云审计服务

用户指南

文档版本 01

发布日期 2024-07-30

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

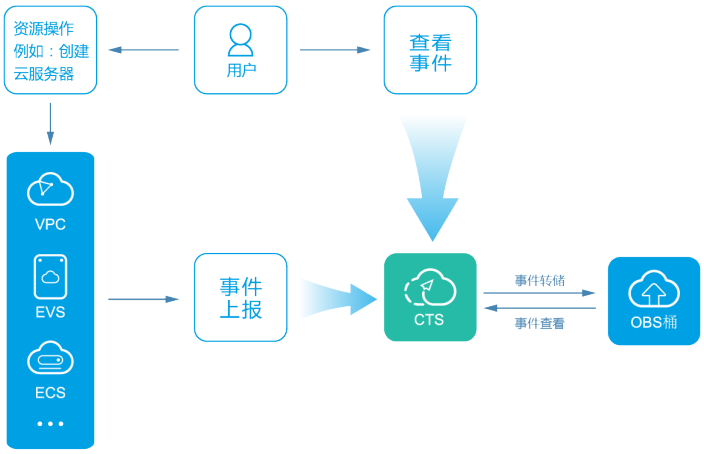
1 产品介绍

1.1 什么是云审计服务

日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。

云审计服务（Cloud Trace Service，以下简称CTS），是安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪、问题回溯和问题定位等常见应用场景。

图 1-1 云审计服务介绍



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，或转储至云日志服务（Log Tank Service，简称LTS）下的LTS日志流，转储时会按照服务维度压缩审计日志为事件文件。
- 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。

云审计服务记录的操作有以下三种：

- 用户登录管理控制台的操作。
- 用户通过云服务支持的API执行的操作。
- 系统内各服务内部触发的操作。

1.2 基本概念

追踪器

首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。

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。

目前，一个租户仅支持开通1个追踪器。

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。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。

事件指管理事件，是云服务上报的事件。

事件列表

事件列表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。事件列表最多显示近7天的事件，默认情况下显示最近1小时的事件，并且不会记录查询操作的相关信息。

- 管理类事件指云账户中对云服务资源新建、修改、删除等操作的详细信息。

事件文件

事件文件是系统自动生成的事件集，云审计服务将按照服务、转储周期两个维度，生成多个事件文件，同步保存至用户指定的OBS桶中。通常情况下，单个服务在单个转储周期内产生的所有事件仅会压缩生成一个事件文件，但在事件数量较多时，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。

事件文件的格式为json，呈现事件的原始内容如**图1-2**所示。

图 1-2 事件文件示例


```
[{
    "time": 1491482532828,
    "user": {
        "id": "59f40829165447fb9470b56f41dff599",
        "name": "[redacted]",
        "domain": {
            "name": "[redacted]",
            "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
        }
    },
    "request": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "disabled"
    },
    "response": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "disabled",
        "tracker_name": "system"
    },
    "service_type": "CTS",
    "resource_type": "tracker",
    "resource_name": "system",
    "source_ip": "[redacted]",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482532857,
    "trace_id": "7519ef09-1ac6-11e7-8cc0-3d812829baf6",
    "trace_status": "normal"
},
{
    "time": 1491482535203,
    "user": {
        "id": "59f40829165447fb9470b56f41dff599",
        "name": "[redacted]",
        "domain": {
            "name": "[redacted]",
            "id": "0f27bc42d1eb46a69482a72cbfc33ed2"
        }
    },
    "request": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "enabled"
    },
    "response": {
        "bucket_name": "obs-570f",
        "file_prefix_name": "-RsU",
        "status": "enabled",
        "tracker_name": "system"
    },
    "service_type": "CTS",
    "resource_type": "tracker",
    "resource_name": "system",
    "source_ip": "[redacted]",
    "trace_name": "updateTracker",
    "trace_type": "ConsoleAction",
    "api_version": "1.0",
    "record_time": 1491482535224,
    "trace_id": "76831bfb-1ac6-11e7-98ff-a1036f244dcd",
    "trace_status": "normal"
}]
```


事件文件完整性校验

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。因此云审计服务适时推出了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。

事件文件完整性校验功能使用业界标准算法构建，对事件文件生成原始哈希值，当事件文件被修改或者删除时，该哈希值就会发生改变，通过对哈希值进行追踪查看就能确定事件文件是否被修改；同时采用RSA算法对摘要文件进行签名，保证摘要文件不被修改。这样任何对事件文件进行修改或者删除的蛛丝马迹都会被云审计服务完整记录下来。

