云审计服务

用户指南

文档版本 01

发布日期 2025-01-22

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 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，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，也可以保存至LTS日志流。开通云审计服务之前，需要开通对象存储服务和云日志服务，且用户对即将要使用的OBS桶和LTS日志流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。

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。
- 配置事件转储功能，需要开通对象存储服务(OBS)和云日志服务(LTS)。
- 启用关键操作通知功能，需要开通消息通知服务(SMN)。

关联服务

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

说明

管理类事件追踪器记录用户对所有云服务资源的相关操作，例如创建、登录、删除等。云审计服务当前支持的云服务的详细信息，请参见**支持审计的服务及操作列表**。

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7天的事件操作记录。

----结束

相关信息

云审计服务的功能主要包括：

- 记录审计日志：支持记录用户通过管理控制台或API接口发起的操作，以及各服务内部自触发的操作。
- 审计日志查询：支持在管理控制台对7天内操作记录按照事件类型、事件来源、资源类型、筛选类型、操作用户和事件级别等多个维度进行组合查询。
- 审计日志转储：支持将审计日志周期性的转储至**对象存储服务**（Object Storage Service，简称OBS）下的OBS桶，转储时会按照服务维度压缩审计日志为事件文件，或转储至**云日志服务**（Log Tank Service，简称LTS）下的LTS日志流。
- 事件文件加密：支持在转储过程中使用**数据加密服务**（Data Encryption Workshop，简称DEW）中的密钥对事件文件进行加密。
- 关键操作通知：支持在发生特定操作时使用**消息通知服务**（Simple Message Notification，简称SMN）向用户手机、邮箱发送消息。

2 查询云审计事件

2.1 查询云审计事件

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。
- CTS新版事件列表不显示数据类审计事件，您需要在旧版事件列表查看数据类审计事件。
- 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，不支持人工删除。

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。

   说明

   您可以参考**云审计服务应用示例**，来学习如何查询具体的事件。
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

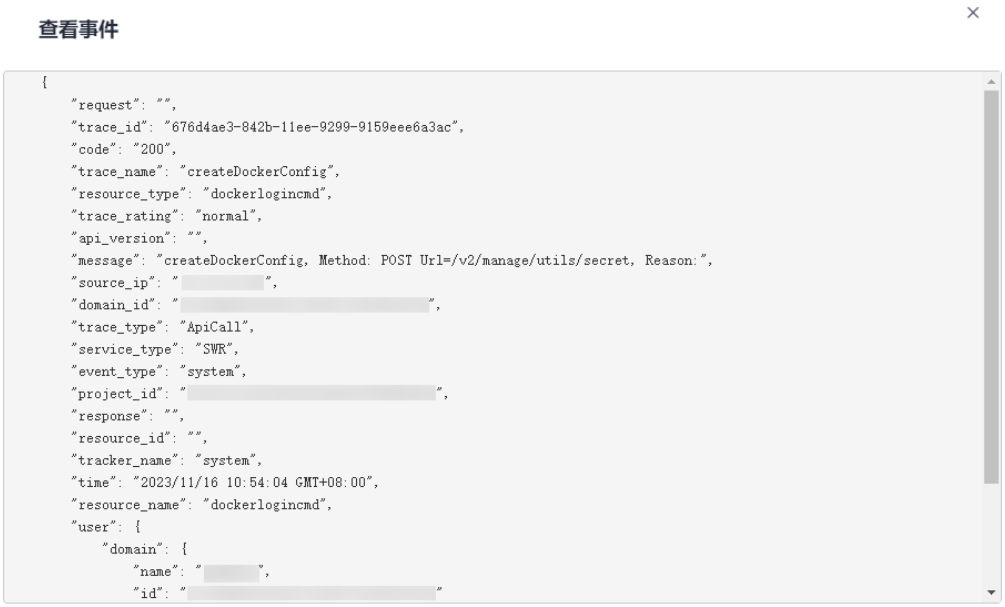
1. 登录管理控制台。
2. 单击左上角，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。

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。

   说明

   您可以参考**云审计服务应用示例**，来学习如何查询具体的事件。
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。

2.2 查询云审计服务转储事件

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。

使用限制

全局级服务需要在中心region（ 北京四 ）的云审计控制台配置追踪器，才能使用审计事件转储至OBS/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。

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。配置转储的方法请参见**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 2-1 选择 OBS

5. 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>cn-north-4>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：FilePrefix_CloudTrace_cn-north-4_2024-12-13T01-29-19Z_47b9d51830deff47.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。
   - 用户在配置追踪器转储至OBS时，关闭“路径按云服务划分”开关后，转储文件路径中不会显示“服务类型目录”。例如：User Define>CloudTraces>region>2016>5>19>system。

   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 2-2 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，下载解压后的json文件如图2-3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 2-3 下载解压后的 json 文件

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。

图 2-4 选择 LTS

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。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

3 管理类事件追踪器

云审计服务提供的追踪器分两类，包括管理类事件追踪器和数据类事件追踪器。

管理类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。数据类事件追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。

本章节介绍管理类追踪器的相关操作。

3.1 创建追踪器

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的管理类事件追踪器。管理类事件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。

使用限制

- CTS仅记录最近7天内的操作事件，您需要配置追踪器转储至OBS或LTS服务来保存更长时间的事件，否则将无法追溯7天前的操作事件。配置转储后，追踪器会将事件持续保存到您指定的OBS桶或LTS日志流中。
- 管理类追踪器只能有一个，删除后依旧会保留历史事件操作记录，重新开通云审计服务后可恢复管理类追踪器。

3.2 配置追踪器

操作场景

云审计服务管理控制台支持对已创建的管理类追踪器增加OBS转储、LTS转储等相关配置。

用户可以选择是否将已记录的事件发送到OBS桶永久保存。如果用户想要对管理类事件进行统一管理，还可以设置将多个账号记录的事件统一转储到一个OBS桶。

配置追踪器完成后，系统立即以新的规则开始记录操作。

本节介绍如何配置管理类事件追踪器。

使用限制

1. 全局级服务需要在中心region（北京四）的云审计控制台配置追踪器，才能使用审计事件转储至OBS/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。

2. OBS桶有标准存储、低频访问存储和归档存储三种类型。由于云审计服务需要高频次的访问转储的OBS桶，您在云审计控制台新建的OBS桶默认是一个单AZ标准存储的私有桶。如果您需要其他额外配置，建议提前在OBS服务创建OBS桶。详情请参考**创建桶**。
3. 当您配置追踪器转储至OBS时，您需要选择一个OBS桶，配置完成后，如果您在OBS服务删除了配置转储时选择的OBS桶，CTS的审计日志将无法转储至OBS，您将无法查询7天以上的历史审计记录。
4. 在CTS配置追踪器转储至OBS/LTS后，转储事件的保存周期以您在OBS/LTS控制台的配置为准：
   - 配置OBS桶存储时间需要您提前在OBS服务创建OBS桶，根据您的业务诉求选择“存储类别”，不同存储类别的OBS桶具有不同的存储时间，详情请参考**创建桶**。创建并配置好OBS桶后，在CTS配置追踪器转储至OBS时，选择已有OBS桶，转储事件的保存周期默认沿用您在OBS的配置。
   - 在CTS配置事件转储至LTS后，事件日志存储的周期以LTS日志组配置的日志存储时间为准，详情请参考**管理日志组**。

前提条件

已开通云审计服务。

配置管理类事件追踪器

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。

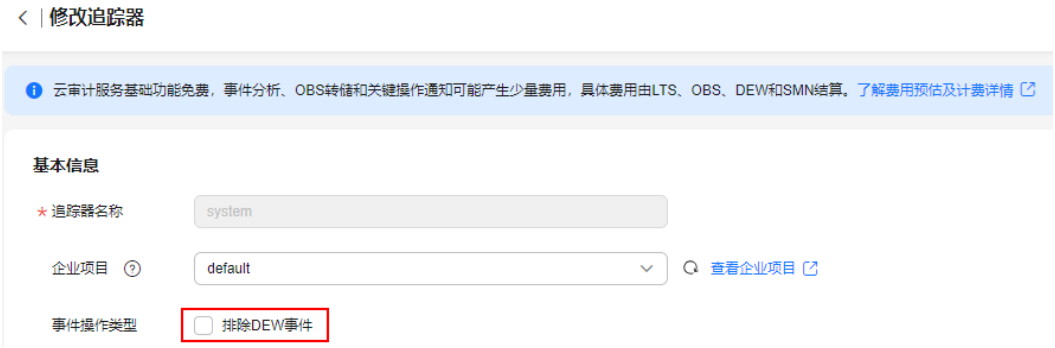
步骤4 单击左侧导航树的“追踪器”，进入追踪器信息页面。

步骤5 在管理类追踪器信息右侧，单击操作下的“配置”。

图 3-1 追踪器配置

步骤6 设置追踪器的基本信息，单击“下一步”。

图 3-2 排除 DEW 事件



参数名称	说明
追踪器名称	默认为system，不可修改。
企业项目	选择一个企业项目。 **说明** 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**。
排除DEW事件	默认不勾选。勾选后，用户对数据加密服务（DEW）的createDataKey操作和decryptDatakey操作将不会被转储到OBS/LTS。 **说明** 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**。

步骤7 在配置转储页面，您可以设置追踪器的转储信息。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)或配置转储到云日志服务(LTS)。具体参数说明参见**表3-1**和**表3-2**。

表 3-1 配置转储到 OBS 参数说明

参数名称	参数说明
转储到OBS	当“转储到OBS”开关打开时，您可以选择已存在的OBS桶或直接通过配置页面新建OBS桶，并配置事件文件前缀。 如果“转储到OBS”开关关闭时，则无需配置相应参数。
创建云服务委托	必选，勾选创建云服务委托后，用户在创建追踪器时，云审计服务将会自动创建一个云服务委托，委托授权您使用对象存储服务（OBS）。

参数名称	参数说明
OBS桶所属用户	云审计服务支持用户将事件转储至其他用户的OBS桶中，方便用户统一管理。 ● 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OBS	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”。详情请参考**创建桶**。 选择已有OBS桶：选择当前区域已创建的OBS桶。
OBS桶名称	当“选择OBS”选择“新建OBS桶”时，直接新建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。 当“选择OBS”选择“选择已有OBS桶”时，可以选择已存在的OBS桶。
保存周期	管理类事件追踪器的保存周期默认沿用在OBS的配置，不支持修改。
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。
是否压缩	压缩后可以减少对象存储空间的使用量。 ● 不压缩：按照 *.json格式转储。 ● gzip：按照*.json.gz格式转储。
路径按云服务划分	● “路径按云服务划分”开关打开后，转储文件路径中将增加云服务名，OBS同时出现多个小文件。例如：/CloutTrace/cn-north-7/2022/11/8/doctest/云服务/_XXX.json.gz ● “路径按云服务划分”开关关闭后，转储文件路径中不会增加云服务名。例如：/CloutTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz
日志转储路径	日志转储的路径，系统自动填写。
文件校验	可以检验转储至OBS桶的数据是否被篡改，保障事件文件的完整性。如何校验文件完整性可参考**校验云审计事件文件完整性**。

参数名称	参数说明
加密事件文件	当OBS所属用户选择“当前用户”时，可以为事件配置加密密钥。 “加密事件文件”开关打开时，云审计会从数据加密服务（DEW）获取当前用户的密钥ID，在下拉选项可以直接选择密钥。 **说明** 使用数据加密服务（DEW）中的密钥对OBS桶中的对象进行全量加密或者部分加密，详细操作请参见**OBS服务端加密**。

表 3-2 配置转储到 LTS 参数说明

参数名称	参数说明
转储到LTS	当“转储到LTS”开关打开时，表示操作事件将转储到日志流中。
日志组名称	当“转储到LTS”开关打开时，日志组名称默认为“CTS”。如果“转储到LTS”开关关闭时，则无需配置该参数。

步骤8 单击“下一步 > 配置”，完成配置管理类事件追踪器。

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。

步骤9 （可选）在追踪器页面，单击标签列下的，可以为该追踪器添加标签。

图 3-3 添加标签

标签以键值对的形式表示，用于标识追踪器，便于对追踪器进行分类和搜索。此处的标签仅用于追踪器的过滤和管理。一个追踪器最多添加20个标签。

如果您的组织已经设定云审计服务的相关标签策略，则需按照标签策略规则为追踪器添加标签。标签策略详细介绍请参考**标签策略**，标签管理详细介绍请参考**标签管理**。

表 3-3 标签说明

参数	说明	举例
标签键	输入标签的键，同一个追踪器标签的键不能重复。键可以自定义，也可以选择预先在标签服务（TMS）创建好的标签的键。 键命名规则如下： ● 长度范围为1到128个字符。 ● 可以包含任意语种字母、数字、空格和_.:=+-@，但首尾不能含有空格，不能以_sys_开头。	Key_0001
标签值	输入标签的值，标签的值可以重复，并且可以为空。 标签值的命名规则如下： ● 长度范围为0到255个字符。 ● 可以包含任意语种字母、数字、空格和_.:/=+-@。	Value_0001

----结束

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/启用已创建的追踪器。追踪器停用成功后对已有的操作记录没有影响。

本节介绍如何停用/启用追踪器。

使用限制

停用追踪器后，操作事件仍可以正常上报到云审计服务。您可以在事件列表查看已有的7天内的操作记录，但是您无法查看新的操作记录、转储事件至OBS/LTS和接收关键事件通知。

