云审计

快速入门

文档版本 01

发布日期 2025-08-01

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

场景描述

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，您可以很方便地实现安全审计、问题跟踪、资源定位，帮助您更好地规划和利用已有资源、甄别违规或高危操作。

什么是事件

事件即云审计服务追踪并保存的云服务资源的操作日志，操作包括用户对云服务资源新增、修改、删除等操作。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。

什么是管理类追踪器和数据类追踪器

管理追踪器会自动识别并关联当前用户所使用的所有云服务，并将当前用户的所有操作记录在该追踪器中。管理追踪器记录的是管理类事件，即用户对云服务资源新建、修改、删除等操作事件。

数据追踪器会记录用户对OBS桶中的数据操作的详细信息。数据类追踪器记录的是数据类事件，即OBS服务上报的用户对OBS桶中数据的操作事件，例如上传数据、下载数据等。

约束与限制

- 管理类追踪器未开启组织功能之前，单账号跟踪的事件可以通过云审计控制台查询。管理类追踪器开启组织功能之后，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。组织追踪器的详细介绍请参见**组织追踪器概述**。
- 用户通过云审计控制台只能查询最近7天的操作记录，过期自动删除，不支持人工删除。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。
- 用户对云服务资源做出创建、修改、删除等操作后，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。

前提条件

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**。

查看审计事件

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 CTS 新版事件列表查看审计事件

步骤1 登录**CTS控制台**。

步骤2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

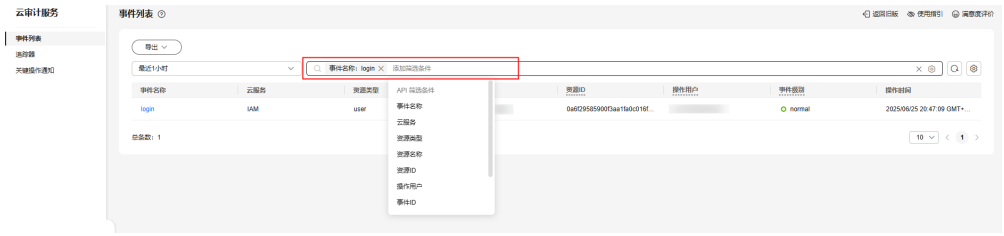
步骤3 在列表上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

步骤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。

表 1-1 事件筛选参数说明

参数名称	说明
事件名称	操作事件的名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务支持审计的操作事件的名称请参见**支持审计的服务及详细操作列表**。 示例：updateAlarm
云服务	云服务的名称缩写。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 示例：IAM

参数名称	说明
资源名称	操作事件涉及的云资源名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 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。 示例：ecs-name
资源ID	操作事件涉及的云资源ID。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该资源类型无资源ID或资源创建失败时，该字段为空。 示例：*{虚拟机ID}*
事件ID	操作事件日志上报到CTS后，查看事件中的trace_id参数值。 输入的值需全字符匹配，不支持模糊匹配模式。 示例：01d18a1b-56ee-11f0-ac81-******1e229
资源类型	操作事件涉及的资源类型。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务的资源类型请参见**支持审计的服务及详细操作列表**。 示例：user
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	下拉选项包含“normal”、“warning”、“incident”，只可选择其中一项。 • normal代表操作成功。 • warning代表操作失败。 • incident代表比操作失败更严重的情况，如引起其他故障等。
企业项目ID	资源所在的企业项目ID。 查看企业项目ID的方式：在EPS服务控制台的“项目管理”页面，可以查看企业项目ID。 示例：b305ea24-c930-4922-b4b9-******1eb2
访问密钥ID	访问密钥ID，包含临时访问凭证和永久访问密钥。 查看访问密钥ID的方式：在控制台右上方，用户名下拉选项中，选择“我的凭证 > 访问密钥”，可以查看访问密钥ID。 示例：HSTAB47V9V*******TLN9



