ALIBABA CLOUD

阿里云

操作审计

操作审计公共云合集

文档版本：20220708

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.动态与公告 08
1.1. 新功能发布记录 08
1.2. 产品公告 12
2.快速入门 13
3.管理权限 15
3.1. 为RAM用户授权 15
3.2. 操作审计服务关联角色 18
3.3. 操作事件投递的系统权限策略 20
4.事件记录的内容 24
4.1. 管控事件结构定义 24
4.2. Insight事件结构定义 32
4.3. 操作审计支持被审计的事件说明 34
4.4. 登录事件示例 37
4.4.1. 阿里云账号登录事件 37
4.4.2. RAM用户登录事件 39
4.5. 角色扮演事件示例 42
4.5.1. 容器服务通过角色扮演创建TCP监听 42
4.5.2. RAM用户角色扮演 44
4.5.3. 通过角色扮演查询操作审计的事件 46
4.5.4. 通过角色SSO进行角色扮演 48
4.5.5. 通过角色SSO查询操作审计事件 50
4.6. 订单相关事件 52
4.6.1. 资源购买事件 52
4.6.2. 资源续费事件 54
4.6.3. 资源变配事件 56
4.6.4. 资源释放事件 58

4.7. 常见云服务事件示例 59
4.7.1. CDN 59
4.7.2. ECS 65
4.7.3. KMS 72
4.7.4. OSS 76
4.7.5. RDS 84
4.7.6. SLB 93
4.7.7. IMS 101
4.7.8. STS 107
4.7.9. ActionTrail 112
5.智能分析Insight事件 119
5.1. Insight事件视频指导 119
5.1.1. 开通Insight事件 119
5.1.2. 使用Insight事件 119
5.2. Insight事件概览 119
5.3. 通过操作审计控制台查询Insight事件 124
5.4. 通过SLS或OSS控制台查询Insight事件 125
6.事件告警 128
6.1. 事件告警概览 128
6.2. 启用并设置事件告警 128
6.3. 基础操作 136
6.3.1. 管理内容模板 136
6.3.2. 管理行动策略 139
6.3.3. 创建自定义告警规则 141
6.3.4. 管理告警规则 144
7.多账号跟踪（适用于企业用户） 147
7.1. 多账号跟踪概览 147
7.2. 管理委派管理员账号 148

7.3. 创建多账号跟踪 150
7.4. 更新多账号跟踪 153
7.5. 删除多账号跟踪 154
7.6. 关闭多账号跟踪 154
8.跨账号投递事件 156
8.1. 将资源目录中多个成员的事件投递到同一账号 156
8.2. 将多个阿里云账号的事件投递到同一账号 160
9.历史事件投递任务 164
9.1. 创建历史事件投递任务 164
10.AccessKey审计 165
10.1. AccessKey审计概览 165
10.2. 查询AccessKey日志 165
10.3. AccessKey审计支持的云服务及事件 166
11.API参考 167
11.1. API概览 167
11.2. 附录 167
11.2.1. 通过VPC调用API 167
12.SDK参考 170
12.1. SDK概览 170
12.2. Java SDK示例 170
13.教程 173
13.1. 通过RAM对操作审计进行权限管理 173
13.2. 使用操作审计监控AccessKey的使用 174
13.3. 使用操作审计监控阿里云账号的使用 177
13.4. 使用DLA分析OSS中的事件 179
13.5. 将事件持续投递到指定服务 183
13.6. 在日志服务SLS中分析操作事件 186
13.7. 使用操作审计查询事件 189

13.8. 下载操作审计的事件 190
13.9. 使用SDK创建跟踪 193
13.10. 使用Terraform自动化创建跟踪 196
13.11. 使用操作审计为资源自动绑定标签 198
13.12. 长期存储完整的事件 201

1.动态与公告

1.1. 新功能发布记录

本文介绍了操作审计（ActionTrail）产品主要功能的发布时间、发布地域和相关文档。

2021年12月

功能名称	功能描述	发布时间	发布地域	相关文档
基于场景进行事件高级查询	在支持自定义查询事件的基础上，操作审计新增支持基于场景进行事件高级查询： • 查询阿里云账号或AccessKey相关事件 • 查询CIS标准相关事件 • 查询资源生命周期事件	2021-12	全部地域	• 查询阿里云账号或AccessKey相关事件 • 查询CIS标准相关事件 • 查询资源生命周期事件

2021年11月

功能名称	功能描述	发布时间	发布地域	相关文档
基于事件的自定义告警	操作审计支持基于事件创建自定义告警规则。您可以通过撰写SQL和设置阈值来自定义告警项。	2021-11	全部地域	创建自定义告警规则

2021年08月

功能名称	功能描述	发布时间	发布地域	相关文档
智能分析Insight事件	智能分析Insight事件功能帮助您从管控事件中发现异常行为，及时洞察云上管控风险并尽快采取补救措施。启用Insight事件后，操作审计将基于管控事件识别异常并生成Insight事件，然后将Insight事件投递到日志服务SLS或对象存储OSS。 说明 您需要通过提交工单，获取Insight事件的使用权限。	2021-08	除华南2（河源）、华南3（广州）和阿联酋（迪拜）外的其他地域	Insight事件概览

2021年04月

功能名称	功能描述	发布时间	发布地域	相关文档
事件告警	当您创建跟踪并投递到SLS Logstore时，可以基于跟踪设置事件告警。当敏感操作或异常操作发生时，您可以收到告警并及时响应。	2021-04	全部地域	事件告警概览

2021年03月

功能名称	功能描述	发布时间	发布地域	相关文档
跨账号投递事件	操作审计支持将多个阿里云账号或资源目录中多个成员的事件投递到同一账号的日志服务SLS或对象存储OSS中，从而实现统一的审计数据归档和监控。	2021-03	全部地域	• 将资源目录中多个成员的事件投递到同一账号 • 将多个阿里云账号的事件投递到同一账号
平台操作审计支持新的服务和事件字段	• 平台操作审计功能新增支持密钥管理服务KMS、数据安全中心DSC。 • 平台操作事件新增EmployeeID字段，表示平台工作人员实际操作人的内部工号密文。	2021-03	全部地域	• 平台操作审计概览 • 平台操作事件结构定义

2021年01月

功能名称	功能描述	发布时间	发布地域	相关文档
历史事件投递任务	将操作审计平台已记录的90天历史事件投递到日志服务SLS，以便分析或下载最近90天的历史事件。	2021-01	全部地域	创建历史事件投递任务

2020年12月

功能名称	功能描述	发布时间	发布地域	相关文档
事件高级查询	当您创建跟踪并投递到SLS Logstore时，可以基于跟踪对事件进行高级查询。您可以跨多个地域、多个产品、多个条件综合查询超过90天的事件。	2020-12	全部地域	自定义查询事件

2020年10月

功能名称	功能描述	发布时间	发布地域	相关文档
事件聚合搜索	操作审计控制台新增事件聚合搜索功能，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。	2020-10	全部地域	事件聚合查询

2020年09月

功能名称	功能描述	发布时间	发布地域	相关文档

实践场景	操作审计控制台新增实践场景页面，为您提供创建跟踪、分析事件等最佳实践案例。	2020-09	全部地域	• 基础入门
				  ○ 将事件持续投递到指定服务
				  ○ 使用操作审计查询事件
				  ○ 使用Terraform自动化创建跟踪
				• 数据分析
				  ○ 使用DLA分析OSS中的事件
				  ○ 在日志服务SLS中分析事件
				• 安全场景
				  ○ 使用操作审计监控AccessKey的使用
				  ○ 使用操作审计监控阿里云账号的使用
				• 事件响应与自动化
				使用操作审计为资源自动绑定标签

2020年08月

功能名称	功能描述	发布时间	发布地域	相关文档
优化跟踪功能	支持在某个地域查看所有地域中创建的跟踪，方便您管理跟踪。同时更新了创建跟踪的操作方法。	2020-08	全部地域	• 创建单账号跟踪 • 创建多账号跟踪

2020年07月

功能名称	功能描述	发布时间	发布地域	相关文档
新增事件注释	对事件进行简要说明，如事件源（产品）、操作者、事件名称等。	2020-07	全部地域	通过操作审计控制台查询事件

2020年03月

功能名称	功能描述	发布时间	发布地域	相关文档
多账号跟踪	支持企业将资源目录内的所有成员的操作日志统一投递到日志服务SLS或对象存储OSS。	2020-03	全部地域	• 多账号跟踪概览 • 创建多账号跟踪

2020年02月

功能名称	功能描述	发布时间	发布地域	相关文档
增加支持的云服务	接入更多云服务事件。	2020-02	全部地域	支持的云服务
在线事件查询引擎优化	支持设置多个查询条件，同一个条件支持取多个值。	2020-02	全部地域	通过操作审计控制台查询事件

2020年01月

功能名称	功能描述	发布时间	发布地域	相关文档
日志投递通知	支持您订阅投递事件的通知，当操作审计向您指定的OSS存储空间投递日志文件时，您可通过MNS Topic接收通知。	2020-01	全部地域	创建单账号跟踪
OSS服务端加密	支持为日志投递到OSS存储空间开启服务端加密。	2020-01	全部地域	创建单账号跟踪

2019年12月

功能名称	功能描述	发布时间	发布地域	相关文档
与ECS控制台集成	您可以在ECS控制台的实例详情页面查看实例对应的操作日志。	2019-12	全部地域	通过ECS控制台查询事件
支持创建多个跟踪	每个区域最多可创建5个跟踪，可根据实际需要分别跟踪不同地域的事件、不同的事件类型并投递到不同的存储空间。	2019-12	全部地域	创建单账号跟踪
支持跟踪部分地域的事件	您可以创建跟踪，根据您的实际需要选择仅追踪一个或部分地域的事件。	2019-12	全部地域	创建单账号跟踪
支持在线查询最近90天日志	不创建跟踪，默认支持在线查询日志天数从30天提升至90天。如果需要更长期的存储和查询，您需要创建跟踪。	2019-12	全部地域	通过操作审计控制台查询事件

2019年11月

功能名称	功能描述	发布时间	发布地域	相关文档
操作审计支持免开通	所有阿里云有效账号免开通。	2019-11	全部地域	计费说明
最佳实践	操作审计最佳实践上线，引导您使用操作审计的同时，了解更多云上合规审计的信息。	2019-11	全部地域	• 使用操作审计监控AccessKey的使用 • 使用操作审计监控阿里云账号的使用

2019年10月

功能名称	功能描述	发布时间	发布地域	相关文档
增加支持的云服务	接入更多云服务事件。	2019-10	全部地域	支持的云服务

2019年09月

功能名称	功能描述	发布时间	发布地域	相关文档
平台操作日志	阿里云向您开放部分由平台发起对您云上资源的操作日志，提升云平台运维的可见性。当前仅支持对象存储OSS，需提工单申请方能使用。	2019-9	中国站地域	开通平台操作审计

1.2. 产品公告

操作审计（ActionTrail）帮助您监控并记录阿里云账号对云上产品和服务的访问和使用行为事件，事件数据将默认使用在本文所示的场景列表中。
以下场景中的云产品将查询并使用操作审计的事件，但不会对您的产品功能使用及费用支出产生任何影响。

场景	说明
云服务器ECS（Elastic Compute Service）运维支持场景	阿里云运维人员处理工单问题时，可能需要从您操作ECS的事件记录中获取操作详情，以便快速解决您的问题。此外，通过分析ECS异常和错误行为，可以帮助阿里云业务人员优化产品设计，为您提供更好的产品体验。 在ECS运维支持场景中，ECS服务会获取并留存最长3年的ECS操作事件。
弹性容器实例ECI（Elastic Container Instance）运维支持场景	阿里云运维人员处理工单问题时，可能需要从您操作ECI的事件记录中获取操作详情，以便快速解决您的问题。此外，通过分析ECI异常和错误行为，可以帮助阿里云业务人员优化产品设计，为您提供更好的产品体验。 在ECI运维支持场景中，ECI服务会获取并留存最长3年的ECI操作事件。

2.快速入门

操作审计（ActionTrail）帮助您监控并记录阿里云账号的活动。首次使用操作审计时，您可以创建跟踪将事件投递到日志服务SLS或对象存储OSS，然后创建历史事件投递任务将最近90天的事件投递到SLS，以便长期存储完整的事件。您也可以通过操作审计控制台查询多个地域超过90天的事件。

前提条件

- 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。
- 请确保您已经通过提交工单，获取历史事件投递任务和Insight事件的使用权限。

步骤一：创建跟踪

本文以创建单账号跟踪并投递到日志服务SLS为例，为您介绍如何创建您的第一个跟踪。

您也可以创建多账号跟踪，或者将跟踪投递到对象存储OSS。更多信息，请参见创建单账号跟踪和创建多账号跟踪。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在顶部菜单栏，选择您想创建单账号跟踪的地域。

   > **说明** 该地域将成为单账号跟踪的Home地域，即创建跟踪的地域。

4. 在**跟踪列表**页面，单击**创建跟踪**。
5. 在**跟踪基本属性**页面，输入**跟踪名称**，将管控事件的**事件类型**设置为**所有事件**，选中**Insight事件**，然后单击**下一步**。
6. 在**审计事件投递**页面，选择**将事件投递到日志服务SLS**，然后选择**投递到本账号**，设置如下参数。

参数	描述
日志库所属地域	日志项目所在地域。
日志项目名称	日志服务SLS中日志项目的名称。同一账号下，日志项目名称不能重复。 ○ 当您选中**创建新的日志项目**时，将通过操作审计控制台新建日志项目，输入日志项目名称。 ○ 当您选中**选择已有的日志项目**时，在日志服务SLS中选择已有日志项目名称。关于如何在日志服务SLS中新建日志项目，请参见快速入门。

7. 单击**下一步**。
8. 在**预览并创建**页面，确认跟踪信息，然后单击**提交**。

步骤二：创建历史事件投递任务

创建跟踪仅能投递跟踪创建时间之后的事件，为了将最近90天的事件进行完整的存储，您还需创建历史事件投递任务，补投递跟踪创建时间往前一段时间的事件。

关于历史事件投递任务的更多信息，请参见创建历史事件投递任务。

1. 在左侧导航栏，单击**历史事件投递任务**。
2. 在顶部导航栏选择您需要投递历史事件的地域。

> **说明** 该地域必须与跟踪所在地域相同。

3. 在**历史事件投递任务**页面，单击**创建任务**。
4. 在**创建任务**页面，选择跟踪。

> **说明** 选择跟踪后，系统将自动填入跟踪的地域、日志项目地域、日志项目名称和日志库信息。

5. 单击**确定**。

   创建任务后，您可以在**历史事件投递任务**页面查看关联跟踪、可补历史事件范围、投递状态、任务创建时间、任务完成时间等信息。

步骤三：进行事件高级查询

操作审计提供事件基础查询、事件聚合查询和事件高级查询等多种事件查询方式。本文以事件高级查询为例为您介绍如何通过操作审计控制台查询事件。

关于事件基础查询、事件聚合查询的更多信息，请参见事件基础查询和事件聚合查询。

1. 在左侧导航栏，单击**跟踪列表**。
2. 在**跟踪列表**页面，单击目标跟踪名称。
3. 单击**启用高级功能**右侧的**设置**。
4. 在左侧导航栏，单击**事件高级查询**。
5. 在顶部导航栏选择您想进行事件高级查询的地域。
6. 在**事件高级查询**页面，单击**自定义查询**页签，然后查询事件。

> **说明** 如果不设置筛选条件，默认查询全部事件。

方式一：通用模式（默认） 方式二：简洁模式

后续步骤

当您将事件投递到SLS或OSS后，可以通过SLS或OSS查询或分析事件。具体操作，请参见：

- 通过SLS或OSS控制台查询事件
- 通过SLS控制台分析事件
- 通过DLA分析OSS中的事件

3.管理权限

3.1. 为RAM用户授权

您可以授予RAM用户访问和管理操作审计的权限，包括查询事件、管理跟踪、管理事件告警等。

前提条件

- 请确保您已创建RAM用户。具体操作，请参见创建RAM用户。
- 请确保您已创建操作审计服务关联角色（AliyunServiceRoleForActionTrail）。具体操作，请参见创建服务关联角色。

操作步骤

1. 登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，单击目标RAM用户**操作**列的**添加权限**。
4. 在**添加权限**面板，选择**授权应用范围**为**整个云账号**，然后选择权限策略。
   - **系统策略**：从**权限策略名称**列表，选择需要的权限。

权限策略名称	说明
AliyunActionTrailReadOnlyAccess	查看操作审计
AliyunActionTrailFullAccess	管理操作审计
AliyunOSSReadOnlyAccess	查看对象存储
AliyunLogReadOnlyAccess	查询日志服务

   - **自定义策略**：从**权限策略名称**列表，选择需要的权限。
     关于如何创建自定义策略，请参见创建自定义权限策略。

- 示例一：授予RAM用户操作审计的所有权限，以及获取OSS Bucket列表和SLS Project列表的权限，以便管理跟踪。
  示例代码：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "actiontrail:*",
                "oss:GetService",
                "log:ListProject"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

  权限说明：

Action	说明
oss:GetService	获取OSS Bucket列表的权限
log:ListProject	获取SLS Project列表的权限
actiontrail:*	操作审计所有操作的权限

- 示例二：授予RAM用户管理跟踪和在日志服务SLS中管理Logstore、索引、看板、图表、日志项目的相关权限，以便管理事件告警。
  示例代码：

```
{
    "Version": "1",
    "Statement": [
      {
     "Effect": "Allow",
     "Action": [
       "actiontrail:DescribeTrails",
       "actiontrail:SetDefaultTrail",
       "actiontrail:GetDefaultTrail",
       "actiontrail:CreateTrail"
     ],
     "Resource": "*"
     },
   {
     "Effect": "Allow",
     "Action": [
       "log:CreateLogStore",
       "log:CreateIndex",
       "log:UpdateIndex"
     ],
     "Resource": [
       "acs:log:*:*:project/Project名称/logstore/internal-alert-history",
       "acs:log:*:*:project/sls-alert-*/logstore/internal-alert-center-log"
     ]
     },
   {
     "Effect": "Allow",
     "Action": [
       "log:CreateDashboard",
       "log:CreateChart",
       "log:UpdateDashboard"
     ],
     "Resource": "acs:log:*:*:project/Project名称/dashboard/*"
   },
   {
     "Effect": "Allow",
     "Action": [
       "log:*"
     ],
     "Resource": "acs:log:*:*:project/Project名称/job/*"
     },
   {
     "Effect": "Allow",
     "Action": [
       "log:CreateProject"
     ],
     "Resource": [
       "acs:log:*:*:project/sls-alert-*"
     ]
   }
 ]
}
```

权限说明：

Action	说明
actiontrail:DescribeTrails	查询跟踪
actiontrail:SetDefaultTrail	设置事件告警的默认跟踪
actiontrail:GetDefaultTrail	获取事件告警的默认跟踪
actiontrail:CreateTrail	创建跟踪
log:CreateLogstore	创建Logstore
log:CreateIndex	创建索引
log:UpdateIndex	更新索引
log:CreateDashboard	创建看板
log:CreateChart	创建图表
log:UpdateDashboard	更新看板
log:CreateProject	创建日志项目

5. 单击**确定**。
6. 单击**完成**。

3.2. 操作审计服务关联角色

本文为您介绍操作审计服务关联角色（AliyunServiceRoleForActionTrail）的应用场景、权限策略及相关操作。

应用场景

操作审计服务关联角色（AliyunServiceRoleForActionTrail）的应用场景如下：

- 访问日志服务SLS（Log Service）
  当您创建跟踪并设置了SLS Project地址用于接收操作事件时，操作审计需要向您指定的SLS Project创建Logstore并写入操作事件，需要通过服务关联角色获取写入SLS Logstore的权限。
- 访问对象存储OSS（Object Storage Service）
  当您创建跟踪并设置了OSS存储空间用于接收操作事件时，操作审计需要向您指定的OSS存储空间写入操作事件，需要通过服务关联角色获取写入OSS存储空间的权限。
- 访问消息服务MNS（Message Notification Service）
  当您创建跟踪并设置了OSS存储空间用于接收操作事件时，您可以设置当投递发生时向您的MNS主题推送消息。操作审计需向对应默认的MNS主题写入消息事件，需要通过服务关联角色获取通过MNS推送消息的权限。
- 访问资源目录（Resource Directory）
  当您通过创建多账号跟踪将整个资源目录所有成员的操作事件收集到统一的存储空间时，操作审计需要获取您的资源目录结构和成员列表，需要通过服务关联角色获取查看资源目录和成员的权限。

关于服务关联角色的更多信息，请参见服务关联角色。

权限说明

角色名称：AliyunServiceRoleForActionTrail

权限策略：AliyunServiceRolePolicyForActionTrail

权限说明：操作审计默认使用此角色来访问您的OSS、SLS、MNS、RD等其他云产品资源。

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "oss:ListObjects",
                "oss:PutObject",
                "oss:GetBucketLocation"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:GetProject"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:PostLogStoreLogs",
                "log:CreateLogstore",
                "log:GetLogstore",
                "log:CreateIndex",
                "log:UpdateIndex",
                "log:GetIndex"
            ],
            "Resource": [
                "acs:log:*:*:project/*/logstore/actiontrail_*",
                "acs:log:*:*:project/*/logstore/innertrail_*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:CreateDashboard",
                "log:UpdateDashboard"
            ],
            "Resource": "acs:log:*:*:project/*/dashboard/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:CreateSavedSearch",
                "log:UpdateSavedSearch"
            ],
            "Resource": [
                "acs:log:*:*:project/*/savedsearch/actiontrail_*",
```

```
                "acs:log:*:*:project/*/savedsearch/innertrail_*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "mns:PublishMessage"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "resourcemanager:GetResourceDirectory",
                "resourcemanager:ListAccounts",
                "resourcemanager:GetResourceDirectoryAccount"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "actiontrail.aliyuncs.com"
                }
            }
        }
    ]
}
```

创建服务关联角色

系统会在以下场景中自动创建服务关联角色（AliyunServiceRoleForActionTrail）：

- 当您调用CreateTrail接口首次创建跟踪时，会自动创建服务关联角色。
- 当您在操作审计控制台首次创建跟踪时，会自动创建服务关联角色。

删除服务关联角色

删除服务关联角色前，您需要在操作审计控制台删除所有的跟踪。具体操作，请参见删除单账号跟踪和删除多账号跟踪。

您可以在RAM控制台删除服务关联角色。具体操作，请参见删除RAM角色。

3.3. 操作事件投递的系统权限策略

本文为您介绍操作事件投递的系统权限策略（AliyunActionTrailDeliveryPolicy）的应用场景和权限说明。

应用场景

- 访问日志服务SLS（Log Service）
  当您创建跟踪并设置了SLS Project地址用于接收操作事件时，操作审计需要向您指定的SLS Project创建Logstore并写入操作事件。此时需要访问日志服务SLS的相关权限。

- 访问对象存储OSS（Object Storage Service）
  当您创建跟踪并设置了OSS存储空间用于接收操作事件时，操作审计需要向您指定的OSS存储空间写入操作事件。此时需要访问对象存储OSS的相关权限。

权限策略说明

权限策略名称：AliyunActionTrailDeliveryPolicy

权限策略内容：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "oss:PutObject",
                "oss:GetBucketLocation"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:GetProject"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:PostLogStoreLogs",
                "log:CreateLogstore",
                "log:GetLogstore",
                "log:CreateIndex",
                "log:UpdateIndex",
                "log:GetIndex"
            ],
            "Resource": "acs:log:*:*:project/*/logstore/actiontrail_*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:CreateDashboard",
                "log:UpdateDashboard"
            ],
            "Resource": "acs:log:*:*:project/*/dashboard/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:CreateSavedSearch",
                "log:UpdateSavedSearch"
            ],
            "Resource": "acs:log:*:*:project/*/savedsearch/actiontrail_*",
            "Effect": "Allow"
        }
    ]
}
```

权限策略说明：操作审计使用此策略访问SLS和OSS中的资源。权限说明如下表所示。

Action	说明
oss:GetBucketLocation	获取OSS所在地域
oss:PutObject	向OSS写入操作事件
log:GetProject	查询Project是否存在
log:PostLogStoreLogs	向SLS写入操作事件
log:GetLogstore	查询Logstore是否存在
log:CreateLogstore	创建Logstore
log:CreateIndex	创建索引
log:UpdateIndex	更新索引
log:GetIndex	获取索引
log:CreateDashboard	创建看板
log:UpdateDashboard	更新看板
log:CreateSavedSearch	创建快速查询
log:UpdateSavedSearch	更新快速查询

4.事件记录的内容

4.1. 管控事件结构定义

本文为您介绍一个管控事件包含的关键字段及其含义，并为您提供相关的示例。

管控事件的关键字段

名称	类型	是否非空	示例	描述
acsRegion	String	是	cn-hangzhou	阿里云地域。

名称	类型	是否非空	示例	描述

additionalEventData	JSON	否	Schema: "http"	事件的补充信息。补充信息含义及示例代码如下：
				• 无实际意义
				`additionalEventData: {`
				`  Schema: "http"`
				`}`
				• 登录事件
				`{`
				`  "additionalEventData": {`
				`  "callbackUrl":"https://homenew.console.aliyun.com/",`
				`  "mfaChecked":"true"`
				`  }`
				`}`
				• MaxCompute
				`{`
				`  "additionalEventData": {`
				`  "TableName": "table_1",`
				`  "Partition": "dt=20210708,hh=17,region=cn-shenzhen",`
				`  "CurrentProject": "project_1",`
				`  "ProjectName": "project_1",`
				`  "SesssionId": "202107081800166d37d****"`
				`  }`
				`}`

apiVersion	String	否	2014-05-26	当eventType取值为*ApiCall*时，事件代表一个API的调用。此时，该字段为API的版本信息。

名称	类型	是否非空	示例	描述
eventCategory	String	是	Management	事件分类。取值： • Management：管控事件。 • Insight：Insight事件。
eventId	String	是	F23A3DD5-7842-4EF9-9DA1-3776396A****	事件ID。操作审计为每个管控事件所产生的一个GUID。
eventName	String	是	CreateNetworkInterface	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。
eventRW	String	是	Write	事件的读写类型。取值： • Write：写类型。 • Read：读类型。
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*：API调用事件。大多阿里云控制台基于API开发，对应的操作行为也会记录为ApiCall。 • *ConsoleOperation（ConsoleCall）*：部分控制台或售卖页的管控事件。由于这些控制台或售卖页并不是基于API来开发的，因此操作审计会将此类事件类型记录为ConsoleOperation或ConsoleCall。此类事件的名称并不一定是API名称， 但能够传达基本操作行为的含义。 • *AliyunServiceEvent*：此类事件为阿里云平台对您的资源执行的管控事件，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	管控事件格式的版本，当前版本为1。

名称	类型	是否非空	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。
requestParameterJson	String	否	"{"AcsHost":"actiontrail.cn-hangzhou.aliyuncs.com","AcsProduct":"Actiontrail","RequestId":"32B8BA8F-3738-46D3-BCCA-1B2257AEF9BB","AcceptLanguage":"zh-CN","Region":"cn-hangzhou","HostId":"actiontrail.cn-hangzhou.aliyuncs.com","Name":"create-service-tmp"}"	requestParameters的JSON格式。 **说明** 仅投递到日志服务SLS的事件包含requestParameterJson。

名称	类型	是否非空	示例	描述
resourceName	String	否	`"i-0xiiz1v0vw4epqjc****;sg-0xi2js0u6m03jbmv****;aliyun_2_1903_x64_20G_alibase_20200529.vhd;sshkey-cn-hangzhou;vsw-0xikxv8p1akh4ki43****"`	事件的相关资源名称，是资源的唯一标识。 该参数可以在日志服务中作为索引，可按照资源名称查询相关事件。 根据事件涉及的资源和资源类型的不同，resourceName的取值规则不同，具体如下： • 事件涉及单个资源类型的单个资源：`i-bp1example1`。 • 事件涉及单个资源类型的多个资源：`i-bp1example1,i-bp1example2`。 • 事件涉及多种资源类型的多个资源：`i-bp1example1,i-bp1example2;v-bp1example1`。 **说明** 同类型的资源名称（ID）之间以半角逗号（,）间隔，不同类型的资源名称（ID）之间以半角分号（;）间隔。
resourceType	List	否	`"ACS::ECS::Instance;ACS::ECS::SecurityGroup;ACS::ECS::Image;ACS::ECS::KeyPair;ACS::VPC::VSwitch"`	事件的相关资源类型。 该参数可以在日志服务中作为索引，可按照资源类型查询相关事件。 根据事件涉及的资源和资源类型的不同，resourceType的取值规则不同，具体如下： • 事件涉及单个资源类型的单个资源：`ACS::ECS::Instance`。 • 事件涉及单个资源类型的多个资源：`ACS::ECS::Instance`。 • 事件涉及多种资源类型的多个资源：`ACS::ECS::Instance;ACS::VPC::VPC`。 **说明** 多个资源类型之间以半角分号（;）间隔。
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。

名称	类型	是否非空	示例	描述
serviceName	String	是	Ecs	事件相关的阿里云服务名称。
sourceIpAddress	String	否	11.168.XX.XX	事件发起的源IP地址。
userAgent	String	否	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。 更多信息，请参见userIdentity包含的字段。

userIdentity包含的字段如下表所示。

userIdentity包含的字段

名称	类型	是否非空	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*：阿里云账号。 • *ram-user*：RAM用户。 • *assumed-role*：RAM角色。 • *system*：阿里云服务。 • *cloudsso-user*：云SSO用户。 • *saml-user*：企业自有身份。 • *alibaba-cloud-account*：跨阿里云账号授权时被授权的身份。

名称	类型	是否非空	示例	描述

principalId	String	否	28815334868278****	当前请求者的ID，需结合type来唯一确认请求者身份。
				• 如果type取值为*root-account*，则记录阿里云账号ID。
				• 如果type取值为*ram-user*，则记录RAM用户ID。
				• 如果type取值为*assumed-role*，则记录RoleID:RoleSessionName。
				• 如果type取值为*cloudsso-user*，则记录云SSO用户ID。
				• 如果type取值为*alibaba-cloud-account*
				  ○ 当阿里云账号跨账号操作时，记录阿里云账号ID。
				  ○ 当RAM用户跨账号操作时，记录RAM用户ID。
				  ○ 当扮演角色跨账号操作时，记录RoleID:RoleSessionName。
				• 如果type取值为*saml-user*或*system*，不记录principalId。

accountId	String	否	112233445566****	当前请求身份所属的阿里云账号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。 • 如果请求者通过安全令牌进行访问，则记录临时访问密钥ID。
userName	String	否	Alice	当前请求者的身份名称。 • 如果type取值为*ram-user*，则记录RAM用户名。 • 如果type取值为assumed-role，则记录RoleName:RoleSessionName。 • 如果type取值为*root-account*，userName取值为“root”。 • 如果type取值为*cloudsso-user*，则记录云SSO用户的用户名。 • 如果type取值为*saml-user*，则记录企业自有身份的用户名。 • 如果type取值为*alibaba-cloud-account*，不记录userName。

名称	类型	是否非空	示例	描述
sessionContext	String	否	{"attributes": {"mfaAuthenticated": "true", "creationDate": "2020-01-09T12:12:14Z" }	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

```
{
    "acsRegion":"cn-hangzhou",
    "additionalEventData":{
        "Scheme":"http"
    },
    "apiVersion":"2014-05-26",
    "eventCategory":"Management",
    "eventId":"F7393A43-6A4A-4409-AEDD-8B1C47DE****",
    "eventName":"RunInstances",
    "eventRW":"Write",
    "eventSource":"ecs-cn-hangzhou-inner.aliyuncs.com",
    "eventTime":"2021-07-13T07:33:46Z",
    "eventType":"ApiCall",
    "eventVersion":"1",
    "referencedResources":{
        "ACS::ECS::Instance":[
            "i-0xiiz1v0vw4epqjc****"
        ],
        "ACS::ECS::SecurityGroup":[
            "sg-0xi2js0u6m03jbmv****"
        ],
        "ACS::ECS::Image":[
            "aliyun_2_1903_x64_20G_alibase_20200529.vhd"
        ],
        "ACS::ECS::KeyPair":[
            "sshkey-cn-hangzhou"
        ],
        "ACS::VPC::VSwitch":[
            "vsw-0xikxv8p1akh4ki43****"
        ]
    },
    "requestId":"F7393A43-6A4A-4409-AEDD-8B1C47DE45ED",
    "requestParameters":{
        "Amount":1,
        "VSwitchId":"vsw-0xikxv8p1akh4ki43****"
    },
    "resourceName":"i-0xiiz1v0vw4epqjc****;sg-0xi2js0u6m03jbmv****;aliyun_2_1903_x64_20G_al
ibase_20200529.vhd;sshkey-cn-hangzhou;vsw-0xikxv8p1akh4ki43****",
    "resourceType":"ACS::ECS::Instance;ACS::ECS::SecurityGroup;ACS::ECS::Image;ACS::ECS::Ke
yPair;ACS::VPC::VSwitch",
    "responseElements":{
        "RequestId":"F7393A43-6A4A-4409-AEDD-8B1C47DE45ED",
```

```
        "InstanceIdSets":{
            "InstanceIdSet":[
                "i-0xiiz1v0vw4epqjc****"
            ]
        }
    },
    "serviceName":"Ecs",
    "sourceIpAddress":"Internal",
    "userAgent":"AlibabaCloud (Linux; amd64) Java/1.8.0_102-b52 Core/4.5.3 HTTPClient/Inter
nalHttpClient",
    "userIdentity":{
        "accessKeyId":"STS.NUQNP4PiGyckMsNiGELCs****",
        "accountId":"116214297662****",
        "principalId":"32886943330935****:ess-session-ecs_default",
        "sessionContext":{
            "attributes":{
                "mfaAuthenticated":"false",
                "creationDate":"2021-07-13T07:33:46Z"
            }
        },
        "type":"assumed-role",
        "userName":"aliyunserviceroleforautoscaling:ess-session-ecs_default"
    }
}
```

4.2. Insight事件结构定义

本文为您介绍一个Insight事件包含的关键字段及其含义，并为您提供相关的示例。

Insight事件的关键字段

名称	类型	是否非空	示例	描述
eventVersion	String	是	1	Insight事件格式的版本，当前版本为1。
eventTime	String	是	2021-03-10T21:00:00Z	事件产生时间（UTC格式）。
acsRegion	String	是	cn-hangzhou	阿里云地域。
eventId	String	是	F23A3DD5-7842-4EF9-9DA1-3776396A****	事件ID。
eventType	String	是	ActionTrailInsight	产生的事件类型。 取值：ActionTrailInsight，表示Insight事件。
recipient	String	是	112233445566****	接收事件的阿里云账号ID。

名称	类型	是否非空	示例	描述
insightDetails	字典	是	不涉及	Insight事件的具体信息。 更多信息，请参见InsightDetails包含的字段。
eventCategory	String	是	Insight	事件分类。取值： • Management：管控事件。 • Insight：Insight事件。
userIdentity	字典	是	不涉及	请求者的身份信息。 更多信息，请参见userIdentity包含的字段。

InsightDetails包含的字段如下表所示。

InsightDetails包含的字段

名称	类型	是否非空	示例	描述
sourceIpAddress	String	是	42.120.XX.XX	事件发起的源IP地址，在IPInsight中也代表异常IP地址。
insightType	String	是	IpInsight	Insight事件类型。 取值：IpInsight，表示异常IP调用事件。
insightContext	字典	是	不涉及	Insight相关信息。 更多信息，请参见insightContext包含的字段。

insightContext包含的字段如下表所示。

insightContext包含的字段

名称	类型	是否非空	示例	描述
statistics	字典	是	不涉及	Insight事件的基本信息。例如：期望阈值、实际预测值、持续时间（以秒为单位）、触发次数等。
baseline	字典	是	不涉及	Insight事件标准测量数据。
threshold	double	是	0.6	Insight事件的标准阈值。如果实际预测值大于标准阈值，则视为正常，否则视为异常。
insight	字典	是	不涉及	Insight事件实际测量数据。
predict	double	是	0.1	Insight事件的实际预测值。如果实际预测值大于标准阈值，则视为正常，否则视为异常。

名称	类型	是否非空	示例	描述
insightDuration	int	是	300	Insight事件的持续时间。 单位：秒。
insightCount	int	是	10	Insight事件持续时间内产生的次数。

示例

```
{
  "event": {
    "eventVersion": "1",
    "eventTime": "2021-03-10T21:00:00Z",
    "acsRegion": "cn-hangzhou",
    "eventID": "F23A3DD5-7842-4EF9-9DA1-3776396A****",
    "eventType": "ActionTrailInsight",
    "recipient": "116214297662****",
    "insightDetails": {
      "sourceIpAddress": "42.120.XX.XX",
      "insightType": "IpInsight",
      "insightContext": {
        "statistics": {
          "baseline": {
            "threshold": 0.6
          },
          "insight": {
            "predict": 0.12
          },
          "insightDuration": 300,
          "insightCount": 10
        }
      }
    },
    "userIdentity": {
      "accountId": "112432432434****",
      "principalId": "231321312321****"
    },
    "eventCategory": "Insight"
  }
}
```

4.3. 操作审计支持被审计的事件说明

操作审计自身也是一款云服务，和其他云服务一样，您对操作审计服务所做的管控操作也可以在操作审计中查看对应的记录。操作审计支持将管控事件投递到日志服务SLS的日志库（Logstore）或对象存储OSS的存储空间中，满足实时审计、问题回溯分析等需求。

操作审计记录了用户通过OpenAPI或控制台等方式操作云资源时产生的管控事件，具体事件如下表所示。

事件名称	事件含义
CheckOssConfig	检查跟踪关联的OSS配置

事件名称	事件含义
CreateDeliveryHistoryJob	创建历史事件投递任务
CreateInnerTrail	创建平台事件跟踪
CreateServiceLinkedRole	创建操作审计服务关联角色
CreateTrail	创建跟踪
DeleteDeliveryHistoryJob	删除历史事件投递任务
DeleteInnerTrail	删除平台事件跟踪
DeleteTrail	删除跟踪
DescribeInnerTrails	查询某地域的平台事件跟踪列表
DescribeInsightEnabledTrails	查询开启了Insight的跟踪列表
DescribeInsightIpList	查询Insight累积检测的IP地址列表
DescribeInsightMetricData	查询Insight指标数据
DescribeInsightStrategy	查询Insight策略列表
DescribeRegions	查询您可以使用的阿里云地域
DescribeResourceLifeCycleEvents	查询资源生命周期事件
DescribeScenes	查询所有场景
DescribeSearchTemplates	查询所有模板
DescribeSupportedServices	查询操作审计支持的云服务列表
DescribeTrailDeliveryMetricData	查询投递监控指标
DescribeTrails	查询某地域的跟踪列表
GetAccessKeyLastUsedEvents	获取AccessKey最后调用的事件列表
GetAccessKeyLastUsedInfo	获取AccessKey最后调用的用户信息
GetAccessKeyLastUsedIps	获取AccessKey最后使用的IP

事件名称	事件含义
GetAccessKeyLastUsedProducts	获取AccessKey最后使用的产品
GetAccessKeyLastUsedResources	获取AccessKey最后使用的资源
GetDefaultTrail	查询默认跟踪
GetDeliveryHistoryJob	查询历史事件投递任务详情
GetEventsCount	查询用户事件量
GetInsightEventCount	查询Insight处理事件数
GetInsightIpCount	查询Insight统计的IP地址个数
GetInsightSelectors	查询Insight配置
GetTrailStatus	查询跟踪的状态
ListDeliveryHistoryJobs	查询历史事件投递任务列表
ListEventNames	查询事件名称
ListProductResourceType	查询产品资源类型
ListServiceTrail	查询服务跟踪列表
LookupAggregationEvents	检索聚合事件
LookupEvents	检索详细事件
LookupInsightEvents	查询Insight事件
ModifyInsightStrategy	修改Insight策略
OpenService	开通服务
PutInsightSelectors	修改Insight功能
RemoveDefaultTrail	移除默认跟踪
SetDefaultTrail	设置默认跟踪
StartInnerTrailLogging	启用平台事件跟踪
StartLogging	启用跟踪
StopInnerTrailLogging	禁用平台事件跟踪

事件名称	事件含义
StopLogging	禁用跟踪
UpdateInnerTrail	更新平台事件跟踪
UpdateTrail	更新跟踪

4.4. 登录事件示例

4.4.1. 阿里云账号登录事件

当您使用阿里云账号登录阿里云控制台时，会产生登录事件（ConsoleSignin）。本文为您介绍阿里云账号登录事件示例及含义。

示例一：未进行MFA认证登录事件

以下示例表示阿里云账号 `151266687691****` 未启用MFA认证，在北京时间2021年01月01日08:00:00登录了控制台。

```
{
  "requestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
  "eventType": "ConsoleSignin",
  "userIdentity": {
    "accountId": "151266687691****",
    "principalId": "151266687691****",
    "type": "root-account",
    "userName": "root"
  },
  "AcsRegion": "cn-hangzhou",
  "eventName": "ConsoleSignin",
  "eventSource": "http://account.aliyun.com/login/login_aliyun.htm",
  "serviceName": "AasCustomer",
  "eventTime": "2021-01-01T00:00:00Z",
  "userAgent": "Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15
(KHTML, like Gecko) Mobile/19A5307g Ariver/1.1.0 AliApp(AP/10.2.28.6000) Nebula WK RVKType(
1) AlipayDefined(nt:WIFI,ws:390|780|3.0) AlipayClient/10.2.28.6000 Language/zh-Hans Region/
CN NebulaX/1.0.0",
  "eventId": "2546c4b7-6b56-403e-97d3-500d8d29****",
  "additionalEventData": {
    "loginAccount": "Alice",
    "isMFAChecked": "false"
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```

示例中关键字段含义如下：

- `eventType` ：发生的事件类型。取值为 `ConsoleSignin` ，表示控制台登录事件。

- `userIdentity.accountId` ：请求者的阿里云账号ID。
- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
- `eventTime` ：事件的发生时间（UTC格式）。取值为 `2021-01-01T00:00:00Z` ，表示北京时间2021年01月01日08:00:00。
- `additionalEventData.isMFAChecked` ：是否启用MFA认证。取值为 `false` ，表示未启用MFA认证。

示例二：进行MFA认证登录事件

以下示例表示阿里云账号 `151266687691****` 已启用MFA认证，在北京时间2021年01月01日08:00:00登录了控制台。

```
{
  "eventId": "2546c4b7-6b56-403e-97d3-500d8d29****",
  "eventVersion": 1,
  "eventSource": "http://account.aliyun.com/account_init/skip2Login.htm",
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
ecko) Chrome/92.0.4515.107 Safari/537.36",
  "eventType": "ConsoleSignin",
  "userIdentity": {
    "accountId": "151266687691****",
    "principalId": "151266687691****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "AasCustomer",
  "additionalEventData": {
    "loginAccount": "Alice",
    "isMFAChecked": "true"
  },
  "extend": "2",
  "requestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
  "eventTime": "2021-01-01T00:00:00Z",
  "isGlobal": true,
  "acsRegion": "cn-hangzhou",
  "eventName": "ConsoleSignin"
}
```

示例中关键字段含义如下：

- `eventType` ：事件的类型。取值为 `ConsoleSignin` ，表示控制台登录事件。
- `userIdentity.accountId` ：请求者的阿里云账号ID。
- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
- `additionalEventData.isMFAChecked` ：是否启用MFA认证。取值为 `true` ，表示已启用MFA认证。
- `eventTime` ：事件的发生时间（UTC格式）。取值为 `2021-01-01T00:00:00Z` ，表示北京时间2021年01月01日08:00:00。

示例三：登录失败事件

以下示例表示阿里云账号 `151266687691****` 在北京时间2021年01月01日08:00:00登录控制台失败。

