

云审计服务

# 常见问题

文档版本 01  
发布日期 2024-04-30



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

## 目录

1 使用 IAM 用户（子账号）在 CTS 配置转储，操作 OBS 桶也必须是 IAM 用户么？ .....	1
2 事件列表用于记录哪些信息？ .....	2
3 用户公有云账户欠费给云审计服务带来的影响？ .....	3
4 哪些用户应该开通云审计服务？ .....	4
5 如果用户已开通云审计服务，但 OBS 桶未配置正确的策略，会出现什么情况？ .....	5
6 云审计服务是否支持事件文件的完整性校验？ .....	6
7 为什么查看事件窗口中的有些事件的字段为空？ .....	7
8 为什么事件列表中的某些操作被记录了两次？ .....	8
9 关键操作通知服务支持哪些服务？ .....	9
10 CTS 如何长期保存事件文件——转储至 OBS 桶.....	10
11 为什么有些 trace_type 为 systemAction 的事件，存在 user 和 source_ip 为空的情况？ .....	11
12 如何通过云审计服务确认 ECS 的创建用户.....	12
13 如何查询 IAM 用户登录的 IP 地址.....	13
14 为什么按需和包周期创建虚拟机的时候会有两个 deleteMetadata 事件？ .....	14
15 查询不到事件怎么办？ .....	15
16 云审计功能申请打开之后是否可以自助关闭？ .....	16
17 如何配置 CTS 审计日志存储 180 天？ .....	17
18 在 CTS 控制台无法创建追踪器.....	22
19 使用 IAM 用户无法开通 CTS 怎么办？ .....	23
20 如何给云硬盘添加告警通知？ .....	24
21 可以接收重复的事件吗？ .....	25
22 跨租户密钥授权 OBS 桶转储失败怎么办？ .....	26
23 cts_admin_trust 委托是否包含 OBS 授权？ .....	28

# 1 使用 IAM 用户（子账号）在 CTS 配置转储，操作 OBS 桶也必须是 IAM 用户么？

---

不是，操作OBS桶的用户不区分IAM用户和账号，只需要用户具备操作OBS桶的权限即可。

## 2 事件列表用于记录哪些信息?

事件列表记录了两种事件，分别为管理类事件和数据类事件。管理类事件指云账户中对云服务资源新建、配置、删除等操作的详细信息。数据类事件指针对数据的操作日志，例如上传、下载等。事件列表不记录查询操作的相关信息。

# 3 用户公有云账户欠费给云审计服务带来的影响?

---

当用户公有云账户欠费时，云审计服务依旧可以接收所支持服务发送的操作信息，但只能保存近7天的操作记录。因为7天之前的历史操作记录会以事件文件的形式实时保存至OBS桶，而将事件文件存储于OBS桶所产生的流量需要付费。

此时只能对追踪器执行“删除”操作。

# 4 哪些用户应该开通云审计服务?

所有云用户均应该开通云审计服务。

- 从政策、行业规范角度，云审计服务是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分，也是很多行业标准、审计规范的必备组成部分。
- 从应用角度，云审计服务是云资源出现问题时，降低问题定位时间和人力成本的有效手段，能够精确定位到问题发生时的所有操作，借以减小问题排查范围。

# 5 如果用户已开通云审计服务，但 OBS 桶未配置正确的策略，会出现什么情况？

---

云审计服务会根据既有的OBS存储桶策略来传送事件文件。如果错误地配置OBS存储桶策略，那么云审计服务将无法传送事件文件。

被删除或有异常的OBS桶，管理控制台界面会显示相应的错误提示信息。用户可选择重新[创建OBS桶](#)或重新[配置OBS桶的访问权限](#)。



# 6 云审计服务是否支持事件文件的完整性校验?

---

支持。原则上进行完整性校验时必须包含以下字段：time、service\_type、resource\_type、trace\_name、trace\_rating、trace\_type，其他字段由各服务自己定义。

