ALIBABA CLOUD

Alibaba Cloud

操作审计

历史事件管理

文档版本：20200825

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.查询历史事件

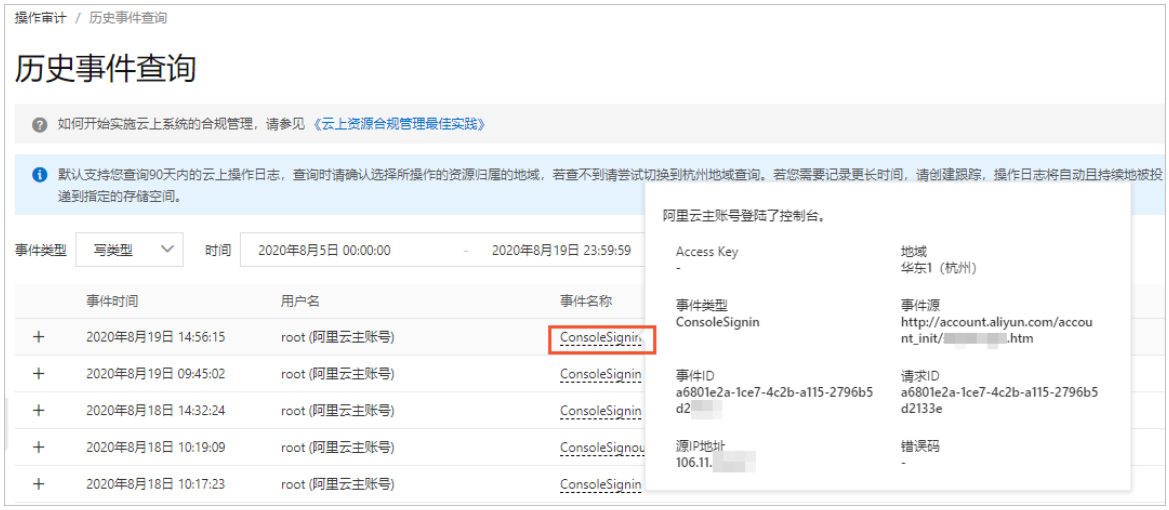
1.1. 通过操作审计控制台或API查询历史事件

操作审计默认为每个阿里云账号记录最近90天的历史事件，您可以通过操作审计控制台或API查询。此外，您还可以从操作审计控制台下载最近90天的历史事件。

> **说明** 只有单账号跟踪的历史事件可以通过操作审计控制台或API查询，且每秒最多可以查询两次。多账号跟踪的历史事件不能通过操作审计控制台或API查询，只能在对应的OSS Bucket或SLS Logstore中查询。

通过操作审计控制台查询历史事件

1. 登录操作审计控制台。
2. 在顶部导航栏选择您想查询的历史事件的地域。
3. 在左侧导航栏，单击**操作审计 > 历史事件查询**，查询最近90天的历史事件。
4. 在**历史事件查询**页面找到待查询的事件，鼠标悬停至**事件名称**，查询事件详情。



5. 如果需要查询事件代码记录，您可以单击历史事件前面的加号，单击**查看事件**。

> **说明** 您可以设置事件类型、用户名、事件名称、资源类型、资源名称、产品类型、Access Key以及时间范围等高级搜索条件来过滤查询事件。全局事件可以在所有地域的历史事件中查询到。

通过API查询历史事件

您可以通过调用LookupEvents接口查询最近90天的历史事件。

1.2. 在存储空间中查询历史事件

如果您创建了跟踪并将日志投递到OSS Bucket或SLS Logstore，您可以前往对象存储OSS或日志服务SLS控制台查看已投递的日志，或使用OSS或SLS的OpenAPI对日志进行读取和分析。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，单击跟踪列表。
3. 找到您创建的跟踪。
   - 单击日志分析可跳转到您已设置的SLS Logstore。
   - 单击日志报表可跳转到SLS Logstore对应的报表看板地址，查看您的日志报表。
   - 单击OSS Bucket名称可跳转到对应的OSS Bucket，查看已投递的日志文件。

> 说明 您也可以使用OSS和SLS提供的OpenAPI以编程方式读取、分析操作事件。

1.3. 在云产品控制台查询历史事件

操作审计已与云服务器ECS、区块链、负载均衡、配置审计等云产品集成，您可以在这些云产品的控制台查询最近90天的资源历史事件。如需查询更长时间的历史事件，请在操作审计控制台创建跟踪并投递到对象存储或日志服务。