前提条件

已开通云审计服务。

停用/启用管理类事件追踪器

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。

步骤4 单击左侧导航树的“追踪器”，进入追踪器信息页面。

步骤5 在管理类追踪器信息右侧，单击操作下的“停用”。

图 3-4 停用追踪器

步骤6 单击“确定”，停用追踪器。追踪器停用成功后，操作下的“停用”切换为“启用”。

步骤7 如果您需要重新启用管理类追踪器，单击“启用 > 确定”，则系统重新开始记录新的操作。

----结束

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管理类事件追踪器，删除管理类事件追踪器对已有的操作记录没有影响。本章节介绍如何在管理控制台删除管理类事件追踪器。

使用限制

删除追踪器后，操作事件仍可以正常上报到云审计服务。您可以在事件列表查看已有的7天内的操作记录，但是您无法查看新的操作记录、转储事件至OBS/LTS和接收关键操作通知。

重新“开通云审计服务”可恢复管理类追踪器。

前提条件

已开通云审计服务。

删除管理类事件追踪器

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。

步骤4 单击左侧导航树的“追踪器”，进入追踪器信息页面。

步骤5 单击管理类追踪器对应操作列的“删除”。

图 3-5 删除追踪器

步骤6 在弹框中单击“确定”，完成删除管理类追踪器。

----结束

4 数据类事件追踪器

云审计服务提供的追踪器分两类，包括管理类追踪器和数据类追踪器。管理类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。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。

本章节介绍数据类追踪器的相关操作。

4.1 创建追踪器

操作场景

云审计服务支持创建数据类事件追踪器，用于记录数据操作日志。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。

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，故后续您自行创建的追踪器均为数据类事件追踪器。

使用限制

- CTS仅记录最近7天内的操作事件，您需要配置追踪器来保存更长时间的事件，否则将无法追溯7天前的操作事件。追踪器会将事件持续保存到您指定的LTS日志流或者OBS桶中。

前提条件

已开通云审计服务。开通云审计服务具体操作请参见**入门指引**。

创建数据类事件追踪器

1. 登录管理控制台。
2. 在服务列表选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 在左侧导航栏选择“追踪器”，单击页面右上角的“创建追踪器”。
4. 基本信息。新建“追踪器名称”便于识别，选择一个企业项目。单击“下一步”，基本信息填写成功。

数据类事件追踪器命名规则：名称只能包含大小写字母、数字、-和_，且必须由大小写字母或数字开头。名称不能为空，且输入长度不能超过32个字符。名称不能为“system”或“system-trace”。

5. 选择转储事件。填写相关参数，单击“下一步”。

表 4-1 选择转储事件参数表

参数名称	参数说明
数据事件来源	数据事件的存储容器，当前为OBS桶。
OBS桶名称	在下拉列表中选择对应OBS桶。
事件操作类型	• 选择需要记录事件的数据操作。 • 目前支持“读操作”和“写操作”，且至少选择其中一种操作。

6. 配置转储。填写相关参数，单击“下一步”。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)或配置转储到云日志服务(LTS)。具体参数说明参见表4-2和表4-3。

表 4-2 配置转储到 OBS 参数列表

参数名称	参数说明
转储到OBS	当“转储到OBS”开关打开时，您可以选择已存在的OBS桶或直接通过配置页面新建OBS桶，并配置事件文件前缀。 如果“转储到OBS”开关关闭时，则无需配置相应参数。
创建云服务委托	必选，勾选创建云服务委托后，用户在创建追踪器时，云审计服务将会自动创建一个云服务委托，委托授权您使用对象存储服务（OBS）。
选择OBS	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。
OBS桶名称	当“选择OBS”选择“新建OBS桶”时，直接新建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。 当“选择OBS”选择“选择已有OBS桶”时，可以选择已存在的OBS桶。

参数名称	参数说明
保存周期	转储至OBS桶中日志的保存周期。该配置会修改被选择桶的桶策略，影响范围为桶内的所有文件。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，建议设置保存周期不低于180天。 ● 数据类事件追踪器：保存周期支持设置为30天、60天、90天、180天、三年和沿用OBS配置。
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。
是否压缩	压缩后可以减少对象存储空间的使用量。 ● 不压缩：按照 *.json格式转储。 ● gzip：按照*.json.gz格式转储。
路径按云服务划分	● “路径按云服务划分”开关打开后，转储文件路径中将增加云服务名，OBS同时出现多个小文件。例如：/CloutTrace/cn-north-7/2022/11/8/doctest/云服务/_XXX.json.gz ● “路径按云服务划分”开关关闭后，转储文件路径中不会增加云服务名。例如：/CloutTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz
日志转储路径	日志转储的路径，系统自动填写。
文件校验	可以检验转储至OBS桶的数据是否被篡改，保障事件文件的完整性。如何校验文件完整性可参考**校验云审计事件文件完整性**。

表 4-3 配置转储到 LTS 参数列表

参数名称	参数说明
转储到LTS	当“转储到LTS”开关打开时，表示操作事件将转储到日志流中。
日志组名称	当“转储到LTS”开关打开时，日志组名称默认为“CTS”。如果“转储到LTS”开关关闭时，则无需配置该参数。

7. 预览追踪器信息无误后，单击“创建”完成追踪器的创建。
8. 单击“确定”完成追踪器的创建。

4.2 配置追踪器

操作场景

云审计服务管理控制台支持对已创建的管理类追踪器增加OBS转储、LTS转储等相关配置。

用户可以选择是否将已记录的事件发送到OBS桶永久保存。如果用户想要对管理类事件进行统一管理，还可以设置将多个账号记录的事件统一转储到一个OBS桶。

配置追踪器完成后，系统立即以新的规则开始记录操作。

本节介绍如何配置数据类事件追踪器。

使用限制

1. 全局级服务需要在中心region（北京四）的云审计控制台配置追踪器，才能使用审计事件转储至OBS/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。
2. OBS桶有标准存储、低频访问存储和归档存储三种类型。由于云审计服务需要高频次的访问转储的OBS桶，您在云审计控制台新建的OBS桶默认是一个单AZ标准存储的私有桶。如果您需要其他额外配置，建议提前在OBS服务创建OBS桶。详情请参考**创建桶**。
3. 当您配置追踪器转储至OBS时，您需要选择一个OBS桶，配置完成后，如果您在OBS服务删除了配置转储时选择的OBS桶，CTS的审计日志将无法转储至OBS，您将无法查询7天以上的历史审计记录。
4. 在CTS配置追踪器转储至OBS/LTS后，转储事件的保存周期以您在OBS/LTS控制台的配置为准：
   - 配置OBS桶存储时间需要您提前在OBS服务创建OBS桶，根据您的业务诉求选择“存储类别”，不同存储类别的OBS桶具有不同的存储时间，详情请参考**创建桶**。创建并配置好OBS桶后，在CTS配置追踪器转储至OBS时，选择已有OBS桶，转储事件的保存周期默认沿用您在OBS的配置。
   - 在CTS配置事件转储至LTS后，事件日志存储的周期以LTS日志组配置的日志存储时间为准，详情请参考**管理日志组**。

前提条件

已开通云审计服务，且已创建一个数据类事件追踪器。

配置数据类事件追踪器

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。

步骤4 单击左侧导航树的“追踪器”，进入追踪器信息页面。

步骤5 在数据类追踪器信息右侧，单击操作下的“配置”。

图 4-1 追踪器配置

步骤6 配置数据类追踪器时，数据事件来源的“OBS桶名称”默认为当前OBS桶名称，不可以修改。在配置转储页面可以修改该追踪器的转储信息。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)或配置转储到云日志服务(LTS)。具体参数说明参见表4-4和表4-5。

表 4-4 配置转储到 OBS 参数列表

参数名称	参数说明
转储到OBS	当“转储到OBS”开关打开时，您可以选择已存在的OBS桶或直接通过配置页面新建OBS桶，并配置事件文件前缀。 如果“转储到OBS”开关关闭时，则无需配置相应参数。
创建云服务委托	必选，勾选创建云服务委托后，用户在创建追踪器时，云审计服务将会自动创建一个云服务委托，委托授权您使用对象存储服务（OBS）。
选择OBS	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。
OBS桶名称	当“选择OBS”选择“新建OBS桶”时，直接新建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。 当“选择OBS”选择“选择已有OBS桶”时，可以选择已存在的OBS桶。
保存周期	转储至OBS桶中日志的保存周期。该配置会修改被选择桶的桶策略，影响范围为桶内的所有文件。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，建议设置保存周期不低于180天。 ● 数据类事件追踪器：保存周期支持设置为30天、60天、90天、180天、三年和沿用OBS配置。

参数名称	参数说明
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。
是否压缩	压缩后可以减少对象存储空间的使用量。 ● 不压缩：按照 *.json格式转储。 ● gzip：按照*.json.gz格式转储。
路径按云服务划分	● “路径按云服务划分”开关打开后，转储文件路径中将增加云服务名，OBS同时出现多个小文件。例如：/CloutTrace/cn-north-7/2022/11/8/doctest/云服务/_XXX.json.gz ● “路径按云服务划分”开关关闭后，转储文件路径中不会增加云服务名。例如：/CloutTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz
日志转储路径	日志转储的路径，系统自动填写。
文件校验	可以检验转储至OBS桶的数据是否被篡改，保障事件文件的完整性。如何校验文件完整性可参考**校验云审计事件文件完整性**。

表 4-5 配置转储到 LTS 参数列表

参数名称	参数说明
转储到LTS	当“转储到LTS”开关打开时，表示操作事件将转储到日志流中。
日志组名称	当“转储到LTS”开关打开时，日志组名称默认为“CTS”。如果“转储到LTS”开关关闭时，则无需配置该参数。

步骤7 单击“下一步 > 配置”，完成配置数据类事件追踪器。

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。

步骤8 （可选）在追踪器页面，单击标签列下的，可以为该追踪器添加标签。

图 4-2 添加标签

标签以键值对的形式表示，用于标识追踪器，便于对追踪器进行分类和搜索。此处的标签仅用于追踪器的过滤和管理。一个追踪器最多添加20个标签。

如果您的组织已经设定云审计服务的相关标签策略，则需按照标签策略规则为追踪器添加标签。标签策略详细介绍请参考**标签策略**，标签管理详细介绍请参考**标签管理**。

表 4-6 标签说明

参数	说明	举例
标签键	输入标签的键，同一个追踪器标签的键不能重复。键可以自定义，也可以选择预先在标签服务（TMS）创建好的标签的键。 键命名规则如下： ● 长度范围为1到128个字符。 ● 可以包含任意语种字母、数字、空格和_.:=+-@，但首尾不能含有空格，不能以_sys_开头。	Key_0001
标签值	输入标签的值，标签的值可以重复，并且可以为空。 标签值的命名规则如下： ● 长度范围为0到255个字符。 ● 可以包含任意语种字母、数字、空格和_.:/=+-@。	Value_0001

----结束

4.3 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/启用已创建的追踪器。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/启用追踪器。

使用限制

停用追踪器后，操作事件仍可以正常上报到云审计服务。您可以在事件列表查看已有的7天内的操作记录，但是您无法查看新的操作记录、转储事件至OBS/LTS和接收关键事件通知。

前提条件

已在云审计服务中成功创建数据类追踪器。

停用/启用数据类事件追踪器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 单击左上角 ☰，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。
4. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
5. 在数据类追踪器信息右侧，单击操作下的“停用”。

图 4-3 停用追踪器

6. 单击“确定”，停用追踪器。追踪器停用成功后，操作下的“停用”切换为“启用”。
7. 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。

4.4 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类事件追踪器，删除数据类事件追踪器对已有的操作记录没有影响。本章节介绍如何在管理控制台删除数据事件追踪器。

使用限制

删除追踪器后，操作事件仍可以正常上报到云审计服务。您可以在事件列表查看已有的7天内的操作记录，但是您无法查看新的操作记录、转储事件至OBS/LTS和接收关键操作通知。

前提条件

已成功创建数据类事件追踪器。

删除数据类事件追踪器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击左上角 ☰，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。
4. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
5. 单击目标追踪器对应操作列的“删除”。

图 4-4 删除追踪器

6. 在弹框中单击“确定”，完成删除追踪器。

5 组织追踪器

5.1 组织追踪器概述

组织云服务（Organizations）为企业用户提供多账号关系的管理能力。Organizations支持用户将多个华为云账号整合到创建的组织中，并可以集中管理组织下的所有账号。用户可以在组织中设置访问策略，帮助用户更好地满足业务的安全性和合规性需求。

云审计服务支持组织云服务的多账号关系的管理能力：

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。

使用限制

1. 一个组织只允许开启一个组织追踪器。
2. 目前仅管理类事件追踪器支持组织功能，数据类事件追踪器不支持组织功能。
3. 取消委托管理员前请先禁用组织追踪器，然后在组织服务界面取消委托管理员。
4. 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-trace日志流下面去查看。
5. 组织追踪器功能依赖组织服务某些接口，涉及企业项目权限管理的用户如需升级此能力，需要单独配置IAM权限，否则原有仅对CTS:*授权的用户将无法使用组织服务的多账号关系管理能力。