步骤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。

步骤6 （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。

----结束

在 CTS 旧版事件列表查看审计事件

步骤1 登录CTS控制台。

步骤2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

步骤3 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。

步骤4 在页面右上方，可以通过筛选时间范围，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。

步骤5 事件列表支持通过筛选来查询对应的操作事件。

表 1-2 事件筛选参数说明

参数名称	说明
事件类型	事件类型分为“管理事件”和“数据事件”。 • 管理类事件，即用户对云服务资源新建、修改、删除等操作事件。 • 数据类事件，即OBS服务上报的OBS桶中的数据的操作事件，例如上传数据、下载数据等。
云服务	在下拉选项中，选择触发操作事件的云服务名称。
资源类型	在下来选项中，选择操作事件涉及的资源类型。 各个云服务的资源类型请参见支持审计的服务及详细操作列表。

参数名称	说明
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	可选项包含“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。 • Normal代表操作成功。 • Warning代表操作失败。 • Incident代表比操作失败更严重的情况，如引起其他故障等。

步骤6 选择完查询条件后，单击“查询”。

步骤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。

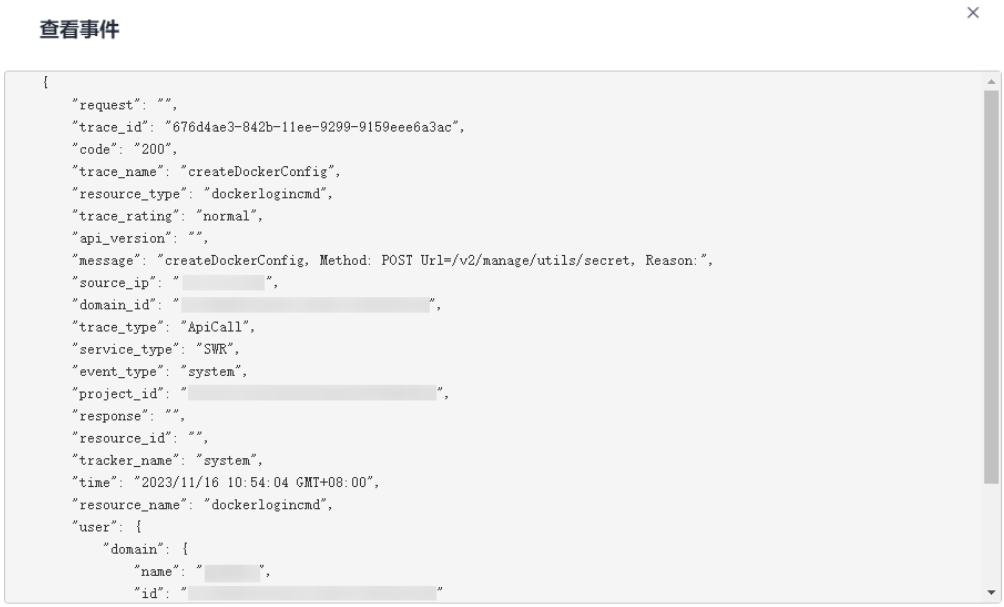
- 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
- 单击按钮，可以获取到事件操作记录的最新信息。

步骤8 在事件的“是否篡改”列中，您可以查看该事件是否被篡改：

- 上报的审计日志没有被篡改，显示“否”；
- 上报的审计日志被篡改，显示“是”。

步骤9 在需要查看的事件左侧，单击 展开该记录的详细信息。

步骤10 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。



步骤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。

----结束

相关文档

- 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**。
- 您可以通过以下示例，来学习如何查询具体的事件：
  - 使用云审计服务，审计最近两周内云硬盘服务的创建和删除操作。具体操作，请参见**安全审计**。
  - 使用云审计服务，定位现网某个弹性云服务器在某日上午发生的故障，以及定位现网创建弹性云服务器操作失败的问题。具体操作，请参见**问题定位**。
  - 使用云审计服务，查看某个弹性云服务器的所有的操作记录。具体操作，请参见**资源跟踪**。

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地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。

使用限制

- **全局级服务需要在中心region（中国-香港）的云审计控制台配置追踪器，才能使用审计事件转储至OBS功能。全局级服务在其他region的云审计控制台配置时，上述功能不会生效。您可以在约束与限制中，查阅目前华为云的全局级服务信息。**
- 在您没有配置转储前，云审计控制台对用户的操作事件日志保留7天，过期自动删除，在配置转储后也无法查看。

