云审计服务

用户手册

天翼云科技有限公司

目 录

1 简介

1.1 什么是云审计服务？

云审计服务（Cloud Trace Service，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。

云审计服务记录的操作有以下三种：

- 用户登录管理控制台的操作。
- 用户通过云服务支持的 API 执行的操作。
- 系统内各服务内部触发的操作。

您可以在云审计服务管理控制台查询近 7 天内的操作记录。如果需要保存 7 天之前的操作记录，您可以通过对象存储服务（Object Storage Service，以下简称 OBS），将操作记录实时同步保存至 OBS。

1.2 基本概念

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 1 个管理追踪器和 100 个数据追踪器。

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：

- 管理事件

  指云服务上报的事件。
- 数据事件

  指 OBS 服务上报的读写操作事件。

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。

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

1.3 工作原理

云审计服务直接对接云服务平台上的其他服务，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文件形式实时保存至 OBS 桶中。

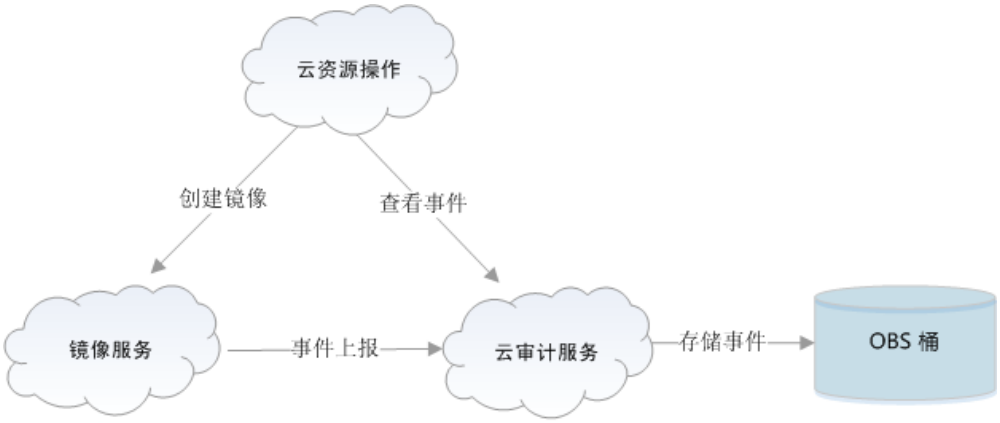
用户可以对事件文件执行以下两种操作：

- 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 OBS 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 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 天前的操作记录且已配置 OBS 服务，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、配置等操作。

以用户创建镜像为例，在用户使用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 OBS 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



1.4 使用场景

云审计服务能够为您提供云服务资源的操作记录，记录的信息包括发起操作的用户身份、IP 地址、具体的操作内容的信息，以及操作返回的响应信息。根据这些操作记录，可以很方便的实现审计类功能，以帮助用户更好地规划和利用已有资源、甄别违规或高危操作。

以下介绍三种典型应用场景。

- **安全审计场景**

  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。

- **问题定位场景**

  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。

- **资源跟踪场景**

  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。

2 入门

2.1 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，开启云审计服务后系统会自动创建一个名称为“system”，类型为“管理事件”的追踪器，系统记录的所有操作将关联在该追踪器中。

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。云服务平台默认仅开通 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。

开通 OBS 的方法，请参见《对象存储服务用户指南》的“开通 OBS 服务”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 CTS”，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“开通云审计服务”。
5. 在开启云审计服务详情页面，单击“开启”，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，您可以在追踪器信息页面查看系统自动创建的追踪器的详细信息。

追踪器记录创建追踪器的该租户的云服务资源的相关操作。云审计服务当前支持的云服务的详细信息，请参见支持审计的服务列表。

2.2 查看追踪事件

操作场景

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. 选择“服务列表 > 管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
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：
   - 事件类型、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。
   - 时间范围：可选择查询最近七天内任意时间段的操作事件。
5. 在需要查看的事件左侧，单击展开该记录的详细信息。
6. 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口显示该操作事件结构的详细信息。

   关于事件结构的关键字段详解，请参见《云审计服务 用户指南》的“事件结构”和“事件样例”章节。

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 OBS 桶。事件文件是按照服务、转储周期两个维度生成的事件集，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。