相关链接

什么是组织云服务

启用、禁用可信服务

添加、查看和取消委托管理员

5.2 启用云审计可信服务

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。

使用限制

CTS可信服务功能当前在苏州201、贵阳202、华东-青岛、华北-乌兰察布-汽车一、华北-乌兰察布一、华南-广州-友好用户环境、中东-利雅得、华北-北京四、华东-上海一、华东-上海二、华南-广州、西南-贵阳一、中国-香港、亚太-曼谷、亚太-新加坡、亚太-雅加达、非洲-约翰内斯堡、土耳其-伊斯坦布尔、拉美-墨西哥城一、拉美-墨西哥城二、拉美-圣保罗一和拉美-圣地亚哥区域开放。

前提条件

1. 当前登录用户的账号类型是组织管理员账号。
2. 提前规划安全运营管理审计事件的委托管理员账号。

开启云审计可信服务

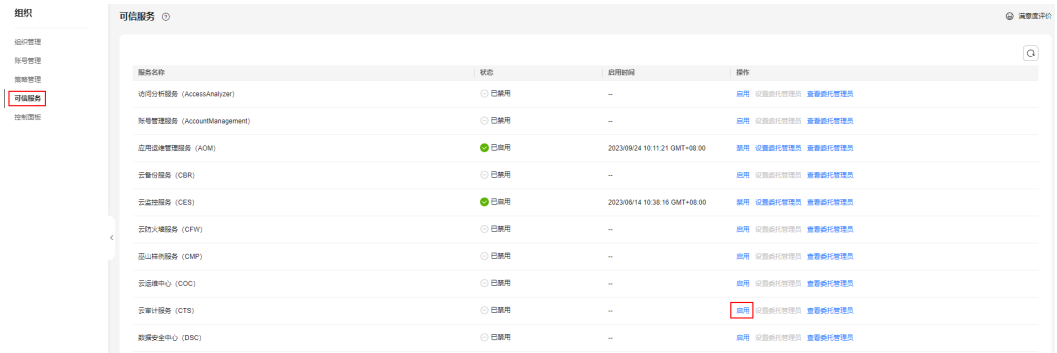
步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 > 组织 Organizations”，进入Organizations控制台。

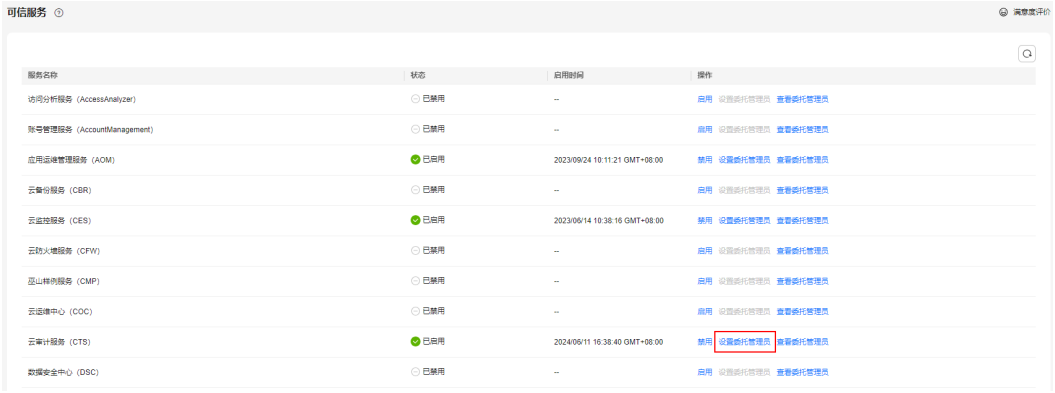
步骤4 左侧菜单栏选择“可信服务”，找到云审计服务，单击“启用”，即可开启云审计可信服务。

图 5-1 启动云审计可信服务



步骤5 单击云审计服务右侧的“设置委托管理员”按钮，为云审计服务设置委托管理员。

图 5-2 设置委托管理员



----结束

取消委托管理员权限

步骤1 进入Organizations控制台。

步骤2 左侧菜单栏选择“可信服务”，找到云审计服务。

步骤3 单击云审计服务右侧的“查看委托管理员”按钮。

步骤4 选择要取消的委托管理员账号，单击“取消委托”，在弹出的提示框中单击“确认”，即可取消该账号的委托管理员权限。

----结束

5.3 配置组织追踪器

使用委托管理员账号或组织管理员账号，在云审计服务中开启管理类追踪器的组织功能，即配置组织追踪器。

前提条件

1. 当前登录用户的账号类型是委托管理员账号或组织管理员账号。
2. 组织管理员账号在组织服务中开启了CTS可信服务。
3. 建议规划用来存储审计事件的委托管理员的OBS桶。

配置组织追踪器

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计控制台。

步骤4 左侧菜单选择“追踪器”，单击管理类事件追踪器右侧的“配置”按钮。如果界面未显示管理类追踪器，需要先**开通云审计服务**。

图 5-3 管理类事件追踪器

步骤5 进入配置追踪器的基本信息页面，打开“应用到我的组织”开关，单击“下一步”。

图 5-4 应用到我的组织

步骤6 在配置转储页面，打开转储到OBS和LTS开关。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)或配置转储到云日志服务(LTS)。具体参数说明参见表5-1和表5-2。其中OBS桶所属用户选择“当前用户”，配置OBS转储需要“选择已有OBS桶”，OBS选择管理员已经规划的OBS桶。配置完成后，单击“下一步 > 配置”按钮。

表 5-1 配置转储到 OBS 参数说明

参数名称	参数说明
转储到OBS	当“转储到OBS”开关打开时，您可以选择已存在的OBS桶或直接通过配置页面新建OBS桶，并配置事件文件前缀。 如果“转储到OBS”开关关闭时，则无需配置相应参数。
创建云服务委托	必选，勾选创建云服务委托后，用户在创建追踪器时，云审计服务将会自动创建一个云服务委托，委托授权您使用对象存储服务（OBS）。
OBS桶所属用户	云审计服务支持用户将事件转储至其他用户的OBS桶中，方便用户统一管理。 ● 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。

参数名称	参数说明
选择OBS	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”。详情请参考**创建桶**。 选择已有OBS桶：选择当前区域已创建的OBS桶。
OBS桶名称	当“选择OBS”选择“新建OBS桶”时，直接新建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。 当“选择OBS”选择“选择已有OBS桶”时，可以选择已存在的OBS桶。
保存周期	管理类事件追踪器的保存周期默认沿用在OBS的配置，不支持修改。
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。
是否压缩	压缩后可以减少对象存储空间的使用量。 ● 不压缩：按照 *.json格式转储。 ● gzip：按照*.json.gz格式转储。
路径按云服务划分	● “路径按云服务划分”开关打开后，转储文件路径中将增加云服务名，OBS同时出现多个小文件。例如：/CloutTrace/cn-north-7/2022/11/8/doctest/云服务/_XXX.json.gz ● “路径按云服务划分”开关关闭后，转储文件路径中不会增加云服务名。例如：/CloutTrace/cn-north-7/2022/11/8/doctest/_XXX.json.gz
日志转储路径	日志转储的路径，系统自动填写。
文件校验	可以检验转储至OBS桶的数据是否被篡改，保障事件文件的完整性。如何校验文件完整性可参考**校验云审计事件文件完整性**。
加密事件文件	当OBS所属用户选择“当前用户”时，可以为事件配置加密密钥。 “加密事件文件”开关打开时，云审计会从数据加密服务（DEW）获取当前用户的密钥ID，在下拉选项可以直接选择密钥。 **说明** 使用数据加密服务（DEW）中的密钥对OBS桶中的对象进行全量加密或者部分加密，详细操作请参见**OBS服务端加密**。

表 5-2 配置转储到 LTS 参数说明

参数名称	参数说明
转储到LTS	当“转储到LTS”开关打开时，表示操作事件将转储到日志流中。
日志组名称	当“转储到LTS”开关打开时，日志组名称默认为“CTS”。如果“转储到LTS”开关关闭时，则无需配置该参数。

步骤7 配置完成后，管理员可以在追踪器界面查看OBS桶和LTS日志组信息。

图 5-5 管理员查看追踪器

步骤8 使用组织成员账号登录云审计服务，可以看到追踪器界面上的“是否开通组织“一栏显示为“是”。

组织成员的追踪器界面，第一行显示管理员账户的system追踪器信息，第二行显示当前账户的system追踪器信息。组织成员账户的审计日志在汇聚转储到管理员账户OBS桶和LTS日志组的同时，也可以配置转储到当前账户的OBS桶和LTS日志组。

图 5-6 组织成员查看追踪器

----结束

6 创建关键操作通知

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。

使用限制

- 全局级服务需要在中心region（北京四）的云审计控制台配置关键操作通知，才能使用关键操作消息通知功能。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。
- 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。
- 当您创建关键操作通知后，如果停用或删除该关键操作通知，CTS将无法发送关键操作通知给消息订阅者。

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）”。

     表 6-1 高级筛选参数说明

筛选参数	参数说明
api_version	事件对应的云服务接口版本。 枚举值： • v1 • v3
code	事件对应接口返回的HTTP状态码。
trace_rating	事件等级目前有三种：正常(normal)，警告(warning)，事故(incident)。 枚举值： • normal • warning • incident

筛选参数	参数说明
trace_type	跟踪的操作事件类型，包括管理控制台或API接口发起的操作，以及各服务内部自触发的操作。 枚举值： ● ApiCall ● ConsoleAction ● SystemAction
resource_id	事件对应的云服务资源ID。 示例：5a0215bed7a14de38193a******facef。
resource_name	事件对应的的资源名称。

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6-2。

表 6-2 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。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

7 云审计服务应用示例

7.1 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。

本章节介绍，通过云审计服务如何审计最近两周内云硬盘服务的创建和删除操作。

使用限制

查询超过7天的操作记录，您必须对追踪器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。否则，您将无法追溯7天以前的操作记录。

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**入门指引**。

在新版事件列表查看审计事件

步骤1 以CTS管理员权限登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。

步骤4 单击左侧导航树的“事件列表”，进入事件列表界面。

步骤5 时间范围选择“最近1周”，然后在搜索框中依次查询：

- 创建操作：“云服务：EVS” > “资源类型：evs” > “事件名称：createVolume”，查看过滤结果。

- 删除操作：“云服务：EVS” > “资源类型：evs” > “事件名称：deleteVolume”，查看过滤结果。

说明

- 默认查询过去1小时以内所有创建或删除EVS的操作。通过设置时间范围，最多可以查询7天以内所有创建或删除EVS的操作。
- 在**支持审计的服务及操作列表**中可以查看目前云平台的支持审计的全部云服务及操作。

步骤6 若要获取最近7天以前的操作记录，则需要到OBS桶或LTS日志组中查询。查询历史事件的详细操作请参照**查询云审计服务转储事件**。

步骤7 在操作记录中，以createVolume和deleteVolume作为关键字检索，找到对应记录。

步骤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。

----结束

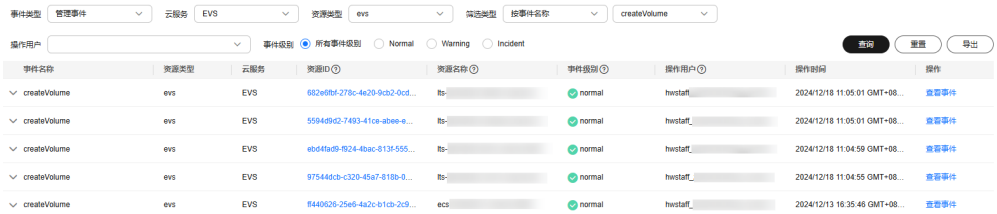
在旧版事件列表查看审计事件

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CTS管理员权限登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击左上角 ，选择“管理与监管>云审计服务 CTS”，进入云审计服务详情页面。
4. 单击左侧导航树的“事件列表”，进入事件列表界面。
5. 时间范围选择“最近1周”，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，默认查询过去1小时以内所有创建或删除EVS的操作。通过设置时间范围，最多可以查询7天以内所有创建或删除EVS的操作。



6. 若要获取最近7天以前的操作记录，则需要到OBS桶或LTS日志组中查询。查询历史事件的详细操作请参照**查询云审计服务转储事件**。
7. 参照**查询云审计服务转储事件**下载7天之前或者所有的事件。
8. 在操作记录中，以createVolume和deleteVolume作为关键字检索，找到对应记录。
9. 从第**5**步和第**8**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。

7.2 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。

本章节介绍，通过云审计服务如何定位现网某个弹性云服务器在某日上午发生的故障，以及如何定位现网创建弹性云服务器操作失败的问题。

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**入门指引**。

在新版事件列表查看审计事件

以现网某个弹性云服务器在某日上午发生故障后的辅助定位为例：

步骤1 以CTS管理员权限登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 >云审计服务 CTS”，进入云审计服务详情页面。

步骤4 单击左侧导航树的“事件列表”，进入事件列表界面。

步骤5 时间范围选择某日上午6点到中午12点，然后在搜索框中依次查询：

“云服务：ECS” > “资源类型：ecs” > “资源ID：*{问题虚拟机ID}*”，或直接搜索*{问题虚拟机ID}*，查看过滤结果。

步骤6 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。

----结束

以现网进行创建弹性云服务器操作失败报错后的辅助定位为例：

步骤1 以CTS管理员权限登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。

步骤4 单击左侧导航树的“事件列表”，进入事件列表界面。

步骤5 在搜索框中依次查询：

“云服务：ECS” > “资源类型：ecs” > “事件级别：warning”，根据创建虚拟机弹性云服务器失败的操作，在结果中查看事件名称为“createServer”操作记录事件。

