目录

历史事件查询

操作审计仅默认为每个金山云账号记录最近93天的操作事件。若您需要记录更长时间，请创建事件跟踪，操作日志将自动且持续地被投递到指定的存储空间。

操作步骤

1.登录操作审计控制台 2.在左侧导航栏，单击**历史事件记录**。 3.在事件聚合查询页面输入搜索条件，设置查询的时间范围然后单击**查询**按钮。

您可以设置事件名称、服务名称、读写类型、AccessKey ID等搜索条件来过滤查询事件。

4.单击目标**事件名称**查询事件详细记录。关于事件中字段的更多信息，请参见事件结构说明。

事件结构说明

本文为您介绍一个事件包含的关键字段及其含义，并为您提供相关的示例。

事件结构定义

名称	是否非空	描述
CreateTime	是	事件的创建时间
ServiceName	是	事件相关的云服务名称，例如iam
EventSource	是	事件来源。例如 iam.inner.api.ksyun.com
RequestParameters	否	API请求的输入参数。
SourceIpAddress	是	事件发起的源IP地址。
EventType	是	发生的事件类型。取值： ApiCall：API调用事件。大多金山云控制台基于API开发，对应的操作行为也会记录为ApiCall。 ConsoleSignin：控制台登录事件。
EventId	是	事件ID。操作审计为每个管控事件所产生的一个UUID。 例如55733e91-4e3b-4**b-053787278d2e
EventRw	是	事件的读写类型。 read：读类型 write：写类型
EventName	是	事件名称。 如果eventType取值为ApiCall，该字段为API的名称。 如果eventType取值不为ApiCall，该字段为简单的英文短句，表示事件含义。
UserIdentity	是	请求者的身份信息。 UserType:Root-金山云主账号；User-IAM子用户，Role-IAM角色 AccountId:金山云账号ID UserName： —如果是金山云主账号，记录为root —如果是IAM子用户，记录为username —如果为IAM角色，则记录accouid：rolename RoleName：如果是角色访问，则记录为角色名称 AccessKey：如果请求者通过Openapi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。
ReferencedResources	否	事件影响的资源列表。
Region	是	地域，例如cn-beijing-6
RequestId	是	请求ID。例如ae7d9265-c82d-4f15-b98a-67ef278ff129
EventTime	否	事件的发生时间。例如：2021-08-10 17:40:59
ErrorCode	否	错误代码，例如：AccessDenied
ErrorMessage	是	错误信息，例如：The request was rejected because the old password was incorrect
UserAgent	是	发送API请求的客户端代理标识。

事件示例

```
{
    "ErrorMessage": "",
    "CreateTime": "2021-08-11 10:19:12",
```

```
    "ServiceName": "passport",
    "EventSource": "api.passport.ksyun.com",
    "ApiVersion": "",
    "RequestParameters": "",
    "SourceIpAddress": "59.172.244.24",
    "EventVersion": "1",
    "EventType": "ConsoleSignin",
    "EventId": "81da2066-e81a-4aa3-8196-34daaaeaae3e",
    "EventRw": "write",
    "EventName": "ConsoleSignin",
    "UserIdentity": {
        "RoleName": "",
        "AccountId": "20001***964",
        "UserType": "Account",
        "UserName": "root",
        "AccessKey": ""
    },
    "ErrorCode": "",
    "Region": "",
    "RequestId": "d54f7851-f09c-d610-b1d9-221fecae5a40",
    "EventTime": "2021-08-11 10:19:12",
    "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/5
37.36"
}
```


事件聚合查询

您可以通过操作审计控制台进行事件聚合查询。操作审计每两小时对事件聚合一次，方便您查询聚合结果，大幅提升在线事件搜索和查询效率。

使用限制

- 操作审计事件聚合查询功能只能查询最近30天的事件。
- 每隔2小时整点为您聚合最新相关事件。

操作步骤

1.登录操作审计控制台 2.在左侧导航栏，单击**事件聚合查询**。 3.在事件聚合查询页面输入搜索条件，设置查询的时间范围然后单击**查询**按钮。

您可以设置事件名称、服务名称、读写类型、AccessKey ID等搜索条件来过滤查询事件。

4.单击目标**事件名称**查询事件记录。您可以查看到事件详情以及在该时间段内事件的发生次数。

创建事件跟踪

操作审计默认为每个金山云账号记录最近30天的操作事件，如果不创建跟踪，您将无法追溯30天以前的操作事件。本文为您介绍如何创建事件跟踪，将操作事件投递到KS3对象存储服务，以便对操作事件进行长久保存及分析。

操作步骤

1.登录操作审计控制台 2.在左侧导航栏，单击**事件跟踪列表**。 3.在事件跟踪列表，单击**创建事件跟踪**。 4.在创建事件跟踪页面，设置如下信息

跟踪名称：跟踪的名称，必须以小写字母开头，只能包括小写字母、数字、连字符（-）和下划线（_）。 事件类型：选择您要投递到存储空间的事件类型，有全部、读事件、写事件。 KS3 bucket域名：要投递的存储空间的bucket域名，请在对应存储空间详情页获取。 日志文件前缀：操作事件存放的日志文件前缀，方便后续查找操作事件。 5.单击**确定**，提交完成。

执行结果

创建跟踪后，将会每天推送前一天的事件日志您指定的存储空间的文件夹下存储路径格式为： ks3:///<日志文件前缀>/KsyunLogs/Actiontrail/<年>/<月>/<日>/<日志文件>