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 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，全球各级信息、数据安全管理部门已对此发布多份标准，如：IS0 IEC27000、GB/T 20945-2013、COSO、COBIT、ITIL、NISTSP800 等。

云审计服务（Cloud Trace Service，以下简称 CTS），是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、资源类型、事件名称、资源名称/ID、事件级别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（Object Storage Service，简称 OBS）下的 OBS 桶，转储时会按照服务维度压缩审计日志为事件文件。

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 OBS 桶的历史操作记录。

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 OBS 桶中。

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": "[redacted]",
        "domain": {
            "name": "[redacted]",
            "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": "[redacted]",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482532857,
    "trace_id": "7519ef09-1ac6-11e7-8cc0-3d812829baf6",
    "trace_status": "normal"
},
{
    "time": 1491482535203,
    "user": {
        "id": "59f40829165447fb9470b56f41dff599",
        "name": "[redacted]",
        "domain": {
            "name": "[redacted]",
            "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": "[redacted]",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482535224,
    "trace_id": "76831bfb-1ac6-11e7-98ff-a1036f244dcd",
    "trace_status": "normal"
}]
```


获取事件文件的方法请参见 2.4 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。

1.2 工作原理

云审计服务直接对接公有云上的其他服务，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 OBS 桶中。

开通云审计服务之前，需要开通对象存储服务。开通云审计服务时关联的追踪器可以跟踪生成事件文件，并将事件文件保存在对象存储服务创建的 OBS 桶中。

用户可以对事件文件执行以下两种操作：

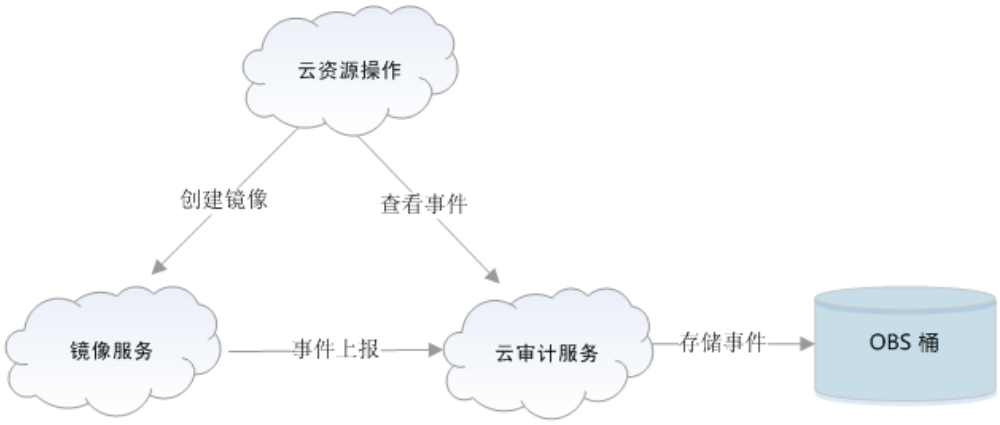
- 事件文件的创建和保存：

- 当用户在弹性云主机、云硬盘服务、镜像服务等其它与云审计服务完成对接的服务中，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。
- 云审计服务务管理控制台会保存最近 7 天的操作记录，并定期将操作记录同步保存到用户定义的 OBS 桶中进行长期保存。

- 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。
  - 若要查询 7 天前的操作记录，可以在对应的 OBS 桶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、等操作。

以用户创建镜像为例，在用户使用公有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，云审计服务将事件转存至 OBS 桶中。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 支持审计的服务

用户开启云审计服务后，系统会自动识别当前云平台上所开通的云服务，自动抓取各云服务的各项关键操作并主动向云审计服务上报各项关键操作的审计日志。

对于 Region 级服务的审计日志，根据被操作资源的归属情况，记录在各个 region 或 project 下。

云审计服务支持的 region 级服务的关键操作列表如下：

- 6.1 弹性云主机的关键操作列表
- 6.2 镜像服务的关键操作列表
- 6.3 物理机服务的关键操作列表
- 6.4 弹性伸缩的关键操作列表
- 6.5 专属云的关键操作列表
- 6.6 虚拟私有云的关键操作列表
- 6.7 弹性负载均衡的关键操作列表
- 6.8 云硬盘服务的关键操作列表
- 6.9 云硬盘备份服务的关键操作列表
- 6.10 云审计服务的关键操作列表
- 6.11 云监控的关键操作列表
- 6.12 关系型数据库服务的关键操作列表
- 6.13 云桌面的关键操作列表

