ALIBABA CLOUD

阿里云

操作审计

教程

文档版本：20200828

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。

通用约定

格式	说明	样例
危险	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。	危险 重置操作将丢失用户配置数据。
警告	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。
注意	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。
说明	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`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	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.使用RAM对操作审计进行权限管理

通过RAM的权限管理功能，您可以创建自定义策略并授予RAM用户，RAM用户便可以登录操作审计服务进行相应的操作。

前提条件

- 进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。
- 使用RAM对操作审计进行授权前，请先了解操作审计的权限定义。详情请参见RAM鉴权。

操作步骤

1. 创建RAM用户。
2. 创建自定义策略。

   您可以根据下述权限策略示例创建自定义策略。
3. 为RAM用户授权。

权限策略示例

- 示例1：授予RAM用户只读权限。

```
{
"Version": "1",
"Statement": [{
"Effect": "Allow",
"Action": [
"actiontrail:LookupEvents",
"actiontrail:Describe*",
"actiontrail:Get*"
],
"Resource": "*"
}]
}
```

- 示例2：仅允许RAM用户从指定的IP地址发起只读操作。

```
{
"Version": "1",
"Statement": [{
"Effect": "Allow",
"Action": [
"actiontrail:LookupEvents",
"actiontrail:Describe*",
"actiontrail:Get*"
],
"Resource": "*",
"Condition":{
"IpAddress": {
"acs:SourceIp": "42.120.XX.X/24"
}
}
}]
}
```

2.通过操作审计监控AccessKey的使用

本文将介绍如何通过操作审计将操作事件投递到日志服务（Log Service），从而实现对AccessKey的监控和报警。

前提条件

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

背景信息

开通操作审计之后，可查询最近90天的操作事件，您可以通过AccessKeyId来检索事件，详情请参见通过操作审计控制台或API查询历史事件。您也可以将操作事件投递到日志服务，从而保存更长时间。

创建跟踪

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. **适用跟踪到所有的区域**选择**是**。
6. **事件类型**选择**所有类型**。
7. 打开**是否开启日志记录**开关，选择投递目标为**SLS Logstore**。
8. **是否新建 SLS Project**选择**是**，选择**日志服务Project区域**并填写**日志服务Project名称**。

   > 说明 此处设置的Project用于存储审计日志。您可以填写已选择地域下的Project名称，也可以输入一个新的Project名称。

9. 单击**确定**。
10. 在提示对话框中，单击**确定**。

    > 说明 创建跟踪需要授予访问日志服务和对象存储的权限。如果您已经授权，将不会弹出此对话框。

11. 在**云资源访问授权**页面下，单击**同意授权**。

    > 说明 成功创建跟踪后，操作审计会将所有地域的操作事件都投递到指定的Logstore中。

配置日志服务

1. 找到创建好的跟踪，单击其**日志服务**列下的**日志分析**。

   > 说明 您也可以通过登录日志服务控制台进行配置。

2. 输入查询语句：`event.userIdentity.accessKeyId: "LTAI********eB7Z" | select count(1) as use_ak_LTAI**`

******eB7Z，然后单击查询/分析。

3. 将日志另存为快速查询或另存为告警。
   - 另存为快速查询：单击页面右上角的另存为快速查询，输入快速查询名称后，单击确定。

     > **说明** 将日志另存为快速查询后，您可以在日志服务控制台直接选择该快速查询。

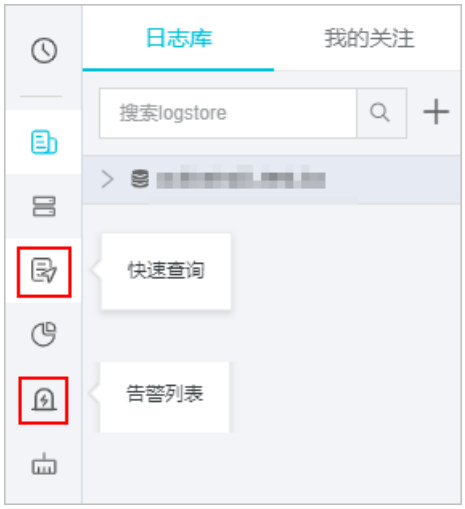
     关于快速查询的详细信息，请参见快速查询。
   - 另存为告警：单击页面右上角的另存为告警，根据下图在告警配置页签下进行告警配置并在通知页签下选择通知类型。

