阿里云
操作审计

用户指南

文档版本：20190729

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
	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，恢复业务所需时间约10分钟。
	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。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 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。	`swich` *`{stand | slave}`*

目录

1 产品限制

表 1-1: 业务限制说明

限制项	限制范围
一个用户允许创建的 Trail 数目	用户在所有区域只能创建一个跟踪
一个 Trail 允许配置的 OSS Bucket 数目	1
用户操作后需要多长时间才能通过控制台查询到	一般不超过 10 分钟
用户操作需要多长时间才能在 OSS Bucket 中访问到数据	一般不超过 10 分钟
用户通过控制台或 API 能查询最近多长时间的操作历史记录	30天
保存到 OSS Bucket 中的记录文件对象（压缩后）Size	<= 2KB

2 ActionTrail 支持的云服务

本文为您罗列了 ActionTrail 支持的云服务列表。

弹性计算

- 云服务器 ECS
- 弹性伸缩
- 容器服务
- 容器镜像服务
- 轻量应用服务器
- 批量计算
- 弹性高性能计算 E-HPC
- Web 应用托管服务
- 弹性容器实例 ECI
- 运维编排服务

存储

- 文件存储
- 智能云相册

数据库

- 云数据库 RDS 版
- 数据传输服务 DTS
- HybridDB for MySQL
- HybridDB for PostgreSQL
- 云数据库 Redis 版
- 云数据库POLARDB

网络

- 专有网络 VPC
- NAT 网关
- 弹性公网 IP
- 高速通道
- 全球加速

- 共享流量包
- 共享带宽
- 云企业网
- 负载均衡
- 智能接入网关

视频与CDN

- CDN
- 视频点播
- 视频直播
- 媒体处理
- PCDN

域名与网站（万网）

- 域名
- 云解析 DNS

应用服务

- API 网关
- 云 AP
- 云桌面
- 区块链服务

互联网中间件

消息队列 RocketMQ

云通信

- 短信服务
- 短信服务 API
- 语音服务
- 语音服务 API
- 流量服务
- 流量服务 API

安全

- DDoS 防护包

- DDoS 高防 IP
- Web 应用防火墙
- Web 应用防火墙 API
- 安骑士
- 堡垒机
- 加密服务
- 数据库审计
- 云防火墙
- 数据风控
- 网站威胁扫描系统

大数据

- E-MapReduce
- QuickBI

人工智能

智能语音交互

物联网

阿里云物联网平台

管理与监控

- 云监控
- 访问控制
- 身份管理服务
- 账号登录服务，包括以下产品：
  - 云账号登录服务
  - RAM 用户登录服务
- 安全令牌
- 资源管理
- 操作审计
- 资源编排
- 密钥管理服务

会员服务

费用中心 API

3 控制台操作指南

3.1 常用操作导航

通过 ActionTrail 控制台执行的常用操作包括：

- 创建跟踪
- 历史事件查询

4 控制用户的访问权限

4.1 RAM 支持的 ActionTrail 操作和资源

您可以使用阿里云 RAM 服务，创建 RAM 用户并授权其 ActionTrail 的操作权限。为了遵循最佳安全实践，建议您使用 RAM 用户来操作 ActionTrail。

RAM 中可授权的 ActionTrail 操作列表

RAM 中可授权的 ActionTrail 的操作（Action）如下：

- CreateTrail
- UpdateTrail
- DeleteTrail
- DescribeTrails
- GetTrailStatus
- StartLogging
- StopLogging
- LookupEvents

资源标识格式

在 RAM 的权限策略中，云资源按以下格式标识：

资源（Resource）	说明
*	所有云资源。
acs:actiontrail:${region}:${AccountId}:*	指定区域的资源。

授权策略样例

- 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 地址发起的只读操作。

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

4.2 授权 RAM 用户操作 ActionTrail

本文介绍了通过 RAM 的权限管理能力，通过创建用户并授予相应的权限，以满足 RAM 用户操作 ActionTrail 的资源。

前提条件

创建 RAM 用户。

使用系统策略为 RAM 用户授权

ActionTrail 支持的系统策略有：

表 4-1: 系统策略

系统策略名称	说明
AliyunActionTrailFullAccess	ActionTrail 完全管理权限
AliyunActionTrailReadOnlyAccess	ActionTrail 只读权限