```
{
  "requestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
  "eventType": "ConsoleSignin",
  "userIdentity": {
    "accountId": "151266687691****",
    "principalId": "151266687691****",
    "type": "root-account",
    "userName": "root"
  },
  "AcsRegion": "cn-hangzhou",
  "eventName": "ConsoleSignin",
  "eventSource": "http://account.aliyun.com/login/login_aliyun.htm",
  "serviceName": "AasCustomer",
  "eventTime": "2021-01-01T00:00:00Z",
  "userAgent": "Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15
(KHTML, like Gecko) Mobile/19A5307g Ariver/1.1.0 AliApp(AP/10.2.28.6000) Nebula WK RVKType(
1) AlipayDefined(nt:WIFI,ws:390|780|3.0) AlipayClient/10.2.28.6000 Language/zh-Hans Region/
CN NebulaX/1.0.0",
  "eventId": "2546c4b7-6b56-403e-97d3-500d8d29****",
  "additionalEventData": {
    "callbackUrl": "https://actiontrail.console.aliyun.com/cn-hangzhou/event-list?accounttr
aceid=******",
    "mfaChecked": "false"
  },
  "errorCode": "Authentication.Failed",
  "errorMessage": "Failed authentication.",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```

示例中关键字段含义如下：

- `eventType` ：发生的事件类型。取值为 `ConsoleSignin` ，表示控制台登录事件。
- `userIdentity.accountId` ：请求者的阿里云账号ID。
- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
- `eventTime` ：事件的发生时间（UTC格式）。取值为 `2021-01-01T00:00:00Z` ，表示北京时间2021年01月01日08:00:00。
- `errorCode` ：错误码。取值为 `Authentication.Failed` ，表示登录失败。

4.4.2. RAM用户登录事件

当您使用RAM用户登录阿里云控制台时，会产生登录事件（ConsoleSignin）。本文为您介绍RAM用户登录事件示例及含义。

示例一：未进行MFA认证登录事件

以下示例表示RAM用户 `Alice` 未启用MFA认证，在北京时间2021年01月01日08:00:00登录了控制台。

```
{
  "requestId": "1.167_1627549154939_339a",
  "eventType": "ConsoleSignin",
  "userIdentity": {
    "accountId": "159498693826****",
    "principalId": "23890260100229****",
    "type": "ram-user",
    "userName":  "Alice"
  },
  "acsRegion": "cn-hangzhou",
  "eventName": "ConsoleSignin",
  "eventSource": "signin.aliyun.com",
  "serviceName": "AasSub",
  "eventTime": "2021-01-01T00:00:00Z",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
ecko) Chrome/91.0.4472.164 Safari/537.36",
  "eventId": "1.167_1627549154939_****",
  "additionalEventData": {
    "callbackUrl": "https://actiontrail.console.aliyun.com/cn-hangzhou/event-list?accounttr
aceid=******",
    "mfaChecked": "false"
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```

示例中关键字段含义如下：

- `eventType`：事件的类型。取值为`ConsoleSignin`，表示控制台登录事件。
- `userIdentity.type`：请求者的身份类型。取值为`ram-user`，表示RAM用户。
- `userIdentity.userName`：请求者的RAM用户名称。
- `eventTime`：事件的发生时间（UTC格式）。取值为`2021-01-01T00:00:00Z`，表示北京时间2021年01月01日08:00:00。
- `additionalEventData.isMFAChecked`：是否启用MFA认证。取值为`false`，表示未启用MFA认证。

示例二：进行MFA认证登录事件

以下示例表示RAM用户`Alice`已启用MFA认证，在北京时间2021年01月01日08:00:00登录了控制台。

```
{
  "requestId": "1.167_1627549154939_339a",
  "eventType": "ConsoleSignin",
  "userIdentity": {
    "accountId": "159498693826****",
    "principalId": "23890260100229****",
    "type": "ram-user",
    "userName":  "Alice"
  },
  "acsRegion": "cn-hangzhou",
  "eventName": "ConsoleSignin",
  "eventSource": "signin.aliyun.com",
  "serviceName": "AasSub",
  "eventTime": "2021-01-01T00:00:00Z",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
ecko) Chrome/91.0.4472.164 Safari/537.36",
  "eventId": "1.167_1627549154939_****",
  "additionalEventData":{
    "callbackUrl": "https://actiontrail.console.aliyun.com/cn-hangzhou/event-list?accounttr
aceid=******",
    "mfaChecked": "true"
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```

示例中关键字段含义如下：

- `eventType`：事件的类型。取值为`ConsoleSignin`，表示控制台登录事件。
- `userIdentity.type`：请求者的身份类型。取值为`ram-user`，表示RAM用户。
- `userIdentity.userName`：请求者的RAM用户名称。
- `eventTime`：事件的发生时间（UTC格式）。取值为`2021-01-01T00:00:00Z`，表示北京时间2021年01月01日08:00:00。
- `additionalEventData.isMFAChecked`：是否启用MFA认证。取值为`true`，表示已启用MFA认证。

示例三：登录失败事件

以下示例表示RAM用户`Alice`在北京时间2021年01月01日08:00:00登录控制台失败。

```
{
  "eventId": "1.167_1627549154939_****",
  "eventVersion": 1,
  "errorMessage": "Password is error",
  "eventSource": "signin.aliyun.com",
  "errorCode": "Authentication.Failed",
  "sourceIpAddress":"192.168.XX.XX",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
ecko) Chrome/92.0.4515.107 Safari/537.36",
  "eventType": "ConsoleSignin",
  "userIdentity": {
    "accountId": "159498693826****",
    "principalId": "23890260100229****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "AasSub",
  "additionalEventData": {
    "callbackUrl": "https://actiontrail.console.aliyun.com/cn-hangzhou/event-list?accounttr
aceid=****",
    "mfaChecked": "false"
  },
  "extend": "USER_LOGIN",
  "requestId": "1.167_1627549154939_339a",
  "eventTime": "2021-01-01T00:00:00Z",
  "isGlobal": true,
  "acsRegion": "cn-hangzhou",
  "eventName": "ConsoleSignin"
}
```

示例中关键字段含义如下：

- `errorCode` ：错误码。取值为 `Authentication.Failed` ，表示登录失败。
- `eventType` ：事件的类型。取值为 `ConsoleSignin` ，表示控制台登录事件。
- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `userIdentity.userName` ：请求者的RAM用户名称。
- `eventTime` ：事件的发生时间（UTC格式）。取值为 `2021-01-01T00:00:00Z` ，表示北京时间2021年01月01日08:00:00。

4.5. 角色扮演事件示例

4.5.1. 容器服务通过角色扮演创建TCP监听

本文为您介绍阿里云容器服务Kubernetes版（Alibaba Cloud Container Service for Kubernetes）通过角色扮演创建TCP监听的事件示例及含义。

示例

以下示例表示容器服务在北京时间2021年01月01日08:00:00通过扮演 `159498693826****` 账号的 `aliyuncsdefaultrole` 角色来为 `159498693826****` 账号创建TCP监听。

```
{
```

```
  "apiVersion": "2014-05-15",
  "requestId": "A2D14EC1-BE40-4AF2-92D5-E54A",
  "eventType": "ApiCall",
  "userIdentity": {
    "accessKeyId": "STS.NUQNP4PiGyckMsNiGELCs****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-01T00:00:00Z"
      }
    },
    "accountId": "159498693826****",
    "principalId": "34359792600393****:ccm-provision-role-1627631749",
    "type": "assumed-role",
    "userName": "aliyuncsdefaultrole:ccm-provision-role-1627631749"
  },
  "acsRegion": "cn-hangzhou",
  "eventName": "CreateLoadBalancerTCPListener",
  "requestParameters": {
    "ListenerPort": 6443,
    "AcsHost": "slb.aliyuncs.com",
    "RequestId": "A2D14EC1-BE40-4AF2-92D5-***",
    "LoadBalancerId": "lb-bp19byhscefk3x0li****",
    "SignatureType": "",
    "HostId": "slb.aliyuncs.com",
    "BackendServerPort": 6443,
    "StsTokenPrincipalName": "aliyuncsdefaultrole/cs-provision-role-1623911494",
    "AcsProduct": "Slb",
    "Bandwidth": -1,
    "RegionId": "cn-hangzhou",
    "StsTokenPlayerUid": 178498693826****,
    "HealthCheckType": "tcp"
  },
  "eventSource": "slb.aliyuncs.com",
  "serviceName": "Slb",
  "eventTime": "2021-01-01T00:00:00Z",
  "referencedResources": {
    "ACS::SLB::LoadBalancer": [
      "lb-bp1***"
    ]
  },
  "userAgent": "AlibabaCloud (linux; amd64) Golang/1.11.4 Core/0.0.1",
  "eventId": "A2D14EC1-BE40-4AF2-92D5-****",
  "additionalEventData": {
    "Scheme": "http"
  },
  "responseElements": {
    "requestId": "A2D14EC1-BE40-4AF2-92D5-EA54"
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```

示例中关键字段含义如下：

- `userIdentity.accountId` ：请求者的阿里云账号ID，在本示例中表示RAM角色归属的账号ID。取值为 `159498693826****` 。
- `userIdentity.principalId` ：请求者的ID。格式为 `{roleId}:{sessionName}` ， `roleId` 表示被扮演的RAM角色ID， `sessionName` 表示进行角色扮演时指定的名称。取值为 `34359792600393****:ccm-provision-role-1627631749` ，表示被扮演的RAM角色ID是 `34359792600393****` ，进行角色扮演时指定的名称为 `ccm-provision-role-1627631749` 。
- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示通过扮演RAM角色进行的访问。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `aliyuncsdefaultrole:ccm-provision-role-1627631749` ，表示被扮演的RAM角色名称是 `aliyuncsdefaultrole` ，进行角色扮演时指定的名称为 `ccm-provision-role-1627631749` 。

  > **说明** `aliyuncsdefaultrole` 是容器服务的默认RAM角色名称，容器服务在进行集群操作时默认使用 `aliyuncsdefaultrole` 来访问其他云服务中的资源。

- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `178498693826****` 。
- `eventTime` ：事件的发生时间（UTC格式）。取值为 `2021-01-01T00:00:00Z` ，表示北京时间2021年01月01日08:00:00。

4.5.2. RAM用户角色扮演

RAM用户可以调用AssumeRole接口扮演可信实体为阿里云账号的RAM角色。本文为您介绍RAM用户角色扮演事件的示例及含义。

示例

以下示例表示ID为 `23890260100229****` 的RAM用户 `Alice` ，在北京时间2021年08月02日11:42:19通过调用AssumeRole接口扮演 `159498693826****` 账号的 `custom-role-for-actiontrail` 角色。

```
{
  "eventId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
  "eventVersion": 1,
  "responseElements": {
    "requestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
    "assumedRoleUser": {
      "arn": "acs:ram::159498693826****:role/custom-role-for-actiontrail/Alice",
      "assumedRoleId": "39484351102463****:Alice"
    },
    "credentials": {
      "accessKeyId": "STS.NUQNP4PiGyckMsNiGELCs****",
      "accessKeySecret": "Ss7sq2j0ZoJujZnmVgXcu6QT9e****",
      "expiration": "2021-08-02T04:42:19Z"
    }
  },
  "eventSource": "sts.aliyuncs.com",
  "requestParameters": {
    "AcsHost": "sts.aliyuncs.com",
```

```
    "AcsProduct": "Sts",
    "RequestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
    "RoleSessionName": "Alice",
    "DurationSeconds": 3600,
    "HostId": "sts.aliyuncs.com",
    "RoleArn": "acs:ram::159498693826****:role/custom-role-for-actiontrail"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "Jakarta Commons-HttpClient/3.1",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RAM::AccessKey": [
      "STS.NUQNP4PiGyckMsNiGELCs****"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T03:42:19Z"
      }
    },
    "accountId": "159498693826****",
    "principalId": "23890260100229****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Sts",
  "additionalEventData": {
    "Scheme": "https",
    "CallerBid": "26842"
  },
  "apiVersion": "2015-04-01",
  "requestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
  "eventTime": "2021-08-02T03:42:19Z",
  "isGlobal": false,
  "acsRegion": "cn-shanghai",
  "eventName": "AssumeRole"
}
```


示例中关键字段含义如下：

- `userIdentity.accountId` ：请求者的阿里云账号ID，在本示例中表示RAM用户归属的账号ID。取值为 `159498693826****` 。
- `userIdentity.principalId` ：请求者的ID，即发起角色扮演的RAM用户ID。
- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户发起请求，申请扮演某个RAM角色。
- `userIdentity.userName` ：请求者的用户名。取值为 `Alice` 。
- `userIdentity.attributes.creationDate` ：事件的发生时间（UTC格式）。取值为 `2021-08-02T03:42:19Z` ，表示北京时间2021年08月02日11:42:19。
- `requestParameters.RoleArn` ：被扮演的RAM角色ARN。取值为 `acs:ram::159498693826****:role/c`

`ustom-role-for-actiontrail`，`159498693826****`表示角色所属的阿里云账号，`custom-role-for-actiontrail`表示角色的名称。

- `responseElements.assumedRoleUser.assumedRoleId`：扮演成功后，RAM用户`Alice`后续操作时的身份ID。格式为`{roleId}:{sessionName}`，`roleId`表示被扮演的RAM角色ID，`sessionName`表示进行角色扮演时指定的名称。取值为`39484351102463****:Alice`，表示被扮演的RAM角色ID是`39484351102463****`，进行角色扮演时指定的名称为`Alice`。
- `referencedResources`：相关资源列表。取值为`{ "ACS::RAM::AccessKey": [ "STS.NUQNP4PiGyckMsNiGELCs****"]}`，表示本次角色扮演获取的临时凭证。

4.5.3. 通过角色扮演查询操作审计的事件

本文为您介绍通过角色扮演查询操作审计的事件示例及含义。

示例

以下示例表示北京时间2021年01月01日08:00:00，阿里云账号`175498693826****`中的RAM用户通过扮演阿里云账号`159498693826****`下的`custom-role-for-actiontrail`角色来查询操作审计的事件。

```
{
  "apiVersion": "2020-07-06",
  "requestId": "3462D6AF-4434-4690-8CAD-E54A",
  "eventType": "ApiCall",
  "userIdentity": {
    "accessKeyId": "STS.NUQNP4PiGyckMsNiGELCs****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-01T00:00:00Z"
      }
    },
    "accountId": "159498693826****",
    "principalId": "34359792600393****:u1",
    "type": "assumed-role",
    "userName": "custom-role-for-actiontrail:u1"
  },
  "acsRegion": "cn-hangzhou",
  "eventName": "LookupEvents",
  "requestParameters": {
    "stsTokenPrincipalName": "custom-role-for-actiontrail/u1",
    "AcsHost": "actiontrail.cn-hangzhou.aliyuncs.com",
    "ServiceCode": "actiontrail",
    "AcsProduct": "Actiontrail",
    "RequestId": "3462D6AF-4434-4690-8CAD-E54A",
    "Region": "cn-hangzhou",
    "LookupAttribute.1.Value": "Write",
    "RegionId": "cn-hangzhou",
    "HostId": "actiontrail.cn-hangzhou.aliyuncs.com",
    "stsTokenPlayerUid": 175498693826****,
    "LookupAttribute.1.Key": "EventRW"
  },
  "eventSource": "actiontrail.cn-hangzhou.aliyuncs.com",
  "serviceName": "Actiontrail",
  "eventTime": "2021-01-01T00:00:00Z",
  "userAgent": "AlibabaCloud (Mac OS X; x86_64) Java/1.8.0_252-b09 Core/4.4.6 HTTPClient/Ap
acheHttpClient",
  "eventId": "3462D6AF-4434-4690-8CAD-****",
  "additionalEventData": {
    "Scheme": "http"
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```


示例中关键字段含义如下：

- `userIdentity.accountId` ：请求者的阿里云账号ID，在本示例中表示RAM角色归属的账号ID。取值为 `159498693826****` 。
- `userIdentity.principalId` ：请求者的ID。格式为 `{roleId}:{sessionName}` ， `roleId` 表示被扮

演的RAM角色ID，`sessionName`表示进行角色扮演时指定的名称。取值为`34359792600393****:u1`，表示被扮演的RAM角色ID是`34359792600393****`，进行角色扮演时指定的名称为`u1`。

- `userIdentity.type`：请求者的身份类型。取值为`assumed-role`，表示通过扮演RAM角色进行的访问。
- `userIdentity.userName`：请求者的用户名。格式为`{roleName}:{sessionName}`，`roleName`表示被扮演的角色名称，`sessionName`表示进行角色扮演时指定的名称。取值为`custom-role-for-actiontrail:u1`，表示被扮演的RAM角色名称是`custom-role-for-actiontrail`，进行角色扮演时指定的名称为`u1`。

> **说明** `custom-role-for-actiontrail`是操作审计的自定义角色名称，具有查询操作审计事件的权限。

- `userIdentity.creationDate`：事件的发生时间（UTC格式）。取值为`2021-01-01T00:00:00Z`，表示北京时间2021年01月01日08:00:00。
- `requestParameters.stsTokenPlayerUid`：扮演者账号所属的阿里云账号ID。取值为`175498693826****`，表示阿里云账号`175498693826****`中的RAM用户跨账号扮演`159498693826****`账号下的RAM角色。

4.5.4. 通过角色SSO进行角色扮演

进行角色SSO时，通过调用AssumeRoleWithSAML接口，可以获取一个扮演该角色的临时身份。本文为您介绍通过角色SSO进行角色扮演的事件示例及含义。

示例

以下示例表示名为`Alice@example.com`的企业自有身份的用户，在北京时间2021年08月02日14:05:20使用阿里云账号`159498693826****`下的`testrole`角色进行了角色SSO。

```
{
  "apiVersion": "2015-04-01",
  "requestId": "3462D6AF-4434-4690-8CAD-E54A",
  "eventType": "ApiCall",
  "userIdentity": {
    "accountId": "159498693826****",
    "type": "saml-user",
    "userName": "Alice@example.com"
  },
  "acsRegion": "cn-shanghai",
  "eventName": "AssumeRoleWithSAML",
  "requestParameters": {
    "AcsHost": "sts.aliyuncs.com",
    "SAMLAssertion": "****",
    "AcsProduct": "Sts",
    "RequestId": "3462D6AF-4434-4690-8CAD-E54A",
    "DurationSeconds": 3600,
    "HostId": "sts.aliyuncs.com",
    "SAMLProviderArn": "acs:ram::159498693826****:saml-provider/test",
    "RoleArn": "acs:ram::159498693826****:role/testrole"
  },
  "eventSource": "sts.aliyuncs.com",
  "serviceName": "Sts",
  "eventTime": "2021-08-02T06:05:20Z",
```

```
  "referencedResources": {
    "ACS::RAM::AccessKey": [
      "STS.NUQNP4PiGyckMsNiGELCs****"
    ]
  },
  "userAgent": "Jakarta Commons-HttpClient/3.1",
  "eventId": "3462D6AF-4434-4690-8CAD-****",
  "additionalEventData": {
    "Scheme": "https"
  },
  "responseElements": {
    "RequestId": "3462D6AF-4434-4690-8CAD-E54A",
    "SAMLAssertionInfo": {
      "SubjectType": "persis****",
      "Issuer": "https://sts.windows.net/d1ee1acd9a83906adg****/",
      "Recipient": "https://signin.aliyun.com/saml-role/sso",
      "Subject": "Alice@example.com"
    },
    "AssumedRoleUser": {
      "Arn": "acs:ram::159498693826****:role/testrole/Alice",
      "AssumedRoleId": "179432153826****:Alice"
    },
    "Credentials": {
      "AccessKeyId": "STS.NUQNP4PiGyckMsNiGELCs****",
      "AccessKeySecret": "Ss7sq2j0ZoJujZnmVgXcu6QT9e****",
      "Expiration": "2021-08-02T07:05:20Z"
    }
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```

示例中关键字段含义如下：

- `userIdentity.accountId` ：扮演角色所属的阿里云账号ID。取值为 `159498693826****` ，表示RAM角色所属的阿里云账号。
- `userIdentity.type` ：请求者的身份类型。取值为 `saml-user` ，表示企业自有身份的用户。
- `userIdentity.userName` ：请求者的用户名。取值为 `Alice@example.com` ，表示当前进行角色SSO的用户名。
- `eventName` ：事件名称。取值为 `AssumeRoleWithSAML` ，表示获取一个扮演该角色的临时身份。
- `SAMLProviderArn` ：RAM中创建的身份提供商的ARN。格式为 `acs:ram::<account_ID>:saml-provider/<saml_provider_ID>` ， `account_ID` 表示阿里云账号ID， `saml_provider_ID` 表示身份提供商名称。取值为 `acs:ram::159498693826****:saml-provider/test` ，表示阿里云账号ID为 `159498693826****` ，身份提供商名称为 `test` 。
- `RoleArn` ：要扮演的角色的ARN。格式为 `acs:ram::<accountID>:role/<roleName>` ， `account_ID` 表示阿里云账号ID， `roleName` 表示要扮演的角色名称。取值为 `acs:ram::159498693826****:role/testrole` ，表示阿里云账号ID为 `159498693826****` ，要扮演的角色名称为 `testrole` 。
- `AssumedRoleUser` ：角色扮演临时身份。取值为 `{"Arn": "acs:ram::159498693826****:role/testro`

`le/Alice","AssumedRoleId": "179432153826****:Alice"}` ，表示临时身份的ARN为 `acs:ram::159498693826****:role/testrole/Alice` 、临时身份的ID为 `179432153826****:Alice` 。

- `Credentials` ：访问凭证。取值为 `{"AccessKeyId": "STS.NUQNP4PiGyckMsNiGELCs****","AccessKeySecret": "Ss7sq2j0ZoJujZnmVgXcu6QT9e****","Expiration": "2021-08-02T07:05:20Z"}` ，表示访问密钥ID为 `STS.NUQNP4PiGyckMsNiGELCs****` 、访问密钥为 `Ss7sq2j0ZoJujZnmVgXcu6QT9e****` 、失效时间为 `2021-08-02T07:05:20Z` 。
- `referencedResources` ：事件影响的资源列表。取值为 `{ "ACS::RAM::AccessKey": [ "STS.NUQNP4PiGyckMsNiGELCs****"]}` ，表示本次角色扮演获取的临时凭证。
- `eventTime` ：事件的发生时间（UTC格式）。取值为 `2021-08-02T06:05:20Z` ，表示北京时间2021年08月02日14:05:20。

4.5.5. 通过角色SSO查询操作审计事件

进行角色SSO时，通过调用AssumeRoleWithSAML接口，可以获取一个扮演该角色的临时身份。本文为您介绍通过角色SSO查询操作审计事件的示例及含义。

示例

以下示例表示北京时间2021年08月02日14:05:24，企业自有身份用户通过扮演阿里云账号 `159498693826****` 下的 `testrole` 角色来查询操作审计事件。

```
{
  "apiVersion": "2016-11-11",
  "requestId": "3462D6AF-4434-4690-8CAD-E54AED8B",
  "eventType": "ApiCall",
  "userIdentity": {
    "accessKeyId": "STS.NUQNP4PiGyckMsNiGELCs****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T06:05:24Z"
      }
    },
    "accountId": "159498693826****",
    "principalId": "179432153826****:Alice@159498693826****.com",
    "type": "assumed-role",
    "userName": "testrole:Alice@159498693826****.com"
  },
  "acsRegion": "cn-shanghai",
  "eventName": "LookUpEvents",
  "requestParameters": {
    "stsTokenPrincipalName": "testrole:Alice@159498693826****.com",
    "AcsHost": "actiontrail.cn-hangzhou.aliyuncs.com",
    "ServiceCode": "actiontrail",
    "AcsProduct": "Actiontrail",
    "RequestId": "3462D6AF-4434-4690-8CAD-E54AED8B",
    "Region": "cn-hangzhou",
    "LookupAttribute.1.Value": "Write",
    "RegionId": "cn-hangzhou",
    "HostId": "actiontrail.cn-hangzhou.aliyuncs.com",
    "stsTokenPlayerUid": 10001,
    "LookupAttribute.1.Key": "EventRW"
  },
  "eventSource": "actiontrail.cn-hangzhou.aliyuncs.com",
  "serviceName": "Actiontrail",
  "eventTime": "2021-08-02T06:05:24Z",
  "userAgent": "",
  "eventId": "3462D6AF-4434-4690-8CAD-E54A****",
  "additionalEventData": {
    "Scheme": "https"
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```

示例中关键字段含义如下：

- `userIdentity.accountId` ：请求者的阿里云账号ID。取值为 `159498693826****` ，表示RAM角色的阿里云账号。
- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表

示被扮演的角色名称，`sessionName`表示进行角色扮演时指定的名称。取值为`testrole:Alice@159498693826****.com`，表示被扮演的RAM角色名称是`testrole`，进行角色扮演时指定的名称为`Alice@159498693826****.com`。

- `userIdentity.attributes.creationDate`：事件的发生时间（UTC格式）。取值为`2021-08-02T06:05:24Z`，表示北京时间2021年08月02日14:05:24。

4.6. 订单相关事件

4.6.1. 资源购买事件

当您使用阿里云服务的控制台、API或售卖页面购买资源时，会产生资源购买事件。本文为您举例说明资源购买事件。

> **说明** 当您使用阿里云服务的控制台或API购买资源时，可能出现跟API名称同名的资源购买事件，例如：CreateInstance事件。当您使用售卖页面购买资源时，资源购买事件名称大多为Create。

以下示例表示，在北京时间2021年08月02日14:30:17，阿里云账号`151266687691****`登录ECS服务售卖页面购买了一台ID为`i-bp67acfmxazb4p****`的ECS实例。

```
{
  "requestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
  "eventType": "ConsoleOperation",
  "userIdentity": {
    "accountId": "151266687691****",
    "principalId": "151266687691****",
    "type": "root-account",
    "userName": "root"
  },
  "acsRegion": "cn-hangzhou",
  "eventName": "Create",
  "requestParameters": {},
  "eventSource": "ecs.aliyuncs.com",
  "serviceName": "Ecs",
  "eventTime": "2021-08-02T06:30:17Z",
  "referencedResources": {
    "ACS::ECS::Instance": [
      "i-bp67acfmxazb4p****"
    ]
  },
  "userAgent": "AliyunConsole",
  "eventId": "2546c4b7-6b56-403e-97d3-500d8d29****",
  "additionalEventData": {
      "orderIds": "2105464****",
    "2105464****": {
      "resourceId": "i-bp67acfmxazb4p****",
      "articleConfig": {
        "vm_yundun_monitor": "1",
        "iooptimized": "optimized",
        "vm_cpu": "4",
        "vm_iz": "random",
        "vm_yundun_service": "1",
        "vm_web_type": "1",
        "vm_bandwidth": "1024,5",
        "systemdisk": "cloud_essd,/dev/xvda,200,PL0",
        "vm_region_no": "cn-hangzhou-dg-a01",
        "vm_vpc_switch_id": "vsw-bp1bnszwnkvjpdhkh****",
        "instance_type": "ecs.g6e,ecs-5,ecs.g6e.xlarge",
        "vm_os": "linux,64,centos_7_9_x64_20G_alibase_2021****.vhd",
        "vm_ram": "16384"
      }
    }
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```


示例中关键字段含义如下：

- `userIdentity.accountId` ：请求者的阿里云账号ID。
- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。

- `eventName`：事件名称。取值为 `Create`，表示资源购买事件。
- `eventTime`：事件的发生时间（UTC格式）。取值为 `2021-08-02T06:30:17Z`，表示北京时间2021年08月02日14:30:17。
- `referencedResources`：相关资源列表。取值为 `{"ACS::ECS::Instance": ["i-bp67acfmxazb4p****"]}`，表示ID为 `i-bp67acfmxazb4p****` 的ECS实例。

4.6.2. 资源续费事件

包年包月计费方式的资源到期后会影响使用，此时您需要对资源进行续费，产生资源续费事件。本文为您举例说明资源续费事件。

> **说明** 当您使用阿里云服务的控制台或API对资源进行续费时，可能出现跟API名称同名的资源续费事件，例如：RenewInstances事件。当您使用售卖页面对资源进行续费时，资源续费事件名称大多为Renew。

以下示例表示，在北京时间2021年08月02日12:06:36，系统自动为ECS实例 `i-bp67acfmxazb4p****` 进行了续费操作。

```
{
  "requestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
  "eventType": "AliyunServiceEvent",
  "userIdentity": {
    "type": "system"
  },
  "acsRegion": "cn-hangzhou",
  "eventName": "Renew",
  "requestParameters": {},
  "eventSource": "ecs.aliyuncs.com",
  "serviceName": "Ecs",
  "eventTime": "2021-08-02T04:06:36Z",
  "referencedResources": {
    "ACS::ECS::Instance": [
      "i-bp67acfmxazb4p****"
    ]
  },
  "userAgent": "usercenter2.aliyun.com/renew/auto",
  "eventId": "2546c4b7-6b56-403e-97d3-500d8d29****",
  "additionalEventData": {
      "2105464****": {
      "resourceId": "i-bp67acfmxazb4p****",
      "articleConfig": {
        "vm_bandwidth": "0,1",
        "systemdisk": "cloud_efficiency,/dev/xvda,80",
        "vm_region_no": "cn-hangzhou-dg-a01",
        "iooptimized": "optimized",
        "vm_cpu": "2",
        "vm_iz": "cn-hangzhou-i",
        "datadisk": "cloud_ssd,40,true",
        "instance_type": "ecs.g6,ecs-5,ecs.g6.large",
        "vm_os": "linux,64,centos_8_3_x64_20G_alibase_2021****.vhd",
        "vm_ram": "8192",
        "vm_web_type": "1"
      }
    },
    "orderIds": "2105464****"
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "Internal"
}
```


示例中关键字段含义如下：

- `userIdentity.type`：请求者的身份类型。取值为 `system`，表示阿里云服务，即事件由系统自动发起。
- `eventName`：事件名称。取值为 `Renew`，表示资源续费事件。
- `referencedResources`：事件影响的资源列表。取值为 `{"ACS::ECS::Instance": ["i-bp67acfmxazb4p****"]}`，表示ID为 `i-bp67acfmxazb4p****` 的ECS实例。

- `eventTime`：事件的发生时间（UTC格式）。取值为`2021-08-02T04:06:36Z`，表示北京时间2021年08月02日12:06:36。

4.6.3. 资源变配事件

资源购买后可以根据业务需求进行变配，此时会产生资源变配事件。本文为您举例说明资源变配事件。

> **说明** 当您使用阿里云服务的控制台或API对资源进行变配时，可能出现跟API名称同名的资源变配事件，例如：ModifyInstance事件。当您使用售卖页面对资源进行变配时，资源变配事件名称大多为Modify。

以下示例表示，在北京时间2021年08月02日15:04:50，阿里云账号`151266687691****`登录SLB服务售卖页面对SLB实例`i-lb-bp1h66tp5uat8********`进行了变配操作。

```
{
  "eventId": "2546c4b7-6b56-403e-97d3-500d8d29****",
  "eventVersion": 1,
  "eventSource": "slb.aliyuncs.com",
  "requestParameters": {},
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "AliyunConsole",
  "eventType": "ConsoleOperation",
  "referencedResources": {
    "ACS::SLB::LoadBalancer": [
      "lb-bp1h66tp5uat8****"
    ]
  },
  "userIdentity": {
    "accountId": "151266687691****",
    "principalId": "151266687691****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Slb",
  "additionalEventData": {
    "2105464****": {
      "resourceId": "lb-bp1h66tp5uat8****",
      "articleConfig": {
        "slb_web_type": "0",
        "slaveZoneId": "cn-hangzhou-g",
        "slb_bandwidth_max": "25600",
        "slb_flow_out": "0",
        "masterZoneId": "cn-hangzhou-b",
        "slb_yundun_service": "1",
        "slb_rentalfee": "1",
        "billing_component": "excludeflowout",
        "slb_instance": "internet",
        "loadbalancerSpec": "slb.s2.small",
        "slb_region_no": "cn-hangzhou-dg-a01",
        "ZoneType": "many"
      }
    },
    "2105464****": {
      "resourceId": "lb-bp1h66tp5uat8****",
      "articleConfig": {}
    },
    "orderIds": "2105464****,2105464****"
  },
  "requestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
  "eventTime": "2021-08-02T07:04:50Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "Modify"
}
```


示例中关键字段含义如下：

- `userIdentity.accountId` ：请求者的阿里云账号ID。
- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
- `eventName` ：事件名称。取值为 `Modify` ，表示变配事件。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::SLB::LoadBalancer": ["lb-bp1h66tp5uat8****"]}` ，表示ID为 `lb-bp1h66tp5uat8****` 的SLB实例。
- `eventTime` ：事件的发生时间（UTC格式）。取值为 `2021-08-02T07:04:50Z` ，表示北京时间2021年08月02日15:04:50。

4.6.4. 资源释放事件

当您不再需要已购买资源时可以释放资源，以节省成本，此时会产生资源释放事件。本文为您举例说明资源释放事件。

> **说明** 当您使用阿里云服务的控制台或API释放资源时，可能出现跟API名称同名的资源释放事件，例如：DeleteInstances事件。按量付费或包年包月实例到期后系统自动释放，此时资源释放事件名称大多为Release。

以下示例表示，在北京时间2021年08月02日12:06:36，系统自动释放了已到期的ECS实例 `i-bp67acfmxazb4p****` 。

```
{
  "requestId": "2546c4b7-6b56-403e-97d3-500d8d29339a",
  "eventType": "AliyunServiceEvent",
  "userIdentity": {
    "type": "system",
    "userName": "ecs.aliyuncs.com"
  },
  "acsRegion": "cn-hangzhou",
  "eventName": "Release",
  "requestParameters": {
    "RegionId": "cn-hangzhou-dg-a01"
  },
  "eventSource": "ecs.aliyuncs.com",
  "serviceName": "Ecs",
  "eventTime": "2021-08-02T04:06:36Z",
  "referencedResources": {
    "ACS::ECS::Instance": [
      i-bp67acfmxazb4p****"
    ]
  },
  "userAgent": "ecs.aliyuncs.com",
  "eventId": "2546c4b7-6b56-403e-97d3-500d8d29****",
  "additionalEventData": [],
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "Internal"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `system` ，表示阿里云服务，即事件由系统自动发起。
- `eventName` ：事件名称。取值为 `Release` ，表示资源释放事件。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::ECS::Instance": ["i-bp67acfmxazb4p****"]}` ，表示ID为 `i-bp67acfmxazb4p****` 的ECS实例。
- `eventTime` ：事件的发生时间（UTC格式）。取值为 `2021-08-02T04:06:36Z` ，表示北京时间2021年08月02日12:06:36。

4.7. 常见云服务事件示例

4.7.1. CDN

操作审计支持查询阿里云内容分发网络CDN（Content Delivery Network）相关事件。您可以快速查询CDN事件并获取事件发生的时间、地域、域名等信息。本文为您举例说明CDN相关事件。

阿里云账号通过控制台添加CDN加速域名

以下示例表示，在北京时间2021年08月05日14:10:01，阿里云账号调用AddCdnDomain接口通过CDN控制台添加了CDN加速域名 `example.com` 。

```
{
  "eventId": "3F44719F-9858-5016-AC54-794BBEE449C3",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "3F44719F-9858-5016-AC54-794BBEE449C3"
  },
  "eventSource": "cdn-share.aliyuncs.com",
  "requestParameters": {
    "charset": "UTF-8",
    "AcsHost": "cdn-share.aliyuncs.com",
    "AcsProduct": "Cdn",
    "RequestId": "3F44719F-9858-5016-AC54-794BBEE449C3",
    "ResourceGroupId": "rg-acfmxl27ech****",
    "Scope": "domestic",
    "DomainName": "example.com",
    "AcceptLanguage": "zh-CN",
    "CdnType": "web",
    "HostId": "cdn-share.aliyuncs.com",
    "Sources": [
      {
        "Type": "oss",
        "Content": "hao-nan.oss-cn-shanghai.aliyuncs.com",
        "Priority": "20",
        "Port": 80,
        "index": 0,
        "Weight": "10"
      }
    ]
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "cdnnext.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
```

```
    "ACS::CDN::Domain": [
      "cdns.example.com"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T06:10:01Z"
      }
    },
    "accountId": "128022060925****",
    "principalId": "128022060925****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Cdn",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2018-05-10",
  "requestId": "3F44719F-9858-5016-AC54-794BBEE449C3",
  "eventTime": "2021-08-05T06:10:01Z",
  "isGlobal": true,
  "acsRegion": "cn-shanghai",
  "eventName": "AddCdnDomain"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Cdn` ，表示CDN。
- `eventName` ：事件名称。取值为 `AddCdnDomain` ，表示添加CDN加速域名。
- `referencedResources` ：相关资源列表。取值为 `{"ACS::CDN::Domain": ["example.com"}` ，表示CDN加速域名 `example.com` 。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T06:10:01Z` ，表示北京时间2021年08月05日14:10:01。

RAM用户通过控制台添加CDN加速域名

以下示例表示，在北京时间2021年08月05日13:54:39，RAM用户 `dev` 调用AddCdnDomain接口通过CDN控制台添加了CDN加速域名 `example.com` 。

```
{
  "eventId": "93DA5CD8-7D32-51E1-ACC5-7EFE0E1AD93E",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "93DA5CD8-7D32-51E1-ACC5-7EFE0E1AD93E",
  },
  "eventSource": "cdn-share.aliyuncs.com",
  "requestParameters": {
    "charset": "UTF-8",
```

```
    "AcsHost": "cdn-share.aliyuncs.com",
    "AcsProduct": "Cdn",
    "RequestId": "93DA5CD8-7D32-51E1-ACC5-7EFE0E1AD93E",
    "Scope": "domestic",
    "DomainName": "example.com",
    "AcceptLanguage": "zh-CN",
    "CdnType": "web",
    "HostId": "cdn-share.aliyuncs.com",
    "Sources": [
      {
        "Type": "oss",
        "Content": "lxhy-h5-****.oss-cn-chengdu.aliyuncs.com",
        "Priority": "20",
        "Port": 80,
        "index": 0,
        "Weight": "10"
      }
    ]
  },
  "errorCode": "DomainAlreadyExist",
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "cdn.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::CDN::Domain": [
      "example.com"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T05:54:39Z"
      }
    },
    "accountId": "159702607145****",
    "principalId": "24749552624582****",
    "type": "ram-user",
    "userName": "dev"
  },
  "serviceName": "Cdn",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2018-05-10",
  "requestId": "93DA5CD8-7D32-51E1-ACC5-7EFE0E1AD93E",
  "eventTime": "2021-08-05T05:54:39Z",
  "isGlobal": true,
  "acsRegion": "cn-shanghai",
  "eventName": "AddCdnDomain"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `userIdentity.userName` ：请求者的RAM用户名称。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Cdn` ，表示CDN。
- `eventName` ：事件名称。取值为 `AddCdnDomain` ，表示添加CDN加速域名。
- `referencedResources` ：相关资源列表。取值为 `{"ACS::CDN::Domain": ["example.com"]}` ，表示CDN实例 `example.com` 。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T05:54:39Z` ，表示北京时间2021年08月05日13:54:39。

RAM用户通过AK调用API添加CDN加速域名

以下示例表示，在北京时间2021年08月04日19:07:28，RAM用户 `Alice` 通过AK `LTAI4GHbFgwYxAHRqcsr****` 调用AddCdnDomain接口添加了CDN加速域名 `example.com` 。

```
{
  "eventId": "2FB7E0AD-F3E1-5164-BBDA-8A1D846F9176",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "2FB7E0AD-F3E1-5164-BBDA-8A1D846F9176",
    "Message": "Owner verification of the root domain failed.",
    "Recommend": "https://error-center.aliyun.com/status/search?Keyword=DomainOwnerVerifyFa
il&source=PopGw",
    "HostId": "cdn.aliyuncs.com",
    "Code": "DomainOwnerVerifyFail"
  },
  "errorMessage": "Owner verification of the root domain failed.",
  "eventSource": "cdn.aliyuncs.com",
  "requestParameters": {
    "q": 0.9,
    "AcsHost": "cdn.aliyuncs.com",
    "AcsProduct": "Cdn",
    "RequestId": "2FB7E0AD-F3E1-5164-BBDA-8A1D846F9176",
    "DomainName": "example.com",
    "v": "b3",
    "CdnType": "web",
    "HostId": "cdn.aliyuncs.com",
    "Sources": [
      {
        "type": "domain",
        "content": "aliyundoc.com"
      }
    ]
  },
  "errorCode": "DomainOwnerVerifyFail",
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.87 Safari/537.36 SE 2.X MetaSr 1.0",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::CDN::Domain": [
      "example.com"
```

```
    ]
  },
  "userIdentity": {
    "accessKeyId": "LTAI4GHbFgwYxAHRqcsr****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-04T11:06:44Z"
      }
    },
    "accountId": "166878994059****",
    "principalId": "20223100810693****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Cdn",
  "additionalEventData": {
    "Scheme": "https",
    "CallerBid": "26842"
  },
  "apiVersion": "2018-05-10",
  "requestId": "2FB7E0AD-F3E1-5164-BBDA-8A1D846F9176",
  "eventTime": "2021-08-04T11:07:28Z",
  "isGlobal": true,
  "acsRegion": "cn-shanghai",
  "eventName": "AddCdnDomain"
}
```

示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAI4GHbFgwYxAHRqcsr****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `20223100810693****` 。
- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Cdn` ，表示CDN。
- `eventName` ：事件名称。取值为 `AddCdnDomain` ，表示添加CDN加速域名。
- `referencedResources` ：相关资源列表。取值为 `{"ACS::CDN::Domain": ["example.com"]}` ，表示CDN加速域名 `example.com` 。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-04T11:07:28Z` ，表示北京时间2021年08月04日19:07:28。