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并开通了云审计服务，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 申请云审计服务

云审计服务目前以项目制的方式为客户提供，如客户需要申请云审计服务，请与客户经理或天翼云客服联系。

2.2 开通云审计服务

操作场景

使用云审计服务前需要开启云审计服务，开通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。

为了保存操作记录，需要将事件文件保存至对象存储服务中的存储对象的容器，即 OBS 桶。因此，开通云审计服务之前，需要开通对象存储服务，且用户对即将要使用的 OBS 桶具有完全的使用权限。公有云平台默认仅开通 OBS 的服务所有者能够访问 OBS 桶及其包含的所有对象，但服务所有者可以通过编写访问策略来向其他服务和用户授予访问权。

本节介绍如何开通云审计服务。

前提条件

已开通对象存储服务。

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. 填写 OBS 桶和操作事件文件前缀。参数说明如表 2-1 所示。

表2-1 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
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。手动命名可包含大小写字母、数字、中划线、下划线、点，长度为 0 ~ 64 位字符。创建追踪器时，系统会自动随机生成，生成规则和手动命名规则一致。	-

6. 单击“确定”，完成开通云审计服务。

开通云审计服务成功后，您可以在追踪器页面查看已创建的追踪器的详细信息。

2.3 查看追踪事件

操作场景

在您开通了云审计服务后，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。

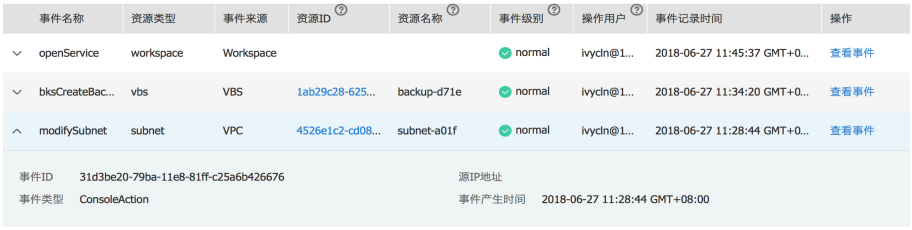
  选择资源 ID 时，还需选择或者手动输入某个具体的资源 ID。

  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



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

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。

2.4 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 OBS 桶。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 OBS 中通过下载事件文件查看已保存至 OBS 桶的历史操作记录。

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“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 管理控制台中对应 OBS 桶的对象管理界面。

   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* > *追踪器名称* >*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“更多”-“下载为”按键。

- 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>追踪器名称 >服务类型目录

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

- 事件文件命名格式：

  ***操作事件文件前缀_CloudTrace_区域标示/区域标示-项目标示_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": "[redacted]",
        "domain": {
            "name": "[redacted]",
            "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": "[redacted]",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482532857,
    "trace_id": "7519ef09-1ac6-11e7-8cc0-3d812829baf6",
    "trace_status": "normal"
},
{
    "time": 1491482535203,
    "user": {
        "id": "59f40829165447fb9470b56f41dff599",
        "name": "[redacted]",
        "domain": {
            "name": "[redacted]",
            "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": "[redacted]",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482535224,
    "trace_id": "76831bfb-1ac6-11e7-98ff-a1036f244dcd",
    "trace_status": "normal"
}]
```