# 7 为什么查看事件窗口中的有些事件的字段为空?

可以为空的字段有source\_ip、code、request、response和message，这些字段并非云审计服务规定的必备字段：

- source\_ip：当trace type为SystemAction时，表示本次操作由服务内部触发，此时缺失IP字段为正常情况。
- request/response/code：这三个字段是表示本次操作所对应的请求内容、请求结果及HTTP返回码，在有些情况下，这些字段本身为空，或不具备业务意义，产生该事件的云服务会根据实际情况选择某字段留空。
- message：该字段为预留字段，若其他云服务基于业务需要，需要增加额外信息时，可附加在该字段内，缺失为正常情况。

# 8 为什么事件列表中的某些操作被记录了两次？

对于异步调用事件，会产生两条事件记录，其事件名称、资源类型、资源名称等字段相同。在事件列表中，看起来是重复记录了操作（例如，Workspace的deleteDesktop事件），但实际上，这两条事件是相互关联、但内容不同的两条记录，典型的异步调用场景时间如下：

- 第一条事件：记录用户发起的请求；
- 第二条事件：记录用户请求的操作结果，通常与第一条时间记录有数分钟的延迟，记录用户请求的实际响应结果。

两条事件需要结合在一起，才能反映用户本次操作的真实结果。

# 9 关键操作通知服务支持哪些服务?

云审计服务支持对全部的关键操作发送通知，支持的服务类型包括ECS、EVS、VPC、DEW、IAM和原生OpenStack等，支持的操作类型上包括创建、删除、登录和对原生OpenStack接口等操作。

# 10 CTS 如何长期保存事件文件——转储至 OBS 桶

---

云审计服务仅保存近7天的事件，可以对追踪器增加OBS转储的相关配置，将事件同步、长期保存至OBS桶。具体操作请参考[配置追踪器](#)。

# 11 为什么有些 trace\_type 为 systemAction 的事件，存在 user 和 source\_ip 为空的情况？

---

trace\_type字段的业务意义为标示请求来源，该字段可以是控制台（ConsoleAction）、API网关（ApiCall）及系统内调用（SystemAction）。

系统内调用为非用户触发的操作，例如自动触发的告警、弹性伸缩、定时备份任务以及为完成用户请求产生的系统内部次级调用等，这种情况下，不存在直接触发操作的用户或设备，根据审计的客观性原则，该两个字段为空。

# 12 如何通过云审计服务确认 ECS 的创建用户

## 问题描述

如果您需要确定一台ECS的创建用户，可以通过CTS记录的事件进行查看。

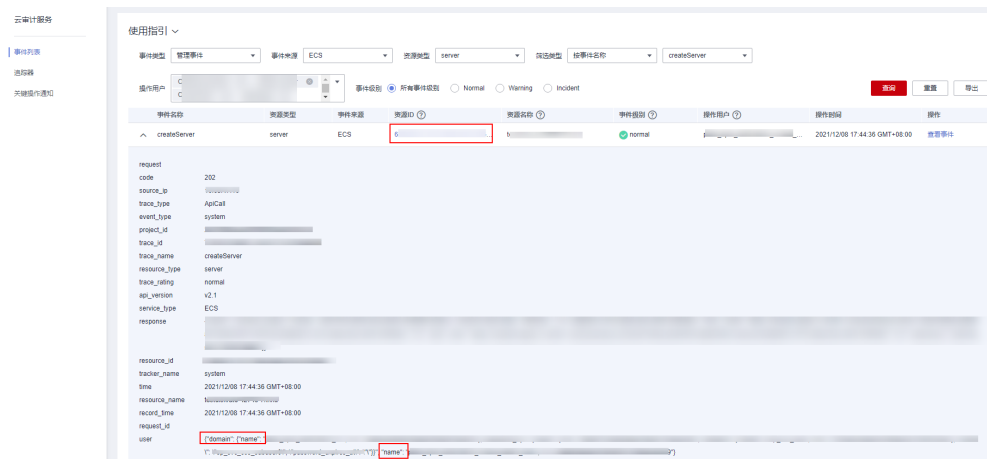
## 前提条件

- 已开启云审计服务
- 已开启获取创建的ECS主机的资源ID

## 操作方法

进入云审计服务控制台，在事件来源中筛选“ECS”，在列出的ECS事件列表中，寻找“createServer”事件，并找到对应的资源ID的事件，展开事件详情。

user列表表示创建该台ECS的用户详情，{"name":"账号名","id":"用户的账号ID","domain":{"name":"IAM用户名","id":"IAM用户ID"}}，如果是账号本身创建的该台ECS，则账号名与IAM用户名，名称相同。



