



天翼云 3.0 • 云审计服务 用户使用指南

中国电信股份有限公司云计算分公司

目 录

1 简介.....	1
1.1 概念	1
1.1.1 什么是云审计服务?	1
1.1.2 追踪器	2
1.1.3 事件	2
1.1.4 事件列表	2
1.1.5 事件文件	2
1.1.6 事件文件完整性校验	3
1.1.7 区域	4
1.1.8 项目	4
1.2 工作原理	4
1.3 使用场景	5
1.4 服务资费	5
1.5 访问云审计服务	6
2 入门.....	7
2.1 开启云审计服务	7
2.2 查看追踪事件	8
2.3 查看已归档事件	9
2.4 对追踪事件进行关键字查询	11
3 管理.....	13
3.1 配置追踪器	13
3.2 停用/启用追踪器	15
3.3 删除追踪器	16
4 云审计服务应用示例	17
4.1 安全审计	17
4.2 问题定位	18
4.3 资源跟踪	19
5 云审计服务事件参考	20
5.1 事件结构	20

5.2 事件样例	22
6 常见问题.....	25
6.1 一个租户下可以开通多个追踪器吗?	25
6.2 事件列表用于记录哪些信息?	26
6.3 事件列表中的信息可以删除吗?	26
6.4 用户云账户欠费给云审计服务带来的影响?	26
6.5 哪些用户应该开通云审计服务?	26
6.6 事件文件可以存储多长时间?	26
6.7 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?	26
6.8 云审计服务是否支持事件文件的关键字验证?	27
6.9 启用云审计服务是否会影响其他云服务资源的性能?	27
6.10 为什么查看事件窗口中, 有些事件的 IP、code、request、response 和 message 字段为空?	27
6.11 为什么事件列表中有些事件的资源 ID 为超链接可以跳转, 有些为非超链接?	27
6.12 为什么事件列表中的某些操作被记录了两次?	27
6.13 为什么在事件列表中按照操作用户进行筛选时, 存在 user_account/op_service 用户?	28
6.14 关键操作通知服务支持哪些服务?	28
6.15 对事件文件进行 KMS 加密是否收费?	28

1 简介

- 1.1 概念
- 1.2 工作原理
- 1.3 使用场景
- 1.4 服务资费
- 1.5 支持的服务
- 1.6 访问云审计服务

1.1 概念

1.1.1 什么是云审计服务？

日志审计模块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。在信息系统逐步云化的背景下，包括我国 SAC/TC 在内的全球各级信息、数据安全管理部门已对此发布多份标准，如：ISO IEC27000、GB/T 20945-2013、COSO、COBIT、ITIL、NISTSP800 等。

云审计服务（Cloud Trace Service，以下简称 CTS），是天翼云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

云审计服务的功能主要包括：

- 记录审计日志：支持记录用户通过管理控制台或 API 接口发起的操作，以及各服务内部自触发的操作。
- 审计日志查询：支持在管理控制台对 7 天内操作记录按照事件来源、事件名称、操作类型、资源名称/ID、事件状态和时间范围等多个维度进行组合查询。
- 审计日志转储：支持将审计日志周期性的转储至对象存储服务（，转储时会按照服务维度压缩审计日志为事件文件。
- 事件文件加密：支持在转储过程中使用密钥管理服务（Key Management Service，简称 KMS）中的密钥对事件文件进行加密。

- 关键操作通知：支持在检测到部分关键操作时，使用消息通知服务（Simple Message Notification，简称 SMN）向用户发送邮件、短信通知。

1.1.2 追踪器

使用云审计服务前需要开通云审计服务，开通云审计服务时系统会自动创建一个追踪器。该追踪器会自动识别并关联当前租户所使用的所有云服务，并将当前租户的所有操作记录在该追踪器中。