如何为用户组授权，请参考：为 RAM 用户授权。

使用自定义策略为 RAM 用户授权

如果上述系统策略不能满足您的需要，您可以创建自定义策略并为 RAM 用户授权。

以下示例表示：只允许从某一 IP 地址范围发起 ActionTrail 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"
            }
        }
    }]
}
```

5 操作事件(Event)结构定义

一个事件记录内容包含的关键字段

apiVersion

- 类型：String
- 必须：是
- 描述：所调用的云服务 API 版本。

eventId

- 类型：String
- 必须：是
- 描述：事件 ID，由 ActionTrail 服务为每个操作事件所产生的一个 GUID。

eventName

- 类型：String
- 必须：是
- 描述：API 操作名称，可参考各服务的 API 操作列表，比如`Ecs`的`StopInstance`。

eventSource

- 类型：String
- 必须：是
- 描述：处理 API 请求的服务端，比如 ram.aliyuncs.com 。

eventTime

- 类型：String
- 必须：是
- 描述：API 请求的发生时间（UTC格式）。

eventType

- 类型：String
- 必须：是
- 描述：发生的事件类型，如`ApiCall`（控制台或API操作）， `ConsoleSignin`（用户登录）。

eventVersion

- 类型：String

- 必须：是
- 描述：ActionTrail 事件格式的版本，当前版本为"1"。

errorCode

- 类型：String
- 必须：否
- 描述：如果云服务处理 API 请求时发生了错误，这里记录了相应的错误码，比如 `NoPermission`。·

errorMessage

- 类型：String
- 必须：否
- 描述：如果云服务处理API请求时发生了错误，这里记录了相应的错误消息，比如 “You are not authorized.”

requestId

- 类型：String
- 必须：是
- 描述：云服务处理 API 请求时所产生的消息请求 ID。

requestParameters

- 类型：字典
- 必须：否
- 描述：API 请求的输入参数，具体参数含义需参考相应云服务的 API 文档。

responseElements

- 类型：字典
- 必须：否
- 描述： API 响应的数据，具体格式需参考相应云服务的 API 文档。

referencedResources

- 类型：字典
- 必须：否
- 描述： API 操作的资源。

serviceName

- 类型：String

- 必须：是
- 描述：云服务名称，如`Ecs`, `Rds`, `Ram`。

sourceIpAddress

- 类型：String
- 必须：是
- 描述：发送 API 请求的源 IP 地址。如果 API 请求是由用户通过控制台操作触发，那么这里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。

userAgent

- 类型：String
- 必须：是
- 描述：发送 API 请求的客户端代理标识，比如控制台为`AliyunConsole`，SDK 为`aliyuncli/2.0.6`。

userIdentity

- 类型：字典
- 必须：是
- 描述：请求者的身份信息。

userIdentity包含如下属性字段

名称	是否必需	描述
type	是	身份类型。当前支持的身份类型包括`root-account`（主账号）、`ram-user`（RAM 用户）、`assumed-role`（RAM 角色）。
principalId	是	当前请求者的 ID。如果身份类型是`root-account`，则记录主账号 ID；如果是`ram-user`，则记录 RAM 用户名；如果是`assumed-role`，则记录 RoleID:RoleSessionName。
accountId	是	主账号 ID。

名称	是否必需	描述
accessKeyId	否	请求者通过 SDK 访问云服务 API 时记录该字段。如果通过控制台访问，则该字段不显示。
userName	否	如果请求者类型为`ram-user`，则记录 RAM 用户名；如果请求者类型为`assumed-role`，则记录 roleName:roleSessionName。
sessionContext	否	如果调用 API 请求时使用的是临时安全凭证 #unique_16，则记录该信息；通过控制台执行操作时也会触发session的创建并记录该信息。Session 内容包括：creationDate（Session创建时间）、mfaAuthenticated（用户登录控制台时是否使用多因素认证）

userIdentity示例

- RAM 用户通过 SDK 执行操作：