启用事件文件完整性校验功能后，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。

云审计使用公有和私有密钥对每个摘要文件进行签名，摘要文件转储到OBS桶后，您可以使用公有密钥校验摘要文件。

1.3 工作原理

云审计服务直接对接云平台上的其他服务，记录用户的云服务资源的操作信息，实现用户操作云服务资源动作和结果的实时记录功能。

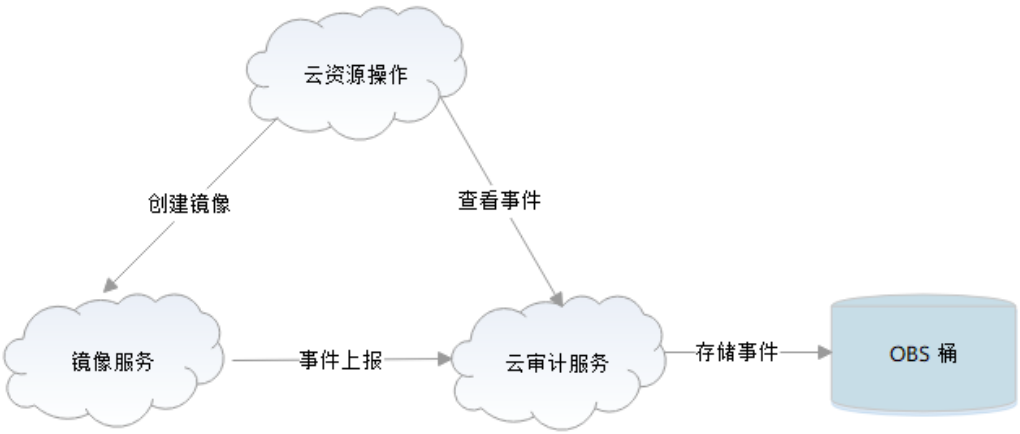
使用云审计服务创建追踪器可以跟踪记录事件文件。如已配置事件转储至OBS服务和LTS服务，事件文件将保存在OBS桶和LTS日志组中。

用户可以对事件文件执行以下两种操作：

- 事件文件的创建和保存：
  - 当用户在弹性云服务器、云硬盘服务、镜像服务等其它与云审计服务完成对接的服务中，进行了增加、删除、修改类型的操作时，被操作的服务会自动记录操作动作及操作结果，并按照指定的格式发送事件到云审计服务完成事件归档。
  - 云审计服务管理控制台会保存最近7天的操作记录，如已配置OBS服务或LTS服务，云审计服务会定期将操作记录同步保存到用户定义的OBS桶或LTS日志组中进行长期保存。
- 事件文件查询：
  - 在“事件列表”页面，用户可以按照通过系统自带的条件和时间过滤功能，查询最近7天的操作记录。
  - 若要查询7天前的操作记录且已配置OBS服务或LTS服务，可以在对应的OBS桶中下载事件文件进行查看，或在对应的LTS日志组中查看日志。
  - 在云审计服务页面的追踪器界面，用户可以对追踪器进行启用、停用、删除、配置等操作。

以用户创建镜像为例，在用户使用镜像服务执行创建镜像的操作过程中，镜像服务会将用户操作事件上报至云审计服务，如已配置OBS服务，云审计服务将事件转存至OBS桶中。用户也可以通过云审计服务的事件列表查看事件文件。云审计服务工作原理示意如图1-3所示。

图 1-3 云审计服务工作原理示意图



1.4 使用场景

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，可以很方便的实现审计类功能，以帮助用户更好地规划和利用已有资源、甄别违规或高危操作。

云审计服务主要有以下应用场景：

- **合规审计**

  云审计服务能够助力客户的业务系统通过PCI DSS、ISO 27001等常见行业硬性规范中关于审计部分的认证。云审计服务所提供的操作日志记录、查询等功能及安全控制能力，是企事业单位特别是金融、支付类企业满足认证要求的必备条件。

  对业务上云的客户而言，关于审计方面的合规认证内容通常分为两部分：云服务商所负责的客户业务系统平台与资源的合规以及客户负责的自身业务系统的合规。

  一方面，云审计服务是合规性的组成部分之一，其几乎覆盖所有服务、所有资源的操作记录能力，以及审计日志在传输、存储、加密、容灾、防篡改等方面的安全能力，是认证中针对业务系统平台与资源合规的核心保障。另一方面，针对客户自身的业务系统的合规认证，云审计服务将在认证过程中积极响应，协助完成待满足项的解决方案设计和实现，支撑客户通过认证。

- **关键操作通知**

  云审计服务与函数工作流服务（FunctionGraph）共同提供关键操作通知功能，通知对象包括自然人及业务接口。实际应用场景举例如下：

  客户可配置面向己方独立审计系统的http/https通知，将CTS收到的审计日志即时同步到客户自有的审计系统，独立审计。

  客户可在FunctionGraph中，选择某类型的审计日志作为触发器（如文件上传），触发预设的工作流（如转换文件格式），从而简化业务开展、运维或规避问题和风险。

- **数据价值挖掘**

  云审计服务支持对审计日志中的数据进行挖掘，为业务健康度分析、风险分析、资源跟踪、成本分析等提供支撑，并支持开放审计数据给客户，供客户自行挖掘数据价值。

  审计日志中包含时间、操作人、操作设备ip、被操作资源、操作详情等各类信息，具有挖掘价值。

  客户可通过配置http/https通知的模式，将审计日志即时同步到自有系统进行分析。CTS也正在对接云监控、云日志，提供高危操作展示、越权操作分析、资源使用分布等功能，并为业务健康度分析、成本分析提供数据支撑。

- **问题定位分析**

  云审计服务可通过配置查询条件，精确查找问题发生时的操作及其详情，降低问题发现、定位和解决的时间、人力成本。

  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。

  云审计服务提供的检索维度包括事件类型、事件来源、资源类型、筛选类型、操作用户和事件级别等，且在审计日志中，包含本次操作的请求和响应的详情信息，是定位云上问题最快捷、最有效的定位手段之一。