     关于告警的配置详情，请参见设置告警。

> **说明** 将日志另存为告警后，当满足条件便可以收到告警通知。按照上图进行告警配置后，如果 `accessKeyId` 在5分钟内被使用过，那么就报警。

执行结果

创建的快速查询和报警均可在日志服务控制台进行快速查看和管理。



3.通过操作审计监控主账号的使用

本文将介绍如何通过操作审计将操作事件投递到日志服务（Log Service），从而实现对主账号的监控和报警。

前提条件

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

创建跟踪

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. **适用跟踪到所有的区域**选择**是**。
6. **事件类型**选择**所有类型**。
7. 打开**是否开启日志记录**开关，选择投递目标为**SLS Logstore**。
8. **是否新建 SLS Project**选择**是**，选择**日志服务Project区域**并填写**日志服务Project名称**。

   > 说明 此处设置的Project用于存储审计日志。您可以填写已选择地域下的Project名称，也可以输入一个新的Project名称。

9. 单击**确定**。
10. 在提示对话框中，单击**确定**。

    > 说明 创建跟踪需要授予访问日志服务和对象存储的权限。如果您已经授权，将不会弹出此对话框。

11. 在**云资源访问授权**页面下，单击**同意授权**。

    > 说明 成功创建跟踪后，操作审计会将所有地域的操作事件都投递到指定的Logstore中。

配置日志服务

1. 找到创建好的跟踪，单击其**日志服务**列下的**日志分析**。

   > 说明 您也可以通过登录日志服务控制台进行配置。

2. 输入查询语句：`event.userIdentity.type:"root-account"| select count(1) as use_root`，然后单击**查询/分析**。

3. 将日志**另存为快速查询**或**另存为告警**。
   - **另存为快速查询**：单击页面右上角的**另存为快速查询**，输入**快速查询名称**后，单击**确定**。

     > **说明** 将日志另存为快速查询后，您可以在日志服务控制台直接选择该快速查询。

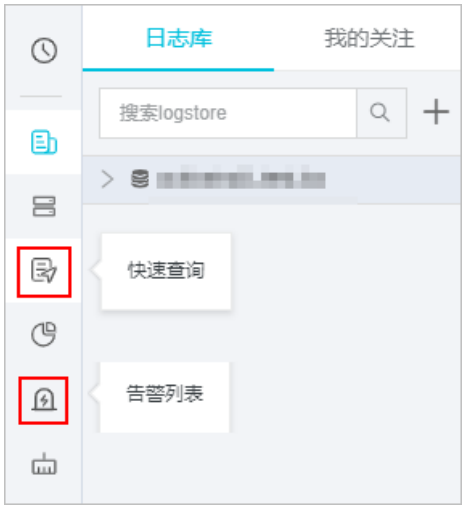
     关于快速查询的详细信息，请参见**快速查询**。
   - **另存为告警**：单击页面右上角的**另存为告警**，根据下图在**告警配置**页签下进行**告警配置**并在**通知**页签下选择通知类型。

     关于告警的配置详情，请参见**设置告警**。

> **说明** 将日志另存为告警后，当满足条件便可以收到告警通知。按照上图进行告警配置后，如果主账号在5分钟内被使用过，那么就报警。

执行结果

创建的快速查询和报警均可在日志服务控制台进行快速查看和管理。



4.使用DLA分析OSS中的操作日志

通过操作审计创建跟踪，可以持续将操作日志投递到指定的OSS Bucket中。您可以使用数据湖分析DLA（Data Lake Analytics）可视化地查询和分析OSS Bucket中的操作日志。

前提条件

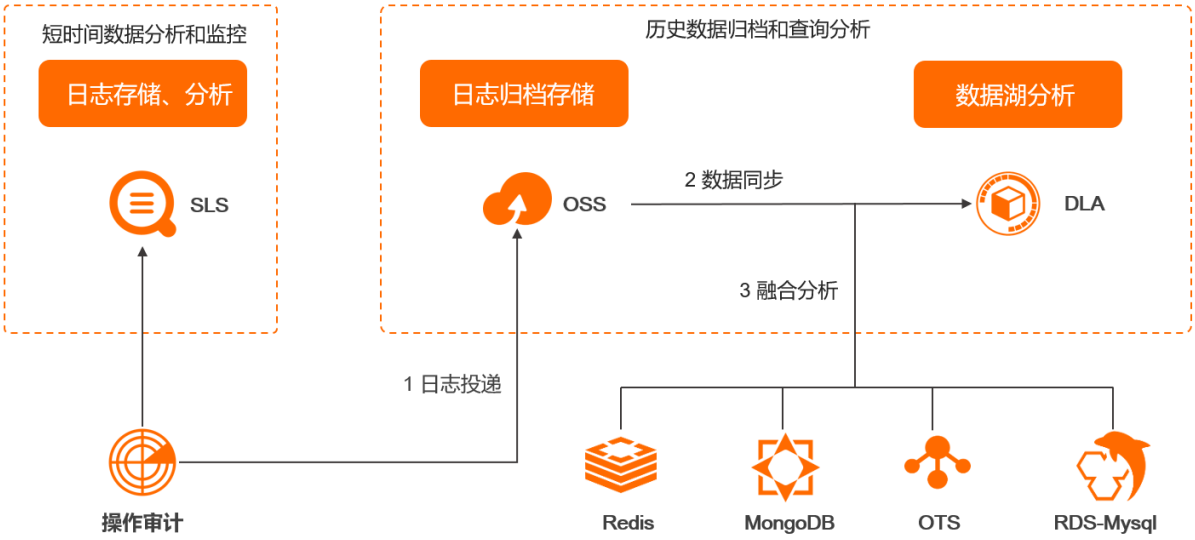
- 请确保您已经在操作审计创建了跟踪，并将操作事件投递到OSS Bucket中。详情请参见创建单账号跟踪和创建多账号跟踪。
- 请确保您已经开通了DLA服务，详情请参见开通数据湖分析服务。