步骤6 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。

----结束

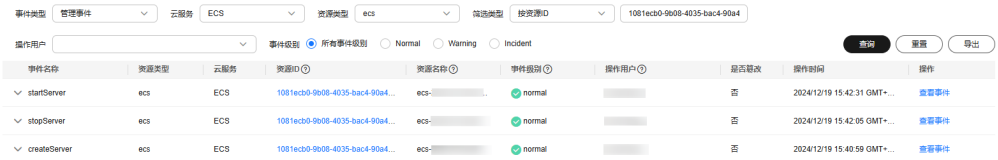
在旧版事件列表查看审计事件

以现网某个弹性云服务器在某日上午发生故障后的辅助定位为例：

1. 以CTS管理员权限登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击左上角 ，选择“管理与监管>云审计服务 CTS”，进入云审计服务详情页面。
4. 单击左侧导航树的“事件列表”，进入事件列表界面。
5. 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”>“按资源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。



6. 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服务器操作失败报错后的辅助定位为例：

1. 以CTS管理员权限登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击左上角 ，选择“管理与监管>云审计服务 CTS”，进入云审计服务详情页面。
4. 单击左侧导航树的“事件列表”，进入事件列表界面。
5. 根据创建虚拟机弹性云服务器失败的操作，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。
6. 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。

7.3 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。

本章节介绍，通过云审计服务如何查看某个弹性云服务器的所有的操作记录。

使用限制

查询超过7天的操作记录，您必须对追踪器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。否则，您将无法追溯7天以前的操作记录。

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入门指引。

在新版事件列表查看审计事件

步骤1 以CTS管理员权限登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务详情页面。

步骤4 单击左侧导航树的“事件列表”，进入事件列表界面。

步骤5 在搜索框中依次查询：

“云服务：ECS” > “资源类型：ecs” > “资源ID：*{虚拟机ID}*”，或直接搜索*{虚拟机ID}*，查看过滤结果。

说明

默认查询过去1小时以内的操作记录。通过设置时间范围，最多可以查看最近7天的操作记录。

步骤6 若要获取最近7天以前的操作记录，则需要到OBS桶或LTS日志组中查询。查询历史事件的详细操作请参照**查询云审计服务转储事件**。

步骤7 从第**5**步和第**6**步的结果中，检视该弹性云服务器的所有操作和变更记录。

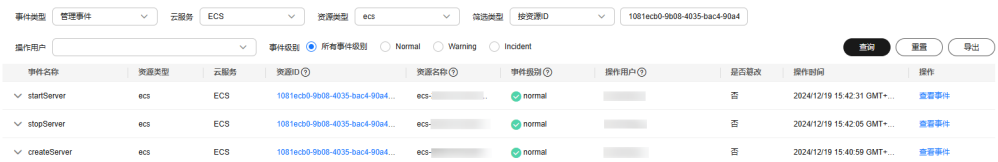
----结束

在旧版事件列表查看审计事件

1. 以CTS管理员权限登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击左上角 ，选择“管理与监管>云审计服务 CTS”，进入云审计服务详情页面。
4. 单击左侧导航树的“事件列表”，进入事件列表界面。
5. 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”>“按资源ID”>“虚拟机ID”，单击“查询”执行搜索，默认查询过去1小时以内的操作记录。通过设置时间范围，最多可以查看最近7天的操作记录。

6. 单击左侧导航树的“追踪器”，进入追踪器详情页面，获取OBS桶名或LTS日志组信息。
7. 参照**查询云审计服务转储事件**查询7天之前或者所有的事件。

8. 从第5步和第7步的结果中，检视该弹性云服务器的所有操作和变更记录。

8 云审计服务事件参考

8.1 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8-1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 8-1 事件的关键字段

字段名称	是否必选	类型	描述
time	是	Long	标识事件产生的时间戳。以当地标准时间进行展示，例如：1660927593570。在接口中，该字段以时间戳格式进行传输和存储。该字段为当地时间1970年01月01日00时00分00秒至现在的总毫秒数。
user	是	UserInfo object	标识触发事件的用户信息。
request	否	Structure	标识事件对应接口请求内容，即资源操作请求体。
response	否	Structure	记录用户请求的响应，标识事件对应接口响应内容，即资源操作结果返回体。
service_type	是	String	标识查询事件列表对应的云服务类型。
event_type	是	String	标识事件对应的事件类型。
project_id	是	String	标识事件所属的项目ID。
resource_type	是	String	查询事件列表对应的资源类型。

字段名称	是否必选	类型	描述
resource_account_id	否	String	标识资源所在的账号ID。仅在跨租户操作资源时有值。例如：租户A操作租户B下面的资源，此处为账号B的account_id。 说明：在跨租户场景下，如果用户涉及到租户A操作租户B的某个资源的时候，CTS会复制一份审计日志，在租户A和租户B的云审计服务中均可查看该条操作记录。
read_only	否	boolean	标识用户请求是不是只读。
tracker_name	否	String	标识记录事件对应的追踪器名称。 ● 当"trace_type"字段值为"system"时，该字段值默认为"system"。 ● 当"trace_type"字段值为"data"时，该字段值为对应数据类追踪器名称。
operation_id	是	String	记录事件对应的操作ID。
resource_name	否	String	标识事件对应的资源名称。
resource_id	否	String	标识事件对应的云服务资源ID。
source_ip	是	String	标识触发事件的租户IP。若为系统内调用，则为空。
domain_id	是	String	标识触发事件的账户ID。
trace_name	是	String	标识查询事件列表对应的事件名称。
trace_rating	是	String	标识事件等级，分为normal（正常）、warning（警告）和incident（事故）。 ● normal：代表本次操作成功。 ● warning：代表本次操作失败。 ● incident：代表本次操作引起了比失败更严重的后果，比如会造成节点故障或用户业务故障等情况。
trace_type	是	String	标识事件发生源头类型，管理类事件主要包括API调用（ApiCall），Console页面调用（ConsoleAction）和系统间调用（SystemAction）。数据类事件主要包括ObsSDK，ObsAPI。
api_version	否	String	标识事件对应的云服务接口版本。
message	否	Structure	标识其他云服务为此条事件添加的备注信息。
record_time	是	Number	标识云审计服务记录本次事件的时间戳。
trace_id	是	String	标识事件的ID，由系统生成的UUID。

字段名称	是否必选	类型	描述
code	否	String	记录用户请求的响应，标识事件对应接口返回的HTTP状态码。
request_id	否	String	记录本次请求的request id。
location_info	否	String	记录本次请求出错后，问题定位所需要的辅助信息。
endpoint	否	String	该操作涉及云资源的详情页面的endpoint。
resource_url	否	String	该操作涉及云资源的详情页面的访问链接（不含endpoint）。
enterprise_project_id	是	String	标识资源所在的企业项目ID。
user_agent	否	String	请求客户端代理标识。
content_length	否	Number	请求消息体的长度。
total_time	否	Number	请求的响应时间。

表 8-2 UserInfo

字段名称	是否必选	类型	描述
type	否	String	操作者的身份类型。
principal_id	否	String	操作用户的身份Id。 ● 如果是 IAM 用户身份，格式为 <user-id> ● 如果是 IAM 委托会话身份，格式为 <agency-id>:<agency-session-name> ● 如果是 IAM 联邦身份，格式为 <idp_id>:<user-session-name>
principal_urn	否	String	操作用户身份的URN。 ● 如果是 IAM 用户身份，格式如 iam::<account-id>:user:<user-name> ● 如果是 IAM 委托会话 身份，格式如 sts::<account-id>:assumed-agency:<agency-name>/<agency-session-name> ● 如果是 IAM 联邦身份，格式如 sts::<account-id>:external-user:<idp_id>/<user-session-name>

字段名称	是否必选	类型	描述
account_id	否	String	账号ID。账号ID是指：在控制台右上角用户名的下拉选项中，选择“我的凭证”，在我的凭证页面中的“账号ID”。
access_key_id	否	String	访问密钥ID。
id	是	String	用户ID。用户ID是指：在控制台右上角用户名的下拉选项中，选择“我的凭证”，在我的凭证页面中的“IAM用户ID”。
name	是	String	用户名称。用户名称是指：在控制台右上角用户名的下拉选项中，选择“我的凭证”，在我的凭证页面中获取“IAM用户名”。
domain	是	**BaseUser** object	标识触发事件的用户domain信息。
user_name	否	String	用户名称。 说明：user_name与name字段的含义一致。
principal_is_root_user	否	String	是否是根用户。 • 值为“true”时，表示操作者是根用户。 • 值为“false”时，表示操作者是委托会话身份、联邦身份或非根用户的IAM用户。
invoked_by	否	Array of strings	发出请求的服务的名称。控制台操作时为["service.console"]
session_context	否	**SessionContext** object	临时安全凭据属性。
OriginUser	否	String	发起委托会话的原始用户信息。

表 8-3 BaseUser

字段名称	是否必选	类型	描述
id	是	String	账号ID。账号ID是指：在控制台右上角用户名的下拉选项中，选择“我的凭证”，在我的凭证页面中的“账号ID”。
name	是	String	账号名称。账号名称是指：在控制台右上角用户名的下拉选项中，选择“我的凭证”，在我的凭证页面中的“账号名”。

表 8-4 SessionContext

字段名称	是否必选	类型	描述
attributes	否	**Attributes** object	临时安全凭据的属性。

表 8-5 Attributes

字段名称	是否必选	类型	描述
mfa_authenticated	否	String	是否已经通过MFA身份认证。
created_at	否	String	颁发临时安全凭证时的时间。

8.2 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**事件结构**章节。

- **创建云服务器实例**
- **云硬盘实例**

创建云服务器实例


```
{
    "trace_id": "cbdd4480-2e03-11ef-82de-cf140e2a70fb",
    "trace_name": "createServer",
    "resource_type": "ecs",
    "trace_rating": "normal",
    "api_version": "1.0",
    "source_ip": "124.71.93.243",
    "domain_id": "7e0d78c85***d0b9b7cba",
    "trace_type": "ConsoleAction",
    "service_type": "ECS",
    "event_type": "system",
    "project_id": "07066c6fc90025a02f6dc01e105b286e",
    "read_only": false,
    "tracker_name": "system",
    "operation_id": "ListSubscriptions",
    "resource_account_id": "7e0d78c85***d0b9b7cba",
    "time": 1718777931170,
    "resource_name": "ecs-test",
    "user": {
        "access_key_id": "HSTAZVL6WYS0J5MYE2GA",
        "account_id": "7e0d78c85***d0b9b7cba",
        "user_name": "IAMUserA",
        "domain": {
            "name": "IAMDomainB",
            "id": "7e0d78c85***d0b9b7cba"
        },
        "name": "IAMUserA",
        "principal_is_root_user": "true",
        "id": "f36972ced***d619f1214",
```



```
        "principal_urn": "iam::7e0d78c85***d0b9b7cba:user:IAMUserA",
        "type": "User",
        "principal_id": "f36972ced***d619f1214"
    },
    "record_time": 1718777931170,
    "request": "{\"server\":{\"adminPass\":\"********\",\"extendparam\":{\"chargingMode\":\"0\",\"regionID
\":\"cn-north-4\"},\"count\":1,\"metadata\":{\"op_svc_userid
\":\"f36972ced***d619f1214\",\"__support_agent_list\":\"hss,ces\"},\"availability_zone\":\"cn-north-4c
\",\"description\":\"\",\"name\":\"ecs-test\",\"imageRef\":\"7d940784-ac0a-425f-
b3fa-8478f1a1df70\",\"root_volume\":{\"volumetype\":\"GPSSD\",\"extendparam\":{\"resourceSpecCode
\":\"GPSSD\",\"resourceType\":\"3\"},\"size\":40,\"metadata\":null,\"hw:passthrough\":\"false\",\"cluster_type
\":null,\"cluster_id\":null,\"iops\":null,\"throughput\":null},\"data_volumes\":[],\"flavorRef
\":\"sn3.small.1\",\"personality\":[],\"vpcid\":\"250ad46d-9c89-44ec-a97d-293da771b06b\",\"security_groups
\":[{\"id\":\"3bb87748-e387-42e5-ad7a-4331638f1321\"}],\"nics\":[{\"subnet_id\":\"1a02d148-e7f9-4a3c-
ba58-18099dfbf752\",\"nictype\":\"\",\"ip_address\":\"\",\"port_id\":null,\"binding:profile\":
{\"disable_security_groups\":\"false\"},\"extra_dhcp_opts\":[],\"ipv6_bandwidth\":null,\"ipv6_enable
\":false,\"driver_mode\":null,\"allowed_address_pairs\":null,\"efi_enable\":false,\"efi_protocol
\":null}],\"publicip\":{\"id\":null,\"eip\":{\"bandwidth\":{\"name\":\"ecs-test-bandwidth\",\"size\":1,\"id
\":null,\"sharetype\":\"PER\",\"productid\":\"\",\"chargemode\":\"traffic\"},\"extendparam\":{\"chargingMode
\":\"postPaid\"},\"iptype\":\"5_bgp\",\"ipproductid\":\"\"}},\"key_name\":\"KeyPair-ebbe\",\"isAutoRename
\":false,\"server_tags\":[],\"batch_create_in_multi_az\":false,\"spod_enable\":false,\"user_data\":\"\"}}",
    "message": "success",
    "response": "{\"job_id\":\"ff8080828fe9028a01902f2542df1b10\",\"job_type\":\"createSingleServer
\",\"begin_time\":\"2024-06-19T06:18:09.502Z\",\"end_time\":\"2024-06-19T06:18:51.169Z\",\"status
\":\"SUCCESS\",\"error_code\":null,\"fail_reason\":null,\"entities\":{\"server_id\":\"7285ea5d-
f15c-4d9c-9e4e-37d37023f2f4\"}}",
    "resource_id": "7285ea5d-f15c-4d9c-9e4e-37d37023f2f4",
    "request_id": "null"
}
```