  当客户遇到云上问题时，可设置条件检索问题发生时间段内的可疑操作，将审计日志同步给处理问题的运维、客服人员。

1.5 计费说明

云审计服务本身免费，包括开通追踪器、事件跟踪以及7天内事件的存储和检索。同时云审计服务与其他云服务可以组合使用（**可能会产生部分由其他服务收取的费用**），为您提供事件文件转储、事件文件加密等增值服务，这些增值服务可能产生额外费用，通常情况下，云审计服务产生的增值服务费用很低，因此建议您根据实际需要搭配使用。

增值服务列表如下：

- 事件转储：需要使用对象存储服务（OBS），管理类追踪器配置的转储事件文件将永久保存。
- 事件文件加密存储：在开通事件转储的基础上，需要使用数据加密服务（DEW）对存储在OBS桶中的事件文件进行加密。
- 日志转储：CTS提供将审计日志转储至LTS的功能，但依赖云日志服务（LTS）的日志存储功能收费。
- 关键操作通知：CTS提供关键操作通知功能，可在发生特定操作时向用户手机、邮箱发送消息，但发送消息需要使用消息通知服务（SMN）订阅主题。

1.6 权限管理

如果您需要对云上购买的CTS资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并使用策略来控制他们对资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有CTS的使用权限，但是不希望他们拥有删除CTS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CTS，但是不允许删除CTS的权限策略，控制他们对CTS资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CTS服务的其它功能。

IAM提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。请参见《IAM产品介绍》。

CTS 权限

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CTS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问CTS时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略，策略是角色的升级版。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，CTS管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分。

如表1-1所示，包括了CTS的所有系统权限。

表 1-1 CTS 系统权限

系统角色/策略名称	描述	类别	依赖关系
CTS FullAccess	云审计服务的所有权限。	系统策略	无
CTS ReadOnlyAccess	云审计服务的只读权限。	系统策略	无
CTS Administrator	云审计服务的管理员权限，拥有CTS的所有权限。 拥有该权限的用户拥有除IAM外，其他所有服务的只读权限。	系统角色	该角色有依赖，需要在同项目中勾选依赖的角色：Tenant Guest、OBS Administrator和Security Administrator。

表1-2列出了CTS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 1-2 常用操作与系统权限的关系

操作	CTS FullAccess	CTS ReadOnlyAccess	CTS Administrator
查询事件列表	√	√	√
查询配额	√	√	√
创建追踪器	√	×	√
修改追踪器	√	×	√
停用追踪器	√	×	√
启用追踪器	√	×	√
查询追踪器	√	√	√
删除追踪器	√	×	√
创建关键操作通知	√	×	√
修改关键操作通知	√	×	√
停用关键操作通知	√	×	√
启用关键操作通知	√	×	√
查询关键操作通知	√	√	√

操作	CTS FullAccess	CTS ReadOnlyAccess	CTS Administrator
删除关键操作通知	√	×	√
批量添加标签	√	×	√
批量删除标签	√	×	√

自定义权限策略

如果系统预置的权限策略，不满足用户授权需求，CTS支持自定义权限策略。

- 自定义权限策略中可以添加的授权项请参考“《 CTS API指南 》 > 权限及授权项说明”。
- 自定义权限策略具体创建步骤请参见“《 IAM 用户指南 》 > 创建自定义策略”。

2 快速入门

2.1 入门指引

操作场景

使用云审计服务前需要开启云审计服务，开启云审计服务后系统会自动创建一个名称为“system”，类型为“管理事件”的追踪器，系统记录的所有操作将关联在该追踪器中。

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

- 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。

  说明

  由于云审计服务需要高频次的访问转储的OBS桶，因此必须选择使用标准存储类型的OBS桶。
- 数据加密服务（Data Encryption Workshop，简称DEW）：为事件文件加密功能提供密钥。
- 云日志服务（Log Tank Service，简称LTS）：提供日志存储功能。
- 消息通知服务（Simple Message Notification，简称SMN）：检测到关键操作时，调用消息通知服务向用户发送邮件、短信通知。

首次开通云审计服务

步骤1 登录管理控制台。

步骤2 单击左上角 ☰，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务。

步骤3 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**支持审计的服务及详细操作列表**。

步骤4 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

2.2 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。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

- 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。

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“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。

- 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
- 云服务：在下拉框中选择对应的云服务名称。
- 资源类型：在下拉框中选择对应的资源类型。
- 操作用户：在下拉框中选择一个或多个具体的操作用户。
- 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
  - normal：表示操作成功。
  - warning：表示操作失败。
  - incident：表示比操作失败更严重的情况，例如引起其他故障等。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