目前，一个租户仅支持创建一个追踪器。

1.1.3 事件

事件即云审计服务追踪并保存的云服务资源的操作日志。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。

事件分为以下两类：

- 追踪事件
指近 7 天的操作记录。
- 已归档事件
指已保存至对象存储服务的历史操作记录。

1.1.4 事件列表

事件列表记录了租户对云服务资源新建、修改、删除等操作的详细信息。事件列表最多显示近 7 天的事件。

1.1.5 事件文件

事件文件是系统自动生成的事件集，云审计服务将按照服务、转储周期两个维度，生成多个事件文件，同步保存至用户指定的对象存储服务中。

通常情况下，单个服务在单个转储周期内产生的所有事件仅会压缩生成一个事件文件，但在事件数量较多时，系统会根据当前负载情况调整每个事件文件包含的事件数。

事件文件的格式为 json，呈现事件的原始内容如图 1-1 所示。

图1-1 事件文件示例

```
{
  "time": 1491482532828,
  "user": {
    "id": "59f40829165447fb9470b56f41dff599",
    "name": " ",
    "domain": {
      "name": " ",
      "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
    }
  },
  "request": {
    "bucket_name": "obs-570f",
    "file_prefix_name": "-RsU",
    "status": "disabled"
  },
  "response": {
    "bucket_name": "obs-570f",
    "file_prefix_name": "-RsU",
    "status": "disabled",
    "tracker_name": "system"
  },
  "service_type": "CTS",
  "resource_type": "tracker",
  "resource_name": "system",
  "source_ip": " ",
  "trace_name": "updateTracker",
  "trace_type": "ConsoleAction",
  "api_version": "1.0",
  "record_time": 1491482532857,
  "trace_id": "7519ef09-lac6-11e7-8cc0-3d812829baf6",
  "trace_status": "normal"
},
{
  "time": 1491482535203,
  "user": {
    "id": "59f40829165447fb9470b56f41dff599",
    "name": " ",
    "domain": {
      "name": " ",
      "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
    }
  },
  "request": {
    "bucket_name": "obs-570f",
    "file_prefix_name": "-RsU",
    "status": "enabled"
  },
  "response": {
    "bucket_name": "obs-570f",
    "file_prefix_name": "-RsU",
    "status": "enabled",
    "tracker_name": "system"
  },
  "service_type": "CTS",
  "resource_type": "tracker",
  "resource_name": "system",
  "source_ip": " ",
  "trace_name": "updateTracker",
  "trace_type": "ConsoleAction",
  "api_version": "1.0",
  "record_time": 1491482535224,
  "trace_id": "76831bfb-lac6-11e7-98ff-a1036f244dcd",
  "trace_status": "normal"
}
```

获取事件文件的方法请参见 2.3 查看已归档事件，事件文件中事件结构的关键字段详解，请参见 5.1 事件结构。

1.1.6 事件文件完整性校验

在安全和事故调查中，通常由于事件文件被删除或者被私下篡改，而导致操作记录的真实性受到影响，无法对调查提供有效真实的依据。因此云审计服务适时推出了事件文件完整性校验功能，旨在帮助您确保事件文件的真实性。

事件文件完整性校验功能使用业界标准算法构建，对事件文件生成原始哈希值，当事件文件被修改或者删除时，该哈希值就会发生改变，通过对哈希值进行追踪查看就能确定事件文件是否被修改；同时采用 RSA 算法对摘要文件进行签名，保证摘要文件不被修改。这样任何对事件文件进行修改或者删除的蛛丝马迹都会被云审计服务完整记录下来。

启用事件文件完整性校验功能后，云审计服务会在每个小时将上一个小时内所有事件文件的哈希值生成一个摘要文件，并将该摘要文件同步存储至当前追踪器配置的对象存储服务中。

云审计使用公有和私有密钥对每个摘要文件进行签名，摘要文件转储到对象存储服务后，您可以使用公有密钥校验摘要文件。

1.1.7 区域

区域指安装云审计服务的服务器所在的物理区域，同一物理区域的可用分区之间内网是互通的。

1.1.8 项目

项目用于将 OpenStack 的资源（计算资源、存储资源和网络资源）进行分组和隔离。一个帐户下可以创建多个项目，项目可以是一个部门或者一个项目组。

1.2 工作原理

云审计服务直接对接云上的其他服务，记录租户的云服务资源的操作信息，实现云帐户操作各个云服务资源动作和结果的实时记录功能，并将记录内容以事件形式实时保存至对象存储服务中。

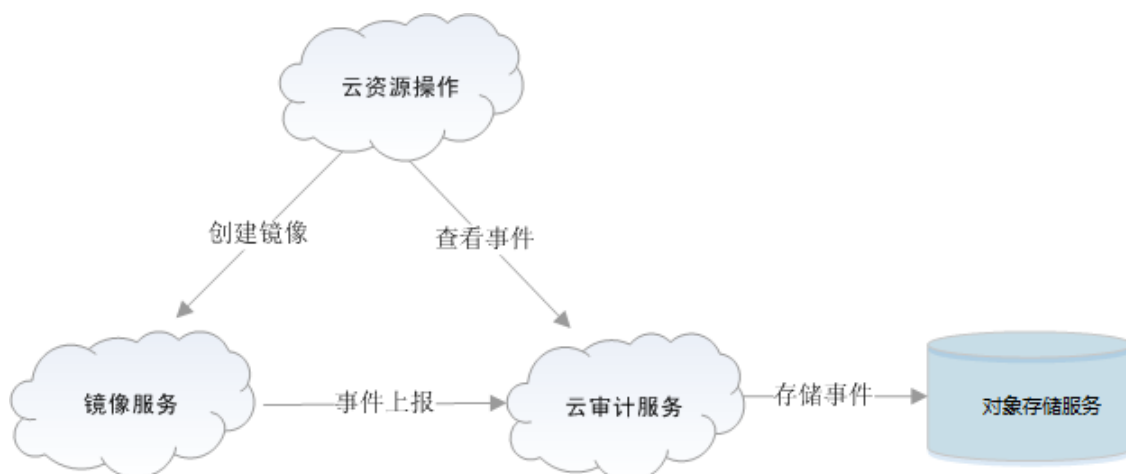
开通云审计服务时关联的追踪器可以跟踪记录事件文件。如已配置对象存储服务，事件文件将保存在对象存储服务中创建的对象存储服务中。

用户可以对事件文件执行以下两种操作：

- 事件文件的创建和保存：
 - 当用户在弹性云服务器、云硬盘服务、镜像服务等其它与云审计完成对接的服务中，进行了增加、删除、修改类型的操作时，被操作的服务会自动记录操作动作及操作结果，并按照指定的格式发送事件文件到云审计服务完成事件归档。
 - 云审计服务管理控制台会保存最近 7 天的操作记录，如已配置对象存储服务，云审计服务会定期将操作记录同步保存到用户定义的对象存储服务中进行长期保存。
- 事件文件查询：
 - 在“事件列表”页面，用户可以按照通过系统自带的条件和时间过滤功能，查询最近 7 天的操作记录。同时支持直接跳转到云日志服务页面，对事件文件按照关键字进行模糊查询。
 - 若要查询 7 天前的操作记录且已配置对象存储服务，可以在对应的对象存储服务中下载事件文件进行查看。
 - 在云审计服务页面的追踪器界面，用户可以对追踪器进行启用、停用、删除、配置等操作。

