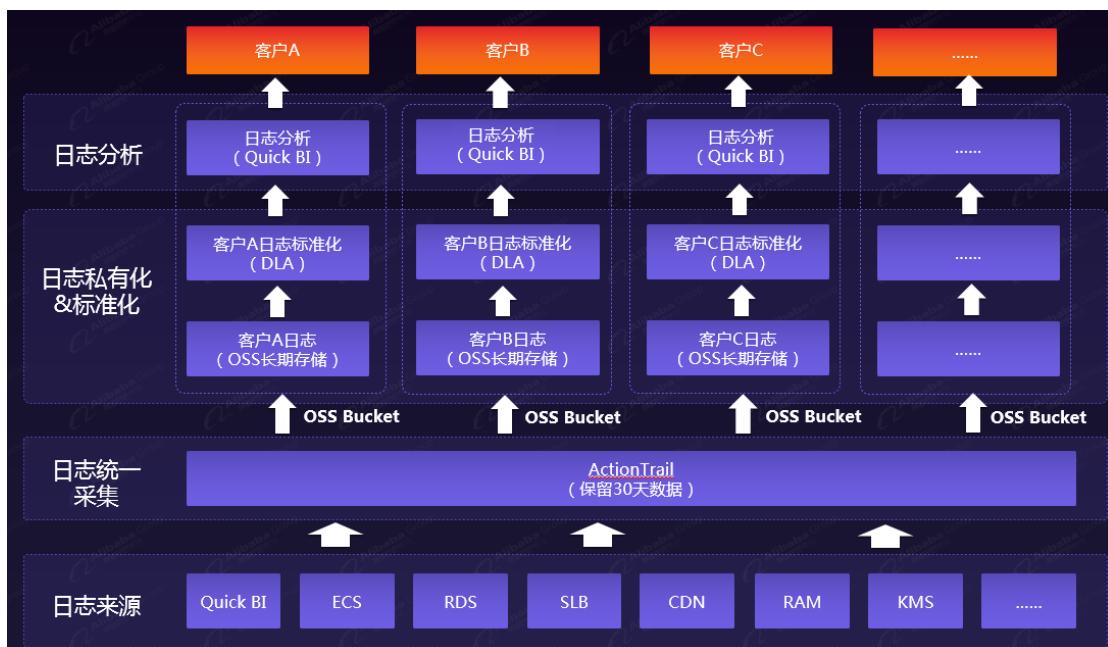


# 阿里云审计日志持久化联合解决方案

## 引言

随着网络信息化的成熟发展、“国家网络安全法规”的深入落实要求，企业组织也越来越重视操作日志的保存与分析，其中云计算中的资源的操作记录是一类非常重要的日志。阿里云构建了操作审计(ActionTrail)产品，为云上客户提供审计日志服务。那么如何利用阿里云操作审批(ActionTrail)来构建长周期的云上操作审计方案呢？小编推“ActionTrail+OSS+DLA+Quick BI”的组合解决方案，将ActionTrail的审计日志定时同步到OSS进行长周期保存，利用Data Lake Analytics将日志数据标准化，利用Quick BI进行审计日志的主题式分析。

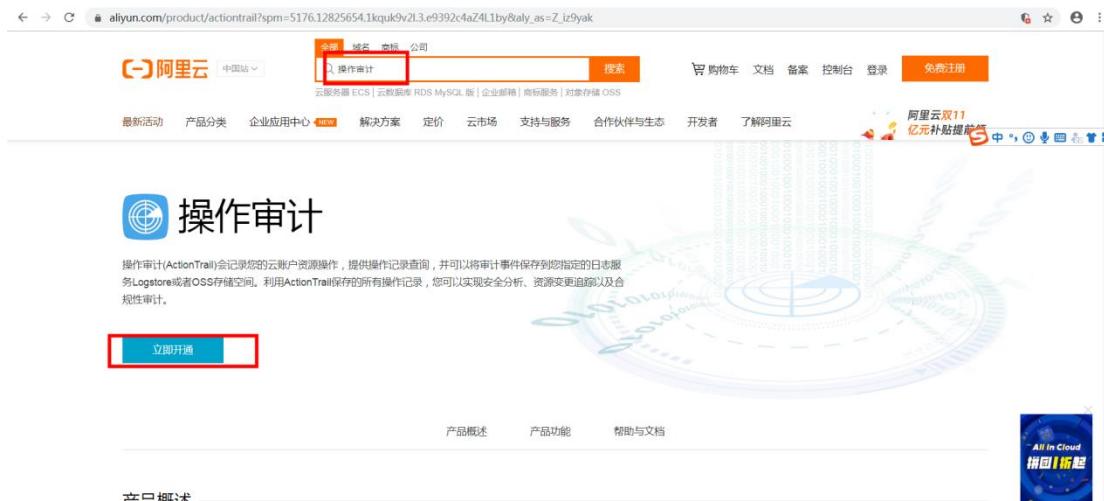


## ActionTrail 审计日志：审计日志统一采集

操作审计(ActionTrail)会记录您的云账户资源操作，提供操作记录查询，并可以将审计事件保存到您指定的日志服务 Logstore 或者 OSS 存储空间。利用 ActionTrail 保存的所有操作记录，您可以实现安全分析、资源变更追踪以及合规性审计。需要开通操作审计功能，才可以实现审计日志统计收集。