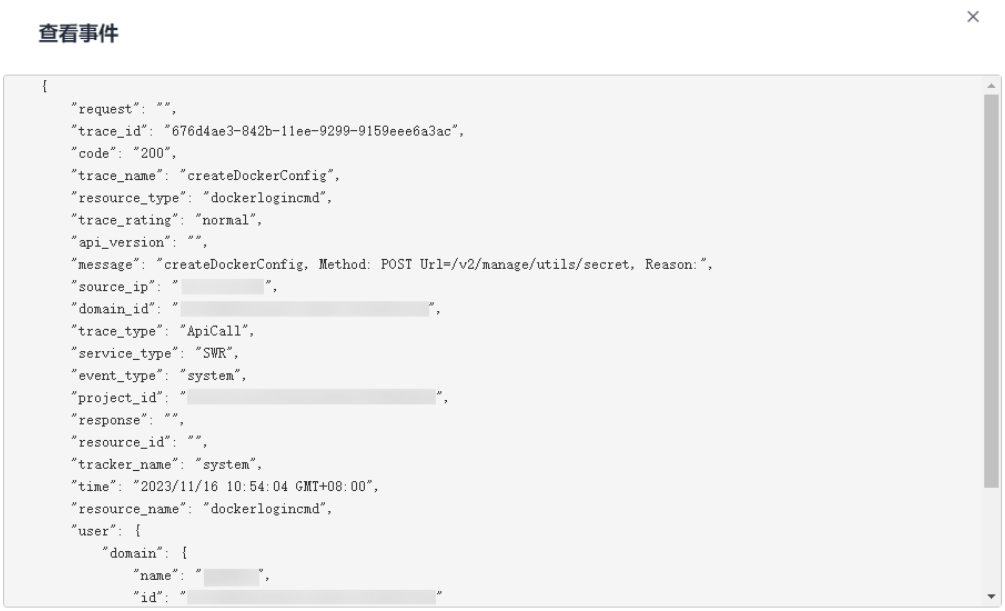
5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
   - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
   - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击按钮，可以获取到事件操作记录的最新信息。
   - 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。
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“管理与部署 > 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“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。
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。

2.3 查询转储事件

操作场景

云审计服务会定时将跟踪到的事件以事件文件的形式按周期保存至OBS桶。事件文件是按照服务、转储周期两个维度生成的事件集，系统会根据当前负载情况调整每个事件文件包含的事件数。云审计服务还支持将审计日志保存到LTS日志流中。

本节介绍如何在OBS中通过下载事件文件查看已保存至OBS桶的历史操作记录，以及如何在LTS日志流中查看事件记录。

前提条件

已在云审计服务中成功配置追踪器，且打开OBS转储开关或LTS转储开关。配置转储的方法请参见**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“管理与部署 >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。
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>region>2016>5>19>system>ECS***
   - 事件文件命名格式：

     操作事件文件前缀_CloudTrace_区域标示/区域标示-项目标示_日志文件上传至OBS的时间标示：年-月-日T时-分-秒Z_系统随机生成字符.json.gz

     例如：***File Prefix*_CloudTrace_region-project_2016-05-30T16-20-56Z_21d36ced8c8af71e.json.gz**

   说明

   OBS桶名和事件前缀为用户设置，其余参数均为系统自动生成。

   下载将产生请求费用和流量费用。

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

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2-1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 2-1 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“管理与部署 > 云审计服务 CTS”，进入云审计服务控制台页面。

步骤3 单击左侧导航树的“追踪器”，进入追踪器信息页面。

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

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

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

步骤6 单击按钮，可以下载日志文件到本地。

说明

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

----结束

2.4 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。

使用说明

- 由于云审计服务的关键操作通知需要使用消息通知服务向相关的订阅者发送通知，因此需要提前了解消息通知服务的创建主题、添加订阅等操作。
- 云审计服务支持创建100个关键操作通知：
  - 自定义类型的关键操作通知支持单独设置触发操作范围、指定操作用户和通知主题。
  - 完整类型的关键操作通知，支持通知主题。
- 如果云审计服务和云监控服务使用同一消息主题，则接受终端一样，但是发送的内容不同。
- 单个关键操作通知支持最多对10个用户组的50个用户发起的操作进行通知配置。单个关键操作通知不支持一次选择多个用户组，但是可以分次添加不同用户组中的用户在同一个关键操作通知。

创建关键操作通知

1. 登录管理控制台。
2. 单击左上角  ，选择“管理与部署 > 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 2-1 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
trace_type	事件的类型。
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：
     - 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“管理与部署 > 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2-2。

表 2-2 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。 **说明** 只有配置了SMN的关键操作通知，云审计服务才能正常启用/停用关键操作通知，未配置SMN则无法启用关键操作通知。
修改关键操作通知	单击操作列“修改”，可修改该关键操作通知的配置信息。
删除关键操作通知	单击操作列“删除”，可删除该关键操作通知。
搜索通知	在列表上方的搜索框，可以过滤通知名称、状态、模板名称和SMN主题来搜索通知。
刷新通知	单击右上角的  按钮，可刷新关键操作通知列表信息。
基础设置	单击右上角的  按钮，可以设置表格内容折行、固定操作列和自定义列表项的展示/隐藏。

----结束

3 查询事件

3.1 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。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

- 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。

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“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。

- 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
- 云服务：在下拉框中选择对应的云服务名称。
- 资源类型：在下拉框中选择对应的资源类型。
- 操作用户：在下拉框中选择一个或多个具体的操作用户。
- 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
  - normal：表示操作成功。
  - warning：表示操作失败。
  - incident：表示比操作失败更严重的情况，例如引起其他故障等。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近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“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。
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