```
"userIdentity": {
    "type": "ram-user",
    "principalId": "28815334868278****",
    "accountId": "112233445566****",
    "accessKeyId": "55nCtAwmPLkk****",
    "userName": "B**"
}
```

- RAM 用户通过控制台执行操作：

```
"userIdentity": {
    "type": "ram-user",
    "principalId": "28815334868278****",
    "accountId": "112233445566****",
    "userName": "B**",
    "sessionContext": {
        "attributes": {
            "mfaAuthenticated": "true",
            "creationDate": "2015-12-31T06:33:14Z"
        }
    }
```

```
}
```

- **RAM 角色通过 SDK 执行操作：**

```
"userIdentity": {
    "type": "assumed-role",
    "principalId": "28815334868278****:a****",
    "accountId": "112233445566****",
    "accessKeyId": "STS.F24gnHkUE7dER4rsFFQ4n****",
    "userName": "manager:a****"
}
```

6 操作事件(Event)样例

6.1 ECS

RAM用户通过控制台停止ECS实例


```
{
    "apiVersion": "2014-05-26",
    "eventId": "f4788483-70fc-476b-839b-af5ed11170cd",
    "eventName": "StopInstance",
    "eventSource": "ecs-cn-hangzhou.aliyuncs.com",
    "eventTime": "2016-01-04T09:47:40Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "recipientAccountId": "4****",
    "requestId": "275A832E-4C6A-47BE-A432-C18DDD79FDAB",
    "requestParameters": {
        "ForceStop": "true",
        "InstanceId": "i-22nyr****"
    },
    "serviceName": "Ecs",
    "sourceIpAddress": "42.120.XX.XX",
    "userAgent": "AliyunConsole",
    "userIdentity": {
        "type": "ram-user",
        "accountId": "4****",
        "principalId": "28815334868278****",
        "userName": "B**",
        "sessionContext": {
            "attributes": {
                "creationDate": "2016-01-04T09:47:40Z",
                "mfaAuthenticated": "true"
            }
        }
    }
}
```


RAM用户通过SDK停止ECS实例


```
{
    "apiVersion": "2014-05-26",
    "eventId": "e0cdf18f-e5ec-4c5f-b37c-99b608b9418c",
    "eventName": "StopInstance",
    "eventSource": "ecs-cn-hangzhou.aliyuncs.com",
    "eventTime": "2016-01-04T09:47:40Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "recipientAccountId": "4****",
    "requestId": "FC33D0AB-1C6B-4B4E-911D-E939122AA248",
    "requestParameters": {
        "ForceStop": "true",
        "InstanceId": "i-84udj****"
    },
    "serviceName": "Ecs",
```

```
    "sourceIpAddress": "42.120.XX.XX",
    "userAgent": "aliyuncli/2.0.6",
    "userIdentity": {
        "type": "ram-user",
        "accountId": "4****",
        "principalId": "28815334868278****",
        "userName": "B**",
        "accessKeyId": "IE8ITksrR3SD****"
    }
}
```


6.2 SLB

RAM用户通过控制台停止SLB实例


```
{
    "apiVersion": "2014-05-15",
    "eventId": "a8a6d6db-6bc8-4f4d-8b9e-7aaad259079d",
    "eventName": "DeleteLoadBalancer",
    "eventSource": "slb-pop.aliyuncs.com",
    "eventTime": "2016-01-04T09:48:49Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "recipientAccountId": "4****",
    "requestId": "AC792886-742C-4384-948E-24CE0026FC42",
    "requestParameters": {
        "LoadBalancerId": "1520c072d76-ap-southeast-os30****"
    },
    "serviceName": "Slb",
    "sourceIpAddress": "42.120.XX.XX",
    "userAgent": "AliyunConsole",
    "userIdentity": {
        "type": "ram-user",
        "accountId": "4****",
        "principalId": "28815334868278****",
        "userName": "B**",
        "sessionContext": {
            "attributes": {
                "creationDate": "2016-01-04T09:48:49Z",
                "mfaAuthenticated": "true"
            }
        }
    }
}
```


RAM用户通过SDK停止SLB实例


