阿里云
操作审计

跟踪管理

文档版本：20200314

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. **阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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。**

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意:** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击设置 > 网络 > 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击**确定**。
`Courier字体`	命令。	执行`cd /d C:/window`命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{}或者{a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1 创建跟踪

本文为您介绍如何通过操作审计控制台创建跟踪。创建跟踪可以将操作事件保存更长的时间，以便对操作事件进行分析。

背景信息

跟踪可以圈定追踪数据的地域、事件类型和投递地址。您也可以创建多个跟踪，每个阿里云账号在每个地域最多可以创建五个跟踪。

> 说明:
> 当您使用多个跟踪时，建议您不要将多个跟踪设置为同一个投递地址，这可能造成事件的重复投递和存储空间的浪费。

多个跟踪可以解决以下问题：

- 创建多个跟踪可以将不同的数据投递到不同的存储空间，并授予企业角色相应的权限，从而实现不同角色审计不同范围的操作事件。
- 创建多个跟踪到不同的国家和地域，分别投递到当地的存储空间，可以合规管理多区域的审计数据。
- 为操作事件创建多个副本备份，以免数据的丢失。

操作审计支持多个跟踪后，为避免全局事件的重复记录，会根据以下原则处理全局事件：

- 当您在线查看操作事件时，无论将控制台切换到哪个地域，都可以看到所有的全局事件。
- 当您创建跟踪时将操作事件投递到OSS Bucket后，全局事件默认与Home地域的事件在同一个文件中。

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跟踪的地域。

   > 说明:
   > 该地域将成为目标跟踪的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，单击适用跟踪到所有的区域下的输入框，根据需要选择目标地域。
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，您可以在开启服务器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*#unique_4*。
     - 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*#unique_5*。
   - 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，单击日志服务Project名称下的输入框，根据需要选择目标Project。
9. 单击确定。

预期结果

创建跟踪后，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。

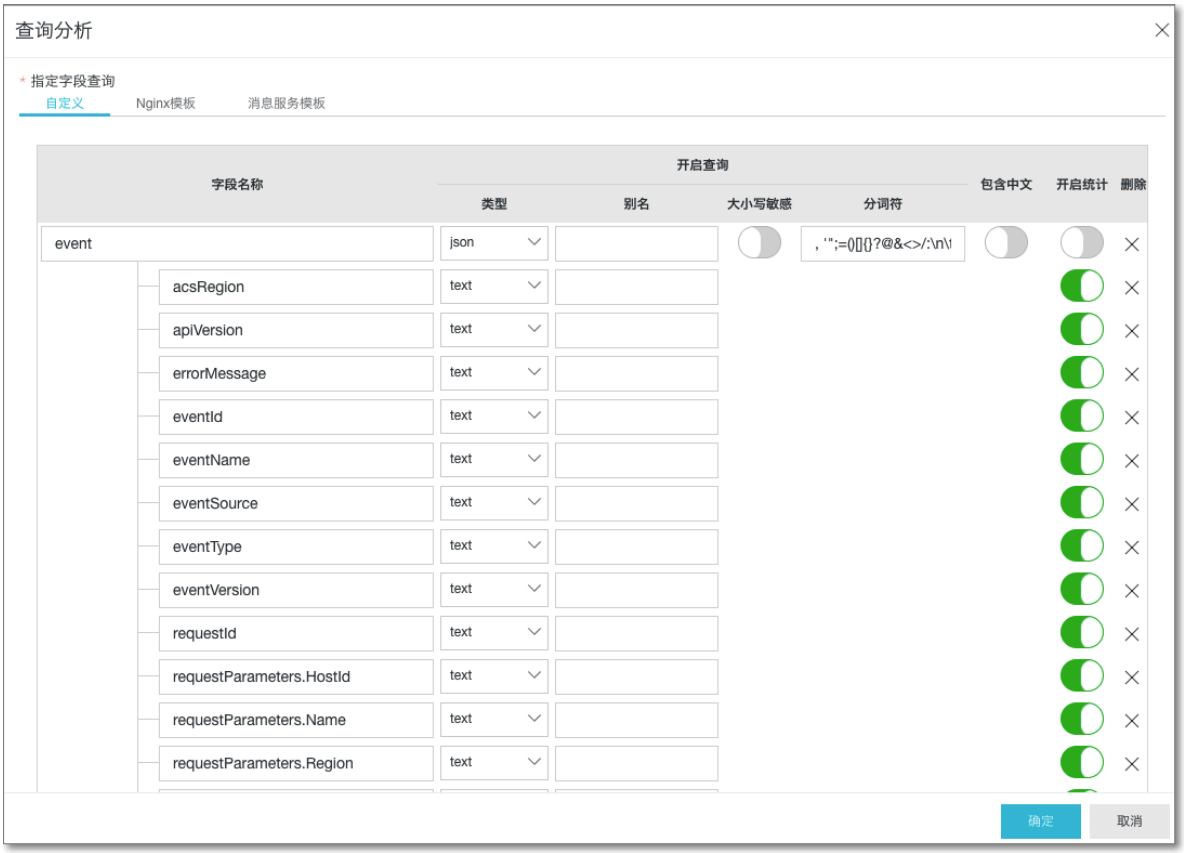
- **OSS bucket：操作事件以压缩格式保存，大小不超过2KB。您可以通过Elastic MapReduce服务或自行授权第三方日志分析服务来分析此操作事件。**