以用户创建镜像为例，在用户使用云平台的镜像服务执行创建镜像的操作过程中，镜像服务会将用户操作事件上报至云审计服务，如已配置对象存储服务，云审计服务将事件转存至对象存储服务中。用户也可以通过云审计服务的事件列表查看事件文件。云审计服务工作原理示意如图 1-2 所示。

图1-2 云审计服务工作原理示意图



1.3 使用场景

云审计服务主要有以下四种应用场景

- 合规审计**

云审计服务所提供的操作日志记录、查询等功能及安全控制能力，是企事业单位特别是金融、支付类企业满足认证要求的必备条件，例如：PCI DSS、GB/T 24589.1、COSO 认证等。
- 资源跟踪**

云审计服务支持按资源维度检索，可跟踪某一云资源从产生到注销的完整生命周期中的所有操作、变更，并呈现每次操作或变更的来源信息和操作结果，以供用户记录、追溯资源的真实使用情况。
- 问题定位**

在其他云资源出现故障时，可根据云审计记录的故障发生时间、操作用户等信息，快速检索事发时的可疑操作及操作结果，极大程度的降低问题发现、定位和解决的时间、人力成本。
- 安全分析**

可根据企事业单位需求，设定高危操作或关键操作范围，定期检索何人、何时、何 IP 发起了需要被关注的操作请求，继而通过这些关键信息便捷地进行安全分析。

1.4 服务资费

云审计服务基础功能免费，包括开通追踪器、事件跟踪以及 7 天内事件的存储和检索。同时云审计服务与天翼云其他云服务组合使用，为您提供事件文件转储、事件文件加密、关键操作通知等增值服务，这些增值服务可能产生额外费用，具体由提供该功能的服务结算。

通常情况下，云审计服务产生的增值服务费用很低，因此建议您根据实际需要搭配使用。

1.5 访问云审计服务

天翼云提供了 Web 化的服务管理平台，支持通过管理控制台方式访问云审计服务。如果用户已注册天翼云，可直接登录管理控制台，选择管理与部署下的“云审计服务”。

2 入门

- 2.1 开启云审计服务
- 2.2 查看追踪事件
- 2.3 查看已归档事件
- 2.4 对追踪事件进行关键字查询
- 2.5 校验云审计事件文件完整性

2.1 开启云审计服务

操作场景


使用云审计服务前需要开启云审计服务，开启云审计服务后系统会自动创建一个追踪器，系统记录的所有操作将关联在该追踪器中。目前，一个云账户系统仅支持创建一个追踪器。

本节介绍如何开启云审计服务。

前提条件

开通对象存储服务。

操作步骤

1. 登录管理控制台。
2. 单击  服务列表，选择“管理与部署 > 云审计服务”进入云审计服务信息页面。
3. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
4. 单击“开启云审计服务”。
5. 在弹出的开启云审计服务详情页面，选择已开通的对象存储服务，完成开启云审计服务，系统会自动分配一个追踪器。

开启云审计服务成功后，您可以在追踪器页面查看已创建的追踪器的详细信息。

2.2 查看追踪事件

操作场景

在您开启了云审计服务后，系统开始记录云服务资源的操作。云审计服务管理控制台保存最近 7 天的操作记录。

本节介绍如何在云审计服务管理控制台查看最近 7 天的操作记录。

操作步骤



1. 登录管理控制台。
2. 单击  服务列表，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
 - 事件来源、资源类型和筛选类型。
在下拉框中选择查询条件。
其中筛选类型选择事件名称时，还需选择某个具体的事件名称。
选择资源 ID 时，还需选择或者手动输入某个具体的资源 ID。
选择资源名称时，还需选择或手动输入某个具体的资源名称。
 - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
 - 事件级别：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
 - 起始时间、结束时间：可通过选择时间段查询操作事件。
5. 在需要查看的记录左侧，单击  展开该记录的详细信息，展开记录如图 2-1 所示。

图2-1 展开记录

事件名称	资源类型	事件来源	资源ID	资源名称	事件级别	操作用户	事件记录时间	操作
login	user	IAM	26e96eda18034ae9a44130b...		normal		2017/06/29 10:22:32 GMT+08...	查看事件
事件ID: ce90cce3-5c71-11e7-910d-57ac1cd228ee								
事件地址: 2017/06/29 10:20:52 GMT+08:00								
事件产生时间: 2017/06/29 10:20:52 GMT+08:00								

6. 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图 2-2 所示，显示了该操作事件结构的详细信息。

图2-2 查看事件

查看事件

```
{
  "time": "2017/08/17 10:20:31 GMT+08:00",
  "service_type": "CTS",
  "resource_type": "tracker",
  "api_version": "1.0",
  "user": {
    "id": "26e96eda18034ae9a44130bacb967b96",
    "name": " ",
    "domain": {
      "name": " ",
      "id": "1f9b9ba51f6b4061bd5c1736b28469f8"
    }
  },
  "trace_type": "ConsoleAction",
  "source_ip": " ",
  "request": {
    "bucket_name": "28ab",
    "file_prefix_name": "26ze",
    "is_obs_created": true,
    "smn": {
      "is_support smn": true
    }
  }
}
```

