云审计

快速入门

文档版本 01

发布日期 2024-08-30

华为云计算技术有限公司

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 在 CTS 事件列表查看云审计事件

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)或云日志服务(LTS)，才可在OBS桶或LTS日志组里面查看历史事件信息。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。
- 企业项目ID：输入企业项目ID。
- 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
- 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7天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

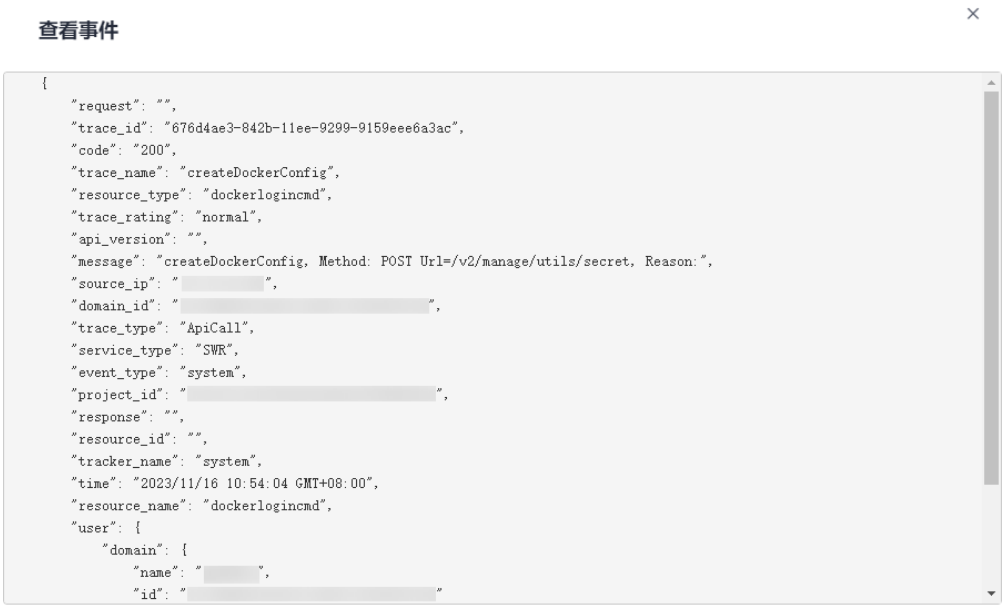
1. 登录管理控制台。
2. 单击左上角，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。

- 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1小时、最近1天、最近1周的操作事件，也可以自定义最近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。

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。



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。

2 配置云审计事件转储至 OBS 并查看

云审计服务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，记录的事件信息会在云审计中保存7天。如果需要将操作记录保存7天以上，则需要配置事件转储至OBS功能，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。