3 管理

3.1 修改追踪器

操作场景

云审计服务管理控制台支持修改已创建的追踪器的 OBS 桶和操作事件文件前缀。当修改云审计服务的追踪器中的"OBS 桶"时，云审计服务会自动为重新选择的 OBS 桶挂载一个对应的策略，使得追踪器修改成功后，云审计服务所支持的全部事件文件会存储至该重新选择的 OBS 桶。当修改云审计服务的追踪器中的"操作事件文件前缀"时，不影响对应 OBS 桶的策略。修改追踪器完成后，系统立即以新的规则开始记录操作。

本节介绍如何修改追踪器。

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"修改"。您可以选择重新指定的用于存储操作事件的已存在的 OBS 桶，或者重新命名操作事件文件前缀。
5. 单击"确定"，完成修改追踪器。

   追踪器修改成功后，您可以在追踪器信息页面查看修改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，因此当您修改了追踪器所对应的 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变更后的 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。

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

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 申请云审计服务。

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 2.4 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 申请云审计服务。

操作步骤

以现网某个弹性云主机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主机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主机失败的操作，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 申请云审计服务。

操作步骤

以查看某个弹性云主机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 2.4 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，检视该弹性云主机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

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。

字段名称	是否必选	类型	描述
			该字段在 API 接口中以 String 类型进行传输和存储。
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 表示通过公有云管理控制台执行的操作。 • SystemAction 表示公有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

字段名称	是否必选	类型	描述
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_XWO68TFC",
            "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 支持审计的服务及详细操作列表

6.1 弹性云主机的关键操作列表

弹性云主机（Elastic Cloud Server，以下简称 ECS）是由 CPU、内存、镜像、云硬盘组成的一种可随时获取、弹性可扩展的计算服务器，同时它结合 VPC、虚拟防火墙、数据多副本保存等能力，为您打造一个高效、可靠、安全的计算环境，确保您的服务持久稳定运行。

通过云审计服务，您可以记录与弹性云主机相关的操作事件，便于日后的查询、审计和回溯。

表6-1 云审计服务支持的 ECS 操作列表

操作名称	资源类型	事件名称
创建云服务器	ecs	createServer
删除云服务器	ecs	deleteServer
启动云服务器	ecs	startServer
重启云服务器	ecs	rebootServer
关闭云服务器	ecs	stopServer
添加云服务器网卡	ecs	addNic
删除云服务器网卡	ecs	deleteNic
云服务器挂载磁盘	ecs	attachVolume
云服务器挂载磁盘（EVS 页面触发）	ecs	attachVolume2
云服务器卸载磁盘	ecs	detachVolume

操作名称	资源类型	事件名称
重装操作系统	ecs	reinstallOs
切换操作系统	ecs	changeOs
重装操作系统	ecs	reinstallOsV2
切换操作系统	ecs	changeOsV2
变更规格	ecs	resizeServer
配置虚拟机自动恢复标签	ecs	addAutoRecovery
删除虚拟机自动恢复标签	ecs	deleteAutoRecovery
创建安全组	ecs	createSecurityGroup

6.2 镜像服务的关键操作列表

镜像服务（Image Management Service，以下简称 IMS）提供简单方便的镜像自助管理功能，用户可以使用公共镜像或者私有镜像灵活便捷的申请弹性云主机。同时，用户还能通过已有的云服务器或使用外部镜像文件创建私有镜像。

通过云审计服务，您可以记录与镜像服务相关的操作事件，便于日后的查询、审计和回溯。

表6-2 云审计服务支持的 IMS 操作列表

操作名称	资源类型	事件名称
创建镜像	ims	createImage
修改镜像	ims	updateImage
批量删除镜像	ims	deleteImage
复制镜像	ims	copyImage
导出镜像	ims	exportImage
新增成员	ims	addMember