### 1. 开通审计日志服务

在阿里云官网搜索并开通审计日志服务，必须是主账号开通。当前已经接入 Quick BI、ECS、RDS、SLB、CDN、RAM、KMS 等产品的部分日志。



## 2. 审计日志控制台

开通服务后，该主账号已购买服务的操作日志将同步到 Actiontrail，日志默认保留 30 天。

审计日志持久化：基于 ActionTrail 将日志同步到 OSS

基于 ActionTrail 的创建跟踪功能，我们可以以便保存更长时间的审计事件。操作审计会将事件保存到我们指定的 OSS Bucket 中。

## 1. 选择日志同步 Region

进入 ActionTrail 的跟踪列表功能，在控制台右上角选择跟踪投递的目标 Region。

The screenshot shows the Alibaba Cloud Audit Log interface. At the top right, there is a search bar and several navigation links: 消息 (Messages), 费用 (Cost), 工单 (Work Orders), 备案 (Registration), 企业 (Enterprise), 支持与服务 (Support & Services), and 简体中文 (Simplified Chinese). A red box highlights the 'Audit Log' button at the top right of the main content area.

## 2. 创建日志跟踪服务

- 1) 选择日志服务 Project 区域，并且输入日志服务 Project 名称；

The screenshot shows the 'Create Log Tracking Service' configuration page. On the left, there is a sidebar with '操作审计 ActionTrail' and '历史事件查询'. The main area has a title '创建跟踪' with a '返回' button. Below it, a note says '跟踪必须选择一个投递目标。请选择将审计事件投递至OSS Bucket或者日志服务中。' The configuration section starts with '跟踪列表' and '跟踪名称' (input: 'at-product-account-audit'). Under '事件类型', the '所有类型' radio button is selected. The next section is '将审计事件投递到OSS Bucket' with '是否创建新的OSS Bucket?' (radio buttons: '是' and '否', '否' is selected). It includes fields for 'OSS Bucket名称' (input: '请输入Bucket名字') and '日志文件前缀' (input: ''). The final section is '将审计事件投递到日志服务' with '日志服务Project区域' (dropdown: '华东2 (上海)') and '日志服务Project名称' (input: 'at-product-account-audit'). A red box highlights the '日志服务Project区域' dropdown and the '日志服务Project名称' input field. At the bottom, there is a '是否开启日志记录' switch (on), a '提交' button, and a '清除' button.

- 2) OSS Bucket: 如果创建新的 OSS Bucket, 请在文本框中输入一个名称; 否则单击 OSS Bucket 名称输入框, 会出现可供选择的 Bucket 列表。

操作审计 ActionTrail

创建跟踪 [返回](#)

历史事件查询

跟踪列表

跟踪名称: at-product-account-audit

事件类型:  所有类型  读类型  写类型

**将审计事件投递到OSS Bucket**

是否创建新的OSS Bucket?  是  否

OSS Bucket名称: at-product-account-audit

日志文件前缀: secloud

**将审计事件投递到日志服务**

日志服务Project区域: 华东2 (上海)

日志服务Project名称: 请输入新的或者已存在的Project

是否开启日志记录:

提交 清除

3) 同意授权: 首次创建跟踪, 界面会提示授权 ActionTrail 访问 OSS 和日志服务的权限。

云资源访问授权

温馨提示: 如需修改角色权限, 请前往RAM控制台 [角色管理](#) 中设置, 需要注意的是, 错误的配置可能导致ActionTrail无法获取到必要的权限。 [X](#)

ActionTrail请求获取访问您云资源的权限

下方是系统创建的可供 ActionTrail 使用的角色, 授权后, ActionTrail 拥有对您云资源相应的访问权限。

**AliyunActionTrailDefaultRole**

描述: ActionTrail默认使用此角色来访问您在其他云产品中的资源

权限描述: 用于ActionTrail服务默认角色的授权策略, 包括OSS的对象列出及写入权限

同意授权 取消

## 日志标准化: 基于 DLA 实现 ActionTrail 审计日志标准化

将 ActionTrail 的审计日志投递到 OSS 之后, 我们发现递到 OSS 的日志格式是非 HADOOP 标准 JSON 格式且存在大量小文件, 非常不利于审计日志解析和查看。联合 DLA 专项定制了 ActionTrail 日志清洗服务, 基于 ActionTrail 日志清洗功能, 我们可以快速实现 ActionTrail 日志数据的格式化, 而且可以基于 DLA 实现亿级别数据的快速查询与分析。

### 1. 开通 DLA 服务

1) 在阿里云官网搜索并开通 DLA 服务。如下所示:

The screenshot shows the Alibaba Cloud search interface. The search bar at the top has 'DLA' entered. Below the search bar, there's a list of search results, with the first item being 'Data Lake Analytics'. This item is highlighted with a red box. To the right of the search results, there's a '产品推荐' (Product Recommendation) sidebar with various services like CA证书服务, 数据传输, MaxCompute, etc.