在ECS控制台查询历史事件

1. 登录ECS管理控制台。
2. 在左侧导航栏，单击实例。
3. 单击实例右侧的管理。

4. 在实例详情页中单击本实例操作记录查询历史事件。

在区块链服务控制台查询历史事件

1. 登录区块链服务控制台。
2. 在左侧导航栏，单击Hyperledger Fabric、蚂蚁区块链、企业以太坊下的日志查询历史事件。

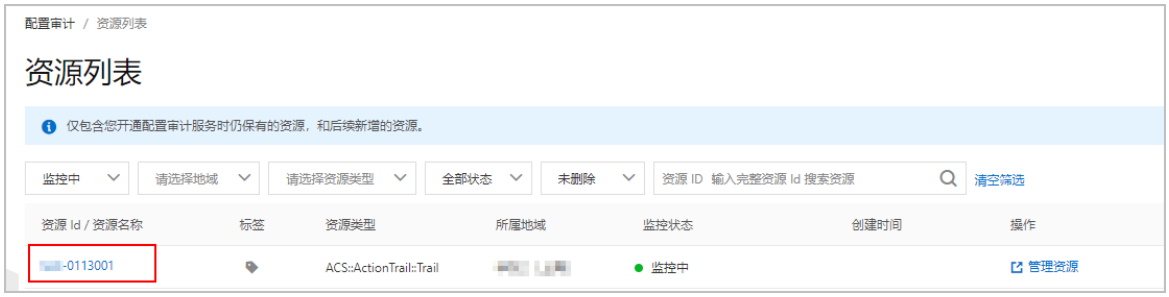
在负载均衡控制台查询历史事件

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择日志管理>操作日志查询历史事件。

在配置审计控制台查询历史事件

您可以在配置审计控制台查询资源某一次变更相关的历史事件。

1. 登录配置审计控制台。
2. 在左侧导航栏，单击资源列表。
3. 在资源Id/资源名称列，单击您要查询的资源。



4. 选择**配置时间线>操作审计**查询历史事件。

2.操作事件结构定义

本文为您介绍一个操作事件包含的关键字段及其含义，并为您提供相关的示例。

操作事件的关键字段

名称	类型	是否必选	示例	描述
acsRegion	String	必选	cn-hangzhou	阿里云地域。
apiVersion	String	是	2014-05-26	当eventType的取值是*ApiCall*，操作事件代表一个API的调用。此时，该字段为API的版本信息。
eventId	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。
eventName	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。
eventSource	String	是	ecs.aliyuncs.com	事件来源。
eventTime	String	是	2020-01-09T12:12:14Z	事件的发生时间（UTC格式）。
eventType	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。
eventVersion	String	是	1	操作事件格式的版本，当前版本为1。

名称	类型	是否必选	示例	描述
errorCode	String	否	NoPermission	云服务处理API请求发生错误时，记录的错误码。·
errorMessage	String	否	You are not authorized.	云服务处理API请求发生错误时，记录的错误消息。
requestId	String	是	F23A3DD5-7842-4EF9-9DA1-3776396AD58D	请求ID。
requestParameters	字典	否	不涉及	API请求的输入参数。
responseElements	字典	否	不涉及	API响应的数据。
referencedResources	字典	否	不涉及	事件影响的资源列表。
serviceName	String	是	Ecs	事件相关的云服务名称。
sourceIpAddress	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。
userAgent	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)*。
userIdentity	字典	是	不涉及	请求者的身份信息。

userIdentity包含的字段如下表所示。

名称	类型	是否必选	示例	描述

名称	类型	是否必选	示例	描述
type	String	是	ram-user	身份类型。当前支持的身份类型包括： • *root-account*：阿里云主账号。 • *ram-user*：RAM 用户。 • *assumed-role*：RAM角色。 • *system*：阿里云服务。
principalId	String	是	28815334868278****	当前请求者的ID。 • 如果type的取值是*root-account*，则记录阿里云主账号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。
accountId	String	是	112233445566****	阿里云主账号ID。
accessKeyId	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。
userName	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。
sessionContext	String	否	{"attributes": {"mfaAuthenticated": "true", "creationDate": "2015-12-31T06:33:14Z" }	请求者通过临时安全令牌调用API或通过控制台登录时记录该字段。该字段的内容包括： • `creationDate`：创建时间。 • `mfaAuthenticated`：用户登录控制台时是否使用多因素认证。