操作名称	资源类型	事件名称
批量修改成员	ims	updateMember
批量删除成员	ims	deleteMemeber

6.3 物理机服务的关键操作列表

物理机服务（以下简称 BMS）提供单租户专属的物理服务器，通过卓越的计算性能，满足核心应用场景对高性能及稳定性的需求，同时可以和 VPC 等其他云产品灵活结合使用，结合了传统托管主机带来的稳定性能与云上资源高度弹性的优势。

通过云审计服务，您可以记录与裸金属服务器相关的操作事件，便于日后的查询、审计和回溯。

表6-3 云审计服务支持的 BMS 操作列表

操作名称	资源类型	事件名称
创建裸金属服务器	bms	createBareMetalServers
删除裸金属服务器	bms	deleteBareMetalServers
启动裸金属服务器	bms	startBareMetalServers
关闭裸金属服务器	bms	stopBareMetalServers
重启裸金属服务器	bms	rebootBareMetalServers
裸金属服务器挂载数据卷	bms	attachDataVolume
裸金属服务器卸载数据卷	bms	detachDataVolume

6.4 弹性伸缩的关键操作列表

弹性伸缩（Auto Scaling，以下简称 AS）可根据用户的业务需求和预设策略，自动调整计算资源，使云服务器数量自动随业务负载增长而增加，随业务负载降低而减少，保证业务平稳健康运行。

通过云审计服务，您可以记录与弹性伸缩相关的操作事件，便于日后的查询、审计和回溯。

表6-4 云审计服务支持的 AS 操作列表

操作名称	资源类型	事件名称
创建伸缩组	scaling_group	createScalingGroup
修改伸缩组	scaling_group	modifyScalingGroup
删除伸缩组	scaling_group	deleteScalingGroup
启用伸缩组	scaling_group	enableScalingGroup
停用伸缩组	scaling_group	disableScalingGroup
创建伸缩配置	scaling_configuration	createScalingConfiguration
删除伸缩配置	scaling_configuration	deleteScalingConfiguration
批量删除伸缩配置	scaling_configuration	batchDeleteScalingConfiguration
创建伸缩策略	scaling_policy	createScalingPolicy
修改伸缩策略	scaling_policy	modifyScalingPolicy
删除伸缩策略	scaling_policy	deleteScalingPolicy
启用伸缩策略	scaling_policy	enableScalingPolicy
停用伸缩策略	scaling_policy	disableScalingPolicy
立即执行伸缩策略	scaling_policy	executeScalingPolicy
移除伸缩组实例	scaling_instance	removeInstance
批量移除实例	scaling_instance	batchRemoveInstances
批量添加实例	scaling_instance	batchAddInstances

6.5 专属云的关键操作列表

专属云（Dedicated Cloud，以下简称 DeC）是在公有云上隔离出来的专属虚拟化资源池。在专属云内，用户可申请独占物理设备，独享计算和网络资源，并使用可靠的分布式存储。

通过云审计服务，您可以记录与专属云相关的操作事件，便于日后的查询、审计和回溯。

表6-5 云审计服务支持的 DeC 操作列表

操作名称	资源类型	事件名称
开通 DeC	dec	openDEC

6.6 虚拟私有云的关键操作列表

虚拟私有云（Virtual Private Cloud，以下简称 VPC）为弹性云主机构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户企业云中资源的安全性，简化用户的网络部署。

通过云审计服务，您可以记录与虚拟私有云相关的操作事件，便于日后的查询、审计和回溯。

表6-6 云审计服务支持的 VPC 操作列表

操作名称	资源类型	事件名称
修改 Bandwidth	bandwidth	modifyBandwidth
创建 EIP	eip	createEip
释放 EIP	eip	deleteEip
绑定 EIP	eip	bindEip
解绑定 EIP	eip	unbindEip
创建 PrivateIp	privateIps	createPrivateIp
删除 PrivateIp	privateIps	deletePrivateIp
创建 Security Group	security_group	createSecurityGroup
修改 Security Group	security_group	modifySecurityGroup