前提条件

已在云审计服务中成功配置追踪器。配置方法请参见《云审计服务用户指南》的“配置追踪器”章节。

操作步骤

1. 登录管理控制台。
2. 选择“服务列表 > 管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
4. 单击“转储 OBS 桶”下的指定的 OBS 桶名称，页面跳转到 OBS 管理控制台中对应 OBS 桶的对象管理界面。
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*”，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>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_*区域标示_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《云审计服务用户指南》的“事件结构”和“事件样例”章节。
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 文件如图 2-1 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2-1 下载解压后的 json 文件

2.4 配置关键操作通知

操作场景

云审计服务在记录某些特定关键操作时，支持对这些关键操作通过消息通知服务实时向相关订阅者发送通知，该功能由云审计服务触发，消息通知服务（SMN）完成通知发送。主要应用于以下场景：

- 高危操作（重启虚拟机、变更安全配置等）、成本敏感操作（创建、删除高价资源等）、业务敏感操作（网络配置变更等）的实时感知和确认；
- 越权操作感知：如高权限用户的登录、某用户进行了其权限范围之外的操作的实时感知和确认；
- 对接用户自有审计日志分析系统：将所有审计日志实时对接到用户自有的审计日志分析系统，进行接口调用成功率分析、越权分析、安全分析、成本分析等。

使用说明

- 由于云审计服务的关键操作通知需要使用消息通知服务向相关的订阅者发送通知，因此需要提前了解消息通知服务的创建主题、添加订阅等操作；
- 目前云审计服务支持创建 100 个自定义的关键操作通知，每个通知支持单独设置触发操作范围、指定操作用户和通知主题；
- 如果云审计服务和云监控服务使用同一消息主题，则接受终端一样，但是发送的内容不同；
- 单个关键操作通知主题最多支持对 100 个服务的 1000 个关键操作进行选择；
- 自定义关键通知功能是原有关键操作通知的升级版本，配置上更丰富，功能上更强大。

操作步骤

1. 登录管理控制台。
2. 选择“服务列表 > 管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 在左侧导航栏中选择“关键操作通知”，页面跳转到关键操作通知页面。
4. 单击页面右上角的“创建关键操作通知”，页面跳转到创建关键操作通知参数填写页面。
5. 填写“基本信息”参数。

   通知名称：用于标识和区分关键操作通知，必选参数。命名可包含英文、中文、数字、下划线，长度不超过 64 位。
6. 配置关键操作。

   根据具体使用场景，选择“典型”、“完整”和“自定义操作”三种触发场景：
   - 典型：适用于企业日常审计，目前支持对 ECS/VPC/EVS/DEW 部分核心资源的创建和删除操作以及 IAM 服务的登录操作进行通知。
   - 完整：更适合对接用户自有审计系统，支持对所有已对接云审计服务的所有操作发送 SMN 通知。该模式下用户不可配置，默认发送对象为支持服务的所有事件。此场景下建议用户使用订阅协议为 https 的 SMN 主题。
   - 自定义：适合对高危操作、成本敏感操作、业务敏感操作、越权操作等有实时感知和确认的企业，亦可对接用户自有审计日志分析系统进行分析。触发通知的操作范围支持自定义选择，单个关键操作通知支持对 100 个服务的 1000 个关键操作进行选择，具体的操作列表详见《云审计服务用户指南》中“支持审计的服务及详细操作列表”章节。
7. 配置用户。

   当指定的用户发起关键操作时，通过 SMN 通知相关的订阅者。
   - 当选择“不指定”用户时，所有用户发起的关键操作，将通过 SMN 通知相关的订阅者。
   - 当选择“指定用户”时，需要手动指定用户，当这些用户发起关键操作时，将通过 SMN 通知相关的订阅者。
8. 配置 SMN 主题。
   - 当选择发送通知时，需要选择已创建的 SMN 主题或者点击链接跳转到消息通知服务页面创建新的主题。
   - 当选择不发送通知时，则无需配置。

3 管理

3.1 创建追踪器

操作场景

云审计服务管理控制台支持创建数据事件追踪器，用于记录数据操作日志。

追踪器分两类，包括管理事件追踪器和数据事件追踪器。管理事件追踪器用于记录管理事件，即针对所有云资源的操作日志，例如创建、登录、删除等。数据事件追踪器用于记录数据事件，即针对数据的操作日志，例如上传、下载等。