```
{
    "apiVersion": "2014-05-15",
    "eventId": "87b31697-aa12-4a0c-ad9c-c1b2b4c1a374",
    "eventName": "DeleteLoadBalancer",
    "eventSource": "slb-pop.aliyuncs.com",
    "eventTime": "2016-01-04T09:48:49Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
```

```
    "recipientAccountId": "4****",
    "requestId": "D090401A-7BF6-48C8-BC14-2E774436630C",
    "requestParameters": {
        "LoadBalancerId": "1520c072d76-ap-southeast-os30****"
    },
    "serviceName": "Slb",
    "sourceIpAddress": "42.120.XX.XX",
    "userAgent": "aliyuncli/2.0.6",
    "userIdentity": {
        "type": "ram-user",
        "accountId": "4****",
        "principalId": "28815334868278****",
        "accessKeyId": "55nCtAwmPLkk****",
        "userName": "B**"
    }
}
```

6.3 RAM

RAM用户通过控制台操作RAM

```
{
    "apiVersion":"2015-05-01",
    "eventId":"2cc52dee-d8d2-40c2-8de0-3a2cf1df****",
    "eventName":"DeleteGroup",
    "eventSource":"ram.aliyuncs.com",
    "eventTime":"2015-11-03T13:41:49Z",
    "eventType":"ApiCall",
    "eventVersion":"1",
    "requestId":"9AE24F49-C52C-4F0F-BCF9-9A4B8C22B147",
    "requestParameters":{
        "GroupName":"grp1",
    },
    "serviceName":"Ram",
    "sourceIpAddress":"42.120.XX.XX",
    "userAgent":"AliyunConsole",
    "userIdentity":{
        "type":"ram-user",
        "principalId":"27418064654829****",
        "accountId":"123456789012****",
        "userName":"Alice",
        "sessionContext":{
            "sessionAttributes":{
                "creationDate":"2015-11-03T13:41:48Z",
                "mfaAuthenticated":"true"
            }
        }
    }
}
```

RAM用户通过SDK操作RAM

```
{
    "apiVersion": "2015-05-01",
    "eventId": "234ef3c7-8938-4bd7-bb80-11754b7b****",
    "eventName": "CreateGroup",
    "eventSource": "ram.aliyuncs.com",
    "eventTime": "2016-01-04T08:58:50Z",
    "eventType": "ApiCall",
```

```
    "eventVersion": "1",
    "recipientAccountId": "4****",
    "requestId": "1485748C-DB62-4693-AB7E-4BA3F3A970E1",
    "requestParameters": {
        "Comments": "this is a test group",
        "GroupName": "grp1"
    },
    "serviceName": "Ram",
    "sourceIpAddress": "42.120.XX.XX",
    "userAgent": "aliyuncli/2.0.6",
    "userIdentity": {
        "type": "ram-user",
        "principalId": "27418064654829****",
        "accountId": "4****",
        "accessKeyId": "f6Iz********EI4d",
        "userName": "Alice"
    }
}
```


6.4 STS

RAM用户通过控制台调用STS切换角色


```
{
    "apiVersion": "2015-04-01",
    "eventId": "64e9b93e-13da-4ea4-8b72-081069ff4d8c",
    "eventName": "AssumeRole",
    "eventSource": "sts.aliyuncs.com",
    "eventTime": "2016-01-05T02:41:58Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "recipientAccountId": "102440540619****",
    "requestId": "F678C471-BEAA-4DE4-B09E-FD7F5A5248E8",
    "requestParameters": {
        "RoleArn": "acs:ram::43274:role/ram-admin",
        "RoleSessionName": "lisi"
    },
    "serviceName": "Sts",
    "sourceIpAddress": "42.120.74.96",
    "userAgent": "AliyunConsole",
    "userIdentity": {
        "type": "ram-user",
        "accountId": "102440540619****",
        "principalId": "24894915196108****",
        "userName": "lisi",
        "sessionContext": {
            "attributes": {
                "creationDate": "2016-01-05T02:41:58Z",
                "mfaAuthenticated": "true"
            }
        }
    }
}
```


RAM用户通过SDK调用STS