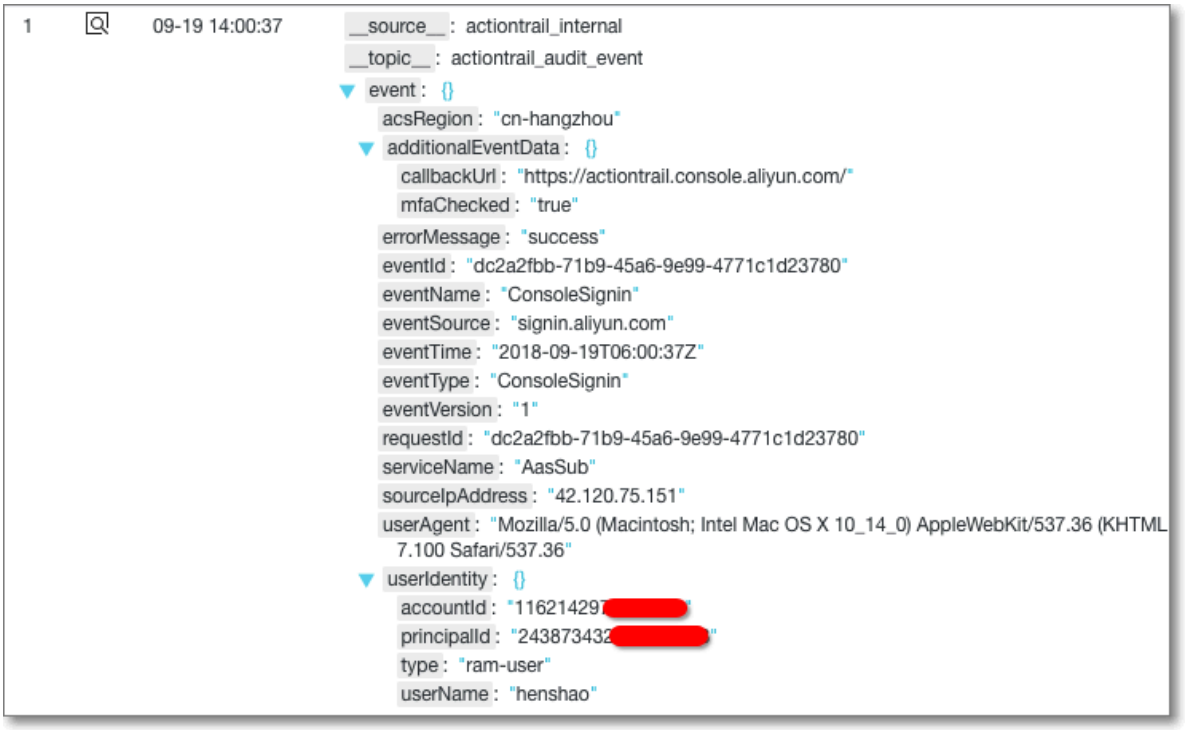
  OSS存储路径格式：

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

- **SLS Logstore：操作审计会自动创建一个名为`actiontrail_`跟踪名称的Logstore及索引和图表。**

  更多详细信息，请参见*ActionTrail*访问日志。




1
09-19 14:00:37
__source__ : actiontrail_internal
__topic__ : actiontrail_audit_event
event : {}
acsRegion : "cn-hangzhou"
additionalEventData : {}
callbackUrl : "https://actiontrail.console.aliyun.com/"
mfaChecked : "true"
errorMessage : "success"
eventId : "dc2a2fbb-71b9-45a6-9e99-4771c1d23780"
eventName : "ConsoleSignin"
eventSource : "signin.aliyun.com"
eventTime : "2018-09-19T06:00:37Z"
eventType : "ConsoleSignin"
eventVersion : "1"
requestId : "dc2a2fbb-71b9-45a6-9e99-4771c1d23780"
serviceName : "AasSub"
sourceIpAddress : "42.120.75.151"
userAgent : "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML
7.100 Safari/537.36"
userIdentity : {}
accountId : "116214297
principalId : "243873432
type : "ram-user"
userName : "henshao"

2 更新跟踪

您可以使用操作审计控制台更新跟踪。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，单击跟踪列表，然后单击要更新的跟踪的名称。
3. 在刷新的页面上，更新此跟踪的参数设置，详见创建跟踪。
4. 单击确定。

3 删除跟踪

您可以使用操作审计控制台删除跟踪。如果要删除来自所有地域的日志文件的跟踪，则必须选择最初创建此跟踪的地域。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，单击跟踪列表。
3. 找到需要删除的跟踪，单击删除。
4. 在弹出的删除跟踪对话框，单击确定将此跟踪从跟踪列表中删除。

> **注意:**
> 已经投递到日志服务或OSS Bucket中的日志文件将不会被删除。

4 关闭跟踪的日志记录

本文介绍如何关闭跟踪的日志记录。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，单击跟踪列表。
3. 在跟踪名称列，单击目标跟踪名称。
4. 关闭是否开启日志记录。

   说明:

   再次单击开关可以开启日志记录。
5. 单击确定。