由于您在开通云审计服务时，系统已为您自动创建了一个管理事件追踪器，管理事件追踪器只能有一个且不可删除，故您自行创建的追踪器均为数据事件追踪器。

操作步骤

1. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
2. 单击页面右上角的“创建追踪器”。
3. 在创建追踪器页面填写相关参数。
   - 基本信息
     - 追踪器类型：仅可选择“数据事件”。
     - 追踪器名称：为追踪器取名，便于识别。
     - 追踪对象：选择您存储数据的容器，当前为 OBS 桶。
     - 追踪操作：选择需要记录日志的数据操作。
     - 事件分析：开启“事件分析”。
     - 事件分析位置。

- OBS 转储
  - OBS 转储：

    当选择是否转储 OBS 为“转储”时，您可以选择已存在的 OBS 桶，并配置事件文件前缀。

    如果配置 OBS 桶转储为“不转储”时，则无需配置相应参数。
  - 转储 OBS 桶：您可以选择已存在的 OBS 桶。
  - 保存周期：选择转储至 OBS 桶中日志的保存时长。
  - 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。

4. 单击“确定”完成追踪器的创建。

3.2 配置追踪器

操作场景

云审计服务管理控制台支持配置已开启的追踪器的 OBS 桶、事件文件前缀和配置已创建的追踪器关键事件操作通知。

- 用户可选择已存在的 OBS 桶。云审计服务会自动为该 OBS 桶挂载转储所需的桶策略。
- 当配置云审计服务的追踪器中的“事件文件前缀”时，不影响对应 OBS 桶的策略。

配置追踪器完成后，系统立即以新的规则开始记录操作。

本节介绍如何配置追踪器。

前提条件

已开通云审计服务。

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 CTS”，进入云审计服务详情页面。
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，并配置事件文件前缀。
   - 如果配置 OBS 桶转储为“不转储”时，则无需配置相应参数。
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。

3.3 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 CTS”，进入云审计服务详情页面。
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“是”，完成停用追踪器。

   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。

3.4 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数据事件追踪器。删除数据事件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。

说明

您在开通云审计服务时，系统已为您自动创建了一个管理事件追踪器，管理事件追踪器只能有一个且不可删除。

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 CTS”，进入云审计服务详情页面。
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。

操作步骤

以审计最近两周内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 CTS”，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. 在事件列表界面依次选择过滤条件，“事件类型”>“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。

说明

过滤条件查询示例：依次选择“管理事件”>“evs”>“evs”>“按事件名称”>“createVolume”或“管理事件”>“evs”>“evs”>“按事件名称”>“deleteVolume”，单击“查询”按钮执行搜索，查询七天以内所有创建或删除 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《云审计服务快速入门》中的“查看已归档事件”章节下载 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 5 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 开通云审计服务。

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 CTS”，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. 在事件列表界面依次选择过滤条件，“事件类型”>“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“管理事件”>“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 CTS”，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：“管理事件”>“ecs”>“ecs”>“事件级别”>“Warning”，在结果中查看事件名称为“createServer”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 开通云审计服务。

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 CTS”，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. 在事件列表界面依次选择过滤条件，“事件类型”>“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“管理事件”>“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 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。 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_rating	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 表示通过管理控制台执行的操作。 • SystemAction 表示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。