RAM用户通过角色扮演添加CDN加速域名

以下示例表示，在北京时间2021年08月02日14:15:46，阿里云账号 `111526800165****` 中的RAM用户通过扮演阿里云账号 `147048327155****` 下的RAM角色 `aliyunid-ag-ram-role-admin` ，添加了CDN加速域名 `example.com` 。

```
{
  "eventId": "79229ED7-C2B6-45C5-B665-23AF88783660",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "79229ED7-C2B6-45C5-B665-23AF88783660",
    "Message": "Owner verification of the root domain failed.",
```

```
    "Recommend": "https://error-center.aliyun.com/status/search?Keyword=DomainOwnerVerifyFa
il&source=PopGw",
    "HostId": "cdn.aliyuncs.com",
    "Code": "DomainOwnerVerifyFail"
  },
  "errorMessage": "Owner verification of the root domain failed.",
  "eventSource": "cdn.aliyuncs.com",
  "requestParameters": {
    "stsTokenPrincipalName": "aliyunid-ag-ram-role-admin/BASEMENT",
    "AcsHost": "cdn.aliyuncs.com",
    "AcsProduct": "Cdn",
    "RequestId": "79229ED7-C2B6-45C5-B665-23AF88783660",
    "DomainName": "example.com",
    "CdnType": "web",
    "RegionId": "cn-zhangjiakou",
    "HostId": "cdn.aliyuncs.com",
    "stsTokenPlayerUid": 111526800165****,
    "Sources": [
      {
        "port": 443,
        "type": "domain",
        "content": "aliyundoc.com"
      }
    ]
  },
  "errorCode": "DomainOwnerVerifyFail",
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "AlibabaCloud (Linux; amd64) Java/1.8.0_252-b09 Core/4.5.19 HTTPClient/Apach
eHttpClient",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::CDN::Domain": [
      "example.com"
    ]
  },
  "userIdentity": {
    "accessKeyId": "STS.NSrwtDuh5hbwR1gtWwZhS****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-07-25T02:40:34Z"
      }
    },
    "accountId": "147048327155****",
    "principalId": "30304522804117****:BASEMENT",
    "type": "assumed-role",
    "userName": "aliyunid-ag-ram-role-admin:BASEMENT"
  },
  "serviceName": "Cdn",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2018-05-10",
```

```
  "requestId": "79229ED7-C2B6-45C5-B665-23AF88783660",
  "eventTime": "2021-08-02T06:15:46Z",
  "isGlobal": true,
  "acsRegion": "cn-shanghai",
  "eventName": "AddCdnDomain"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `aliyunid-ag-ram-role-admin:BASEMENT` ，表示被扮演的RAM角色名称是 `aliyunid-ag-ram-role-admin` ，进行角色扮演时指定的名称为 `BASEMENT` 。
- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `111526800165****` 。
- `referencedResources` ：相关资源列表。取值为 `{"ACS::CDN::Domain": ["example.com"]}` ，表示CDN加速域名 `example.com` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Cdn` ，表示CDN。
- `eventName` ：事件名称。取值为 `AddCdnDomain` ，表示添加CDN加速域名。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-02T06:15:46Z` ，表示北京时间2021年08月02日14:15:46。

4.7.2. ECS

操作审计支持查询云服务器ECS（Elastic Compute Service）相关事件。当ECS操作出现异常时，您可以快速查询事件并获取事件发生的时间、地域、ECS实例等信息。本文为您举例说明ECS相关事件。

阿里云账号通过控制台停止ECS实例

以下示例表示，在北京时间2021年08月04日14:11:36，阿里云账号调用StopInstance接口停止了北京地域ID为 `i-2zeip56clb391fpf****` 的ECS实例。

```
{
  "eventId": "239EB588-CD24-522E-B0B5-174A1A588BE0",
  "eventVersion": 1,
  "eventSource": "ecs-cn-hangzhou-share.aliyuncs.com",
  "requestParameters": {
    "charset": "UTF-8",
    "AcsHost": "ecs-cn-hangzhou-share.aliyuncs.com",
    "AcsProduct": "Ecs",
    "RequestId": "239EB588-CD24-522E-B0B5-174A1A588BE0",
    "InstanceId": "i-2zeip56clb391fpf****",
    "ForceStop": false,
    "AcceptLanguage": "zh-CN"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "Apache-HttpClient/4.5.7 (Java/1.8.0_275)",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::ECS::Instance": [
      "i-2zeip56clb391fpf****"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-04T06:11:36Z"
      }
    },
    "accountId": "154735325685****",
    "principalId": "154735325685****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Ecs",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-05-26",
  "requestId": "239EB588-CD24-522E-B0B5-174A1A588BE0",
  "eventTime": "2021-08-04T06:11:36Z",
  "isGlobal": false,
  "acsRegion": "cn-beijing",
  "eventName": "StopInstance"
}
```


示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Ecs` ，表示ECS。
- `eventName` ：事件名称。取值为 `StopInstance` ，表示停止实例。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::ECS::Instance": ["i-2zeip56clb391`

`fpf****"]}`，表示ECS实例 `i-2zeip56clb391fpf****` 。

- `acsRegion` ：事件发生的地域。取值为 `cn-beijing` ，表示北京地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-04T06:11:36Z` ，表示北京时间2021年08月04日14:11:36。

RAM用户通过控制台停止ECS实例

以下示例表示，在北京时间2021年08月04日13:29:30，RAM用户 `ecs_operator3` 调用StopInstance接口停止了北京地域ID为 `i-2zegxcy8f0htnq1o****` 的ECS实例。

```
{
  "eventId": "5E197C8B-081F-5A0C-A86A-4B6F266CA80B",
  "eventVersion": 1,
  "eventSource": "ecs-cn-hangzhou.aliyuncs.com",
  "requestParameters": {
    "AcsHost": "ecs-cn-hangzhou.aliyuncs.com",
    "AcsProduct": "Ecs",
    "RequestId": "5E197C8B-081F-5A0C-A86A-4B6F266CA80B",
    "InstanceId": "i-2zegxcy8f0htnq1o****",
    "ForceStop": "True",
    "https": "False"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "ros.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::ECS::Instance": [
      "i-2zegxcy8f0htnq1o****"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-04T05:29:30Z"
      }
    },
    "accountId": "182872313731****",
    "principalId": "20499042382297****",
    "type": "ram-user",
    "userName": "ecs_operator3"
  },
  "serviceName": "Ecs",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-05-26",
  "requestId": "5E197C8B-081F-5A0C-A86A-4B6F266CA80B",
  "eventTime": "2021-08-04T05:29:30Z",
  "isGlobal": false,
  "acsRegion": "cn-beijing",
  "eventName": "StopInstance"
}
```


示例中关键字段含义如下：

- `userIdentity.type`：请求者的身份类型。取值为`ram-user`，表示RAM用户。
- `userIdentity.userName`：请求者的RAM用户名称。
- `serviceName`：事件相关的阿里云服务名称。取值为`Ecs`，表示ECS。
- `eventName`：事件名称。取值为`StopInstance`，表示停止实例。

- `referencedResources`：事件影响的资源列表。取值为 `{"ACS::ECS::Instance": ["i-2zegxcy8f0htnq1o****"]}`，表示ECS实例 `i-2zegxcy8f0htnq1o****`。
- `acsRegion`：事件发生的地域。取值为 `cn-beijing`，表示北京地域。
- `eventTime`：事件发生的时间（UTC格式）。取值为 `2021-08-04T05:29:30Z`，表示北京时间2021年08月04日13:29:30。

RAM用户通过AK调用API停止ECS实例

以下示例表示，在北京时间2021年08月04日11:42:20，RAM用户通过AK `LTAIIzSdydLc****` 调用StopInstance接口停止了杭州地域ID为 `i-bp1buct0j6jywbfp****` 的ECS实例。

```
{
  "eventId": "A9171DC9-638E-5561-BA2E-69B1B956C8F4",
  "eventVersion": 1,
  "eventSource": "ecs.aliyuncs.com",
  "requestParameters": {
    "AcsHost": "ecs.aliyuncs.com",
    "AcsProduct": "Ecs",
    "RequestId": "A9171DC9-638E-5561-BA2E-69B1B956C8F4",
    "InstanceId": "i-bp1buct0j6jywbfp****",
    "ForceStop": true
  },
  "sourceIpAddress": "192.168.XX.XX",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::ECS::Instance": [
      "i-bp1buct0j6jywbfp****"
    ]
  },
  "userIdentity": {
    "accessKeyId": "LTAIIzSdydLc****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-04T03:42:20Z"
      }
    },
    "accountId": "122196828764****",
    "principalId": "23079124770506****",
    "type": "ram-user",
    "userName": "hz-perf-cluster"
  },
  "serviceName": "Ecs",
  "additionalEventData": {
    "Scheme": "https",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-05-26",
  "requestId": "A9171DC9-638E-5561-BA2E-69B1B956C8F4",
  "eventTime": "2021-08-04T03:42:20Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "StopInstance"
}
```


示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAIIzSdydLc****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `23079124770506****` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Ecs` ，表示ECS。
- `eventName` ：事件名称。取值为 `StopInstance` ，表示停止实例。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::ECS::Instance": ["i-bp1buct0j6jyw`

`bfp****"]}`，表示ECS实例 `i-bp1buct0j6jywbfp****` 。

- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-04T03:42:20Z` ，表示北京时间2021年08月04日11:42:20。

RAM角色通过角色扮演停止ECS实例

以下示例表示，在北京时间2021年08月04日14:50:10，阿里云服务弹性伸缩通过扮演服务关联角色 `aliyunserviceroleforautoscaling` ，停止了北京地域ID为 `i-2zeeryqubk6402qw****` 的ECS实例。


```
{
  "eventId": "E7233050-120B-5684-93E4-49A6754D8252",
  "eventVersion": 1,
  "eventSource": "ecs-cn-hangzhou-inner.aliyuncs.com",
  "requestParameters": {
    "securityToken": "CAISlQJ1q6Ft5B2yfSjIr5beG4322+YZ0baYaVWElTksTe4VtfD8szz2IH9NenVoA+wet
Pg+mmtT6/welr5+UIQAXkHfdsp36NFa+hiWb4fPstGx8eThLDMywS/BZSTg1er+Ps/bLrqECNrPBnnAkihsu8iYERyp
Q12iN7CQlJdjda55dwKkbD1Adrw0T0kY3618D3bKMuu3ORPHm3fZCFES2jBxkmRi86+ysKb+g1j89AShmrJJ9tqoc8P
7NpU2Z8xFPo3rjLAsRM3oyzVN7hVGzqBygZFf9C3P1tPnWAYIvUneabaMqIE+clQiO/JmAdlNqPntiPtjt/bNlo/60R
FJMO9SSS3CWIe7y8LAGeWmJgLCqWAjiPSnGoABEJShxrqPitmfV2/wirLqZhYsiElHL0LIma0PRByFDMqa3Jo5O1xee
GvbhnLnHiqdTYUjap8X/fiew+pgNlLmjPwZ7AjWKFZVuO3yedhEpUE7aE14PJ2asbOw2b5T1CVH9FHYNWaCUliWBTIj
AqI3UYkRktOiecZ2ZExp8g3+****=",
    "stsTokenPrincipalName": "aliyunserviceroleforautoscaling/ess-session-ecs_default",
    "AcsHost": "ecs-cn-hangzhou-inner.aliyuncs.com",
    "ServiceCode": "ecs",
    "AcsProduct": "Ecs",
    "RequestId": "E7233050-120B-5684-93E4-49A6754D8252",
    "InstanceId": "i-2zeeryqubk6402qw****",
    "RegionId": "cn-beijing",
    "stsTokenPlayerUid": 158643649596****
  },
  "sourceIpAddress": "Internal",
  "userAgent": "AlibabaCloud (Linux; amd64) Java/1.8.0_102-b52 Core/4.5.3 HTTPClient/Intern
alHttpClient",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::ECS::Instance": [
      "i-2zeeryqubk6402qw****"
    ]
  },
  "userIdentity": {
    "accessKeyId": "STS.NUkP7B698ftsks5q9yAa9****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-04T06:50:10Z"
      }
    },
    "accountId": "138549619371****",
    "principalId": "37164024024963****:ess-session-ecs_default",
    "type": "assumed-role",
    "userName": "aliyunserviceroleforautoscaling:ess-session-ecs_default"
  },
  "serviceName": "Ecs",
```

```
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-05-26",
  "requestId": "E7233050-120B-5684-93E4-49A6754D8252",
  "eventTime": "2021-08-04T06:50:10Z",
  "isGlobal": false,
  "acsRegion": "cn-beijing",
  "eventName": "StopInstance"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `aliyunservicerolefor autoscaling:ess-session-ecs_default` ，表示被扮演的RAM角色名称是 `aliyunserviceroleforautosc aling` ，进行角色扮演时指定的名称为 `ess-session-ecs_default` 。

  > **说明** `aliyunserviceroleforautoscaling` 是弹性伸缩服务的服务关联角色，用于授权弹性伸缩服务访问关联云资源。

- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `158643649596****` 。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::ECS::Instance": ["i-2zeeryqubk640 2qw****"]}` ，表示ECS实例 `i-2zeeryqubk6402qw****` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Ecs` ，表示ECS。
- `eventName` ：事件名称。取值为 `StopInstance` ，表示停止实例。
- `acsRegion` ：事件发生的地域。取值为 `cn-beijing` ，表示北京地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-04T06:50:10Z` ，表示北京时间2021年08月04日14:50:10。

4.7.3. KMS

操作审计支持查询密钥管理服务KMS（Key Management Service）相关事件。您可以快速查询KMS事件并获取事件发生的时间、地域和密钥等信息。本文为您举例说明KMS相关事件。

阿里云账号通过控制台获取密钥信息

以下示例表示，在北京时间2021年08月05日17:21:32，阿里云账号调用DescribeKey接口获取了杭州地域密钥 `3a6a031d-87ad-4a84-9c17-aa22e0b0****` 的信息。

```
{
  "eventId": "ab35a7a7-373a-4a36-a4f8-01fd6adcc6a0",
  "eventVersion": 1,
  "eventSource": "kms-intranet.cn-hangzhou.aliyuncs.com",
  "requestParameters": {
    "KeyId": "3a6a031d-87ad-4a84-9c17-aa22e0b0****"
  },
  "sourceIpAddress": "Internal",
  "userAgent": "AliyunConsole",
  "eventType": "ApiCall",
  "userIdentity": {
    "accountId": "506899367883****",
    "principalId": "506899367883****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Kms",
  "apiVersion": "2016-01-20",
  "requestId": "ab35a7a7-373a-4a36-a4f8-01fd6adcc6a0",
  "eventTime": "2021-08-05T09:21:32Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DescribeKey"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Kms` ，表示KMS。
- `eventName` ：事件名称。取值为 `DescribeKey` ，表示获取密钥信息。
- `requestParameters.KeyId` ：密钥ID。取值为 `3a6a031d-87ad-4a84-9c17-aa22e0b0****` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T09:21:32Z` ，表示北京时间2021年08月05日17:21:32。

RAM用户通过控制台获取密钥信息

以下示例表示，在北京时间2021年08月05日16:53:03，RAM用户 `Alice` 调用DescribeKey接口获取了杭州地域密钥 `e1ea5c30-04d3-41e4-b445-1eb5b656****` 的信息。

```
{
  "eventId": "c8d094ca-64b8-49cf-bbf3-2a9b540abed9",
  "eventVersion": 1,
  "eventSource": "kms-intranet.cn-hangzhou.aliyuncs.com",
  "requestParameters": {
    "KeyId": "e1ea5c30-04d3-41e4-b445-1eb5b656****"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "AliyunConsole",
  "eventType": "ApiCall",
  "userIdentity": {
    "accountId": "111737649404****",
    "principalId": "23899132441193****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Kms",
  "apiVersion": "2016-01-20",
  "requestId": "c8d094ca-64b8-49cf-bbf3-2a9b540abed9",
  "eventTime": "2021-08-05T08:53:03Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DescribeKey"
}
```

示例中关键字段含义如下：

- `userIdentity.type`：请求者的身份类型。取值为`ram-user`，表示RAM用户。
- `userIdentity.userName`：请求者的RAM用户名称。
- `serviceName`：事件相关的阿里云服务名称。取值为`Kms`，表示KMS。
- `eventName`：事件名称。取值为`DescribeKey`，表示获取密钥信息。
- `requestParameters.KeyId`：密钥ID。取值为`e1ea5c30-04d3-41e4-b445-1eb5b656****`。
- `acsRegion`：事件发生的地域。取值为`cn-hangzhou`，表示杭州地域。
- `eventTime`：事件发生的时间（UTC格式）。取值为`2021-08-05T08:53:03Z`，表示北京时间2021年08月05日16:53:03。

RAM用户通过AK调用API获取密钥信息

以下示例表示，在北京时间2021年08月05日17:02:30，RAM用户`kms-test`通过AK`LTAI4GDYPA5jNycoezLH****`调用DescribeKey接口获取了杭州地域密钥`e1ea5c30-04d3-41e4-b445-1eb5b656****`的信息。

```
{
  "eventId": "da43d031-cf5a-44ec-aec8-4a13f468aa12",
  "eventVersion": 1,
  "eventSource": "kms.cn-hangzhou.aliyuncs.com",
  "requestParameters": {
    "KeyId": "e1ea5c30-04d3-41e4-b445-1eb5b656****"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "AlibabaCloud (Linux; amd64) Java/1.8.0_212-b04 Core/4.5.1 HTTPClient/Apache
HttpClient",
  "eventType": "ApiCall",
  "userIdentity": {
    "accessKeyId": "LTAI4GDYPA5jNycoezLH****",
    "accountId": "164165083897****",
    "principalId": "21682348916186****",
    "type": "ram-user",
    "userName": "kms-test"
  },
  "serviceName": "Kms",
  "apiVersion": "2016-01-20",
  "requestId": "da43d031-cf5a-44ec-aec8-4a13f468aa12",
  "eventTime": "2021-08-05T09:02:30Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DescribeKey"
}
```

示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAI4GDYPA5jNycoezLH****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `21682348916186****` 。
- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `userIdentity.userName` ：请求者的RAM用户名称。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Kms` ，表示KMS。
- `eventName` ：事件名称。取值为 `DescribeKey` ，表示获取密钥信息。
- `requestParameters.KeyId` ：密钥ID。取值为 `e1ea5c30-04d3-41e4-b445-1eb5b656****` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T09:02:30Z` ，表示北京时间2021年08月05日17:02:30。

RAM用户通过角色扮演获取密钥信息

以下示例表示，在北京时间2021年08月05日17:20:28，阿里云账号 `132295042695****` 中的RAM用户通过扮演账号 `119997133354****` 下的RAM角色 `aliyunedasdefaultrole` ，获取了杭州地域密钥 `e1ea5c30-04d3-41e4-b445-1eb5b656****` 的信息。

```
{
  "eventId": "4e059394-8b95-4788-84cf-efe7aa8f6935",
  "eventVersion": 1,
  "eventSource": "kms.cn-hangzhou.aliyuncs.com",
  "requestParameters": {
    "KeyId": "e1ea5c30-04d3-41e4-b445-1eb5b656****",
    "stsTokenPlayerUid": "132295042695****"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "AlibabaCloud (Linux; amd64) Java/1.8.0_92-b18 Core/4.5.6 HTTPClient/ApacheH
ttpClient",
  "eventType": "ApiCall",
  "userIdentity": {
    "accessKeyId": "STS.NUCmmh2n5RQcqryWqxsuv****",
    "accountId": "119997133354****",
    "principalId": "34933955188809****:fb23c186-5930-498a-a630-0a****",
    "type": "assumed-role",
    "userName": "aliyunedasdefaultrole:fb23c186-5930-498a-a630-0a****"
  },
  "serviceName": "Kms",
  "apiVersion": "2016-01-20",
  "requestId": "4e059394-8b95-4788-84cf-efe7aa8f6935",
  "eventTime": "2021-08-05T09:20:28Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DescribeKey"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `aliyunedasdefaultrole:fb23c186-5930-498a-a630-0a****` ，表示被扮演的RAM角色名称是 `aliyunedasdefaultrole` ，进行角色扮演时指定的名称为 `fb23c186-5930-498a-a630-0a****` 。

  > **说明** 企业级分布式应用服务EDAS默认使用 `aliyunedasdefaultrole` 角色来访问您在其他云服务中的资源。

- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `132295042695****` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Kms` ，表示KMS。
- `eventName` ：事件名称。取值为 `DescribeKey` ，表示获取密钥信息。
- `requestParameters.KeyId` ：密钥ID。取值为 `e1ea5c30-04d3-41e4-b445-1eb5b656****` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T09:20:28Z` ，表示北京时间2021年08月05日17:20:28。

4.7.4. OSS

操作审计支持查询阿里云对象存储OSS（Object Storage Service）中存储空间（Bucket）的部分管控事件。您可以快速查询管控事件并获取事件发生的时间、地域、关联的存储空间（Bucket）等信息。本文为您举例说明OSS相关事件。

> **说明** OSS存储空间（Bucket）管控事件列表，请参见特殊云服务事件说明。

创建存储空间

- **阿里云账号通过控制台创建存储空间**
  以下示例表示，在北京时间2021年08月09日16:24:43，阿里云账号 `189217171671****` 调用PutBucket接口创建了OSS存储空间 `test-123` 。

```
{
  "eventId": "6110E64B004C4034363CDC5E",
  "eventVersion": 1,
  "eventSource": "test-123.oss-cn-hangzhou-cross.aliyuncs.com",
  "sourceIpAddress": "Internal",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::OSS::Bucket": [
      "test-123"
    ]
  },
  "userIdentity": {
    "accountId": "189217171671****",
    "principalId": "189217171671****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Oss",
  "additionalEventData": {
    "CallerBid": "26842"
  },
  "requestId": "6110E64B004C4034363CDC5E",
  "eventTime": "2021-08-09T08:24:43Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "PutBucket"
}
```

  示例中关键字段含义如下：
  - `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
  - `serviceName` ：事件相关的阿里云服务名称。取值为 `Oss` ，表示对象存储OSS。
  - `eventName` ：事件名称。取值为 `PutBucket` ，表示创建存储空间。
  - `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::OSS::Bucket": ["test-123"]}` ，表示存储空间名称为 `test-123` 。
  - `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
  - `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-09T08:24:43Z` ，表示北京时间2021年08月09日16:24:43。

- **RAM用户通过控制台创建存储空间**

以下示例表示，在北京时间2021年08月09日16:47:02，RAM用户 `Alice` 调用PutBucket接口在杭州地域创建了OSS存储空间 `test-123` 。

```
{
  "eventId": "6110EB86141D4F39389301A2",
  "eventVersion": 1,
  "eventSource": "test-123.oss-cn-hangzhou-cross.aliyuncs.com",
  "sourceIpAddress": "Internal",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::OSS::Bucket": [
      "test-123"
    ]
  },
  "userIdentity": {
    "accountId": "189217171671****",
    "principalId": "26135379175722****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Oss",
  "additionalEventData": {
    "CallerBid": "26842"
  },
  "requestId": "6110EB86141D4F39389301A2",
  "eventTime": "2021-08-09T08:47:02Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "PutBucket"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `userIdentity.userName` ：请求者的RAM用户名称。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Oss` ，表示对象存储OSS。
- `eventName` ：事件名称。取值为 `PutBucket` ，表示创建存储空间。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::OSS::Bucket": ["test-123"]}` ，表示存储空间名称为 `test-123` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-09T08:47:02Z` ，表示北京时间2021年08月09日16:47:02。

- **RAM用户通过AK调用API创建存储空间**
  以下示例表示，在北京时间2021年08月09日16:41:04，RAM用户 `Alice` 通过AK `LTAI4FimByATXqiFP9ni****` 调用PutBucket接口在杭州地域创建了OSS存储空间 `test-123` 。

```
{
  "eventId": "6110EA20EEC7423834B49315",
  "eventVersion": 1,
  "eventSource": "test-123.oss-cn-hangzhou.aliyuncs.com",
  "sourceIpAddress": "192.168.XX.XX",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::OSS::Bucket": [
      "test-123"
    ]
  },
  "userIdentity": {
    "accessKeyId": "LTAI4FimByATXqiFP9ni****",
    "accountId": "127894427633****",
    "principalId": "22111447899160****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Oss",
  "additionalEventData": {
    "CallerBid": "26842"
  },
  "requestId": "6110EA20EEC7423834B49315",
  "eventTime": "2021-08-09T08:41:04Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "PutBucket"
}
```

示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAI4FimByATXqiFP9ni****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `22111447899160****` 。
- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Oss` ，表示对象存储OSS。
- `eventName` ：事件名称。取值为 `PutBucket` ，表示创建存储空间。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::OSS::Bucket": ["test-123"]}` ，表示存储空间名称为 `test-123` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-09T08:41:04Z` ，表示北京时间2021年08月09日16:41:04。

- **RAM用户通过角色扮演创建存储空间**
  以下示例表示，在北京时间2021年08月09日16:49:20，阿里云账号 `189217171671****` 中的RAM用户通过扮演自己账号下的RAM角色 `oss-role` ，调用Put Bucket接口在杭州地域创建了OSS存储空间 `test-123` 。

```
{
  "eventId": "6110EC1086A4803039D44C7A",
  "eventVersion": 1,
  "eventSource": "test-123.oss-cn-hangzhou-cross.aliyuncs.com",
  "requestParameters": {
    "stsTokenPlayerUid": "189217171671****"
  },
  "sourceIpAddress": "Internal",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::OSS::Bucket": [
      "test-123"
    ]
  },
  "userIdentity": {
    "accessKeyId": "STS.NTThE5nV7fh3q4fPkQdQH****",
    "accountId": "189217171671****",
    "principalId": "39484351102463****:roleTest123",
    "type": "assumed-role",
    "userName": "oss-role:roleTest123"
  },
  "serviceName": "Oss",
  "additionalEventData": {
    "CallerBid": "26842"
  },
  "requestId": "6110EC1086A4803039D44C7A",
  "eventTime": "2021-08-09T08:49:20Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "PutBucket"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `oss-role:roleTest123` ，表示被扮演的RAM角色名称是 `oss-role` ，进行角色扮演时指定的名称为 `roleTest123` 。
- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `189217171671****` 。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::OSS::Bucket": ["test-123"]}` ，表示OSS存储空间名称为 `test-123` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Oss` ，表示对象存储OSS。
- `eventName` ：事件名称。取值为 `PutBucket` ，表示创建存储空间。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-09T08:49:20Z` ，表示北京时间2021年08月09日16:49:20。

删除存储空间

- **阿里云账号通过控制台删除存储空间**

以下示例表示，在北京时间2021年08月09日16:26:56，阿里云账号 `189217171671****` 调用DeleteBucket接口删除了OSS存储空间 `test-123` 。

```
{
  "eventId": "6110E6D0E310653237000581",
  "eventVersion": 1,
  "eventSource": "test-123.oss-cn-hangzhou-cross.aliyuncs.com",
  "sourceIpAddress": "Internal",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::OSS::Bucket": [
      "test-123"
    ]
  },
  "userIdentity": {
    "accountId": "189217171671****",
    "principalId": "189217171671****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Oss",
  "additionalEventData": {
    "CallerBid": "26842"
  },
  "requestId": "6110E6D0E310653237000581",
  "eventTime": "2021-08-09T08:26:56Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DeleteBucket"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Oss` ，表示对象存储OSS。
- `eventName` ：事件名称。取值为 `DeleteBucket` ，表示删除存储空间。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::OSS::Bucket": ["test-123"]}` ，表示存储空间名称为 `test-123` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-09T08:26:56Z` ，表示北京时间2021年08月09日16:26:56。

- **RAM用户通过控制台删除存储空间**
  以下示例表示，在北京时间2021年08月09日16:47:11，RAM用户 `Alice` 调用DeleteBucket接口在杭州地域删除了OSS存储空间 `test-123` 。

```
{
  "eventId": "6110EB8F7912BA33318EFEC6",
  "eventVersion": 1,
  "eventSource": "test-123.oss-cn-hangzhou-cross.aliyuncs.com",
  "sourceIpAddress": "Internal",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::OSS::Bucket": [
      "test-123"
    ]
  },
  "userIdentity": {
    "accountId": "189217171671****",
    "principalId": "26135379175722****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Oss",
  "additionalEventData": {
    "CallerBid": "26842"
  },
  "requestId": "6110EB8F7912BA33318EFEC6",
  "eventTime": "2021-08-09T08:47:11Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DeleteBucket"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `userIdentity.userName` ：请求者的RAM用户名称。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Oss` ，表示对象存储OSS。
- `eventName` ：事件名称。取值为 `DeleteBucket` ，表示删除存储空间。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::OSS::Bucket": ["test-123"]}` ，表示存储空间名称为 `test-123` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-09T08:47:11Z` ，表示北京时间2021年08月09日16:47:11。

- **RAM用户通过AK调用API删除存储空间**
  以下示例表示，在北京时间2021年08月09日17:14:50，RAM用户 `Alice` 通过AK `LTAI4G2wxd32KLGARfid****` 调用DeleteBucket接口在杭州地域删除了OSS存储空间 `test-123` 。

```
{
  "eventId": "6110F20A1B319838338E95DB",
  "eventVersion": 1,
  "eventSource": "test-123.oss-cn-hangzhou-internal.aliyuncs.com",
  "sourceIpAddress": "192.168.XX.XX",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::OSS::Bucket": [
      "test-123"
    ]
  },
  "userIdentity": {
    "accessKeyId": "LTAI4G2wxd32KLGARfid****",
    "accountId": "184538913914****",
    "principalId": "24576749206513****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Oss",
  "additionalEventData": {
    "CallerBid": "26842"
  },
  "requestId": "6110F20A1B319838338E95DB",
  "eventTime": "2021-08-09T09:14:50Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DeleteBucket"
}
```

示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAI4G2wxd32KLGARfid****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `24576749206513****` 。
- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Oss` ，表示对象存储OSS。
- `eventName` ：事件名称。取值为 `DeleteBucket` ，表示删除存储空间。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::OSS::Bucket": ["test-123"]}` ，表示存储空间名称为 `test-123` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-09T09:14:50Z` ，表示北京时间2021年08月09日17:14:50。

- **RAM用户通过角色扮演删除存储空间**
  以下示例表示，在北京时间2021年08月09日16:49:27，阿里云账号 `189217171671****` 中的RAM用户通过扮演自己账号下的RAM角色 `oss-role` ，调用DeleteBucket接口在杭州地域删除了OSS存储空间 `test-123` 。

```
{
  "eventId": "6110EC176C9A3A31332831C7",
  "eventVersion": 1,
  "eventSource": "test-123.oss-cn-hangzhou-cross.aliyuncs.com",
  "requestParameters": {
    "stsTokenPlayerUid": "189217171671****"
  },
  "sourceIpAddress": "Internal",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::OSS::Bucket": [
      "test-123"
    ]
  },
  "userIdentity": {
    "accessKeyId": "STS.NTThE5nV7fh3q4fPkQdQH****",
    "accountId": "189217171671****",
    "principalId": "39484351102463****:roleTest123",
    "type": "assumed-role",
    "userName": "oss-role:roleTest123"
  },
  "serviceName": "Oss",
  "additionalEventData": {
    "CallerBid": "26842"
  },
  "requestId": "6110EC176C9A3A31332831C7",
  "eventTime": "2021-08-09T08:49:27Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DeleteBucket"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `oss-role:roleTest123` ，表示被扮演的RAM角色名称是 `oss-role` ，进行角色扮演时指定的名称为 `roleTest123` 。
- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `189217171671****` 。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::OSS::Bucket": ["test-123"]}` ，表示OSS存储空间名称为 `test-123` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Oss` ，表示对象存储OSS。
- `eventName` ：事件名称。取值为 `DeleteBucket` ，表示删除存储空间。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-09T08:49:27Z` ，表示北京时间2021年08月09日16:49:27。

4.7.5. RDS

操作审计支持查询阿里云关系型数据库RDS（Relational Database Service）相关事件。您可以快速查询RDS事件并获取事件发生的时间、地域、RDS实例等信息。本文为您举例说明RDS相关事件。

阿里云账号通过控制台重启RDS实例

以下示例表示，在北京时间2021年08月04日15:34:58，阿里云账号调用RestartDBInstance接口重启了杭州地域ID为 `rm-bp18vn5itslhw****` 的RDS实例。

```
{
  "eventId": "4EC856C0-A735-52D0-A7E6-E5CD09A5BCD4",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "4EC856C0-A735-52D0-A7E6-E5CD09A5BCD4"
  },
  "eventSource": "rds-inc-share.aliyuncs.com",
  "requestParameters": {
    "charset": "UTF-8",
    "AcsHost": "rds-inc-share.aliyuncs.com",
    "AcsProduct": "Rds",
    "RequestId": "4EC856C0-A735-52D0-A7E6-E5CD09A5BCD4",
    "DBInstanceId": "rm-bp18vn5itslhw****",
    "AcceptLanguage": "zh-CN",
    "HostId": "rds-inc-share.aliyuncs.com"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "rdsnext.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RDS::DBInstance": [
      "rm-bp18vn5itslhw****"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-04T07:34:58Z"
      }
    },
    "accountId": "147395807376****",
    "principalId": "147395807376****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Rds",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-08-15",
  "requestId": "4EC856C0-A735-52D0-A7E6-E5CD09A5BCD4",
  "eventTime": "2021-08-04T07:34:58Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "RestartDBInstance"
}
```


示例中关键字段含义如下：

- `userIdentity.type`：请求者的身份类型。取值为`root-account`，表示阿里云账号。
- `serviceName`：事件相关的阿里云服务名称。取值为`Rds`，表示RDS。

- `eventName`：事件名称。取值为`RestartDBInstance`，表示重启实例。
- `referencedResources`：事件影响的资源列表。取值为`{"ACS::RDS::DBInstance": ["rm-bp18vn5itslhw****"]}`，表示RDS实例`rm-bp18vn5itslhw****`。
- `acsRegion`：事件发生的地域。取值为`cn-hangzhou`，表示杭州地域。
- `eventTime`：事件发生的时间（UTC格式）。取值为`2021-08-04T07:34:58Z`，表示北京时间2021年08月04日15:34:58。

RAM用户通过控制台重启RDS实例

以下示例表示，在北京时间2021年08月04日10:54:38，RAM用户`Alice`调用RestartDBInstance接口重启了杭州地域ID为`rm-bp15hkr5tb57v****`的RDS实例。

```
{
  "apiVersion": "2014-08-15",
  "requestId": "532F2CED-F931-57FC-B08E-5AF8FF443DD5",
  "eventType": "ApiCall",
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-04T02:54:38Z"
      }
    },
    "accountId": "183080612160****",
    "principalId": "20816241517167****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "acsRegion": "cn-hangzhou",
  "eventName": "RestartDBInstance",
  "requestParameters": {
    "charset": "UTF-8",
    "AcsHost": "rds-inc-share.aliyuncs.com",
    "AcsProduct": "Rds",
    "RequestId": "532F2CED-F931-57FC-B08E-5AF8FF443DD5",
    "DBInstanceId": "rm-bp15hkr5tb57v****",
    "AcceptLanguage": "zh-CN",
    "HostId": "rds-inc-share.aliyuncs.com"
  },
  "eventSource": "rds-inc-share.aliyuncs.com",
  "serviceName": "Rds",
  "eventTime": "2021-08-04T02:54:38Z",
  "referencedResources": {
    "DBInstance": [
      "rm-bp15hkr5tb57v****"
    ],
    "ACS::RDS::DBInstance": [
      "rm-bp15hkr5tb57v****"
    ]
  },
  "userAgent": "rdsnext.console.aliyun.com",
  "eventId": "532F2CED-F931-57FC-B08E-5AF8FF443DD5",
  "additionalEventData": {
    "Scheme": "http"
  },
  "responseElements": {
    "RequestId": "532F2CED-F931-57FC-B08E-5AF8FF443DD5"
  },
  "errorCode": "",
  "errorMessage": "",
  "eventVersion": "1",
  "sourceIpAddress": "192.168.XX.XX"
}
```


示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `userIdentity.userName` ：请求者的RAM用户名称。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Rds` ，表示RDS。
- `eventName` ：事件名称。取值为 `RestartDBInstance` ，表示重启实例。
- `referencedResources` ：事件影响的资源列表。取值为 `{"DBInstance": ["rm-bp15hkr5tb57v****"], "ACS::RDS::DBInstance": ["rm-bp15hkr5tb57v****"]}` ，表示RDS实例 `rm-bp15hkr5tb57v****` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-04T02:54:38Z` ，表示北京时间2021年08月04日10:54:38。

阿里云账号通过AK调用API重启RDS实例

以下示例表示，在北京时间2021年08月04日10:29:37，阿里云账号通过AK `LTAICy8jSBYN****` 调用RestartDBInstance接口重启了上海地域ID为 `rm-1udt95gm98274****` 的RDS实例。

```
{
  "eventId": "55149DB3-9B17-5F96-99D7-10BCEC5A669D",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "55149DB3-9B17-5F96-99D7-10BCEC5A669D"
  },
  "eventSource": "rds.aliyuncs.com",
  "requestParameters": {
    "AcsHost": "rds.aliyuncs.com",
    "AcsProduct": "Rds",
    "RequestId": "55149DB3-9B17-5F96-99D7-10BCEC5A669D",
    "DBInstanceId": "rm-1udt95gm98274****",
    "HostId": "rds.aliyuncs.com",
    "ClientToken": "4d31085d-8403-4f43-a600-41294335****"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "Apache-HttpClient/4.5.2 (Java/1.8.0_191)",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RDS::DBInstance": [
      "rm-1udt95gm98274****"
    ]
  },
  "userIdentity": {
    "accessKeyId": "LTAICy8jSBYN****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-04T02:29:37Z"
      }
    },
    "accountId": "514024858446****",
    "principalId": "514024858446****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Rds",
  "additionalEventData": {
    "Scheme": "https",
    "CallerBid": "26888"
  },
  "apiVersion": "2014-08-15",
  "requestId": "55149DB3-9B17-5F96-99D7-10BCEC5A669D",
  "eventTime": "2021-08-04T02:29:37Z",
  "isGlobal": false,
  "acsRegion": "cn-shanghai",
  "eventName": "RestartDBInstance"
}
```


示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAICy8jSBYN****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `514024858446****` 。

- `userIdentity.type` ：请求者的身份类型。取值为 `root-account` ，表示阿里云账号。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Rds` ，表示RDS。
- `eventName` ：事件名称。取值为 `RestartDBInstance` ，表示重启实例。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::RDS::DBInstance": ["rm-1udt95gm98274****"]}` ，表示RDS实例 `rm-1udt95gm98274****` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-shanghai` ，表示上海地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-04T02:29:37Z` ，表示北京时间2021年08月04日10:29:37。

RAM用户通过角色扮演重启RDS实例

以下示例表示，在北京时间2021年08月02日14:15:46，阿里云账号 `165367888785****` 中的RAM用户通过扮演账号 `109052579984****` 下的RAM角色 `aliyunid-ag-ram-role-admin` ，重启了杭州地域ID为 `rm-bp1cw83fsi6j3****` 的RDS实例。

```
{
  "eventId": "191D3EE5-82C7-48BC-B128-37A0BE30FF38",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "191D3EE5-82C7-48BC-B128-37A0BE30FF38"
  },
  "eventSource": "rds-inc-share.aliyuncs.com",
  "requestParameters": {
    "stsTokenPrincipalName": "aliyunid-ag-ram-role-admin/default",
    "charset": "UTF-8",
    "AcsHost": "rds-inc-share.aliyuncs.com",
    "AcsProduct": "Rds",
    "RequestId": "191D3EE5-82C7-48BC-B128-37A0BE30FF38",
    "DBInstanceId": "rm-bp1cw83fsi6j3****",
    "AcceptLanguage": "zh-CN",
    "HostId": "rds-inc-share.aliyuncs.com",
    "stsTokenPlayerUid": 165367888785****
  },
  "sourceIpAddress": "Internal",
  "userAgent": "rdsnext.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RDS::DBInstance": [
      "rm-bp1cw83fsi6j3****"
    ]
  },
  "userIdentity": {
    "accessKeyId": "STS.NTXdTaxSSKZv3dNhvXZcT****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T06:15:46Z"
      }
    },
    "accountId": "109052579984****",
    "principalId": "36661865364550****:default",
    "type": "assumed-role",
    "userName": "aliyunid-ag-ram-role-admin:default"
  },
  "serviceName": "Rds",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-08-15",
  "requestId": "191D3EE5-82C7-48BC-B128-37A0BE30FF38",
  "eventTime": "2021-08-02T06:15:46Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "RestartDBInstance"
}
```


示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `aliyunid-ag-ram-role-admin:default` ，表示被扮演的RAM角色名称是 `aliyunid-ag-ram-role-admin` ，进行角色扮演时指定的名称为 `default` 。
- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `165367888785****` 。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::RDS::DBInstance": ["rm-bp1cw83fsi6j3****"]}` ，表示RDS实例 `rm-bp1cw83fsi6j3****` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Rds` ，表示RDS。
- `eventName` ：事件名称。取值为 `RestartDBInstance` ，表示重启实例。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-02T06:15:46Z` ，表示北京时间2021年08月02日14:15:46。

4.7.6. SLB

操作审计支持查询负载均衡SLB（Server Load Balancer）相关事件。当SLB操作出现异常时，您可以快速查询事件并获取事件发生的时间、地域、SLB实例等信息。本文为您举例说明SLB相关事件。

阿里云账号通过控制台删除SLB实例

以下示例表示，在北京时间2021年08月03日20:21:55，阿里云账号调用DeleteLoadBalancer接口删除了杭州地域ID为 `lb-bp1b3iffgeccmaww3****` 的SLB实例。

```
{
  "eventId": "51D55867-8194-5C55-8F33-4385D7C37D99",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "51D55867-8194-5C55-8F33-4385D7C37D99"
  },
  "eventSource": "slb-pop.aliyuncs.com",
  "requestParameters": {
    "AcsHost": "slb-pop.aliyuncs.com",
    "AcsProduct": "Slb",
    "RequestId": "51D55867-8194-5C55-8F33-4385D7C37D99",
    "LoadBalancerId": "lb-bp1b3iffgeccmaww3****",
    "SlbApi__domiain": "slb-pop.aliyuncs.com",
    "https": "False",
    "HostId": "slb-pop.aliyuncs.com"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "ros.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::SLB::LoadBalancer": [
      "lb-bp1b3iffgeccmaww3****"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-03T12:21:55Z"
      }
    },
    "accountId": "162728028114****",
    "principalId": "162728028114****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Slb",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-05-15",
  "requestId": "51D55867-8194-5C55-8F33-4385D7C37D99",
  "eventTime": "2021-08-03T12:21:55Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DeleteLoadBalancer"
}
```


示例中关键字段含义如下：

- `userIdentity.type`：请求者的身份类型。取值为`root-account`，表示阿里云账号。
- `serviceName`：事件相关的阿里云服务名称。取值为`Slb`，表示SLB。

- `eventName`：事件名称。取值为 `DeleteLoadBalancer`，表示删除SLB实例。
- `referencedResources`：事件影响的资源列表。取值为 `{"ACS::SLB::LoadBalancer": ["lb-bp1b3iffgeccmaww3****"]}`，表示SLB实例 `lb-bp1b3iffgeccmaww3****`。
- `acsRegion`：事件发生的地域。取值为 `cn-hangzhou`，表示杭州地域。
- `eventTime`：事件发生的时间（UTC格式）。取值为 `2021-08-03T12:21:55Z`，表示北京时间2021年08月03日20:21:55。

RAM用户通过控制台删除SLB实例

以下示例表示，在北京时间2021年08月05日11:21:50，RAM用户 `Alice` 调用DeleteLoadBalancer接口删除了杭州地域ID为 `lb-bp160ovcr2iicm8y4****` 的SLB实例。

