ALIBABA CLOUD

Alibaba Cloud

操作审计

快速入门

文档版本：

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

目录

1.创建单账号跟踪

本文为您介绍如何通过操作审计控制台创建单账号跟踪。创建单账号跟踪可以将操作日志投递到OSS Bucket或SLS Logstore中，以便对日志进行分析。如果未创建跟踪，操作审计控制台仅能查看近90天的操作日志。

操作步骤

1. 登录操作审计控制台。
2. 在顶部导航栏选择您想创建单账号跟踪的地域。

   > 说明 该地域将成为单账号跟踪的Home地域。

3. 在左侧导航栏，单击**操作审计 > 跟踪列表**。
4. 单击**创建跟踪**，输入**跟踪名称**。
5. 根据需要选择是否**适用跟踪到所有的区域**。
   - 若选择**是**，创建的单账号跟踪在所有地域均可以查看。

     > 说明 若无特殊情况，为避免遗漏事件，建议您选择此选项。

   - 若选择**否**，从**地域**列表中，选择目标地域。
6. 在**事件类型**区域，选择**写类型**、**读类型**或**所有类型**。
   - **写类型**：对云上资源运行产生影响的事件，需重点关注。
   - **读类型**：不影响资源的实际运行的事件。一般事件量非常大，会占用较多存储空间。
   - **所有类型**：查看资源所有行为的事件。
7. 在**是否开启日志记录**区域，打开投递开关。

   > 说明 开启日志记录后，请您至少选择一项投递服务。

8. 在**选择投递服务**区域，选择将操作事件投递到**OSS bucket**或**SLS Logstore**。

   > 说明 目前投递的日志范围，是单账号跟踪生效后产生的新日志，不包括原有的最近90天日志。后续我们会默认将最近90天的日志一次性投递给您，最大限度、最大范围满足您的需求。

   - **OSS bucket**：您可以根据需要选择是否将操作事件投递到新的OSS Bucket。
     - 若选择**是**，在文本框中输入**OSS Bucket名称**和**日志文件前缀**。
       此时，您可以在**开启服务端加密**区域为操作事件开启**AES256**或**KMS**加密。关于OSS服务器加密功能，请参见服务器端加密。
     - 若选择**否**，单击**OSS Bucket名称**下的输入框，根据需要选择目标Bucket。
       此时，若您需要为操作事件开启服务器端加密，请前往OSS管理控制台自行开启，详情请参见设置服务器端加密。
   - **SLS Logstore**：您可以根据需要选择是否将操作事件投递到新的SLS Project。
     - 若选择**是**，选择**日志服务Project区域**，并在文本框中输入**日志服务Project名称**。
     - 若选择**否**，选择**日志服务Project区域**和**日志服务Project名称**。
9. 单击**确定**。

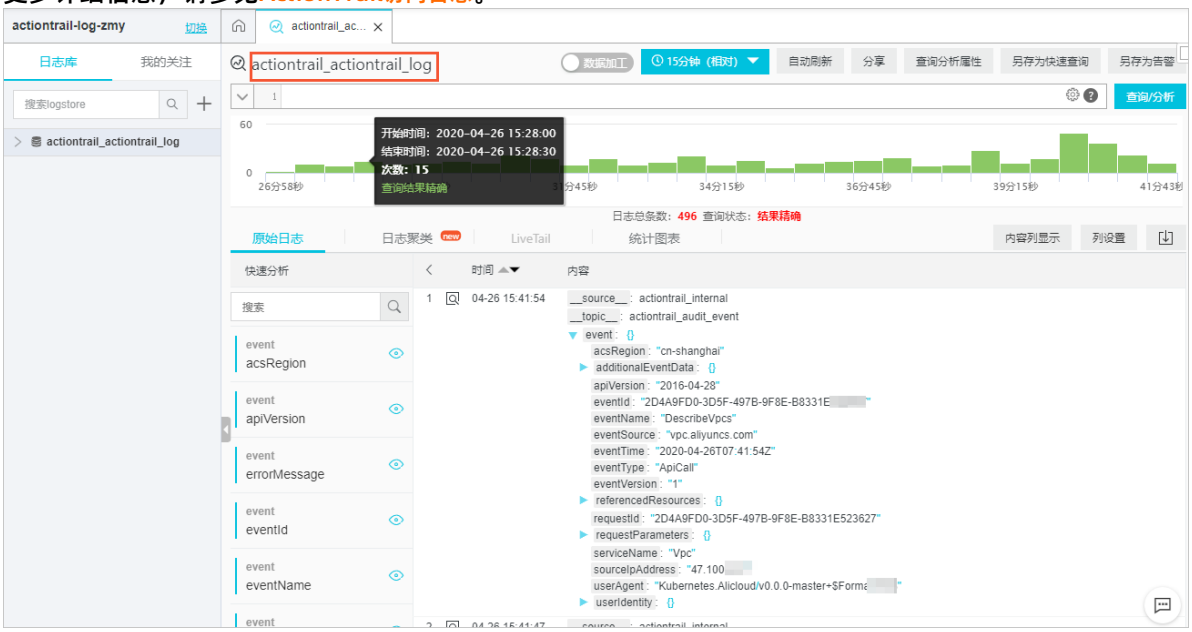
执行结果

创建单账号跟踪后，操作事件会以JSON格式保存在OSS Bucket或SLS Logstore中，便于您对操作事件进行查询和分析。您可以在OSS Bucket或SLS Logstore中查看操作日志：

- OSS Bucket：您可以通过Elastic MapReduce服务或自行授权第三方日志分析服务来分析此操作事件。
  OSS存储路径格式：

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

- SLS Logstore：操作审计会自动创建一个名为`actiontrail_单账号跟踪名称`的Logstore，以及日志的索引和图表。
  更多详细信息，请参见ActionTrail访问日志。



2.通过操作审计控制台或API查询历史事件

操作审计默认为每个阿里云账号记录最近90天的历史事件，您可以通过操作审计控制台或API查询。此外，您还可以从操作审计控制台下载最近90天的历史事件。

> **说明** 只有单账号跟踪的历史事件可以通过操作审计控制台或API查询，且每秒最多可以查询两次。多账号跟踪的历史事件不能通过操作审计控制台或API查询，只能在对应的OSS Bucket或SLS Logstore中查询。

通过操作审计控制台查询历史事件

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**历史事件查询**，可以查看最近90天的历史事件。
3. 单击每个历史事件前面的加号，可以查看该事件的详细信息。
4. 单击**查看事件**可以查询事件的代码记录。
5. 您可以设置高级搜索条件来过滤搜索结果。

> **说明** 高级搜索支持对用户名、事件名称、资源类型、资源名称、产品类型、Access Key以及时间范围进行条件过滤查询。全局事件可以在所有地域的历史事件中查询到。

通过API查询历史事件

您可以通过调用API接口LookupEvents查询最近90天的历史事件。LookupEvents接口详情，请参见LookupEvents。