

云审计

快速入门

文档版本 01
发布日期 2024-05-14



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。

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目录

1 入门指引.....	1
2 查询审计事件.....	3
3 查询转储事件.....	6
4 关键操作通知.....	9
5 入门实践.....	12

1 入门指引

操作场景

用户首次进入云审计服务时，在追踪器页面单击“开通云审计服务”，系统会自动为您创建一个名为system的管理追踪器，之后您也可以在追踪器页面创建多个数据追踪器。管理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。数据追踪器会记录租户对OBS桶中的数据操作的详细信息。

用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)，才可在OBS桶里面查看历史文件。否则，您将无法追溯7天以前的操作记录。

前提条件

已[注册华为账号并开通华为云](#)，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。
- 云日志服务（Log Tank Service，简称LTS）：提供日志存储功能。
- 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。

首次开通云审计服务

步骤1 登录管理控制台。

步骤2 如果您是以主账号登录华为云，请直接进行[步骤3](#)；如果您是以IAM用户登录华为云，需要联系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3** 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。
- 步骤4** 在左侧导航栏选择“追踪器”，单击右上方的“开通云审计服务”按钮，系统会自动为您创建一个名为system的管理类事件追踪器。管理类事件追踪器用于记录管理类事件，即针对所有云资源的操作日志，例如创建、登录、删除等。
- 步骤5** 后续您创建的追踪器均为数据类事件追踪器。数据追踪器会记录租户对OBS桶中的数据操作的详细信息。
- 步骤6** 在左侧导航栏选择“事件列表”，可以查看最近七天的事件操作记录。

----结束

2 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近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：

- [在新版事件列表查看审计事件](#)
- [在旧版事件列表查看审计事件](#)

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)，才可在OBS桶里面查看历史文件。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。

在新版事件列表查看审计事件

1. 登录管理控制台。
2. 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，您可以在筛选器组合一个或多个筛选条件：
 - 事件名称：输入事件的名称。
 - 事件ID：输入事件ID。
 - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。

- 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
 - 云服务：在下拉框中选择对应的云服务名称。
 - 资源类型：在下拉框中选择对应的资源类型。
 - 操作用户：在下拉框中选择一个或多个具体的操作用户。
 - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
 - normal：表示操作成功。
 - warning：表示操作失败。
 - incident：表示比操作失败更严重的情况，例如引起其他故障等。
 - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。
5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
- 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
 - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击按钮，可以获取到事件操作记录的最新信息。
 - 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见[事件结构](#)和[事件样例](#)。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 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. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 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。
 - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
 - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
 - 筛选类型按资源名称筛选时，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7天内任意时间段的操作事件。
 - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
6. 选择完查询条件后，单击“查询”。
 7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
 - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击按钮，可以获取到事件操作记录的最新信息。
 8. 在需要查看的事件左侧，单击展开该记录的详细信息。

事件名称	资源类型	云服务	资源ID	资源名称	事件级别	操作用户	操作时间	操作
createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	normal		2023/11/16 10:54:04 GMT+08:00	查看事件

request

Trace_id

code

trace_name

resource_type

trace_rating

api_version

message

source_ip

domain_id

trace_type

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。

查看事件

```
{
  "request": "",
  "trace_id": "676d4ae3-842b-11ee-9299-9159eee6a3ac",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/manager/utils/secret, Reason:",
  "source_ip": "",
  "domain_id": "",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": "",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "2023/11/16 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": "",
      "id": ""
    }
  }
}
```

10. 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》中的[事件结构](#)和[事件样例](#)。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

3 查询转储事件

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。云审计服务还支持将审计日志保存到LTS日志流中。

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，以及如何在LTS日志流中查看事件记录。

前提条件

已在云审计服务中成功配置追踪器，且打开OBS转储开关或LTS转储开关。配置方法请参见[配置追踪器](#)。

查询 OBS 中转储事件

配置追踪器时，若打开“转储到OBS”开关，操作事件将以事件文件的形式按周期保存至OBS桶。

1. 登录管理控制台。
2. 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“存储服务”下的指定的OBS桶名称，页面跳转到OBS管理控制台上对应OBS桶的对象管理界面。

图 3-1 选择 OBS



- 在OBS桶中，按照事件文件存储路径选择需要查看的历史事件，然后单击右侧的“下载”，文件将下载到浏览器默认下载路径。如需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>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-project_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。
 下载将产生请求费用和流量费用。
 关于云审计服务事件结构的关键字段详解，请参见[事件结构](#)和[事件样例](#)。

