToGroup	Group 等 2 个	grp2 等 2 个	
2016-01-05 14:03:58	root	CreateGroup	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。