在以上信息中，可以重点关注如下字段：

- "time"：标识事件产生的时间戳，本例中为1718777931170。
- "user"：记录了操作用户的信息，本例中操作用户为账户（domain字段）IAMDomainB下的用户（name字段）IAMUserA。
- "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ecs-test-bandwidth，资源id（vpcid字段）为250ad46d-9c89-44ec-a97d-293da771b06b。
- "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


```
{
  "trace_id": "c4ddaa0b-2e05-11ef-bdc6-e1851d8cb7fb",
  "trace_name": "deleteVolume",
  "resource_type": "evs",
  "trace_rating": "normal",
  "api_version": "1.0",
  "source_ip": "124.71.93.243",
  "domain_id": "7e0d78c85***d0b9b7cba",
  "trace_type": "ConsoleAction",
  "service_type": "EVS",
  "event_type": "system",
  "project_id": "07066c6fc90025a02f6dc01e105b286e",
  "read_only": false,
  "resource_id": "bc661a99-3088-4e86-899f-fb4f46c2bb71",
  "tracker_name": "system",
  "resource_account_id": "7e0d78c85***d0b9b7cba",
  "time": 1718778778419,
  "user": {
    "access_key_id": "HSTAA8960GPIROJGW19L",
    "account_id": "7e0d78c85***d0b9b7cba",
    "user_name": "IAMUserA",
```



```
  "domain": {
    "name": "IAMDomainB",
    "id": "7e0d78c85***d0b9b7cba"
  },
  "name": "IAMUserA",
  "principal_is_root_user": "true",
  "id": "f36972ced***d619f1214",
  "principal_urn": "iam::7e0d78c85***d0b9b7cba:user:IAMUserA",
  "type": "User",
  "principal_id": "f36972ced***d619f1214"
 },
 "record_time": 1718778778419,
 "request": "",
 "response": "{\"job_id\":\"defe9cf7b5ca4566860edbebb181e17a\",\"job_type\":\"deleteVolume
\",\"begin_time\":\"2024-06-19T06:32:53.018Z\",\"end_time\":\"2024-06-19T06:32:58.411Z\",\"status
\":\"SUCCESS\",\"error_code\":null,\"fail_reason\":null,\"entities\":{\"volume_type\":\"GPSSD\",\"volume_id
\":\"bc661a99-3088-4e86-899f-fb4f46c2bb71\",\"size\":10,\"name\":\"volume-d64d\"}}",
 "resource_name": "volume-d64d",
 "request_id": "defe9cf7b5ca4566860edbebb181e17a"
}
```


在以上信息中，可以重点关注如下字段：

- "time"：标识事件产生的时间戳，本例中为1718778778419。
- "user"：记录了操作用户的信息，本例中操作用户为账户（domain字段）IAMDomainB下的用户（name字段）IAMUserA。
- "request"：非必选字段，此处为空。
- "response"：记录了删除磁盘的返回结果。
- "trace_rating"：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**事件结构**章节中约束，即代表操作成功。

8.3 IAM 身份与操作用户对应关系

华为云统一身份认证服务（Identity and Access Management，简称IAM）提供不同类型的身份，IAM提供的身份包括：IAM用户、IAM委托、云服务委托、IAM身份中心、联邦用户。

不同的操作用户身份在进行操作时，上报到CTS审计日志中的“操作用户”信息有区别，以下展示不同身份的“操作用户”的操作用户名称（user.name字段）、身份ID（principal_id字段）格式规范：

操作用户身份	身份类型（type）	操作用户名称格式（user.name）	身份ID格式（principal_id）
IAM用户	User	<user-name>	<user-id>
IAM委托	AssumedAgency	<domain-name>/<agency-name>	<agency-id>:<agency-session-name>
云服务委托	AssumedAgency	<domain-name>/<agency-name>	<agency-id>:<agency-session-name>
IAM身份中心	AssumedAgency	<domain-name>/<agency-name>	<agency-id>:<agency-session-name>

操作用户身份	身份类型（type）	操作用户名称格式（user.name）	身份ID格式（principal_id）
联邦用户	ExternalUser	<idp_id>/<user-session-name>	<idp_id>:<user-session-name>

在云审计事件列表的“操作用户”一栏，可以查看对应事件的操作用户（user.name）信息。

本章节将介绍说明不同的操作用户身份在操作资源时，对应的事件列表中“操作用户”信息的示例，以方便用户更直观的理解操作用户信息。

IAM 用户身份

操作用户为“IAM用户”时，审计日志中的user字段示例如下：

```
{
    "access_key_id": "HSTAZ***YE2GA",
    "account_id": "7e0d78c85***d0b9b7cba",
    "user_name": "IAMUserA",
    "domain": {
        "name": "IAMDomainB",
        "id": "7e0d78c85***d0b9b7cba"
    },
    "name": "IAMUserA",
    "principal_is_root_user": "true",
    "id": "f36972ced***d619f1214",
    "principal_urn": "iam::7e0d78c85***d0b9b7cba:user:IAMUserA",
    "type": "User",
    "principal_id": "f36972ced***d619f1214"
}
```

在以上信息中，"user"字段记录了操作用户的信息，本示例中操作用户为"IAMUserA"（name字段）。在以上信息中，可以重点关注如下字段：

字段名	说明
user_name	操作用户的用户名称。在控制台右上角用户名的下拉选项中，选择“我的凭证”，在我的凭证页面中获取“IAM用户名”。本示例中为"IAMUserA"。
name	
id	操作用户的用户ID。在控制台右上角用户名的下拉选项中，选择“我的凭证”，在我的凭证页面中的“IAM用户ID”。本示例中为"f36972ced***d619f1214"。
principal_id	操作用户的身份ID。格式为 user-id。本示例中为"f36972ced***d619f1214"。

字段名	说明
principal_urn	操作用户身份的URN。格式为 iam::<account-id>:user:<user-name>。本示例中为"iam::7e0d78c85***d0b9b7cba:user:IAMUserA"。
domain.name	操作用户的账号名称。在控制台右上角用户名的下拉选项中，选择“我的凭证”，在我的凭证页面中的“账号名”。本示例中为"IAMUserB"。
domain.id	操作用户的账号ID。在控制台右上角用户名的下拉选项中，选择“我的凭证”，在我的凭证页面中的“账号ID”。本示例中为"7e0d78c85***d0b9b7cba"。
account_id	

IAM 委托身份

操作用户为“IAM委托身份”时，审计日志中的user字段示例如下：

```
{
   "access_key_id": "HSTAB***6DEEB",
   "invoked_by": [
     "service.console"
   ],
   "account_id": "302893da***5a7453e5733",
   "domain": {
     "name": "hc_beta_***",
     "id": "302893da***5a7453e5733"
   },
   "name": "hc_beta_***/agencyname",
   "session_context": {
     "attributes": {
       "created_at": "1724744585642",
       "mfa_authenticated": "false"
     },
     "assumed_by": {
       "principal_id": "3cd5b27548***a58b5801d9d"
     }
   },
   "principal_urn": "sts::302893da***5a7453e5733:assumed-agency:agencyname/null",
   "type": "AssumedAgency",
   "principal_id": "40c79f4571***8bc54784b61:null"
}
```

在以上信息中，"user"字段记录了操作用户的信息，本示例中操作用户为"hc_beta_***/agencyname"（name字段）。在以上信息中，可以重点关注如下字段：

字段名	说明
name	操作用户的用户名称。格式为<domain-name>/<agency-name>。
principal_id	操作用户的身份ID。格式为 <agency-id>:<agency-session-name>。本示例中为"40c79f4571***8bc54784b61:null"。
principal_urn	操作用户身份的URN。IAM委托身份的格式为sts::<account-id>:assumed-agency:<agency-name>/<agency-session-name> 。本示例中为"sts::302893da***5a7453e5733:assumed-agency:agencyname/null"。

字段名	说明
session_context.assumed_by.principal_id	被委托方账号在IAM "切换角色" 的用户ID。详情请参见**切换角色（被委托方操作）**。

云服务委托身份

操作用户为“云服务委托身份”时，审计日志中的user字段示例如下：

```
{
   "access_key_id": "HSTAR***LG6FC",
   "account_id": "302893da***53e5733",
   "domain": {
     "name": "hc_beta_***",
     "id": ""302893da***53e5733""
   },
   "name": "hc_beta_***/ServiceLinkedAgencyForCloudTraceService",
   "session_context": {
     "attributes": {
       "created_at": "1724744380046",
       "mfa_authenticated": "false"
     },
     "assumed_by": {
       "service_principal": "service.CTS"
     }
   },
   "principal_urn": "sts::302893da***53e5733:assumed-agency:ServiceLinkedAgencyForCloudTraceService/
302893da***53e5733",
   "type": "AssumedAgency",
   "principal_id": "4bc820d3***b786c83:302893da***53e5733"
}
```

在以上信息中，"user"字段记录了操作用户的信息，本示例中操作用户为"hc_beta_***/ServiceLinkedAgencyForCloudTraceService"（name字段）。在以上信息中，可以重点关注如下字段：

字段名	说明
name	操作用户的用户名称。格式为<domain-name>/<agency-name>。本示例中为"hc_beta_***/ServiceLinkedAgencyForCloudTraceService"。
principal_id	操作用户的身份ID。格式为 <agency-id>:<agency-session-name>。本示例中为"4bc820d3***b786c83:302893da***53e5733"。
principal_urn	操作用户身份的URN。格式为sts::<account-id>:assumed-agency:<agency-name>/<agency-session-name> 。本示例中为"sts::302893da***53e5733:assumed-agency:ServiceLinkedAgencyForCloudTraceService/302893da***53e5733"。
session_context.assumed_by.service_principal	委托云服务的名称。格式为service.<service-name>。

IAM 身份中心身份

操作用户为“IAM身份中心身份”时，审计日志中的user字段示例如下：

```
{
    "access_key_id": "HSTA9***CKG7E",
    "invoked_by": [
      "service.console"
    ],
    "account_id": "302893da***53e5733",
    "domain": {
      "name": "hc_beta_***",
      "id": "302893da***53e5733"
    },
    "name": "hc_beta_***/SysReservedV3_evs-FullAccess-***",
    "session_context": {
      "attributes": {
        "created_at": "1724744395079",
        "mfa_authenticated": "false"
      },
      "assumed_by": {
        "service_principal": "service.IdentityCenter"
      }
    },
    "principal_urn": "sts::302893da***53e5733:assumed-agency:SysReservedV3_evs-FullAccess-***/
IdentityCenterUsername",
    "type": "AssumedAgency",
    "principal_id": "dbc60d8***ef5fd807:***"
}
```

在以上信息中，"user"字段记录了操作用户的信息，本示例中操作用户为"hc_beta_***/SysReservedV3_evs-FullAccess-***"（name字段）。在以上信息中，可以重点关注如下字段：

字段名	说明
name	操作用户的用户名称。服务关联委托身份的格式为<domain-name>/<agency-name>。本示例中为"hc_beta_***/SysReservedV3_evs-FullAccess-***"。
principal_id	操作用户的身份ID。格式为 <agency-id>:<agency-session-name>。本示例中为"dbc60d8***ef5fd807:***"。
principal_urn	操作用户身份的URN。格式为sts::<account-id>:assumed-agency:<agency-name>/<agency-session-name> 。本示例中为"sts::302893da***53e5733:assumed-agency:SysReservedV3_evs-FullAccess-***/IdentityCenterUsername"。
session_context.assumed_by.service_principal	委托云服务的名称。固定为service.IdentityCenter。

联邦用户身份

操作用户为“联邦用户身份”时，审计日志中的user字段示例如下：


```
{
  "access_key_id": "HSTAX***3IBZB",
  "account_id": "797c8fc3c***2dc6bf70bd",
  "domain": {
    "name": "***",
    "id": "797c8fc3c***2dc6bf70bd"
  },
  "name": "provider_name/UserA",
  "session_context": {
    "federation_data": {
      "identity_provider": "provider_name",
      "protocol": "SAML",
      "group_Ids": [
        "fedf7a460***46451be85"
      ]
    }
  },
  "principal_urn": "sts::797c8fc3c***2dc6bf70bd:external-user:provider_name/UserA",
  "type": "ExternalUser",
  "principal_id": "provider_name:UserA"
}
```


在以上信息中，"user"字段记录了操作用户的信息，本示例中操作用户为"provider_name/UserA"（name字段）。在以上信息中，可以重点关注如下字段。