```
{
  "eventId": "458F7AFB-53D5-561E-979A-20B2FC1476CF",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "458F7AFB-53D5-561E-979A-20B2FC1476CF"
  },
  "eventSource": "slb-openapi-share.aliyuncs.com",
  "requestParameters": {
    "charset": "UTF-8",
    "AcsHost": "slb-openapi-share.aliyuncs.com",
    "AcsProduct": "Slb",
    "RequestId": "458F7AFB-53D5-561E-979A-20B2FC1476CF",
    "AcceptLanguage": "zh-CN",
    "LoadBalancerId": "lb-bp160ovcr2iicm8y4****",
    "RegionId": "cn-hangzhou",
    "HostId": "slb-openapi-share.aliyuncs.com"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "slb.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::SLB::LoadBalancer": [
      "lb-bp160ovcr2iicm8y4****"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "true",
        "creationDate": "2021-08-05T03:21:50Z"
      }
    },
    "accountId": "173376625463****",
    "principalId": "20804860793058****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Slb",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-05-15",
  "requestId": "458F7AFB-53D5-561E-979A-20B2FC1476CF",
  "eventTime": "2021-08-05T03:21:50Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DeleteLoadBalancer"
}
```


示例中关键字段含义如下：

- `userIdentity.type`：请求者的身份类型。取值为`ram-user`，表示RAM用户。

- `userIdentity.userName` ：请求者的RAM用户名称。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Slb` ，表示SLB。
- `eventName` ：事件名称。取值为 `DeleteLoadBalancer` ，表示删除SLB实例。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::SLB::LoadBalancer": ["lb-bp160ovcr2iicm8y4****"]}` ，表示SLB实例 `lb-bp160ovcr2iicm8y4****` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T03:21:50Z` ，表示北京时间2021年08月05日11:21:50。

阿里云账号通过AK调用API删除SLB实例

以下示例表示，在北京时间2021年08月05日11:31:19，阿里云账号通过AK `LTAI4GAhAbUyrykxM3mY****` 调用DeleteLoadBalancer接口删除了杭州地域ID为 `lb-bp19gskmju1h6tm3v****` 的SLB实例。

```
{
  "eventId": "89E7EA51-53A0-5C85-9D3C-3838F9CEA99D",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "89E7EA51-53A0-5C85-9D3C-3838F9CEA99D"
  },
  "eventSource": "slb.aliyuncs.com",
  "requestParameters": {
    "AcsHost": "slb.aliyuncs.com",
    "AcsProduct": "Slb",
    "RequestId": "89E7EA51-53A0-5C85-9D3C-3838F9CEA99D",
    "LoadBalancerId": "lb-bp19gskmju1h6tm3v****",
    "SignatureType": "",
    "RegionId": "cn-hangzhou",
    "HostId": "slb.aliyuncs.com"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "AlibabaCloud (linux; amd64) Golang/1.12.9 Core/0.0.1 HashiCorp-Terraform/0.
12.1-1.55.4",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::SLB::LoadBalancer": [
      "lb-bp19gskmju1h6tm3v****"
    ]
  },
  "userIdentity": {
    "accessKeyId": "LTAI4GAhAbUyrykxM3mY****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T03:31:19Z"
      }
    },
    "accountId": "152239434953****",
    "principalId": "152239434953****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Slb",
  "additionalEventData": {
    "Scheme": "https",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-05-15",
  "requestId": "89E7EA51-53A0-5C85-9D3C-3838F9CEA99D",
  "eventTime": "2021-08-05T03:31:19Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DeleteLoadBalancer"
}
```


示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAI4GAhAbUyrykxM3mY****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `152239434953****` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Slb` ，表示SLB。
- `eventName` ：事件名称。取值为 `DeleteLoadBalancer` ，表示删除SLB实例。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::SLB::LoadBalancer": ["lb-bp19gskmju1h6tm3v****"]}` ，表示SLB实例 `lb-bp19gskmju1h6tm3v****` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T03:31:19Z` ，表示北京时间2021年08月05日11:31:19。

RAM角色通过角色扮演删除SLB实例

以下示例表示，在北京时间2021年08月05日09:10:13，容器服务ACK通过扮演角色 `aliyuncsdefaultrole` ，删除了杭州地域ID为 `lb-bp1bqozygmlt8wohe****` 的SLB实例。

```
{
  "eventId": "379F4611-D4C0-5DE7-A152-DDEA715A5E79",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "379F4611-D4C0-5DE7-A152-DDEA715A5E79"
  },
  "eventSource": "slb-pop.aliyuncs.com",
  "requestParameters": {
    "stsTokenPrincipalName": "aliyuncsdefaultrole/cs-provision-role-1628125309",
    "AcsHost": "slb-pop.aliyuncs.com",
    "AcsProduct": "Slb",
    "RequestId": "379F4611-D4C0-5DE7-A152-DDEA715A5E79",
    "LoadBalancerId": "lb-bp1bqozygmlt8wohe****",
    "SlbApi__domiain": "slb-pop.aliyuncs.com",
    "https": "False",
    "HostId": "slb-pop.aliyuncs.com",
    "stsTokenPlayerUid": 175434791765****
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "ros",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::SLB::LoadBalancer": [
      "lb-bp1bqozygmlt8wohe****"
    ]
  },
  "userIdentity": {
    "accessKeyId": "STS.9huAj27vmkaWKAoJytpctKRapi8sUSJerq7GFAAs9Lb9twgPzg****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T01:10:13Z"
      }
    },
    "accountId": "190885984155****",
    "principalId": "33370898817881****:cs-provision-role-1628125309",
    "type": "assumed-role",
    "userName": "aliyuncsdefaultrole:cs-provision-role-1628125309"
  },
  "serviceName": "Slb",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2014-05-15",
  "requestId": "379F4611-D4C0-5DE7-A152-DDEA715A5E79",
  "eventTime": "2021-08-05T01:10:13Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "DeleteLoadBalancer"
}
```


示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `aliyuncsdefaultrole:cs-provision-role-1628125309` ，表示被扮演的RAM角色名称是 `aliyuncsdefaultrole` ，进行角色扮演时指定的名称为 `cs-provision-role-1628125309` 。

  > **说明** 容器服务ACK在集群操作时默认使用 `aliyuncsdefaultrole` 角色来访问您在其他云服务中的资源。

- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `175434791765****` 。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::SLB::LoadBalancer": ["lb-bp1bqozygmlt8wohe****"]}` ，表示SLB实例 `lb-bp1bqozygmlt8wohe****` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `SLB` ，表示SLB。
- `eventName` ：事件名称。取值为 `DeleteLoadBalancer` ，表示删除SLB实例。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T01:10:13Z` ，表示北京时间2021年08月05日09:10:13。

4.7.7. IMS

操作审计支持查询访问控制IMS（Identity Management Service）相关事件。您可以快速查询IMS事件并获取事件发生的时间、地域、RAM用户等信息。本文为您举例说明IMS相关事件。

阿里云账号通过控制台创建RAM用户

以下示例表示，在北京时间2021年08月05日14:59:52，阿里云账号调用CreateUser接口创建了一个RAM用户 `Alice@163205818484****.onaliyun.com` 。

```
{
  "eventId": "80648075-F89C-555D-974B-78E436FE4331",
  "eventVersion": 1,
  "responseElements": {
    "User": {
      "UpdateDate": "2021-08-05T06:59:52Z",
      "Email": "username@example.com",
      "Comments": "",
      "UserId": "212842128146 79*****",
      "LastLoginDate": "",
      "DisplayName": "Alice",
      "UserPrincipalName": "Alice@163205818484****.onaliyun.com",
      "CreateDate": "2021-08-05T06:59:52Z",
      "MobilePhone": "1381111****"
    },
    "RequestId": "80648075-F89C-555D-974B-78E436FE4331"
  },
  "eventSource": "ims-share.aliyuncs.com",
  "requestParameters": {
    "charset": "UTF-8",
    "AcsHost": "ims-share.aliyuncs.com",
    "AcsProduct": "Ims",
    "RequestId": "80648075-F89C-555D-974B-78E436FE4331",
```

```
    "DisplayName": "Alice",
    "AcceptLanguage": "zh-CN",
    "AkProxySuffix": "ram",
    "UserPrincipalName": "Alice@163205818484****.onaliyun.com",
    "HostId": "ims-share.aliyuncs.com"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "ram.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RAM::User": [
      "Alice@163205818484****.onaliyun.com"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T06:59:52Z"
      }
    },
    "accountId": "163205818484****",
    "principalId": "163205818484****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Ims",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26888"
  },
  "apiVersion": "2019-08-15",
  "requestId": "80648075-F89C-555D-974B-78E436FE4331",
  "eventTime": "2021-08-05T06:59:52Z",
  "isGlobal": true,
  "acsRegion": "cn-shanghai",
  "eventName": "CreateUser"
}
```


示例中关键字段含义如下：

- `userIdentity.type`：请求者的身份类型。取值为`root-account`，表示阿里云账号。
- `serviceName`：事件相关的阿里云服务名称。取值为`Ims`，表示IMS。
- `eventName`：事件名称。取值为`CreateUser`，表示创建RAM用户。
- `referencedResources`：事件影响的资源列表。取值为`{"ACS::RAM::User": ["Alice@163205818484****.onaliyun.com"]}`，表示RAM用户`Alice@163205818484****.onaliyun.com`。
- `eventTime`：事件发生的时间（UTC格式）。取值为`2021-08-05T06:59:52Z`，表示北京时间2021年08月05日14:59:52。

RAM用户通过控制台创建RAM用户

以下示例表示，在北京时间2021年08月05日14:44:37，RAM用户 `Alice` 调用CreateUser接口创建了一个RAM用户 `test@189217171671****.onaliyun.com` 。


```
{
  "eventId": "BB774582-E706-5B89-8540-84D9490D0F11",
  "eventVersion": 1,
  "responseElements": {
    "User": {
      "UpdateDate": "2021-08-05T06:44:37Z",
      "Email": "username@example.com",
      "Comments": "",
      "UserId": "27688052814587****",
      "LastLoginDate": "",
      "DisplayName": "test",
      "UserPrincipalName": "test@189217171671****.onaliyun.com",
      "CreateDate": "2021-08-05T06:44:37Z",
      "MobilePhone": "1381111****"
    },
    "RequestId": "BB774582-E706-5B89-8540-84D9490D0F11"
  },
  "eventSource": "ims-share.aliyuncs.com",
  "requestParameters": {
    "charset": "UTF-8",
    "AcsHost": "ims-share.aliyuncs.com",
    "AcsProduct": "Ims",
    "RequestId": "BB774582-E706-5B89-8540-84D9490D0F11",
    "DisplayName": "test",
    "AcceptLanguage": "zh-CN",
    "AkProxySuffix": "ram",
    "UserPrincipalName": "test@189217171671****.onaliyun.com",
    "HostId": "ims-share.aliyuncs.com"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "ram.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RAM::User": [
      "test@189217171671****.onaliyun.com"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T06:44:37Z"
      }
    },
    "accountId": "189217171671****",
    "principalId": "26135379175722****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Ims",
  "additionalEventData": {
```

```
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2019-08-15",
  "requestId": "BB774582-E706-5B89-8540-84D9490D0F11",
  "eventTime": "2021-08-05T06:44:37Z",
  "isGlobal": true,
  "acsRegion": "cn-shanghai",
  "eventName": "CreateUser"
}
```

示例中关键字段含义如下：

- `userIdentity.type`：请求者的身份类型。取值为`ram-user`，表示RAM用户。
- `userIdentity.userName`：请求者的RAM用户名称。
- `serviceName`：事件相关的阿里云服务名称。取值为`Ims`，表示IMS。
- `eventName`：事件名称。取值为`CreateUser`，表示创建RAM用户。
- `referencedResources`：事件影响的资源列表。取值为`{"ACS::RAM::User": ["test@189217171671****.onaliyun.com"]}`，表示RAM用户`test@189217171671****.onaliyun.com`。
- `eventTime`：事件发生的时间（UTC格式）。取值为`2021-08-05T06:44:37Z`，表示北京时间2021年08月05日14:44:37。

RAM用户通过AK调用API创建RAM用户

以下示例表示，在北京时间2021年08月05日14:52:21，RAM用户`Alice`通过AK`LTAI4Fz1ykT4qxgNMvN6****`调用CreateUser接口创建了一个RAM用户`test@example.onaliyun.com`。

```
{
  "eventId": "ED377CCF-2F1E-542D-96E6-25ACD4C866E3",
  "eventVersion": 1,
  "responseElements": {
    "User": {
      "UpdateDate": "2021-08-05T06:52:21Z",
      "Email": "username@example.com",
      "Comments": "",
      "UserId": "237054828146 34****",
      "LastLoginDate": "",
      "DisplayName": "test",
      "UserPrincipalName": "test@example.onaliyun.com",
      "CreateDate": "2021-08-05T06:52:21Z",
      "MobilePhone": "1381111****"
    },
    "RequestId": "ED377CCF-2F1E-542D-96E6-25ACD4C866E3"
  },
  "eventSource": "ims.aliyuncs.com",
  "requestParameters": {
    "AcsHost": "ims.aliyuncs.com",
    "AcsProduct": "Ims",
    "RequestId": "ED377CCF-2F1E-542D-96E6-25ACD4C866E3",
    "DisplayName": "test",
    "UserPrincipalName": "test@example.onaliyun.com",
    "HostId": "ims.aliyuncs.com"
  }
```

```
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "AlibabaCloud (Mac OS X; x86_64) Java/1.8.0_151-b12 tea-util/0.2.6 TeaDSL/1"
,
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RAM::User": [
      "test@example.onaliyun.com"
    ]
  },
  "userIdentity": {
    "accessKeyId": "LTAI4Fz1ykT4qxgNMvN6****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T06:52:21Z"
      }
    },
    "accountId": "121410627017****",
    "principalId": "29041080637456****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Ims",
  "additionalEventData": {
    "Scheme": "https",
    "CallerBid": "26842"
  },
  "apiVersion": "2019-08-15",
  "requestId": "ED377CCF-2F1E-542D-96E6-25ACD4C866E3",
  "eventTime": "2021-08-05T06:52:21Z",
  "isGlobal": true,
  "acsRegion": "cn-shanghai",
  "eventName": "CreateUser"
}
```

示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAI4Fz1ykT4qxgNMvN6****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `29041080637456****` 。
- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Ims` ，表示IMS。
- `eventName` ：事件名称。取值为 `CreateUser` ，表示创建RAM用户。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::RAM::User": ["test@example.onaliyun.com"]}` ，表示RAM用户 `test@example.onaliyun.com` 。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T06:52:21Z` ，表示北京时间2021年08月05日14:52:21。

RAM用户通过角色扮演创建RAM用户

以下示例表示，在北京时间2021年08月05日14:50:12，阿里云账号 `189217171671****` 中的RAM用户通过扮演自己账号下的 `ram-role` 角色创建了一个RAM用户 `test@189217171671****.onaliyun.com` 。

```
{
  "eventId": "7831E25F-2AAF-522B-A6A8-228ED41396C0",
  "eventVersion": 1,
  "responseElements": {
    "User": {
      "UpdateDate": "2021-08-05T06:50:12Z",
      "Email": "username@example.com",
      "Comments": "",
      "UserId": "20560232814621****",
      "LastLoginDate": "",
      "DisplayName": "test",
      "UserPrincipalName": "test@189217171671****.onaliyun.com",
      "CreateDate": "2021-08-05T06:50:12Z",
      "MobilePhone": "1381111****"
    },
    "RequestId": "7831E25F-2AAF-522B-A6A8-228ED41396C0"
  },
  "eventSource": "ims-share.aliyuncs.com",
  "requestParameters": {
    "stsTokenPrincipalName": "ram-role/roleTest123",
    "charset": "UTF-8",
    "AcsHost": "ims-share.aliyuncs.com",
    "AcsProduct": "Ims",
    "RequestId": "7831E25F-2AAF-522B-A6A8-228ED41396C0",
    "DisplayName": "test",
    "AcceptLanguage": "zh-CN",
    "AkProxySuffix": "ram",
    "UserPrincipalName": "test@189217171671****.onaliyun.com",
    "HostId": "ims-share.aliyuncs.com",
    "stsTokenPlayerUid": 189217171671****
  },
  "sourceIpAddress": "Internal",
  "userAgent": "ram.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RAM::User": [
      "test@189217171671****.onaliyun.com"
    ]
  },
  "userIdentity": {
    "accessKeyId": "STS.NTGje1eLLVFMNcgRsLVic****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T06:50:12Z"
      }
    },
    "accountId": "189217171671****",
    "principalId": "37177545076791****:roleTest123",
    "type": "assumed-role",
    "userName": "ram-role:roleTest123"
  },
  "serviceName": "Ims",
  "additionalEventData": {
```

```
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2019-08-15",
  "requestId": "7831E25F-2AAF-522B-A6A8-228ED41396C0",
  "eventTime": "2021-08-05T06:50:12Z",
  "isGlobal": true,
  "acsRegion": "cn-shanghai",
  "eventName": "CreateUser"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `ram-role:roleTest123` ，表示被扮演的RAM角色名称是 `ram-role` ，进行角色扮演时指定的名称为 `roleTest123` 。
- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `189217171671****` 。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::RAM::User": ["test@189217171671****.onaliyun.com"]}` ，表示RAM用户 `test@189217171671****.onaliyun.com` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Ims` ，表示IMS。
- `eventName` ：事件名称。取值为 `CreateUser` ，表示创建RAM用户。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T06:50:12Z` ，表示北京时间2021年08月05日14:50:12。

4.7.8. STS

操作审计支持查询阿里云临时安全令牌STS（Security Token Service）相关事件。您可以快速查询STS事件并获取事件发生的时间、地域、临时身份等信息。本文为您举例说明STS相关事件。

RAM用户通过控制台调用STS切换角色身份

以下示例表示，在北京时间2021年08月05日15:59:47，RAM用户 `Alice` 调用AssumeRole接口通过扮演阿里云账号 `127812487797****` 下的 `cna-manager-test-role` 角色获取了一个临时身份。

```
{
  "eventId": "FC410992-13D4-5D33-89A7-D8F4100CEE6B",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "FC410992-13D4-5D33-89A7-D8F4100CEE6B",
    "AssumedRoleUser": {
      "Arn": "acs:ram::127812487797****:role/cna-manager-test-role/169074",
      "AssumedRoleId": "33618118978621****:169074"
    },
    "Credentials": {
      "AccessKeyId": "STS.NUQ79dzjpMPxYesi1YY5U****",
      "AccessKeySecret": "gS09k8a8fDwwgR0ey9IeCFuNfr****",
      "Expiration": "2021-08-05T08:59:47Z"
    }
  },
  "eventSource": "sts.aliyuncs.com",
  "requestParameters": {
```

```
    "requestParameters": {
      "AcsHost": "sts.aliyuncs.com",
      "AcsProduct": "Sts",
      "RequestId": "FC410992-13D4-5D33-89A7-D8F4100CEE6B",
      "RoleSessionName": 169074,
      "RegionId": "cn-hangzhou",
      "HostId": "sts.aliyuncs.com",
      "RoleArn": "acs:ram::127812487797****:role/cna-manager-test-role"
    },
    "sourceIpAddress": "192.168.XX.XX",
    "userAgent": "AlibabaCloud (Linux; amd64) Java/1.8.0_152-b187 Core/4.5.17 HTTPClient/Apac
heHttpClient",
    "eventType": "ApiCall",
    "referencedResources": {
      "ACS::RAM::AccessKey": [
        "STS.NUQ79dzjpMPxYesi1YY5U****"
      ]
    },
    "userIdentity": {
      "sessionContext": {
        "attributes": {
          "mfaAuthenticated": "false",
          "creationDate": "2021-08-05T07:59:46Z"
        }
      },
      "accountId": "146411043369****",
      "principalId": "21336811218169****",
      "type": "ram-user",
      "userName": "Alice"
    },
    "serviceName": "Sts",
    "additionalEventData": {
      "Scheme": "https",
      "CallerBid": "26842"
    },
    "apiVersion": "2015-04-01",
    "requestId": "FC410992-13D4-5D33-89A7-D8F4100CEE6B",
    "eventTime": "2021-08-05T07:59:47Z",
    "isGlobal": false,
    "acsRegion": "cn-hangzhou",
    "eventName": "AssumeRole"
  }
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `userIdentity.userName` ：请求者的RAM用户名称。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Sts` ，表示STS。
- `eventName` ：事件名称。取值为 `AssumeRole` ，表示获取一个扮演该角色的临时身份，此处RAM用户扮演的是受信实体为阿里云账号类型的RAM角色。
- `requestParameters.RoleArn` ：扮演角色的ARN信息。取值为 `acs:ram::127812487797****:role/cna-manager-test-role` ， `127812487797****` 表示角色所属的阿里云账号ID， `cna-manager-test-role`

`` 表示角色名称。

- `referencedResources`：事件影响的资源列表。取值为 `{"ACS::RAM::AccessKey": ["STS.NUQ79dzjpMPxYesi1YY5U****"]}`，表示扮演角色获取的临时身份凭证 `STS.NUQ79dzjpMPxYesi1YY5U****`。
- `eventTime`：事件发生的时间（UTC格式）。取值为 `2021-08-05T07:59:47Z`，表示北京时间2021年08月05日15:59:47。

RAM用户通过调用SDK获取临时访问令牌

以下示例表示，在北京时间2021年08月05日16:03:31，RAM用户 `Alice` 调用AssumeRole接口通过扮演阿里云账号 `193875730500****` 下的 `aliyunosstokengeneratorrole` 角色获取了一个临时身份。

```
{
  "eventId": "B936D2EE-05DC-5AC1-9163-48F0DE28B963",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "B936D2EE-05DC-5AC1-9163-48F0DE28B963",
    "AssumedRoleUser": {
      "Arn": "acs:ram::193875730500****:role/aliyunosstokengeneratorrole/X5wpmS6EgkM080aE0K
ym****",
      "AssumedRoleId": "30815480203992****:X5wpmS6EgkM080aE0Kym****"
    },
    "Credentials": {
      "AccessKeyId": "STS.NTobFuYYn6EBxAVhC18ta****",
      "AccessKeySecret": "gS09k8a8fDwwgR0ey9IeCFuNfr****",
      "Expiration": "2021-08-05T09:03:31Z"
    }
  },
  "eventSource": "sts.cn-hangzhou.aliyuncs.com",
  "requestParameters": {
    "Policy": {
      "Version": "1",
      "Statement": [
        {
          "Condition": {},
          "Action": [
            "oss:PutObject"
          ],
          "Resource": [
            "acs:oss:*:*:taowo/image/disucss/2021/8/5/xNodqHMtGkX9arNrAkrz4d****/*",
            "acs:oss:*:*:taowo/video/disucss/2021/8/5/xNodqHMtGkX9arNrAkrz4d****/*",
            "acs:oss:*:*:taowo/sound/disucss/2021/8/5/xNodqHMtGkX9arNrAkrz4d****/*"
          ],
          "Effect": "Allow"
        }
      ]
    },
    "AcsHost": "sts.cn-hangzhou.aliyuncs.com",
    "AcsProduct": "Sts",
    "RequestId": "B936D2EE-05DC-5AC1-9163-48F0DE28B963",
    "RoleSessionName": "X5wpmS6EgkM080aE0Kym****",
    "Region": "cn-hangzhou",
    "SignatureType": "",
    "RegionId": "cn-hangzhou",
    "HostId": "sts.cn-hangzhou.aliyuncs.com",
```

```
    "RoleArn": "acs:ram::193875730500****:role/aliyunosstokengeneratorrole"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "AlibabaCloud (Linux 3.10.0-1127.19.1.el7.x86_64;x86_64) Python/3.8.8 Core/2
.13.32 python-requests/2.18.3",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RAM::AccessKey": [
      "STS.NTobFuYYn6EBxAVhC18ta****"
    ]
  },
  "userIdentity": {
    "accessKeyId": "LTAI2jP0BF0f****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T08:03:31Z"
      }
    },
    "accountId": "193875730500****",
    "principalId": "21365465900895****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Sts",
  "additionalEventData": {
    "Scheme": "https",
    "CallerBid": "26842"
  },
  "apiVersion": "2015-04-01",
  "requestId": "B936D2EE-05DC-5AC1-9163-48F0DE28B963",
  "eventTime": "2021-08-05T08:03:31Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "AssumeRole"
}
```

示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAI2jP0BF0f****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `21365465900895****` 。
- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Sts` ，表示STS。
- `eventName` ：事件名称。取值为 `AssumeRole` ，表示获取一个扮演该角色的临时身份，此处RAM用户扮演的是受信实体为阿里云账号类型的RAM角色。
- `requestParameters.RoleArn` ：扮演角色的ARN信息。取值为 `acs:ram::193875730500****:role/aliyunosstokengeneratorrole` ， `193875730500****` 表示角色所属的阿里云账号ID， `aliyunosstokengeneratorrole` 表示角色名称。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::RAM::AccessKey": ["STS.NTobFuYYn6EBxAVhC18ta****"]}` ，表示扮演角色获取的临时身份凭证为 `test@example.onaliyun.com` 。

- `eventTime`：事件发生的时间（UTC格式）。取值为`2021-08-05T08:03:31Z`，表示北京时间2021年08月05日16:03:31。

企业用户通过角色SSO获取阿里云角色身份

以下示例表示，在北京时间2021年08月05日16:04:56，企业用户`Alice`调用AssumeRoleWithSAML接口通过角色SSO扮演`189186630579****`账号下的`cruisetestrole`角色获取了一个临时身份。


```
{
  "eventId": "66FDD0F9-3546-567A-8964-2BD734198356",
  "eventVersion": 1,
  "responseElements": {
    "RequestId": "66FDD0F9-3546-567A-8964-2BD734198356",
    "SAMLAssertionInfo": {
      "SubjectType": "transient",
      "Issuer": "https://testidp/saml",
      "Recipient": "https://signin.aliyun.com/saml-role/sso",
      "Subject": "Alice"
    },
    "AssumedRoleUser": {
      "Arn": "acs:ram::189186630579****:role/cruisetestrole/cruisetest",
      "AssumedRoleId": "37924473051351****:cruisetest"
    },
    "Credentials": {
      "AccessKeyId": "STS.NUTNKhGR8BR3QL9sJkSHp****",
      "AccessKeySecret": "gS09k8a8fDwwgR0ey9IeCFuNfr****",
      "Expiration": "2021-08-05T09:04:56Z"
    }
  },
  "eventSource": "sts.aliyuncs.com",
  "requestParameters": {
    "AcsHost": "sts.aliyuncs.com",
    "SAMLAssertion": "***",
    "AcsProduct": "Sts",
    "RequestId": "66FDD0F9-3546-567A-8964-2BD734198356",
    "DurationSeconds": 3600,
    "HostId": "sts.aliyuncs.com",
    "SAMLProviderArn": "acs:ram::189186630579****:saml-provider/mockedIdp",
    "RoleArn": "acs:ram::189186630579****:role/cruisetestrole"
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "Jakarta Commons-HttpClient/3.1",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::RAM::AccessKey": [
      "STS.NUTNKhGR8BR3QL9sJkSHp****"
    ]
  },
  "userIdentity": {
    "accountId": "189186630579****",
    "samlProviderName": "mockedIdp",
    "type": "saml-user",
    "userName": "Alice",
    "samlIssuer": "https://testidp/saml"
  },
```

```
  "serviceName": "Sts",
  "additionalEventData": {
    "Scheme": "https",
    "CallerBid": "26842"
  },
  "apiVersion": "2015-04-01",
  "requestId": "66FDD0F9-3546-567A-8964-2BD734198356",
  "eventTime": "2021-08-05T08:04:56Z",
  "isGlobal": false,
  "acsRegion": "cn-shanghai",
  "eventName": "AssumeRoleWithSAML"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `saml-user` ，表示企业自有身份的用户。
- `userIdentity.userName` ：发起角色SSO的企业用户的用户名。
- `requestParameters.RoleArn` ：扮演角色的ARN信息。取值为 `cs:ram::189186630579****:role/cruisetestrole` ， `189186630579****` 表示角色所属的阿里云账号ID， `cruisetestrole` 表示角色名称。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::RAM::AccessKey": ["STS.NUTNKhGR8BR3QL9sJkSHp****"]}` ，表示扮演角色获取的临时身份凭证为 `STS.NUTNKhGR8BR3QL9sJkSHp****` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Sts` ，表示STS。
- `eventName` ：事件名称。取值为 `AssumeRoleWithSAML` ，表示通过角色SSO获取阿里云角色身份。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T08:04:56Z` ，表示北京时间2021年08月05日16:04:56。

4.7.9. ActionTrail

操作审计支持查询操作审计（ActionTrail）自身相关事件。您可以快速查询ActionTrail事件并获取事件发生的时间、地域和跟踪等信息。本文为您举例说明操作审计相关事件。

阿里云账号通过控制台更新跟踪

以下示例表示，在北京时间2021年08月05日08:25:26，阿里云账号调用UpdateTrail接口在杭州地域更新了跟踪 `alicetest` 。

```
{
  "eventId": "A5A4BB74-EFBC-5D8B-BD8A-1B9131429438",
  "eventVersion": 1,
  "responseElements": {
    "SlsProjectArn": "acs:log:cn-hangzhou:196813227629****:project/limansls",
    "EventRW": "Write",
    "RequestId": "A5A4BB74-EFBC-5D8B-BD8A-1B9131429438",
    "HomeRegion": "cn-hangzhou",
    "OssKeyPrefix": "",
    "OssBucketName": "",
    "SlsWriteRoleArn": "acs:ram::196813227629****:role/aliyunserviceroleforactiontrail",
    "OssWriteRoleArn": "",
    "TrailRegion": "All",
    "Name": "alicetest"
  },
  "eventSource": "actiontrail-openapi-share.cn-hangzhou.aliyuncs.com",
```

```
  "requestParameters": {
    "SlsLogStore": "actiontrail_test",
    "charset": "UTF-8",
    "AcsHost": "actiontrail-openapi-share.cn-hangzhou.aliyuncs.com",
    "RequestId": "A5A4BB74-EFBC-5D8B-BD8A-1B9131429438",
    "HostId": "actiontrail-openapi-share.cn-hangzhou.aliyuncs.com",
    "TrailRegion": "All",
    "Name": "limantest",
    "SlsProjectArn": "acs:log:cn-hangzhou:196813227629****:project/Alicesls",
    "EventRW": "Write",
    "AcsProduct": "Actiontrail",
    "OssKeyPrefix": "",
    "AcceptLanguage": "zh-CN",
    "Region": "cn-hangzhou",
    "OssBucketName": ""
  },
  "sourceIpAddress": "2409:8a20:4d15:e150:90f5:26ed:cc45:6922",
  "userAgent": "actiontrail.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::ActionTrail::Trail": [
      "alicetest"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T00:25:25Z"
      }
    },
    "accountId": "196813227629****",
    "principalId": "196813227629****",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "Actiontrail",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2020-07-06",
  "requestId": "A5A4BB74-EFBC-5D8B-BD8A-1B9131429438",
  "eventTime": "2021-08-05T00:25:26Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "UpdateTrail"
}
```


示例中关键字段含义如下：

- `userIdentity.type`：请求者的身份类型。取值为`root-account`，表示阿里云账号。
- `serviceName`：事件相关的阿里云服务名称。取值为`Actiontrail`，表示操作审计。

- `eventName` ：事件名称。取值为 `UpdateTrail` ，表示更新跟踪。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::ActionTrail::Trail": ["alicetest"]}` ，表示跟踪名称为 `alicetest` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T00:25:26Z` ，表示北京时间2021年08月05日08:25:26。

RAM用户通过控制台更新跟踪

以下示例表示，在北京时间2021年08月05日17:57:32，RAM用户 `Alice` 调用UpdateTrail接口在杭州地域更新了跟踪 `test-trail` 。


```
{
  "eventId": "86045124-4D86-5AD3-8848-CF78A20402AC",
  "eventVersion": 1,
  "responseElements": {
    "SlsProjectArn": "acs:log:cn-hangzhou:189217171671****:project/test-123",
    "EventRW": "Write",
    "RequestId": "86045124-4D86-5AD3-8848-CF78A20402AC",
    "HomeRegion": "cn-hangzhou",
    "OssKeyPrefix": "",
    "OssBucketName": "",
    "SlsWriteRoleArn": "acs:ram::189217171671****:role/aliyunserviceroleforactiontrail",
    "OssWriteRoleArn": "",
    "TrailRegion": "All",
    "Name": "test-trail"
  },
  "eventSource": "actiontrail-openapi-share.cn-hangzhou.aliyuncs.com",
  "requestParameters": {
    "SlsLogStore": "actiontrail_test-trail",
    "charset": "UTF-8",
    "AcsHost": "actiontrail-openapi-share.cn-hangzhou.aliyuncs.com",
    "RequestId": "86045124-4D86-5AD3-8848-CF78A20402AC",
    "HostId": "actiontrail-openapi-share.cn-hangzhou.aliyuncs.com",
    "TrailRegion": "All",
    "Name": "test-nnn",
    "SlsProjectArn": "acs:log:cn-hangzhou:189217171671****:project/test-123",
    "EventRW": "Write",
    "AcsProduct": "Actiontrail",
    "OssKeyPrefix": "",
    "AcceptLanguage": "zh-CN",
    "Region": "cn-hangzhou",
    "OssBucketName": ""
  },
  "sourceIpAddress": "192.168.XX.XX",
  "userAgent": "actiontrail.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::ActionTrail::Trail": [
      "test-trail"
    ]
  },
  "userIdentity": {
```

```
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T09:57:32Z"
      }
    },
    "accountId": "189217171671****",
    "principalId": "26135379175722****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Actiontrail",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2020-07-06",
  "requestId": "86045124-4D86-5AD3-8848-CF78A20402AC",
  "eventTime": "2021-08-05T09:57:32Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "UpdateTrail"
}
```

示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `userIdentity.userName` ：请求者的RAM用户名称。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Actiontrail` ，表示操作审计。
- `eventName` ：事件名称。取值为 `UpdateTrail` ，表示更新跟踪。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::ActionTrail::Trail": ["test-trail"]}` ，表示跟踪名称为 `test-trail` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T09:57:32Z` ，表示北京时间2021年08月05日17:57:32。

RAM用户通过AK调用API更新跟踪

以下示例表示，在北京时间2021年08月04日10:29:37，RAM用户 `Alice` 通过AK `LTAIcgRmWRaj****` 调用UpdateTrail接口在杭州地域更新了跟踪 `tf-testaccactiontrail` 。

```
{
  "eventId": "86C37F50-950C-599D-B07A-88C0493784A9",
  "eventVersion": 1,
  "responseElements": {
    "SlsProjectArn": "",
    "EventRW": "Write",
    "RequestId": "86C37F50-950C-599D-B07A-88C0493784A9",
    "HomeRegion": "cn-hangzhou",
    "OssKeyPrefix": "",
    "OssBucketName": "tf-testaccactiontrail",
    "SlsWriteRoleArn": "",
```

```
    "OssWriteRoleArn": "acs:ram::118272523431****:role/aliyunactiontraildefaultrole",
    "TrailRegion": "All",
    "Name": "tf-testaccactiontrail"
  },
  "eventSource": "actiontrail.cn-hangzhou.aliyuncs.com",
  "requestParameters": {
    "AcsHost": "actiontrail.cn-hangzhou.aliyuncs.com",
    "EventRW": "Write",
    "AcsProduct": "Actiontrail",
    "RequestId": "86C37F50-950C-599D-B07A-88C0493784A9",
    "Region": "cn-hangzhou",
    "OssBucketName": "tf-testaccactiontrail",
    "OssWriteRoleArn": "acs:ram::118272523431****:role/aliyunactiontraildefaultrole",
    "RegionId": "cn-hangzhou",
    "HostId": "actiontrail.cn-hangzhou.aliyuncs.com",
    "TrailRegion": "All",
    "Name": "tf-testaccactiontrail"
  },
  "sourceIpAddress": "Internal",
  "userAgent": "AlibabaCloud (linux; amd64) Golang/1.12.10 Core/0.01 TeaDSL/1 HashiCorp-Ter
raform/ Terraform-Provider/1.129.0 Terraform-Module/Default/LTAIcgRmWRaj****:41d6e7ac-9fd7-
4b05-b80d-9cf147e9fb4f",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::ActionTrail::Trail": [
      "tf-testaccactiontrail"
    ]
  },
  "userIdentity": {
    "accessKeyId": "LTAIcgRmWRaj****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-04T23:09:19Z"
      }
    },
    "accountId": "118272523431****",
    "principalId": "28544203916248****",
    "type": "ram-user",
    "userName": "Alice"
  },
  "serviceName": "Actiontrail",
  "additionalEventData": {
    "Scheme": "https",
    "CallerBid": "26842"
  },
  "apiVersion": "2020-07-06",
  "requestId": "86C37F50-950C-599D-B07A-88C0493784A9",
  "eventTime": "2021-08-04T02:29:37Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "UpdateTrail"
}
```

示例中关键字段含义如下：

- `userIdentity.accessKeyId` ：发起API调用的AccessKey ID。取值为 `LTAIcgRmWRaj****` 。
- `userIdentity.principalId` ：AK所属的账号ID。取值为 `28544203916248****` 。
- `userIdentity.type` ：请求者的身份类型。取值为 `ram-user` ，表示RAM用户。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Actiontrail` ，表示操作审计。
- `eventName` ：事件名称。取值为 `UpdateTrail` ，表示更新跟踪。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::ActionTrail::Trail": ["tf-testacc actiontrail"]}` ，表示跟踪名称为 `tf-testaccactiontrail` 。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-04T02:29:37Z` ，表示北京时间2021年08月04日10:29:37。

RAM用户通过角色扮演更新跟踪

以下示例表示，在北京时间2021年08月05日17:59:02，阿里云账号 `189217171671****` 中的RAM用户通过扮演账号 `189217171671****` 下的RAM角色 `trail-role` ，调用UpdateTrail接口在杭州地域更新了跟踪 `test-trail` 。

```
{
  "eventId": "C8E1ADC3-0DF3-5133-A40E-A0EE2B96A46A",
  "eventVersion": 1,
  "responseElements": {
    "SlsProjectArn": "acs:log:cn-hangzhou:189217171671****:project/test-123",
    "EventRW": "All",
    "RequestId": "C8E1ADC3-0DF3-5133-A40E-A0EE2B96A46A",
    "HomeRegion": "cn-hangzhou",
    "OssKeyPrefix": "",
    "OssBucketName": "",
    "SlsWriteRoleArn": "acs:ram::189217171671****:role/aliyunserviceroleforactiontrail",
    "OssWriteRoleArn": "",
    "TrailRegion": "All",
    "Name": "test-trail"
  },
  "eventSource": "actiontrail-openapi-share.cn-hangzhou.aliyuncs.com",
  "requestParameters": {
    "SlsLogStore": "actiontrail_test-trail",
    "charset": "UTF-8",
    "AcsHost": "actiontrail-openapi-share.cn-hangzhou.aliyuncs.com",
    "RequestId": "C8E1ADC3-0DF3-5133-A40E-A0EE2B96A46A",
    "HostId": "actiontrail-openapi-share.cn-hangzhou.aliyuncs.com",
    "TrailRegion": "All",
    "Name": "test-nnn",
    "stsTokenPrincipalName": "trail-role/roleTest123",
    "SlsProjectArn": "acs:log:cn-hangzhou:189217171671****:project/test-123",
    "EventRW": "All",
    "AcsProduct": "Actiontrail",
    "OssKeyPrefix": "",
    "AcceptLanguage": "zh-CN",
    "Region": "cn-hangzhou",
    "OssBucketName": "",
    "stsTokenPlayerUid": 189217171671****
```

```
  },
  "sourceIpAddress": "Internal",
  "userAgent": "actiontrail.console.aliyun.com",
  "eventType": "ApiCall",
  "referencedResources": {
    "ACS::ActionTrail::Trail": [
      "test-trail"
    ]
  },
  "userIdentity": {
    "accessKeyId": "STS.NTZxJ8V63CNgtAbsutWVs****",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-05T09:59:02Z"
      }
    },
    "accountId": "189217171671****",
    "principalId": "39484351102463****:roleTest123",
    "type": "assumed-role",
    "userName": "trail-role:roleTest123"
  },
  "serviceName": "Actiontrail",
  "additionalEventData": {
    "Scheme": "http",
    "CallerBid": "26842"
  },
  "apiVersion": "2020-07-06",
  "requestId": "C8E1ADC3-0DF3-5133-A40E-A0EE2B96A46A",
  "eventTime": "2021-08-05T09:59:02Z",
  "isGlobal": false,
  "acsRegion": "cn-hangzhou",
  "eventName": "UpdateTrail"
}
```


示例中关键字段含义如下：

- `userIdentity.type` ：请求者的身份类型。取值为 `assumed-role` ，表示RAM角色。
- `userIdentity.userName` ：请求者的用户名。格式为 `{roleName}:{sessionName}` ， `roleName` 表示被扮演的角色名称， `sessionName` 表示进行角色扮演时指定的名称。取值为 `trail-role:roleTest123` ，表示被扮演的RAM角色名称是 `trail-role` ，进行角色扮演时指定的名称为 `roleTest123` 。
- `requestParameters.stsTokenPlayerUid` ：扮演者的阿里云账号ID。取值为 `189217171671****` 。
- `referencedResources` ：事件影响的资源列表。取值为 `{"ACS::ActionTrail::Trail": ["test-trail"]}` ，表示跟踪名称为 `test-trail` 。
- `serviceName` ：事件相关的阿里云服务名称。取值为 `Actiontrail` ，表示操作审计。
- `eventName` ：事件名称。取值为 `UpdateTrail` ，表示更新跟踪。
- `acsRegion` ：事件发生的地域。取值为 `cn-hangzhou` ，表示杭州地域。
- `eventTime` ：事件发生的时间（UTC格式）。取值为 `2021-08-05T09:59:02Z` ，表示北京时间2021年08月05日17:59:02。

5.智能分析Insight事件

5.1. Insight事件视频指导

5.1.1. 开通Insight事件

5.1.2. 使用Insight事件

5.2. Insight事件概览

操作审计支持Insight事件，帮助您从管控事件中发现异常行为。启用Insight事件后，操作审计将基于管控事件识别异常并生成Insight事件，然后将Insight事件投递到日志服务SLS或对象存储OSS。Insight事件帮助您及时洞察云上管控风险并尽快采取补救措施。

Insight事件与管控事件的区别

事件类型	说明	相关文档
管控事件	用户通过登录阿里云账号，使用阿里云上的身份对云资源进行管控而被记录的操作日志。每一条管控事件是一次操作日志。	管控事件结构定义
Insight事件	基于管控事件的分析结果，Insight事件呈现了一种异常情况的发生。目前仅支持IPInsight事件。您在跟踪中启用IPInsight事件功能后，操作审计会基于过去已有的管控操作事件分析出常规的来访IP特征，然后判断新的来访IP是否为异常IP。当发现一个异常IP，将生成一个IPInsight事件向您通报异常IP的情况。 Insight事件基于管控事件的分析结果而产生，一个Insight事件会关联多个管控事件。例如：一个IPInsight事件代表一个异常的来访IP，IPInsight事件会关联多个通过异常来访IP访问的管控事件。	Insight事件结构定义