操作名称	资源类型	事件名称
创建 Subnet	subnet	createSubnet
删除 Subnet	subnet	deleteSubnet
修改 Subnet	subnet	modifySubnet
创建 VPC	vpc	createVpc
删除 VPC	vpc	deleteVpc
修改 VPC	vpc	modifyVpc
创建 VPN	vpn	createVpn
删除 VPN	vpn	deleteVpn
修改 VPN	vpn	modifyVpn
创建 Nat 网关	natgateway	createNatGateway
更新 Nat 网关	natgateway	updateNatGateway
删除 Nat 网关	natgateway	deleteNatGateway
创建 Snat 规则	snatrule	createSnatRule
删除 Snat 规则	snatrule	deleteSnatRule
创建 Dnat 规则	dnatrule	createDnatRule
删除 Dnat 规则	dnatrule	deleteDnatRule

6.7 弹性负载均衡的关键操作列表

弹性负载均衡（Elastic Load Balance ，以下简称 ELB）通过将访问流量自动分发到多台弹性云主机，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。

用户通过基于浏览器、统一化视图的云计算管理图形化界面，可以创建 ELB，为服务配置需要监听的端口，配置云服务器。消除单点故障，提高整个系统的可用性。

通过云审计服务，您可以记录与弹性负载均衡相关的操作事件，便于日后的查询、审计和回溯。

表6-7 云审计服务支持的 ELB 操作列表

操作名称	资源类型	事件名称
配置访问日志	accesslog	create access log
删除访问日志	accesslog	delete access log
创建证书	certificate	create certificate
更新证书	certificate	update certificate
删除证书	certificate	delete certificate
创建健康检查	healthmonitor	create healthmonitor
更新健康检查	healthmonitor	update healthmonitor
删除健康检查	healthmonitor	delete healthmonitor
创建转发策略	l7policy	create forwarding policy
更新转发策略	l7policy	update forwarding policy
删除转发策略	l7policy	delete forwarding policy
创建转发规则	l7rule	create forwarding rule
更新转发规则	l7rule	update forwarding rule
删除转发规则	l7rule	delete forwarding rule
创建监听器	listener	create listener
更新监听器	listener	update listener
删除监听器	listener	delete listener
创建负载均衡器	loadbalancer	create loadbalancer
更新负载均衡器	loadbalancer	update loadbalancer
删除负载均衡器	loadbalancer	delete loadbalancer
添加后端云服务器	member	add backend ecs
更新后端云服务器	member	update backend ecs
移除后端云服务器	member	remove backend ecs

操作名称	资源类型	事件名称
创建后端云服务器组	pool	create backend member group
更新后端云服务器组	pool	update backend member group
删除后端云服务器组	pool	delete backend member group

6.8 云硬盘服务的关键操作列表

云硬盘服务（Elastic Volume Service，以下简称 EVS）是一种基于分布式架构的，可弹性扩展的虚拟块存储设备。您可以在线进行操作，使用方式与传统服务器硬盘完全一致。同时，云硬盘具有更高的数据可靠性，更高的 I/O 吞吐能力和更加简单易用等特点，适用于文件系统、数据库或者其他需要块存储设备的系统软件或应用。

通过云审计服务，您可以记录与云硬盘相关的操作事件，便于日后的查询、审计和回溯。

表6-8 云审计服务支持的 EVS 操作列表

操作名称	资源类型	事件名称
创建磁盘	evs	createVolume
更新磁盘	evs	updateVolume
扩容磁盘	evs	extendVolume
删除磁盘	evs	deleteVolume

6.9 云硬盘备份服务的关键操作列表

云硬盘备份服务（Volume Backup Service，以下简称 VBS）提供对公有云环境中云服务器的基于云硬盘快照技术的本地数据保护服务。VBS 支持全量备份和增量备份。第一次做备份时，系统默认做全量备份，非第一次的备份，系统默认做增量备份。无论是全量还是增量都可以方便的将磁盘恢复至备份时刻的状态。