字段名	说明
name	操作用户的用户名称。格式为<idp_id>/<user-session-name>。本示例中为"provider_name/UserA"。
principal_id	操作用户的身份ID。格式为 <idp_id>:<user-session-name>。本示例中为"provider_name:UserA"。
principal_urn	操作用户身份的URN。格式为 sts::<account-id>:external-user:<idp_id>/<user-session-name>。本示例中为"sts::797c8fc3c***2dc6bf70bd:external-user:provider_name/UserA"。

说明

idp_id是指IAM身份提供商名称。idp_id获取方式：进入统一身份认证服务控制台，在身份供应商页面查看身份供应商名称（idp_id）。

9 跨租户转储授权

操作场景

如果用户想要对管理类事件进行统一管理，可以设置管理类追踪器将多个账号记录的事件统一转储到一个OBS桶。本节介绍如何配置跨租户转储。

授权跨租户转储

1. 租户B登录管理控制台。

   说明

   - 租户A为需要配置跨租户转储的账号，租户B为OBS桶所在的账号。
   - OBS不支持跨region转储，目前OBS桶所处区域只能是不同租户的同一个region。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击左上角 ，选择“存储 > 对象存储服务OBS”，进入对象存储服务详情页面。
4. 左侧导航栏选择“桶列表”。在桶列表单击云审计服务需要配置转储的桶名称，进入“对象”页面。
5. 在左侧导航栏，单击“访问权限控制 > 桶策略”。
6. 在界面右上方选择“JSON视图”，单击“编辑”，按照如下格式给租户A授权，其中加粗斜体的字段需要根据实际值填写。桶策略由JSON描述，详细格式定义请参考**桶策略参数说明**。

   根据租户A登录方式的不同，桶策略有不同的授权对象，包含以下场景：以普通用户登录租户A账号、以联邦租户登录租户A账号、以委托身份切换到租户A账号、以IAM身份中心用户登录租户A账号。

   - 以普通用户登录租户A配置CTS追踪器：

```
{
    "Statement": [{
            "Sid": "xxxx",
            "Effect": "Allow",
            "Principal": {
                "ID": [
                    "domain/租户A的domainId:agency/cts_admin_trust"
                ]
            },
            "Action": [
                "PutObject"
```



```
            ],
            "Resource": [
                "exampleBucketName/*"
            ]
        }, {
            "Sid": "xxxx1",
            "Effect": "Allow",
            "Principal": {
                "ID": [
                    "domain/租户A的domainId:user/*"
                ]
            },
            "Action": [
                "HeadBucket",
                "ListBucket"
            ],
            "Resource": [
                "exampleBucketName"
            ]
        }
    ]
}
```

- 以联邦租户登录租户A配置CTS追踪器：

```
{
    "Statement": [{
            "Sid": "xxxx",
            "Effect": "Allow",
            "Principal": {
                "ID": [
                    "domain/租户A的domainId:agency/cts_admin_trust"
                ]
            },
            "Action": [
                "PutObject"
            ],
            "Resource": [
                "exampleBucketName/*"
            ]
        }, {
            "Sid": "xxxx1",
            "Effect": "Allow",
            "Principal": {
                "Federated": [
                    "domain/租户A的domainId:identity-provider/provider-name"
                ]
            },
            "Action": [
                "HeadBucket",
                "ListBucket"
            ],
            "Resource": [
                "exampleBucketName"
            ]
        }
    ]
}
```

- 以委托身份切换到租户A账号配置CTS追踪器：

```
{
    "Statement": [{
            "Sid": "xxxx",
            "Effect": "Allow",
            "Principal": {
                "ID": [
                    "domain/租户A的domainId:agency/cts_admin_trust"
                ]
            },
            "Action": [
                "PutObject"
```



```
        ],
        "Resource": [
            "exampleBucketName/*"
        ]
    }, {
        "Sid": "xxxx1",
        "Effect": "Allow",
        "Principal": {
            "ID": [
                "domain/租户A的domainId:agency/agency_name"
            ]
        },
        "Action": [
            "HeadBucket",
            "ListBucket"
        ],
        "Resource": [
            "exampleBucketName"
        ]
    }
  ]
}
```

- 以IAM身份中心用户登录租户A账号配置CTS追踪器：

  说明

  此处的agency_name是IAM身份中心在租户A账号下面创建的委托，委托对象是IAM身份中心，委托名称格式如下图所示。


```
{
  "Statement": [{
        "Sid": "xxxx",
        "Effect": "Allow",
        "Principal": {
            "ID": [
                "domain/租户A的domainId:agency/cts_admin_trust"
            ]
        },
        "Action": [
            "PutObject"
        ],
        "Resource": [
            "exampleBucketName/*"
        ]
    }, {
        "Sid": "xxxx1",
        "Effect": "Allow",
        "Principal": {
            "ID": [
                "domain/租户A的domainId:agency/agency_name"
            ]
        },
        "Action": [
            "HeadBucket",
            "ListBucket"
        ],
```



```
        "Resource": [
          "exampleBucketName"
        ]
      }
    ]
}
```

表 9-1 桶策略参数说明

参数	描述
Sid	statement Id，描述statement的字符串。
Action	指定本条statement作用的操作，Action字段为OBS支持的所有操作集合，以字符串形式表示，不区分大小写。CTS只需要"PutObject"和"HeadBucket"两个action。
Effect	指定本条statement的权限是允许还是拒绝，Effect的值必须为Allow或者Deny。
Principal	桶策略被授权租户A，domainId可以通过控制台在“我的凭证”页面获取。Principal格式： ● “domain/账号ID:agency/cts_admin_trust”（表示授权给租户A下的cts_admin_trust委托，即CTS服务可通过该委托来转储日志到OBS桶）。参考**桶策略参数说明**。 ● “domain/账号ID:user/*”（表示授权给租户A下的所有子用户）。 ● “domain/账号ID:identity-provider/provider-name”（表示授权给租户A下的指定身份提供商名称）。
Resource	指定statement起作用的一组资源，支持通配符“*”，表示所有资源。CTS配置跨账号转储时需要*exampleBucketName*/*和*exampleBucketName*。

7. 单击“保存”，完成桶策略配置。
8. 如果租户B下的OBS桶配置了桶加密功能，且加密密钥类型选择了“自定义密钥”，则需要在数据加密服务(DEW)对租户A进行授权，详细操作请参考**创建授权**。

说明

跨租户桶配置加密时，建议使用自定义密钥。默认密钥有可能使用租户A的OBS默认密钥进行加密，会存在租户B无法下载转储文件的风险。

9. 租户A登录管理控制台。
10. 在管理控制台左上角单击 图标，选择区域和项目。
11. 单击左上角 ，选择“管理与监管 >云审计服务 CTS”，进入云审计服务详情页面。
12. 单击左侧导航树的“追踪器”，进入追踪器信息页面。
13. 在管理事件追踪器信息右侧，单击操作下的“配置”。
14. 选择是否转储OBS为“转储”，OBS桶所属用户设置为“其他用户”，需要手动输入待转储的租户B已授权OBS桶的桶名。
15. 单击“配置”，完成配置追踪器。

10 校验云审计事件文件完整性

10.1 开启事件文件完整性校验功能

操作场景

在安全和事故调查中，通常由于事件文件被删除或者被私下篡改，而导致操作记录的真实性受到影响，无法对调查提供有效真实的依据。事件文件完整性校验功能旨在帮助您确保事件文件的真实性。云审计服务支持对配置了OBS转储的追踪器设置事件文件的完整性校验。

开启事件文件完整性校验功能

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
4. 单击左侧导航树的“追踪器”，进入追踪器信息页面。

   说明

   若未开通云审计服务，单击“开通云审计服务”， 开通云审计服务步骤请参见**入门指引**。
5. 单击管理类追踪器system右侧的“配置”按钮，在弹出的“配置追踪器”窗口中单击下一步，在配置转储页面打开“文件校验”开关，即可开启事件文件完整性校验功能。

10.2 摘要文件

摘要文件简介及存储路径

摘要文件均包含前一小时内提交到OBS桶事件文件的名称、事件文件的哈希值以及前一摘要文件的数字签名。同时摘要文件的数字签名存储在摘要文件对象的元数据属性中。

OBS桶名*>CloudTraces>*地区标示*>*时间标示：年*>*时间标示：月*>*时间标示：日*>*trackername*>*Digest*>*服务类型目录

例如：***User Define*>CloudTraces>region>2016>5>19>system>Digest>ECS**

摘要文件命名格式

摘要文件的命名格式如下：

***操作事件文件前缀*_CloudTrace-Digest_*区域标示/区域标示-项目标示*_*摘要文件提交至OBS的时间标示：年-月-日*T*时-分-秒*Z.json.gz**

例如：File Prefix_CloudTrace-Digest_region/region-project_2016-05-30T16-20-56Z.json.gz

摘要文件结构

表 10-1 摘要文件的关键字段

字段名称	是否必选	类型	描述
project_id	是	String	摘要文件记录的事件的用户ID。
digest_start_time	是	String	摘要文件记录的事件文件的起始UTC时间。
digest_end_time	是	String	摘要文件记录的事件文件的结束UTC时间。
digest_bucket	是	String	摘要文件提交到的OBS桶的名称。
digest_object	是	String	摘要文件存储在OBS桶中的位置。
digest_signature_algorithm	是	String	用于对摘要文件进行签名的算法。
digest_end	是	Boolean	该摘要文件是否为摘要结束文件。
previous_digest_bucket	否	String	前一摘要文件提交到的OBS桶的名称。
previous_digest_object	否	String	前一摘要文件存储在OBS桶中的位置。
previous_digest_hash_value	否	String	前一摘要文件的十六进制编码哈希值。
previous_digest_hash_algorithm	否	String	用于对前一摘要文件进行哈希处理的哈希算法。
previous_digest_signature	否	String	前一摘要文件的数字签名。
previous_digest_end	是	Boolean	前一摘要文件是否为摘要结束文件。
log_files	否	Array	摘要文件记录的事件文件列表。

字段名称	是否必选	类型	描述
bucket	是	String	事件文件提交到的OBS桶的名称。
object	是	String	事件文件存储在OBS桶中的位置。
log_hash_value	是	String	事件文件的十六进制编码哈希值。
log_hash_algorithm	是	String	用于对事件文件进行哈希处理的哈希算法。

摘要文件样例

摘要文件均包含前一小时内提交到OBS桶事件文件的名称、事件文件的哈希值以及前一摘要文件的数字签名。同时摘要文件的数字签名存储在摘要文件对象的元数据属性中。

摘要文件样例如下：

样例中的字段说明请参考**表10-1**。


```
{
 "project_id": "3cfb09080bd944d0b4cdd72ef2685712",
 "digest_start_time": "2017-03-28T01-09-17Z",
 "digest_end_time": "2017-03-28T02-09-17Z",
 "digest_bucket": "bucket",
 "digest_object": "CloudTraces/cn-north-01/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_cn-north-01/
_2017-03-28T02-09-17Z.json.gz",
 "digest_signature_algorithm": "SHA256withRSA",
 "digest_end": false,
 "previous_digest_bucket": "bucket",
 "previous_digest_object": "CloudTraces/cn-north-01/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_cn-
north-01/_2017-03-28T01-09-17Z.json.gz",
 "previous_digest_hash_value": "5e08875de01b894eda5d1399d7b049fe",
 "previous_digest_hash_algorithm": "MD5",
 "previous_digest_signature":
"7af7cbef4f3c78eab5048030d402810841400cf70eb22f93d4fedd13b13a8208a5dc04ce2f8bd0a4918f933ca3fc
b17595ae59386a2dc3e3046fa97688a9815a2d036fa10193534c0ebbecff67221e22ac9cf8b781cbae3a81eaccfc
0a2bd1a99081b1e4fe99b19caa771876ba7cce16d002feb4578cd89bc6f1faaca639ab48f3cb56007bcc5e248968
f4a17a95b8cdbc7d8bbd7c63630da878cd4d471fc75c60bac5f730d94fefe8fdd2f2fa8accd62dbe100eab7773e79
15e91be4474291b9dacea63a8267390bcb4855b5825554ebb07d4a29ce077c364213c575c461d1e9fafa0c29fde
1c6de1d5630e015200821b2f3ae91e53cd8591433dd7c0b4c8bc",
 "previous_digest_end": false,
 "log_files": [{
  "bucket": "bucket",
  "object": "CloudTraces/cn-north-01/2017/3/28/ECS/mylog_CloudTrace_cn-north-01/
_2017-03-28T02-09-17Z_0faa86bc40071242.json.gz",
  "log_hash_value": "633a8256ae7996e21430c3a0e9897828",
  "log_hash_algorithm": "MD5"
 }]
}
```


摘要文件签名

摘要文件的签名信息位于摘要文件对象的两个元数据属性中。每个摘要文件都有如下两个元数据项：

- meta-signature

  摘要文件签名的十六进制编码值。下面是示例签名：


  ```
  7af7cbef4f3c78eab5048030d402810841400cf70eb22f93d4fedd13b13a8208a5dc04ce2f8bd0a4918f933c
  a3fcb17595ae59386a2dc3e3046fa97688a9815a2d036fa10193534c0ebbecff67221e22ac9cf8b781cbae3
  ```


a81eaccfc0a2bd1a99081b1e4fe99b19caa771876ba7cce16d002feb4578cd89bc6f1faaca639ab48f3cb560
07bcc5e248968f4a17a95b8cdbc7d8bbd7c63630da878cd4d471fc75c60bac5f730d94fefe8fdd2f2fa8accd
62dbe100eab7773e7915e91be4474291b9dacea63a8267390bcb4855b5825554ebb07d4a29ce077c3642
13c575c461d1e9fafa0c29fde1c6de1d5630e015200821b2f3ae91e53cd8591433dd7c0b4c8bc