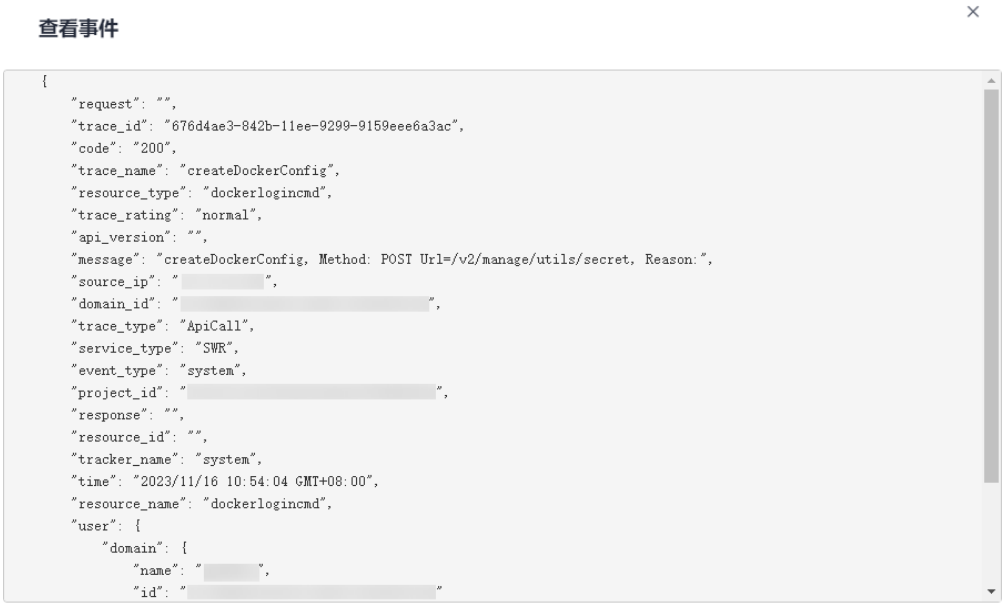
1. 登录管理控制台。
2. 单击左上角，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
     - 筛选类型按事件名称筛选时，还需选择某个具体的事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

- 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“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

3.2 查询转储事件

操作场景

云审计服务会定时将跟踪到的事件以事件文件的形式按周期保存至OBS桶。事件文件是按照服务、转储周期两个维度生成的事件集，系统会根据当前负载情况调整每个事件文件包含的事件数。云审计服务还支持将审计日志保存到LTS日志流中。

本节介绍如何在OBS中通过下载事件文件查看已保存至OBS桶的历史操作记录，以及如何在LTS日志流中查看事件记录。

前提条件

已在云审计服务中成功配置追踪器，且打开OBS转储开关或LTS转储开关。配置转储的方法请参见**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“管理与部署 >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。
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>region>2016>5>19>system>ECS***
   - 事件文件命名格式：

     操作事件文件前缀_CloudTrace_区域标示/区域标示-项目标示_日志文件上传至OBS的时间标示：年-月-日T时-分-秒Z_系统随机生成字符.json.gz

     例如：***File Prefix*_CloudTrace_region-project_2016-05-30T16-20-56Z_21d36ced8c8af71e.json.gz**

   说明

   OBS桶名和事件前缀为用户设置，其余参数均为系统自动生成。

   下载将产生请求费用和流量费用。

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

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3-1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 3-1 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“管理与部署 > 云审计服务 CTS”，进入云审计服务控制台页面。

步骤3 单击左侧导航树的“追踪器”，进入追踪器信息页面。

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

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

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

步骤6 单击按钮，可以下载日志文件到本地。

说明

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

----结束

4 管理类事件追踪器

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。

本章节介绍管理类追踪器的相关操作。

4.1 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。

说明

- 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。
- 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。

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。

说明

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，因此必须使用标准存储类型的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。

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“管理与部署 > 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”。

步骤6 设置追踪器的基本信息，单击“下一步”。

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《企业管理服务 用户指南》中的“创建企业项目”章节。

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4-1和表4-2。

表 4-1 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。
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	选择已有OBS桶：需要您选择一个已有的OBS桶。

参数名称	参数说明
OBS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秘钥。 “加密事件文件”开关打开时，云审计会从数据加密服务（DEW）获取当前用户的秘钥ID，在下拉选项可以直接选择秘钥。

表 4-2 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。

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。

表 4-3 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

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。

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“管理与部署 > 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”。

步骤6 单击“确定”，停用追踪器。

----结束

追踪器停用成功后，操作下的“停用”切换为“启用”，停用期间事件仍可以正常上报。如果您需要重新启用管理类追踪器，单击“启用 > 确定”。

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。

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“管理与部署 > 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”。

步骤6 在弹框中单击“确定”，完成删除管理类追踪器。

说明

删除管理类追踪器后，云审计服务依旧会保留历史事件操作记录，重新“开通云审计服务”可恢复管理类追踪器。

----结束

5 云审计服务应用示例

5.1 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。

前提条件

已开通云审计服务且追踪器状态正常。

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“管理与部署 > 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**查询转储事件**。

说明

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。

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“管理与部署>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**查询转储事件**。

   说明

   查询超过7天的操作记录，您必须对管理类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。
7. 参照**查询转储事件**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。

5.2 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。

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“管理与部署 >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“管理与部署 > 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“管理与部署>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“管理与部署>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。

5.3 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。

前提条件

已开通云审计服务且追踪器状态正常。

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“管理与部署 > 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：*{问题虚拟机ID}*”，或直接搜索*{问题虚拟机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**查询转储事件**。

说明

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。

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“管理与部署>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”>“问题虚拟机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。

6 云审计服务事件参考

6.1 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6-1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 6-1 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。必须为已对接CTS的云服务的英文缩写，且服务类型一般为大写字母。
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。
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。
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）。
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。
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）。

字段名称	是否必选	类型	描述
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 6-2 UserInfo

