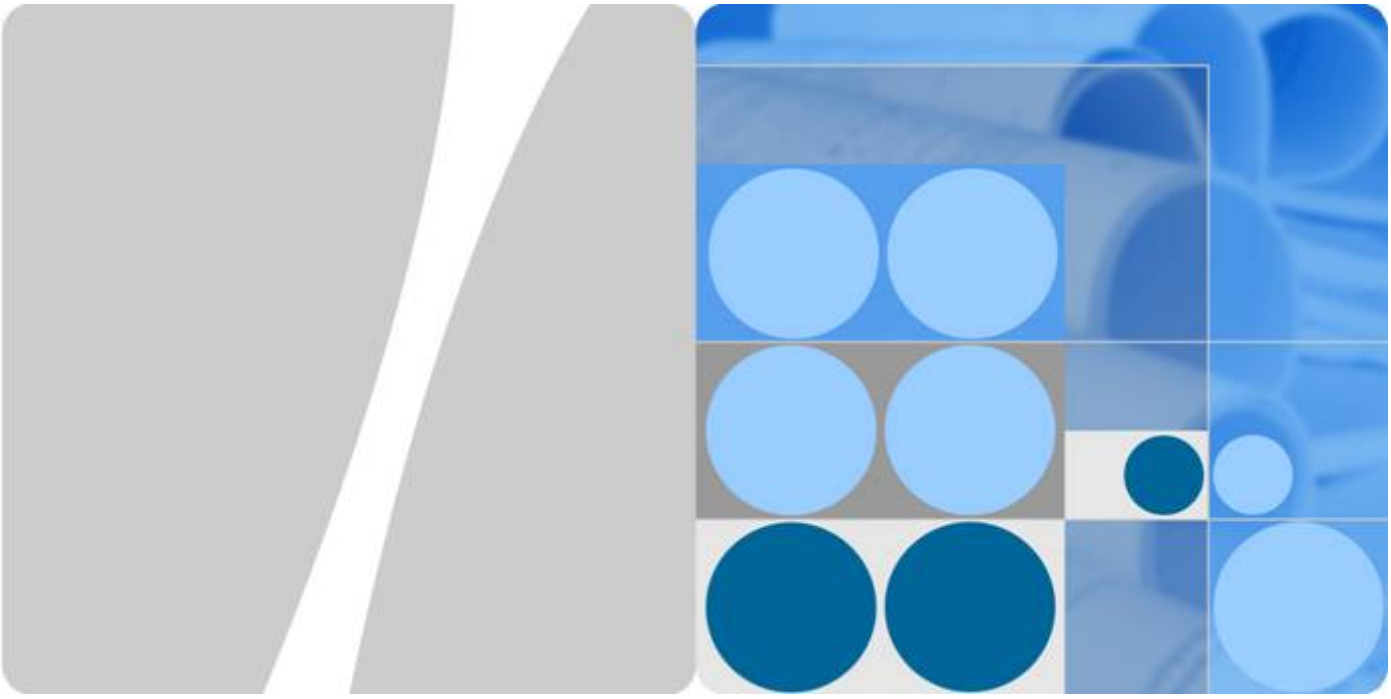


云审计服务

快速入门

文档版本　01

发布日期　2020-03-13

华为技术有限公司

HUAWEI

商标声明


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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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 开通云审计服务

操作场景

使用云审计服务前需要先开通云审计服务，如果不开通云审计服务，则无法对资源操作进行记录。开通后CTS会自动创建一个追踪器，并将当前租户的所有操作记录在该追踪器中。CTS最多显示近7天的事件，为了长期保存操作记录，可以将事件文件保存至对象存储服务中。因此，开通云审计服务之前，请先开通对象存储服务，且用户对即将要使用的OBS桶具有完全的使用权限。

本节介绍如何开通云审计服务。

前提条件

已注册华为云，并且通过了实名认证。

关联服务

- 对象存储服务（Object Storage Service，简称OBS）：存储事件文件。

  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。

- 数据加密服务（Data Encryption Workshop，简称DEW）：为事件文件加密功能提供密钥。
- 消息通知服务（Simple Message Notification，简称SMN）：检测到关键操作时，调用消息通知服务向用户发送邮件、短信通知。