- meta-signature-algorithm

  摘要文件签名的算法。下面是示例算法：

  SHA256withRSA

摘要文件注意事项

- 启动摘要文件

  启动事件文件完整性校验时，将生成一个启动摘要文件。在启动摘要文件中，与前一摘要文件相关的以下字段将为空：

  - previous_digest_bucket
  - previous_digest_object
  - previous_digest_hash_value
  - previous_digest_hash_algorithm
  - previous_digest_signature

- “空”摘要文件

  即使在摘要文件记录的一小时时间段内您的账户中没有事件活动，云审计也将提交摘要文件，该摘要文件内容最后的log_files:[]字段将为空。如果需要确定在摘要文件记录的一小时内未提交事件文件，这非常有用。

- 摘要文件链

  摘要文件包含前一摘要文件（如果存在）的数字签名及哈希值，这样可实现一个“链”，在指定时间范围内的摘要文件可以从最近开始往前连续校验。

- 摘要文件桶

  摘要文件提交到和事件文件相同的与跟踪器关联的OBS桶中。

- 摘要文件存储文件夹

  摘要文件存放在与事件文件不同的文件夹中，分开放置便于您执行细粒度安全策略。

10.3 事件文件完整性校验

操作场景

由于云审计采用了行业标准、可公开使用的签名算法和哈希函数，因此，您可以自行创建用于校验云审计事件文件完整性的工具。原则上进行完整性校验时必须包含字段time、service_type、resource_type、trace_name、trace_rating、trace_type，其他字段由各服务自己定义。

启用事件文件完整性校验后，云审计将摘要文件提交到您的OBS桶中，您可以使用这些文件实现自己的校验解决方案。有关摘要文件的更多信息，请参阅**摘要文件**。

操作前提

在进行事件文件完整性校验前，您需先了解云审计摘要文件的签名方式：

云审计摘要文件使用RSA数字签名，对于每个摘要文件，云审计执行以下操作：

1. 创建数字签名字符串（由指定摘要文件字段构成），获取RSA私钥。
2. 将数字签名字符串的哈希值和私钥传递给RSA算法，生成数字签名，将数字签名编码成十六进制格式。
3. 将该数字签名放入摘要文件对象的meta-signature元数据属性中。

数字签名字符串包含以下摘要文件字段：

- UTC扩展格式的摘要文件结束时间戳（2017-03-28T02-09-17Z）。
- 当前摘要文件的OBS存储路径。
- 当前摘要文件（压缩后的）的哈希值（十六进制编码）。
- 前一摘要文件的十六进制数字签名。

校验事件文件完整性

实现事件文件完整性校验方案时，您需要先校验摘要文件，然后再校验其引用的事件文件。

1. 获取摘要文件。
   a. 从OBS桶中获取需要验证的时间范围的最新摘要文件。
   b. 检查该摘要文件在OBS桶中的存储位置是否与摘要文件中记录的OBS桶存储位置匹配。
   c. 从摘要文件对象的 meta-signature元数据属性中获取摘要文件的数字签名。
2. 获取用于校验数字签名的RSA公钥。

   当前云审计系统的RSA公钥是

   ```
   MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsjQDkl8COPRhOCvm7ZI8sYZ20ojl+ay/
   gwRSk9q0gkY3pP0RrAhSsEzgYdYjaMCqixkmbpt4AH9AROJU4drnoCAZSMqRxgv0bGC9kVd4q95l4zibsw
   AsksjuNQo/XoJjBl+rRAqCa+1uetgVU4k4Yx8RryYxYx/tImvMe/O4mGAIaTf+rsqt3VXR1QIj5lYR/nx41BEgC/
   Kb1elYAfDaaab8WS5INRprj7qdu6oAo4Ug47WqbecvEtG3JRpj5+oqLyW41Fvse3osC0h5DQdxTt4x00/rVZ
   +gH7Kua00y7gC8YOxFVpYbfn/oW61PUDeHG/N9hUjOrIgDDJpD2YbCIQIDAQAB。
   ```

3. 获取数字签名字符串。

   有了摘要文件的数字签名及RSA公钥后，您需要计算数字签名字符串。计算出数字签名字符串后，您就有了验证数字签名所需的输入。

   数字签名字符串采用以下格式：

   ```
   signature_string = digest_end_time
   + digest_object
   + Hex(hash(digest-file-content))
   + previous_digest_signature
   ```

   下面是数字签名字符串的示例：

   ```
   2017-03-28T02-09-17ZCloudTraces/cn-north-01/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_cn-north-01/
   _2017-03-28T02-09-17Z.json.gze280d203da44015e0eda3faa7a2ec9612221cc0dc8b0fe320db4febe6014
   2350641ad19da18cb6d3f5e7faad792c3efe98836c6d6547f5e5c7a48f7088000a057af26cc3bb913cae163
   7befa9e4231b7d1fd6d98eaba735e509e7c5ea3c6757f732b4468f7418ef18e3312ac696dd786ec5792eacf
   94aee27cd7be76bf23b641c5e9a686cca6414745787254100c2bee31e584a15c2229270f9dee81f9043574
   ```

4. 校验摘要文件。

   将**3**获取的数字签名字符串、摘要文件的数字签名和公钥传给 RSA 签名验证算法。如果输出为 true，则数字签名匹配，摘要文件有效。

5. 校验事件文件。

   校验摘要文件有效后，您可以校验其记录的事件文件。

摘要文件记录了事件文件的哈希值，文件上传到OBS后会在其ETag元数据中存储该文件的哈希值，如果某个事件文件在云审计提交到OBS桶后发生修改，则其哈希值会发生变化，且摘要文件的数字签名也不匹配。

如下是校验事件文件的具体步骤：

a. 从摘要文件信息中获取事件文件的bucket 和object 信息。
b. 调用OBS客户端接口获取事件文件对象头信息中的ETag元数据的值。
c. 从摘要文件对应事件的log_hash_value字段获取事件文件的原始哈希值。
d. 比较ETag元数据的值和摘要文件中事件文件的原始哈希值，如果哈希值匹配，则事件文件有效。

6. 校验之前的摘要文件和事件文件。

在每个摘要文件中，如下字段提供了前一摘要文件的位置和签名：

- previous_digest_bucket
- previous_digest_object
- previous_digest_signature

按照**4**和**5**校验每个摘要文件的签名及其记录的事件文件。

对于**6**的摘要文件，您不需要从摘要文件对象的meta-signature元数据属性中获取数字签名。previous_digest_signature字段提供了前一摘要文件的数字签名。您可以一直向前校验摘要文件和事件文件，直到到达起始的摘要文件，或摘要文件链断开。

下面的示例代码段提供校验云审计摘要和事件文件的框架代码，该代码段使用的jar包如下，推荐使用下面jar包版本：

- esdk-obs-java-2.1.16.jar
- commons-logging-1.2.jar
- httpasyncclient-4.1.2.jar
- httpclient-4.5.3.jar
- httpcore-4.4.4.jar
- httpcore-nio-4.4.4.jar
- java-xmlbuilder-1.1.jar
- jna-4.1.0.jar
- log4j-api-2.8.2.jar
- log4j-core-2.8.2.jar
- commons-codec-1.9.jar
- json-20160810.jar
- commons-io-2.5.jar

示例校验代码段：

```
import java.io.BufferedInputStream;
import java.io.BufferedReader;
import java.io.ByteArrayInputStream;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.Arrays;
import java.util.zip.GZIPInputStream;
```



```
import org.apache.commons.codec.binary.Base64;
import org.apache.commons.codec.binary.Hex;
import org.apache.commons.io.IOUtils;
import org.json.JSONObject;

import com.obs.services.ObsClient;
import com.obs.services.ObsConfiguration;
import com.obs.services.model.ObjectMetadata;
import com.obs.services.model.S3Object;

public class DigestFileValidator {
    public static void main(String[] args) {
        // 摘要文件所在桶名称
        String digestBucket = "bucketname";
        // 摘要文件存储路径，样例：CloudTraces/eu-de/2017/11/15/Digest/ECS/tGPYa_CloudTrace-
Digest_eu-de_2017-11-15T10-12-10Z.json.gz
        String digestObject = "digestObject";

        // 认证用的ak和sk直接写到代码中有很大的安全风险，建议在配置文件或者环境变量中密文存放，使
用时解密，确保安全
        // 本示例以ak和sk保存在环境变量中来实现身份验证为例，运行本示例前请先在本地环境中设置环境
变量HUAWEICLOUD_SDK_AK和HUAWEICLOUD_SDK_SK
        String ak = System.getenv("HUAWEICLOUD_SDK_AK");
        String sk = System.getenv("HUAWEICLOUD_SDK_SK");

        ObsConfiguration obsConfig = new ObsConfiguration();
        obsConfig.setEndPoint("obs.cn-north-4.myhuaweicloud.com");

        ObsClient client = new ObsClient(ak, sk, obsConfig);

        try {
            // 获取摘要文件对象
            S3Object object = client.getObject(digestBucket, digestObject);

            InputStream is = new BufferedInputStream(object.getObjectContent());
            byte[] digestFileBytes = IOUtils.toByteArray(is);

            // 获取摘要文件哈希值
            MessageDigest messageDigest = MessageDigest.getInstance("MD5");
            messageDigest.update(digestFileBytes);
            byte[] digestFileHashBytes = messageDigest.digest();

            StringBuilder outStr = new StringBuilder();
            GZIPInputStream gis = new GZIPInputStream(new ByteArrayInputStream(digestFileBytes));
            BufferedReader bufferedReader = new BufferedReader(new InputStreamReader(gis, "UTF-8"));
            String line;
            while ((line = bufferedReader.readLine()) != null) {
                outStr.append(line);
            }
            bufferedReader.close();
            String digestInfo = outStr.toString();

            // 从OBS桶中的摘要文件头中获取元数据meta-signature的值，即该摘要文件的数字签名
            ObjectMetadata objectMetadata = client.getObjectMetadata(digestBucket, digestObject);
            String digestSignature = objectMetadata.getMetadata().get("meta-signature").toString();
            JSONObject digestFile = new JSONObject(digestInfo);
            // 校验摘要文件在OBS桶中是否移动过
            if (!digestFile.getString("digest_bucket").equals(digestBucket) || !
digestFile.getString("digest_object")
                .equals(digestObject)) {
                System.err.println("Digest file has been moved from its original location.");
            } else {
                // 获取数字签名字符串
                String signatureString = digestFile.getString("digest_end_time") +
digestFile.getString("digest_object")
                    + Hex.encodeHexString(digestFileHashBytes) +
digestFile.getString("previous_digest_signature");
```



```
            String publicKeyString
                =
"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsjQDkl8COPRhOCvm7ZI8sYZ20ojl+ay/
gwRSk9q0gkY3pP0RrAhSsEzgYdYjaMCqixkmbpt4AH9AROJU4drnoCAZSMqRxgv0bGC9kVd4q95l4zibsw
AsksjuNQo/XoJjBl+rRAqCa+1uetgVU4k4Yx8RryYxYx/tImvMe/O4mGAIaTf+rsqt3VXR1QIj5lYR/nx41BEgC/
Kb1elYAfDaaab8WS5INRprj7qdu6oAo4Ug47WqbecvEtG3JRpj5+oqLyW41Fvse3osC0h5DQdxTt4x00/rVZ
+gH7Kua00y7gC8YOxFVpYbfn/oW61PUDeHG/N9hUjOrIgDDJpD2YbCIQIDAQAB";

            // 解密公钥
            byte[] publicKeyBytes = Base64.decodeBase64(publicKeyString);
            // 构造X509EncodedKeySpec对象
            X509EncodedKeySpec x509EncodedKeySpec = new X509EncodedKeySpec(publicKeyBytes);

            // 指定加密算法
            KeyFactory keyFactory = KeyFactory.getInstance("RSA");
            // 取公钥匙对象
            PublicKey publicKey = keyFactory.generatePublic(x509EncodedKeySpec);

            Signature signatureInstance = Signature.getInstance("SHA256withRSA");
            signatureInstance.initVerify(publicKey);
            signatureInstance.update(signatureString.getBytes("UTF-8"));

            byte[] signatureHashExpect = Hex.decodeHex(digestSignature.toCharArray());

            // 校验签名是否有效
            if (signatureInstance.verify(signatureHashExpect)) {
                System.out.println("Digest file signature is valid, validating log files…");

                for (int i = 0; i < digestFile.getJSONArray("log_files").length(); i++) {
                    JSONObject logFileJson = digestFile.getJSONArray("log_files").getJSONObject(i);
                    String logBucket = logFileJson.getString("bucket");
                    String logObject = logFileJson.getString("object");

                    // 从OBS桶中的事件文件头中获取元数据ETag的值，即事件文件的哈希值
                    ObjectMetadata objectLogMetadata = client.getObjectMetadata(logBucket,
logObject);
                    String logHashValue = objectLogMetadata.getMetadata().get("ETag").toString();
                    logHashValue = logHashValue.replace("\"", "");
                    byte[] logFileHash = Hex.decodeHex(logHashValue.toCharArray());

                    // 从摘要文件中获取事件文件的哈希值
                    byte[] expectedHash = logFileJson.getString("log_hash_value").getBytes();
                    boolean hashMatch = Arrays.equals(expectedHash, logFileHash);
                    if (!hashMatch) {
                        System.err.println("Validate log file hash failed.");
                    } else {
                        System.out.println("Log file hash is valid.");
                    }
                }
            } else {
                System.err.println("Validate digest signature failed.");
            }

            System.out.println("Digest file validation completed.");

            // 获取前一摘要文件的previous_digest_bucket, previous_digest_object,
previous_digest_signature，获取到该摘要文件后校验摘要文件哈希值及数字签名
            String previousDigestBucket = digestFile.getString("previous_digest_bucket");
            String previousDigestObject = digestFile.getString("previous_digest_object");

            // 从摘要文件对象头中的meta-signature元数据属性中获取该摘要文件的数字签名
            ObjectMetadata objectPreviousMetadata = client.getObjectMetadata(previousDigestBucket,
                previousDigestObject);
            String signatruePrevious = objectPreviousMetadata.getMetadata().get("meta-
signature").toString();
            String signatruePreviousExpect = digestFile.getString("previous_digest_signature");
            if (signatruePrevious.equals(signatruePreviousExpect)) {
                System.out.println(
                    "Previous digest file signature is valid, " + "validating previous digest file hash value…
```



```
");

                    String digestPreviousHashValue =
objectPreviousMetadata.getMetadata().get("ETag").toString();
                    // ETag元数据的值是事件文件的哈希值用双引号引起来，这里需把双引号去掉
                    String digestPreviousHashValueExpect = "\"" +
digestFile.getString("previous_digest_hash_value")
                        + "\"";
                    if (digestPreviousHashValue.equals(digestPreviousHashValueExpect)) {
                        System.out.println("Previous digest file hash value is valid.");
                    } else {
                        System.err.println("Validate previous digest file hash value failed.");
                    }
                }
            }
        } catch (Exception e) {
            System.out.println("Validate digest file failed.");
        }
    }
}
```