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。

创建云主机实例

```
{
    "time": "2016/12/08 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 8 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": "2016/12/08 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": "2016/12/08 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 8 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 计算

6.1.1 弹性云主机

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
创建云主机	ecs	createServer
删除云主机	ecs	deleteServer
启动云主机	ecs	startServer
重启云主机	ecs	rebootServer
关闭云主机	ecs	stopServer

操作名称	资源类型	事件名称
添加云主机网卡	ecs	addNic
删除云主机网卡	ecs	deleteNic
云主机挂载磁盘	ecs	attachVolume
云主机卸载磁盘	ecs	detachVolume
重装操作系统	ecs	reinstallOs
切换操作系统	ecs	changeOs
变更规格	ecs	resizeServer

说明

表 6-2 中 ECS 的操作，为底层（OpenStack）服务触发；部分事件名称与表 6-1 中重复，是因为这些事件采用了异步调用的模式：操作下发会产生上表中描述的事件，而操作结果响应会产生表 6-2 中描述的事件。

表6-2 云审计服务支持的 ECS 操作列表（由底层服务触发）

操作名称	资源类型	事件名称
创建虚拟机	server	createServer
更新虚拟机	server	updateServer
删除虚拟机	server	deleteServer
操作虚拟机	server	operateServer
设置元数据	server	setMetadata
更新元数据/设置指定 key 的元数据	server	updateMetadata
删除指定 key 的元数据	server	deleteMetadata
虚拟机添加网卡	server	createInterface
虚拟机卸载网卡	server	detachInterface
清除指定虚拟机的密码(DB)	server	clearAdminPassword
虚拟机挂载卷	server	attachVolume
虚拟机卸载卷	server	detachVolume
更新配额	quotaSets	updateQuotas
删除配额	quotaSets	revertQuotasToDefaults
创建虚拟机组	serverGroup	createServerGroup

操作名称	资源类型	事件名称
删除虚拟机组	serverGroup	deleteServerGroup
开启服务	computeService	enableService
停止服务	computeService	disableService
添加停止服务的原因	computeService	logDisabledInfo
删除服务	computeService	deleteService
创建规格	flavor	createFlavor
删除规格	flavor	deleteFlavor
添加/删除租户访问规格权限	flavor	operateFlavorAccess
创建规格扩展属性	flavor	createExtraSpecs
更新规格指定扩展属性	flavor	updateExtraSpec
删除规格指定扩展属性	flavor	deleteExtraSpec
创建 keypair	keypair	createKeypair
删除 keypair	keypair	deleteKeypair
创建主机组	hostAggregates	createAggregate
更新主机组	hostAggregates	updateAggregate
删除主机组	hostAggregates	deleteAggregate
向主机组添加主机/从主机组移除主机/设置主机组元数据	hostAggregates	operateAggregate

6.1.2 镜像服务

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主机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6-3 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

操作名称	资源类型	事件名称
批量删除镜像	ims	deleteImage
新增成员	ims	addMember
批量修改成员	ims	updateMember
批量删除成员	ims	deleteMember

说明

表 6-4IMS 的操作，为底层（OpenStack）服务触发；部分事件名称与表 6-3 中重复，是因为这些事件采用了异步调用的模式：操作下发会产生上表中描述的事件，而操作结果响应会产生表 6-4 中描述的事件。

表6-4 云审计服务支持的 IMS 操作列表（由底层服务触发）

操作名称	资源类型	事件名称
创建镜像	image	createImage
修改镜像信息/上传镜像	image	updateImage
删除镜像	image	deleteImage
添加标签	image	addTag
删除标签	image	deleteTag
添加镜像成员	image	addMember
修改镜像成员信息	image	updateMember
删除镜像成员	image	deleteMember

6.1.3 弹性伸缩

弹性伸缩（Auto Scaling，以下简称 AS）是根据用户的业务需求，通过策略自动调整其业务资源的服务。您可以根据业务需求自行定义伸缩配置和伸缩策略，降低人为反复调整资源以应对业务变化和高峰压力的工作量，帮助您节约资源和人力成本。

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6-5 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

操作名称	资源类型	事件名称
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
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
批量设置实例保护	scaling_instance	batchProtectInstances
批量取消实例保护	scaling_instance	batchUnprotectInstances