# 13 如何查询 IAM 用户登录的 IP 地址

---

## 问题描述

如果您想查询IAM用户的登录IP地址和登录时间，以确认当前账号是否存在安全风险，可以通过CTS记录的事件进行查看。

## 前提条件

已开启云审计服务。

## 操作方法

**步骤1** 进入云审计服务控制台，在事件来源中筛选“IAM”，选择筛选时间段后，单击“查询”。

**步骤2** 单击“查看事件”，可以查看到具体的时间内容。其中"source\_ip"为登录IP，"record\_time"为登录时间。

----结束



# 14 为什么按需和包周期创建虚拟机的时候 会有两个 deleteMetadata 事件?

---

由于系统在创建虚拟机的时候需要使用metadata存储临时信息，在创建虚拟机完成后会自动删除该信息，因此会触发两个deleteMetadata信息。

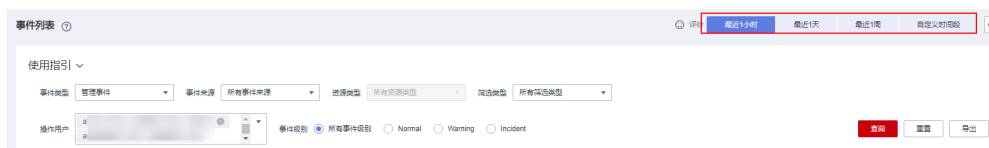
# 15 查询不到事件怎么办？

## 问题描述

在CTS控制台查询不到事件。

## 操作方法

**步骤1** 查看是否已选择正确的时间范围。



**步骤2** 查看筛选条件是否选择正确。



**步骤3** 对于IAM等不区分region的服务，需要在中心region（北京四）开通CTS服务并创建system追踪器，其他region才能上报事件。如需实现IAM的操作记录发送短信邮件，也需要在中心region配置通知规则。

**步骤4** 以上步骤确认正确后，依然查询不到应有事件，可以提交工单，联系技术工程师为您解决。

----结束

# 16 云审计功能申请打开之后是否可以自助关闭?

云审计服务本身免费，包括开通追踪器、事件跟踪以及7天内事件的存储和检索，只有配置转储等增值服务才会收费，本身没有必要关闭。

如果用户检查需要关闭云审计功能，有以下两种方法：

- 可以在追踪器中将已有追踪器删除或停用，删除或停用后，事件仍可以正常上报。
- 可以在IAM委托中将CTS委托删除，审计服务将无法使用。



# 17 如何配置 CTS 审计日志存储 180 天?

## 问题描述

搜索回溯一些问题，需要审计日志存储180天，如何配置审计日志存储时间并进行搜索分析？


## 操作步骤


- **配置转储**

开通云审计日志后，系统会自动创建一个名为system的管理事件追踪器，并将当前租户的所有操作记录在该追踪器中。在追踪器中配置CTS转储到LTS，配置完成后会在LTS自动创建日志组日志流，日志流默认存储时间为30天，可以在LTS修改日志流存储时间为180天，即可实现CTS审计日志存储180天。

a. 登录管理控制台。

- 如果您是以主账号登录华为云，请直接执行3。
- 如果您是以IAM用户登录华为云，请先联系管理员（主账号、admin用户组中的用户）对IAM用户授予以下权限，授权方法请参见[给IAM用户授权](#)。
  - CTS FullAccess