本文将为您介绍云审计服务（CTS）配置事件转储至OBS的操作流程，并指导您在OBS桶中查看历史事件记录，帮助您快速上手云审计服务。

1. **准备工作**

   在配置事件转储至OBS之前，您需要完成注册华为云并实名认证、为账户充值、为用户添加操作权限的准备工作。

2. **配置事件转储至OBS**

   在管理类事件追踪器配置页面，开启“转储到OBS”功能后，您就能将审计日志周期性的转储至对象存储服务下的OBS桶。

3. **在OBS桶中查看历史事件记录**

   在对象存储服务的OBS桶中，您可以下载事件文件查看已保存至OBS桶的历史操作记录。

准备工作

1. **注册华为云并实名认证。**

   如果您已有一个华为账户，请跳到下一个任务。如果您还没有华为账户，请参考以下步骤创建。

   a. 打开**华为云官网**，单击“注册”。

   b. 根据提示信息完成注册，详细操作请参见**如何注册华为云管理控制台的用户?**。

      注册成功后，系统会自动跳转至您的个人信息界面。

   c. 参考**实名认证**完成个人或企业账号实名认证。

2. **为账户充值。**

   使用事件转储至OBS功能会产生额外费用，您需要确保账户有足够金额。

   - 关于OBS服务的价格，请参见**对象存储服务价格详情**。
   - 关于充值，请参见**如何给华为账户充值**。

3. **为用户添加操作权限。**

如果您是以主账号登录华为云，请跳到下一个任务。

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**。

配置事件转储至 OBS

步骤1 进入**云审计服务页面**。

步骤2 在“区域”下拉列表中，选择靠近您应用程序的区域，可降低网络延时、提高访问速度。

在本案例中，选择“华北-北京四”区域。

步骤3 在左侧导航栏，单击“追踪器”，进入追踪器页面。

步骤4 在system追踪器右侧的操作栏，单击“配置”。

图 2-1 配置 system 追踪器

步骤5 在基本信息页面，按照如下参数进行设置，设置完成后，单击“下一步”。

图 2-2 设置基本信息

表 2-1 设置基本信息

参数	参数说明	本案例示例
追踪器名称	管理类事件追踪器的名称默认为“system”，不可修改。	system

参数	参数说明	本案例示例
企业项目	企业项目是一种云资源管理方式，由企业项目管理服务提供将云资源统一按项目管理、项目内的资源管理或成员管理。开启企业项目的具体操作请参考**创建企业项目**。 ● 如果您没有开通企业项目管理服务，请跳到下一项。 ● 如果您开通了企业项目管理服务，在本案例中，企业项目选择“default”即可。	default
应用到我的组织	云审计服务支持组织云服务的多账号关系的管理能力，开启“应用到我的组织”后，可以实现以下能力，具体操作请参考**组织追踪器**。 1. 使用组织管理员账号，在组织云服务中启用云审计可信服务并设置委托管理员账号。 2. 使用委托管理员账号，在云审计服务中配置组织追踪器，配置完成后，委托管理员账号就可以实现安全审计等云审计能力。	不开启开关
事件操作类型	勾选“排除KMS事件”后，追踪器将不会转储您对数据加密服务（DEW）的相关操作。 数据加密服务（DEW）的相关审计操作请参考**数据加密服务相关的操作事件**。	不勾选“排除KMS事件”

步骤6 在配置转储页面，按照如下参数进行设置，设置完成后，单击“下一步 > 配置”，配置追踪器完成后，系统立即以新的规则开始记录操作。

图 2-3 配置转储

表 2-2 设置基本信息

参数	参数说明	本案例示例
转储到OBS	云审计服务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，记录的事件信息会在云审计中保存7天。如果需要将操作记录保存7天以上，则需要配置事件转储至OBS功能，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。 开启“转储到OBS”功能后，您就能将审计日志周期性的转储至对象存储服务下的OBS桶。	开启开关
创建云服务委托	用户开启“转储到OBS”功能后，必须勾选“创建云服务委托”，云审计服务将会自动创建一个云服务委托cts_admin_trust，委托授权您使用对象存储服务（OBS）。	勾选“创建云服务委托”
OBS桶所属用户	您可以将事件转储至当前用户或其他用户的OBS桶中，方便统一管理。 ● 选择当前用户：无需授予转储权限。 ● 选择其他用户：转储前需要OBS桶所属用户已经对您当前用户授予转储权限，否则会造成转储失败。授予转储权限的方法请参考**跨租户转储授权**。	选择“当前用户”
选择OBS	您可以选择新建OBS桶或选择已有OBS桶，若所选的OBS桶的区域与当前所在区域不同，则不支持创建新的OBS桶，只能选择已有OBS桶。 ● 新建OBS桶：在您填写一个桶名后系统将自动为您创建一个OBS桶。 ● 选择已有OBS桶：需要您选择一个已有的OBS桶。	选择“新建OBS桶”
OBS桶名称	OBS桶名称不能为空，仅支持小写字母、数字、“-”和“.”，且长度范围为3-63个字符。禁止两个“.”相邻（如“my..bucket”），禁止“.”和“-”相邻（如“my-.bucket”和“my.-bucket”），禁止使用ip为桶名称。	system-bucket-01
保存周期	不同类型、不同级别的合规认证标准对审计日志的保存时间有不同的要求，当您配置管理类事件追踪器时，保存周期默认“沿用OBS配置”，不支持修改。	沿用OBS配置

参数	参数说明	本案例示例
事件文件名前缀	事件文件名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。事件文件名前缀只能由英文字母、数字、下划线(_)、中划线(-)和小数点(.)组成，且长度范围为0-64个字符。 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：FilePrefix_CloudTrace_region-project_2016-05-30T16-20-56Z_21d36ced8c8af71e.json.gz	FilePrefix
文件校验	开启“文件校验”开关，即可启用事件文件完整性校验功能，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OBS桶中，您可以使用这些文件实现自己的校验解决方案。 事件文件完整性校验详细操作请参考**事件文件完整性校验**。 有关摘要文件的更多信息，请参阅**摘要文件**。	不开启开关
加密事件文件	云审计支持对事件文件加密存储，在转储过程中需使用数据加密服务（简称DEW）中的密钥对存储在OBS桶中的事件文件进行加密。 当OBS所属用户选择“当前用户”时，开启“加密事件文件”开关，云审计会从DEW获取当前用户的秘钥ID，在下拉选项可以直接选择秘钥。	不开启开关