删除标签	scaling_tag	deleteScalingTag
创建/更新标签	scaling_tag	updateScalingTag

6.2 存储

6.2.1 云硬盘服务

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6-6 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

说明

表 6-7 中 EVS 的操作，为底层（OpenStack）服务触发；部分事件名称与上表 6-6 重复，是因为这些事件采用了异步调用的模式：操作下发会产生上表中描述的事件，而操作结果响应会产生表 6-7 中描述的事件。

表6-7 云审计服务支持的 EVS 操作列表（由底层服务触发）

操作名称	资源类型	事件名称
创建卷	volumes	createVolumes
创建 type	types	createTypes
创建快照	snapshots	createSnapshots
创建备份	backups	createBackups
创建一致性组	consistencygroups	createConsistencygroups
创建快照一致性组	cgsnapshots	createCgsnapshots
创建 qos-specs	qos-specs	createQos-specs
创建卷传递	os-volume-transfer	createOs-volume-transfer
添加卷快照的元数据	snapshots	createSnapshotsMetadata
添加卷的元数据	volumes	createVolumesMetadata
为卷类型创建新的扩展参数	types	createTypesExtra_specs
导入卷备份记录信息	backups	createBackupsImport_record
恢复卷备份	backups	createBackupsRestore
强制删除卷	volumes	volumesOs-force_delete
挂载卷	volumes	volumesOs-attach
卸载卷	volumes	volumesOs-detach
保留卷	volumes	volumesOs-reserve

操作名称	资源类型	事件名称
预卸载卷	volumes	volumesOs-begin_detaching
回滚预卸载卷	volumes	volumesOs-roll_detaching
挂卷初始化连接	volumes	volumesOs-initialize_connection
卸卷断开连接	volumes	volumesOs-terminate_connection
卷上传镜像	volumes	volumesOs-volume_upload_image
扩容卷	volumes	volumesOs-extend
取消保留卷	volumes	volumesOs-unreserve
设置为为只读	volumes	volumesOs-update_readonly_flag
更改卷的卷类型	volumes	volumesOs-retype
设置卷为可启动卷	volumes	volumesOs-set_bootable
强制删除快照	snapshots	volumesOs-force_delete
删除卷	volumes	deleteVolumes
删除类型	types	deleteTypes
删除卷快照	snapshots	deleteSnapshots
删除备份	backups	deleteBackups
删除卷快照的单个元数据	snapshots	deleteSnapshotsSingleMetadata
删除一致性组	consistencygroups	createConsistencygroupsDelete
删除快照一致性组	cgsnapshots	deleteCgsnapshots
删除 qos-specs	qos-specs	deleteQos-specs
删除卷传递过程	os-volume-transfer	deleteOs-volume-transfer
删除卷的单个元数据	volumes	deleteVolumesSingleMetadata
更新快照信息	snapshots	updateSnapshots
更新卷	volumes	updateVolumes
更新租户的配额信息	os-quota-sets	updateOs-quota-sets
更新租户的配额等级	os-quota-class-sets	updateOs-quota-class-sets
替换卷快照的元数据	snapshots	updateSnapshotsMetadata
替换卷的元数据	volumes	updateVolumesMetadata
更新一致性组	consistencygroups	updateConsistencygroupsUpdate

操作名称	资源类型	事件名称
更新卷的单个元数据	volumes	updateVolumesSingleMetadata
更新卷快照的单个元数据	snapshots	updateSnapshotsSingleMetadata

6.3 网络

6.3.1 虚拟私有云

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6-8 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
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

操作名称	资源类型	事件名称
删除 VPN	vpn	deleteVpn
修改 VPN	vpn	modifyVpn

说明

表 6-9 中 VPC 的操作，为底层（OpenStack）服务触发；部分事件名称与表 6-8 中重复，是因为这些事件采用了异步调用的模式：操作下发会产生上表中描述的事件，而操作结果响应会产生表 6-9 中描述的事件。

表6-9 云审计服务支持的 VPC 操作列表（由底层服务触发）

操作名称	资源类型	事件名称
创建虚拟网络	network	createNetwork
更新虚拟网络	networks	updateNetwork
删除虚拟网络	networks	deleteNetwork
创建虚拟子网	subnets	createSubnet
更新虚拟子网	subnets	updateSubnet
删除虚拟子网	subnets	deleteSubnet
创建虚拟端口	ports	createPort
更新虚拟端口	ports	updatePort
删除虚拟端口	ports	deletePort
创建浮动 IP	floatingips	createFloatingip
更新浮动 IP	floatingips	updateFloatingip
删除浮动 IP	floatingips	deleteFloatingip
创建虚拟路由	routes	createRouter
更新虚拟路由	routes	updateRouter
删除虚拟路由	routes	deleteRouter
添加虚拟路由的接口	routes	addRouterInterface