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“中国-香港”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
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DEW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DEW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地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。 ● 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。 **说明** 当前创建的OBS桶是一个单AZ标准存储的私有桶。如果需要其他额外配置，建议提前在OBS服务创建OBS桶，然后“选择已有OBS桶”。 ● 选择已有OBS桶：选择当前区域已创建的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_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_ap-southeast-1_2024-12-13T01-29-19Z_47b9d51830deff47.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获取当前用户的密钥ID，在下拉选项可以直接选择密钥。	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”。

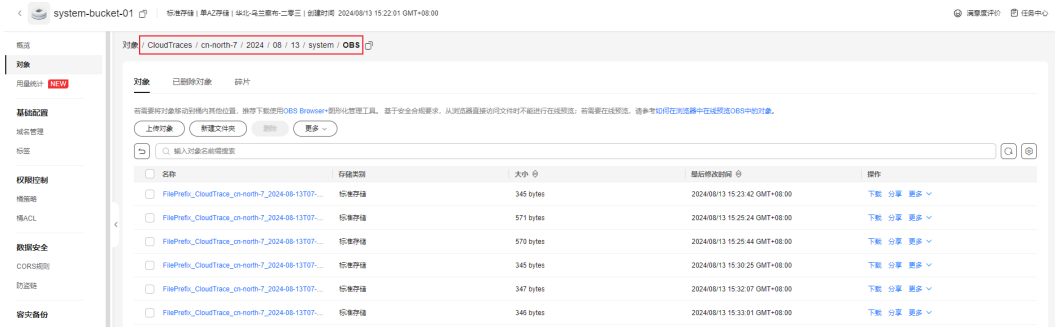
步骤3 在对象页面，请您需要按照事件文件存储路径依次点开文件夹。

在本案例中，请您依次点开“CloudTraces > ap-southeast-1 > 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_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_ap-southeast-1_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LTS的操作流程，并指导您在LTS日志流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地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。

使用限制

- **全局级服务需要在中心region（中国-香港）的云审计控制台配置追踪器，才能使用审计事件转储至LTS功能。全局级服务在其他region的云审计控制台配置时，上述功能不会生效。您可以在约束与限制中，查阅目前华为云的全局级服务信息。**
- 在您没有配置转储前，云审计控制台对用户的操作事件日志保留7天，过期自动删除，在配置转储后也无法查看。

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“接入 > 接入中心”，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“中国-香港”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DEW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DEW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地转储至云日志服务下的LTS日志流。	开启开关
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。

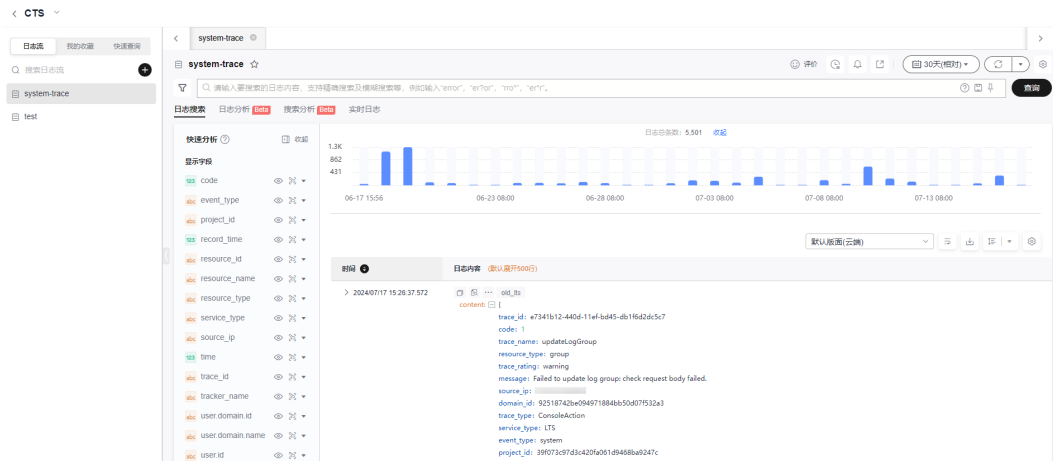
步骤1 在追踪器页面，system追踪器的“存储服务”一栏，会显示您在配置转储时设置的LTS日志流“CTS/system-trace”，单击日志流名称，页面跳转到云日志服务控制台上“CTS/system-trace”日志流界面。

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。

----结束