关于云审计服务事件结构的关键字段详解，请参见 5.1 事件结构和 5.2 事件样例。

2.3 查看已归档事件

操作场景

云审计服务会定时将跟踪到的事件以事件文件的形式按周期保存至对象存储服务。事件文件是按照服务、转储周期两个维度生成事件集，系统会根据当前负载情况调整每个事件文件包含的事件数。

本节介绍如何在对象存储服务中通过下载事件文件查看已保存至对象存储服务的历史操作记录。

前提条件

已在云审计服务中成功配置追踪器。配置追踪器方法请参见 3.1 配置追踪器章节。

操作步骤

1. 登录管理控制台。

2. 单击 **服务列表**，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。
3. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
4. 单击“OBS 桶”下的指定的 OBS 桶名称，如图 2-3 所示，页面跳转到 OBS 管理控制台。

图2-3 选择 OBS



5. 在 OBS 桶中选择需要查看的历史事件，按照事件文件存储路径选择“OBS 桶名 > CloudTraces > 地区标示 > 时间标示: 年 > 时间标示: 月 > 时间标示: 日 > 服务类型目录”，如图 2-4 所示，单击右侧的“下载”，文件将下载到浏览器默认下载路径，如需要将事件文件保存到自定义路径下，请单击右侧的“下载为”按钮。

– 事件文件存储路径:

OBS 桶名>CloudTraces>地区标示>时间标示: 年>时间标示: 月>时间标示: 日>服务类型目录

例如: *User Define>CloudTraces>region>2016>5>19>ECS*

– 事件文件命名格式:

操作事件文件前缀_CloudTrace_地区标示_日志文件上传至 OBS 的时间标示: 年-月-日 T 时-分-秒 Z_系统随机生成字符.json.gz

例如: *File Prefix_CloudTrace_region_2016-05-30T16-20-56Z_21d36ced8c8af71e.json.gz*



说明

OBS 桶名和事件前缀为用户设置，其余参数均为系统自动生成。

关于云审计服务事件结构的关键字段详解，请参见 5.1 事件结构和 5.2 事件样例。

图2-4 查看事件文件内容



6. 文件下载到本地后，通过解压可以得到与压缩包同名的 json 文件，下载解压后的 json 文件内容如图 2-5 所示，通过记事本等 txt 文档编辑软件即可查看到保存的追踪日志信息。

图2-5 下载解压后的json 文件

```
[{"time": 1491482532828,
  "user": {
    "id": "59f40829165447fb9470b56f41dff599",
    "name": " ",
    "domain": {
      "name": " ",
      "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
    }
  },
  "request": {
    "bucket_name": "obs-570f",
    "file_prefix_name": "-RsU",
    "status": "disabled"
  },
  "response": {
    "bucket_name": "obs-570f",
    "file_prefix_name": "-RsU",
    "status": "disabled",
    "tracker_name": "system"
  },
  "service_type": "CIS",
  "resource_type": "tracker",
  "resource_name": "system",
  "source_ip": " ",
  "trace_name": "updateTracker",
  "trace_type": "ConsoleAction",
  "api_version": "1.0",
  "record_time": 1491482532857,
  "trace_id": "7519ef09-lac6-11e7-8cc0-3d812829baf6",
  "trace_status": "normal"
},
{"time": 1491482535203,
  "user": {
    "id": "59f40829165447fb9470b56f41dff599",
    "name": " ",
    "domain": {
      "name": " ",
      "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
    }
  },
  "request": {
    "bucket_name": "obs-570f",
    "file_prefix_name": "-RsU",
    "status": "enabled"
  },
  "response": {
    "bucket_name": "obs-570f",
    "file_prefix_name": "-RsU",
    "status": "enabled",
    "tracker_name": "system"
  },
  "service_type": "CIS",
  "resource_type": "tracker",
  "resource_name": "system",
  "source_ip": " ",
  "trace_name": "updateTracker",
  "trace_type": "ConsoleAction",
  "api_version": "1.0",
  "record_time": 1491482535224,
  "trace_id": "76831bfb-lac6-11e7-98ff-a1036f244dcd",
  "trace_status": "normal"
}]
```

2.4 对追踪事件进行关键字查询

操作场景

当某个云服务出现故障时，通过对事件文件进行关键字查询，帮助用户快速定位问题。

本节介绍如何通过云审计服务跳转到云日志服务页面，借助日志搜索功能对最近 7 天的操作记录进行关键字查询。

前提条件

已经通过云日志服务公测申请，申请公测方法参见《云日志服务用户指南》中的“申请公测”章节。

3 管理

- 3.1 配置追踪器
- 3.2 停用/启用追踪器
- 3.3 删除追踪器

3.1 配置追踪器

操作场景

云审计服务管理控制台支持对已创建的追踪器增加 OBS 转储和关键事件操作通知的相关配置。

- 配置 OBS 转储：用户可以选择是否将已记录的事件发送到 OBS 桶永久保存。
 - 用户可选择已存在的 OBS 桶或直接通过配置页面新建 OBS 桶。云审计服务会自动为该 OBS 桶挂载转储所需的桶策略。



说明

由于云审计服务需要高频次的访问转储的 OBS 桶，因此必须选择使用标准存储类型的 OBS 桶。

- “操作事件文件前缀”用于标识被转储的事件文件，该字段支持用户自定义，会自动添加在转储事件文件的文件名前端，方便用户快速进行筛选。
 - “开启文件校验”可以检验转储至 OBS 桶的数据是否被篡改，保障事件文件的完整性。
 - 用户可以选择是否对待转储的事件文件加密，提升事件文件存储的安全性，加密密钥由 KMS 提供。
- 配置关键事件通知：用户可以选择是否在发生关键操作时向用户发送邮件、短信通知，用户可自定义发送的通知主题。该功能由云审计服务触发，消息通知服务（SMN）完成通知发送，因此在启用该配置项前，需要启用消息通知服务，并创建通知主题。