功能特性

- 自动生成Insight事件：操作审计会分析过去一段时间您阿里云账号中事件的来访IP，总结正常来访IP的特征模型。在您后续长期的云上访问过程中，不断为您扫描并鉴别新出现的来访IP，识别其中的异常IP，然后生成Insight事件。
- 快速查询Insight事件：您可以通过操作审计控制台查询最近90天的Insight事件的IP地址、开始时间、结束时间、IP异常事件数等基础信息，也可以查询Insight事件代码。
- 长时间存储Insight事件：操作审计会将Insight事件投递到跟踪指定的日志服务SLS或对象存储OSS，以便长时间存储或分析Insight事件。

工作原理

- Insight事件的生成条件：当您首次对跟踪启用Insight事件时，操作审计需要至少分析10000条管控事件来生成第一个Insight事件，所以当您现存的事件量不足时，将不会立即生成Insight事件。Insight事件是对异常行为的洞察，如果您的阿里云账号中不存在异常行为，也不会生成Insight事件。
- Insight事件的统计范围：Insight事件是分地域的。针对同一个地域发生的管控事件进行Insight事件的分析，所以Insight事件与管控事件所在地域相同。对于全局事件，Insight事件只会在跟踪创建的地域进行分析。如果您关闭了跟踪，Insight事件也会停止记录。
- Insight事件的判定规则：目前仅支持IPInsight事件，用于洞察异常IP的访问。IPInsight事件统计IP异常事件

数时采用IP关联度算法，可能导致一些新出现的来访IP被错误地识别为异常IP，因此新出现的IP会在第一次被检测到时生成一个异常IP事件。在接下来的7天内，如果出现大于2天的访问则会自动认为该IP为正常IP，否则会被判定为异常IP，在第8天开始持续推送异常IP事件。

使用说明

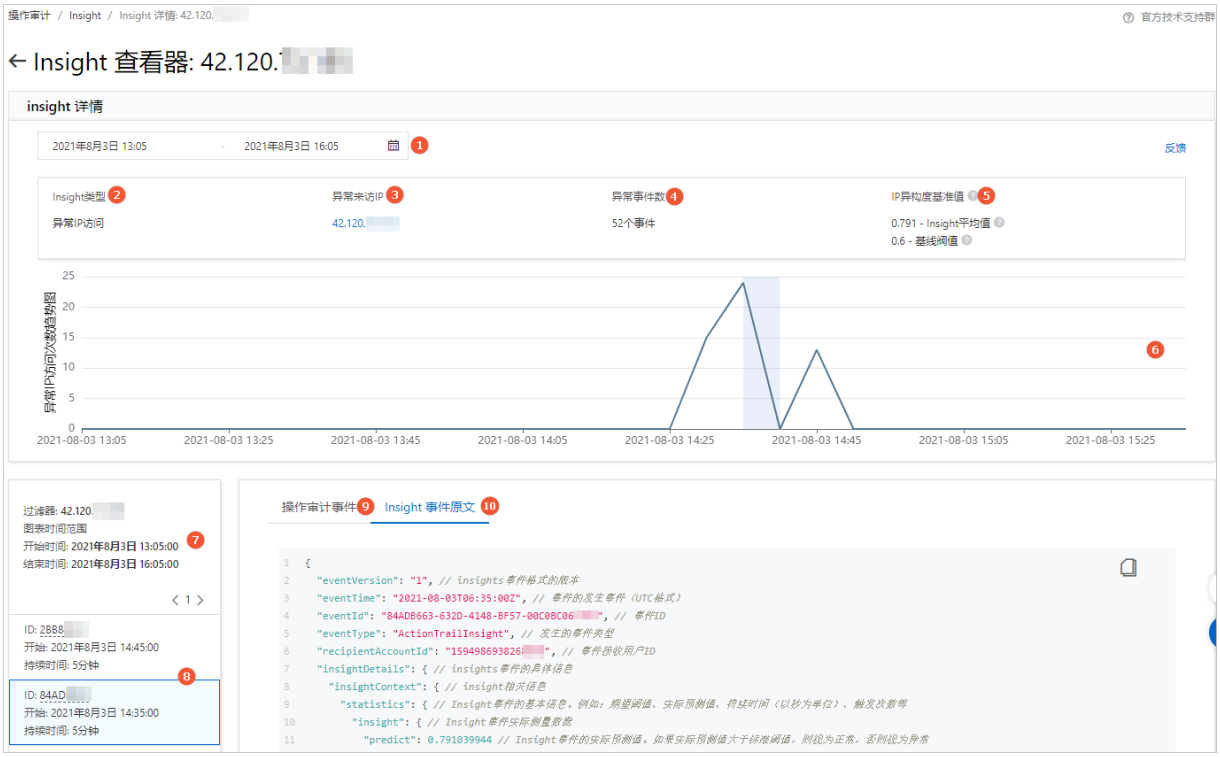
- 您需要通过提交工单，获取Insight事件的使用权限。
- 操作审计暂不支持查询华南2（河源）、华南3（广州）和阿联酋（迪拜）地域的Insight事件。关于Insight事件支持的地域，请参见操作审计支持的地域中除华南2（河源）、华南3（广州）和阿联酋（迪拜）外的其他地域。
- Insight事件功能目前支持免费试用，后续收费情况，请参见计费说明。
- 您需要创建跟踪的地域为全部地域、跟踪的事件类型为所有事件的单账号跟踪，并为跟踪开启Insight事件。对于全局事件，操作审计仅基于跟踪创建地域的全局管控事件生成Insight事件。
- 如果只有一个跟踪启用了Insight事件，当您禁用Insight事件再次启用后，需要在第二天才能重新生成Insight事件。
- 云上操作后10分钟才可以通过操作审计控制台查询相关Insight事件。

查询Insight事件

- 通过操作审计控制台查询Insight事件
  您可以通过操作审计控制台，查询单账号跟踪当前地域最近90天的Insight事件。关于Insight事件的更多信息，请参见Insight事件详情。
- 通过SLS或OSS控制台查询Insight事件
  如果需要查询超过90天的Insight事件，请访问跟踪指定的存储服务。

Insight事件详情

您可以通过操作审计控制台查询Insight事件详情，具体如下：



序号	说明	示例
1	Insight事件的查询时间范围（开始时间和结束时间）。	2021年08月03日13:55:00至2021年08月03日16:55:00
2	Insight类型。 异常行为的类型。	异常IP访问
3	异常来访IP。 您可以单击异常来访IP地址访问**Insight**页面，查询该IP地址的所有Insight事件。	42.120.XX.XX
4	异常事件数。 查询时间范围内来自该异常IP的管控事件数的总和。	115个事件
5	IP异构度基准值，包含Insight平均值和基线阈值。 **说明** 异构度=（基线阈值 - 实际值）/基线阈值*100。 • IP异构度基准值：本次访问IP与常用IP之间的关联关系。异构度越高，表明该IP特征越不符合常规，风险越高。 • Insight平均值：Insight事件的实际预测值。如果实际预测值大于标准阈值，则视为正常，否则视为异常。此处为选定时间内的平均值。 • 基线阈值：Insight事件的标准阈值。如果实际预测值大于基线阈值，则视为正常，否则视为异常。	• Insight平均值：0.0121 • 基线阈值：0.6
6	异常访问次数趋势图。	参见控制台图形

7	过滤器IP地址和图表时间范围（查询时间范围）。	• 过滤器：42.120.XX.XX
		• 图表时间范围：
		  ○ 开始时间：2021年08月03日14:00:00
		  ○ 结束时间：2021年08月03日17:00:00

8	Insight事件ID、开始时间和持续时间。 单个Insight事件分析窗口持续时间固定为5分钟。	• ID：2D30**** • 开始：2021年08月03日15:30:00 • 持续时间：5分钟
		事件代码示例： {

序号	说明	示例

9	选中Insight事件ID后，查询异常来访IP对应的管控事件及代码。	"eventId": "DFB8EB15-8F65-1B88-8F9E-6D8A5865****",
		"eventVersion": 1,
		"eventSource": "actiontrail.cn-hangzhou.aliyuncs.com",
		"requestParameters": { // API请求的输入参数
		"AcsProduct": "Actiontrail",
		"EndTime": "2021-08-03T07:35:00Z",
		"NextToken": "eyJhY2NvdW50IjoiMTU5NDk4NjkzODI2ODg5OCIsImV2ZW50SWQiOiIwRDMwMjYxNS03NDJFLTEyRjQtODM1Ri0xNDMzNUUyM0RFRDkiLCJpcCI6IjQyLjEyMC43NS4xNTQiLCJsb2dJZCI6IjYyLTE1OTQ5ODY5MzgyNjg4OTgiLCJ0aW1lIjoxNjI3OTc1ODQwMD****",
		"MaxResults": 20,
		"StartTime": "2021-08-03T07:30:00Z",
		"AcceptLanguage": "zh-CN",
		"Region": "cn-hangzhou",
		"LookupAttribute.1.Value": "42.120.XX.XX",
		"RegionId": "cn-hangzhou",
		"LookupAttribute.1.Key": "SourceIpAddress"
		},
		"sourceIpAddress": "42.120.XX.XX", // 事件发起的源IP地址
		"userAgent": "actiontrail.console.aliyun.com",
		"eventType": "ApiCall",
		"userIdentity": { // 请求者的身份信息
		"sessionContext": {
		"attributes": {
		"mfaAuthenticated": "false"
		}
		},
		"accountId": "159498693826****", // 阿里云账号ID
		"principalId": "159498693826****", // 当前请求者的ID
		"type": "root-account", // 阿里云账号
		"userName": "root"
		},
		"serviceName": "Actiontrail", // 事件相关的云服务名称
		"apiVersion": "2020-07-06",
		"requestId": "DFB8EB15-8F65-1B88-8F9E-6D8A586580A7",
		"eventTime": "2021-08-03T07:58:56Z", // 事件的发生时间（UTC格式）
		"isGlobal": false,
		"acsRegion": "cn-hangzhou", // 阿里云地域

序号	说明	示例
		"eventName": "LookupEvents" // 事件名称 关于管控事件的字段含义，请参见管控事件结构定义。

10	选中Insight事件ID后，查询Insight事件代码。	事件代码示例：
		{
		"event": {
		"eventVersion": "1",
		"eventTime": "2021-03-10T21:00:00Z",
		"acsRegion": "cn-hangzhou",
		"eventID": "F23A3DD5-7842-4EF9-9DA1-3776396A****",
		"eventType": "ActionTrailInsight",
		"recipient": "116214297662****",
		"insightDetails": {
		"sourceIpAddress": "42.120.XX.XX",
		"insightType": "IpInsight",
		"insightContext": {
		"statistics": {
		"baseline": {
		"threshold": 0.6
		},
		"insight": {
		"predict": 0.12
		},
		"insightDuration": 300,
		"insightCount": 10
		}
		}
		},
		"userIdentity": {
		"accountId": "112432432434****",
		"principalId": "231321312321****"
		},
		"eventCategory": "Insight"
		}
		}
		关于Insight事件的字段含义，请参见Insight事件结构定义。

序号	说明	示例

5.3. 通过操作审计控制台查询Insight事件

Insight事件帮助您从管控事件中发现异常行为。启用Insight事件后，操作审计将基于管控事件识别异常的IP调用事件并生成Insight事件。您可以通过操作审计控制台查询Insight事件，及时洞察云上管控风险并尽快采取补救措施。

前提条件

- 请确保您已经通过提交工单，获取Insight事件的使用权限。
- 请确保您已经创建了满足以下条件的单账号跟踪：
  - 跟踪的地域为全部地域。
  - 跟踪的事件类型为所有事件。

  具体操作，请参见创建单账号跟踪。

步骤一：启用Insight事件

您可以在创建跟踪时启用Insight事件，也可以为已有跟踪启用Insight事件。如下以已有跟踪为例为您介绍如何启用Insight事件。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在**跟踪列表**页面，单击目标跟踪名称。
4. 在**日志事件**区域，打开**异常IP访问**事件**状态**右侧的开关。

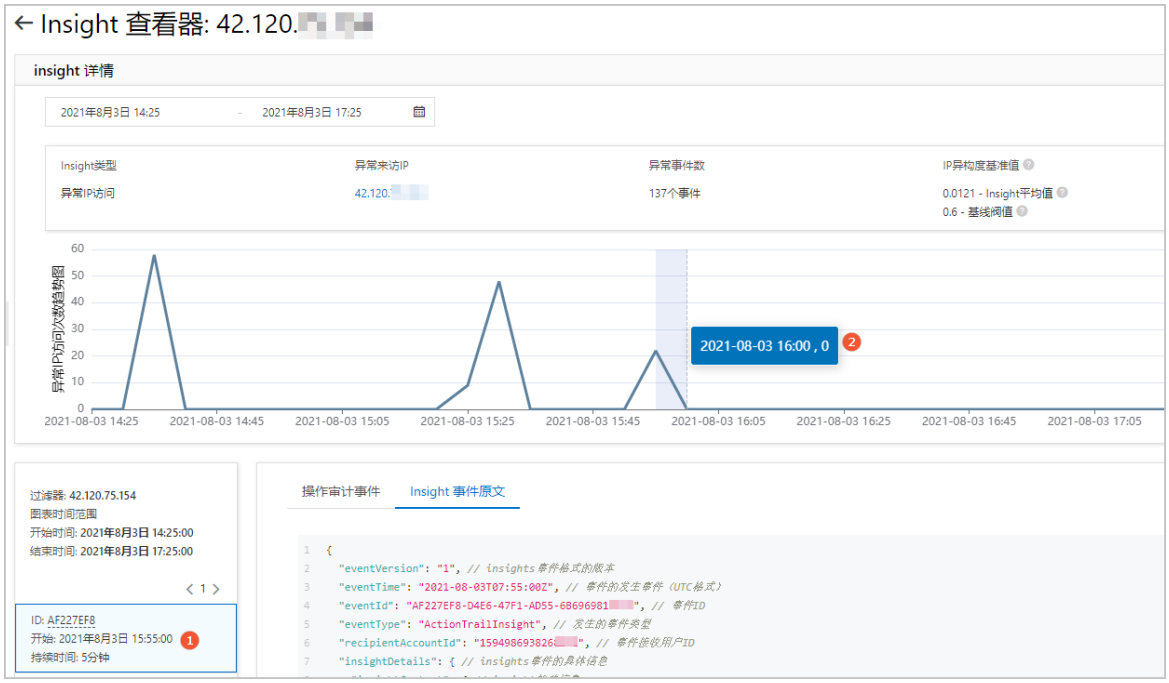
步骤二：查询Insight事件

1. 在左侧导航栏，单击**Insight**。
2. 在顶部导航栏，选择您想查询事件的地域。
3. 在**Insight**页面，输入搜索条件（例如：IP地址），设置查询的时间范围，然后单击

图标。

> **说明**
>
> - 您可以设置IP地址、Insight类型和事件ID等单个搜索条件来过滤查询事件。
> - 全局事件分析得出的Insight事件仅可以在跟踪的Home地域查询到。

4. 单击目标IP地址，在**Insight详情**区域查询异常事件数和IP异构度。
5. 单击事件列表，在趋势图中查询事件产生的时间和频率。



6. （可选）您可以在**操作审计事件**页签查询该异常IP相关的事件详情。也可以单击**Insight事件原文**页签，查询Insight事件代码记录。

5.4. 通过SLS或OSS控制台查询Insight事件

为跟踪启用Insight事件后，如果操作审计识别到异常调用操作并生成了Insight事件，操作审计会将Insight事件投递到跟踪指定的日志服务SLS或对象存储OSS。您可以通过SLS或OSS控制台查询Insight事件，以便查询90天以上的Insight事件或分析Insight事件。

前提条件

- 请确保您已经通过提交工单，获取Insight事件的使用权限。
- 请确保您已经创建了满足以下条件的单账号跟踪：
  - 跟踪的地域为全部地域。
  - 跟踪的事件类型为所有事件。

  具体操作，请参见创建单账号跟踪。
- 请确保您已经启用了Insight事件。具体操作，请参见启用Insight事件。

通过SLS控制台查询Insight事件

Insight事件和管控事件会投递到相同的SLS Logstore，您需要通过SQL语句 `* and event.eventType: ActionTrailInsight` 在SLS中查询Insight事件，以便分析Insight事件。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**Insight**。
3. 在顶部导航栏，选择您想查询事件的地域。
4. 在**Insight**页面，单击

   图标，然后将鼠标悬停至跟踪对应**存储服务**列的

   图标，最后单击日志库名称。

5. 在SLS控制台，单击**15分钟（相对）**，设置查询的时间范围。
6. 在搜索框中输入代码 `* and event.eventType: ActionTrailInsight`，然后单击**查询/分析**，查询Insight事件。

通过OSS控制台查询Insight事件

Insight事件和管控事件会投递OSS存储空间中不同的路径，Insight事件路径如下：

```
oss://<bucket>/<日志文件前缀>/AliyunLogs/Actiontrail-Insight/<region>/<年>/<月>/<日>/<日志文件>
```

1. 在操作审计控制台的**Insight**页面，单击

   图标，然后将鼠标悬停至跟踪对应**存储服务**列的

   图标，最后单击OSS存储空间名称。

2. 在OSS控制台的左侧导航栏，单击**文件管理**。
3. 单击**AliyunLogs**，然后单击**Actiontrail-Insight**，根据地域和日期查询Insight事件。

对象存储 / Bucket 列表 / gx-test-insight-oss / 文件管理
任务列表
gx-test-insight-oss / 华东1（杭州）
版本控制 未开通
读写权限 私有
类型 标准存储（本地冗余）
概览
用量查询
文件管理
权限管理
基础设置
冗余与容错
传输管理
日志管理
数据处理
数据安全
上传文件
新建目录
碎片管理
授权
批量操作
刷新
已选择：1 / 1
请输入文件名前缀匹配
文件名
文件大小
存储类型
更新时间
操作
/ AliyunLogs/ Actiontrail-Insight/ cn-hangzhou/ 2021/ 07/ 23/
Actiontrail_cn-hangzhou_20210723060000_1002_1_371_229fd0ea441211a55f14...
0.362KB
标准存储
2021年7月23日14:08:02
详情
更多

6.事件告警

6.1. 事件告警概览

操作审计支持事件告警功能。当您设置告警规则、用户和用户组后，如果检测到云上异常事件，操作审计将通过多种通知方式向用户和用户组发送告警通知，方便用户和用户组成员快速处理。

功能特性

- 实时检测事件：当您设置告警规则后，操作审计将实时检测云上异常事件，快速发现风险。
- 支持设置告警规则：操作审计内置关于账号安全、权限管理、资源管理等多条告警规则，也支持创建自定义告警规则。您可以一键开启告警规则，操作审计每15分钟执行一次检测，扫描指定跟踪中过去半小时内的事件。
- 支持多种通知方式：支持短信、邮件和钉钉等多种通知方式。1小时内相同告警通知不会重复发送。例如：操作审计10：00向用户和用户组发送了一次告警通知，10：00~11：00之间产生的告警通知将不会再次发送。
- 支持用户组管理：支持创建用户和用户组，灵活配置告警通知对象。

操作步骤

步骤	说明
步骤一：创建跟踪	操作审计事件告警功能支持检测指定跟踪中的事件，您需要先创建跟踪。
步骤二：启用事件告警	您需要启用事件告警，检测指定跟踪中的事件。
步骤三：创建用户和用户组	您需要创建用户和用户组，指定告警通知对象。
步骤四（可选）：创建内容模板	操作审计默认使用SLS ActionTrail内置内容模板为您发送告警通知。您也可以根据需要创建自定义的内容模板。
步骤五（可选）：创建行动策略	操作审计默认使用SLS ActionTrail内置行动策略为您发送告警通知。您也可以根据需要创建自定义的行动策略。
步骤六：开启告警规则	您需要开启告警规则，方便操作审计根据告警规则检测事件。当事件满足告警规则时将触发告警。
步骤七（可选）：设置告警参数	告警规则开启后，默认采用系统预置的严重度检测事件。您也可以根据需要设置告警参数。 说明 仅内置告警规则支持设置告警参数。
步骤八（可选）：创建白名单	如果您希望部分阿里云账号、RAM用户、RAM角色和IP地址不受告警规则限制，可以创建白名单。

6.2. 启用并设置事件告警

操作审计支持事件告警功能，当检测到云上异常操作事件时，将通过多种通知方式向用户和用户组发送告警通知，方便用户和用户组成员快速处理。本文为您介绍如何启用并设置事件告警。

步骤一：创建跟踪

请创建满足以下条件的跟踪：

- 跟踪的地域为全部地域。
- 跟踪的事件类型为所有事件。
- 跟踪投递的存储空间为日志服务SLS。

具体操作，请参见创建单账号跟踪和创建多账号跟踪。

步骤二：启用事件告警

您需要启用事件告警，检测指定跟踪中的操作事件。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在**跟踪列表**页面，单击目标跟踪名称。
4. 单击**启用高级功能**右侧的**设置**。

> **说明** **启用高级功能**右侧显示**是**，表示已经成功启用事件告警。

步骤三：创建用户和用户组

用户和用户组用于指定告警通知对象。例如：创建用户（Alice和Kumer）、用户组（操作审计运维组），并将Alice和Kumer加入到操作审计运维组中。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件告警**。
3. 创建用户。
   i. 在**事件告警**页面，选择**告警管理 > 用户管理**。
   ii. 在**用户管理**区域，单击**批量添加**。

iii. 在**添加用户**对话框的**待添加**页签，输入用户信息，然后单击**确认**。

用户信息代码示例：

```
#标识符，姓名，是否启用，国家号-手机号，可收短信，可接电话
1001,Kumer,true,86-1381111*****,true,true
1002,Alice,true,86-1381111*****,true,true
```

参数说明：

参数	描述	示例
标识符	用户唯一标识，不可重复。 长度为5~60个字符，以英文字母开头，可包含英文字母、数字、下划线（_）、短划线（-）和半角句号（.）。	1001、1002
姓名	用户姓名。 长度为1~20个字符，不能包含特殊字符：`"\$|~?&<>{}` `'`。	Kumer、Alice
是否启用	是否允许操作审计向该用户发送告警通知。取值： ■ true：允许。 ■ false：不允许。	true
国家号-手机号	用户手机号码，其中国家号为数字形式，长度为1~4个字符。	86-1381111*****、86-1381112*****
可收短信	是否允许操作审计给该手机号码发送短信通知。取值： ■ true：允许。 ■ false：不允许。	true
可接电话	是否允许操作审计给该手机号码发送语音通知。 ■ true：允许。 ■ false：不允许。	true

4. 创建用户组。

   i. 在**告警管理**下拉列表，选择**用户组管理**。

   ii. 在**用户组管理**区域，单击**创建**。

iii. 在**添加用户组**对话框，配置以下参数，然后单击**确认**。

重要参数说明和配置示例如下所示：

参数	描述	示例
标识符	用户组唯一标识，不可重复。 长度为5~60个字符，以英文字母开头，可包含英文字母、数字、下划线（_）、短划线（-）和半角句号（.）。	group-01
组名	用户组名称。 长度不超过20个字符，不能包含特殊字符：`\$|~?&<>{}` `'"` 。	操作审计运维组
待添加成员	您已创建的用户。	Kumer、Alice
已添加成员	已添加到用户组的用户。	Kumer、Alice
启用	是否允许操作审计向该用户组发送告警通知。取值： ■ 启用：允许。 ■ 不启用：不允许。	启用

步骤四（可选）：创建内容模板

操作审计默认使用SLS ActionTrail内置内容模板为用户/用户组发送告警通知。您也可以根据需要创建自定义的内容模板。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件告警**。
3. 在**事件告警**页面，选择**告警管理 > 内容模板**。
4. 单击**添加**。
5. 在**添加内容模板**对话框，设置ID和名称。
6. 设置各个渠道的告警通知内容。

告警渠道	配置项
短信	短信渠道的内容模板说明如下： ○ **非定制内容语言**：告警通知内容的语言，支持中文和英文。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
语音	语音渠道的内容模板说明如下： ○ **非定制内容语言**：告警通知内容的语言，支持中文（推荐）和英文。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。

告警渠道	配置项
邮件	邮件渠道的内容模板说明如下： ○ **非定制内容语言**：告警通知内容的语言，支持中文和英文。 ○ **主题**：告警消息的主题。您还可以使用模板变量定义主题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
钉钉	钉钉渠道的内容模板说明如下： ○ **标题**：告警消息的标题。您还可以使用模板变量定义标题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
WebHook-自定义	WebHook渠道的内容模板说明如下： ○ **发送方式**：支持逐条发送和合并发送。 例如发送内容配置为 `{ "project": "${project}", "alert_name": "${alert_name}"}` ，当触发两个告警时： ■ 逐条发送：发送两次告警通知，其内容分别为 `{ "project": "project-1", "alert_name": "alert-1"}` 和 `{ "project": "project-2", "alert_name": "alert-2"}` 。 ■ 合并发送：发送一次告警通知，其内容为 `[{ "project": "project-1", "alert_name": "alert-1"}, { "project": "project-2", "alert_name": "alert-2"}]` 。 ■ 选择合并发送时，如果限制了单个分组最多发送的条数，则只发送合并集合中的前N条告警。 ■ 选择合并发送时，如果您配置的内容可解析为JSON格式，则最终发送的内容为JSON格式。否则为字符串数组格式。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。 **说明** 发送告警通知时默认添加请求头信息Content-Type: application/json;charset=utf-8 Header。如果Webhook接收端需要其它格式的请求头，您可以在配置通知渠道时，自定义请求头信息。更多信息，请参见Webhook-自定义。
通知中心	通知中心渠道内容模板说明如下： ○ **非定制内容语言**：告警通知内容的语言，支持中文和英文。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。

告警渠道	配置项
企业微信	企业微信渠道的内容模板说明如下： ○ **标题**：告警消息的标题。您还可以使用模板变量定义标题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
飞书	飞书渠道的内容模板说明如下： ○ **标题**：告警消息的标题。您还可以使用模板变量定义标题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
Slack	Slack渠道的内容模板说明如下： ○ **标题**：告警消息的标题。您还可以使用模板变量定义标题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
EventBridge	事件总线（EventBridge）渠道的内容模板说明如下： ○ **主题**：告警消息的主题。您还可以使用模板变量定义主题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
函数计算	函数计算（FC）渠道的内容模板说明如下： ○ **发送方式**：支持逐条发送和合并发送。 例如发送内容配置为 `{ "project": "${project}", "alert_name": "${alert_name}"}` ，当触发两个告警时： ■ 逐条发送：发送两次告警通知，其内容分别为 `{ "project": "project-1", "alert_name": "alert-1"}` 和 `{ "project": "project-2", "alert_name": "alert-2"}` 。 ■ 合并发送：发送一次告警通知，其内容为 `[{ "project": "project-1", "alert_name": "alert-1"}, { "project": "project-2", "alert_name": "alert-2"}]` 。 ■ 选择合并发送时，如果限制了单个分组最多发送的条数，则只发送合并集合中的前N条告警。 ■ 选择合并发送时，如果您配置的内容可解析为JSON格式，则最终发送的内容为JSON格式。否则为字符串数组格式。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。

7. 单击**确认**。

步骤五（可选）：创建行动策略

行动策略用于控制告警通知的渠道和频率。操作审计内置告警规则默认使用SLS ActionTrail内置行动策略为您发送告警通知，您也可以创建行动策略，设置告警触发条件、通知渠道和接收人等信息。

1. 登录操作审计控制台。

2. 在左侧导航栏，单击**事件告警**。
3. 在**事件告警**页面，选择**告警管理 > 行动策略**。
4. 单击**添加**。
5. 在**添加行动策略**对话框，输入ID和名称。
6. 在**第一行动列表**页签，创建行动策略。
   i. 单击图标。
   ii. 配置触发告警通知的条件，然后单击**确认**。

参数	描述	示例
条件	取值： ■ **所有**：每个告警集合中所有的告警都满足所有条件时才会执行相应的行动组。 ■ **任意**：每个告警集合中任意一条告警满足所有条件时就会执行相应的行动组。	任意
条件表达式	针对符合条件的告警进行渠道分派。系统根据您配置的条件（对象、操作符、对象值），执行相应的行动组。	■ 对象：阿里云账号 ■ 操作符：等于 ■ 对象值：154035569884****
模式	您可以通过标准模式或高级模式添加多个条件。取值： ■ **标准模式**：多个条件之间为and关系。 ■ **高级模式**：多个条件之间可以为and或or关系，支持您使用圆括号将多个条件归为一组，且支持条件嵌套。	标准模式

iii. 配置行动组。

根据控制台界面，配置通知渠道及相关参数。通知渠道包括短信、语音、邮件、钉钉、WebHook和消息中心。更多信息，请参见通知渠道说明。

iv. 单击**条件**、**行动组**对话框对应的图标，结束第一行动列表配置。

> **说明** 如果您需要继续添加条件和行动组，请单击图标。

7. 单击**确认**。

步骤六：开启告警规则

操作审计支持内置告警规则和自定义告警规则，请根据实际需要开启对应的告警规则。例如：您希望在专有网络路由配置发生变更后触发告警，可以开启VPC网络路由变更告警。

> **说明** 您可以在操作审计控制台，将鼠标悬浮在告警规则名称右侧的
>
> 图标，查询告警规则详情。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件告警**。
3. 在**事件告警**页面，单击**规则/事务**页签。
4. 单击目标告警规则右侧**操作**列的**开启**。

   状态列显示**已开启**，表示成功开启告警规则。

步骤七（可选）：设置告警参数

告警规则开启后，默认采用系统预置的严重程度检测操作事件。您也可以根据需要设置告警参数。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件告警**。

3. 在**事件告警**页面，单击**规则/事务**页签。
4. 单击目标告警规则右侧**操作**列的**设置**。
5. 在**参数设置**对话框，设置以下参数，然后单击**保存**。

参数	描述	示例
行动策略	告警通知的渠道和频率。	网站日志告警行动策略
严重度	告警规则的严重程度。	高

> **说明** 您可以为账号连续登录失败告警设置**最大失败登录次数**，或者为未授权的API调用告警设置**未授权调用的最大次数**。

步骤八（可选）：创建白名单

如果您希望阿里云账号、RAM用户、RAM角色和IP地址不受告警规则限制，可以创建白名单。

> **说明** 仅部分告警规则支持创建白名单，请以控制台显示为准。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件告警**。
3. 在**事件告警**页面，单击**规则/事务**页签。
4. 单击目标告警规则右侧**外部配置**列的**白名单**。
5. 在**数据管理**对话框，单击**添加**。
6. 在**添加数据**对话框，根据控制台提示添加白名单信息（例如：154035569884****）。
7. 单击**确认**。

   添加成功后，您可以在白名单用户右侧**操作**列进行修改或删除操作。

6.3. 基础操作

6.3.1. 管理内容模板

操作审计按照内容模板中定义的内容给您配置的用户/用户组发送告警内容。本文为您介绍如何创建、修改、删除内容模板。

创建内容模板

操作审计默认使用SLS ActionTrail内置内容模板为用户/用户组发送告警通知。您也可以根据需求创建自定义的内容模板。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件告警**。
3. 在**事件告警**页面，选择**告警管理 > 内容模板**。
4. 单击**添加**。
5. 在**添加内容模板**对话框，设置**ID**和**名称**。
6. 设置各个渠道的告警通知内容。

告警渠道	配置项
短信	短信渠道的内容模板说明如下： ○ **非定制内容语言**：告警通知内容的语言，支持中文和英文。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
语音	语音渠道的内容模板说明如下： ○ **非定制内容语言**：告警通知内容的语言，支持中文（推荐）和英文。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
邮件	邮件渠道的内容模板说明如下： ○ **非定制内容语言**：告警通知内容的语言，支持中文和英文。 ○ **主题**：告警消息的主题。您还可以使用模板变量定义主题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
钉钉	钉钉渠道的内容模板说明如下： ○ **标题**：告警消息的标题。您还可以使用模板变量定义标题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
WebHook-自定义	WebHook渠道的内容模板说明如下： ○ **发送方式**：支持逐条发送和合并发送。 例如发送内容配置为 `{ "project": "${project}", "alert_name": "${alert_name}"}` ，当触发两个告警时： ■ 逐条发送：发送两次告警通知，其内容分别为 `{ "project": "project-1", "alert_name": "alert-1"}` 和 `{ "project": "project-2", "alert_name": "alert-2"}` 。 ■ 合并发送：发送一次告警通知，其内容为 `[{ "project": "project-1", "alert_name": "alert-1"}, { "project": "project-2", "alert_name": "alert-2"}]` 。 ■ 选择合并发送时，如果限制了单个分组最多发送的条数，则只发送合并集合中的前N条告警。 ■ 选择合并发送时，如果您配置的内容可解析为JSON格式，则最终发送的内容为JSON格式。否则为字符串数组格式。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。 **说明** 发送告警通知时默认添加请求头信息Content-Type: application/json;charset=utf-8 Header。如果Webhook接收端需要其它格式的请求头，您可以在配置通知渠道时，自定义请求头信息。更多信息，请参见Webhook-自定义。

告警渠道	配置项
通知中心	通知中心渠道内容模板说明如下： ○ **非定制内容语言**：告警通知内容的语言，支持中文和英文。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
企业微信	企业微信渠道的内容模板说明如下： ○ **标题**：告警消息的标题。您还可以使用模板变量定义标题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
飞书	飞书渠道的内容模板说明如下： ○ **标题**：告警消息的标题。您还可以使用模板变量定义标题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
Slack	Slack渠道的内容模板说明如下： ○ **标题**：告警消息的标题。您还可以使用模板变量定义标题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
EventBridge	事件总线（EventBridge）渠道的内容模板说明如下： ○ **主题**：告警消息的主题。您还可以使用模板变量定义主题。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。
函数计算	函数计算（FC）渠道的内容模板说明如下： ○ **发送方式**：支持逐条发送和合并发送。 例如发送内容配置为 `{ "project": "${project}", "alert_name": "${alert_name}"}` ，当触发两个告警时： ■ 逐条发送：发送两次告警通知，其内容分别为 `{ "project": "project-1", "alert_name": "alert-1"}` 和 `{ "project": "project-2", "alert_name": "alert-2"}` 。 ■ 合并发送：发送一次告警通知，其内容为 `[{ "project": "project-1", "alert_name": "alert-1"}, { "project": "project-2", "alert_name": "alert-2"}]` 。 ■ 选择合并发送时，如果限制了单个分组最多发送的条数，则只发送合并集合中的前N条告警。 ■ 选择合并发送时，如果您配置的内容可解析为JSON格式，则最终发送的内容为JSON格式。否则为字符串数组格式。 ○ **发送内容**：告警通知内容。您还可以使用模板变量定义内容。更多信息，请参见内容模板变量说明（新版）。

7. 单击**确认**。

修改内容模板

1. 单击目标内容模板右侧**操作**列的**修改**。
2. 在**编辑内容模板**对话框，修改**名称**、告警通知渠道和各个渠道的内容。
3. 单击**确认**。

删除内容模板

删除前请确保内容模板没有用于告警规则的行动策略。如果您删除了告警规则行动策略对应的内容模板，操作审计将使用SLS ActionTrail内置内容模板为您发送告警通知。

> **说明** 请不要删除SLS ActionTrail内置内容模板，以免告警通知异常。

1. 单击目标内容模板右侧**操作**列的**删除**。
2. 单击**确认**。

6.3.2. 管理行动策略

行动策略用于控制告警通知的渠道和频率。本文为您介绍如何创建、修改、删除行动策略。

创建行动策略

操作审计内置告警规则默认使用SLS ActionTrail内置行动策略。您也可以根据需求创建自定义的行动策略。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件告警**。
3. 在**事件告警**页面，选择**告警管理 > 行动策略**。
4. 单击**添加**。
5. 在**添加行动策略**对话框，输入**ID**和**名称**。
6. 在**第一行动列表**页签，创建行动策略。
   i. 单击 图标。

ii. 配置触发告警通知的条件，然后单击**确认**。

参数	描述	示例
条件	取值： ■ **所有**：每个告警集合中所有的告警都满足所有条件时才会执行相应的行动组。 ■ **任意**：每个告警集合中任意一条告警满足所有条件时就会执行相应的行动组。	任意
条件表达式	针对符合条件的告警进行渠道分派。系统根据您配置的条件（对象、操作符、对象值），执行相应的行动组。	■ 对象：阿里云账号 ■ 操作符：等于 ■ 对象值：154035569884****
模式	您可以通过标准模式或高级模式添加多个条件。取值： ■ **标准模式**：多个条件之间为and关系。 ■ **高级模式**：多个条件之间可以为and或or关系，支持您使用圆括号将多个条件归为一组，且支持条件嵌套。	标准模式

iii. 配置行动组。

根据控制台界面，配置通知渠道及相关参数。通知渠道包括短信、语音、邮件、钉钉、WebHook和消息中心。更多信息，请参见通知渠道说明。

iv. 单击**条件**、**行动组**对话框对应的图标，结束第一行动列表配置。

> **说明** 如果您需要继续添加条件和行动组，请单击图标。

7. 单击**确认**。

修改行动策略

1. 单击目标行动策略右侧**操作**列的**修改**。
2. 在**编辑行动策略**对话框，修改条件和行动组。
3. 单击**确认**。

删除行动策略

删除前请确保行动策略没有用于告警规则。如果您删除了告警规则使用的行动策略，基于告警规则的事件监控将发生异常。

> **说明** 操作审计内置告警规则默认使用SLS ActionTrail内置行动策略，请不要删除SLS ActionTrail内置行动策略，以免告警通知异常。

1. 单击目标行动策略右侧**操作**列的**删除**。
2. 单击**确认**。

6.3.3. 创建自定义告警规则

您可以创建自定义告警规则，配置需要监控的事件，从而更灵活地进行企业安全监控。通过添加查询统计，设置自定义告警语句，可以针对不同场景进行告警。本文为您介绍如何创建自定义告警规则、不同场景的自定义告警语句和自定义告警示例。

背景信息

自定义告警规则使用SQL（Structured Query Language）语法筛选事件。关于SQL语法的更多信息，请参见查询概述和分析简介。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件告警**。
3. 在**事件告警**页面，单击**新建告警**。
4. 在**告警监控规则**面板，添加查询统计。
   i. 单击**查询统计**右侧的**添加**。
   ii. 在**查询统计**对话框的**高级配置**页签，选择**类型**为**日志库**、**授权方式**为**默认**。

   > **说明** **区域**和**项目**将自动填入，与启用事件告警的跟踪相同，无需手动设置。

   iii. 选择跟踪投递的日志库（日志库名称格式为 `actiontrail_<跟踪名称>` ）。
   iv. 在**查询**右侧的文本框，输入自定义告警语句，然后单击**预览**。

   关于自定义告警语句的更多信息，请参见自定义告警语句。

   v. 单击**确认**。
5. 在**告警监控规则**面板，选择行动策略。
   i. 选择**告警策略**为**普通模式**。
   ii. 选择行动策略。
6. 在**告警监控规则**面板，设置**规则名称**、**检查频率**、**分组评估**、**触发条件**、**添加标签**、**添加标注**、**恢**

复通知、**连续触发阈值**、**无数据告警**和**重复等待**等参数。

关于参数的更多信息，请参见告警监控规则参数。

7. 单击**确定**。

   创建自定义告警规则成功后，告警规则列表中将增加**类别**为**自定义告警**的告警规则，您可以根据需求管理告警规则。具体操作，请参见管理告警规则。

自定义告警语句

场景	说明	自定义告警语句

筛选云服务和事件	通过指定云服务名称（serviceName）和事件名称（eventName），对特定云服务和事件进行告警。	• 指定单个服务的单个事件。例如：指定云服务器ECS的创建实例事件。
		`serviceName: Ecs and eventName: RunInstances`
		• 指定单个服务的多个事件。例如：指定云数据库RDS的释放实例事件。
		`event.serviceName: RDS and (event.eventName: DeleteDBInstance or event.eventName: Release or event.eventName: DestroyDBInstance)`
		• 指定多个服务的多个事件。例如：指定资源管理（Resource Management）和访问控制RAM的权限变更事件。
		`(event.serviceName: ResourceManager and (event.eventName: AttachPolicy or event.eventName: DetachPolicy)) or (event.serviceName: Ram and (event.eventName: AttachPolicyToUser or event.eventName: AttachPolicyToGroup or event.eventName: AttachPolicyToRole or event.eventName: DetachPolicyFromUser or event.eventName: DetachPolicyFromGroup or event.eventName: DetachPolicyFromRole))`

获取和指定参数	事件参数以JSON格式存储在event.requestParameterJson参数中，操作审计可以针对事件参数的具体取值进行告警。	• 获取云服务器ECS修改实例属性中实例释放保护属性为false的事件。
		`event.serviceName: Ecs and event.eventName: ModifyInstanceAttribute | SELECT * FROM (SELECT cast(json_extract("event.requestParameterJson", '$.DeletionProtection') as varchar) as deletion_protection FROM log) WHERE deletion_protection = 'false'`
		• 获取云数据库RDS将白名单设置为0.0.0.0的事件。
		`event.serviceName: Rds and event.eventName: ModifySecurityIps | SELECT * FROM (SELECT cast(json_extract("event.requestParameterJson", '$.SecurityIps') as varchar) as security_ips FROM log) WHERE security_ips like '%0.0.0.0%'`

获取资源	通过指定事件的相关资源名称（resourceName）和事件的相关资源类型（resourceType），获取事件的资源。 关于参数的更多信息，请参见管控事件结构定义。	获取单个资源。例如：获取云服务器ECS释放实例事件中操作的实例ID。 `event.serviceName: Ecs and (event.eventName: DeleteInstances or event.eventName: DeleteInstance or event.eventName: Release) | SELECT resourceArray[num] as instance_id FROM (SELECT split("event.resourceName", ';') as resourceArray, array_position(split("event.resourceType", ';'), 'ACS::ECS::Instance') as num FROM log) where num > 0`

场景	说明	自定义告警语句

获取身份	您可以获取事件中的身份信息，对指定身份进行告警。
	身份信息（userIdentity）包含身份类型（type）、身份名称（userName）、身份ID（principalId）、阿里云账号ID（accountId）等多个参数。关于参数的更多信息，请参见userIdentity包含的字段。
		• 获取身份类型。
		`* | SELECT "event.userIdentity.type" as user_type`
		• 获取身份名称。
		`* | SELECT "event.userIdentity.userName" as user_name`
		• 获取身份ID。
		`* | SELECT "event.userIdentity.principalId" as principal_id`
		• 获取阿里云账号ID。
		`* | SELECT "event.userIdentity.accountId" as account_id`

统计数量	您可以统计事件发生次数，超过指定次数时进行告警。	• ECS实例重启次数过多告警。例如：ECS实例重启次数超过2次进行告警。 `event.serviceName: Ecs and (event.eventName: RebootInstances or event.eventName: RebootInstance) | SELECT account_id, resourceArray[num] as instance_id, count(*) as cnt FROM (SELECT "event.userIdentity.accountId" as account_id, split("event.resourceName", ';') as resourceArray, array_position(split("event.resourceType", ';'), 'ACS::ECS::Instance') as num FROM log) where num > 0 group by account_id, instance_id` • 账号登录错误次数过多告警。例如：登录错误次数超过2次进行告警。 `event.eventName: ConsoleSignin and event.userIdentity.type: ram-user and not event.errorMessage: success | select "event.userIdentity.principalId" as user_id, "event.userIdentity.userName" as user_name, count(1) as cnt group by user_id, user_name`