通过云审计服务，您可以记录与云硬盘备份相关的操作事件，便于日后的查询、审计和回溯。

表6-9 云审计服务支持的 VBS 操作列表

操作名称	资源类型	事件名称
创建备份	vbs	bksCreateBackup
删除备份	vbs	bksDeleteBackup
恢复备份	vbs	bksRestoreBackup
绑定备份策略	autobackup	addPolicyResource
解绑备份策略	autobackup	deletePolicyResource
立即执行备份策略	autobackup	actionPolicy
创建备份策略	autobackup	createPolicy
删除备份策略	autobackup	deletePolicy
修改备份策略	autobackup	modifyPolicy
备份策略调度创备份	autobackup	scheduleCreateBackup
备份策略自动删备份	autobackup	scheduleDeleteBackup
修改备份策略标签	autobackup	modifyPolicyTag
删除备份策略标签	autobackup	deletePolicyTag

6.10 云审计服务的关键操作列表

云审计服务（CloudTrace Service，以下简称 CTS）为您提供云服务资源的操作记录，供您查询、审计和回溯使用。

通过云审计服务，您可以记录云审计自身服务相关的操作事件，便于日后的查询、审计和回溯。

表6-10 云审计服务支持的自身服务操作列表

操作名称	资源类型	事件名称
创建追踪器	tracker	createTracker

操作名称	资源类型	事件名称
修改追踪器	tracker	updateTracker
停用追踪器	tracker	updateTracker
启用追踪器	tracker	updateTracker
删除追踪器	tracker	deleteTracker

6.11 云监控的关键操作列表

云监控（Cloud Eye）是一个开放性的监控平台，即可提供资源的近似实时监控、告警、通知等服务。

通过云审计服务，您可以记录与云监控相关的操作事件，便于日后的查询、审计和回溯。

表6-11 云审计服务支持的 Cloud Eye 操作列表

操作名称	资源类型	事件名称
创建告警规则	alarm_rule	createAlarmRule
删除告警规则	alarm_rule	deleteAlarmRule
停用告警规则	alarm_rule	disableAlarmRule
启用告警规则	alarm_rule	enableAlarmRule
修改告警规则	alarm_rule	updateAlarmRule
状态更新为告警	alarm_rule	alarmStatusChangeToAlarm
状态更新为数据不足	alarm_rule	alarmStatusChangeToInsufficientData
状态更新为正常	alarm_rule	alarmStatusChangeToOk
创建自定义告警模板	alarm_template	createAlarmTemplate
删除自定义告警模板	alarm_template	deleteAlarmTemplate
修改自定义告警模板	alarm_template	updateAlarmTemplate

操作名称	资源类型	事件名称
创建监控面板	dashboard	createDashboard
删除监控面板	dashboard	deleteDashboard
修改监控面板	dashboard	updateDashboard
添加监控数据	metric	addMetricData
导出监控数据	metric	downloadMetricsReport

6.12 关系型数据库服务的关键操作列表

关系型数据库服务（Relational Database Service，以下简称 RDS）是一种基于云计算平台的可即开即用、稳定可靠、按需扩展、便捷管理的在线关系型数据库服务。

通过云审计服务，您可以记录与关系型数据库服务相关的操作事件，便于日后的查询、审计和回溯。

表6-12 云审计服务支持的 RDS 操作列表

操作名称	资源类型	事件名称
创建实例、恢复到新实例（Console、OPENAPI、TROVEAPI）	instance	createInstance
创建只读 （Console、OPENAPI、TROVEAPI）	instance	createReadReplicate
实例重启、扩容、规格变更、恢复到原有实例操作（Console、OPENAPI 、TROVEAPI）	instance	instanceAction
重置密码（Console）	instance	resetPassword
设置数据库版本配置参数（OPENAPI）	instance	setDBParameters