字段名称	是否必选	类型	描述
type	是	String	操作者的身份类型。
principal_id	是	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	是	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::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>
account_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”。
access_key_id	是	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”。

字段名称	是否必选	类型	描述
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	是	String	用户名称。 说明：user_name与name字段的含义一致。
principal_is_root_user	是	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	是	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。

表 6-3 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 6-4 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 6-5 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。

6.2 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",
    "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。

7 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。

```
{
    "Statement": [{
            "Sid": "xxxx",
            "Effect": "Allow",
            "Principal": {
                "ID": [
                    "domain/{{租户A domainId}}:agency/*"
                ]
            },
            "Action": [
                "PutObject",
                "PutObjectAcl"
            ],
            "Resource": [
                "{{bucketName}}/*"
            ]
        },
        {
            "Sid": "xxxx1",
            "Effect": "Allow",
```



```
        "Principal": {
        // 租户B OBS桶授权给租户A下的所有子用户后，A的子用户即可配置跨租户转储。
            "ID": [
                "domain/{{租户A domainId}}:user/*"
            ]
        // 联合身份用户场景配置如下。授权给租户A下指定身份提供商名称后，联邦登录账号即可配置跨租户转储。如果不涉及联合身份场景，可删除该行。
        //   "Federated": "domain/{{租户A domainId}}:identity-provider/{{provider-name}}"
        },
        "Action": [
            "HeadBucket"   // 部分不支持HeadBucket action的reigon，可以用ListBucket替代。
        ],
        "Resource": [
            "{{bucketName}}"
        ]
      }
   ]
}
```

表 7-1 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"，"PutObjectAcl"和"HeadBucket"三个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/*”（表示被授权用户A下的所有委托）。 ● “domain/账号ID:user/*”（表示被授权用户A下的所有子用户）。
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bucketName/*和bucketName。

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。

   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“管理与部署 >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。

8 校验云审计事件文件完整性

8.1 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。此功能只针对管理类事件。

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“管理与部署 > 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”。
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。

   说明

   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。

8.2 摘要文件

8.2.1 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**

8.2.2 摘要文件命名格式

***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**

8.2.3 摘要文件结构

表 8-1 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。

字段名称	是否必选	类型	描述
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。
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。

8.2.4 摘要文件样例


```
{
 "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/eu-west-0/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_eu-west-0/
_2017-03-28T02-09-17Z.json.gz",
 "digest_signature_algorithm": "SHA256withRSA",
 "digest_end": false,
 "previous_digest_bucket": "bucket",
 "previous_digest_object": "CloudTraces/eu-west-0/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_eu-
west-0/_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/eu-west-0/2017/3/28/ECS/mylog_CloudTrace_eu-west-0/
_2017-03-28T02-09-17Z_0faa86bc40071242.json.gz",
  "log_hash_value": "633a8256ae7996e21430c3a0e9897828",
  "log_hash_algorithm": "MD5"
 }]
}
```


8.2.5 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

8.2.6 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。

8.3 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/eu-west-0/2017/3/28/Digest/EVS/mylog_CloudTrace-Digest_eu-
   west-0/
   _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";


        ObsConfiguration obsConfig = new ObsConfiguration();