示例


```
{
"eventId": "F23A3DD5-7842-4EF9-9DA1-3776396A****",
"responseElements": {
"RequestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
"NetworkInterfaceId": "eni-bp12f9rjb****ktzjqau"
},
"eventVersion": "1",
```

```
"requestParameters": {
"securityToken": "********",
"Tag.1.Key": "CreatedBy",
"RequestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
"SecurityGroupId": "sg-bp10mvd8****lfks143r",
"Tag.1.Value": "StreamCompute",
"VSwitchId": "vsw-bp1iqqmaj4****2c81noh",
"RegionId": "cn-hangzhou",
"SignatureType": "",
"stsTokenPlayerUid": 165266****475569
},
"eventSource": "ecs.aliyuncs.com",
"sourceIpAddress": "11.***.***.232",
"userIdentity": {
"sessionContext": {
"attributes": {
"mfaAuthenticated": "false",
"creationDate": "2020-01-09T12:12:14Z"
}
},
"accessKeyId": "STS.NUnj6********aEoMZGsTnuqK",
"accountId": "116214****628250",
"principalId": "3164566****6066448:116214****628250",
"userName": "aliyunstreamdefaultrole:116214****628250",
"type": "assumed-role"
},
"eventType": "ApiCall",
"referencedResources": {
"VSwitch": [
"vsw-bp1iqqma****402c81noh"
],
"SecurityGroup": [
"sg-bp10mvd****6lfks143r"
]
},
"serviceName": "Ecs",
"additionalEventData": {
"Scheme": "http"
},
"apiVersion": "2014-05-26",
"requestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D"
```

```
"requestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
"eventTime": "2020-01-09T12:12:14Z",
"acsRegion": "cn-hangzhou",
"eventName": "CreateNetworkInterface",
"__expanded": true
}
```

3.操作事件示例

3.1. ECS

本文为您提供几个ECS操作事件的相关示例。

RAM用户通过控制台停止ECS实例


```
{
"apiVersion": "2014-05-26",
"eventId": "f4788483-70fc-476b-839b-af5ed111****",
"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-99b608b9****",
"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****"
}
}
```


3.2. RDS

本文为您提供几个RDS操作事件的相关示例。

RAM用户通过控制台重启RDS实例

```
{
"apiVersion": "2014-08-15",
"eventId": "2687bb47-548b-4338-8c0c-e839cd80****",
"eventName": "RestartDBInstance",
"eventSource": "rds-cn-hangzhou.aliyuncs.com",
"eventTime": "2016-01-04T09:48:13Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "4****",
"requestId": "EC7BC9A6-C198-4187-AA52-61519826A3D5",
"requestParameters": {
"DBInstanceId": "rds43zn9z7w7qrq2****"
},
"serviceName": "Rds",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"type": "ram-user",
"accountId": "4****",
"principalId": "28815334868278****",
"userName": "***",
"sessionContext": {
"attributes": {
"creationDate": "2016-01-04T09:48:13Z",
"mfaAuthenticated": "true"
}
}
}
}
```


RAM用户通过SDK重启RDS实例

```
{
"apiVersion": "2014-08-15",
"eventId": "b14e6544-c5c0-47bd-a81f-893b7567****",
"eventName": "RestartDBInstance",
"eventSource": "rds-cn-hangzhou.aliyuncs.com",
"eventTime": "2016-01-04T09:48:13Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "4****",
"requestId": "804431E9-3912-4544-B0F8-8737532D0117",
"requestParameters": {
"DBInstanceId": "rds43zn9z7w7qrq2****"
},
"serviceName": "Rds",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"accountId": "4****",
"principalId": "28815334868278****",
"userName": "***",
"accessKeyId": "I8EITksrR3S****"
}
}
```


3.3. SLB

本文为您提供几个SLB操作事件的相关示例。

RAM用户通过控制台停止SLB实例

```
{
"apiVersion": "2014-05-15",
"eventId": "a8a6d6db-6bc8-4f4d-8b9e-7aaad259****",
"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-c1b2b4c1****",
"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**"
}
}
```


3.4. CDN

本文为您提供几个CDN操作事件的相关示例。

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"
}
}
```


3.5. RAM

本文为您提供几个RAM操作事件的相关示例。

RAM用户通过控制台删除用户组

```
{
"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":"****",
"sessionContext":{
"sessionAttributes":{
"creationDate":"2015-11-03T13:41:48Z",
"mfaAuthenticated":"true"
}
}
}
}
```


RAM用户通过SDK创建用户组

```
{
"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": "****"
}
}
```


3.6. STS

本文为您提供几个STS操作事件的相关示例。

RAM用户通过控制台调用STS切换角色