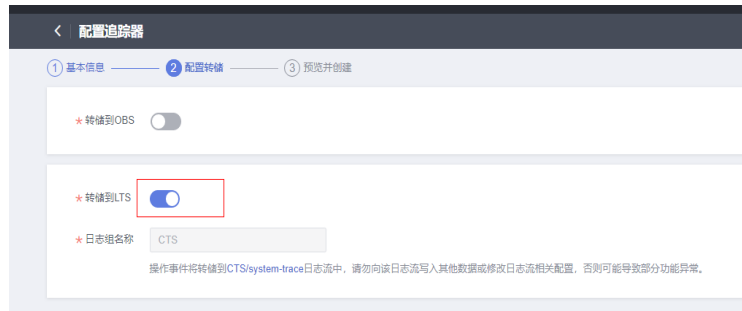
b. 在管理控制台左上角单击  图标，选择区域和项目。

c. 单击左上角  ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。

d. 配置system追踪器，将审计日志接入LTS，单击操作列中的“配置”。

e. 配置转储时，打开“转储到LTS”开关，系统会自动在LTS创建日志组：CTS，日志流：system-trace。

图 17-1 转储 LTS




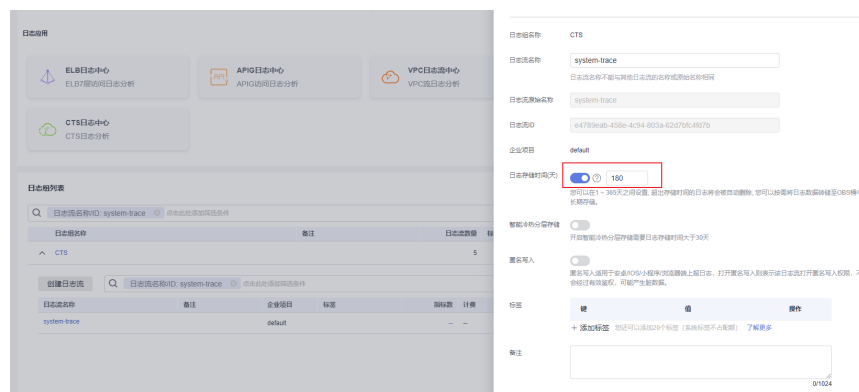
- f. 配置转储到LTS，修改LTS的日志流为180天存储，配置结构化规则为CTS。
  - i. 单击左上角 ，选择“管理与监管 > 云日志服务 LTS”，进入云日志服务控制台页面。
  - ii. 在日志管理页面，单击e中创建的system-trace日志流对应操作列的“编辑”，打开“日志存储时间（天）”开关，修改日志流存储时间为180天。

图 17-2 编辑日志流



图 17-3 修改存储时间



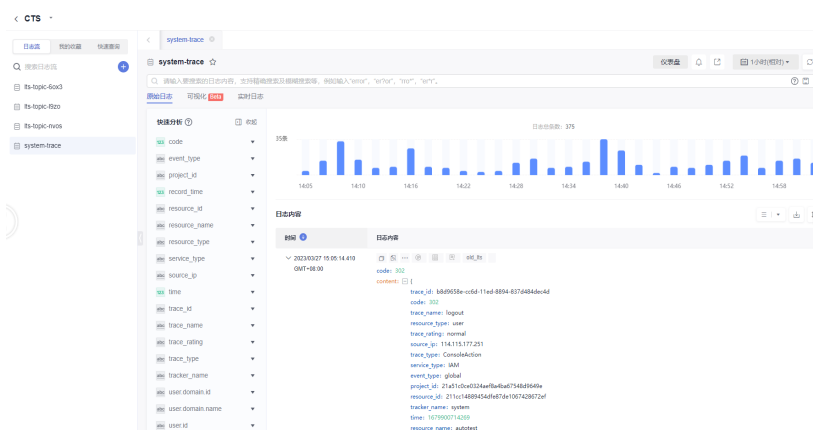
- iii. 在“日志接入 > 云审计 CTS”页面，选择日志组：CTS，日志流：system-trace。