        obsConfig.setEndPoint("***Provide OBS EndPoint ***");
        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.");
    }
  }
}
```


9 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 9-1 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

10 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。

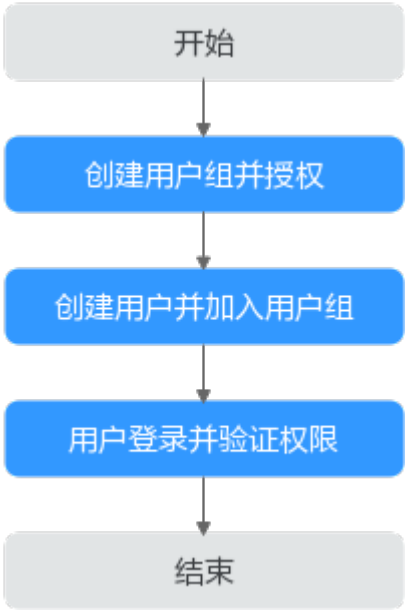
如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用CTS服务的其它功能。

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**。

示例流程

图 10-1 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。

11 支持审计的服务及操作列表

表 11-1 支持审计的服务及操作列表

分类	云服务	审计操作参考文档
计算	弹性云服务器	弹性云服务器支持审计的操作列表
	镜像服务	镜像服务支持审计的操作列表
	弹性伸缩	弹性伸缩支持审计的操作列表
	函数工作流	函数工作流支持审计的操作列表
存储	云服务器备份	云服务器备份支持审计的操作列表
	云硬盘备份	云硬盘备份支持审计的操作列表
	云备份	云备份支持审计的操作列表
网络	弹性负载均衡	弹性负载均衡支持审计的操作列表
	云解析服务	云解析服务支持审计的操作列表
容器	云容器引擎	云容器引擎支持审计的操作列表
迁移	主机迁移服务	主机迁移服务支持审计的操作列表
管理与监管	云审计服务	云审计服务支持审计的操作列表
	统一身份认证	统一身份认证支持审计的操作列表
	标签管理服务	标签管理服务支持审计的操作列表
	消息通知服务	消息通知服务支持审计的操作列表
应用与中间件	分布式消息服务	分布式消息服务支持审计的操作列表
	分布式消息服务 Kafka	分布式消息服务 Kafka支持审计的操作列表
	分布式消息服务 RocketMQ版	分布式消息服务RocketMQ版支持审计的操作列表

分类	云服务	审计操作参考文档
	分布式缓存服务	分布式缓存服务支持审计的操作列表
	API网关	API网关支持审计的操作列表
数据库	分布式数据库中间件	分布式数据库中间件支持审计的操作列表
	数据管理服务	数据管理服务支持审计的操作列表
安全	数据加密服务	数据加密服务支持审计的操作列表
	Web应用防火墙	Web应用防火墙支持审计的操作列表
人工智能	AI开发平台	AI开发平台支持审计的操作列表
大数据	MapReduce服务	MapReduce服务支持审计的操作列表
	数据仓库服务 GaussDB	数据仓库服务 GaussDB支持审计的操作列表
	云搜索服务	云搜索服务支持审计的操作列表
CDN与智能边缘	智能边缘平台	智能边缘平台支持审计的操作列表

12 常见问题

12.1 使用 IAM 用户（子账号）在 CTS 配置转储，操作 OBS 桶也必须是 IAM 用户么?

不是，操作OBS桶的用户不区分IAM用户和账号，只需要用户具备操作OBS桶的权限即可。

12.2 用户账户欠费给云审计服务带来的影响?

当用户账户欠费时，云审计服务依旧可以接收所支持服务发送的操作信息，但只能保存近7天的操作记录。因为7天之前的历史操作记录会以事件文件的形式实时保存至OBS桶，而将事件文件存储于OBS桶所产生的流量需要付费。

此时只能对追踪器执行“删除”操作。

12.3 哪些用户应该开通云审计服务?

所有云用户均应该开通云审计服务。

- 从政策、行业规范角度，云审计服务是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分，也是很多行业标准、审计规范的必备组成部分。
- 从应用角度，云审计服务是云资源出现问题时，降低问题定位时间和人力成本的有效手段，能够精确定位到问题发生时的所有操作，借以减小问题排查范围。

12.4 如果用户已开通云审计服务，但 OBS 桶未配置正确的策略，会出现什么情况?

云审计服务会根据既有的OBS存储桶策略来传送事件文件。如果错误地配置OBS存储桶策略，那么云审计服务将无法传送事件文件。

被删除或有异常的OBS桶，管理控制台界面会显示相应的错误提示信息。用户可选择重新创建OBS桶或重新配置OBS桶的访问权限。

12.5 云审计服务是否支持事件文件的完整性校验?

支持。原则上进行完整性校验时必须包含以下字段：time、service_type、resource_type、trace_name、trace_rating、trace_type，其他字段由各服务自己定义。

12.6 为什么查看事件窗口中的有些事件的字段为空?

可以为空的字段有source_ip、code、request、response和message，这些字段并非云审计服务规定的必备字段：

- source_ip：当trace type为SystemAction时，表示本次操作由服务内部触发，此时缺失IP字段为正常情况。
- request/response/code：这三个字段是表示本次操作所对应的请求内容、请求结果及HTTP返回码，在有些情况下，这些字段本身为空，或不具备业务意义，产生该事件的云服务会根据实际情况选择某字段留空。
- message：该字段为预留字段，若其他云服务基于业务需要，需要增加额外信息时，可附加在该字段内，缺失为正常情况。

12.7 为什么事件列表中的某些操作被记录了两次?

对于异步调用事件，会产生两条事件记录，其事件名称、资源类型、资源名称等字段相同。在事件列表中，看起来是重复记录了操作（例如，Workspace的deleteDesktop事件），但实际上，这两条事件是相互关联、但内容不同的两条记录，典型的异步调用场景时间如下：

- 第一条事件：记录用户发起的请求；
- 第二条事件：记录用户请求的操作结果，通常与第一条时间记录有数分钟的延迟，记录用户请求的实际响应结果。

两条事件需要结合在一起，才能反映用户本次操作的真实结果。

12.8 关键操作通知服务支持哪些服务?

云审计服务支持对全部的关键操作发送通知，支持的服务类型包括ECS、EVS、VPC、DEW、IAM和原生OpenStack等，支持的操作类型上包括创建、删除、登录和对原生OpenStack接口等操作。

12.9 CTS 如何长期保存事件文件——转储至 OBS 桶