目前云审计服务支持发送通知的关键操作如表 3-1 所示。

表3-1 云审计服务支持的事件操作通知的操作列表

资源类型	操作名称	事件名称
ECS	创建云服务器	createServer
	删除云服务器	deleteServer
VPC	创建 VPC	createVpc
	删除 VPC	deleteVpc
EVS	创建磁盘	createVolume
	删除磁盘	deleteVolume
KMS	创建密钥	createKey
	密钥删除风险提示	deleteKeyRiskTips
IAM	用户登录	login


配置追踪器完成后，新规则立即生效。

本节介绍如何配置追踪器。

前提条件

已开启云审计服务。

操作步骤

1. 登录管理控制台。
2. 单击  服务列表，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。
3. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
4. 在追踪器信息右侧，单击操作下的“配置”。
 - 当选择是否转储 OBS 为“转储”时，
 - 您可以选择已存在的 OBS 桶或直接通过配置页面新建 OBS 桶。
 - 您可以选择是否开启文件校验功能，以保障事件文件的完整性。
 - 您可以选择是否为转储在 OBS 桶中的文件进行加密处理，并选择预先创建的密钥。

如果配置 OBS 桶转储为“不转储”时，则无需配置相应参数。
 - 您可以选择是否开启“关键事件通知”功能。
 - 当选择“发送”时，需要配置通知主题和触发条件。
 - 当“关键事件通知”选择“不发送”时，无需配置相应参数。

参数配置如下表 3-2 所示。

表3-2 参数说明

参数	解释	取值样例
OBS 桶	选择用于存储操作的 OBS 桶名称。	buckert-001
操作事件文件前缀	用于标识存储在 OBS 桶中的日志文件，为可选参数。手动命名可包含英文字母、数字、中划线、下划线、小数点，长度不超过 64 位。	-
密钥名称	用于标识加密转储在 OBS 桶中事件文件的密钥名称。	-
通知主题	选择用于发送通知的 SMN 的主题	-
触发条件	支持删除或者创建操作记录发送通知，且至少选择一个触发条件。	-

5. 单击“确定”，完成配置追踪器。

追踪器配置成功后，您可以在追踪器信息页面查看配置的追踪器的详细信息。



说明

因为 CTS 所存储的事件是周期性转储到 OBS 桶的，因此当您配置了追踪器所对应的 OBS 桶后，当前转储周期内（通常为数分钟）已收到事件会转储到配置后的 OBS 桶中。例如当前转储周期为 12:00~12:05，用户在 12:02 分修改了当前追踪器对应的 OBS 桶，那么 12:00~12:02 分之间收到的事件会在 12:05 分时转储到新配置的 OBS 桶中。

3.2 停用/启用追踪器

操作场景


云审计服务管理控制台支持停用已创建的追踪器。追踪器停用成功后，系统将不再记录新的操作，但是您依旧可以查看已有的操作记录。

本节介绍如何停用追踪器。

前提条件

已在云审计服务中成功创建追踪器。

操作步骤

1. 登录管理控制台。
2. 单击  服务列表，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。
3. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
4. 在追踪器信息右侧，单击操作下的“停用”。

5. 单击“确定”，完成停用追踪器。
6. 追踪器停用成功后，操作下的“停用”切换为“启用”。如果您需要重新启用追踪器，单击“启用 > 确定”，则系统重新开始记录新的操作。

3.3 删除追踪器

操作场景

云审计服务管理控制台支持删除已创建的追踪器。删除追踪器对已有的操作记录没有影响，当您重新开通云审计服务后，依旧可以查看已有的操作记录。




删除追踪器一个小时候，用户需要在追踪器对应 OBS 桶中手动删除格式为*:user/* 的桶策略。如 OBS 桶中有多个*:user/* 的桶策略，请联系客服人员进行确认后再删除相关的桶策略。

本节介绍如何删除追踪器。

前提条件

已在云审计服务中成功创建追踪器。

操作步骤

1. 登录管理控制台。
2. 单击  服务列表，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。
3. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
4. 在追踪器信息右侧，单击操作下的“删除”。
5. 单击“确定”，完成删除追踪器。

4 云审计服务应用示例

4.1 安全审计

4.2 问题定位

4.3 资源跟踪

4.1 安全审计

操作场景


根据云审计服务收集的日志记录，通过查询具体的、符合某一特征的记录，执行安全分析，判断用户的操作是否符合权限要求。

前提条件

已开通云审计服务且追踪器状态正常。开通云审计服务请参考章节 2.1 开启云审计服务。

操作步骤

以审计最近两周云硬盘服务的创建和删除操作为例：

1. 以管理员权限登录管理控制台。
2. 单击  服务列表，选择“管理与部署 > 云审计服务”，进入云审计服务详情页面。
3. 单击左侧导航树的“事件列表”，进入事件列表界面。
4. 在事件列表界面单击“筛选”，显示过滤条件查询框，依次选择“事件来源” > “资源类型” > “筛选类型”，单击“查询”按钮执行搜索，查看过滤结果。过滤条件查询示例：依次选择“evs” > “evs” > “按事件名称” > “createVolume” 或 “evs” > “evs” > “按事件名称” > “deleteVolume”，单击“查询”按钮执行搜索，查询所有创建或删除 EVS 的操作。
5. 单击左侧导航树的“追踪器”，进入追踪器详情页面，获取 OBS 桶名。
6. 参照章节 2.3 查看已归档事件下载 7 天之前或者所有的事件。