图 17-4 选择日志流



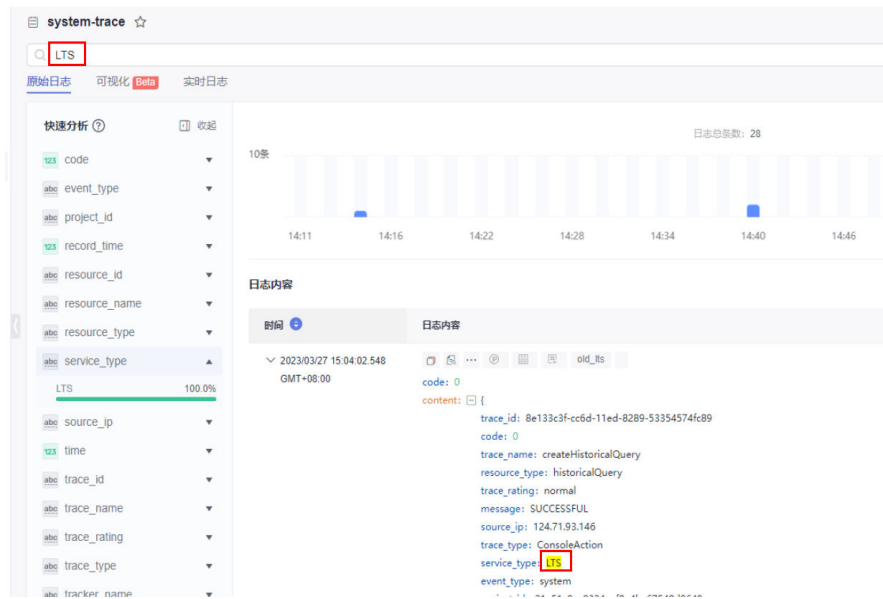
- iv. CTS配置已完成，跳到下一步“日志流配置”，完成CTS日志的结构化配置。
- v. 单击“提交”，即可完成接入LTS配置。
- vi. 单击“查看日志流”，进入日志流详情页面。

图 17-5 日志流详情



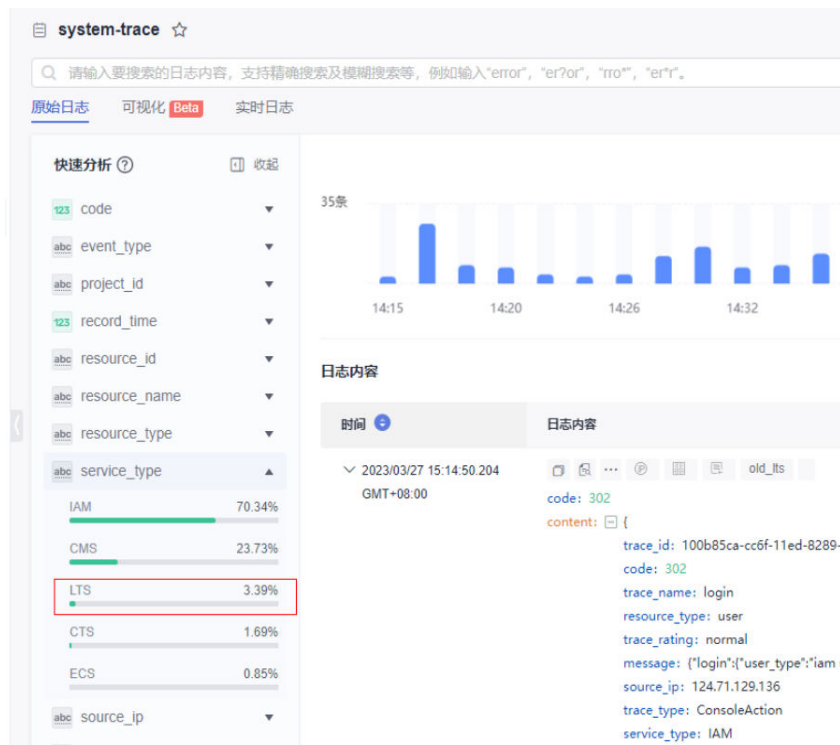
- **日志搜索分析**  
配置转储到LTS完成后，可在LTS进行审计日志的搜索分析。
  - 方式一：直接在搜索框中输入“LTS”，搜索日志。