## 2. 创建 ActionTrail 日志 Schema

1) 进入 DLA 控制台, 选择“Schema 管理”功能;

The screenshot shows the DLA Control Panel. On the left, there's a sidebar with various management options. The 'Schema Management' option is selected and highlighted with a red box. In the main area, there's a table listing existing schemas, and a prominent red box highlights the 'Create Schema' button at the top of the table.

2) 选择 ActionTrail 日志清洗功能下的“使用向导创建”即可;

The screenshot shows the DLA Control Panel again, but this time the focus is on the 'ActionTrail 日志清洗' section. A red box highlights the '使用向导创建' (Use Wizard Creation) button within this section, which is part of the 'ActionTrail 日志清洗' service.

- 3) 按照提示填写对应的 ActionTrail 文件根目录等，定义 Schema 名称，就可以实现快速创建了；

- 4) 日志同步，点击“立即同步”可以立即实现 Schema 创建和数据自动同步，随着审计日志文件定时追加，数据会及时更新。



- 5) 标准化之后的数据格式如下：(以 Quick BI 日志说明为主)

- 格式化后字段说明：

字段 (英文)	名称 (中文)	说明
dt	日志汇通时间 (DAY)	
event_id	事件 ID	
event_name	事件名称	
event_source	事件来源	
event_time	事件发生时间	
event_type	事件类型	QuickbiFunctionLog: 功能操作日志; QuickbiViewLog: 访问行为日志; QuickbiPermissionlog: 授权行为日志;
qbi_granted_type	QBI 授权类型	ALLUSER: 所有用户; PUBLIC: 公开; USER: 用户; USERGROUP: 用户组;
qbi_operation_type	QBI 操作类型	ADD: 增加; MODIFY: 修改; VIEW: 查看; downloads : 下载等; 详见单项说明
qbi_source_flag	QBI 来源标识	COMMON: 普通; PUBLIC: 公开
qbi_target_name	QBI 目标名称	
qbi_target_type	QBI 目标类型	CUBE 数据集

		DASHBOARD：仪表板;DASHBOARDOFFLINEQUERY：自助取数;DATAFORM：数据填报;MENU：数据门户菜单;PAGE：仪表板;PRODUCT：数据门户REPORT：电子表格;WORKSHEET：老工作表 WORKSPACE：工作空间
qbi_workspace_name	QBI 操作对象归属工作空间	
region	来源 Region	
request_parameters	请求参数	
service_name	来源服务	
source_ip_address	来源 IP	
user_agent	user_agent	
user_identity_access_key_id	access_key_id	
user_identity_account_id	访问账号 ID	
user_identity_principal_id	主账号	
user_identity_type	账号类型	
user_name	操作人	

● qbi\_operation\_type 的操作类别说明：

事件类型	操作类型（英文）	操作类型（中文）
QuickbiPermissionlog	PUBLISH	发布
	AGREE_ACCESS	同意访问
	SHARE	分享
	CHANGE_ROLE	变更角色
	CANCEL_PUBLIC	取消发布
	STOP_SHARE	取消分享
	OPEN_ROW_LEVEL	打开行级权限
	ROW_LEVEL_PERMISSION	行级授权
	CLOSE_ROW_LEVEL	关闭行级权限
	DELIVER	数据填报发布
	REFUSE_ACCESS	拒绝访问
	TRANSFER_OWNER	转让所有者
QuickbiFunctionLog	ADD	增加
	DELETE	删除
	COLLECT	收藏
	MODIFY	修改
	MODIFY_PROPERTIES	修改属性
	MOVE	移除
	RENAME	重命名
	CANCEL_COLLECT	取消收藏
	REMOVE_MEMBER	移除组织成员