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”，进入云审计服务页面。
3. 单击“点击开通”，开通云审计服务。
4. 在弹出的开通云审计服务详情页面，单击“开通”，完成开通云审计服务，系统会自动分配一个追踪器。

   “应用到所有region”开关默认开启，表示在所有Region下同步创建追踪器，帮助提升审计日志的全面性和准确性。

5. 填写OBS桶和操作事件文件前缀。参数说明如**表1**所示。

表 1-1 参数说明

参数	解释	取值样例
OBS桶	选择用于存储操作事件的OBS桶名称。 **说明** 由于OBS桶名需全局唯一，在创建桶时需前往中心Region查询是否存在同名桶，因此创建桶操作的日志将记录在中心Region。创建桶成功后，其他操作的日志将记录在各自桶归属的Region。	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。

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以及对OBS桶中数据的操作。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或导出最近7天的操作记录。

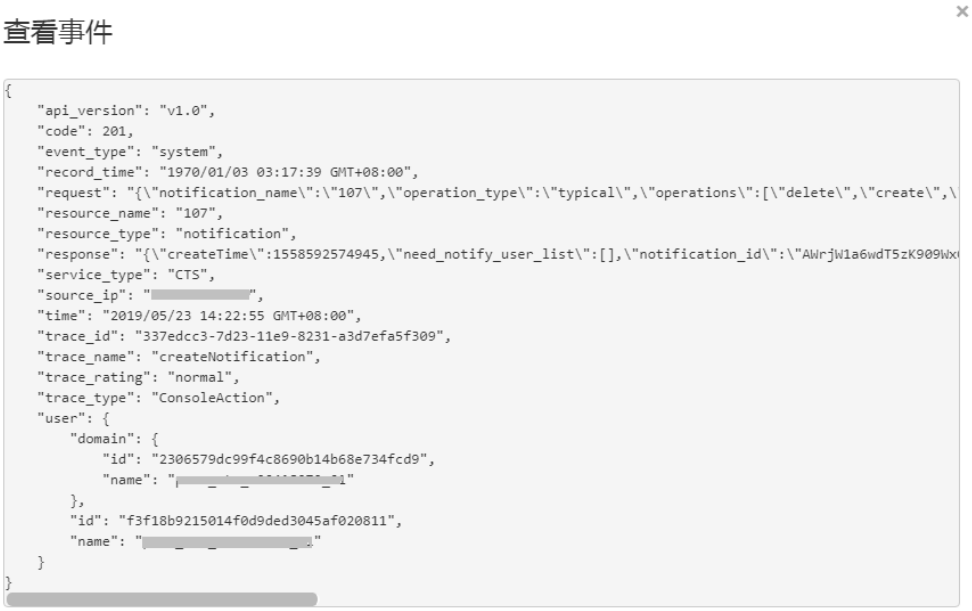
操作步骤

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”，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. 事件列表支持通过高级搜索来查询对应的操作事件。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。
     其中筛选类型选择资源ID时，还需选择或者手动输入某个具体的资源ID。
   - 操作用户：在下拉框中选择某一具体的操作用户。
   - 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：可在页面右上角选择查询最近1小时、最近1天、最近1周及自定义时间段的操作事件。

     说明

     由于IAM是Global服务，因此IAM相关的操作通知项仅在Global中呈现。
5. 选择查询条件后，单击“查询”。
6. 在需要查看的事件左侧，单击 展开该记录的详细信息。

7. 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。



单击右侧的“导出”，将查询结果以CSV格式的文件导出，该CSV文件包含了云审计服务记录的七天以内的操作事件的所有信息。

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。

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”，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。
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*”，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《云审计服务用户指南》的“事件结构”和“事件样例”章节。

图 3-1 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，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。

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。
- 云审计服务最多支持对10个用户组的50个用户发起的操作进行通知配置，用户组不支持多选，但支持对同一用户组下的多个用户进行多选；
- 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，旧版关键操作通知功能将于近期下线。

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”，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。

     说明

     由于IAM是Global服务，因此“登录”操作通知项仅在Global中呈现。

   - 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。目前支持对10个用户组的50个特定用户发起的操作进行配置，用户组不支持多选，但同一用户组下的多个用户支持多选。

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。