图 17-6 搜索日志



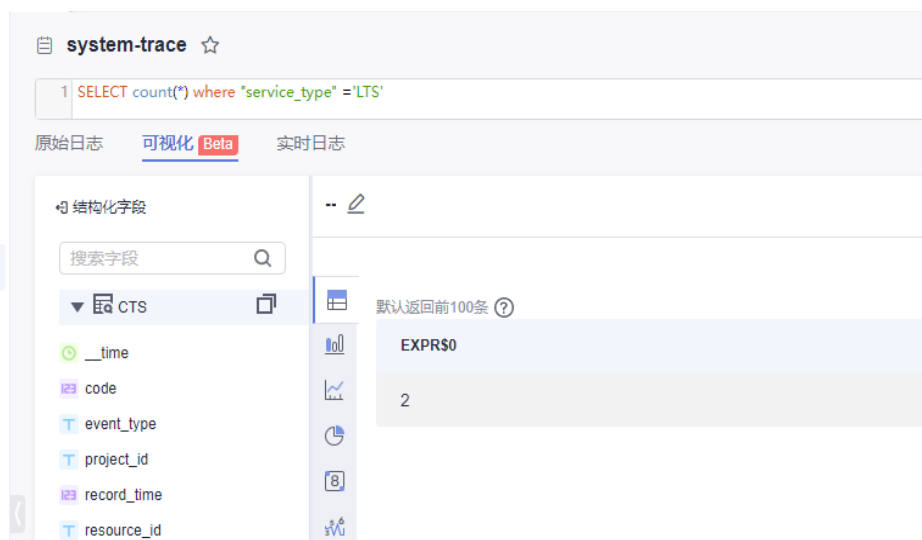
- 方式二：在“快速分析”中找到“service\_type”（审计日志中“service\_type”代表云服务类型），选择“LTS”字段，即可快速搜索到日志。

图 17-7 搜索日志



- 方式三：在“可视化”中输入SQL语句，不仅可以过滤审计日志，还可以统计审计日志的总条数。

图 17-8 SQL 语句查询日志





# 18 在 CTS 控制台无法创建追踪器

## 问题描述

在CTS控制台创建追踪器，系统报错。

## 操作步骤

- 步骤1** 键入F12查看报错信息。如果是请求没有发送，查看是否浏览器安装了拦截插件，关闭插件后可以正常创建。
- 步骤2** 如果用户有权限仍无法创建追踪器，在中心region（北京四）查看是否开通CTS，如未开通则需要使用主账号在中心region开通CTS后创建追踪器。
- 步骤3** 以上步骤确认正确后，依然无法创建追踪器，可以提交工单，联系华为技术工程师为您解答。

----结束

# 19 使用 IAM 用户无法开通 CTS 怎么办?

## 问题描述

使用IAM用户开通CTS失败。

## 操作步骤

**步骤1** 查看IAM用户是否有权限。

是：继续执行[步骤2](#)。

否：联系CTS管理员（主账号或admin用户组中的用户）对IAM用户授予CTS FullAccess权限，授权方法请参见[给IAM用户授权](#)。

**步骤2** IAM用户有权限仍无法创建CTS，则需在中心region查看是否开通CTS，没开通需要主账号在中心region开通CTS。

----结束

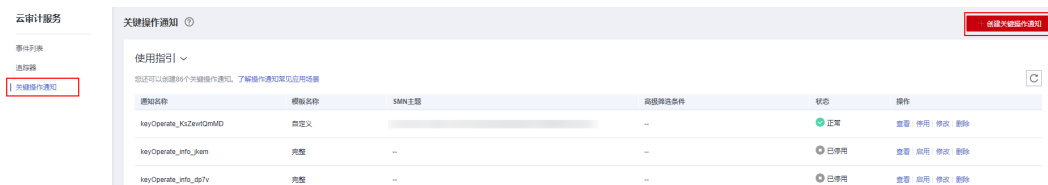
# 20 如何给云硬盘添加告警通知?