自定义告警示例

arbitrary函数用于返回x中任意一个非空的值，语法为：`arbitrary(x)`。关于arbitrary函数的更多信息，请参见arbitrary函数。以下为您介绍两个使用arbitrary函数的自定义告警示例：

- 示例一：RDS实例释放告警

```
event.serviceName: RDS and (event.eventName: DeleteDBInstance or event.eventName: Release or event.eventName: DestroyDBInstance) | SELECT account_id, resourceArray[num] as instance_id, ram_user_id, user_type, user_name FROM (SELECT "event.userIdentity.accountId" as account_id, "event.userIdentity.principalId" as ram_user_id, split("event.resourceName", ';') as resourceArray, array_position(split("event.resourceType", ';'), 'ACS::RDS::DBInstance') as num, "event.userIdentity.type" as user_type, "event.userIdentity.userName" as user_name FROM log) where num > 0
```

- 示例二：安全组配置变更告警

```
 event.eventName: CreateSecurityGroup OR event.eventName: AuthorizeSecurityGroup OR event.e
ventName: AuthorizeSecurityGroupEgress OR event.eventName: RevokeSecurityGroup OR event.even
tName: RevokeSecurityGroupEgress OR event.eventName: JoinSecurityGroup OR event.eventName: L
eaveSecurityGroup OR event.eventName: DeleteSecurityGroup OR event.eventName: ModifySecurity
GroupPolicy) | select "event.userIdentity.accountId" as account_id, "event.userIdentity.prin
cipalId" as ram_user_id, "event.eventName" as event_name, arbitrary("event.userIdentity.type
") as user_type, arbitrary("event.userIdentity.userName") as user_name group by account_id,
ram_user_id, event_name
```

6.3.4. 管理告警规则

操作审计支持内置告警规则和自定义告警规则，用于检测云上异常事件。您可以根据需要开启、关闭、临时关闭、查询、关注、删除告警规则，或者关闭告警通知，也可以对自定义告警规则执行更新和复制操作。

背景信息

您可以在操作审计控制台**事件告警**页面的**规则/事务**页签查询告警规则列表，也可以将鼠标悬浮在告警规则名称右侧的

图标，查询告警规则详情。
操作审计支持创建自定义告警规则。具体操作，请参见创建自定义告警规则。

开启告警规则

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件告警**。
3. 在**事件告警**页面的**规则/事务**页签，单击目标告警规则右侧**操作**列的**开启**。

   告警规则的**状态**列显示**已开启**，表示已经成功开启告警规则。

关闭告警规则

关闭告警规则后，当事件满足告警规则时，操作审计将不再向您指定的用户或用户组发送告警通知。例如：您关闭了VPC网络路由变更告警对应的告警实例，在专有网络路由配置发生变更后将不再触发告警。

关闭告警规则不会对告警规则已有的告警实例产生影响，只是关闭了告警通知。

1. 在**事件告警**页面的**规则/事务**页签，单击目标告警规则右侧**操作**列的**关闭**。
2. 在**提示**对话框，单击**确定**。

   告警规则**状态**列显示**已创建|未开启**，表示已经成功关闭告警规则。

临时关闭与恢复告警规则

临时关闭告警规则时，您可以设置关闭时长。在关闭时长内，当事件满足告警规则时，操作审计将不再向您指定的用户和用户组发送告警通知。例如：您临时关闭了VPC网络路由变更告警对应的告警实例，并设置关闭时长为5分钟。5分钟内在专有网络路由配置发生变更后将不再触发告警，5分钟后会继续触发告警。

在关闭时长内，您可以恢复告警规则，此时操作审计将重新基于该告警规则检测事件。

1. 在**事件告警**页面的**规则/事务**页签，单击目标告警规则右侧**操作**列的**临时关闭**。
2. 在**临时关闭设置**对话框，设置**关闭时长**。

   您可以选择控制台预置的关闭时长，或者自定义关闭时长。
3. 单击**确认**。

   告警规则**状态**列显示临时关闭的具体时间（例如：`临时关闭到2021-05-20 18:34:03`），表示已经成

功临时关闭告警规则。

> **说明** 在临时关闭时长内，您可以单击目标告警规则右侧**操作**列的**恢复**，然后在**提示**对话框单击**确定**，恢复告警规则。

查询告警规则

您可以根据需要查询告警规则的创建时间、检查频率、启用状态、监控状态以及该条告警规则的告警历史。

1. 在**事件告警**页面的**规则/事务**页签，单击目标告警规则右侧**操作**列的**查看**。
2. 在**事件告警**页面，查询告警规则的基础信息和统计报表。

关注与取消关注告警规则

您可以将告警规则添加到关注列表，在日志服务控制台当前Project或控制台首页快速查询和定位告警规则。

1. 在**事件告警**页面的**规则/事务**页签，单击目标告警规则右侧**操作**列的**关注**。
2. 在**添加关注**对话框，选择关注入口。
   - **仅添加到当前Project关注列表**：在日志服务控制台的Project中选择 > **我的关注**，查询关注的告警规则。
   - **同步添加到全局关注列表**：在日志服务控制台首页的**我的关注**区域，查询关注的告警规则。
3. 单击**确认**。

> **说明** 您可以单击目标告警规则右侧**操作**列的**取消关注**，取消关注告警规则。

删除告警规则

当您需要删除告警规则下的所有告警实例时，可以删除告警规则。此时操作审计将不再基于该条告警规则检测事件。

1. 在**事件告警**页面的**规则/事务**页签，单击目标告警规则右侧**操作**列的**删除**。
2. 在**提示**对话框，单击**确认**。

   告警规则**状态**列显示**未创建**，表示已经成功删除告警规则。

关闭与恢复告警通知

当告警监控规则的状态为已开启时，支持关闭告警通知，并设置关闭时长。在关闭告警通知期间，操作审计仍会定期执行告警规则检查，即使满足告警条件也不会发送告警通知。

1. 在**事件告警**页面的**规则/事务**页签，单击目标告警规则右侧**操作**列的**查看**。
2. 在**事件告警**页面，单击**监控状态**右侧的**设置**。
3. 在**关闭告警通知**面板，设置关闭时长，然后单击**确定**。

> **说明** 在关闭告警通知期间，可以在监控状态中查看告警通知的恢复时间。您可以单击**监控状态**右侧的**设置**，在自动恢复告警通知前，手动恢复告警通知。

更新自定义告警规则

您可以根据需要更新自定义告警规则，包括查询统计、行动策略等信息。

1. 在**事件告警**页面的**规则/事务**页签，单击目标告警规则右侧**操作**列的**编辑**。

2. 在**告警监控规则**面板，更新**规则名称**、**检查频率**、**查询统计**、**分组评估**、**触发条件**、**添加标签**、**添加标注**、**恢复通知**、**连续触发阈值**、**无数据告警**、**告警策略**、**行动策略**和**重复等待**。

   关于参数的更多信息，请参见告警监控规则参数。

3. 单击**确定**。

复制自定义告警规则

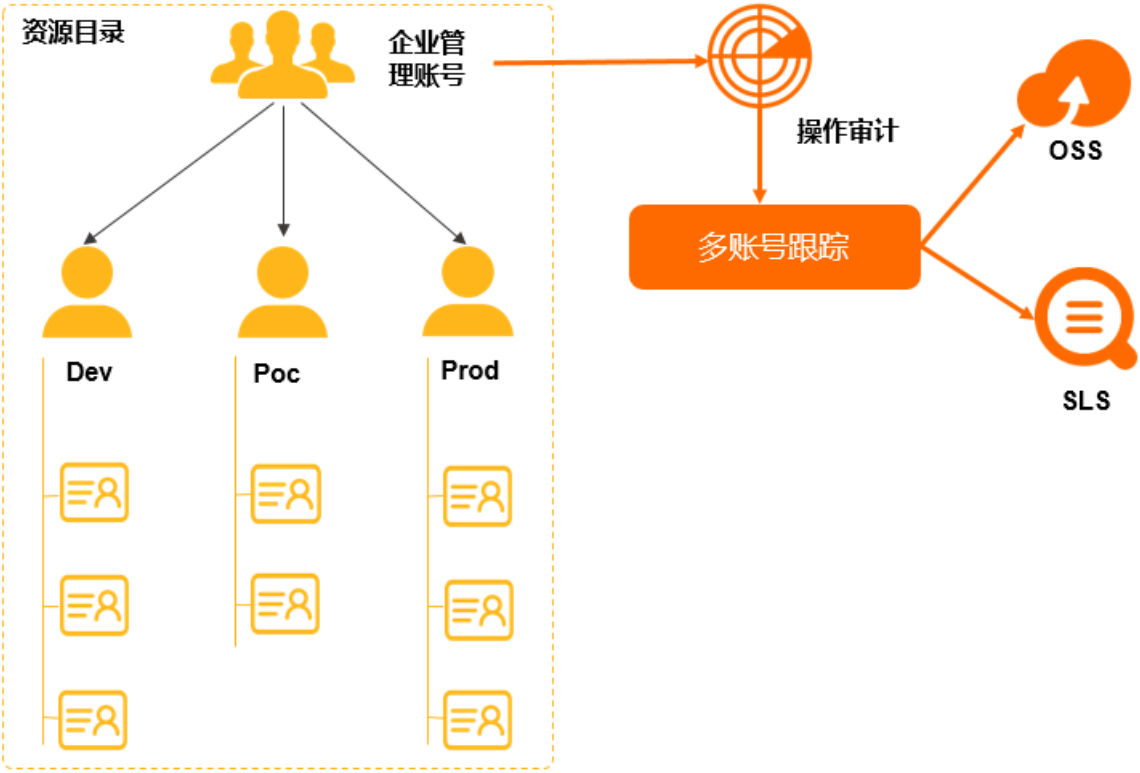
您通过复制自定义告警规则，将自定义告警规则应用于新的Project。

1. 在**事件告警**页面的**规则/事务**页签，单击目标告警规则右侧**操作**列的**复制**。
2. 在**目标Project**区域，选择自定义告警规则生效的Project。
3. 在**更多设置**区域，设置**目标告警名称**、**目标告警状态**和**目标告警ID**。
4. 单击**确定**。
5. 在**复制结果**对话框，查看复制告警状态，然后关闭对话框。

7.多账号跟踪（适用于企业用户）

7.1. 多账号跟踪概览

操作审计仅默认为每个阿里云账号记录最近90天的事件，您必须创建跟踪才能记录更长时间的事件，否则将无法追溯90天以前的事件。当企业开通了资源目录后，委派管理员账号（或者管理账号）可以在操作审计中创建多账号跟踪，将资源目录内的所有成员的事件投递到对象存储OSS或日志服务SLS。
多账号跟踪与资源目录的协作原理如下图所示。



基本概念

概念	说明
管理账号	管理账号是资源目录的超级管理员，也是开通资源目录的初始账号，对其创建的资源目录和成员拥有完全控制权限。只有通过企业实名认证的阿里云账号才能开通资源目录，每个资源目录有且只有一个管理账号。
成员	在资源目录内，成员作为资源容器，是一种资源分组单位。成员通常用于指代一个项目或应用，每个成员中的资源相对其他成员中的资源是物理隔离的。您可以通过管理账号授予RAM用户、RAM用户组或RAM角色对成员内资源的访问权限。 成员被管理账号邀请进入资源目录，或由管理账号在资源目录内直接创建。
委派管理员账号	资源目录的管理账号可以将资源目录中的成员设置为可信服务的委派管理员账号。设置成功后，委派管理员账号将获得管理账号的授权，可以在对应可信服务中访问资源目录组织和成员信息，并在该组织范围内进行业务管理。
多账号跟踪	多账号跟踪是委派管理员账号（或者管理账号）创建的用于记录所有成员事件的跟踪。多账号跟踪会把所有成员的事件投递到多账号跟踪设置的OSS存储空间或SLS Logstore。

概念	说明
单账号跟踪	单账号跟踪是阿里云账号创建的用于记录当前账号事件的跟踪。

多账号跟踪和单账号跟踪的区别

跟踪类型	创建账号	投递事件范围	事件查询方式	创建的最大跟踪数目
单账号跟踪	阿里云账号	当前账号的事件	• 操作审计控制台 • `LookupEvents` 接口 • 对象存储控制台 • 日志服务控制台	每个地域5个

多账号跟踪	委派管理员账号（或者管理账号）	所有成员的事件	• 委派管理员账号（或者管理账号）：
			  ○ 操作审计控制台
			  ○ `LookupEvents` 接口
			• 成员：
			  ○ 对象存储控制台
			  ○ 日志服务控制台
				所有地域1个

资源目录中成员的变化

当资源目录中成员变更时，操作审计将做如下处理：

- 当新成员被邀请进入资源目录，或管理账号在指定资源目录中创建新的成员时，新成员能够在跟踪列表查看多账号跟踪，其事件将被自动投递到指定的OSS存储空间或SLS Logstore。
- 当成员被从资源目录移除时，该成员将无法查看多账号跟踪，并停止将事件投递到指定的OSS存储空间或SLS Logstore，但已经投递的事件不会自动删除。
- 当成员归属的资源目录发生变更时，不会影响事件的投递。

7.2. 管理委派管理员账号

资源目录的管理账号可以将资源目录中的成员设置为操作审计的委派管理员账号。设置成功后，委派管理员账号将获得管理账号的授权，代替管理账号创建多账号跟踪，将资源目录中所有账号的事件投递到资源目录中任意成员下的SLS Logstore或OSS存储空间，实现操作事件的统一收集。

前提条件

- 请确保您已经开通资源目录。具体操作，请参见开通资源目录。
- 请确保您已经在资源目录中创建成员或邀请成员。具体操作，请参见创建成员和邀请阿里云账号加入资源目录。

应用场景

为操作审计添加委派管理员账号，可以将企业内的组织管理职能和审计管理职能从IT架构上隔离开，这对于企业云上IT的安全管理至关重要。

管理账号作为企业的中心管理者默认具有超级管理员权限，在企业IT管理的最佳实践中应使管理账号聚焦在对资源目录的组织管理上，尽量减少对其他云上配置的管理职责，避免超大权限的误操作。但是当企业在云上使用多个账号时，始终要有一些管理是面向全组织的，此时需要管理账号能够通过委派管理员账号来分担职责。例如：管理账号指定某个成员作为操作审计的委派管理员账号，该账号被企业内审计部门所拥有和使用，审计部门通过该账号来统一收集事件并进行审计监督和分析。这也符合企业内实际的岗位分工。

总之，企业使用操作审计的委派管理员账号可以实现以下需求，符合多账号管理的最佳实践。

- 企业内设置专职账号负责审计事件的收集、管理和分析，与业务账号隔离开。
- 委派管理员账号代替管理账号管理操作审计相关的配置操作，分担管理账号的部分职责，尽量规避管理账号的频繁使用。

关于委派管理员账号的更多信息，请参见什么是委派管理员账号。

添加委派管理员账号

企业可以在资源目录中指定一个成员作为专职的审计账号，即操作审计的委派管理员账号。该账号仅用于管理云上的审计配置和留存审计事件，账号下不保有其他资源。这也符合三权分立的安全管理要求，将权限管理、审计管理、资源管理进行账号维度的职能隔离。委派管理员账号用于在本账号中创建面向资源目录的多账号跟踪，并将事件统一投递到指定的存储空间。该存储空间可以在本账号内（推荐），也可以指定另一个专门用于存储事件的账号。您可以使用委派管理员账号长期管理跟踪的配置、存储所有账号的事件和持续的审计分析告警。

操作审计服务的委派管理员账号将获得以下权限：

- 获得管理账号的授权，可以在操作审计服务中访问资源目录组织和成员信息。
- 在操作审计中创建面向全资源目录的多账号跟踪，统一收集资源目录中所有成员的事件。

> **说明** 由于资源目录中只能创建一个多账号跟踪，所以每个资源目录的管理账号最多支持为操作审计添加一个委派管理员账号。

您可以使用企业管理员账号在资源管理控制台添加委派管理员账号。具体操作，请参见添加委派管理员账号。

更换委派管理员账号

当您为操作审计添加委派管理员账号后，不建议变更该账号。委派管理员账号作为企业的固有资产承担业务职能，不应该随意更换，更换账号也将导致一些配置暂时失效，影响企业完整持续的审计。如果一定要更换账号，请先移除原有委派管理员账号（账号A），然后添加新的委派管理员账号（账号B）。

> **注意** 移除委派管理员账号前，需要先删除该账号下的多账号跟踪。删除多账号跟踪会中断事件的收集工作，请在移除前慎重考虑。关于如何删除多账号跟踪，请参见删除多账号跟踪。

1. 在资源管理控制台，使用管理账号在资源目录中移除操作审计原有委派管理员账号（账号A）。

   具体操作，请参见移除委派管理员账号。
2. 在资源管理控制台，添加新的委派管理员账号（账号B）。

   具体操作，请参见添加委派管理员账号。
3. 在操作审计控制台，使用新的委派管理员账号（账号B）创建多账号跟踪，将事件投递到该账号（账号B）中的存储空间。

   具体操作，请参见访问成员和创建多账号跟踪。

4. 在操作审计控制台，使用新的委派管理员账号（账号B）创建历史事件投递任务，将过去90天的事件以任务的方式一次性补投递到指定的存储空间。

   具体操作，请参见创建历史事件投递任务。

5. 在SLS控制台或OSS管理控制台，将原有的委派管理员账号（账号A）中已有的事件合并到新的委派管理员账号（账号B）的存储空间中。

   具体操作，请参见SLS的数据在线迁移和OSS的数据在线迁移。

   > **说明** 更换委派管理员账号后，新的存储空间中将出现约90天的重复事件，以便确保审计的完整性。

7.3. 创建多账号跟踪

本文为您介绍如何通过操作审计控制台创建多账号跟踪。多账号跟踪将把资源目录内所有成员的事件投递到多账号跟踪中设置的SLS Logstore或OSS存储空间。

前提条件

您已经开通资源目录。具体操作，请参见开通资源目录。

操作步骤

1. 通过委派管理员账号（或者管理账号）登录操作审计控制台。

   关于如何设置委派管理员账号，请参见管理委派管理员账号。

2. 在左侧导航栏，单击**跟踪列表**。
3. 在顶部导航栏选择您想创建多账号跟踪的地域。

   > **说明** 该地域将成为多账号跟踪的Home地域，即创建跟踪的地域。

4. 在**跟踪列表**页面，单击**创建跟踪**。
5. 在**跟踪基本属性**页面，设置如下参数，然后单击**下一步**。

参数	说明
跟踪名称	跟踪的名称。您需要在阿里云账号中设置唯一的名称，该名称将用于在SLS中对Logstore命名，命名规则为 `actiontrail_<跟踪名称>` 。

参数	说明
日志事件	跟踪投递的事件。取值：管控事件，表示用户管理云上资源时管控平面的操作记录。 管控事件的事件类型如下： ○ **所有事件**：读事件和写事件。审计相关的法规和标准均强调对审计事件的完整记录，建议您选择**所有事件**。 ○ **写事件**：增加、删除或修改云上资源的事件，例如：CreateInstance（创建一台包年包月或者按量付费的ECS实例）。如果您仅导出事件进行自定义分析，且只关注会影响云资源的事件，则选择**写事件**。 ○ **读事件**：本身没有在云上增加、删除或修改配置的操作意图，也不会对云上配置造成变更，仅读取云服务资源信息的事件，例如：DescribeInstances（查询一台或多台ECS实例的详细信息）。读事件一般事件量非常大，会占用较多存储空间。但审计相关法规和标准均强调对审计事件的完整记录，所以建议您同时投递读事件，以便完整还原AK的使用历史和资源的访问历史。 **说明** 当您通过操作审计控制台创建跟踪时，默认将跟踪投递的地域设置为全部地域。如果需要创建部分地域的跟踪，请调用CreateTrail接口设置TrailRegion参数。
将跟踪应用到所有成员	跟踪的应用范围。取值： ○ **是**：该跟踪为多账号跟踪，将收集管理账号和所有成员的事件，投递到统一的存储空间。为避免遗漏事件，建议您选择此选项。 ○ **否**：该跟踪将成为单账号跟踪，仅投递当前账号的事件。 **说明** ○ 此选项一旦选定不可更改。如果创建多账号跟踪后您需要修改**将跟踪应用到所有成员**选项，则需要删除多账号跟踪后重新创建。 ○ 创建多账号跟踪后，**跟踪列表**页面中的**创建来源**列将显示**将跟踪应用到所有成员**的选择情况。 ■ 若选择**是**，**跟踪类型**列显示**多账号跟踪**。 ■ 若选择**否**，**跟踪类型**列显示**单账号跟踪**。

6. 在**审计事件投递**页面，选择投递方式，然后单击**下一步**。

   您可以将跟踪分别投递到日志服务SLS或对象存储OSS，或者同时进行投递。关于如何选择存储服务，请参见将事件持续投递到指定服务。

   说明 目前投递的事件范围，是多账号跟踪生效后产生的新事件，不包括原有的最近90天事件。您可以创建历史事件投递任务，将最近90天的事件一次性补投递到您跟踪指定的地址，最大限度、最大范围满足您的需求。具体操作，请参见创建历史事件投递任务。

   ○ 选择**将事件投递到日志服务SLS**

- 选择**投递到本账号**，设置如下参数。

参数	描述
日志库所属地域	日志项目所在地域。
日志项目名称	日志服务SLS中日志项目的名称。同一账号下，日志项目名称不能重复。 ■ 当您选中**创建新的日志项目**时，将通过操作审计控制台新建日志项目，输入日志项目名称。 ■ 当您选中**选择已有的日志项目**时，在日志服务SLS中选择已有日志项目名称。 **说明** 投递成功后操作审计会自动创建一个名为 `actiontrail_<跟踪名称>` 的日志库（Logstore），该Logstore会自动帮您设置审计最佳配置，创建查询所需索引和仪表盘，并禁止用户写入，保证审计数据的准确性。您无需提前创建Logstore。

- 选择**投递到其他账号**，设置**日志项目ARN**和**日志写入角色ARN**。
  选择投递到其他账号时需要先在目标账号中创建RAM角色，授予操作审计服务向目标账号投递事件的权限，并提前创建日志项目。具体操作，请参见将资源目录中多个成员的事件投递到同一账号。

- 选择**将事件投递到对象存储OSS**
  - 选择**投递到本账号**，设置如下参数。

参数	描述
存储空间名称	对象存储OSS中存储空间的名称。同一账号下，存储空间名称不能重复。 ■ 当您选中**创建新的存储空间**时，通过操作审计控制台新建存储空间，输入存储空间名称。 ■ 当您选中**选择已有的存储空间**时，在对象存储OSS中选择已有存储空间名称。
日志文件前缀	事件存放的日志文件前缀，方便后续查找事件。
开启服务端加密	存储空间中的日志文件是否加密。当您选中**创建新的存储空间**时，需要设置该参数。取值： ■ **OSS完全托管** ■ **KMS** ■ **否** **说明** 关于OSS服务器加密功能，请参见服务器端加密。

  - 选择**投递到其他账号**，设置**存储空间角色ARN**、**存储空间名称**和**日志文件前缀**。
    选择投递到其他账号时需要先在目标账号中创建RAM角色，授予操作审计服务向目标账号投递事件的权限，并提前创建OSS存储空间。具体操作，请参见将资源目录中多个成员的事件投递到同一账号。

7. 在**预览并创建**页面，确认跟踪信息，然后单击**提交**。

执行结果

创建多账号跟踪后，事件会以JSON格式保存在SLS Logstore或OSS存储空间中。您可以通过管理账号在日志服务SLS或对象存储OSS中查看已投递的事件。

> **说明** 管理账号仅能在对象存储OSS或日志服务SLS中看到资源目录中成员的事件，不能通过操作审计控制台的**事件查询**或 `LookupEvents` 接口查询成员的事件。

- 日志服务SLS：操作审计会自动创建一个名为 `actiontrail_<跟踪名称>` 的日志库（Logstore）。您可以在**跟踪列表**页面将鼠标悬浮到跟踪对应**存储服务**列的 ! 图标，然后单击SLS日志库名称分析事件。
- 对象存储OSS：各成员中产生的全局事件，将与Home地域的事件放在一起。非全局事件存放在资源归属的地域目录下。您可以通过Elastic MapReduce服务或自行授予第三方日志分析服务分析此事件的权限。

  您也可以在**跟踪列表**页面将鼠标悬浮到跟踪对应**存储服务**列的 ! 图标，然后单击OSS Bucket名称，最后单击**文件管理**查看事件。关于OSS存储路径的更多信息，请参见事件投递到OSS存储空间后，存储路径是怎样的？。

7.4. 更新多账号跟踪

本文为您介绍如何使用操作审计控制台更新多账号跟踪。

前提条件

请确保您已经开通资源目录。具体操作，请参见开通资源目录。

操作步骤

1. 通过委派管理员账号（或者管理账号）登录操作审计控制台。

   > **说明**
   > - 成员仅能查看多账号跟踪，无权更新多账号跟踪。
   > - 关于如何设置委派管理员账号，请参见管理委派管理员账号。

2. 在左侧导航栏，单击**跟踪列表**。
3. 在**跟踪列表**页面，单击目标跟踪名称。
4. 单击页面右上角的**编辑**。
5. 在**跟踪基本属性**页面，更新管控事件的**事件类型**，然后单击**下一步**。
6. 在**审计事件投递**页面，更新投递方式，然后单击**下一步**。
   - **将事件投递到日志服务SLS**
     - 选择**投递到本账号**，更新**日志库所属地域**和**日志项目名称**。
     - 选择**投递到其他账号**，更新**日志项目ARN**和**日志写入角色ARN**。
   - **将事件投递到对象存储OSS**
     - 选择**投递到本账号**，更新**存储空间名称**、**日志文件前缀**和**开启服务端加密**。

       > **说明** 仅当您选择**创建新的存储空间**时，支持更新**开启服务端加密**。

     - 选择**投递到其他账号**，更新**存储空间角色ARN**、**存储空间名称**和**日志文件前缀**。

7. 在**预览并创建**页面，确认更新后的跟踪信息，然后单击**提交**。
8. （可选）在弹出的对话框，单击**确定**。

> **说明** 当**将跟踪应用到所有成员**选项为**是**时，需要单击**确定**。此时资源目录中所有成员的参数设置都将被更新。

7.5. 删除多账号跟踪

本文为您介绍如何使用操作审计控制台删除多账号跟踪。删除后多账号跟踪后，将停止收集资源目录中成员的操作事件。

前提条件

启用高级功能的跟踪不支持直接删除，删除跟踪前请确保**启用高级功能**右侧状态为**否**。

操作步骤

1. 通过委派管理员账号（或者管理账号）登录操作审计控制台。

> **说明**
> - 成员仅能查看多账号跟踪，无权删除多账号跟踪。
> - 关于如何设置委派管理员账号，请参见管理委派管理员账号。

2. 在左侧导航栏，单击**跟踪列表**。
3. 在**跟踪列表**页面，单击目标跟踪名称。
4. 单击页面右上角的**删除**。
5. 在**删除跟踪**对话框，单击**确定**。

> **注意** 已经投递到SLS Logstore或OSS存储空间的操作事件将不会被删除。如果您需要删除SLS Logstore或OSS存储空间的操作事件，请参见删除Logstore和删除存储空间。

7.6. 关闭多账号跟踪

本文介绍如何使用操作审计控制台关闭多账号跟踪。关闭后，操作审计会停止将资源目录中成员的操作事件投递到日志服务SLS或对象存储OSS。

操作步骤

1. 通过委派管理员账号（或者管理账号）登录操作审计控制台。

> **说明**
> - 成员仅能查看多账号跟踪，无权关闭多账号跟踪。
> - 关于如何设置委派管理员账号，请参见管理委派管理员账号。

2. 在左侧导航栏，单击**跟踪列表**。
3. 在**跟踪列表**页面，单击目标跟踪名称。
4. 关闭**跟踪状态**开关。

> **说明** 再次单击开关可以开启多账号跟踪。

5. 在**关闭跟踪**对话框，单击**确定**。

8.跨账号投递事件

8.1. 将资源目录中多个成员的事件投递到同一账号

您可以使用操作审计的跨账号投递功能，将资源目录中多个成员的事件投递到同一账号的日志服务SLS或对象存储OSS中，从而实现统一的审计数据归档和监控。

背景信息

在操作审计的跨账号投递功能中，您需要理解目标账号和源账号，具体如下。

账号	说明	操作
目标账号	用于接收其他账号事件的账号。	• 创建用于接收事件的存储空间，例如：SLS Logstore或OSS存储空间。 • 创建可信实体为操作审计服务的RAM角色，其他账号需通过扮演该角色向目标账号写入事件。
源账号	需要向目标账号写入事件的账号。	使用成员对应的管理账号创建跟踪，将事件投递到目标账号的存储空间。

当目标账号和源账号处于同一资源目录时，基于资源目录的结构互信，跨账号投递可以省略很多配置步骤。根据目标账号的不同分为以下两种情况：

- 当目标账号是管理账号时，您可以创建多账号跟踪，将资源目录下所有账号的事件投递到管理账号中的日志服务SLS或对象存储OSS。具体操作，请参见创建多账号跟踪。
- 当目标账号是成员时，请按照本文所述的操作步骤进行配置。

操作步骤

1. 在目标账号中创建RAM角色，并授权操作审计服务向目标账号投递事件的权限。
   i. 使用目标账号登录RAM控制台。
   ii. 创建可信实体为操作审计的RAM角色。
      a. 在左侧导航栏，选择**身份管理 > 角色**。
      b. 在**角色**页面，单击**创建角色**。
      c. 在**创建角色**面板，选择可信实体类型为**阿里云服务**，然后单击**下一步**。
      d. 选择角色类型为**普通服务角色**。
      e. 设置角色名称为**ActionTrailDeliveryRole**。
      f. 选择受信服务为**操作审计**。
      g. 单击**完成**。

iii. 为RAM角色进行精确授权，授予系统策略AliyunActionTrailDeliveryPolicy。

a. 单击**精确授权**。

b. 选择**系统策略**，并设置策略名称为**AliyunActionTrailDeliveryPolicy**。

c. 单击**确定**，然后单击**关闭**。

您可以在**角色**页面，查看RAM角色ActionTrailDeliveryRole绑定的权限策略AliyunActionTrailDeliveryPolicy的详细内容。关于权限策略的更多信息，请参见事件投递的系统权限策略。

iv. 修改RAM角色的信任策略，将 `Service` 字段修改为 `管理账号@actiontrail.aliyuncs.com` 的格式。

例如：管理账号是 `159498693826****` ，则需要将 `Service` 中的 `actiontrail.aliyuncs.com` 修改为 `159498693826****@actiontrail.aliyuncs.com` ，表示该RAM角色可以被管理账号 `159498693826****` 下的操作审计服务扮演。

```
{
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "159498693826****@actiontrail.aliyuncs.com"
                ]
            }
        }
    ],
    "Version": "1"
}
```

具体操作，请参见修改RAM角色的信任策略。

2. 使用目标账号创建日志服务SLS的Project或对象存储OSS的存储空间。

具体操作，请参见创建Project和创建存储空间。

> **说明** 基于数据安全考虑，建议您在创建存储空间时，设置服务器加密和合规保留策略。具体操作，请参见服务器端加密和设置合规保留策略。

3. 使用管理账号创建多账号跟踪，设置投递目标为步骤2创建的Project或存储空间。

i. 使用管理账号登录操作审计控制台。

ii. 在左侧导航栏，单击**跟踪列表**。

iii. 在顶部导航栏选择您想创建多账号跟踪的地域。

> **说明** 该地域将成为多账号跟踪的Home地域。

iv. 在**跟踪列表**页面，单击**创建跟踪**。

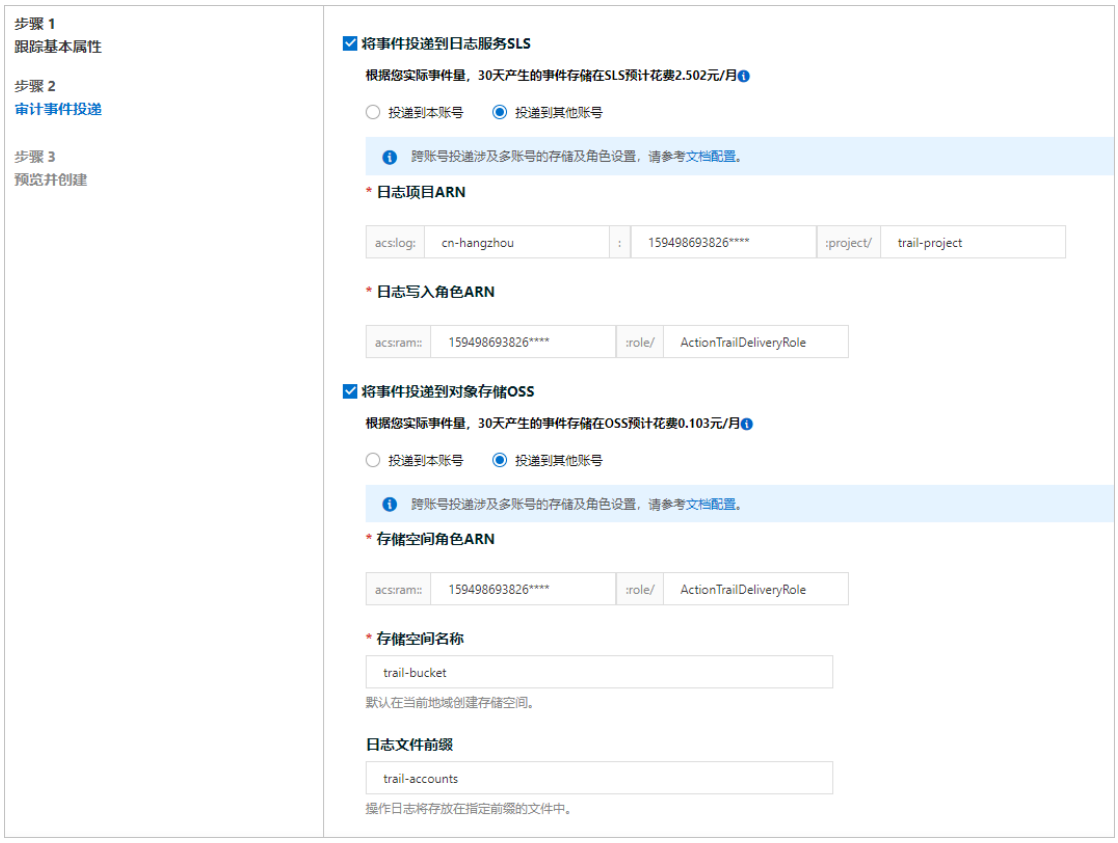
v. 在**跟踪基本属性**页面，设置**跟踪名称**、管控事件的**事件类型**和**将跟踪应用到所有成员**，然后单击**下一步**。

说明

- **将跟踪应用到所有成员**请设置为**是**。
- 系统默认将跟踪投递的地域设置为全部地域。推荐您将**事件类型**设置为**所有事件**，以便跟踪全部地域的全部事件。
- 关于参数的更多信息，请参见创建多账号跟踪。

vi. 在**审计事件投递**页面，选择投递方式，单击**下一步**。

您可以将跟踪分别投递到日志服务SLS或对象存储OSS，或者同时进行投递。关于如何选择存储服务，请参见将事件持续投递到指定服务。



- 选择**将事件投递到日志服务SLS**，然后选择**投递到其他账号**，并设置以下参数。

参数	描述
日志项目ARN	输入日志项目所在地域、目标账号ID和日志项目名称。 其中，日志项目名称为步骤2中创建的Project名称。
日志写入角色ARN	输入目标账号ID和角色名称。 其中，角色名称为步骤1中创建的RAM角色名称（本文示例为ActionTrailDeliveryRole）。

- 选择**将事件投递到对象存储OSS**时，然后选择**投递到其他账号**，并设置以下参数。

参数	描述
存储空间角色ARN	输入目标账号ID和角色名称。 其中，角色名称为步骤1中创建的RAM角色名称（本文示例为ActionTrailDeliveryRole）。
存储空间名称	输入步骤2中创建的存储空间名称。
日志文件前缀	输入事件存放的日志文件前缀。

vii. 在**预览并创建**页面，确认跟踪信息，然后单击**提交**。

执行结果

跟踪创建成功后，您可以使用目标账号查看SLS Project或OSS存储空间中来自多个成员的事件。

8.2. 将多个阿里云账号的事件投递到同一账号

您可以使用操作审计的跨账号投递功能，将多个阿里云账号的事件投递到同一账号的日志服务SLS或对象存储OSS中，从而实现统一的审计数据归档和监控。

背景信息

在操作审计的跨账号投递功能中，您需要理解目标账号和源账号，具体如下。

账号	说明	操作
目标账号	用于接收其他账号事件的账号。	• 创建用于接收事件的存储空间，例如：SLS Logstore或OSS存储空间。 • 创建可信实体为操作审计服务的RAM角色，其他账号需通过扮演该角色向目标账号写入事件。
源账号	需要向目标账号写入事件的账号。	使用阿里云账号创建跟踪，将事件投递到目标账号的存储空间。

当目标账号和源账号是无组织关系的独立阿里云账号时，跨账号投递需要为每个阿里云账号分别创建单账号跟踪。以下以同时将阿里云账号A（源账号）和阿里云账号B（源账号）的事件投递到阿里云账号C（目标账号）为例，为您进行介绍。

创建单账号跟踪时您可以设置Insight事件，Insight事件需要申请才能使用。更多信息，请参见Insight事件概览。

操作步骤

1. 在阿里云账号C中创建RAM角色，并授权操作审计服务向阿里云账号C投递事件的权限。
   i. 使用阿里云账号C登录RAM控制台。
   ii. 创建可信实体为操作审计的RAM角色。
      a. 在左侧导航栏，选择**身份管理 > 角色**。
      b. 在**角色**页面，单击**创建角色**。
      c. 在**创建角色**面板，选择可信实体类型为**阿里云服务**，然后单击**下一步**。
      d. 选择角色类型为**普通服务角色**。
      e. 设置角色名称为**ActionTrailDeliveryRole**。
      f. 选择受信服务为**操作审计**。
      g. 单击**完成**。

iii. 为RAM角色进行精确授权，授予系统策略AliyunActionTrailDeliveryPolicy。

a. 单击**精确授权**。

b. 选择**系统策略**，并设置策略名称为**AliyunActionTrailDeliveryPolicy**。

c. 单击**确定**，然后单击**关闭**。

您可以在**角色**页面，查看RAM角色ActionTrailDeliveryRole绑定的权限策略AliyunActionTrailDeliveryPolicy的详细内容。关于权限策略的更多信息，请参见事件投递的系统权限策略。

iv. 修改RAM角色的信任策略，将 `Service` 字段修改为 `阿里云账号@actiontrail.aliyuncs.com` 的格式。

例如：阿里云账号A是 `159498693825****` 、阿里云账号B是 `123435555956****` ，则需要将 `Service` 中的 `actiontrail.aliyuncs.com` 修改为 `["159498693825****@actiontrail.aliyuncs.com","123435555956****@actiontrail.aliyuncs.com"]` ，表示该RAM角色可以被阿里云账号A `159498693825****` 和阿里云账号B `123435555956****` 下的操作审计服务扮演。

```
{
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "159498693825****@actiontrail.aliyuncs.com",
                    "123435555956****@actiontrail.aliyuncs.com"
                ]
            }
        }
    ],
    "Version": "1"
}
```

具体操作，请参见修改RAM角色的信任策略。

2. 使用阿里云账号C创建日志服务SLS的Project或对象存储OSS的存储空间。

具体操作，请参见创建Project和创建存储空间。

> **说明** 基于数据安全考虑，建议您在创建存储空间时，设置服务器加密和合规保留策略。具体操作，请参见服务器端加密和设置合规保留策略。

3. 使用阿里云账号A创建单账号跟踪，设置投递目标为步骤2创建的Project或存储空间。

i. 使用阿里云账号A登录操作审计控制台。

ii. 在左侧导航栏，单击**跟踪列表**。

iii. 在顶部导航栏选择您想创建单账号跟踪的地域。

> **说明** 该地域将成为单账号跟踪的Home地域。

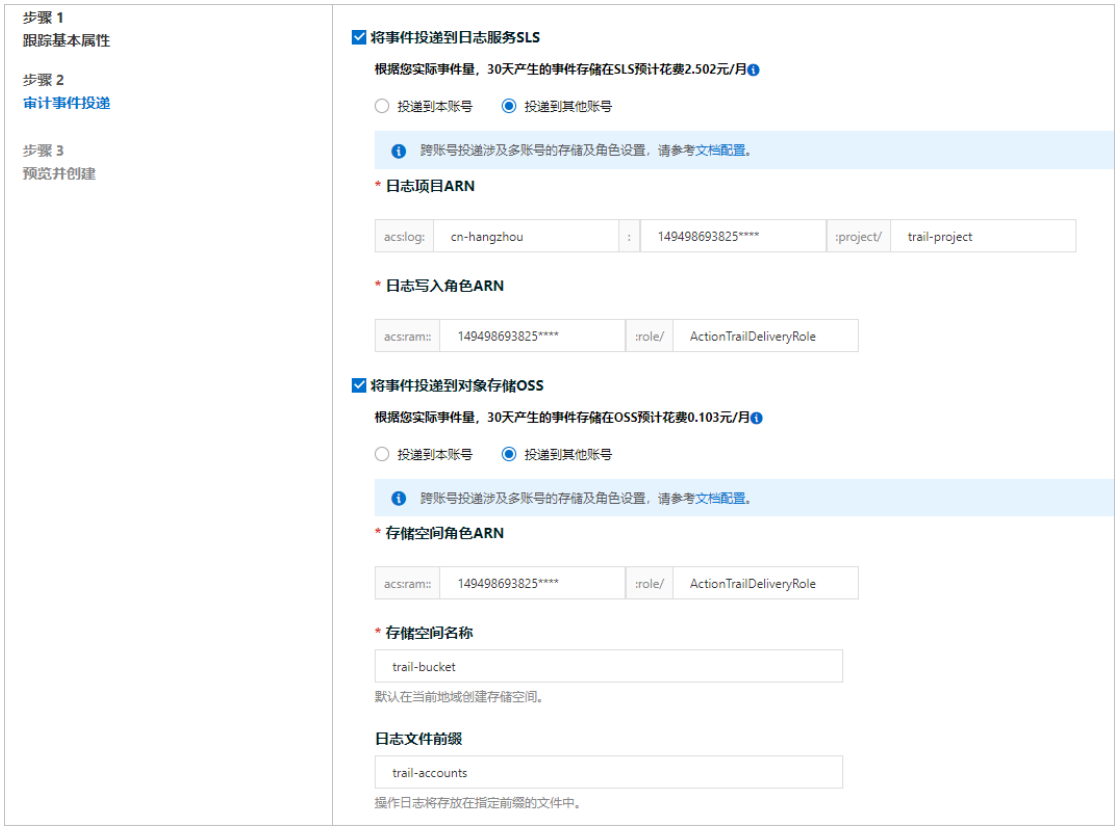
iv. 在**跟踪列表**页面，单击**创建跟踪**。

v. 在**跟踪基本属性**页面，设置**跟踪名称**、管控事件的**事件类型**和**Insight事件**，然后单击**下一步**。

> **说明**
>
> - 系统默认将跟踪投递的地域设置为全部地域。推荐您将**事件类型**设置为**所有事件**，以便跟踪全部地域的全部事件。
> - 关于参数的更多信息，请参见创建单账号跟踪。

vi. 在**审计事件投递**页面，选择投递方式，单击**下一步**。

您可以将跟踪分别投递到日志服务SLS或对象存储OSS，或者同时进行投递。关于如何选择存储服务，请参见将事件持续投递到指定服务。



- 选择**将事件投递到日志服务SLS**，然后选择**投递到其他账号**，并设置以下参数。

参数	描述
日志项目ARN	输入日志项目所在地域、阿里云账号C（目标账号）ID和日志项目名称。 其中，日志项目名称为步骤2中创建的Project名称。
日志写入角色ARN	输入阿里云账号C（目标账号）ID和角色名称。 其中，角色名称为步骤1中创建的RAM角色名称（本文示例为ActionTrailDeliveryRole）。