```
{
    "apiVersion": "2015-04-01",
    "eventId": "23f2a6b5-c628-49bb-8dc9-8f9760503bc6",
    "eventName": "AssumeRole",
    "eventSource": "sts.aliyuncs.com",
    "eventTime": "2016-01-05T02:41:58Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "recipientAccountId": "102440540619****",
    "requestId": "8BE01A78-4026-4E7D-B4E1-95B0323E968E",
    "requestParameters": {
        "RoleArn": "acs:ram::43274:role/ram-admin",
        "RoleSessionName": "lisi"
    },
    "serviceName": "Sts",
    "sourceIpAddress": "42.120.74.96",
    "userAgent": "aliyuncli/2.0.6",
    "userIdentity": {
        "type": "ram-user",
        "accountId": "102440540619****",
        "principalId": "24894915196108****",
        "accessKeyId": "55nCtAwmPLkk****",
        "userName": "lisi"
    }
}
```


6.5 ActionTrail

RAM用户通过控制台操作ActionTrail


```
{
    "apiVersion": "2015-09-28",
    "eventId": "b4e23d3c-9ba7-441e-ad25-04dd2d0aeb0f",
    "eventName": "UpdateTrail",
    "eventSource": "actiontrail.cn-hangzhou.aliyuncs.com",
    "eventTime": "2016-01-06T03:29:15Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "requestId": "3E2B90FE-0B7B-40FB-A9CE-5C80A3F1342F",
    "requestParameters": {
        "CreateNewBucket": "false",
        "Name": "default",
        "OssBucketName": "trail",
        "OssKeyPrefix": "",
        "Region": "cn-hangzhou",
        "RoleName": "aliyunactiontraildefaultrole",
        "StartLogging": "false"
    },
    "serviceName": "Actiontrail",
    "sourceIpAddress": "42.120.74.96",
    "userAgent": "AliyunConsole",
    "userIdentity": {
        "type": "ram-user",
        "principalId": "2881**********4898",
        "accountId": "4***4",
        "userName": "Bob",
        "sessionContext": {
```

```
            "attributes": {
                "creationDate": "2016-01-06T03:29:15Z",
                "mfaAuthenticated": "true"
            }
        }
    }
}
```

RAM用户通过SDK操作ActionTrail

```
{
    "apiVersion": "2015-09-28",
    "eventId": "aee5874f-1478-47df-932f-0ffd1851fc5f",
    "eventName": "UpdateTrail",
    "eventSource": "actiontrail.cn-hangzhou.aliyuncs.com",
    "eventTime": "2016-01-06T03:29:15Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "requestId": "0D690264-0D51-4B4F-8AEE-CDEB3ABD1929",
    "requestParameters": {
        "CreateNewBucket": "false",
        "Name": "default",
        "OssBucketName": "trail",
        "OssKeyPrefix": "",
        "Region": "cn-hangzhou",
        "RoleName": "aliyunactiontraildefaultrole",
        "StartLogging": "false"
    },
    "serviceName": "Actiontrail",
    "sourceIpAddress": "42.120.74.96",
    "userAgent": "aliyuncli/2.0.6",
    "userIdentity": {
        "type": "ram-user",
        "principalId": "2741**********2385",
        "accountId": "4***4",
        "accessKeyId": "f6Iz********EI4d",
        "userName": "Alice"
    }
}
```

6.6 CDN

RAM用户通过控制台调用CDN

```
{
    "apiVersion": "2014-11-11",
    "eventId": "1f869a5d-7542-4f76-94e0-5c24b520****",
    "eventName": "AddCdnDomain",
    "eventSource": "cdn.aliyuncs.com",
    "eventTime": "2016-01-05T03:30:58Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "recipientAccountId": "102440540619****",
    "requestId": "AF2FBB8D-64E1-4CC1-8849-E35C5BDB53A4",
    "requestParameters": {
```