7. 在操作记录中，以 createVolume 和 deleteVolume 作为关键字检索，找到对应记录。
8. 从第 4 步和第 7 步的结果中，抽取操作用户信息，甄别没有授权的操作，即用户越权操作，或不符合用户自身安全操作规范的操作。

4.2 问题定位

操作场景


当现网某个特定资源或动作出现问题，可根据云审计服务收集的日志记录，通过查询对应时间、对应资源的操作记录，查看当时的请求动作和响应，支撑问题定位分析。

前提条件

已开通云审计服务且追踪器状态正常。开通云审计服务请参考章节 2.1 开启云审计服务。

操作步骤

以现网某个弹性云服务器在某日上午发生故障后的辅助定位为例：

1. 以管理员权限登录管理控制台。
2. 单击  服务列表，选择“管理与部署 > 云审计服务”，进入云审计服务详情页面。
3. 单击左侧导航树的“事件列表”，进入事件列表界面。
4. 在事件列表界面单击“筛选”，显示过滤条件查询框，依次选择“事件来源” > “资源类型” > “筛选类型”，单击“查询”，查看过滤结果。




说明

过滤条件查询示例：依次选择“ecs” > “ecs” > “Resource id” > “问题虚拟机 ID”，并在右上角时间条件设置窗口设置时间为某日上午 6 点到中午 12 点，查看过滤结果。

5. 逐条查看操作记录，注意请求的类型和响应结果，特别关注“事件级别”为 warning 和 incident 的事件，以及相应结果为失败的事件。

以现网进行创建弹性云服务器操作失败报错后的辅助定位为例：

1. 以管理员权限登录管理控制台。
2. 单击  服务列表，选择“管理与部署 > 云审计服务”，进入云审计服务详情页面。
3. 单击左侧导航树的“事件列表”，进入事件列表界面。
4. 根据创建虚拟机弹性云服务器失败的操作，设置过滤条件：“ecs” > “ecs” > “事件级别” > “Warning”，在结果中查看事件名称为“createSingleServer”操作记录事件。
5. 查看操作记录，重点关注响应中的错误提示信息，根据错误提示代码或错误提示信息进行问题定位分析。

4.3 资源跟踪

操作场景


根据云审计服务所记录的操作记录，可以查看任意云服务资源在其整个生命周期内的操作记录，并检视具体操作的细节。

前提条件

已开通云审计服务且追踪器状态正常。开通云审计服务请参考章节 2.1 开启云审计服务。

操作步骤

以查看某个弹性云服务器的所有操作记录为例：

1. 以管理员权限登录管理控制台。
2. 单击  服务列表，选择“管理与部署 > 云审计服务”，进入云审计服务详情页面。
3. 单击左侧导航树的“事件列表”，进入事件列表界面。
4. 在事件列表界面单击“筛选”，显示过滤条件查询框，依次选择“事件来源” > “资源类型” > “筛选类型”，单击“查询”执行搜索，查看过滤结果。



说明

过滤条件查询示例：依次选择“ecs” > “ecs” > “Resource id” > “问题虚拟机 ID”，单击“查询”执行搜索，查看最近 7 天的操作记录。

5. 单击左侧导航树的“追踪器”，进入追踪器详情页面，获取 OBS 桶名。
6. 参照章节 2.3 查看已归档事件下载 7 天之前或者所有的事件。
7. 从第 4 步和第 6 步的结果中，检视该弹性云服务器的所有操作和变更记录。

5 云审计服务事件参考

5.1 事件结构

5.2 事件样例

5.1 事件结构

云审计服务用于标示每个操作事件关键字段的详细信息，具体如表 5-1 所示。



说明

- 为方便用户，部分字段在管理控制台呈现时进行了格式优化。
- 本章节将基于 CTS 管理控制台进行介绍和描述。

表5-1 事件的关键字段

字段名称	是否必选	类型	描述
time	是	Date	事件发生时间。以当地标准时间（采用格林威治时间加当地时区形式）进行展示，例如：2016/12/08 11:24:04 GMT+08:00。在接口中，该字段以时间戳格式进行传输和存储。该字段为格林威治时间 1970 年 01 月 01 日 00 时 00 分 00 秒（北京时间 1970 年 01 月 01 日 08 时 00 分 00 秒）至现在的总毫秒数。
user	是	Structure	发起操作的云账户信息。 在界面事件列表中，该字段于 Operator 列呈现。 该字段在 API 接口中以 String 类型进行传输和存储。
request	否	Structure	操作的请求内容。 该字段在 API 接口中以 String 类型进行传输和存储。