- 选择**将事件投递到对象存储OSS**时，然后选择**投递到其他账号**，并设置以下参数。

参数	描述
存储空间角色ARN	输入阿里云账号C（目标账号）ID和角色名称。 其中，角色名称为步骤1中创建的RAM角色名称（本文示例为ActionTrailDeliveryRole）。
存储空间名称	输入步骤2中创建的存储空间名称。
日志文件前缀	输入事件存放的日志文件前缀。

vii. 在**预览并创建**页面，确认跟踪信息，单击**提交**。

4. 以相同的方法，使用阿里云账号B创建单账号跟踪，设置投递目标为步骤2创建的Project或存储空间。

执行结果

跟踪创建成功后，您可以使用阿里云账号C查看SLS Project或OSS存储空间中来自阿里云账号A和阿里云账号B的事件。

相关操作

如果您需要在不同账号中进行数据迁移，请参见以下操作：

- OSS的数据在线迁移
- SLS的数据在线迁移

9.历史事件投递任务

9.1. 创建历史事件投递任务

当您需要分析最近90天的历史事件，或者因审计要求需要下载最近90天的历史事件时，您可以创建历史事件投递任务，将历史事件投递到日志服务SLS。

前提条件

- 通过提交工单或向销售经理申请白名单，获取历史事件投递任务功能的使用权限。
- 请确保您已经在当前地域创建了跟踪。具体操作，请参见创建单账号跟踪和创建多账号跟踪。

使用限制

- 目前只支持将历史事件投递到日志服务SLS。
- 一个阿里云账号同时只能存在一个正在运行的历史事件投递任务。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**历史事件投递任务**。
3. 在顶部导航栏选择您需要投递历史事件的地域。

   > **说明** 该地域必须与跟踪所在地域相同。

4. 在**历史事件投递任务**页面，单击**创建任务**。
5. 在**创建任务**页面，选择跟踪。

   > **说明** 选择跟踪后，系统将自动填入跟踪的地域、日志项目地域、日志项目名称和日志库信息。

6. 单击**确定**。

   创建任务后，您可以在**历史事件投递任务**页面查看关联跟踪、可补历史事件范围、投递状态、任务创建时间、任务完成时间等信息。

   > **说明**
   > - 补投递的历史事件与关联跟踪的地域和事件类型保持一致。例如：您创建跟踪A时将跟踪的地域设置为华东1（杭州）、事件类型设置为写事件，历史事件投递任务将通过跟踪A向您指定的存储空间，补投递最近90天在华东1（杭州）地域的写事件。
   > - 补投递的历史事件时间范围的开始时间为当前时间往前90天，结束时间为关联跟踪生效后5分钟。例如：您创建历史事件投递任务时关联跟踪A已经创建了40天，历史事件投递任务将投递跟踪A创建时间往前50天的历史事件。

10.AccessKey审计

10.1. AccessKey审计概览

AccessKey审计用于查询AccessKey的基本信息、访问的云服务及相关IP地址和资源，帮助您追溯AccessKey使用信息，以便快速应对AccessKey泄露等异常事件，或者为轮换AccessKey提供决策参考。

应用场景

企业在云上使用AccessKey的过程中，可能遇到AccessKey异常告警、AccessKey泄露等情况。此时可以使用操作审计AccessKey审计功能查询AccessKey日志，为后续操作提供参考。AccessKey审计的典型场景如下：

- **追溯AccessKey异常信息**
  当AccessKey使用异常时，需要查询AccessKey的使用记录，评估AccessKey的使用情况是否健康，是否存在预期外的访问。例如：企业A在云安全中心收到AccessKey异常告警，需要查询该AccessKey近一段时间的使用记录，定位具体的异常问题。
- **判断AccessKey是否存在泄露**
  当AccessKey疑似泄露时，需要获取一定时间范围内AccessKey的使用日志判断AccessKey是否泄露，并为AccessKey轮转提供决策参考。例如：企业A发现AccessKey被写在开源文档中，担心AccessKey有泄露的隐患，需要查询AccessKey日志以判断AccessKey是否存在泄露。

使用说明

AccessKey审计将提供自2022年02月01日起，最长400天内使用指定AccessKey访问云服务的概要信息。

支持的云服务及事件

关于AccessKey审计支持的云服务及事件，请参见AccessKey审计支持的云服务及事件。

10.2. 查询AccessKey日志

您可以按需查询AccessKey的基本信息、访问的云服务及相关IP地址和资源。

前提条件

请提前获取待查询的AccessKey ID。具体操作，请参见获取AccessKey。

操作步骤

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**AccessKey审计**。
3. 在**AccessKey审计**页面，输入AccessKey ID，然后单击 图标。
4. 在**基本信息**区域，查询**AccessKey ID**、**账号ID**、**用户名**、**最后使用时间**和**最后使用服务**。
5. 在**访问的云服务**区域，查询AccessKey访问的云服务列表、事件列表、IP列表和资源列表。
   - 云服务列表
     在**访问的云服务**区域，查询**云服务**和**云服务最后使用时间**。
   - 事件列表
     单击目标云服务**操作**列的**事件列表**，查询**事件名称**、**最后使用时间**、**最后使用地域**和事件详情。

> **说明**
>
> - 关于事件中字段的更多信息，请参见管控事件结构定义。
> - 当您启用事件高级查询后，可以单击**查看更多记录**，查询更多事件信息。关于如何启用事件高级查询，请参见启用事件高级查询。

- IP列表
  单击目标云服务**操作**列的**IP列表**，查询**IP**、**最后使用时间**、**最后使用地域**和IP地址详情。
- 资源列表
  单击目标云服务**操作**列的**资源列表**，查询**资源类型**、**资源名称**、**最后使用时间**、**最后使用地域**和资源详情。
  关于AccessKey审计支持的资源类型，请参见资源类型。

10.3. AccessKey审计支持的云服务及事件

本文介绍AccessKey审计支持的云服务及事件。

AccessKey审计支持的云服务

AccessKey审计支持可以使用AccessKey访问的所有云服务。

AccessKey审计支持的事件

AccessKey审计当前支持的事件与操作审计支持的事件相同，后续将持续增加新的事件。操作审计支持的事件列表，请参见操作审计支持的事件。

11.API参考

11.1. API概览

请根据使用场景选择对应的API。

场景	描述	API版本选择	API区别
跟踪管理	管理用户跟踪	• 2020-07-06（推荐） • 2017-12-04	• 2020-07-06版本API支持跨账号投递操作事件。 • 2017-12-04版本API不支持跨账号投递操作事件。
历史事件查询	查询最近90天历史事件	• 2020-07-06（推荐） • 2017-12-04	• 2020-07-06版本API查询延时低，支持查询最近90天、时间跨度为90天的事件，支持使用单个条件筛选事件。 • 2017-12-04版本API查询延时高，支持查询最近90天、时间跨度为30天的事件，支持8个条件组合筛选事件。
历史事件投递任务管理	管理用户历史事件投递任务	2020-07-06	无

11.2. 附录

11.2.1. 通过VPC调用API

如果专有网络（VPC）内的ECS实例没有设置公网IP，则您无法通过公网调用API，但您可以通过VPC调用API。

接入地址

您可以使用下表所示的接入地址，通过VPC调用API。调用时只能操作同地域资源，不支持跨地域操作。

阿里云地域	地域ID	接入地址（Endpoint）
华东 1（杭州）	cn-hangzhou	actiontrail-vpc.cn-hangzhou.aliyuncs.com
华东 2（上海）	cn-shanghai	actiontrail-vpc.cn-shanghai.aliyuncs.com
华北 1（青岛）	cn-qingdao	actiontrail-vpc.cn-qingdao.aliyuncs.com
华北 2（北京）	cn-beijing	actiontrail-vpc.cn-beijing.aliyuncs.com

阿里云地域	地域ID	接入地址（Endpoint）
华北 3（张家口）	cn-zhangjiakou	actiontrail-vpc.cn-zhangjiakou.aliyuncs.com
华北 5（呼和浩特）	cn-huhehaote	actiontrail-vpc.cn-huhehaote.aliyuncs.com
华南 1（深圳）	cn-shenzhen	actiontrail-vpc.cn-shenzhen.aliyuncs.com
华南 2（河源）	cn-heyuan	actiontrail-vpc.cn-heyuan.aliyuncs.com
华南 3（广州）	cn-guangzhou	actiontrail-vpc.cn-guangzhou.aliyuncs.com
西南 1（成都）	cn-chengdu	actiontrail-vpc.cn-chengdu.aliyuncs.com
中国（香港）	cn-hongkong	actiontrail-vpc.cn-hongkong.aliyuncs.com
新加坡	ap-southeast-1	actiontrail-vpc.ap-southeast-1.aliyuncs.com
澳大利亚（悉尼）	ap-southeast-2	actiontrail-vpc.ap-southeast-2.aliyuncs.com
马来西亚（吉隆坡）	ap-southeast-3	actiontrail-vpc.ap-southeast-3.aliyuncs.com
印度尼西亚（雅加达）	ap-southeast-5	actiontrail-vpc.ap-southeast-5.aliyuncs.com
日本（东京）	ap-northeast-1	actiontrail-vpc.ap-northeast-1.aliyuncs.com
德国（法兰克福）	eu-central-1	actiontrail-vpc.eu-central-1.aliyuncs.com
英国（伦敦）	eu-west-1	actiontrail-vpc.eu-west-1.aliyuncs.com
美国（硅谷）	us-west-1	actiontrail-vpc.us-west-1.aliyuncs.com
美国（弗吉尼亚）	us-east-1	actiontrail-vpc.us-east-1.aliyuncs.com
印度（孟买）	ap-south-1	actiontrail-vpc.ap-south-1.aliyuncs.com

阿里云地域	地域ID	接入地址（Endpoint）
阿联酋（迪拜）	me-east-1	actiontrail-vpc.me-east-1.aliyuncs.com

方式一（推荐）：通过SDK调用API

Java SDK核心库在4.5.3版本以后，支持通过VPC调用API。Java代码示例如下：

```
DefaultProfile profile = DefaultProfile.getProfile("<RegionId>", "<AccessKeyId>", "<AccessKeySecret>");
IAcsClient client = new DefaultAcsClient(profile);
// 全局生效配置。其中，<product>为产品名称，操作审计取值为Actiontrail。
DefaultProfile.addEndpoint("<RegionId>", "<product>", "<Endpoint>");
// 只对当前请求生效配置。例如：调用DescribeRegions接口。
DescribeRegionsRequest regionsRequest = new DescribeRegionsRequest();
// 如设置下述productNetwork参数，则无需手动设置SysEndpoint。
regionsRequest.setSysEndpoint("<Endpoint>");
// 设置网络。productNetwork参数取值：vpc、 public。
// vpc为内网调用接入地址选项；public为公网调用API的选项，即默认选项。
regionsRequest.productNetwork = "vpc";
DescribeRegionsResponse regionsResponse = client.getAcsResponse(regionsRequest);
```

方式二：通过阿里云CLI调用API

以DescribeRegions接口为例，调用命令示例如下：

```
aliyun actiontrail DescribeRegions --endpoint actiontrail-vpc.cn-hangzhou.aliyuncs.com
```

12.SDK参考

12.1. SDK概览

操作审计支持Java、Python、C++、PHP、.NET和Go语言。
下表列举了各语言SDK的下载地址和说明文档。更多关于SDK的信息，请访问阿里云开发平台。

Alibaba Cloud SDK	操作审计SDK	说明文档
Alibaba Cloud SDK for Java	Alibaba Cloud Actiontrail SDK for Java	开始使用
Alibaba Cloud SDK for Python	Alibaba Cloud Actiontrail SDK for Python	开始使用
Alibaba Cloud SDK for C++	Alibaba Cloud Actiontrail SDK for C++	无
Alibaba Cloud SDK for PHP	Alibaba Cloud Actiontrail SDK for PHP	开始使用
Alibaba Cloud SDK for .NET	Alibaba Cloud Actiontrail SDK for .NET	开始使用
Alibaba Cloud SDK for Go	Alibaba Cloud Actiontrail SDK for Go	开始使用

12.2. Java SDK示例

本文以Java语言为例，为您介绍如何使用操作审计SDK。

准备工作

在项目目录下的pom.xml文件中，添加Alibaba Cloud SDK（aliyun-java-sdk-core）和操作审计SDK（aliyun-java-sdk-actiontrail）的依赖。

```
<dependencies>
    <dependency>
        <groupId>com.aliyun</groupId>
        <artifactId>aliyun-java-sdk-core</artifactId>
        <version>4.5.20</version>
    </dependency>
    <dependency>
        <groupId>com.aliyun</groupId>
        <artifactId>aliyun-java-sdk-actiontrail</artifactId>
        <version>1.0.6</version>
    </dependency>
</dependencies>
```

说明 关于SDK版本的更多信息，请参见SDK概览。

示例1：查询事件

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.actiontrail.model.v20200706.LookupEventsRequest;
import com.aliyuncs.actiontrail.model.v20200706.LookupEventsResponse;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.profile.DefaultProfile;
import java.util.ArrayList;
import java.util.List;
import java.util.Map;
public class DemoLookupEvents {
    public static void main(String[] args) {
        //创建并初始化DefaultAcsClient实例。
        DefaultProfile profile = DefaultProfile.getProfile(
            "<your-region-id>",           //地域ID。
            "<your-access-key-id>",       //RAM用户的AccessKey ID。
            "<your-access-key-secret>"); //RAM用户的AccessKey Secret。
        IAcsClient client = new DefaultAcsClient(profile);
        //创建LookupEvents请求。
        LookupEventsRequest request = new LookupEventsRequest();
        //设置参数。
        List<LookupEventsRequest.LookupAttribute> lookupAttributes = new ArrayList<>();
        LookupEventsRequest.LookupAttribute lookupAttribute = new LookupEventsRequest.Looku
pAttribute();
        lookupAttribute.setKey("EventRW");
        lookupAttribute.setValue("Write");
        lookupAttributes.add(lookupAttribute);
        request.setLookupAttributes(lookupAttributes);
        //发起请求并处理响应或异常。
        LookupEventsResponse response;
        try {
            response = client.getAcsResponse(request);
            System.out.println("RequestId: " + response.getRequestId());
            System.out.println("--------------------------------");
            System.out.println("eventTime, eventId, serviceName, eventName");
            for (Map<Object, Object> event : response.getEvents()) {
                System.out.println(event.get("eventTime") + ", " + event.get("eventId") + "
, " + event.get("serviceName") + ", " + event.get("eventName"));
            }
        } catch (ClientException e) {
            e.printStackTrace();
        }
    }
}
```

示例2：查询跟踪列表

```
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.actiontrail.model.v20171204.DescribeTrailsRequest;
import com.aliyuncs.actiontrail.model.v20171204.DescribeTrailsResponse;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.profile.DefaultProfile;
public class DemoDescribeTrails {
    public static void main(String[] args) {
        //创建并初始化DefaultAcsClient实例。
        DefaultProfile profile = DefaultProfile.getProfile(
            "<your-region-id>",           //地域ID。
            "<your-access-key-id>",       //RAM用户的AccessKey ID。
            "<your-access-key-secret>"); //RAM用户的AccessKey Secret。
        IAcsClient client = new DefaultAcsClient(profile);
        //创建DescribeTrails请求并设置参数。
        DescribeTrailsRequest request = new DescribeTrailsRequest();
        //发起请求并处理响应或异常。
        DescribeTrailsResponse response;
        try {
            response = client.getAcsResponse(request);
            System.out.println("RequestId: " + response.getRequestId());
            System.out.println("-------------------------------");
            System.out.println("name, trailRegion");
            for (DescribeTrailsResponse.TrailListItem trail : response.getTrailList()) {
                System.out.println(trail.getName() + ", " + trail.getTrailRegion());
            }
        } catch (ClientException e) {
            e.printStackTrace();
        }
    }
}
```

13.教程

13.1. 通过RAM对操作审计进行权限管理

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

背景信息

- 使用RAM对操作审计进行权限管理前，请先了解以下系统策略：
  - AliyunActionTrailFullAccess：管理操作审计的权限。
  - AliyunActionTrailReadOnlyAccess：只读访问操作审计的权限。

  当系统策略不能满足您的需求时，您可以创建自定义策略。
- 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。更多信息，请参见RAM鉴权。

操作步骤

1. 创建RAM用户。

   具体操作，请参见创建RAM用户。
2. 创建自定义策略。

   更多信息，请参见创建自定义权限策略和权限策略示例。
3. 为RAM用户授权。

   具体操作，请参见为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"
            }
        }
    }]
}
```

13.2. 使用操作审计监控AccessKey的使用

AccessKey包括AccessKey ID和AccessKey Secret，用于标识用户和验证用户的密钥。AccessKey泄露会威胁您资源的安全。操作审计帮助您监控AccessKey相关事件，以便您发现AccessKey使用异常时快速应对。

前提条件

请确保您已开通日志服务SLS。

当您首次使用日志服务SLS时，需要登录日志服务控制台，根据页面提示开通日志服务SLS。

背景信息

您可以使用操作审计直接查询AccessKey相关事件，也可以将事件投递到日志服务并对AccessKey相关事件设置告警。

- 查询最近90天AccessKey相关事件：在操作审计控制台事件查询页面，将筛选条件设置为**AccessKeyId**，查询最近90天查询最近90天AccessKey相关事件。具体操作，请参见通过操作审计控制台查询事件。
- 查询90天以上AccessKey相关事件：按照本文的操作步骤进行设置，查询90天以上AccessKey相关事件并设置告警。

步骤一：创建跟踪

以创建单账号跟踪为例，为您介绍如何创建跟踪并将事件投递到日志服务SLS。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在顶部导航栏选择您想创建单账号跟踪的地域。

   > **说明** 该地域将成为单账号跟踪的Home地域，即创建跟踪的地域。

4. 在**跟踪列表**页面，单击**创建跟踪**。
5. 在**跟踪基本属性**页面，设置如下参数，然后单击**下一步**。

参数	说明
跟踪名称	跟踪的名称。同一阿里云账号中跟踪名称不能重复。

参数	说明
日志事件	将管控事件的**事件类型**设置为**所有事件**。

6. 在**审计事件投递**页面，选择**将事件投递到日志服务SLS**，然后选择**投递到本账号**。
7. 选择**创建新的日志项目**，选择**日志库所属地域**，然后设置**日志项目名称**。
8. 单击**下一步**。
9. 在**预览并创建**页面，确认跟踪信息，然后单击**提交**。

步骤二：在日志服务SLS中查询事件并设置告警

1. 在操作审计控制台，单击**跟踪列表**。
2. 将鼠标悬浮到目标跟踪**存储服务**列的

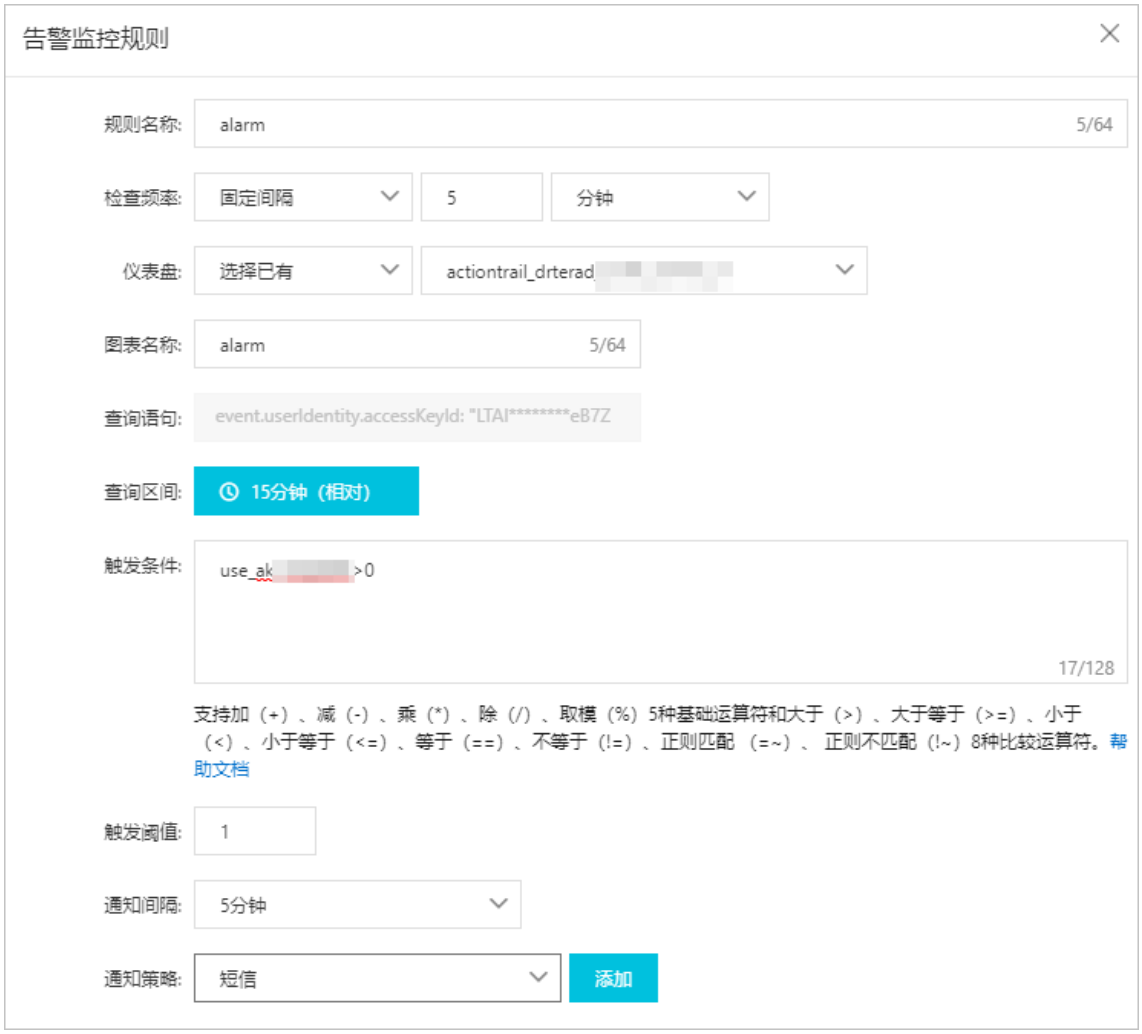
   图标，然后单击SLS日志库名称。
3. 在页面右上角，单击**15分钟（相对）**，设置查询的时间范围。
4. 在搜索框中输入查询语句：`event.userIdentity.accessKeyId: "<YourAccessKeyId>" | select count(1) as use_ak_<YourAccessKeyId>`，然后单击**查询/分析**。

   > **说明** `<YourAccessKeyId>` 请替换为您自己的AccessKey ID。

5. 将事件**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** 将事件另存为快速查询后，您可以在日志服务控制台直接选择该快速查询。

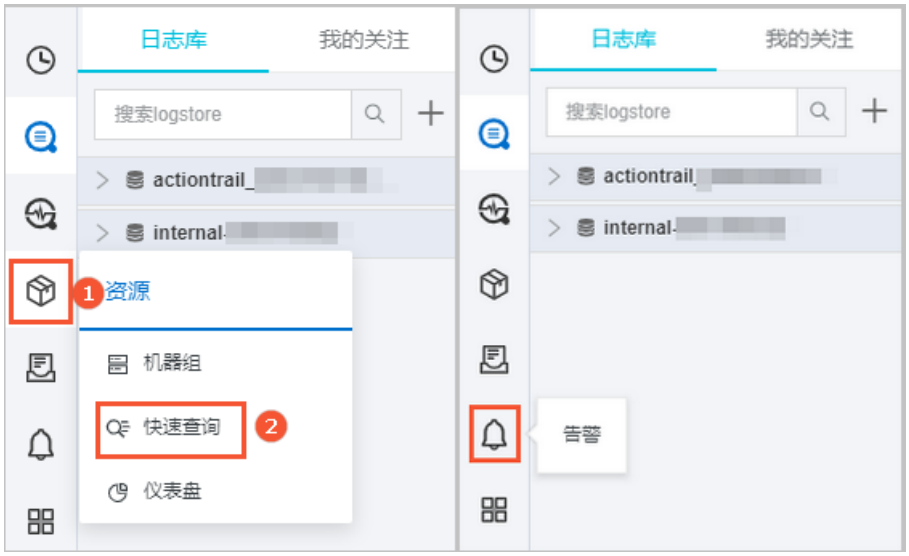
     更多信息，请参见快速查询。
   - **另存为告警**：在页面右上角选择**另存为告警 > 旧版告警**，在**告警监控规则**面板配置相关参数，然后单击**确定**。
     更多信息，请参见设置告警。



说明 将事件另存为告警后，满足触发条件即可收到告警通知，例如：按照上图进行告警配置后，如果 `accessKeyId` 在5分钟内被使用过，则上报告警。

执行结果

创建的快速查询和告警均可在日志服务控制台进行管理。



13.3. 使用操作审计监控阿里云账号的使用

阿里云账号是阿里云资源归属、资源使用计量计费的基本主体。阿里云账号泄露会威胁您所有资源的安全。您可以使用操作审计创建跟踪，将事件投递到日志服务SLS，从而实现对阿里云账号的监控和告警。

前提条件

请确保您已开通日志服务SLS。

当您首次使用日志服务SLS时，需要登录日志服务控制台，根据页面提示开通日志服务SLS。

步骤一：创建跟踪

以创建单账号跟踪为例，为您介绍如何创建跟踪并将事件投递到日志服务SLS。

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在顶部导航栏选择您想创建单账号跟踪的地域。

   > **说明** 该地域将成为单账号跟踪的Home地域，即创建跟踪的地域。

4. 在**跟踪列表**页面，单击**创建跟踪**。
5. 在**跟踪基本属性**页面，设置如下参数，然后单击**下一步**。

参数	说明
跟踪名称	跟踪的名称。同一阿里云账号中跟踪名称不能重复。
日志事件	将管控事件的**事件类型**设置为**所有事件**。

6. 在**审计事件投递**页面，选择**将事件投递到日志服务SLS**，然后选择**投递到本账号**。
7. 选择**创建新的日志项目**，选择**日志库所属地域**，然后设置**日志项目名称**。
8. 单击**下一步**。
9. 在**预览并创建**页面，确认跟踪信息，然后单击**提交**。

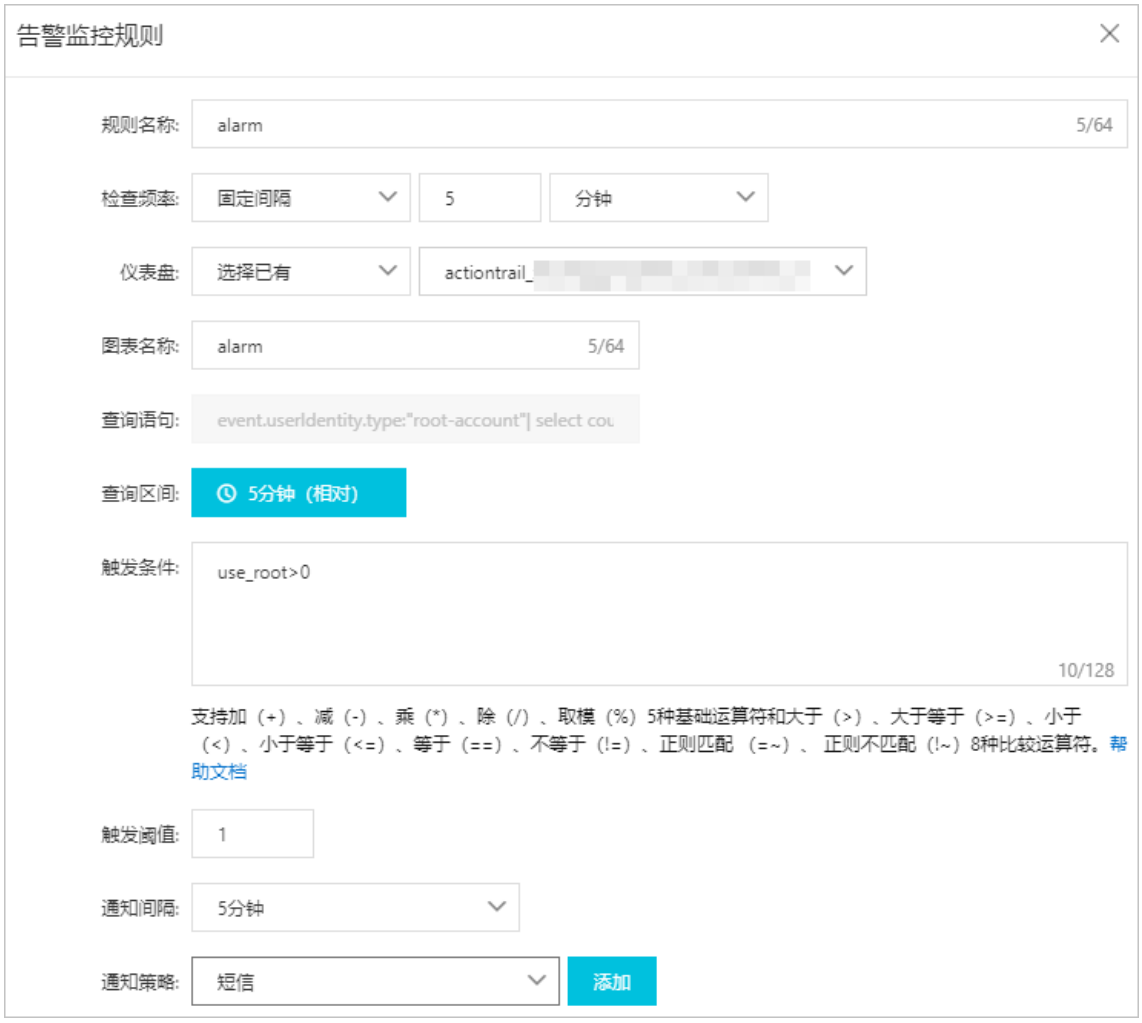
步骤二：在日志服务SLS中查询事件并设置告警

1. 在操作审计控制台，单击**跟踪列表**。
2. 将鼠标悬浮到目标跟踪**存储服务**列的

   图标，然后单击SLS日志库名称。
3. 在页面右上角，单击**15分钟（相对）**，设置查询的时间范围。
4. 在搜索框中输入查询语句：`event.userIdentity.type:"root-account"| select count(1) as use_root`，然后单击**查询/分析**。
5. 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** 将事件另存为快速查询后，您可以在日志服务控制台直接选择该快速查询。

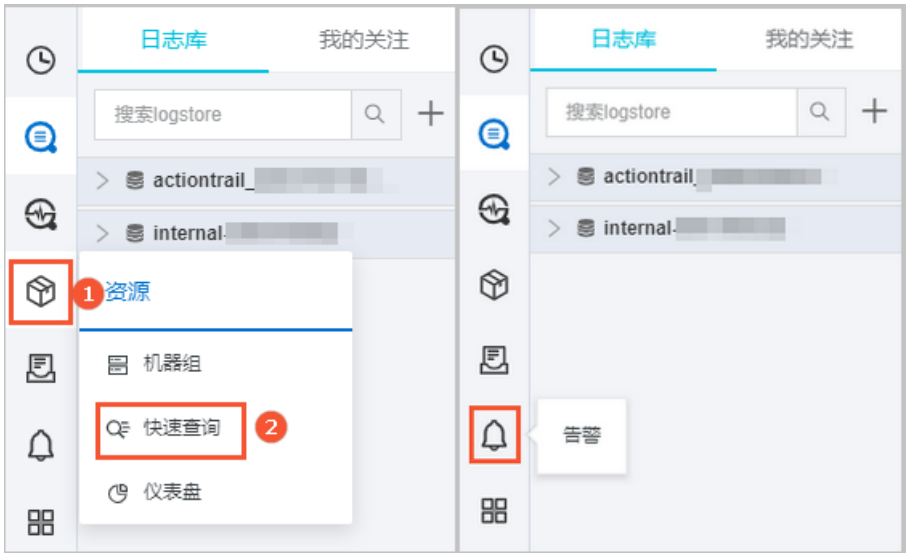
     快速查询详情，请参见快速查询。
   - **另存为告警**：在页面右上角选择**另存为告警 > 旧版告警**，在**告警监控规则**面板配置相关参数，然后单击**确定**。
     告警配置详情，请参见设置告警。



> **说明** 将事件另存为告警后，当满足触发条件即可收到告警通知。按照上图进行告警配置后，如果阿里云账号在5分钟内被使用过，则上报告警。

执行结果

创建的快速查询和告警均可在日志服务控制台进行管理。



13.4. 使用DLA分析OSS中的事件

通过操作审计创建跟踪，可以持续将事件投递到指定的OSS存储空间中。您可以使用数据湖分析DLA（Data Lake Analytics）可视化地查询和分析OSS存储空间中的事件。

前提条件

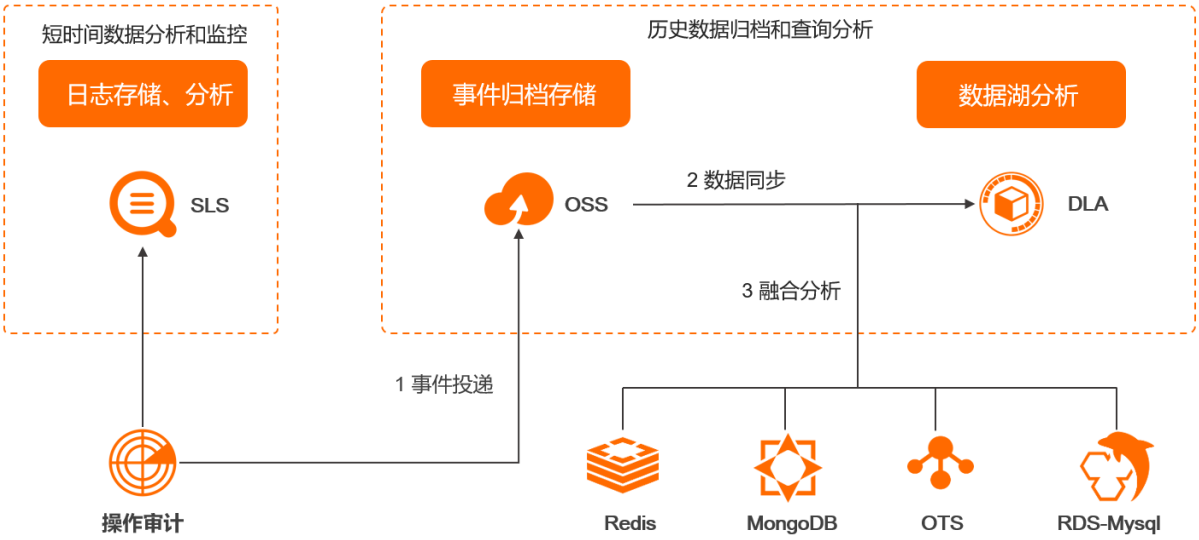
- 请确保您已经在操作审计创建了跟踪，并将事件投递到OSS存储空间中。具体操作，请参见创建单账号跟踪和创建多账号跟踪。
- 请确保您已经开通了DLA服务。具体操作，请参见开通数据湖分析服务。

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。更多信息，请参见什么是云原生数据湖分析。

使用DLA分析OSS中事件的原理如下：

1. 通过操作审计创建跟踪，将事件持续投递到OSS存储空间。
2. 将事件从OSS存储空间导入DLA。
3. DLA将OSS存储空间内以Array形式保存的多条日志记录拆分为多条数据，以JSON保存的每条事件转换为结构化的数据表，使得面向OSS存储空间的数据解析被大大简化，直接实现可视化的标准SQL分析。



说明 DLA不支持分析SLS中的事件，您可以使用SLS分析功能分析事件。

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，选择**数据湖管理 > 数据入湖**。
   iv. 在**数据入湖**页面，单击**更多**，然后单击**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中的事件的存储目录。 ■ **自动发现**：DLA自动设置操作审计投递到OSS中的事件的存储目录。
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存储空间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. 选择**数据湖管理 > 元数据管理**，然后单击目标Schema名**操作**列的**库表详情**。
   iii. 在**元数据管理**页面，单击**表**页签查看同步情况。

   关于Schema表结构的更多信息，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 Presto > 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**。

查询案例

查询指定AccessKey的事件

- 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产生的事件。

查询指定AccessKey访问ECS的事件

- 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产生的事件。

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。操作审计为每个事件所产生的一个GUID。
event_name	String	是	CreateNetworkInterface	事件名称。 • 如果event_type的取值是*ApiCall*，该字段为API的名称。 • 如果event_type的取值不是*ApiCall*，该字段为简单的英文短句，表示事件含义。
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）。

名称	类型	是否必选	示例	描述
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	11.32.XX.XX	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。
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)*。

名称	类型	是否必选	示例	描述
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user_identity_type的取值是*root-account*，则记录阿里云账号ID。 • 如果user_identity_type的取值是*ram-user*，则记录RAM用户ID。 • 如果user_identity_type的取值是*assumed-role*，则记录RoleID:RoleSessionName。
user_identity_account_id	String	是	112233445566****	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	Alice	如果user_identity_type的取值是*ram-user*，则记录RAM用户名。如果user_identity_type的取值是*assumed-role*，则记录RoleName:RoleSessionName。

13.5. 将事件持续投递到指定服务

操作审计默认为每个阿里云账号记录最近90天的事件。但在日常工作中，企业可能需要保留180天及以上的事件，也可能需要对已有的90天事件进行分析。此时需要将这些事件转存到数据分析服务，或持续采集云上的事件并保存到指定存储服务。这需要依赖操作审计的跟踪功能实现。本文以创建单账号跟踪为例，为您介绍不同场景下通过跟踪投递事件的方法。

前提条件

- 请确保您已开通对象存储OSS。具体操作，请参见开通OSS服务。
- 请确保您已开通日志服务SLS。
  当您首次使用日志服务SLS时，需要登录日志服务控制台，根据页面提示开通日志服务SLS。

使用场景

使用操作审计创建跟踪并投递事件，可以满足您不同场景需求。如果不创建跟踪，您将无法追溯90天以前的事件。具体场景如下：

- 场景一：将事件保存180天及以上

操作审计默认记录最近90天的事件，为了满足等保2.0（网络安全等级保护2.0制度）将事件保存180天及以上的要求，您可以创建跟踪持续采集事件并投递到对象存储OSS或日志服务SLS。默认情况下，投递到OSS或SLS的事件会永久保存。如果您需要将事件设置为仅保留180天，请参见OSS修改事件存储时长或SLS修改事件存储时长。

- 场景二：对敏感操作进行分析和告警
  当您需要及时感知敏感操作（例如：产生订单、删除资源等）的发生时，您可以创建跟踪将事件投递到日志服务SLS，并在SLS对需要关注的敏感操作设置告警。
- 场景三：通过MaxCompute分析事件
  当您需要分析事件，而日志服务SLS的分析能力又不能满足您的需求时，您可以使用分析能力更强大的大数据计算服务（MaxCompute）。MaxCompute为您提供多种经典的分布式计算模型，帮助您轻松完成大数据分析。推荐您创建跟踪，将事件投递到日志服务SLS，再通过SLS将数据导出到MaxCompute进行分析。
- 场景四：低成本分析和永久存储事件
  当您需要同时对事件进行实时分析和永久存储时，需充分了解对象存储OSS、日志服务SLS和大数据计算服务（MaxCompute）的功能特性及收费。三者收费情况为：SLS > MaxCompute > OSS，因此推荐您先将事件投递到日志服务SLS进行分析，手动修改事件在SLS的存储时长（存储时长应该更好地满足实时分析的时间跨度要求），然后定时将SLS中的数据导入到MaxCompute或OSS进行永久存储。

场景一：将事件保存180天及以上

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在顶部导航栏选择您想创建跟踪的地域。
4. 在**跟踪列表**页面，单击**创建跟踪**。
5. 在**跟踪基本属性**页面，设置如下参数，单击**下一步**。

参数	说明
跟踪名称	跟踪的名称。同一阿里云账号中跟踪名称不能重复。
日志事件	将管控事件的**事件类型**设置为**所有事件**。

6. 在**审计事件投递**页面，选择投递方式，单击**下一步**。
   - 选择**将事件投递到日志服务SLS**，然后选择**投递到本账号**。
     - **创建新的日志项目**：选择**日志库所属地域**，设置**日志项目名称**。
     - **选择已有的日志项目**：选择**日志库所属地域**和**日志项目名称**。
   - 选择**将事件投递到对象存储OSS**，然后选择**投递到本账号**。
     - **创建新的存储空间**：设置**存储空间名称**、**日志文件前缀**、服务端加密情况。
     - **选择已有的存储空间**：选择**存储空间名称**，设置**日志文件前缀**。
7. 在**预览并创建**页面，确认跟踪信息，单击**提交**。
8. 单击**查看跟踪详情**，然后执行以下操作进入存储服务的控制台查看事件。
   - 对象存储OSS：单击存储空间名称进入OSS管理控制台查看事件。
   - 日志服务SLS：单击日志项目名称或日志库名称，进入日志服务控制台查看事件。

场景二：对敏感操作进行分析和告警

1. 登录操作审计控制台

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在顶部导航栏选择您想创建跟踪的地域。
4. 在**跟踪列表**页面，单击**创建跟踪**。
5. 在**跟踪基本属性**页面，设置如下参数，单击**下一步**。

参数	说明
跟踪名称	跟踪的名称。同一阿里云账号中跟踪名称不能重复。
日志事件	将管控事件的**事件类型**设置为**写事件**。 **说明** 敏感操作多为**写事件**，将**事件类型**设置为**写事件**可以减少审计事件数据量，从而节省成本。

6. 在**审计事件投递**页面，选择**将事件投递到日志服务SLS**，然后选择**投递到本账号**，设置相关参数，单击**下一步**。
   - **创建新的日志项目**：选择**日志库所属地域**，设置**日志项目名称**。
   - **选择已有的日志项目**：选择**日志库所属地域**和**日志项目名称**。
7. 在**预览并创建**页面，确认跟踪信息，单击**提交**。
8. 单击**查看跟踪详情**，然后单击日志项目名称或日志库名称，进入日志服务控制台查看事件分析情况。
9. 在日志服务控制台设置告警。