操作名称	资源类型	事件名称
重置实例的数据库版本配置参数（OPENAPI）	instance	resetDBParameters
设置备份策略-打开,关闭,修改（Console、OPENAPI）	instance	setBackupPolicy
修改数据库端口号（Console）	instance	changeInstancePort
绑定解绑 EIP（Console）	instance	setOrResetPublicIP
修改安全组（Console）	instance	modifySecurityGroup
创建标签（Console、OPENAPI）	instance	createTag
删除标签（Console、OPENAPI）	instance	deleteTag
修改标签（Console、OPENAPI）	instance	modifyTag
删除集群下的实例（Console、OPENAPI、TROVEAPI）	instance	deleteInstance
创建快照（Console、OPENAPI）	backup	createManualSnapshot
复制快照（Console）	backup	copySnapshot
删除快照（Console、OPENAPI）	backup	deleteManualSnapshot
创建参数组（Console、TROVEAPI）	config	createParameterGroup
修改参数组（Console、TROVEAPI）	config	updateParameterGroup
删除参数组（Console、	config	deleteParameterGroup

操作名称	资源类型	事件名称
TROVEAPI ）		
复制参数组（Console ）	config	copyParameterGroup
重置参数组（Console ）	config	resetParameterGroup
比较参数组（Console ）	config	compareParameterGroup
应用参数组（Console ）	config	applyParameterGroup

6.13 云桌面的关键操作列表

云桌面（Workspace ）是一种基于云计算的优于传统桌面的桌面服务。云桌面支持多种设备（包括 Windows 和 Mac 系统的计算机、iPad、iPhone 和 Android 智能设备）接入，从而使您能够在任何时间、任何地点访问和存取文件以及应用，实现移动办公和娱乐。云桌面提供和传统桌面一样的配置（包括 vCPU、GPU、内存、磁盘）以及您所熟悉的 Windows 操作系统，您可以像使用自己的计算机一样使用桌面。

通过云审计服务，您可以记录与云桌面相关的操作事件，便于日后的查询、审计和回溯。

表6-13 云审计服务支持的 Workspace 操作列表

操作名称	资源类型	事件名称
更新云服务状态信息	workspace	updateDesktopMetadata
订购桌面	workspace	orderVm
重启虚拟机	workspace	rebootDesktop
关闭虚拟机	workspace	shutdownDesktop
虚拟机的开机	workspace	startDesktop
删除虚拟机	workspace	deleteDesktop
桌面状态更新	workspace	updateDesktopStatus
删除用户信息	workspace	deleteUser

操作名称	资源类型	事件名称
导出用户信息	workspace	exportUserInfo
用户解锁	workspace	unlockUser
重置密码	workspace	resetUserPassword
下载用户模板	workspace	downloadUserModel
删除按需方法失败的任务	workspace	deleteJob
域用户请求修改密码	workspace	updateDomainUserPassword
统一身份认证服务同步资源租户	workspace	synIamResourceTenant
更新策略组	workspace	updatePolicy
开户	workspace	openService
修改域密码	workspace	updateAdPwd
销户	workspace	tenantClose
重试服务任务（开户、销户失败任务）	workspace	tenantRetryServiceTask
恢复基础架构服务器	workspace	restoreManagerVmBackup
修改云桌面属性	workspace	modifyDesktopAttributes
更新域名	workspace	updateRecordSet

7 常见问题

7.1 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。

7.2 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、修改、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。

7.3 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。

7.4 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。

7.5 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，操作详情请参见《对象存储服务用户指南》的"管理桶"章节。

7.6 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。

7.7 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。

7.8 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。

7.9 为什么事件列表中有些事件的为超链接可以跳转，有些为非超链接？

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

7.10 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。

7.11 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。

7.12 为什么有些 trace_type 为 systemAction 的事件，存在 user、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。