字段名称	是否必选	类型	描述
response	否	Structure	操作的响应内容。 该字段在 API 接口中以 String 类型进行传输和存储。
service_type	是	String	操作来源。
resource_type	是	String	资源类型。
resource_name	否	String	资源名称。
resource_id	否	String	资源的唯一标识。
source_ip	是	String	发起本次操作的用户的 IP，若为系统内调用，则为空。
trace_name	是	String	操作名称。
trace_status	是	String	操作事件等级，分为 normal（正常）、warning（警告）和 incident（事故）。
trace_type	是	String	操作类型，分为如下三种： ConsoleAction 表示通过云管理控制台执行的操作。 SystemAction 表示云系统内部触发的操作。 ApiCall 表示调用 ApiGateway 触发的操作。
api_version	否	String	作为操作来源的云服务的 API 版本号。
message	否	Structure	备注信息。
record_time	是	Number	记录操作的时间，表示方式为时间戳。
trace_id	是	String	操作的唯一标识。
code	否	Number	事件 http 返回码例如 200,400
request_id	否	String	记录本次请求的 request id
location_info	否	String	记录本次请求出错后，问题定位所需要的辅助信息
endpoint	否	String	该操作涉及云资源的详情页面的 endpoint
resource_url	否	String	该操作涉及云资源的详情页面的访问链接（不含 endpoint）

5.2 事件样例

以下提供云审计服务所收集事件的两个页面样例，并对其中常用的观察点进行了描述，以方便用户更直观的理解事件信息。其他服务所产生的事件可参照以下样例理解。

详细的字段解释可参考 5.1 事件结构章节。

创建云服务器实例

```
{
  "time": "2016/12/01 11:07:28 GMT+08:00",
  "user": {
    "name": "aaa/op_service",
    "id": "f2fe9fac63414a35a7d03108d5f1ea73",
    "domain": {
      "name": "aaa",
      "id": "1f9b9ba51f6b4061bd5c1736b28469f8"
    }
  },
  "request": {
    "server": {
      "name": "as-config-15f1_XW068TFC",
      "imageRef": "b2b2c7dc-bbb0-4d6b-81dd-f0904023d54f",
      "flavorRef": "m1.tiny",
      "personality": [],
      "vpcid": "e4c374b9-3675-482c-9b81-4acd59745c2b",
      "nics": [
        {
          "subnet_id": "fff89132-88d4-4e5b-9e27-d9001167d24f",
          "nictype": null,
          "ip_address": null,
          "binding:profile": null,
          "extra_dhcp_opts": null
        }
      ],
      "adminPass": "*****",
      "count": 1,
      "metadata": {
        "op_svc_userid": "26e96eda18034ae9a44130bacb967b96"
      },
      "availability_zone": "az1.dc1",
      "root_volume": {
        "volumetype": "SATA",
        "extendparam": {
          "resourceSpecCode": "SATA"
        },
        "size": 40
      },
      "data_volumes": [],
      "security_groups": [
        {
          "id": "dd597fd7-d119-4994-a22c-891fcfc54be1"
        }
      ]
    }
  },
  "response": {
    "server": {
      "name": "as-config-15f1_XW068TFC",
      "imageRef": "b2b2c7dc-bbb0-4d6b-81dd-f0904023d54f",
      "flavorRef": "m1.tiny",
      "personality": [],
      "vpcid": "e4c374b9-3675-482c-9b81-4acd59745c2b",
      "nics": [
        {
          "subnet_id": "fff89132-88d4-4e5b-9e27-d9001167d24f",
          "nictype": null,
          "ip_address": null,
          "binding:profile": null,
          "extra_dhcp_opts": null
        }
      ],
      "adminPass": "*****",
      "count": 1,
      "metadata": {
        "op_svc_userid": "26e96eda18034ae9a44130bacb967b96"
      },
      "availability_zone": "az1.dc1",
      "root_volume": {
        "volumetype": "SATA",
        "extendparam": {
          "resourceSpecCode": "SATA"
        },
        "size": 40
      },
      "data_volumes": [],
      "security_groups": [
        {
          "id": "dd597fd7-d119-4994-a22c-891fcfc54be1"
        }
      ]
    }
  }
}
```

```

        "key_name": "KeyPair-3e51"
    },
    "response": {
        "status": "SUCCESS",
        "entities": {
            "server_id": "42d39b4a-19b7-4ee2-b01b-a9f1353b4c54"
        },
        "job_id": "4010b39d58b855980158b8574b270018",
        "job_type": "createSingleServer",
        "begin_time": "2016-12-01T03:04:38.437Z",
        "end_time": "2016-12-01T03:07:26.871Z",
        "error_code": null,
        "fail_reason": null
    },
    "service_type": "ECS",
    "resource_type": "ecs",
    "resource_name": "as-config-15f1_XWO68TFC",
    "resource_id": "42d39b4a-19b7-4ee2-b01b-a9f1353b4c54",
    "source_ip": "",
    "trace_name": "createSingleServer",
    "trace_status": "normal",
    "trace_type": "SystemAction",
    "api_version": "1.0",
    "record_time": "2016/12/01 11:07:28 GMT+08:00",
    "trace_id": "4abc3a67-b773-11e6-8412-8f0ed3cc97c6"
}

```

在以上信息中，可以重点关注如下字段：

- "time": 记录了事件发生的时间，本例中为 12 月 1 日上午 11 点 07 分 28 秒。
- "user": 记录了操作用户的信息，本例中操作用户为企业帐户（domain 字段）aaa 下的用户（name 字段）aaa。
- "request": 记录了创建 ECS 服务器的请求，可以抽取该 ECS 服务器的简单信息，如 name 为 as-config-15f1_XWO68TFC，资源 id 为 e4c374b9-3675-482c-9b81-4acd59745c2b。
- "response": 记录了创建 ECS 服务的返回结果，可以抽取其中的关键信息，如创建结果（status 字段）为 Success，错误码（error_code 字段）和失败原因（fail_reason 字段）均为空（null）。