   具体操作，请参见设置告警。

场景三：通过MaxCompute分析事件

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在顶部导航栏选择您想创建跟踪的地域。
4. 在**跟踪列表**页面，单击**创建跟踪**。
5. 在**跟踪基本属性**页面，设置如下参数，单击**下一步**。

参数	说明
跟踪名称	跟踪的名称。同一阿里云账号中跟踪名称不能重复。
日志事件	将管控事件的**事件类型**设置为**所有事件**。

6. 在**审计事件投递**页面，选择**将事件投递到日志服务SLS**，然后选择**投递到本账号**，设置相关参数，单击**下一步**。
   - **创建新的日志项目**：选择**日志库所属地域**，设置**日志项目名称**。
   - **选择已有的日志项目**：选择**日志库所属地域**和**日志项目名称**。
7. 在**预览并创建**页面，确认跟踪信息，单击**提交**。
8. 单击**查看跟踪详情**，然后单击日志项目名称或日志库名称，进入日志服务控制台查看事件分析情况。
9. 在日志服务控制台将事件投递到MaxCompute。

具体操作，请参见投递日志到MaxCompute（旧版）。

> **说明** 事件投递到MaxCompute后，您可以根据需求对事件进行分析。

场景四：低成本分析和永久存储事件

使用操作审计创建跟踪时，如果选择了**创建新的日志项目**，则默认创建以 `actiontrail_<trail_name>` 开头的Logstore，永久保存事件。为了节省成本，推荐您手动修改SLS事件存储时长（例如：180天），再定时将SLS中的数据导入到MaxCompute或OSS进行永久存储。

1. 在操作审计控制台创建跟踪并将事件投递到日志服务SLS。

   关于如何创建跟踪，请参见创建单账号跟踪。

2. 在日志服务控制台修改日志存储时长。
   i. 登录日志服务控制台。
   ii. 在**Project列表**区域，单击事件对应的**Project名称**。
   iii. 单击日志左侧

   >

   图标，然后单击

   图标。
   iv. 在**Logstore属性**页面，关闭**永久保存**开关。
   v. 设置**数据保存时间**，然后单击页面右上角**保存**。
3. 在日志服务控制台将事件投递到MaxCompute或OSS。

   具体操作，请参见：
   - 投递日志到MaxCompute（旧版）
   - 将日志服务数据投递到OSS

13.6. 在日志服务SLS中分析操作事件

操作审计（ActionTrail）帮助您监控阿里云账号的活动并记录最近90天的操作事件。当您需要分析更长时间的操作事件时，可以通过操作审计创建跟踪，将操作事件投递到日志服务SLS，对操作事件进行查询和分析。本文为您介绍在SLS中查询和分析操作事件的典型场景。

前提条件

请确保您已创建跟踪，并将操作事件投递到日志服务SLS。具体操作，请参见创建单账号跟踪和创建多账号跟踪。

场景一：分析AK泄漏情况

某企业发现IP地址存在异常调用，怀疑是由于人事调动导致AK（AccessKey）泄漏。此时可以通过操作审计创建跟踪，将操作事件投递到日志服务SLS，在SLS中分析AK调用轨迹。

您可以获取AK调用来源IP地址所在的城市，一旦发现当前城市非企业所在地，即可明确AK存在泄漏。

1. 登录日志服务控制台。
2. 在**全部的Project**页签，单击操作事件对应的**Project名称**。
3. 单击日志库名称，然后单击**15分钟（相对）**，设置查询的时间范围。

4. 在搜索框中输入如下代码。

```
__topic__: actiontrail_audit_event and event.userIdentity.accessKeyId:<YourAccessKeyId> |
SELECT count(1) as pv, city FROM (SELECT "event.sourceIpAddress" AS ip, ip_to_city("event.
sourceIpAddress") as city FROM log) WHERE ip_to_domain(ip)!='intranet' GROUP BY city ORDER
BY pv DESC
```

> **说明**
> - `<YourAccessKeyId>` 请替换为您自己的AccessKey ID。
> - 以上查询能够获取指定AK所产生调用的来源IP地址，并且给出具体的调用量。如果当前城市非企业所在地，则AK存在泄漏。

5. 单击**查询/分析**，查看分析结果。
6. （可选）当AK泄露时，您可以调整RAM用户权限，解决AK泄漏问题。

   具体操作，请参见为RAM用户移除权限。

场景二：分析ECS实例删除情况

某企业期望可以追溯云资源的高危操作，例如：删除ECS实例。此时可以通过操作审计创建跟踪，将操作事件投递到日志服务SLS，获取执行ECS实例删除动作的操作者。

1. 登录日志服务控制台。
2. 在**全部的Project**页签，单击操作事件对应的**Project名称**。
3. 单击日志库名称，然后单击**15分钟（相对）**，设置查询的时间范围。
4. 在搜索框中输入如下代码。

```
__topic__: actiontrail_audit_event | SELECT serviceName, eventName, userName, count(1) as
pv FROM (SELECT "event.eventName" as eventName, "event.serviceName" as serviceName, "event
.userIdentity.userName" as userName FROM log) WHERE (serviceName = <TargetServiceName> and
eventName = <TargetEventName>) GROUP BY serviceName, eventName, userName
```

> **说明** 您可以将 `<TargetServiceName>` 和 `<TargetEventName>` 分别指定为ECS和DeleteInstances，获取执行ECS实例删除动作的操作者。

5. 单击**查询/分析**，查看分析结果。

   分析结果会统计执行ECS实例删除动作的操作者以及执行次数。定位到ECS实例的非法操作后，您可以根据如下代码获取非法的操作记录，以便进行问题修复。

```
__topic__: actiontrail_audit_event and event.serviceName:<TargetServiceName> and <TargetR
esourceId> and event.userIdentity.accessKeyId:<YourAccessKeyId>
```

场景三：生成数据报表

随着企业自身云上业务的快速发展，对于部分核心资源的调用频率周期需要生成完整的数据报表，以便进行资源容量的预估及风险预判。

例如：企业内部需要生成ECS实例创建近半年来的数据报表，通过分析同比以及环比增长情况来预测未来半年内资源扩充情况，以便合理的控制和规划成本开销。

1. 登录日志服务控制台。
2. 在**全部的Project**页签，单击操作事件对应的**Project名称**。
3. 单击日志库名称，然后单击**15分钟（相对）**，设置查询的时间范围。

4. 在搜索框中输入如下代码。

```
__topic__: actiontrail_audit_event and event.serviceName:<TargetServiceName> and event.eventName:<TargetEventName> | select t, diff[1] as current, diff[2] as last_month, diff[3] as percentage from(select t, compare( pv , 2592000) as diff from (select count(1) as pv, date_format(from_unixtime(__time__), '%m') as t from log group by t) group by t order by t)
```

> **说明** 您可以将 `<TargetServiceName>` 和 `<TargetEventName>` 两个变量分别指定为ECS和CreateInstance，即可获取ECS实例每个月的创建次数，并且展示同比上个月的增长幅度。

5. 单击**查询/分析**，查看分析结果。

6. 单击 图标查看折线图。

您也可以通过类似方法对部分风险等级较高的操作生成数据报表，并且从中分析调用规律以及流程高低峰所在时间点，以便更加合理地规划资源，提升资源利用率。

场景四：异常监控告警

某企业期望某个云服务某日的访问量超过最近60天平均访问量的一定比例时上报告警，此时您可以通过日志服务仪表盘中的查询图表配置监控告警，实现实时服务状态的监控。您也可以将自定义的统计图表添加到仪表盘中，以便实现定制化业务的实时监控。具体操作，请参见添加统计图表到仪表盘。

1. 登录日志服务控制台。
2. 在**全部的Project**页签，单击操作事件对应的**Project名称**。
3. 查询各个云服务在最近60天内的平均流量以及当天的实时流量。
   i. 单击日志库名称，然后单击**15分钟（相对）**，设置查询的时间范围为60天。
   ii. 在搜索框中输入如下代码。

```
__topic__: actiontrail_audit_event |select a.serviceName, a.avg_pv, b.today_pv from (select serviceName, avg(pv) as avg_pv from (select "event.serviceName" as serviceName, count(1) as pv, date_format(from_unixtime(__time__), '%m-%d') as day from log group by serviceName, day) group by serviceName) a join (select "event.serviceName" as serviceName, count(1) as today_pv from log where date_format(from_unixtime(__time__), '%Y-%m-%d')=current_date group by serviceName) b on a.serviceName = b.serviceName
```

   iii. 单击**查询/分析**，查看分析结果。
   iv. 单击 图标查看折线图。

> **说明** 您可以添加过滤条件排除不关注的云服务或者事件。

4. 设置业务告警。
   i. 在页面右上角选择**另存为告警 > 旧版告警**。
   ii. 在**告警监控规则**面板配置相关参数。

   具体操作，请参见设置告警。

iii. 配置触发条件。

```
$0.today_pv > $0.avg_pv && ($0.today_pv - $0.avg_pv)/$0.avg_pv > 0.5
```

其中 `$0` 表示第一条查询语句关联的原始图表数据，即每个云服务的当日访问量以及最近60天的平均访问量。 `$0.avg_pv` 表示云服务最近60天的平均访问量。

iv. 单击**确定**。

13.7. 使用操作审计查询事件

您可以使用操作审计（ActionTrail）审计团队成员的相关操作，帮助团队成员更加规范地使用云服务。例如：您可以通过操作审计定位到是哪个RAM用户在什么时间进行了什么误操作。本文以查询NAT网关的事件为例，为您介绍如何通过操作审计查询事件。

背景信息

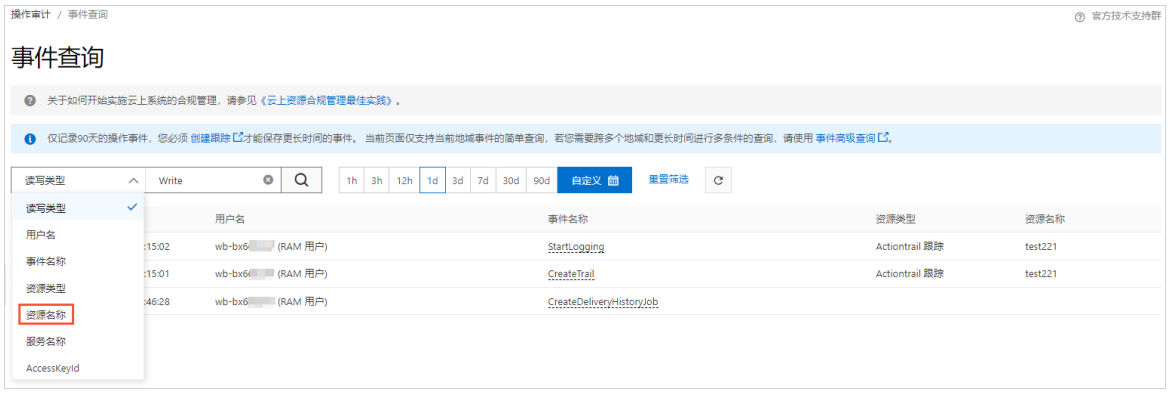
团队管理者使用阿里云账号创建了多个RAM用户供团队成员使用，并为RAM用户授予了管理员权限。

当RAM用户A查询NAT网关时，发现网关被多绑定了一个弹性公网IP。由于团队成员都有管理员权限，因此每个人都可能进行绑定操作。此时您可以通过操作审计查询事件，快速确定绑定的操作者。

说明 单击弹性公网IP地址可查看实例ID等信息。

操作步骤

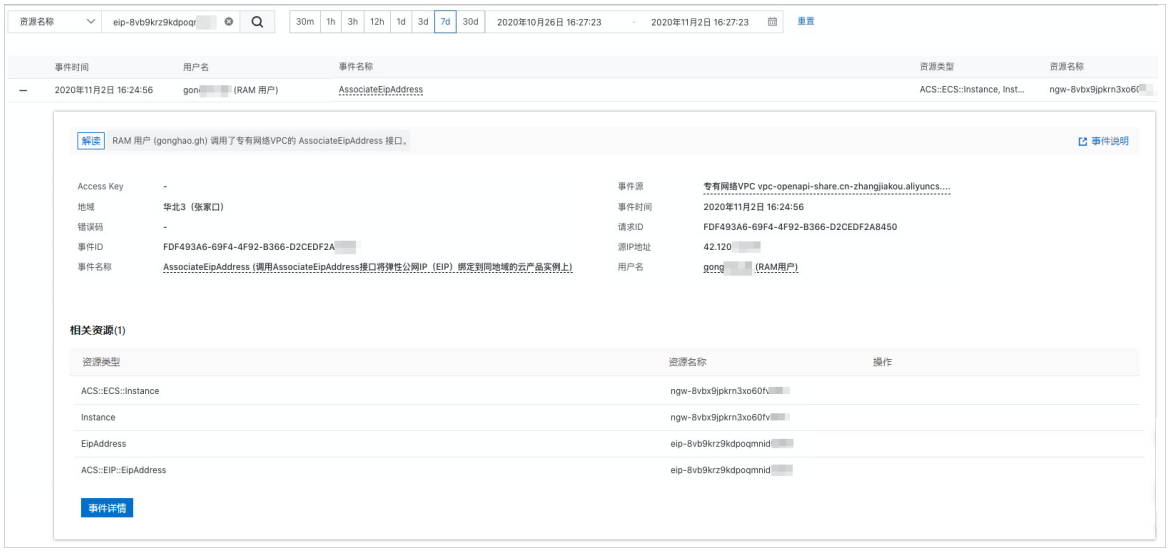
1. 登录操作审计控制台。
2. 在左侧导航栏，单击**事件查询**。
3. 在顶部导航栏，选择目标地域。
4. 从下拉菜单中，选择**资源名称**。



5. 输入待查询弹性公网IP的实例ID，然后单击

图标。

6. 单击事件前面的加号，查询事件详情。



> **说明** 操作记录显示RAM用户B在2020年11月02日16:24:56进行了绑定弹性公网IP操作，从而确定是RAM用户B错误地将弹性公网IP绑定到了RAM用户A的NAT网关上。

7. （可选）如果需要查询事件代码记录，单击**事件详情**。

13.8. 下载操作审计的事件

操作审计仅默认为每个阿里云账号记录最近90天的事件，默认仅支持通过操作审计控制台查询事件。如果您因为审计要求需要获取180天以上的事件，或者需要将事件下载到本地进行分析，则必须创建跟踪将事件投递到SLS或OSS，再通过SLS或OSS的数据下载能力将事件以文件形式下载到本地。

前提条件

请确保您已经通过提交工单，获取Insight事件的使用权限。

背景信息

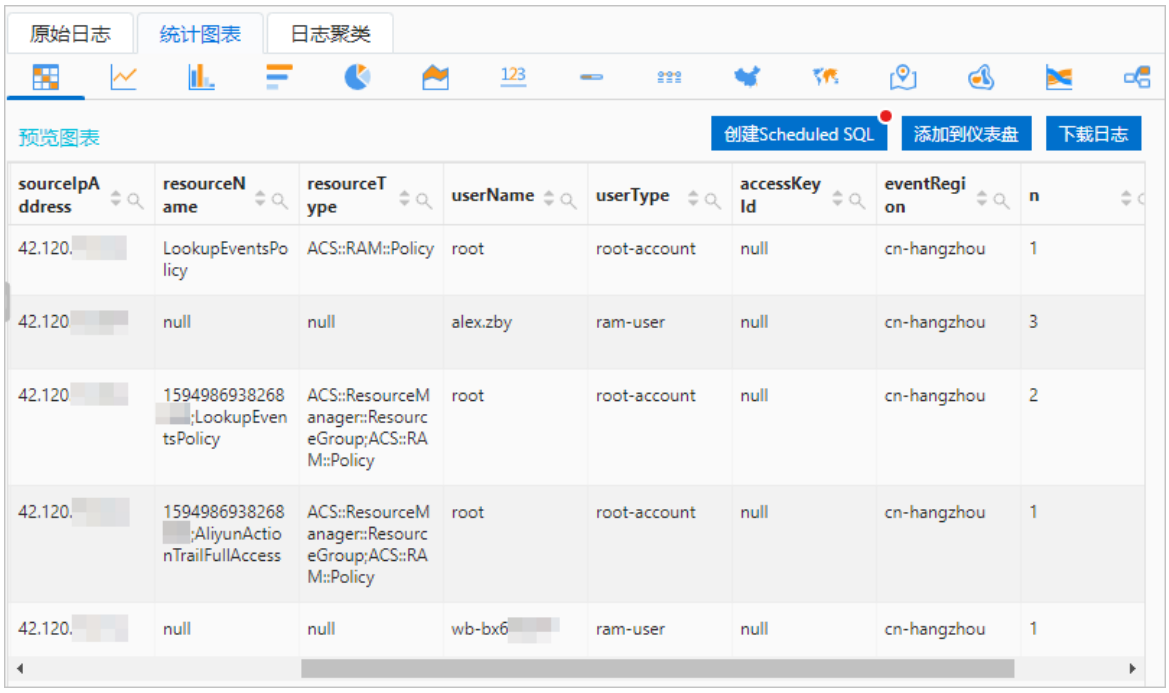
本文以单账号跟踪为例，为您介绍如何在日志服务SLS中下载操作审计的事件，步骤如下：

1. 在操作审计控制台创建跟踪将事件投递到SLS，该跟踪将持续收集新产生的审计事件并持续投递到指定的SLS Logstore。
2. （可选）在操作审计控制台创建历史投递任务，该任务可以将过去90天平台已经记录的历史审计事件以一次性任务的方式投递到跟踪已经指定的SLS Logstore。
3. 在SLS控制台下载事件。您可以根据需求在SLS控制台查询特定的事件，然后使用多种方式下载已经投递到SLS的审计事件。
   例如：通过以下SQL语句查询管控事件中所有写事件的聚合情况。

> **说明** 如果设置的查询时间段较长，建议设置 `LIMIT N` ，返回 `N` 条事件。例如：设置 `LIMIT 20` ，返回20条事件。

```
 * AND "event.eventCategory": Management AND "event.eventRW": Write | SELECT"event.service
Name"AS servieName,"event.eventName"AS eventName,"event.eventRw"AS eventRw,"event.sourceIp
Address"AS sourceIpAddress,"event.resourceName"AS resourceName,"event.resourceType"AS reso
urceType,"event.userIdentity.userName"AS userName,"event.userIdentity.type"AS userType,"ev
ent.userIdentity.accessKeyId"AS accessKeyId,"event.acsRegion"AS eventRegion,COUNT("event.e
ventId")AS n, date_trunc('hour', __time__) AS time GROUP BY time, servieName, eventName, e
ventRw, sourceIpAddress, resourceType, resourceName, accessKeyId, userType, userName, even
tRegion ORDER BY time DESC LIMIT 20
```

查询结果如下图所示（n表示事件聚合次数）：



sourceIpAddress	resourceName	resourceType	userName	userType	accessKeyId	eventRegion	n
42.120.	LookupEventsPolicy	ACS::RAM::Policy	root	root-account	null	cn-hangzhou	1
42.120	null	null	alex.zby	ram-user	null	cn-hangzhou	3
42.120	1594986938268 ;LookupEventsPolicy	ACS::ResourceManager::ResourceGroup;ACS::RAM::Policy	root	root-account	null	cn-hangzhou	2
42.120.	1594986938268 ;AliyunActionTrailFullAccess	ACS::ResourceManager::ResourceGroup;ACS::RAM::Policy	root	root-account	null	cn-hangzhou	1
42.120.	null	null	wb-bx6	ram-user	null	cn-hangzhou	1

步骤一：创建跟踪并投递到SLS

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在顶部菜单栏，选择您想创建单账号跟踪的地域。

> **说明** 该地域将成为单账号跟踪的Home地域，即创建跟踪的地域。

4. 在**跟踪列表**页面，单击**创建跟踪**。
5. 在**跟踪基本属性**页面，输入**跟踪名称**，将管控事件的**事件类型**设置为**所有事件**，选中**Insight事件**，然后单击**下一步**。
6. 在**审计事件投递**页面，选择**将事件投递到日志服务SLS**，然后选择**投递到本账号**，设置如下参数。

参数	描述
日志库所属地域	日志项目所在地域。

参数	描述
日志项目名称	日志服务SLS中日志项目的名称。同一账号下，日志项目名称不能重复。 ○ 当您选中**创建新的日志项目**时，将通过操作审计控制台新建日志项目，输入日志项目名称。 ○ 当您选中**选择已有的日志项目**时，在日志服务SLS中选择已有日志项目名称。关于如何在日志服务SLS中新建日志项目，请参见快速入门。

7. 单击**下一步**。
8. 在**预览并创建**页面，确认跟踪信息，然后单击**提交**。

步骤二（可选）：创建历史事件投递任务

创建跟踪仅能投递跟踪创建时间之后的事件，如果需要下载最近90天的完整事件，您还需创建历史事件投递任务，补投递跟踪创建时间往前一段时间的事件。

> **说明**
> 如果需要创建历史事件投递任务，请通过提交工单，获取历史事件投递任务功能的使用权限。

1. 在左侧导航栏，单击**历史事件投递任务**。
2. 在顶部菜单栏，选择您需要投递历史事件的地域。

   > **说明** 该地域必须与单账号跟踪所在地域相同。

3. 在**历史事件投递任务**页面，单击**创建任务**。
4. 在**创建任务**页面，选择跟踪。

   > **说明** 选择跟踪后，系统将自动填入跟踪的地域、日志项目地域、日志项目名称和日志库信息。

5. 单击**确定**。

步骤三：在SLS控制台下载事件

您可以在SLS控制台查询特定时间范围的事件，然后下载事件。如果查询到多个事件，SLS会将多个事件下载到同一个文件中，方便您后续使用。

1. 在操作审计控制台，进入跟踪所在日志库。
   i. 在左侧导航栏，单击**跟踪列表**。
   ii. 在顶部菜单栏，选择您单账号跟踪和历史事件投递任务所在的地域。
   iii. 在**跟踪列表**页面，将鼠标悬浮到目标跟踪**存储服务**列的 ! 图标，然后单击SLS日志库名称。
2. 在SLS控制台，单击**15分钟（相对）**，设置查询的时间范围（例如：今天）。
3. 输入查询语句，然后单击**查询/分析**。

   关于如何设置查询语句，请参见如何在SLS设置SQL语句查询操作审计的事件。
4. 下载事件。

- 方式一：下载按字段维度分类的事件统计信息。
  在**统计图表**页签，单击

  图标，然后单击**下载日志**。
- 方式二：下载事件代码文件。
  在**原始日志**页签，单击

  图标。

5. 在**日志下载**对话框，选择下载方式，然后单击**确定**。
   - **直接下载**：将本页展示的日志以CSV格式下载到本地。
   - **通过Cloud Shell下载**：请根据页面提示，下载所有日志。

     > **说明** 目前Cloud Shell位于上海地域，如果当前Logstore不在上海地域，下载日志会产生一定的公网流量费用。关于价格的更多信息，请参见产品定价。

   - **通过命令行工具下载**：请根据页面提示，下载所有日志。

     > **说明**
     > - 通过命令行工具下载日志时，需替换命令中的访问密钥（AK）信息。请登录用户信息管理控制台获取阿里云账号AK。如果使用RAM用户进行下载，请登录RAM 控制台创建RAM用户并获取RAM用户的AK信息。
     > - 如果用于安装命令行工具的机器所在地域与当前Project所在地域相同，建议单击**切换为内网endpoint**，下载速度更快且不会产生额外的外网带宽费用。

13.9. 使用SDK创建跟踪

本文为您介绍如何使用SDK创建跟踪，将操作事件投递到日志服务SLS，并配置日志服务报表。

前提条件

- 请确保您已安装Python和pip。
- 请确保您已安装Python编辑工具。本文以Visual Studio Code为例进行介绍。

背景信息

使用操作审计控制台创建跟踪时，操作审计会自动创建日志服务项目（LogProject）、日志库（LogStore）及报表，并开启跟踪。使用SDK创建跟踪时，您需要手动创建日志服务项目（LogProject）、日志库（LogStore）及报表。创建跟踪后，您仍需手动开启跟踪。

步骤1：创建并配置日志服务

创建跟踪前，您需要创建日志项目（LogProject），并创建名为 `actiontrail_{TrailName}` 的日志库（LogStore），其中 `TrailName` 是跟踪名称。

此外，如果需要对操作事件进行分析，还需要对日志库配置索引和报表。您可以使用日志服务的Python SDK（aliyun-log-python-sdk）创建并配置日志服务 。

1. 在Visual Studio Code中新建Python文件。
2. 安装依赖并初始化SDK。

i. 安装依赖。

```
$ pip install -U aliyun-log-python-sdk
```

ii. 初始化SDK。

```
from aliyun.log import LogClient
# 华东 1 （杭州） Region
region = 'cn-hangzhou'
# 日志服务入口
endpoint = '{region}.log.aliyuncs.com'.format(region=region)
# 用户访问密钥对中的AccessKey ID
access_key_id = 'ABCDEFGHIJK****'
# 用户访问密钥对中的AccessKey Secret
access_key_secret = 'OPQRSTUV****'
# 阿里云账号ID
account_id = '123456789'
client = LogClient(endpoint, access_key_id, access_key_secret)
```

说明 地域、AccessKey ID、AccessKey Secret和阿里云账号ID请根据实际情况填写。

3. 创建日志项目（LogProject）和日志库（LogStore）。

```
# 跟踪名称
trail_name = 'cloud_trail'
# 日志项目名称
log_project_name = 'cloud-trail-project'
# 创建日志服务
res = client.create_project(log_project_name, '操作审计事件日志项目')
res.log_print()
# 日志库名称
log_store_name = 'actiontrail_{trail_name}'.format(trail_name=trail_name)
# 创建日志库
res = client.create_logstore(log_project_name, log_store_name, shard_count=3, preserve_
storage=True)
res.log_print()
```

说明 跟踪名称、日志项目名称和日志库名称请根据实际情况填写。创建日志库时，指定 `preserve_storage` 为 `True` 表示永久保存数据。

4. 配置索引。

i. 创建 `log_index.json` 索引配置文件。

访问开源代码仓库，下载索引配置文件。

ii. 创建索引。

```
import json
from aliyun.log import LogClient
from aliyun.log import IndexConfig
def get_json_data(path):
    with open(path) as f:
        return json.load(f)
# 从log_index.json中读取索引配置
index_json = get_json_data('./log_index.json')
index_detail = IndexConfig()
index_detail.from_json(index_json)
# 创建索引
client.create_index(log_project_name, log_store_name, index_detail)
```

5. 创建报表。

   i. 创建 `log_dashboard.json` 报表配置文件。

   访问开源代码仓库，下载报表配置文件。

   ii. 创建报表。

```
#  从log_dashboard.json中读取报表配置
dashboard_detail = get_json_data('./log_dashboard.json')
# 创建报表
client.create_dashboard(log_project_name, dashboard_detail)
```

步骤2：创建并启用跟踪

您可以使用阿里云Python SDK（aliyun-python-sdk-core）创建跟踪。

1. 初始化SDK。

   i. 安装依赖。

```
$ pip install aliyun-python-sdk-core
$ pip install aliyun-python-sdk-actiontrail
```

   ii. 初始化SDK。

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkactiontrail.request.v20171204.CreateTrailRequest import CreateTrailRe
quest
client = AcsClient(access_key_id, access_key_secret, region)
```

2. 创建跟踪到指定日志项目（LogProject）。

   使用SDK调用CreateTrail接口创建跟踪。

```
sls_project_arn = 'acs:log:{region}:{account_id}:project/{log_project_name}'.format(
    region=region,
    account_id=account_id,
    log_project_name=log_project_name,
)
request = CreateTrailRequest()
request.set_accept_format('json')
# 设置跟踪名称
request.set_Name(trail_name)
# 设置SLS Project的ARN
request.set_SlsProjectArn(sls_project_arn)
# 跟踪所有事件
request.set_EventRW("All")
# 跟踪所有地域
request.set_TrailRegion("All")
response = client.do_action_with_exception(request)
print(str(response, encoding='utf-8'))
```

说明 创建跟踪后，跟踪状态为Fresh表示已创建但未开启。您仍需开启跟踪。

3. 启用跟踪。

   使用SDK调用StartLogging接口启用跟踪。

```
from aliyunsdkactiontrail.request.v20171204.StartLoggingRequest import StartLoggingRequest
request = StartLoggingRequest()
request.set_accept_format('json')
request.set_Name(trail_name)
response = client.do_action_with_exception(request)
print(str(response, encoding='utf-8'))
```

说明 您可以访问开源代码仓库，查看完整代码。

13.10. 使用Terraform自动化创建跟踪

您可以使用操作审计创建跟踪，将操作事件持续投递到日志服务SLS或对象存储OSS中。Terraform可以完成自动化创建。

前提条件

运行Terraform程序前，请确保您已开通以下云服务：

- 日志服务SLS
- 对象存储OSS

说明 日志服务和对象存储在超出免费额度后，会产生少量费用。更多信息，请参见日志服务计算说明和对象存储计算说明。

背景信息

Terraform是一个开源的自动化资源编排工具，帮助您自动化构建、配置和管理云上资源。您可以通过Terraform模板创建跟踪。更多信息，请参见Terraform Alibaba Cloud Provider。

创建跟踪

您可以通过Terraform程序将跟踪分别投递到日志服务SLS或对象存储OSS，或者同时进行投递。关于如何选择存储服务，请参见将事件持续投递到指定服务。

场景一：仅投递到SLS | 场景二：仅投递到OSS | 场景三：同时投递到SLS和OSS

当您需要将跟踪投递到SLS时，仅需在Cloud Shell部署SLS相关程序，即可自动创建跟踪。

1. 访问使用Terraform创建操作审计的跟踪 。
2. 在弹出的对话框中，单击**确认**，克隆代码到CloudShell。
3. 输入以下命令，定位用来创建跟踪的Terraform模板的目录。

```
cd ~/tutorial-actiontrail-createdby-terraform/trail-sls
```

4. 输入以下命令，加载Terraform Alibaba Cloud Provider。

```
terraform init
```

5. 输入以下命令，创建跟踪。

```
terraform apply
```

如果返回Resources: X added（X表示新增资源的个数），说明跟踪创建成功，示例如下。

```
Apply complete! Resources: 3 added, 0 changed, 0 destroyed.

Outputs:

sls_project_id = [
  [
    "tutorial-terraform-actiontrail",
  ],
]
trail_id = [
  [
    "tutorial-actiontrail",
  ],
]
```

（可选）删除资源

您可以根据场景选择不同的资源删除方法。删除后，自动投递跟踪程序将失效。

场景一：仅删除SLS和跟踪资源 | 场景二：仅删除OSS和跟踪资源 | 场景三：同时删除SLS、OSS和跟踪资源

Terraform模板参数说明

当您需要修改Terraform程序中的代码时，您可以参考如下参数说明修改Terraform模板。例如：您可以将event_rw设置为Write，仅跟踪写事件。

参数	说明
trail_name	跟踪名称。

参数	说明
event_rw	阿里云操作事件的类型。取值： • Read：读事件。指的是仅读取云资源信息的事件。 • Write：写事件。指的是增加、删除或修改云资源的事件。 • All：所有事件。
oss_bucket_name	OSS Bucket名称。 说明 oss_bucket_name和sls_project_arn需至少指定其中一个参数。
oss_key_prefix	OSS Bucket中操作事件文件的前缀，默认为空。
role_name	用户允许操作审计服务扮演的RAM角色名称，操作审计使用该角色将操作事件投递到您的存储服务，默认值：aliyunserviceroleforactiontrail。 如果该角色不存在，系统会自动进行创建。更多信息，请参见操作审计服务关联角色。
sls_project_arn	日志服务Project ARN。格式为 `acs:log:<region_id>:<account_id>:project/<project_name>` 。 说明 oss_bucket_name和sls_project_arn需至少指定其中一个参数。
sls_write_role_arn	日志服务角色ARN。操作审计将用该角色来将操作事件写入对应SLS Logstore，格式为 `acs:ram::<account_id>:role/<role_name>` 。默认将使用服务关联角色。
trail_region	跟踪地域。默认值：All（跟踪所有地域）。 您也可以指定地域（region_id），多个地域用英文逗号（,）分隔，例如： `cn-beijing,cn-hangzhou` 。
mns_topic_arn	MNS消息主题的ARN。如果设置了该参数，则当操作事件投递到OSS后，操作审计将向对应主题发送一条消息。
status	跟踪状态。取值： • Enable（默认值）：启用跟踪。 • Disable：禁用跟踪。

13.11. 使用操作审计为资源自动绑定标签

本文为您提供了一个自动化绑定标签程序，用于为新创建的资源自动绑定创建者标签，标识该资源的创建者，以此提升分账效率。您可以借助操作审计（ActionTrail）的跟踪功能，实现该任务。

前提条件

运行程序前，请确保您已开通以下云服务：

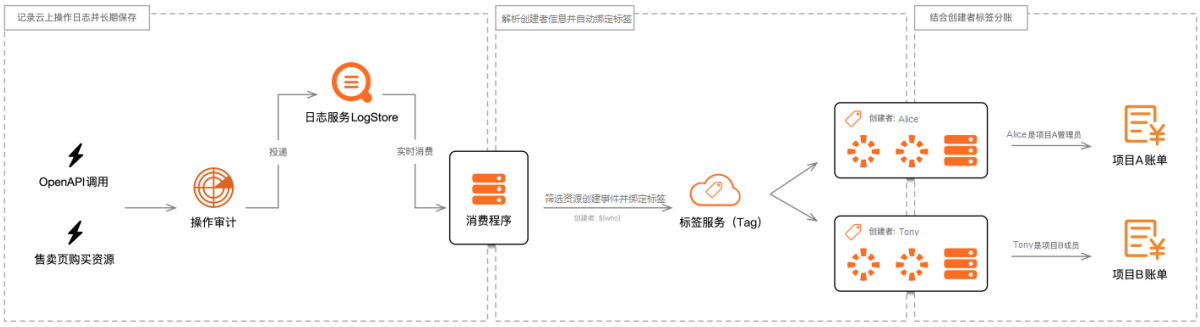
- 访问控制（RAM）
- 操作审计（ActionTrail）
- 函数计算（FC）

- 日志服务（SLS）

> **说明** 访问控制和操作审计目前免费。但您使用操作审计时用到的日志服务、函数计算这两个云服务，在超出免费额度后，会产生少量费用。更多信息，请参见日志服务计算说明、函数计算计费说明。

方案介绍

操作审计会记录阿里云账号内的操作日志，这份操作日志可以被实时消费。因此我们可以部署一个消费程序，在处理到资源创建对应的操作事件时，调用标签服务的API，为资源绑定创建者标签。最后，在用户中心通过标签进行分账。工作流程如下图所示：



1. 在操作审计中创建跟踪。
   使用操作审计的跟踪功能，记录云上操作日志，并投递到日志服务中。
2. 在日志服务中消费日志数据。
   消费方式可以选择函数计算、Flink或是自行开发的程序。本程序采用的是函数计算。
   在完成消费后，调用标签服务的API，为资源绑定标签。
3. 在用户中心查看分账账单。
   您可以基于资源的创建者标签，通过用户中心的分账账单、费用分析或财务单元等功能，查看费用分摊账单。更多信息，请参见分账账单查看方式。

部署程序

以下步骤以VPC为例。在程序部署完成后，当您创建了VPC，系统会自动为该VPC绑定创建者标签。

1. 访问实时消费操作审计日志并自动绑定资源标签。
2. 在弹出的对话框中，单击**确认**，克隆代码到CloudShell。
3. 输入以下命令，一键创建跟踪并部署自动绑定标签程序。

```
./install.sh
```

4. 在程序部署完成后，请等待至少1分钟，然后输入以下命令，创建1个VPC，用来验证自动绑定标签程序是否已经生效。

```
sleep 60
CREATED_VPC_ID=`aliyun vpc CreateVpc --RegionId cn-huhehaote | jq ".VpcId"`
```

5. 请等待1~5分钟，然后输入以下命令，查看刚创建的VPC是否绑定了创建者标签。

```
aliyun vpc DescribeVpcs --RegionId cn-huhehaote --VpcId $CREATED_VPC_ID | jq ".Vpcs.Vpc
[0].Tags"
```

   如果返回如下信息，说明该VPC已成功绑定创建者标签。

```
{
  "Tag": [
    {
      "Key": "created_by",
      "Value": "ram-user:22135730502024****"
    }
  ]
}
```

（可选）删除资源

输入以下命令，删除程序中创建的所有资源。删除后，自动绑定标签程序将失效。

```
./uninstall.sh
```

（可选）修改资源类型

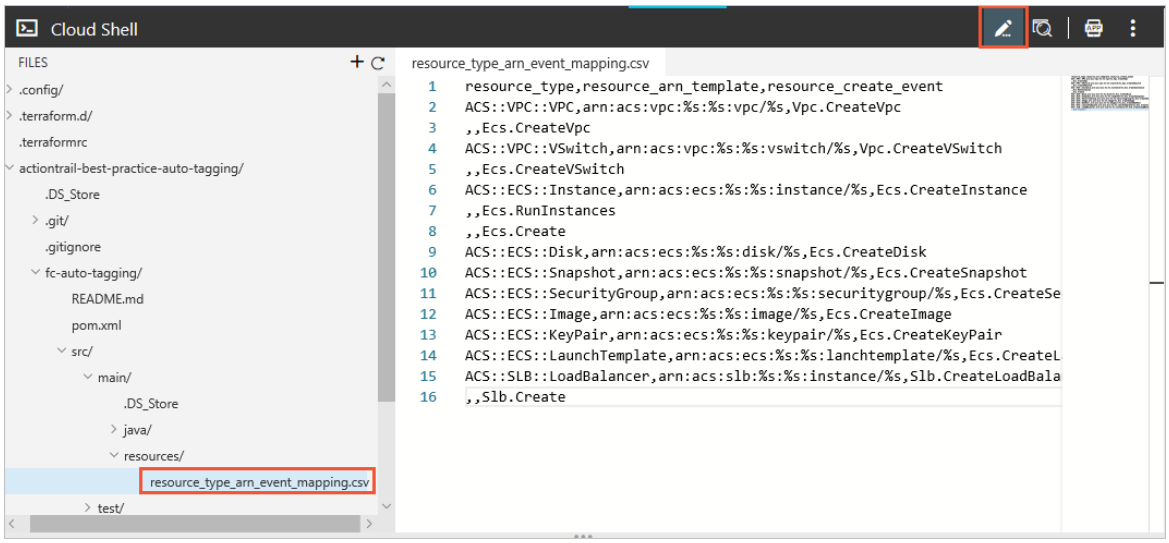
上述程序支持为以下资源类型自动绑定创建者标签：

- 云服务器ECS：ECS实例、云盘、快照、安全组、镜像、密钥对和启动模板。
- 云数据库RDS实例。
- 负载均衡SLB实例。
- 专有网络VPC：专有网络、交换机。

您也可以尝试修改程序的配置文件，为其他资源类型自动绑定创建者标签。资源类型必须支持操作审计和标签，详情请参见支持操作审计的资源类型、支持标签的云服务。

1. 在CloudShell右上角，单击编辑器图标，找到并复制resource_type_arn_event_mapping.csv文件里的内容，然后保存CSV格式的文件到本地。

   resource_type_arn_event_mapping.csv文件访问路径如下：*actiontrail-best-practice-auto-tagging/fc-auto-tagging/src/main/resources/resource_type_arn_event_mapping.csv*



2. 在本地修改resource_type_arn_event_mapping.csv文件中的资源类型。
3. 将新修改的内容复制到CloudShell的resource_type_arn_event_mapping.csv文件中。
4. 输入以下命令，重新部署程序。

```
./reinstall.sh
```

13.12. 长期存储完整的事件

操作审计仅默认为每个阿里云账号存储最近90天的事件，而等保2.0（网络安全等级保护2.0制度）要求将事件保存180天及以上。您可以创建跟踪和历史事件投递任务，以便长期存储完整的事件。否则，将无法追溯90天以前的事件。

前提条件

请确保您已经通过提交工单，获取历史事件投递任务和Insight事件的使用权限。

背景信息

创建跟踪仅能投递跟踪创建时间之后的事件，为了将最近90天的事件进行完整的保存，您还需创建历史事件投递任务，补投递跟踪创建时间往前一段时间的事件。

补投递的历史事件时间范围的开始时间为当前时间往前90天，结束时间为历史事件投递任务关联的跟踪生效后5分钟。例如：您创建历史事件投递任务时关联跟踪A已经创建了40天，历史事件投递任务将投递跟踪A创建时间往前50天的历史事件。

> **说明**
> - 历史事件投递任务仅支持将单账号跟踪的历史事件投递到日志服务SLS。
> - 一个阿里云账号同时只能存在一个正在运行的历史事件投递任务。

步骤一：创建单账号跟踪并将事件投递到日志服务SLS

1. 登录操作审计控制台。
2. 在左侧导航栏，单击**跟踪列表**。
3. 在顶部菜单栏，选择您想创建单账号跟踪的地域。

   > **说明** 该地域将成为单账号跟踪的Home地域，即创建跟踪的地域。

4. 在**跟踪列表**页面，单击**创建跟踪**。
5. 在**跟踪基本属性**页面，输入**跟踪名称**，将管控事件的**事件类型**设置为**所有事件**，选中**Insight事件**，然后单击**下一步**。
6. 在**审计事件投递**页面，选择**将事件投递到日志服务SLS**，然后选择**投递到本账号**，设置如下参数。

参数	描述
日志库所属地域	日志项目所在地域。
日志项目名称	日志服务SLS中日志项目的名称。同一账号下，日志项目名称不能重复。 ○ 当您选中**创建新的日志项目**时，将通过操作审计控制台新建日志项目，输入日志项目名称。 ○ 当您选中**选择已有的日志项目**时，在日志服务SLS中选择已有日志项目名称。关于如何在日志服务SLS中新建日志项目，请参见快速入门。

7. 单击**下一步**。

8. 在**预览并创建**页面，确认跟踪信息，然后单击**提交**。

步骤二：创建历史事件投递任务

1. 在左侧导航栏，单击**历史事件投递任务**。
2. 在顶部菜单栏，选择您需要投递历史事件的地域。

> **说明** 该地域必须与单账号跟踪所在地域相同。

3. 在**历史事件投递任务**页面，单击**创建任务**。
4. 在**创建任务**页面，选择跟踪。

> **说明** 选择跟踪后，系统将自动填入跟踪的地域、日志项目地域、日志项目名称和日志库信息。

5. 单击**确定**。

步骤三（可选）：查询完整的事件

1. 在左侧导航栏，单击**跟踪列表**。
2. 在顶部菜单栏，选择您单账号跟踪和历史事件投递任务所在的地域。
3. 在**跟踪列表**页面，将鼠标悬浮到目标跟踪**存储服务**列的 图标，然后单击SLS日志库名称。
4. 单击**15分钟（相对）**，设置查询的时间范围。
5. 单击**查询/分析**，查询事件。