----结束

在 OBS 桶中查看历史事件记录

您已经配置了system追踪器将事件转储至OBS桶，系统立即以新的规则开始记录操作，您现在可以在OBS桶中下载并查看历史事件文件。

步骤1 在追踪器页面，system追踪器的“存储服务”一栏，会显示您在配置转储时设置的OBS桶“system-bucket-01”，单击OBS桶名称，页面跳转到对象存储服务控制台上“system-bucket-01”桶的管理界面。

图 2-4 单击 OBS 桶名称

步骤2 在“system-bucket-01”桶的管理界面左侧的导航栏，单击“对象”。

步骤3 在对象页面，请您需要按照事件文件存储路径依次点开文件夹。

在本案例中，请您依次点开“CloudTraces > cn-north-4 > 2024 > x月 > x日 > system > OBS”。在本案例中，x月x日是您新建OBS桶“system-bucket-01”的日期。

说明

事件文件存储路径格式：***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***

图 2-5 事件文件存储路径

步骤4 在本案例中，请您找到“最后修改时间”最早的文件，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”。

说明

- 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：FilePrefix_CloudTrace_cn-north-4_2024-08-13T07-23-42Z_eaac2d5c641fe022.json.gz
- 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。

步骤5 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历史操作事件日志信息。

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 2-6 下载解压后的 json 文件

----结束

3 配置云审计事件转储至 LTS 并查看

云审计服务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，控制台事件列表中会保存最近7天的操作记录。如果需要将操作记录保存7天以上，则需要配置事件转储至LTS功能，云审计服务会定期将操作记录同步保存到用户定义的LTS日志流中进行长期保存。