11 支持审计的关键操作

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 11-1 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
创建关键操作通知	notification	createNotification
删除关键操作通知	notification	deleteNotification
修改关键操作通知	notification	updateNotification
修改关键操作通知状态	notification	updateNotificationStatus
停用关键操作通知	notification	updateNotification
启用关键操作通知	notification	updateNotification
导出事件列表事件	trace	getTrace

12 权限管理

如果您需要对您所拥有的*云审计服务*（CTS）进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用CTS。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将CTS资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

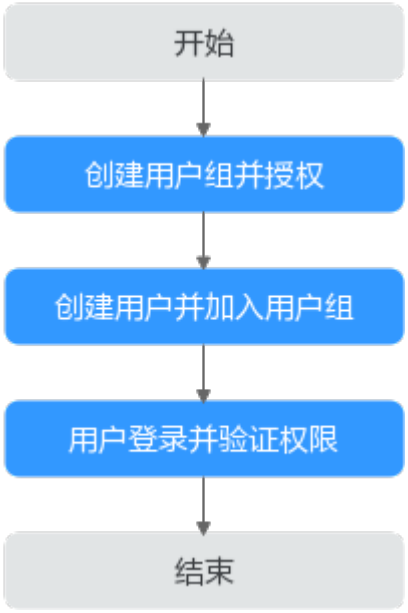
如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用CTS服务的其它功能。

前提条件

给用户组授权之前，请您了解用户组可以添加的CTS权限，并结合实际需求进行选择，CTS支持的系统权限，请参见：**CTS系统权限**。若您需要对除CTS之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

示例流程

图 12-1 给用户授予 CTS 权限



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予权限“CTS Administrator”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，切换至授权区域，验证权限。

13 配额调整

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少关键操作通知。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。
4. 您可以在“服务配额”页面，查看各项资源的总配额、及使用情况。

14 支持审计的服务及操作列表

表 14-1 支持审计的服务及操作列表

分类	云服务	service_type	审计操作参考文档
计算	弹性云服务器	ECS	弹性云服务器支持审计的操作列表
	镜像服务	IMS	镜像服务支持审计的操作列表
	裸金属服务器	BMS	裸金属服务器支持审计的操作列表
	弹性伸缩	AS	弹性伸缩支持审计的操作列表
	函数工作流	FunctionGraph	函数工作流支持审计的操作列表
	云手机	CPH	云手机支持审计的操作列表
存储	云服务器备份	CSBS	云服务器备份支持审计的操作列表
	对象存储服务	OBS	对象存储服务支持审计的操作列表
	云硬盘	EVS	云硬盘支持审计的操作列表
	云硬盘备份	VBS	云硬盘备份支持审计的操作列表
	内容分发网络	CDN	内容分发网络支持审计的操作列表
	高性能弹性文件服务	SFS_Turbo	高性能弹性文件服务支持审计的操作列表
	云备份	CBR	云备份支持审计的操作列表
	云存储网关	CSG	云存储网关支持审计的操作列表
网络	虚拟私有云	VPC	虚拟私有云支持审计的操作列表
	云专线	DC	云专线支持审计的操作列表

分类	云服务	service_type	审计操作参考文档
	弹性负载均衡	ELB	弹性负载均衡支持审计的操作列表
	NAT网关	NAT	NAT网关支持审计的操作列表
	虚拟专用网络	VPN	虚拟专用网络支持审计的操作列表
	VPC终端节点	VPCEP	VPC终端节点支持审计的操作列表
	全球加速	GA	全球加速支持审计的操作列表
	云连接	CC	云连接支持审计的操作列表
	企业路由器	ER	企业路由器支持审计的操作列表
容器	云容器引擎	CCE	云容器引擎支持审计的操作列表
	云容器实例	CCI	云容器实例支持审计的操作列表
	容器镜像服务	SWR	容器镜像服务支持审计的操作列表
	云原生服务中心	OSC	云原生服务中心支持审计的操作列表
迁移	对象存储迁移服务	OMS	对象存储迁移服务支持审计的操作列表
	主机迁移服务	SMS	主机迁移服务支持审计的操作列表
	云数据迁移	CDM	云数据迁移支持审计的操作列表
管理与监管	云监控服务	CES	云监控服务支持审计的操作列表
	云审计服务	CTS	云审计服务支持审计的操作列表
	统一身份认证	IAM	统一身份认证支持审计的操作列表
	标签管理服务	TMS	标签管理服务支持审计的操作列表
	资源访问管理	RAM	资源访问管理支持审计的操作列表
	云日志服务	LTS	云日志服务支持审计的操作列表
	配置审计（Config）	Config	配置审计服务支持审计的操作列表
	应用运维管理	AOM	应用运维管理（1.0）支持审计的操作列表

分类	云服务	service_type	审计操作参考文档
		ICMGR	应用运维管理（1.0）支持审计的操作列表
	应用性能管理	APM	应用性能管理（1.0）支持审计的操作列表
	消息通知服务	SMN	消息通知服务支持审计的操作列表
	应用身份管理服务	OneAccess	应用身份管理服务支持审计的操作列表
	IAM身份中心	IdentityCenter	IAM身份中心支持审计的操作列表
	资源编排服务	RFS	资源编排服务支持审计的操作列表
应用中间件	微服务引擎	CSE	微服务引擎支持审计的操作列表
	分布式消息服务Kafka版	DMS	分布式消息服务Kafka支持审计的操作列表
	分布式消息服务RabbitMQ版	DMS	分布式消息服务RabbitMQ支持审计的操作列表
	分布式消息服务RocketMQ版	DMS	分布式消息服务RocketMQ版支持审计的操作列表
	分布式缓存服务	DCS	分布式缓存服务支持审计的操作列表
	多活高可用服务	MAS	多活高可用服务支持审计的操作列表
	事件网格	EG	事件网格支持审计的操作列表
	API网关	APIG	API网关支持审计的操作列表
数据库	分布式数据库中间件	DDM	分布式数据库中间件支持审计的操作列表
	云数据库	RDS	云数据库RDS for MySQL支持审计的操作列表
		RDS	云数据库RDS for PostgreSQL支持审计的操作列表
		RDS	云数据库RDS for SQL Server支持审计的操作列表
	数据复制服务	DRS	数据复制服务支持审计的操作列表

分类	云服务	service_type	审计操作参考文档
	文档数据库服务	DDS	文档数据库服务支持审计的操作列表
	云数据库 GaussDB	GaussDB	云数据库GaussDB支持审计的操作列表
	云数据库 GeminiDB	NoSQL	GeminiDB Redis支持审计的操作列表
		NoSQL	GeminiDB Influx支持审计的操作列表
		NoSQL	GeminiDB Cassandra支持审计的操作列表
		NoSQL	GeminiDB Mongo支持审计的操作列表
	云数据库 TaurusDB	TaurusDB	云数据库TaurusDB支持审计的操作列表
	数据管理服务	DAS	数据管理服务支持审计的操作列表
	数据库和应用迁移	UGO	数据库和应用迁移支持审计的操作列表
开发与运维	流水线	CloudPipeline	流水线支持审计的操作列表
	编译构建	CodeArtsBuild	编译构建支持审计的操作列表
	性能测试服务	CPTS	性能测试服务支持审计的操作列表
	应用管理与运维平台	ServiceStage	应用管理与运维平台支持审计的操作列表
	开源治理服务	CodeArtsGovernance	开源治理服务支持审计的操作列表
	需求管理	CodeArtsReq	需求管理支持审计的操作列表
	云应用引擎	CAE	云应用引擎支持审计的操作列表
IoT物联网	设备接入	IoTDA	设备接入支持审计的操作列表
	路网数字化服务	DRIS	路网数字化服务支持审计的操作列表
	IoT边缘	IoTEdge	IoT边缘支持审计的操作列表
	全球SIM联接	GlobalSIMLink	全球SIM联接支持审计的操作列表
	IoT数据分析	IoTA	IoT数据分析支持审计的操作列表

分类	云服务	service_type	审计操作参考文档
安全与合规	数据加密服务	DEW	数据加密服务支持审计的操作列表
	云防火墙	CFW	云防火墙支持审计的操作列表
	DDoS防护	AAD	DDoS防护支持审计的操作列表
	Web应用防火墙	WAF	Web应用防火墙支持审计的操作列表
	漏洞管理服务	VSS	漏洞管理服务支持审计的操作列表
	数据库安全服务	DBSS	数据库安全服务支持审计的操作列表
	主机安全服务	HSS	主机安全服务支持审计的操作列表
	数据安全中心	DSC	数据安全中心支持审计的操作列表
	云堡垒机	CBH	云堡垒机支持审计的操作列表
	云证书管理服务	PCA	云证书管理服务支持审计的操作列表
	安全云脑	SecMaster	安全云脑支持审计的操作列表
企业应用	应用与数据集成平台	ROMAConnect	应用与数据集成平台支持审计的操作列表
	域名注册服务	Domains	域名注册服务支持审计的操作列表
	隐私保护通话	PrivateNumber	隐私保护通话支持审计的操作列表
	云解析服务	DNS	云解析服务支持审计的操作列表
	语音通话	VoiceCall	语音通话支持审计的操作列表
区块链	区块链服务	BCS	区块链服务支持审计的操作列表
人工智能	人脸识别服务	FRS	人脸识别服务支持审计的操作列表
	AI开发平台	ModelArts	AI开发平台支持审计的操作列表
	文字识别	OCR	文字识别支持审计的操作列表
大数据	MapReduce服务	MRS	MapReduce服务支持审计的操作列表
	数据湖探索	DLI	数据湖探索支持审计的操作列表

分类	云服务	service_type	审计操作参考文档
	数据仓库服务GaussDB	DWS	数据仓库服务GaussDB支持审计的操作列表
	云搜索服务	CSS	云搜索服务支持审计的操作列表
	数据治理中心	DAYU	数据湖治理中心支持审计的操作列表
	表格存储服务	CloudTable	表格存储服务支持审计的操作列表
	智能数据洞察服务	DataArtsInsight	智能数据洞察服务支持审计的操作列表
CDN与智能边缘	内容分发网络	CDN	内容分发网络支持审计的操作列表
	智能边缘平台	IEF	智能边缘平台支持审计的操作列表
	智能边缘云	IEC	智能边缘云支持审计的操作列表
	智能边缘小站	IES	智能边缘小站支持审计的操作列表
用户服务	企业项目管理	EPS	企业项目管理支持审计的操作列表
	成本中心	CostCenter	成本中心支持审计的操作列表
工业软件	工业数字模型驱动引擎	iDME	工业数字模型驱动引擎支持审计的操作列表
	硬件开发工具链平台云服务	CraftArtsIPDCenter	硬件开发工具链平台云服务支持审计的操作列表
视频	视频直播	LIVE	视频直播支持审计的操作列表
	媒体处理	MPC	媒体处理支持审计的操作列表
开天aPaaS	云地图服务	KooMap	云地图服务支持审计的操作列表
	集成工作台	MSSI	集成工作台支持审计的操作列表
	云盘服务	KooDrive	云盘服务支持审计的操作列表
	应用平台	AppStage	应用平台支持审计的操作列表
其他	消息中心	MESSAGECENTER	消息中心支持审计的操作列表