背景信息

DLA是一款基于Serverless的交互式数据查询分析服务，能够便捷的对不同格式的数据源进行整合并使用统一SQL查询分析。DLA详情，请参见什么是数据湖分析。

使用DLA分析OSS中操作日志的原理如下：

1. 通过操作审计创建跟踪，将操作日志持续投递到OSS Bucket。
2. 将操作日志从OSS Bucket导入DLA。
3. DLA将OSS Bucket内以Array形式保存的多条日志记录拆分为多条数据，以JSON保存的每条操作日志转换为结构化的数据表，使得面向OSS Bucket的数据解析被大大简化，直接实现可视化的标准SQL分析。



操作步骤

1. 在DLA中创建Schema。
   i. 登录数据湖分析管理控制台。
   ii. 在页面左上角，选择与OSS所在地域一致的DLA地域。
   iii. 在左侧导航栏，单击**数据湖管理 > 数据入湖**。
   iv. 在数据入湖页面，单击**ActionTrail日志清洗**右侧的**进入向导**。

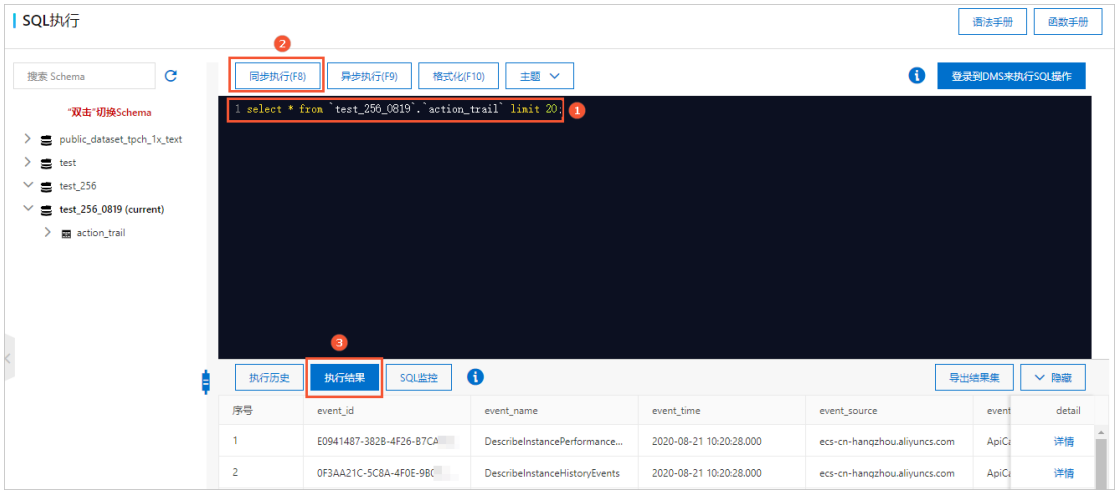
v. 在ActionTrail日志清洗页面，根据控制台提示进行配置。

配置项	说明
ActionTrail文件根目录	操作审计投递到OSS中日志数据的存储目录。目录以 `AliyunLogs/Actiontrail` 结尾。 ■ 选择位置：自定义操作审计投递到OSS中的日志数据的存储目录。 ■ 自动发现：DLA自动设置操作审计投递到OSS中的日志数据的存储目录。
Schema名称	OSS在DLA中的映射数据库名称。
清洗后数据保存位置	DLA清洗OSS数据后，将结果数据写入OSS，即数据清洗后的存储位置。 ■ 不勾选自定义：DLA默认指定存储位置。 ■ 勾选自定义：支持您自定义存储位置。
数据清洗时间	DLA每天清洗OSS数据的时间。 系统默认的数据清洗时间是00:30。您可以根据业务规律，将数据清洗时间设置在业务低峰期，以免清洗过程中对业务造成影响。

