操作审计

快速入门

快速入门

创建跟踪

前提条件

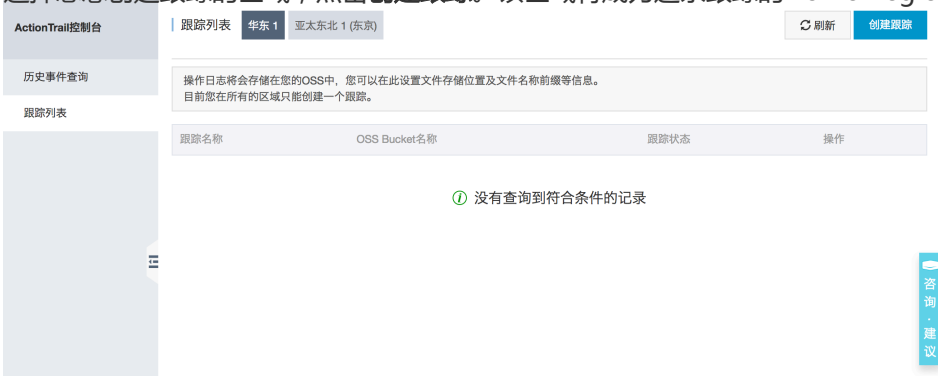
目前操作审计仍处于公测阶段，您需要打开**操作审计产品页面**，点击**获取使用资格**，才可以在阿里云控制台上使用操作审计。

创建跟踪

登录ActionTrail控制台。

在左侧导航栏中，点击**跟踪列表**。

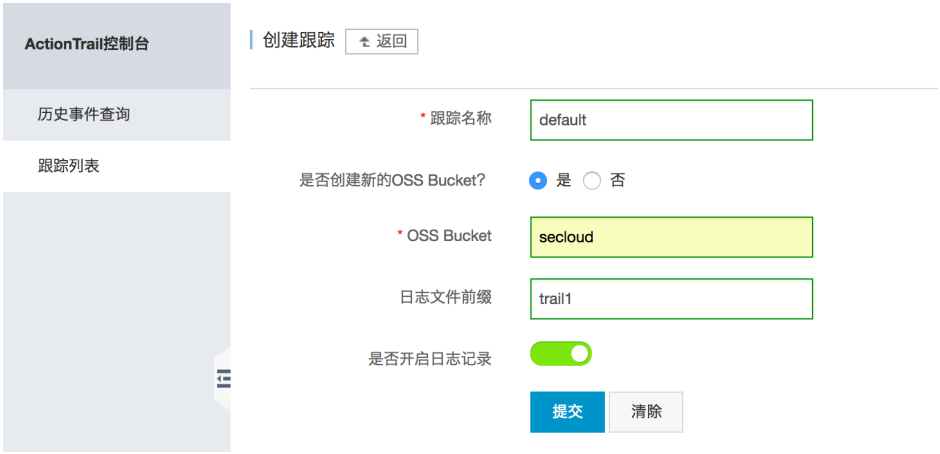
选择您想创建跟踪的区域，点击**创建跟踪**。该区域将成为这条跟踪的Home Region。



输入**跟踪名称**。

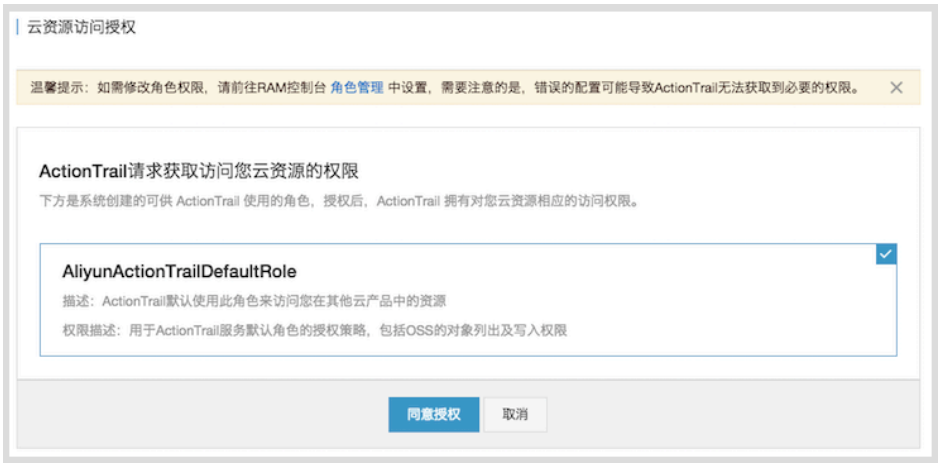
选择**是否创建新的OSS Bucket**。

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。



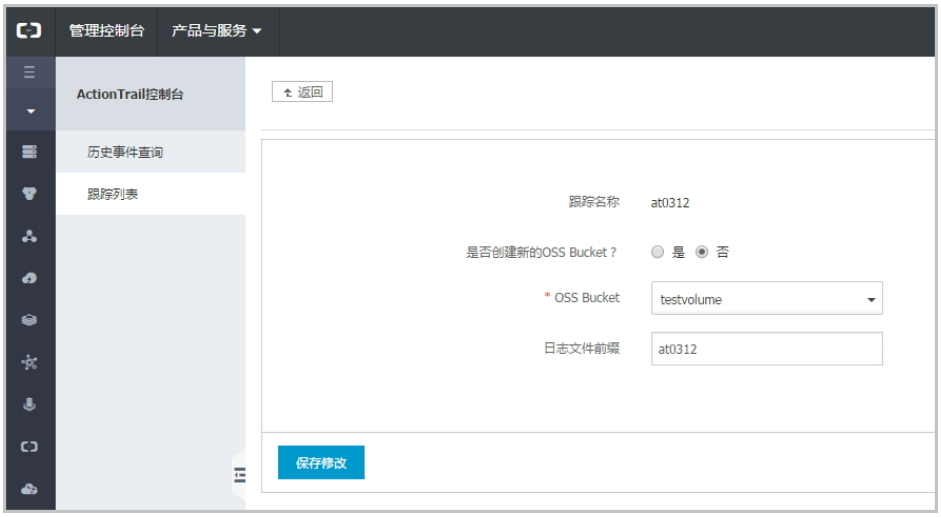
滑动滑块以开启日志记录。

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。



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。



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。

更新跟踪

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。