本文将为您介绍云审计服务（CTS）配置事件转储至OBS的操作流程，并指导您在OBS桶中查看历史事件记录，帮助您快速上手云审计服务。

1. **准备工作**

   在配置事件转储至LTS之前，您需要完成注册华为云并实名认证、为账户充值、为用户添加操作权限的准备工作。

2. **配置事件转储至LTS**

   在管理类事件追踪器配置页面，开启“转储到LTS”功能后，您就能将审计日志周期性的转储至云日志服务下的LTS日志流。

3. **在LTS日志流中查看历史事件记录**

   在云日志服务的LTS日志流中，您可以查看已保存至LTS日志流中的历史操作记录。

准备工作

1. **注册华为云并实名认证。**

   如果您已有一个华为账户，请跳到下一个任务。如果您还没有华为账户，请参考以下步骤创建。

   a. 打开**华为云官网**，单击“注册”。

   b. 根据提示信息完成注册，详细操作请参见**如何注册华为云管理控制台的用户?**。

      注册成功后，系统会自动跳转至您的个人信息界面。

   c. 参考**实名认证**完成个人或企业账号实名认证。

2. **为账户充值。**

   日志转储到LTS功能会产生额外费用，您需要确保账户有足够金额。

   - 关于LTS服务的价格，请参见**云日志服务价格详情**。
   - 关于充值，请参见**如何给华为账户充值**。

3. **为用户添加操作权限。**

如果您是以主账号登录华为云，请跳到下一个任务。

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**。

4. **在云日志服务控制台配置云审计服务CTS接入LTS**

   如果您是第一次使用云审计日志转储到LTS功能，您需要先在云日志服务中配置CTS接入LTS，请参考以下步骤配置。

   a. 进入**云日志服务页面**。

   b. 在左侧导航栏中，选择“日志接入”，单击“云审计 CTS”进行CTS接入配置。

   c. 在配置页面，“所选日志组”和“所选日志流”保持默认，单击“下一步：CTS配置”>“下一步：日志流配置”>“提交”。

配置事件转储至 LTS

步骤1 进入**云审计服务页面**。

步骤2 在“区域”下拉列表中，选择靠近您应用程序的区域，可降低网络延时、提高访问速度。

在本案例中，选择“华北-北京四”区域。

步骤3 在左侧导航栏，单击“追踪器”，进入追踪器页面。

步骤4 在system追踪器右侧的操作栏，单击“配置”。

图 3-1 配置 system 追踪器

步骤5 在基本信息页面，按照如下参数进行设置，设置完成后，单击“下一步”。

图 3-2 设置基本信息

表 3-1 设置基本信息

参数	参数说明	本案例示例
追踪器名称	管理类事件追踪器的名称默认为“system”，不可修改。	system
企业项目	企业项目是一种云资源管理方式，由企业项目管理服务提供将云资源统一按项目管理、项目内的资源管理或成员管理。开启企业项目的具体操作请参考**创建企业项目**。 • 如果您没有开通企业项目管理服务，请跳到下一项。 • 如果您开通了企业项目管理服务，在本案例中，企业项目选择“default”即可。	default
应用到我的组织	云审计服务支持组织云服务的多账号关系的管理能力，开启“应用到我的组织”后，可以实现以下能力，具体操作请参考**组织追踪器**。 1. 使用组织管理员账号，在组织云服务中启用云审计可信服务并设置委托管理员账号。 2. 使用委托管理员账号，在云审计服务中配置组织追踪器，配置完成后，委托管理员账号就可以实现安全审计等云审计能力。	不开启开关
事件操作类型	勾选“排除KMS事件”后，追踪器将不会转储您对数据加密服务（DEW）的相关操作。 数据加密服务（DEW）的相关审计操作请参考**数据加密服务相关的操作事件**。	不勾选“排除KMS事件”

步骤6 在配置转储页面，按照如下参数进行设置，设置完成后，单击“下一步 > 配置”，配置追踪器完成后，系统立即以新的规则开始记录操作。

图 3-3 配置转储

表 3-2 设置基本信息

参数	参数说明	本案例示例
转储到LTS	云审计服务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，控制台事件列表中会保存最近7天的操作记录。如果需要将操作记录保存7天以上，则需要配置事件转储至LTS功能，云审计服务会定期将操作记录同步保存到用户定义的LTS日志流中进行长期保存。 开启“转储到LTS”功能后，您就能将审计日志周期性的转储至云日志服务下的LTS日志流。	开启开关

参数	参数说明	本案例示例
日志组名称	日志组名称默认为“CTS”，不支持修改。操作事件将转储到“CTS/system-trace”日志流中。	CTS

----结束

在 LTS 日志流中查看历史事件记录

您已经配置了system追踪器将事件转储至LTS日志流，系统立即以新的规则开始记录操作，您现在可以在LTS日志流中查看历史事件文件。

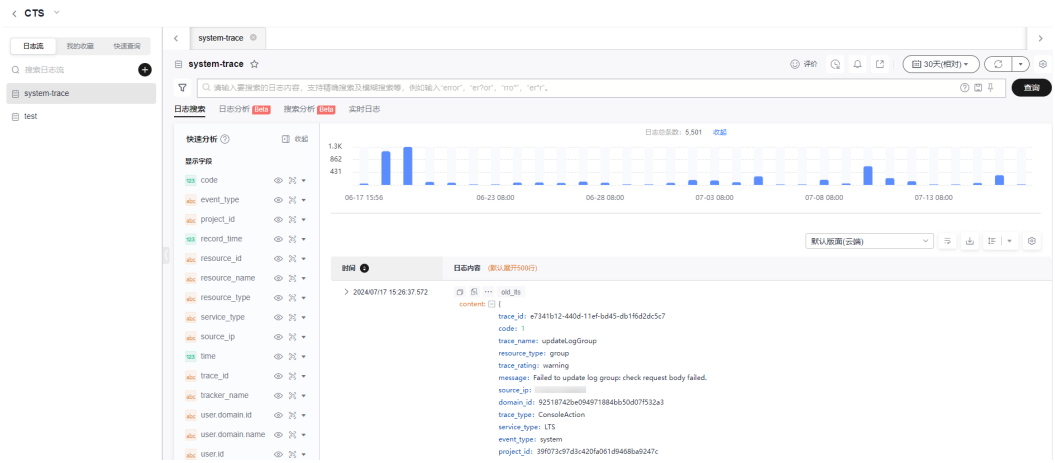
步骤1 在追踪器页面，system追踪器的“存储服务”一栏，会显示您在配置转储时设置的LTS日志流“CTS/system-trace”，单击日志流名称，页面跳转到云日志服务控制台上“CTS/system-trace”日志流界面。

图 3-4 单击日志流名称

步骤2 在“CTS/system-trace”日志流界面，您可以查看历史操作事件日志信息。

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 3-5 system-trace 日志流页面



步骤3 单击按钮，您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 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 4-1 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。