vi. 单击创建。

2. 将操作审计投递到OSS Bucket中的日志数据同步到DLA中。
   i. 在ActionTrail日志清洗页面，单击立即同步。
   ii. 单击Schema列表，在元数据管理页面单击对应Schema名右侧的库表详情。
   iii. 在元数据管理页面，单击表页签查看同步情况。您也可以在配置页签更新Schema配置。Schema表结构详情，请参见Schema表结构。
3. 使用标准SQL语法分析操作审计日志数据。
   i. 在左侧导航栏，选择Serverless SQL > SQL执行。
   ii. 找到待分析的数据库，双击切换到当前数据库。

iii. 输入查询语句，单击同步执行，系统自动生成执行结果。



> **说明** 您可以使用任何符合SQL语法的语句对DLA中的日志信息进行查询。

查询案例

查询指定AccessKey的操作日志

- 查询语句：`select * from `action_trail` where `user_identity_access_key_id` = '目标AccessKey ID' limit 20;`。
- 查询结果：前20条目标AccessKey ID产生的操作日志。

查询指定AccessKey访问ECS的操作日志

- 查询语句：`select * from `action_trail` where `user_identity_access_key_id` = '目标AccessKey ID' AND `service_name` = 'Ecs' limit 20;`。
- 查询结果：前20条目标AccessKey ID访问ECS产生的操作日志。

Schema表结构

Schema表包含以下关键字段。

名称	类型	是否必选	示例	描述
event_id	String	是	F23A3DD5-7842-4EF9-9DA1-3776396A****	事件ID。操作审计为每个操作事件所产生的一个GUID。
event_name	String	是	CreateNetworkInterface	事件名称。 • 如果eventType的取值是*ApiCall*，该字段为API的名称。 • 如果eventType的取值不是*ApiCall*，该字段为简单的英文短句，表示事件含义。

名称	类型	是否必选	示例	描述
event_source	String	是	ecs.aliyuncs.com	事件来源。
event_time	String	是	2020-01-09T12:12:14Z	事件的发生时间（UTC格式）。
event_type	String	是	ApiCall	发生的事件类型。取值： • *ApiCall*：此类事件是最普遍的一类事件。通过userAgent字段可以区分是通过控制台操作还是直接调用API。 • *ConsoleOperation（ConsoleCall）*：操作审计将此类事件客观封装为控制台行为事件。此类事件的名称并不一定是API名称，但能够传达基本的行为性质。 • *AliyunServiceEvent*：此类事件为阿里云平台对您的资源执行的操作事件，目前主要是预付费实例的到期自动释放事件。 • *PasswordReset*：密码重置事件。 • *ConsoleSignin*：控制台登录事件。 • *ConsoleSignout*：控制台登出事件。
request_parameters	字典	否	不涉及	API请求的输入参数。
response_elements	字典	否	不涉及	API响应的数据。
service_name	String	是	Ecs	事件相关的云服务名称。
source_ip_address	String	是	11.XX.XX.232	事件发起的源IP地址。 说明 如果API请求是由用户通过控制台操作触发的，那么该字段记录的是用户浏览器端的IP地址，而不是控制台Web服务器的IP地址。

名称	类型	是否必选	示例	描述
user_agent	String	是	Apache-HttpClient/4.5.7 (Java/1.8.0_152)	发送API请求的客户端代理标识。取值示例： • *AlibabaCloud (Linux 3.10.0-693.2.2.el7.x86_64;x86_64) Python/2.7.5 Core/2.13.16 python-requests/2.18.3*。 • *Apache-HttpClient/4.5.7 (Java/1.8.0_152)*。
user_identity_type	String	是	ram-user	身份类型。当前支持的身份类型包括： • *root-account*：阿里云账号。 • *ram-user*：RAM用户。 • *assumed-role*：RAM角色。 • *system*：阿里云服务。
user_identity_principal_id	String	是	28815334868278****	当前请求者的ID。 • 如果type的取值是*root-account*，则记录阿里云账号ID。 • 如果type的取值是*ram-user*，则记录RAM用户ID。 • 如果type的取值是*assumed-role*，则记录RoleID:RoleSessionName。
user_identity_account_id	String	是	1122334455666****	阿里云账号ID。
user_identity_accessKey_id	String	否	55nCtAwmPLkk****	如果请求者通过SDK访问API，则记录该字段。如果请求者通过控制台登录，则该字段不显示。
user_name	String	否	B**	如果type的取值是*ram-user*，则记录RAM用户名。如果type的取值是*assumed-role*，则记录RoleName:RoleSessionName。