```
        "CdnType": "web",
        "DomainName": "test2.jaso****.com",
        "SourceType": "oss",
        "Sources": "sampleshared.oss-cn-hangzhou.aliyuncs.com"
    },
    "serviceName": "Cdn",
    "sourceIpAddress": "42.120.XX.XX",
    "userAgent": "AliyunConsole",
    "userIdentity": {
        "type": "ram-user",
        "accountId": "102440540619****",
        "principalId": "24894915196108****",
        "userName": "lisi",
        "sessionContext": {
            "attributes": {
                "creationDate": "2016-01-05T03:30:58Z",
                "mfaAuthenticated": "false"
            }
        }
    }
}
```


RAM用户通过SDK调用CDN


```
{
    "apiVersion": "2014-11-11",
    "eventId": "1b6a3ec7-576b-435f-b249-9edca1e9****",
    "eventName": "AddCdnDomain",
    "eventSource": "cdn.aliyuncs.com",
    "eventTime": "2016-01-05T03:30:58Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "recipientAccountId": "102440540619****",
    "requestId": "179CDCB1-CC2D-496A-BE38-723CBAEA241A",
    "requestParameters": {
        "CdnType": "web",
        "DomainName": "test2.jaso****.com",
        "SourceType": "oss",
        "Sources": "sampleshared.oss-cn-hangzhou.aliyuncs.com"
    },
    "serviceName": "Cdn",
    "sourceIpAddress": "42.120.XX.XX",
    "userAgent": "aliyuncli/2.0.6",
    "userIdentity": {
        "type": "ram-user",
        "accountId": "102440540619****",
        "principalId": "24894915196108****",
        "accessKeyId": "55nCtAwmPLkk****",
        "userName": "lisi"
    }
}
```


6.7 KMS

通过控制台获取密钥信息


```
{
```

```
  "eventId": "122fa4a4-26b4-4ae5-bc87-8131edb7896e",
  "eventVersion": "1",
  "requestParameters": {
    "KeyId": "b22d0501-510e-4139-b665-c38cd3e1****"
  },
  "eventSource": "kms-intranet.cn-shanghai.aliyuncs.com",
  "sourceIpAddress": "42.120.XX.XX",
  "userAgent": "AliyunConsole",
  "userIdentity": {
    "accountId": "199655932609****",
    "principalId": "199655932609****",
    "userName": "root",
    "type": "root-account"
  },
  "eventType": "ApiCall",
  "referencedResources": {
    "Key": [
      "b22d0501-510e-4139-b665-c38cd3e1****"
    ]
  },
  "serviceName": "Kms",
  "apiVersion": "2016-01-20",
  "requestId": "122fa4a4-26b4-4ae5-bc87-8131edb7896e",
  "eventTime": "2018-07-24T09:19:28Z",
  "acsRegion": "cn-shanghai",
  "eventName": "DescribeKey"
}
```


使用SDK创建别名


```
{
  "eventId": "52253b9e-97ba-4e08-ae27-56d9892f2f82",
  "eventVersion": "1",
  "requestParameters": {
    "AliasName": "alias/monitor-9da5bffe-d846-49b5-b763-af3ebc5f6394",
    "KeyId": "9da5bffe-d846-49b5-b763-af3ebc5f****"
  },
  "eventSource": "kms.ap-southeast-2.aliyuncs.com",
  "sourceIpAddress": "42.120.XX.XX",
  "userAgent": "Go-http-client/1.1",
  "userIdentity": {
    "accessKeyId": "uG1lPdiFFwfq****",
    "accountId": "199655932609****",
    "principalId": "231824559326 59****",
    "userName": "monitor_user",
    "type": "ram-user"
  },
  "eventType": "ApiCall",
  "referencedResources": {
    "Key": [
      "9da5bffe-d846-49b5-b763-af3ebc5f****"
    ]
  },
  "serviceName": "Kms",
  "apiVersion": "2016-01-20",
  "requestId": "52253b9e-97ba-4e08-ae27-56d9892f2f82",
  "eventTime": "2018-07-24T09:13:04Z",
  "acsRegion": "ap-southeast-2",
  "eventName": "CreateAlias"
}
```