```
{
"apiVersion": "2015-04-01",
"eventId": "64e9b93e-13da-4ea4-8b72-081069ff****",
"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::4****:role/ram-admin",
"RoleSessionName": "l****"
},
"serviceName": "Sts",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"type": "ram-user",
"accountId": "102440540619****",
"principalId": "24894915196108****",
"userName": "l****",
"sessionContext": {
"attributes": {
"creationDate": "2016-01-05T02:41:58Z",
"mfaAuthenticated": "true"
}
}
}
}
```


RAM用户通过SDK调用STS切换角色

```
{
"apiVersion": "2015-04-01",
"eventId": "23f2a6b5-c628-49bb-8dc9-8f976050****",
"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::4****:role/ram-admin",
"RoleSessionName": "l****"
},
"serviceName": "Sts",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"accountId": "102440540619****",
"principalId": "24894915196108****",
"accessKeyId": "55nCtAwmPLkk****",
"userName": "l***"
}
}
```


3.7. KMS

本文为您提供几个KMS操作事件的相关示例。

通过控制台获取密钥信息

```
{
"eventId": "122fa4a4-26b4-4ae5-bc87-8131edb7****",
"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-ae27-56d9892f****",
"eventVersion": "1",
"requestParameters": {
"AliasName": "alias/monitor-9da5bffe-d846-49b5-b763-af3ebc5f****",
"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": "23182455932659****",
"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"
}
```


3.8. ActionTrail

本文为您提供几个ActionTrail操作事件的相关示例。

RAM用户通过控制台更新跟踪

```
{
"apiVersion": "2015-09-28",
"eventId": "b4e23d3c-9ba7-441e-ad25-04dd2d0a****",
"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.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"type": "ram-user",
"principalId": "28815334868278****",
"accountId": "4****",
"userName": "B****",
"sessionContext": {
"attributes": {
"creationDate": "2016-01-06T03:29:15Z",
"mfaAuthenticated": "true"
}
}
}
}
```


RAM用户通过SDK更新跟踪

```
{
"apiVersion": "2015-09-28",
"eventId": "aee5874f-1478-47df-932f-0ffd1851****",
"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.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"principalId": "27418064654829****",
"accountId": "4****",
"accessKeyId": "f6IzzFZMmzNw****",
"userName": "A****"
}
}
```


3.9. ConsoleSignin

本文为您提供几个ConsoleSignin操作事件的相关示例。

RAM用户登录

- 登录成功

```
{
"additionalEventData": {
"callbackUrl": "https://home.console.aliyun.com/",
"mfaChecked": "true"
},
"eventId": "93e806df-a005-40a8-b6b1-f58004ae****",
"eventName": "ConsoleSignin",
"eventSource": "signin.aliyun.com",
"eventTime": "2016-01-20T01:47:45Z",
"eventType": "ConsoleSignin",
"eventVersion": "1",
"requestId": "621948aa-c03a-4acd-b4b0-116a9fa3257a",
"serviceName": "Aas",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36",
"userIdentity": {
"accountId": "112233445566****",
"principalId": "28815334868278****",
"type": "ram-user",
"userName": "z****"
}
}
```


- 登录失败

```
{
"additionalEventData": {
"callbackUrl": "https://home.console.aliyun.com/",
"mfaChecked": "false"
},
"errorCode": "Authentication.Failed",
"errorMessage": "Failed authentication.",
"eventId": "f31de4a1-fb34-4299-b2e1-aee8803c****",
"eventName": "ConsoleSignin",
"eventSource": "signin.aliyun.com",
"eventTime": "2016-01-20T04:17:23Z",
"eventType": "ConsoleSignin",
"eventVersion": "1",
"requestId": "7fecff6c-5ca0-4be5-99b4-61dc7e1d984c",
"serviceName": "Aas",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36",
"userIdentity": {
"accountId": "112233445566****",
"principalId": "28815334868278****",
"type": "ram-user",
"userName": "z****"
}
}
```


主账号登录

登录成功

```
{
"additionalEventData": {
"isMFAChecked": false,
"loginAccount": "testuser@aliyun.com"
},
"eventId": "a53844f9-7d41-4c39-aaf7-350e04ca****",
"eventName": "ConsoleSignin",
"eventSource": "account.aliyun.com",
"eventTime": "2016-01-20T01:48:58Z",
"eventType": "ConsoleSignin",
"eventVersion": "1",
"requestId": "00693be9-3e1c-4d77-84a0-025d44add80b",
"serviceName": "Aas",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/47.0.2526.106 Safari/537.36",
"userIdentity": {
"accountId": "123456789012****",
"principalId": "123456789012****",
"type": "root-account"
}
}
```