云硬盘实例

```

{
    "time": "2016/12/01 11:24:04 GMT+08:00",
    "user": {
        "name": "aaa",
        "id": "26e96eda18034ae9a44130bacb967b96",
        "domain": {
            "name": "aaa",
            "id": "1f9b9ba51f6b4061bd5c1736b28469f8"
        }
    },
    "request": "",
    "response": ""
}

```

```
{
  "service_type": "EVS",
  "resource_type": "evs",
  "resource_name": "volume-39bc",
  "resource_id": "229142c0-2c2e-4f01-a1b4-2dfdf1c678c7",
  "source_ip": "10.146.230.124",
  "trace_name": "deleteVolume",
  "trace_status": "normal",
  "trace_type": "ConsoleAction",
  "api_version": "1.0",
  "record_time": "\"2016/12/01 11:24:04 GMT+08:00\"",
  "trace_id": "c529254f-bcf5-11e6-a89a-7fc778a6c92c"
}
```

在以上信息中，可以重点关注如下字段：

- "time": 记录了事件发生的时间，本例中为 12 月 1 日上午 11 点 24 分 04 秒。
- "user": 记录了操作用户的信息，本例中操作用户为企业帐户（domain 字段）aaa 下的用户（name 字段）aaa。
- "request": 非必选字段，此处为空。
- "response": 非必选字段，此处为空。
- "trace_status": 记录了事件的级别，可代替 response 字段提示用户操作结果，本例中为 normal，按 5.1 事件结构章节中约束，即代表操作成功。

6 常见问题

- 6.1 一个租户下可以开通多个追踪器吗？
- 6.2 事件列表用于记录哪些信息？
- 6.3 事件列表中的信息可以删除吗？
- 6.4 用户云账户欠费给云审计服务带来的影响？
- 6.5 哪些用户应该开通云审计服务？
- 6.6 事件文件可以存储多长时间？
- 6.7 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？
- 6.8 云审计服务是否支持事件文件的关键字验证？
- 6.9 启用云审计服务是否会影响其他云服务资源的性能？
- 6.10 为什么查看事件窗口中，有些事件的 IP、code、request、response 和 message 字段为空？
- 6.11 为什么事件列表中有些事件的资源 ID 为超链接可以跳转，有些为非超链接？
- 6.12 为什么事件列表中的某些操作被记录了两次？
- 6.13 为什么在事件列表中按照操作用户进行筛选时，存在 user_account/op_service 用户？
- 6.14 关键操作通知服务支持哪些服务？
- 6.15 对事件文件进行 KMS 加密是否收费？
- 6.16 OBS 桶有标准存储、低频访问存储和归档存储三种类型，哪一种适用于 CTS 存储事件文件？

6.1 一个租户下可以开通多个追踪器吗？

目前，一个租户系统仅支持开通一个追踪器。

6.2 事件列表用于记录哪些信息？

事件列表记录了云账户中对云服务资源新建、配置、删除等操作的详细信息。事件列表不记录查询操作的相关信息。

6.3 事件列表中的信息可以删除吗？

不可以，根据 SAC/TC 及国际信息、数据安全管理部门发布的规范，审计日志必须保持客观全面、准确，因此不提供删除或修改功能。

6.4 用户云账户欠费给云审计服务带来的影响？

当用户云账户欠费时，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。

此外，云审计服务的追踪器状态会显示为“异常”，此时只能对追踪器执行“删除”操作。

6.5 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，是企业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。

6.6 事件文件可以存储多长时间？

默认情况下，云审计服务管理控制台可存储最近 7 天内的事件文件，而对于已保存至 OBS 桶的历史操作记录，您可以无限期存储这些事件文件。

6.7 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。

6.8 云审计服务是否支持事件文件的关键字验证？

支持。原则上进行关键字验证时必须包含以下字段：time、service_type、resource_type、trace_name、trace_status、trace_type，其他字段由各服务自己定义。

6.9 启用云审计服务是否会影响其他云服务资源的性能？

不会。启用云审计服务不会影响其他云服务资源的性能。

6.10 为什么查看事件窗口中，有些事件的 IP、code、request、response 和 message 字段为空？

IP、code、request、response 和 message 字段并非云审计服务规定的必备字段：

- 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。

6.11 为什么事件列表中有些事件的资源 ID 为超链接可以跳转，有些为非超链接？

目前 CTS 仅支持部分 ECS、EVS、VBS、IMS、AS、CES 和 VPC 的操作通过资源 ID 跳转到对应云资源的详情页面，该功能正在逐步完善。

6.12 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。

6.13 为什么在事件列表中按照操作用户进行筛选时，存在 user_account/op_service 用户？

当用户发起的某些请求涉及后台一些高权限要求的操作或涉及调用其他服务时，可能存在用户自身的权限不足的问题，因此在确保符合安全要求的前提下，会临时对该请求中的用户身份进行提权，请求完成后提权结束，但会将提权行为记录到该请求发送到 CTS 的日志当中，此时的操作用户将记录为 user_account/op_service。

6.14 关键操作通知服务支持哪些服务？

目前云审计服务仅支持对部分关键操作发送通知，支持的服务类型包括 ECS、EVS、VPC、KMS、IAM，支持的操作类型上包括创建、删除、登录等操作。该功能仍在完善中，后续将会支持更多的服务和操作类型。详细情况请参见 4.1 -配置追踪器章节。

6.15 对事件文件进行 KMS 加密是否收费？

加密过程免费，密钥管理服务资费详情参见《密钥管理服务用户指南》中“[服务资费](#)”章节。