## 问题描述

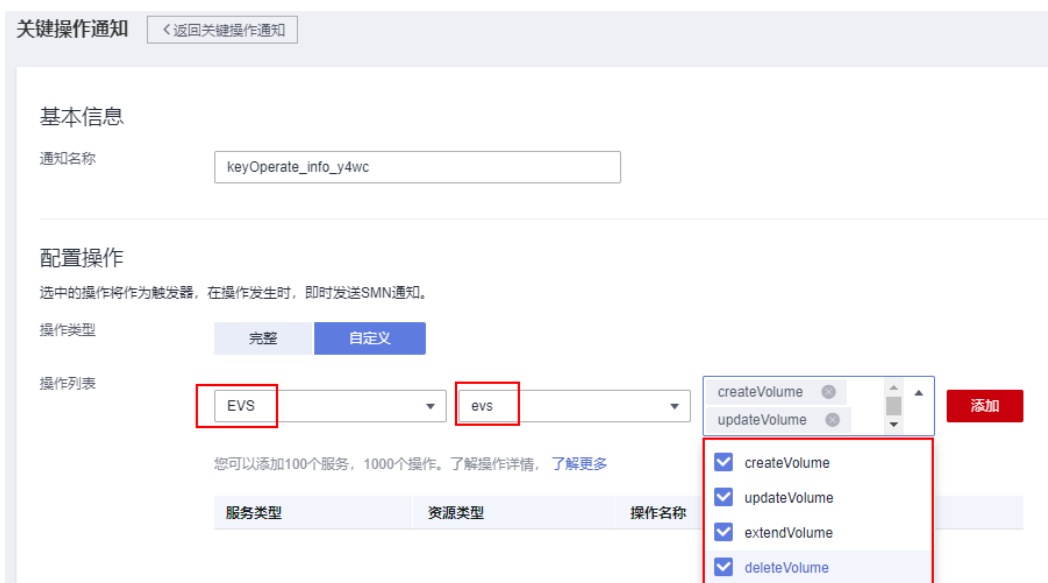
如何给云硬盘的操作添加告警通知。

## 操作步骤

**步骤1** 登录云审计控制台，单击左侧的关键操作通知，然后单击页面右上角的“创建关键操作通知”。



**步骤2** 在“配置操作”模块选择“自定义操作”，依次勾选“EVS > evs”的四个关键操作名称，即可对云硬盘的操作添加告警通知。



----结束

# 21 可以接收重复的事件吗？

---

云审计服务支持向客户的OBS存储桶交付至少一次订阅事件。在某些情况下，云审计服务可能会多次发送同一事件。因此，客户可能会看到重复的事件。


# 22 跨租户密钥授权 OBS 桶转储失败怎么办？

## 问题描述

租户A通过DEW密钥授权机制，通过用户ID方式将DEW密钥共享给另外一个租户的子用户B。用户B创建了使用租户A DEW密钥加密的OBS桶，用户B在配置CTS系统追踪器时，选择转储到该加密OBS桶后，会配置失败。

## 操作步骤


**步骤1** 登录用户B的管理控制台。

**步骤2** 单击左上角服务列表 ，选择“管理与监管 > 统一身份认证服务 IAM”。

**步骤3** 在左侧导航栏选择“委托”，在右上方搜索框输入CTS服务委托“cts\_admin\_trust”，获取到委托ID。



**步骤4** 登录租户A的管理控制台。

**步骤5** 单击左上角服务列表 ，选择“安全与合规 > 数据加密服务 DEW”。

**步骤6** 在密钥管理页面，单击要授权的密钥名称。

**步骤7** 在授权页签单击“创建授权”，在用户ID框内填写步骤3中获取到的cts\_admin\_trust委托ID。



创建授权

密钥ID: 40df0625-5c48-417d-8e30-e2a38d984fc1

★ 被授权对象: **用户** | 账号

28ddc37db413480[掩码]9f305bcd

被授权用户ID可在被授权用户控制台的“我的凭证”中获取。


授权名称: 可填入被授权用户名称

授权操作   全选

<input type="checkbox"/> 创建不含明文数据密钥	<input type="checkbox"/> 查询密钥信息
<input type="checkbox"/> 创建数据密钥	<input type="checkbox"/> 创建授权
<input type="checkbox"/> 加密数据密钥	<input type="checkbox"/> 解密数据密钥
<input type="checkbox"/> 退役授权	<input type="checkbox"/> 加密数据
<input type="checkbox"/> 解密数据	

确定 取消

**步骤8** 登录用户B的管理控制台。

**步骤9** 单击左上角服务列表 ，选择“管理与监管 > 云审计服务 CTS”。

**步骤10** 在配置追踪器转储页面，选择上述设置了DEW共享密钥的OBS桶，即可配置转储。

----结束

# 23 cts\_admin\_trust 委托是否包含 OBS 授权?

## 问题描述

登录统一身份认证服务，查看cts\_admin\_trust委托的授权记录，只显示了KMS和SMN的授权，没有显示OBS的授权。

## 解决方案

cts\_admin\_trust委托没有显示OBS授权，但实际包含了OBS授权，用户可以正常使用。

统一身份认证服务的cts\_admin\_trust委托实际包含的权限如下：

- OBS Administrator
- KMS Administrator
- SMN Administrator