云审计服务仅保存近7天的事件，可以对追踪器增加OBS转储的相关配置，将事件同步、长期保存至OBS桶。具体操作请参考**配置追踪器**。

12.10 为什么有些 trace_type 为 systemAction 的事件，存在 user 和 source_ip 为空的情况?

trace_type字段的业务意义为标示请求来源，该字段可以是控制台（ConsoleAction）、API网关（ApiCall）及系统内调用（SystemAction）。

系统内调用为非用户触发的操作，例如自动触发的告警、弹性伸缩、定时备份任务以及为完成用户请求产生的系统内部次级调用等，这种情况下，不存在直接触发操作的用户或设备，根据审计的客观性原则，该两个字段为空。

12.11 如何通过云审计服务确认 ECS 的创建用户

问题描述

如果您需要确定一台ECS的创建用户，可以通过CTS记录的事件进行查看。

前提条件

- 已开启云审计服务
- 已开启获取创建的ECS主机的资源ID

操作方法

步骤1 登录云审计控制台。

步骤2 单击左侧导航树的“事件列表”，进入事件列表界面。

步骤3 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” > “事件名称：createServer” > “资源ID：*{ECS主机的资源ID}*”。

步骤4 在过滤结果中，单击事件名称，查看事件详细信息。

user列表示创建该台ECS的用户详情，{"name":"账号名","id":"用户的账号ID","domain"{"name":"IAM用户名","id":"IAM用户ID"}}，如果是账号本身创建的该台ECS，则账号名与IAM用户名，名称相同。

----结束

12.12 如何查询 IAM 用户登录的 IP 地址

问题描述

如果您想查询IAM用户的登录IP地址和登录时间，以确认当前账号是否存在安全风险，可以通过CTS记录的事件进行查看。

前提条件

已开启云审计服务。

操作方法

步骤1 进入云审计服务控制台。

步骤2 选择时间范围，然后在搜索框中依次查询：

“云服务：IAM” > “事件名称：login”。

步骤3 在过滤结果中，单击事件名称，可以查看到具体的事件内容。其中"source_ip"为登录IP，"record_time"为登录时间。

----结束

12.13 为什么创建虚拟机的时候会有两个 deleteMetadata 事件?

由于系统在创建虚拟机的时候需要使用metadata存储临时信息，在创建虚拟机完成后会自动删除该信息，因此会触发两个deleteMetadata信息。

12.14 查询不到事件怎么办?

问题描述

在CTS控制台查询不到事件。

操作方法

步骤1 查看是否已选择正确的时间范围。

步骤2 查看筛选条件是否选择正确。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。

步骤3 以上步骤确认正确后,依然查询不到应有事件,可以提交工单,联系技术工程师为您解决。

----结束

12.15 云审计功能申请打开之后是否可以自助关闭?

云审计服务本身免费,包括开通追踪器、事件跟踪以及7天内事件的存储和检索,只有配置转储等增值服务才会收费,本身没有必要关闭。

如果用户检查需要关闭云审计功能,有以下两种方法:

- 可以在追踪器中将已有追踪器删除或停用,删除或停用后,事件仍可以正常上报。
- 可以在统一身份认证服务IAM中将CTS委托删除,审计服务将无法使用。

12.16 如何给云硬盘添加告警通知?

问题描述

如何给云硬盘的操作添加告警通知。

操作步骤

步骤1 登录云审计控制台。

步骤2 左侧导航栏选择“关键操作通知”，单击“创建关键操作通知”。

步骤3 在“配置操作”模块选择“自定义操作”，依次勾选“EVS > evs”的四个关键操作名称，即可对云硬盘的操作添加告警通知。

----结束

12.17 可以接收重复的事件吗?

云审计服务支持向客户的OBS存储桶交付至少一次订阅事件。在某些情况下，云审计服务可能会多次发送同一事件。因此，客户可能会看到重复的事件。

12.18 CTS 会记录云服务器创建失败的事件吗?

CTS会记录云服务器创建失败的事件。用户进行创建云服务器操作时，这个操作动作和操作结果会上报到CTS中。

工作原理

云审计服务支持审计ECS服务，记录云服务器相关的操作事件，便于日后的查询、审计和回溯。

CTS支持审计的ECS关键操作请参考弹性云服务器支持审计的操作列表，当用户对云服务器进行了增加、删除、修改类型的操作时，ECS服务会自动记录操作动作及操作结果，并按照指定的格式发送事件到云审计服务完成事件归档。云审计服务控制台会保存用户最近7天的操作记录，用户可以在“事件列表”界面进行查看。

操作步骤

步骤1 登录云审计控制台。

步骤2 在“事件列表”界面，时间范围选择“最近1周”。

步骤3 在搜索框中查询创建云服务器操作：“云服务：ECS” > “资源类型：ecs” > “事件名称：createServer”，查看过滤结果。

说明

若要获取最近7天以前的操作记录，则需要到OBS桶中查询转储的事件，在操作记录中，以“createServer”作为关键字检索，找到对应记录。

----结束

13 修订记录

表 13-1

发布日期	修订记录
2024-07-19	第十三次正式发布。 • 支持开启企业项目EPS。 • 新增标签特性。 • 更新追踪器界面。 • 支持KMS加密事件文件。 • 关键操作通知支持高级筛选。
2023-11-30	第十二次正式发布。 • 支持**删除管理类追踪器**。 • **配置管理类追踪器**时，支持设置**跨租户转储授权**、是否压缩、路径按云服务划分、日志转储路径。 • **关键操作通知**界面优化，支持搜索通知、设置列表格式。
2023-10-30	第十一次正式发布。 • 优化资料架构。 • 更新**支持审计的服务及操作列表**。
2023-06-15	第十次正式发布： 补充管理追踪器界面操作图片。
2023-03-30	第九次正式发布： • 调整资料架构。 • 更新**支持审计的服务及操作列表**章节。
2022-01-27	第八次正式发布： 分布式数据库中间件服务。

发布日期	修订记录
2021-10-27	第七次正式发布： 新增数据管理服务。
2020-09-21	第六次正式发布： 新增主机迁移服务。
2019-05-17	第五次正式发布： 新增对象存储服务。
2019-02-20	第四次正式发布： 新增密钥管理服务。
2018-11-15	第三次正式发布： 新增对接存储容灾服务。
2017-08-30	第二次正式发布： ● 新增对接裸金属服务。 ● 新增对接资源模板服务。
2017-06-30	第一次正式发布。