删除虚拟路由的接口	routes	removeRouterInterface
为当前 vpc-router 添加扩展路由	routes	addExtraRoute
为当前 vpc-router 删除指定的扩展路由	routes	removeExtraRoute

操作名称	资源类型	事件名称
创建安全组	security-groups	createSecurity-group
删除安全组	security-groups	deleteSecurity-group
更新安全组	security-groups	updateSecurity-group
创建安全组规则	security-group-rules	createSecurity-group-rule
删除安全组规则	security-group-rules	deleteSecurity-group-rule
创建一个 vpnservice	vpn	createVpnService
更新 vpn-service	vpn	updateVpnService
删除 vpn-service	vpn	deleteVpnService
创建密钥交换策略	vpn	createVpnIkepolicy
更新密钥交换策略信息	vpn	updateVpnIkepolicy
删除租户指定 ikepolicy	vpn	deleteVpnIkepolicy
创建一个 ipsecpolicy	vpn	createVpnIpsecpolicy
更新指定 ipsecpolicy	vpn	updateVpnIpsecpolicy
删除指定的 ipsecpolicy	vpn	deleteVpnIpsecpolicy
创建一个 ipsec 连接	vpn	createVpnIpsec-site-connection
更新 ipsec 连接	vpn	updateVpnIpsec-site-connection
删除指定 ipsec 连接	vpn	deleteVpnIpsec-site-connection
Create VPN endpoint group	vpn	createVpnEndpoint-group
Update VPN endpoint group	vpn	updateVpnEndpoint-group
Remove VPN endpoint group	vpn	deleteVpnEndpoint-group
更新代理	agent	updateAgent
删除代理	agent	deleteAgent
指定网络使用的 DHCP Agent	agent	createAgentDhcp-network
移除网络使用的 DHCP Agent	agent	deleteAgentDhcp-network
更新指定租户的配额值	quota	updateQuota
重置指定租户的配额值	quota	deleteQuota

操作名称	资源类型	事件名称
创建 firewall group	FWaaS v2	createFirewallGroup
更新 firewall group	FWaaS v2	updateFirewallGroup
删除 firewall group	FWaaS v2	deleteFirewallGroup
创建 firewall policy	FWaaS v2	createFirewallPolicy
更新 firewall policy	FWaaS v2	updateFirewallPolicy
删除 firewall policy	FWaaS v2	deleteFirewallPolicy
firewall policy 中插入 firewall rule	FWaaS v2	insertFirewallPolicyRule
firewall policy 中移除 firewall rule	FWaaS v2	removeFirewallPolicyRule
创建 firewall rule	FWaaS v2	createFirewallRule
更新 firewall rule	FWaaS v2	updateFirewallRule
删除 firewall rule	FWaaS v2	deleteFirewallRule
创建 loadbalancer	loadbalancer	createLBaaSLoadbalancer
更新指定的 loadbalancer	loadbalancer	updateLBaaSLoadbalancer
删除指定的 loadbalancer	loadbalancer	deleteLBaaSLoadbalancer
创建 listener	listener	createLBaaSListener
更新指定的 listener	listener	updateLBaaSListener
删除指定的 listener	listener	deleteLBaaSlistener
创建 pool	pool	createLBaaSPool
更新指定的 pool	pool	updateLBaaSPool
删除指定的 Pool	pool	deleteLbaasPool
创建 Member	member	createLBaaSPoolMember
更新指定的 Member	member	updateLBaaSPoolMember
删除指定的 member	member	deleteLBaaSPoolMember
创建 healthmonitor	healthmonitor	createLBaaSHealthMonitor
更新指定的 healthmonitor	healthmonitor	updateLBaaSHealthMonitor
删除指定的 healthmonitor	healthmonitor	deleteLBaaSHealthMonitor

6.3.2 弹性负载均衡

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，配置云主机。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6-10 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
创建健康检查	healthcheck	createHealthcheck
删除健康检查	healthcheck	removeHealthcheck
更新健康检查	healthcheck	updateHealthcheck
创建证书	certificate	createCertificate
删除证书	certificate	removeCertificate
更新证书	certificate	updateCertificate
创建监听器	listener	createListener
删除监听器	listener	deleteListener
更新监听器	listener	updateListener
删除 ELB	elb	deleteELB
创建 ELB	elb	createELB
更新 ELB	elb	updateELB
添加后端主机	member	createMember
移除后端主机	member	deleteMember