图 3-2 查看事件文件内容



- 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。

查询 LTS 中转储事件

配置追踪器时，若打开“转储到LTS”开关，操作事件将转储到“CTS/{Tracker Name}”日志流中。{Tracker Name}为当前追踪器的名称，例如管理类追踪器的日志流路径为“CTS/system-trace”。

步骤1 登录管理控制台

步骤2 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务控制台页面。

步骤3 单击左侧导航树的“追踪器”，进入追踪器信息页面。

步骤4 单击“存储服务”下的指定的LTS日志流名称，页面跳转到LTS管理控制台上对应LTS日志流界面。

步骤5 在CTS日志流界面，选择“{Tracker Name}”日志流，查看事件日志。

关于云审计服务事件结构的关键字段详解，请参见[事件结构](#)和[事件样例](#)。

步骤6 单击  按钮，可以下载日志文件到本地。

 **说明**

LTS单次下载支持最大5,000条日志。若所选日志超过5000条，不可使用LTS本地下载功能，请选择OBS转储下载。

----**结束**

4 关键操作通知

云审计服务在记录某些特定关键操作时，支持通过消息通知服务（SMN）对这些关键操作实时向相关订阅者发送通知（向用户手机、邮箱发送消息，也可直接发送http/https消息），该功能由云审计服务触发，消息通知服务完成通知发送。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。

操作场景

关键操作通知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。
- 云审计服务支持创建100个关键操作通知：
 - 自定义类型的关键操作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。
 - 完整类型的关键操作通知，支持通知主题。
- 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。
- 单个关键操作通知支持最多对10个用户组的50个用户发起的操作进行通知配置。单个关键操作通知不支持一次选择多个用户组，但是可以分次添加不同用户组中的用户在同一个关键操作通知。

创建关键操作通知

1. 登录管理控制台。

2. 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。
选中的操作将作为触发器，在操作发生时，即时发送SMN通知。
 - 操作类型：根据具体使用场景，选择“完整”和“自定义操作”触发场景。
 - 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，请参见[支持审计的服务及详细操作列表](#)。
 - 高级筛选：可以通过配置筛选条件设置触发通知的操作范围。当开启高级筛选后，可以对api_version、code、trace_rating、trace_type、resource_id、resource_name 6个参数进行配置，最多可同时对6个参数配置6个筛选条件。当配置多个条件时可以选择多条件的关系，是“当所有条件满足时生效（AND）”还是“有一个条件满足时生效（OR）”。
7. 配置用户。
当指定的用户发起关键操作时，可以通过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：
 - 创建云服务委托：必选，勾选创建云服务委托后，用户在创建关键操作通知时，云审计服务将会自动创建一个云服务委托，委托授权您使用消息通知服务（SMN）。
 - SMN主题：需要选择已创建的SMN主题或者单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。
9. 单击“确定”。

管理关键操作通知

创建完关键操作通知后，可在通知列表中查看关键操作通知的名称、状态、模板、SMN主题等信息，并可根据需要删除。

步骤1 登录管理控制台。

步骤2 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。

步骤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，根据需要执行以下操作，具体请参见表4-1。

表 4-1 相关操作

操作	说明
查看关键操作通知	单击通知名称，可以查看该通知的操作列表和用户列表详细信息。
启/停关键操作通知	单击操作列“启用/停用”，可以开启/关闭该关键操作通知。 说明 只有配置了SMN的关键操作通知，云审计服务才能正常启用/停用关键操作通知，未配置SMN则无法启用关键操作通知。
修改关键操作通知	单击操作列“修改”，可修改该关键操作通知的配置信息。
删除关键操作通知	单击操作列“删除”，可删除该关键操作通知。
搜索通知	在列表上方的搜索框，可以过滤通知名称、状态、模板名称和SMN主题来搜索通知。
刷新通知	单击右上角的  按钮，可刷新关键操作通知列表信息。
基础设置	单击右上角的  按钮，可以设置表格内容折行、固定操作列和自定义列表项的展示/隐藏。

----结束

5 入门实践

当您完成了查看审计事件、配置追踪器等基本操作后，可以根据自身的业务需求使用云审计服务提供的一系列常用实践。

表 5-1 常用最佳实践

实践	描述
结合函数工作流对登录/登出进行审计分析	该实践介绍如何通过CTS云审计服务，完成对公有云账户的各个云服务资源操作和结果的实时记录。 通过在函数工作流服务中创建CTS触发器获取订阅的资源操作信息，经由自定义函数对资源操作的信息进行分析和处理，产生告警日志。再由SMN消息通知服务通过短信和邮件推送告警信息，通知业务人员进行处理。