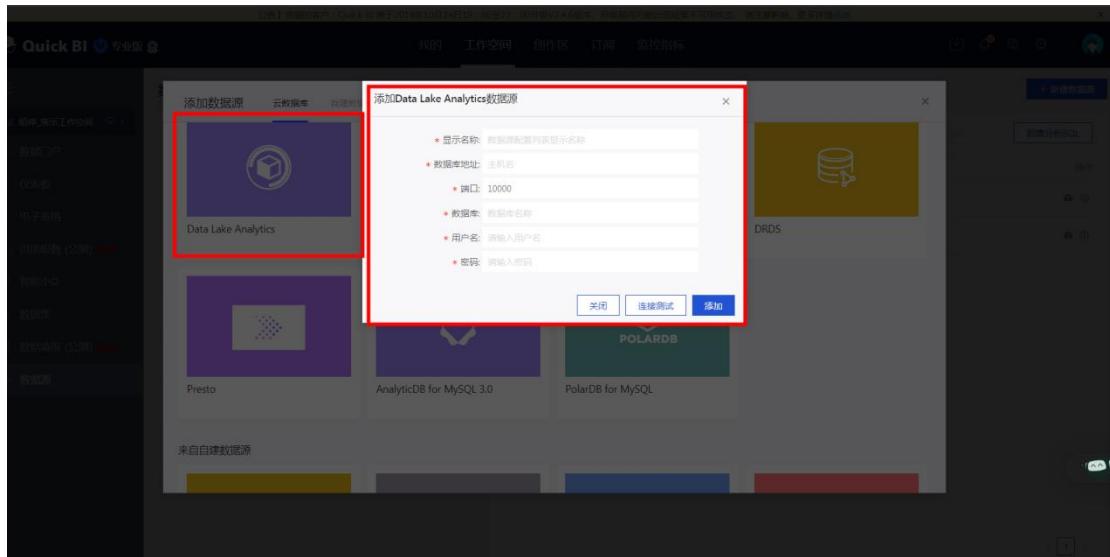
	ADD_MEMBER	新增组织成员
	APPLY_ACCESS	申请访问
	APPLY_IMBEDDING_REPORT	申请嵌入报表
	CANCLE_IMBEDDING_REPORT	取消嵌入报表
QuickbiViewLog	VIEW	查看
	EXPORT	另存为本地（电子表格）
	DOWNLOAD	下载

## 日志分析：基于 Quick BI 实现审计日志自助分析

在 DLA 进行日志标准化基础之上，利用 Quick BI 进行审计日志自助分析。在实际过程中，可以根据日志的来源系统进行业务拆分，形成不同业务分析主题，满足各业务审计日志查询要求。下面以 Quick BI 的审计日志为例，进行使用讲解。

### 1. 创建 DLA 数据源连接

填写在 Quick BI 中新建 DLA 数据源连接，填写对应的数据库连接信息即可。



### 2. 快速创建审计日志数据集

1) 选择 DLA 标准化后的数据表，一键快捷创建数据集。如下所示：

2) 在 Quick BI 的数据集管理功能中，进行数据集处理。“event\_id”可以克隆字段并转换为度量并扩展为 PV 字段；“username”可以克隆字段并转换为度量并扩展为 UV 字段。如下所示：

维度	度量	操作对象名称	操作对象类型		
acs_region	event_id				
cn-shanghai	7a2b3f31-a75c-4469-9190-bcc0cf6d750e_5D93F3186CBF9717C1A88B58	DescribeTable	2019-10-02T00:45:12	TableEvent	MaxCompute
cn-shanghai	12991922-3194-4ae2-872d-d4141d284f49_5D93F319619FC450203A7B8	DescribeTable	2019-10-02T00:45:13	TableEvent	MaxCompute
cn-shanghai	77425331-005d-4307-8071-00de964c60ff_5D93F31983C08908CC43749	DescribeTable	2019-10-02T00:45:13	TableEvent	MaxCompute
cn-shanghai	f6092e52-1824-42dc-9e64-335cc06b794c_5D93F31954CF64C78EB10F15	DescribeTable	2019-10-02T00:45:13	TableEvent	MaxCompute
cn-shanghai	0262695b-fb25-41ce-8e0b-e178a87362a0_a_5D97E37F14242AF65807D764	DescribeTable	2019-10-05T00:27:43	TableEvent	MaxCompute
cn-shanghai	f7Sebbbf-e594-4af3-b07a-14483570d0f8_5D97E380619FC4502CDC447	DescribeTable	2019-10-05T00:27:45	TableEvent	MaxCompute
cn-shanghai	5364417b-c4b1-42eb-bbd7-89d125763ab2_5D97E3876CBF9717C11EA8E3C	DescribeTable	2019-10-05T00:27:51	TableEvent	MaxCompute
cn-shanghai	27d1c70a-2e69-4c29-ae13-f447b13e2e06_5D97E3916CBF9717C11EA049	DescribeTable	2019-10-05T00:28:01	TableEvent	MaxCompute
	8589b692-8b19-44b7-8e10-044077a4e4c_5D97E3916CBF9717C11EA049				

### 3. 创建审计日志分析主题（以 Quick BI 审计日志为例）

在 Quick BI 的仪表板管理中，建立审计日志报表。Quick BI 审计日志参考如下：