配置访问日志	AccessLog	ConfigureAccessLog

6.4 管理与部署

6.4.1 云审计服务

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6-11 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
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

6.4.2 云监控

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6-12 云审计服务支持的云监控操作列表

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
告警规则状态变为 alarm	alarm_rule	alarmStatusChangeToAlarm
告警规则状态变为 ok	alarm_rule	alarmStatusChangeToOk
告警规则状态变为 insufficientData	alarm_rule	alarmStatusChangeToInsufficientData

6.4.3 应用运维管理

应用运维管理（Application Operations Management，以下简称 AOM）为运维人员提供一站式立体运维平台，实时监控应用、资源运行状态，通过数十种指标、告警与日志关联分析，快速锁定问题根源，保障业务顺畅运行。

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

表6-13 云审计服务支持的 AOM 操作列表

操作名称	资源类型	事件名称
创建仪表盘	ams	addDashboard
修改仪表盘	ams	updateDashboard
删除仪表盘	ams	deleteDashboard
创建阈值	ams	addThreshold
修改阈值	ams	updateThreshold
删除阈值	ams	deleteThreshold
创建策略组	pe	createPolicyGroup
删除策略组	pe	deletePolicyGroup
更新策略组	pe	updatePolicyGroup
启用策略组	pe	enablePolicyGroup
停用策略组	pe	disablePolicyGroup
创建策略	pe	createPolicy
删除策略	pe	deletePolicy
更新策略	pe	updatePolicy
启用策略	pe	enablePolicy
停用策略	pe	disablePolicy
更新老化周期	als	updateLogStorgeSetting

6.4.4 应用性能管理

应用性能管理服务（Application Performance Management，简称 APM）是实时监控并管理云应用性能和故障的云服务，提供专业的分布式应用性能分析能力，可以帮助运维人员快速解决应用在分布式架构下的问题定位和性能瓶颈等难题，为用户体验保驾护航。

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

表6-14 云审计服务支持的 APM 操作列表

操作名称	资源类型	事件名称

操作名称	资源类型	事件名称
删除应用	APM	clearApps
设置事务别名	APM	setAlias
更新虚机服务分组	APM	updateVirtualService
更新事务配置	APM	updateTxTypeSettings
更新拓扑 Apdex 阈值	APM	updateThresholds
设置事务分组	APM	txtypeGroupOperation
删除应用配置	apm	deleteAppGroup
更新采集开关配置	apm	setAppPpswitcherConfig
更新智能采样配置	apm	setAppCallChainConfig
更新内存检测机制配置	apm	setAppMwsConfig
更新日志增加 TraceID 配置	apm	setAppLogTransacConfig
更新 SQL 分析开关配置	apm	setAppSqlConfig
更新忽略 HTTP 响应代码或忽略错误和异常配置	apm	setAppIgnoreConfig

6.4.5 统一身份认证

统一身份认证服务（Identity and Access Management，以下简称 IAM）实现用户认证信息的集中管理。用户可以管理自己的已验证邮箱、已验证手机、密码等信息。当用户在调用 API 接口申请云主机或进行云资源管理以及使用多租户方式登录云平台时，也可实时查询所需的项目 ID、访问密钥（AK/SK）以及帐户名。

通过云审计服务，您可以记录与统一身份认证服务相关的操作事件，便于日后的查询、审计和回溯。

表6-15 云审计服务支持的 IAM 操作列表

操作名称	资源类型	事件名称
用户登录	user	login
用户登出	user	logout
登录重置密码	user	changePassword
创建用户	user	createUser
删除用户	user	deleteUser

操作名称	资源类型	事件名称
修改用户	user	updateUser
创建用户组	userGroup	createUserGroup
删除用户组	userGroup	deleteUserGroup
修改用户组	userGroup	updateUserGroup
创建 idp	identityProvider	createIdentityProvider
删除 idp	identityProvider	deleteIdentityProvider
修改 idp	identityProvider	updateIdentityProvider
更新 metadata	identityProvider	updateMetadata
更新帐号登录策略	domain	updateSecurityPolicies
更新密码策略	domain	updatePasswordPolicies
更新 ACL	domain	updateACLPolicies
更新安全警告策略	domain	updateWarningPolicies
创建 AK/SK	user	addCredential
删除 AK/SK	user	deleteCredential
修改邮箱	user	modifyUserEmail
修改手机	user	modifyUserMobile
修改密码	user	modifyUserPassword
登录开启双因子认证	user	modifySMVerify
上传头像	user	modifyUserPicture
创建信任	agency	createAgency
删除信任	agency	deleteAgency
修改信任信息	agency	updateAgency
修改 latch	user	modifyLatchVerify
修改 mc	user	modifyMCConnectVerify
管理员设置用户密码	user	setPasswordByAdmin
切换角色	user	switchRole